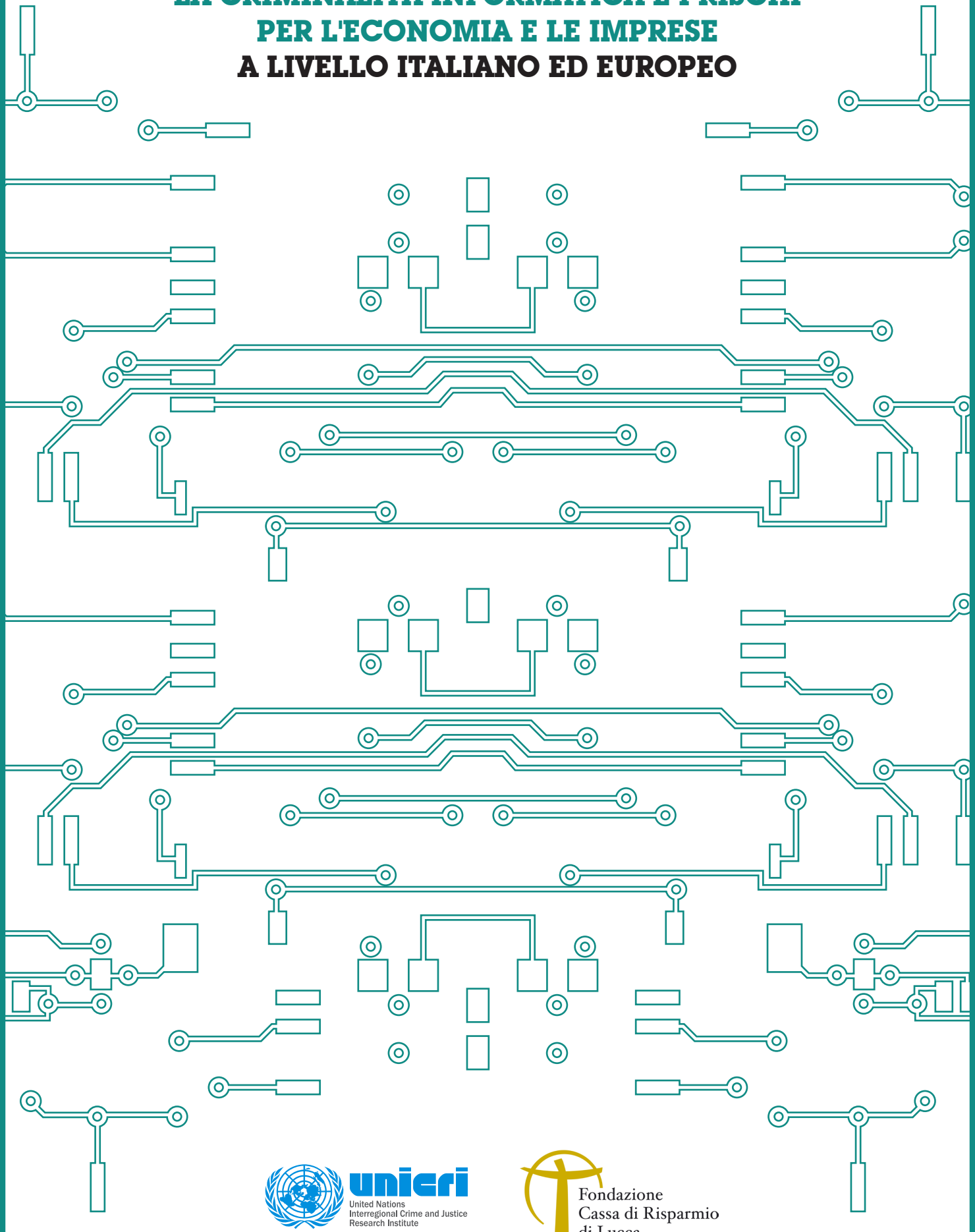
LA CRIMINALITÀ INFORMATICA E I RISCHI PER L'ECONOMIA E LE IMPRESE A LIVELLO ITALIANO ED EUROPEO



unicri
United Nations
Interregional Crime and Justice
Research Institute

Fondazione
Cassa di Risparmio
di Lucca

United Nations
Interregional Crime and Justice
Research Institute

PROGETTO DI RICERCA

La criminalità informatica e i rischi per l'economia e le imprese a livello italiano ed europeo

Il presente studio è stato realizzato dalla Dott.ssa Flavia Zappa.

Disclaimer

Le opinioni espresse nel presente studio rappresentano il punto di vista personale dell'autore e non riflettono necessariamente le posizioni di UNICRI, e in generale delle Nazioni Unite.

Copyright

United Nations Interregional Crime and Justice Research Institute (UNICRI),
Viale Maestri del Lavoro,10
10127 Torino
Italia
Tel 011-6537 111 / Fax 011-6313 368
Sito web: www.unicri.it
E-mail: documentation@unicri.it

“Senza sicurezza, non c'è né privacy, né vera libertà.
Non avete vita privata se la vostra casa non ha pareti;
non si è liberi di camminare per le strade se non è sicuro farlo.”

Neelie KROES, Vice-President of the European Commission
Responsible for the Digital Agenda,
A secure on-line network for Europe,
Cyber security conference Brussels,

28 Febbraio 2014

Prefazione

Negli ultimi anni crimini informatici sono diventati uno dei fenomeni di maggiore diffusione, mettendo in allarme governi, cittadini e settore privato. Violazione dei dati e furti informatici sono in crescita in tutti i settori, colpendo sicurezza e sviluppo nelle società di tutto il mondo.

I crimini informatici non sono più limitati ad attacchi isolati commessi da singoli individui. Negli ultimi anni questa tipologia di crimini si è evoluta fino a diventare un'attività molto proficua e spesso a rischio molto basso per le organizzazioni criminali. L'attuale società sempre più interconnessa è diventata uno sconfinato campo di attività per i criminali che hanno preso di mira in particolar modo settore finanziario e quello di affari.

Gli attacchi informatici implicano imprevedibili perdite economiche e di produttività, ma non si limitano solo a questo tipo di perdite. Le imprese colpite devono farsi carico dei costi della pulizia del malware, investigazione e gestione post-incidente. Talvolta, le imprese rischiano anche di non riprendersi dopo gli attacchi informatici: la perdita dei dati e o il furto dei segreti commerciali può risultare fatale per aziende che dipendono fortemente dalla qualità e segretezza della loro produzione. Molte imprese devono affrontare anche la perdita di credibilità e posizionamento sul mercato.

La concentrazione dei crimini informatici nel settore finanziario delle piccole e medie imprese arriva in un momento delicato, specialmente in Europa, dove le aziende colpite dalla recessione tentano di far fronte alle misure di austerità e ai bassi profitti.

La ricerca si focalizza sull'impatto dei crimini informatici al livello internazionale, nazionale (in Italia) e locale. Le interviste mirate e analisi dei casi di studio sono stati condotti per fornire un'idea sugli strumenti attualmente utilizzati dai criminali, le ragioni più comuni che portano a tali atti criminali, e maggiori rischi e vulnerabilità per le imprese. Le interviste con i rappresentanti delle istituzioni e le aziende hanno aiutato a chiarire i problemi principali e sottolineano la necessità di una strategia coerente per la difesa delle PMI dai crimini informatici.

Le informazioni raccolte nello studio hanno permesso all'UNICRI la messa a punto di una strategia volta alla creazione di una rete di esperti per promuovere la cultura di sicurezza su vari livelli. Questo studio è per noi un punto di partenza: ci impegniamo a crescere e passare dalla comprensione all'iniziativa, dalla conoscenza all'azione.

Jonathan Lucas

Direttore dell'UNICRI

INDICE

RINGRAZIAMENTI

Si ringraziano tutte le persone che hanno contribuito alla realizzazione di questa ricerca fornendo materiale utile e rilasciando interviste preziose per le intuizioni e le osservazioni che hanno permesso. In particolare si ringrazia il Sostituto Procuratore Alberto Perduca e il Sostituto Procuratore Giuseppe Riccaboni della Procura della Repubblica di Torino, il Sostituto Procuratore Andrea Cusani della Procura della Repubblica di Firenze, la dott.ssa Stefania Pierazzi Vice Questore Aggiunto Polizia Postale e delle Telecomunicazioni di Firenze e l'Ispettore Capo di Polizia Franco Bozzi presso la Procura della Repubblica presso il Tribunale di Lucca, per la disponibilità a chiarire gli aspetti giuridico-normativi e procedurali di questo fenomeno. Inoltre si ringrazia la Polizia Postale di Firenze e la Procura della Repubblica di Firenze per i dati fornitici.

Si ringraziano ancora tutte le aziende intervistate: la Giorgini Maggi nella figura di Elena Polacci, l'Industria cartaria Pieretti nelle persone di Tiziano Pieretti, Simone Antonetti e Marino Ninci, la Lucart nelle figure di Franco Pasquini e Alessandro Burresi, la Lucense nella figura di Luca Landucci e la Tagetik nelle persone di Annarita D'Urso, Matteo Fava e Santo Natale.

Un ringraziamento va inoltre al direttore Claudio Romiti e a Daniele Chersi di Assindustria Lucca, Monica Pellegrino di ABI Lab, Veronica Borgogna di Consorzio Bancomat, Domenico Raguseo di IBM, al Sostituto Procuratore Giuseppe Ledda della Procura della Repubblica di Firenze, al dott. Paolo Passeri, all'Osservatorio per le Piccole e Medie Imprese e ad Intesa Sanpaolo, per i dati forniti e la collaborazione dimostrata.

EXECUTIVE SUMMARY

Il cyber crime rappresenta, ad oggi, una delle minacce più insidiose a livello globale, con un incremento su base annua sempre maggiore, e che occorre conoscere in modo approfondito, al fine di mettere in atto valide contromisure. Non è un fenomeno che riguarda solo le grandi imprese, ma sempre più anche quelle di piccole e medie dimensioni. Il suo impatto sull'economia di un Paese è enorme, e dato che il tessuto economico-sociale europeo ed italiano è fortemente rappresentato dalle PMI, scopo di questa ricerca è indagare sul grado di rischio per l'economia e le imprese derivante da questo fenomeno.

La metodologia scelta è di tipo *bottom up*, una ricerca "dal basso" che va ad indagare, attraverso un focus specifico sulla provincia di Lucca ed interviste mirate, sulla reale situazione che le Piccole e Medie Imprese si trovano ogni giorno ad affrontare. Per studiare i rischi che, a livello economico, le PMI corrono a causa di questo fenomeno e fornire le competenze per attuare delle idonee contromisure, si è scelto di interpellare le aziende e le istituzioni vicine ad esse, per capire le loro reali esigenze, la loro relazione e le reazioni ad eventi di cyber crime.

Generalmente la sicurezza informatica è gestita e affrontata con un approccio dall'alto, *top down*, con esperti e specialisti che suggeriscono e implementano varie soluzioni tecniche e best practices da applicare, ma, in questa ricerca, si è scelto di usare una metodologia diversa, proprio in virtù dell'oggetto così specifico, le PMI e degli obiettivi che ci si pone di raggiungere.

Figura 1 - Grafico riassuntivo esplicativo della metodologia utilizzata per la ricerca

Si è scelto, infatti, di indagare proprio sulle caratteristiche e necessità delle PMI, i rischi che si trovano ad affrontare e di cosa hanno bisogno per mettere in atto adeguate contromisure. Il focus sulla provincia di Lucca e sulle sue PMI è, per questo motivo, strumentale a capire i gap esistenti nei confronti della lotta al cyber crime. Si sono svolte inoltre interviste a responsabili di enti istituzionali come Assindustria, Procure e Forze dell'Ordine e aziende private, come ABI Lab, IBM e Consorzio Bancomat. I rappresentanti delle PMI e di associazioni di categoria, infatti, spesso non vengono coinvolti nel processo di implementazione della difesa da queste minacce e si rischia di non mettere in atto soluzioni realmente efficaci.

Per avere un quadro più chiaro del fenomeno cyber crime è opportuno effettuare un'analisi generale del contesto, attraverso lo studio delle principali caratteristiche, attori, strumenti, minacce e tipi di rischi riguardanti le PMI in ambito cyber, analisi che verrà affrontata nel primo capitolo. Il cyber crime è un fenomeno molto vasto e costituisce una tipologia di atto criminoso molto più pericolosa di quella tradizionale, che amplifica le capacità e la pericolosità del soggetto criminale. Il mezzo informatico diventa mezzo per commettere varie tipologie di reato; dal bullismo, alla pedofilia, allo spionaggio industriale ed internazionale.

In questo studio affronteremo l'impatto che il cyber crime ha sull'economia, in riferimento alle PMI, e i relativi rischi e vulnerabilità che rappresenta a livello internazionale come vedremo nel secondo capitolo, e a livello italiano e locale, attraverso un focus sul territorio. Si prenderanno in esame le caratteristiche relative alla dimensione internazionale, europea e nazionale, come si vedrà nel terzo capitolo, del cyber crime, le statistiche di settore più aggiornate e le contromisure messe in atto, realizzando infine nel quarto capitolo un focus sulla Provincia di Lucca, che permetterà di pensare a contromisure ed azioni proattive.

LISTA DEGLI ACRONIMI

ACSC	Advanced Cyber security Center
ADI	Agenda Digitale Italiana
AgID	Agenzia per l'Italia Digitale
AISE	Agenzia Informazioni Sicurezza Esterna
AISI	Agenzia Informazioni Sicurezza Interna
ANR	Autorità Nazionali di Regolamentazione
APP	Application
ATM	Automatic Teller Machine
BI	Business Intelligence
BMBF	Bundesministerium für Bildung und Forschung
BYOD	Bring Your Own Device
CDA	Consiglio di Amministrazione
CEPOL	European Police College
CERT	Computer Emergency Response Team
CERT –EU	Computer Emergency Response Team of European Union
CERT –PA	Computer Emergency Response Team Pubblica Amministrazione
CISP	Cyber security Information Sharing Partnership
CISR	Comitato Interministeriale per la Sicurezza della Repubblica
CNAICIP	Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche
CNCPO	Centro Nazionale per il Contrasto alla Pedofilia On-line
CNP	Card Not Present
COPASIR	Comitato Parlamentare per la Sicurezza della Repubblica
CP	Codice Penale
CPM	Corporate Performance Management
CSES	Center for Strategy & Evaluation Services
DDoS	Distributed Denial of Service
DIS	Dipartimento Informazioni per la Sicurezza
DoS	Denial of Service
EAST	European ATM Security Team
EC3	European Cybercrime Centre
ECI	European Critical Infrastructure
ECTEG	European Cybercrime Training and Education Group
EFTA	European Free Trade Association

EISAS	European Information Sharing and Alert System
ENISA	European Network and Information Security Agency
ERP	Enterprise resource planning
EU	European Union
EUCTF	European Union Cyber-crime Task Force
EUROPOL	European Police Office
FBI	Federal Bureau of Investigation
FSP	Federation of Small Businesses
GDF	Guardia di Finanza
GPRS	General Packet Radio Service
GPS	Global Positioning System
IBAN	International Bank Account Number
IC	Infrastruttura Critica
IC3	Internet Crime Complaint Center
ICT	Information and Communication Technology
iOCTA	The Internet Organised Crime Threat Assessment
IOT	Internet of Things
IP	Internet Protocol address
ISCOM	Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione
ISP	Internet Service Provider
IT	Information Technology
J-CAT	Joint Cybercrime Action Taskforce
MISE	Ministero dello Sviluppo Economico
MTA	Metropolitan Transportation Authority
NCA	National Crime Agency
NIS	Network and Information Security
NYPD	New York Police Department
ONG	Organizzazioni Non Governative
OPMI	Osservatorio Piccole e Medie Imprese
OSINT	Open Source Intelligence
PA	Pubblica Amministrazione
PC	Personal Computer
PDF	Portable Document Format
PEBKAC	Problem Exists Between Keyboard and Chair

PIL	Prodotto Interno Lordo
PMI	Piccole e Medie Imprese
POS	Point of Sale
ROI	Return on Investment
SBA	Small Business Act
SCADA	Supervisory Control And Data Acquisition
SIEM	Security Information and Event Management
SIMU	SIEM für Klein und Mittelständische Unternehmen
SIPAF	Sistema Informatizzato Prevenzione Amministrativa Frodi Carte di Pagamento
SMS	Short Message Service
SO	Sistema Operativo
TIC	Tecnologie dell'Informazione e della Comunicazione
TOR	The Onion Router
USB	Universal Serial Bus
VPN	Virtual Private Network
WEF	World Economic Forum
WEP	Wired Equivalent Privacy
WPA e WPA2	WI-FI Protected Access

CAPITOLO 1

L'IMPORTANZA DELLE PMI E IL CYBER CRIME COME MINACCIA ALL'ECONOMIA

1.1 La necessità di un focus sulle Piccole e Medie Imprese (PMI)

In questi ultimi anni il cyber crime sta ricoprendo un ruolo sempre maggiore tra i rischi che cittadini, imprese e Governi si trovano ad affrontare. L'attenzione mediatica però è spesso focalizzata sugli eventi che riguardano Governi e multinazionali, e spesso non si tiene nella giusta considerazione l'impatto che questo fenomeno ha sull'economia, soprattutto delle Piccole e Medie Imprese (PMI).

Le PMI costituiscono il fulcro del tessuto sociale italiano ed europeo e l'importanza che esse ricoprono è fondamentale sia a livello economico sia per la sicurezza globale. Le PMI e i cittadini infatti costituiscono la maggior parte delle vittime di attacchi informatici mirati.[1]

Per PMI si intendono imprese con meno di 250 dipendenti[2] e con un fatturato o totale di bilancio inferiore rispettivamente ai 50 milioni di euro e ai 43 milioni di euro[3]. All'interno della categoria delle PMI vengono ulteriormente differenziate le piccole e micro imprese. Rispettivamente si intende per piccola impresa quella che occupa meno di 50 persone e realizza un fatturato annuo o un totale di bilancio annuo non superiore a 10 milioni di euro e per microimpresa quella che occupa meno di 10 persone e realizza un fatturato annuo oppure un totale di bilancio annuo che non superi i 2 milioni di euro.

---

[1] *EISAS – European Information Sharing and Alert System A Feasibility Study 2006/2007*, in <http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/files/EISAS_finalreport.pdf> (ultima consultazione 1-11-2014).

[2] In USA per PMI si intendono imprese con meno di 500 dipendenti. Per approfondimenti si veda: *La nuova definizione di PMI Guida dell'utente e modello di dichiarazione. Pubblicazioni della direzione generale per le imprese e l'industria* 2006, in <http://ec.europa.eu/enterprise/policies/sme/files/sme_definition/sme_user_guide_it.pdf> (ultima consultazione 1-11-2014).

[3] Queste soglie si applicano solo ai dati relativi ad imprese autonome. Un'impresa appartenente ad un gruppo più grande può essere tenuta ad includere anche i dati relativi agli effettivi, al fatturato e al totale di bilancio del gruppo. *Raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese, testo integrale dell'atto* [Gazzetta ufficiale L 124 del 20.05.2003], in <http://europa.eu/legislation_summaries/enterprise/business_environment/n26026_it.htm> (ultima consultazione 1-11-2014).

Categoria Impresa	Numero Dipendenti	Massimale Finanziario	
		Fatturato	O Totale di Bilancio
PMI	< 250	≤ € 50 Milioni	≤ € 43 Milioni
Piccole	< 50	≤ € 10 Milioni	≤ € 10 Milioni
Micro	< 10	≤ € 2 Milioni	≤ € 2 Milioni

Tabella 1 - Definizione di Piccole e Medie Imprese nell'Unione Europea
Fonte: Elaborazione da Evaluation of the SME Definition, CSES, 2012[4]

Il ruolo che le PMI svolgono all'interno dell'economia europea è davvero rilevante ed esse rappresentano un considerevole numero tra gli utenti di internet. Si stima infatti che le PMI costituiscano il 99,8% della totalità delle imprese nel territorio europeo[5] impiegando 86,8 milioni di persone, pari al 66,5% della forza lavoro, e producendo più della metà del fatturato totale delle imprese europee.

Le PMI in Europa inoltre sono rappresentate per lo più da micro imprese. Si consideri infatti che delle oltre 20 milioni delle PMI europee, il 92,1 % è costituito da micro imprese che sommate alle piccole rappresentano oltre il 50% dei posti di lavoro per i cittadini europei.

	Numero di Imprese		Dipendenti		Valore Aggiunto al Costo dei Fattori	
	Numero	%	Numero	%	Milioni €	%
Micro	18.783.480	92,10%	37.494.458	28,70%	1.242.724	21,10%
Piccole	1.349.730	6,60%	26.704.352	20,50%	1.076.388	18,30%
Medie	222.628	1,10%	22.615.906	17,30%	1.076.270	18,30%
PMI	20.355.839	99,80%	86.814.717	66,50%	3.395.383	57,60%
Grandi	43.454	0,20%	43.787.013	33,50%	2.495.926	42,40%
Totale	**20.399.291**	**100,00%**	**130.601.730**	**100,00%**	**5.891.309**	**100,00%**

Tabella 2 - Dati relativi alle Piccole e Medie Imprese nell'Unione Europea nel 2013
Fonte: Eurostat, National Statistical Offices, DIW, DIW econ, London Economics, 2013

Considerare le PMI come fulcro dell'economia europea solo per la loro numerosità e per l'occupazione che ne deriva è riduttivo, in quanto esse sono spesso portatrici di innovazione in tutti i campi che ricoprono e strategiche per la competitività del mercato imprenditoriale.

[4] *Evaluation of the SME Definition September 2012*, Final Report Framework, Center for Strategy & Evaluation Services, in <http://ec.europa.eu/enterprise/policies/sme/files/studies/evaluation-sme-definition_en.pdf> (ultima consultazione 6-11-2014).

[5] *A recovery on the horizon? Annual Report on European SMEs 2012/2013*. European Commission, in <http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/performance-review/files/supporting-documents/2013/annual-report-smes-2013_en.pdf> (ultima consultazione 11-11-2014).

Nonostante siano più fragili rispetto alle grandi imprese nei confronti delle imperfezioni del mercato e necessitino di maggior tutela e sostegno per lo sviluppo, tra il 2003 e il 2010 il numero di PMI in Europa è cresciuto di quasi l'11%, fino a raggiungere circa i 21 milioni e il numero di persone impiegate da parte delle PMI è aumentato di 7,5 milioni (circa il 6%).

Nel 2008 le PMI hanno dimostrato di essere, in ambito occupazionale, molto più resistenti alla crisi rispetto alle grandi imprese, anche se successivamente, il periodo 2010-2012 si è rivelato piuttosto impegnativo. A livello di UE27, l'occupazione relativa alle PMI è relativamente stabile e le previsioni di crescita occupazionale e di valore aggiunto sono moderatamente ottimistiche. È previsto che il livello di occupazione delle PMI nel 2014 ritorni ai livelli positivi del 2008.[6]

All'interno dell'Unione Europea il più grande settore, per numero di imprese, per quanto attiene le PMI è quello italiano, rappresentato attualmente da quasi 3,7 milioni di imprese, pari a più del 18% del totale europeo[7].

	Numero di Imprese		Dipendenti		Valore Aggiunto al Costo dei Fattori	
	Numero	**%**	**Numero**	**%**	**Milioni €**	**%**
Micro	3.491.826	94,40%	6.930.947	46,10%	185.000	29,80%
Piccole	183.196	5,00%	3.236.764	21,50%	136.000	21,90%
Medie	19.265	0,50%	1.861.089	12,40%	101.000	16,30%
PMI	3.694.288	99,90%	12.028.799	80,00%	420.000	68,00%
Grandi	3.196	0,10%	3.013.012	20,00%	198.000	32,00%
Totale	**3.697.484**	**100,00%**	**15.041.812**	**100,00%**	**620.000**	**100,00%**

Tabella 3 - Dati relativi alle Piccole e Medie Imprese in Italia nel 2013

Fonte: Enterprise and Industry Italy SBA Fact Sheet, European Commission, 2013

L'Italia si conferma la patria delle PMI, con il 99,9% della totalità delle aziende composto da Piccole e Medie Imprese. Il nostro sistema industriale si fonda su una costellazione di piccolissime aziende, spesso familiari, specializzate nel settore manifatturiero, tipico del *Made in Italy*, come la moda, l'arredamento, il settore alimentare e quello meccanico, con oltre 200 distretti industriali[8], che spesso rappresentano l'eccellenza a livello mondiale[9]. Il 68% della ricchezza italiana è prodotto dai 12 milioni di persone che lavorano in una Piccola o Media Impresa.

[6] *Annual report SMEs 2013 Source: Eurostat, National Statistical Offices, DIW, DIW econ, London Economics*, in <http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/performance-review/files/supporting-documents/2013/annual-report-smes-2013_en.pdf> (ultima consultazione 6-11-2014).

[7] *Enterprise and Industry 2013 SBA Fact Sheet ITALY*, in <http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/performance-review/files/countries-sheets/2013/italy_en.pdf> (ultima consultazione 6-11-2014).

[8] Quadrio Curzio A. e Fortis M. (2002, a cura di), *Complessità e Distretti Industriali. Dinamiche, Modelli, Casi reali*, Il Mulino, Bologna.

[9] Fenomeno del tutto assente, in simili proporzioni, negli altri Paesi maggiormente industrializzati.

Le micro imprese in Italia, che rappresentano il 94,4% del totale, hanno un peso del 46,1% in termini di occupazione contro il 21% della Germania, il 22% della Francia e il 27% della Gran Bretagna.[10]

Nonostante questi dati, solitamente, l'attenzione riguardo i casi di cyber crime in ambito aziendale è spesso rivolta a quegli eventi che coinvolgono grandi aziende come Sony, Google, Amazon, Twitter, ecc., e non verso le PMI che, come abbiamo visto, ricoprono invece un'importanza strategica nell'economia europea e soprattutto italiana, di conseguenza la percezione del rischio si abbassa e con esso il livello di guardia. Di contro, però, i costi per la sicurezza informatica, anche per misure base, sono, in percentuale, più elevati per le PMI rispetto alle grandi imprese.

Dato l'enorme contributo delle PMI alla crescita economica e alla creazione di posti di lavoro è necessario un costante supporto da parte degli Stati Membri e della Comunità europea. Le politiche europee adottate all'interno dello Small Business Act (SBA)[11] mirano proprio a migliorare le condizioni di crescita delle PMI ed a mitigare gli effetti della crisi economica con politiche a loro favore e incentivando la crescita occupazionale all'interno dell'Unione Europea.

Tuttavia le PMI stanno sostenendo il peso della crisi economica meglio delle grandi imprese. Ciò richiede un elevato impegno nella definizione di politiche a supporto di una maggiore spinta alla ripresa economica. Oltre alle politiche di sostegno, riguardanti le condizioni di acceso a finanziamenti, il mercato del lavoro, lo snellimento della burocrazia, è strategico il supporto allo sviluppo con progetti mirati anche in ambito tecnologico e politiche di tutela dalle minacce cyber, in quanto le aziende, con infrastrutture moderne, settori tecnologicamente avanzati e manodopera altamente qualificata, sono più competitive e riescono a recuperare molto più velocemente i livelli di rendimento precedenti alla crisi.

In un momento di incertezza economica, come quello attuale, le imprese più piccole non hanno sufficiente disponibilità economica da poter investire in una maggiore difesa informatica. Anche se la violazione dei propri sistemi comporterebbe perdite maggiori rispetto all'investimento iniziale necessario ad impedirla, non sempre le aziende sono in grado di affrontare questa spesa, anche se in molti casi un sensibile aumento della propria sicurezza sarebbe possibile con un minimo investimento.

Le piccole imprese sono diventate un bersaglio appetibile per gli aggressori informatici a causa delle loro protezioni deboli e insufficienti; il fatto che un'impresa sia piccola non necessariamente significa che sarà difficilmente attaccata, anzi, gli hacker possono attaccare migliaia di piccole imprese simultaneamente, utilizzando le vulnerabilità dei software e degli strumenti prima riservati alle grandi aziende[12], ma che ora possono essere facilmente acquistate e vendute su internet. Un aspetto da non sottovalutare è che, dato il crescente impegno economico

[10] Ricciardi Antonio (2010), *Le Pmi localizzate nei distretti industriali: vantaggi competitivi, evoluzione organizzativa, prospettive future*, in Quaderni di ricerca sull'artigianato N°54 Rivista di Economia, Cultura e Ricerca sociale dell'Associazione Artigiani e Piccole Imprese Mestre CGIA A cura del Centro Studi Sintesi, in <http://www.quaderniartigianato.com/wp-content/uploads/2011/05/Quaderni-N%C2%B054.pdf> (ultima consultazione 11-11-2014).

[11] *"Think Small First" A "Small Business Act" for Europe*, Commission of the European Communities, Brussels, 25-6-2008, in <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0394:FIN:EN:PDF> (ultima consultazione 6-11-2014).

nella *cyber security* delle grandi imprese, i criminali spostano i loro tentativi di attacco verso le PMI come veicolo per colpire imprese più grandi e meglio difese, quindi esse svolgono un ruolo cruciale anche nella difesa dell'intero sistema industriale. Piccoli fornitori e appaltatori diventano così l'anello debole e un vasto mercato, sfruttabile dai cyber criminali, nelle reti delle imprese di maggiori dimensioni. Nel caso Target[13], infatti, la falla che ha permesso la violazione dei sistemi è stata rintracciata in un fornitore. La società ha ammesso che gli hacker hanno utilizzato le credenziali di un venditore per accedere al sistema e sottrarre 40 milioni di numeri di carte di credito e 70 milioni di account degli utenti, con una perdita stimata del 5,3%.

I dati dei clienti presenti sui server di una società possono essere utilizzati per accedere ad un altro servizio, ad esempio, quando i criminali informatici hanno cercato di attaccare Yahoo Mail, Yahoo ha dichiarato che l'elenco di nomi utente e password era stato probabilmente ottenuto da un database di terze parti compromesso dagli hacker.

I rischi che corrono le PMI sono molteplici e spaziano dalla perdita di proprietà intellettuale ed esposizione di dati sensibili, alla perdita di competitività e di posti di lavoro, senza considerare i costi concernenti la distruzione di servizi e i danni d'immagine e alla reputazione aziendale. I costi da sostenere vanno dagli indennizzi da corrispondere ai clienti in caso di violazione dei dati (o derivanti da penalità da contratto) ad essi relativi, ai costi in contromisure e assicurazioni ai costi per l'implementazione di strategie di mitigazione dei rischi e di *recovery* in caso d'incidente.

1.2 Il cyber crime come minaccia per le PMI

Il cyber crime è uno dei temi di maggior interesse degli ultimi dieci anni ed è considerato una delle minacce più serie a livello mondiale. Ogni aspetto della vita quotidiana privata e lavorativa ormai è altamente informatizzato. Tutte le economie mondiali utilizzano la stessa infrastruttura di base, gli stessi software, hardware e standard, con miliardi di dispositivi connessi.[14]

---

[12] Michael Fey ha dichiarato che le imprese di piccole dimensioni sono attaccate perché spesso non mantengono il loro software aggiornato, o mantengono traccia dei loro dati finanziari. *McAfee CTO: Cyber Criminals Target SME's,* Febbraio 2014, di Kevin Wright, in <http://www.itgovernance.co.uk/blog/mcafee-cto-cyber-criminals-target-smes/> (ultima consultazione 6-11-2014).

[13] La catena di grandi magazzini USA ha subito a fine 2013 il furto di dati sensibili relativi a 40 milioni di carte di credito dei propri clienti. Per approfondimenti si veda: *Clonati 40 milioni di carte di credito, i grandi magazzini Target si fanno perdonare con uno sconto del 10% sulla spesa*, 21-12-2013 Il Sole 24 Ore, in <http://www.ilsole24ore.com/art/tecnologie/2013-12-21/clonati-40-milioni-carte-credito-target-si-fa-perdonare-uno-sconto-10percento-spesa-165410.shtml?uuid=ABj2HVl> e *Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores,* 19-12-2013, target Pressroom, in <http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores> (ultima consultazione 7-11-2014).

[14] Rod Beckstrom: *"Anything connected to the Internet can be hacked. Everything is being connected to the Internet So everything is becoming vulnerable and a new dynamic of cybercrimes countered by security measures, countered by new criminal efforts, and so forth, is now unleashed"*, London Conference on Cyberspace, 2 November 2011, in <https://www.icann.org/en/system/files/files/beckstrom-speech-cybersecurity-london-02nov11-en.pdf> (ultima consultazione 7-11-2014).

I rischi legati al *cyber space* sono considerati, secondo una recente ricerca del World Economic Forum (WEF), come tra i maggiori rischi percepiti in termini di impatto e probabilità di verificarsi[15], come si può osservare dalla Figura 2.

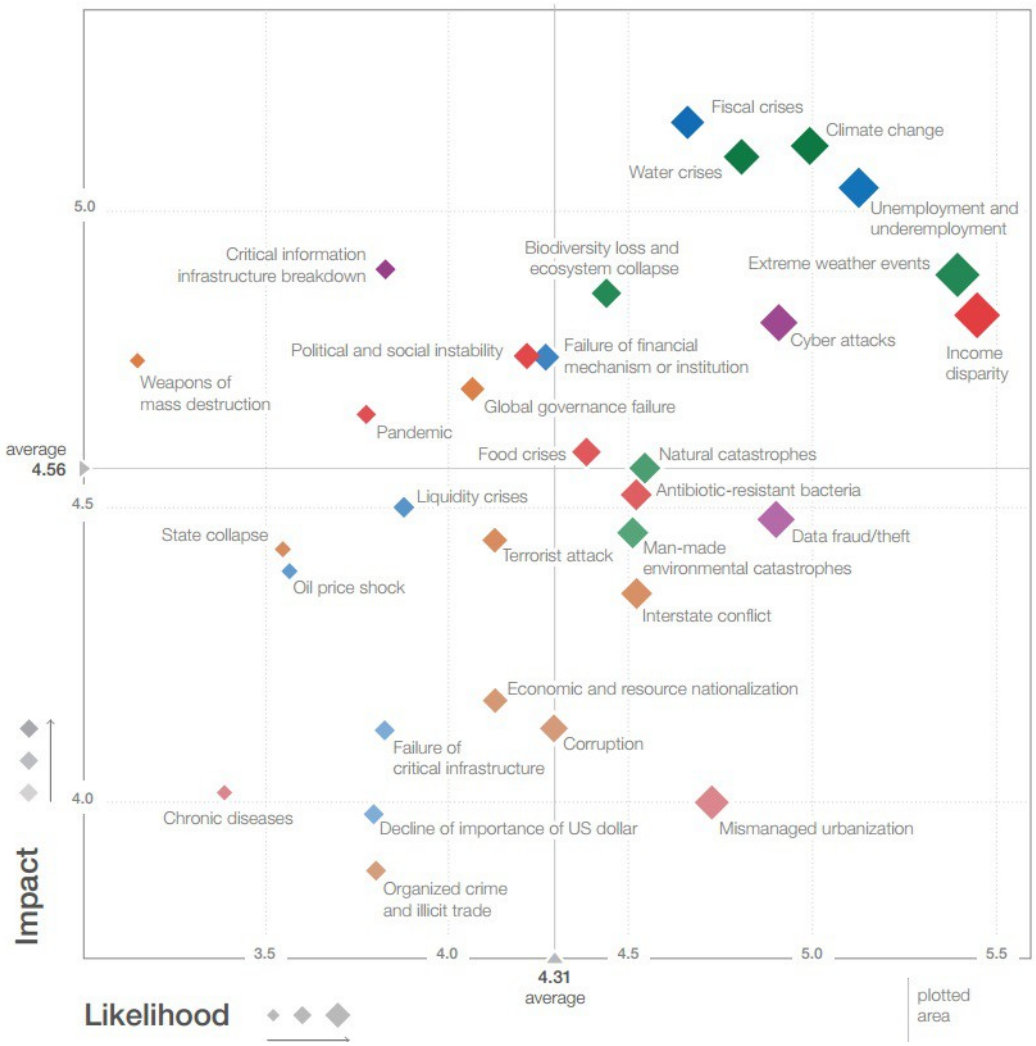


Figura 2 - The Global Risks Landscape 2014

Fonte: Global risks Ninth edition, World Economic Forum, 2014

Il rapporto, inoltre, evidenzia come, da qui al 2020, se le imprese e i Governi non svilupperanno politiche di difesa adeguate e in tempi brevi, le perdite economiche causate dai cyber attacchi potrebbero arrivare fino a 3 mila miliardi di dollari.[16]

Il WEF ha spesso evidenziato come l'interdipendenza dei sistemi informatici introduca nuove vulnerabilità e nuove falle con conseguenze imprevedibili, sottolineando l'impatto macroeconomico dei rischi informatici anche in termini di crescita di PIL. Il WEF enfatizza molto, nel suo ultimo rapporto, la delicatezza di questo tema che, se non affrontato tempestivamente e preso in considerazione da tutti gli *stakeholders*, Governi, aziende e società civile, potrebbe

[15] Il rapporto è stato redatto sulla base delle interviste ad oltre 250 fra esperti e dirigenti d'azienda.

[16] World Economic Forum - Global risks 2014 Ninth edition, in <http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf> (ultima consultazione 6-11-2014).

portare a conseguenze gravi e ad uno scenario in cui internet potrebbe subire la sfiducia degli utenti e non essere più uno strumento libero e una risorsa per l'economia e la libera informazione.

Nonostante ciò, non esiste ancora una definizione giuridicamente condivisa a livello internazionale, principalmente a causa delle differenze nella legislazione dei vari Stati[17], che determini il cyber crime in maniera consistente ed esaustiva; questo comporta ulteriori difficoltà in ambito internazionale per la costruzione di una risposta concertata. Il *Commonwealth of Independent States Agreement*, per esempio, senza usare esplicitamente il termine cyber crime, definisce i reati perpetrati attraverso il mezzo informatico come "criminal *act of which the target is computer information*" e lo *Shanghai Cooperation Organization Agreement* invece definisce gli attacchi informatici come "*the use of information resources and (or) the impact on them in the informational sphere for illegal purposes*."[18]

Ad ogni modo possiamo genericamente definire il cyber crime come l'insieme delle operazioni illegali che avvengono su internet. La criminalità informatica infatti non è da considerarsi un fenomeno alieno o differente dalla criminalità che siamo abituati ad affrontare, ma semplicemente il crimine perpetrato con altri mezzi, attraverso il *cyber space* appunto, e di sicuro un metodo che sta rivoluzionando i reati tradizionali rendendoli più facili ed economici da attuare e per questo maggiormente efficaci. L'aspetto più caratteristico di questo fenomeno, e che lo differenzia dalla criminalità tradizionale, è sicuramente il fatto di non avere confini fisici e non considerare le distanze geografiche. In più, il fatto di poter essere perpetrato da qualsiasi parte del Pianeta, senza alcun tipo di contatto umano, rende più facile la sua realizzazione, annullando di fatto la percezione delle conseguenze dell'atto criminoso. Appare sempre più attuale in riferimento al processo tecnologico il concetto di Buckminster Fuller che esplorò e propose, ormai più di 70 anni fa, il principio dell'"efemeralizzazione" ovvero "fare di più con meno"[19]. Il cyber crime si stima infatti che abbia un ROI molto elevato. A differenza di quello che è lo spazio internet per i comuni utenti, i criminali sfruttano spazi non rintracciabili attraverso motori di ricerca e non facilmente accessibili, comunemente chiamati "*deep web*".

Ma cos'è di preciso il *deep web*? Altro non è che il web sommerso, invisibile ai normali utenti e con i programmi tradizionali. Come è facile immaginare è molto difficile fare una statistica veritiera della dimensione del *deep web*, ma molti esperti concordano nell'affermare che è centinaia di volte più vasto dell'internet che siamo abituati a frequentare. Nel pensiero comune, il *deep web* viene associato esclusivamente a traffici illegali, attività criminose ed illecite, ma in realtà non è solo il nascondiglio per criminali e traffici illeciti. Sono sempre di più le ONG, i dissidenti politici e i blogger che usano il *deep web* come risorsa, in cerca di informazioni o di uno spazio in cui esprimere opinioni, incontrarsi, scambiarsi dati e sostenere "giuste cause" tentando di sfuggire a censura e controlli. Frank La Rue, inviato speciale dell'Onu per la libertà

[17] Spesso risalenti al XIX secolo.

[18] Commonwealth of Independent States Agreement, Art. 1(a) e Shanghai Cooperation Organization Agreement, Annex 1, in *Comprehensive Study on Cybercrime,* UNODC, Febbraio 2013, in <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf> (ultima consultazione 15-11-2014).

[19] Gori Umberto (2012) "*Riflessioni propedeutiche alla cyber intelligence"* in "*Information Warfare 2011. La sfida della Cyber Intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale"* a cura di Umberto Gori e Luigi Sergio Germani. Franco Angeli.

d'espressione, ha chiarito davanti all'assemblea delle Nazioni Unite che "*l'anonimato e la comunicazione sicura sono cruciali per una società aperta e democratica*"[20]. Anche Edward Snowden e gli attivisti della Primavera Araba hanno usato il *deep web* per diffondere documenti riservati che denunciavano azioni illegali da parte dei Governi. I documenti pubblicati da Julian Assange su Wikileaks ad esempio sono stati recuperati attraverso il *deep web*. Vi sono anche numerosi negozi virtuali come il famoso Silk Road, dove si vendono droga, armi e documenti falsi, che poi vengono consegnati a domicilio in maniera anonima. L'FBI stima che Silk Road abbia effettuato tra febbraio 2011 e luglio 2013 transazioni finanziarie per 1,2 miliardi di dollari, guadagnando 80 milioni di dollari di commissioni.[21] In seguito il sito è stato chiuso dall'FBI, ma ha riaperto ad un altro indirizzo. Anche le mafie tradizionali ricorrono ai negozi del *deep web* per condurre i loro traffici, confermando che la criminalità informatica non è un nuovo tipo di criminalità, ma una nuova via per perpetrare i crimini tradizionali. I siti del *deep web* non sono raggiungibili con i normali browser (i programmi per navigare su internet, come Internet Explorer, Firefox o Safari) perché le loro pagine non sono indicizzate dai motori di ricerca come Google o Bing, anzi, l'accesso ai motori di ricerca e alla navigazione tramite i classici link è inibita, inoltre tipicamente gli indirizzi dai quali si possono raggiungere i siti ospitati nel *deep web* cambiano molto velocemente. Nel *deep web* si trovano anche siti accessibili solo attraverso Virtual Private Network (VPN), cioè collegamenti diretti e criptati tra due computer. Il modo più semplice per navigare nel *deep web*, è attraverso una connessione sicura, per la quale occorre *The Onion Router* (TOR), un software, creato per permettere la navigazione nei Paesi dove internet è soggetto a censura, che crittografa i dati di navigazione facendo passare la comunicazione attraverso diversi *proxy* o nodi, modificando di volta in volta l'indirizzo IP con il quale si accede ad una pagina, creando una sorta di catena dalla quale è difficile risalire alla reale posizione geografica dell'utente. Non esistendo, o meglio, essendo molto limitati, i motori di ricerca all'interno del *deep web*, la navigazione è pressoché "a vista" e molti siti sono visitabili solo dietro invito di qualche membro dello staff o delle *community* che hanno già l'accesso. Tra i più famosi motori di ricerca possiamo trovare HiddenWiki, che colleziona link di siti forniti dagli utenti. Il commercio illegale all'interno del *deep web* si basa, per la maggior parte, sull'utilizzo del Bitcoin come valuta, attraverso la quale vengono acquistati e venduti cocaina, armi e materiale pornografico, ed essendo una valuta virtuale e crittografata, permette l'anonimato sia dell'acquirente sia del venditore, ed è la moneta di scambio ideale per questo tipo di traffici.

Il cyber crime costituisce senza dubbio un pericolo in continua ascesa. Secondo uno studio condotto dal Ponemon Institute[22], infatti, il costo del cyber crime è cresciuto del 78% rispetto al 2009, ma il dato più preoccupante riguarda il tempo necessario per la risoluzione di un problema,

[20] *Tutti i segreti del deep web*, Arturo di Corinto, Repubblica.it, in <http://www.repubblica.it/tecnologia/2014/04/20/news/tutti_i_segreti_del_deep_web-84053410/> (ultima consultazione 11-11-2014).

[21] *Feds Arrest Alleged 'Dread Pirate Roberts,' the Brain Behind the Silk Road Drug Site,* di Kim Zetter in Wired 10/2/2013, in <http://www.wired.com/2013/10/silk-road-raided/> (ultima consultazione 6-11-2014).

[22] *The 2013 Cost of Cybercrime Study*, Sponsored by HP Enterprise Security Independently conducted by Ponemon Institute, Ottobre 2013, in <http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf> (ultima consultazione 6-11-2014).

che è aumentato del 130% nello stesso arco temporale. Il furto di dati è la causa delle maggiori perdite, circa il 43% dei costi totali imputabili al cyber crime, mentre danni al business e di perdita di competitività incidono per il 36%.

Secondo il rapporto Symantec 2014[23], il 2013 è stato l'anno delle *mega breach*, in quanto il numero totale delle violazioni di dati[24] è aumentato del 62% rispetto all'anno precedente, ma soprattutto ci sono stati ben otto casi di violazioni che hanno riguardato oltre 10 milioni di utenti, con un numero complessivo annuo di identità violate che supera i 550 milioni di individui (+493% rispetto al 2012).

Il cyber crime complessivamente ha un volume d'affari, sottostimato, di 12 miliardi di dollari annui[25] e il costo in Europa della criminalità informatica, inoltre, è calcolato in oltre 750 miliardi di euro[26] all'anno tra perdite dirette, perdite di tempo, perdita di opportunità di business e di spese per riparare i danni. A questo vanno aggiunti i danni di immagine che hanno effetti che durano per un tempo di gran lunga superiore.[27]

Le minacce derivanti dal *cyber space* sono, senza dubbio, le più strategiche che il mondo contemporaneo si trovi ad affrontare. Gli strumenti utilizzati nel *cyber space* non sono fisici, ma i loro effetti sono imprevedibili e pericolosi. Uno di questi è proprio la difficoltà di prevedere quando l'attacco informatico lanciato avrà successo, come si diffonde e come può evolversi nel tempo. Questo evidenzia un aspetto inquietante, lo strumento informatico ha in sé molteplici effetti collaterali, potrebbe colpire in modo imprevedibile altri sistemi o reti che non sono considerati bersagli, addirittura l'attaccante stesso. Laddove è più diffusa la gestione telematica delle aziende si insidiano le maggiori vulnerabilità in tema di *cyber security*. Le aziende tecnologicamente più avanzate, condizione imprescindibile per mantenersi competitivi nel mercato globale, sono gli obiettivi maggiormente attaccabili. Internet, social network e home banking vengono usati in modo sempre più diffuso, sia in ambito privato sia in ambito lavorativo.

È importante conoscere questo fenomeno in continua evoluzione nel tempo; l'hacker romantico, infatti, legato al nostro immaginario cinematografico, che aveva il gusto per la sfida come spinta motivazionale alle sue azioni, lascia il posto alla criminalità organizzata ed a una molteplicità di attori con motivazioni diverse. Questa situazione si aggrava in maniera

---

[23] *Internet Security Threath Report 2014*, Symantec, Volume 19, Published April 2014, in <http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf> (ultima consultazione 7-11-014).

[24] Dati riguardanti numeri di carte di credito, nomi, date di nascita, login, password, carta d'identità, indirizzi, assicurazione medica, numeri di telefono, informazioni finanziarie, e-mail, ecc.

[25] INTERPOL speech Opening remarks by INTERPOL President Khoo Boon Hui at the 41ST European Regional Conference. Israele, Tel Aviv 8-5-2012, in <http://www.Interpol.int/content/download/14086/99246/version/1/file/41ERC-Khoo-Opening-Speech.pdf> (ultima consultazione 6-11-2014).

[26] *Interpol Ups The War Against Cyber Crime* di Daniella Cheslow, Huffingtonpost 05-08-2012, in <http://www.huffingtonpost.com/2012/05/08/Interpol-cyber-crime_n_1499734.html> (ultima consultazione 6-11-2014).

[27] Si veda per esempio il Caso Sony. *Anonymous Engages in Sony DDoS Attacks Over GeoHot PS3 Lawsuit*, di Jason Mick, in <http://www.dailytech.com/Anonymous+Engages+in+Sony+DDoS+Attacks+Over+GeoHot+PS3+Lawsuit/article21282.htm> (ultima consultazione 6-11-2014).

esponenziale e sempre più rapidamente. Oggi il confine che differenzia queste minacce è davvero labile.

Inizialmente, le minacce informatiche erano prevalentemente virus, worm e trojan, ma con il tempo hanno cominciato a comprendere tecniche legate al *social engineering*, quali il phishing mirato diretto a dipendenti che hanno accesso a database contenenti informazioni aziendali riservate, e si sono aggiunti altri come il pharming, frodi con carta di credito, attacchi DDoS, furto d'identità e furto di dati. Secondo Special Eurobarometer, commissionato dall'Unione Europea,[28] la maggior parte degli utenti di internet in tutta l'UE non si sente completamente sicuro riguardo la propria capacità di fare acquisti on-line o di usare l'on-line banking e non hanno idea di come navigare in sicurezza. Molti affermano di conoscere il fenomeno della criminalità informatica dai giornali o dalla tv ma non si sentono molto informati riguardo i rischi in cui si può incorrere. La poca consapevolezza della propria vulnerabilità da parte dell'utente è ovviamente uno degli aspetti più sfruttati dal cyber crime e ne determina la facilità di realizzazione.

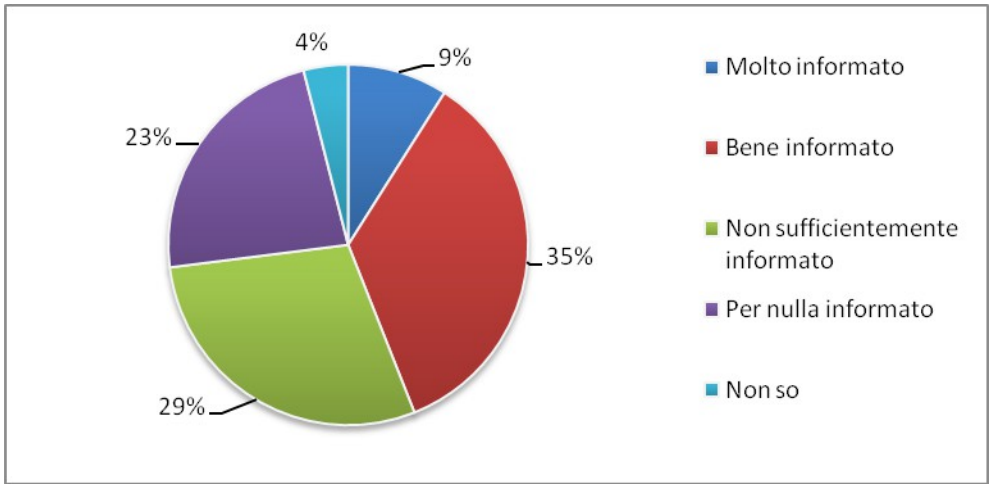


Figura 3 - Statistiche sul livello percepito di informazione dei cittadini europei riguardo il cyber crime, maggio-giugno 2013, UE27

Fonte: Speciale Eurobarometro 404 Cyber security Report, 2013

Inoltre, più di un terzo degli utenti, afferma di aver ricevuto almeno una volta una e-mail truffa e di sentirsi preoccupato per i propri dati sensibili on-line. Se, a tutto ciò, aggiungiamo il numero sempre più alto di cittadini in possesso almeno di uno smartphone, apparecchio attualmente impossibile da difendere e sempre più usato anche come strumento di lavoro, ci rendiamo conto come il cyber crime oggi abbia un terreno più che fertile dove operare. La semplice *cyber threat* di diversi anni fa è, con il tempo, cambiata e non solo ha moltiplicato gli strumenti attraverso i quali viene perpetrata[29], ma si è evoluta in cyber crime, *cyber terrorism*, *cyber espionage*, *cyber war* e *cyber war*fare, sino ad arrivare al fenomeno dell'hacktivism.

L'universo del cyber crime è abbastanza vasto e comprende diverse tipologie di attacco, di attaccanti, rischi e minacce.

---

[28] *Cyber security Report,* Special Eurobarometer 404, 2013, European Commission, in <http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf> (ultima consultazione 6-11-2014).

[29] Exploit, Buffer overflow, Shellcode, Cracking, Backdoor, Port scanning, Sniffing, Keylogging, Spoofing, Trojan, Virus informatici, DoS, Ingegneria sociale, Social Network Poisoning, CMD Tramite Browser, solo per citarne alcune.

Nella prossima sezione verranno analizzate le principali tipologie di attaccanti e attacchi in ambito informatico, tali elenchi non hanno pretesa di essere esaustivi di tutte le minacce presenti nel *cyber space*, ma offrono una panoramica utile a comprendere la reale entità e pericolosità delle minacce più rilevanti e potenzialmente dannose per le Piccole e Medie Imprese, oggetto di questo lavoro. La sempre maggiore informatizzazione di ogni aspetto della nostra vita quotidiana ci rende sempre più vulnerabili alle minacce derivati dal *cyber space*, in particolare, come abbiamo già detto, furto di identità e di dati sensibili, frodi finanziarie che mirano non solo ad organizzazioni e Governi, ma soprattutto imprese ed individui. Il cyber crime diviene così una nuova ulteriore fonte di rischio per le imprese, affiancando le minacce tradizionali.

Si è ritenuto indispensabile quindi cercare di offrire una panoramica degli strumenti attualmente più utilizzati dai criminali, le motivazioni più comuni che portano alla realizzazione di questi atti criminosi e i maggiori rischi e vulnerabilità per le imprese. Come perpetra il suo attacco il cyber criminale? Con quale metodologia e strumenti e con quali fini? Conoscere le basi che riguardano le minacce che le PMI si possono trovare ad affrontare può aiutare ad aumentare il livello di attenzione durante l'attività lavorativa di tutti i giorni. Conoscere la minaccia aiuta senza dubbio a mettere in atto semplici azioni che possono impedire di cadere vittima dei più comuni rischi e fare la differenza.

È importante sottolineare che l'aggiornamento costante è fondamentale perché questi strumenti si evolvono ad una velocità esponenziale. L'European Union Agency for Network and Information Security (ENISA), nel suo report *Threat Landscape 2013*[30], individua le 16 maggiori minacce alla sicurezza informatica, evidenziando quello che è stato il trend per lo scorso anno. Il grafico seguente, elaborato dal suddetto rapporto, riassume le principali minacce per i settori che coinvolgono direttamente le PMI, come mobile e cloud. Come si può notare, con le sole eccezioni di botnet e spam, che hanno mantenuto il livello dell'anno precedente, tutte le altre minacce sono in costante aumento, in quasi tutte le aree più sensibili.

[30] ENISA *Threat Landscape 2013 Overview of current and emerging cyber-threats,* 11-12-2013, in <https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats/at_download/fullReport> (ultima consultazione 6-11-2014).

Top Threats	Current Trends	Top 10 Threat Trends in Emerging Areas				
		Mobile Computing	Social Networ-king	Cloud Compu-ting	Trust Infrastr.	Big Data
1. Drive-by Downloads	↑	↑	↑		↑	↑
2. Worms/ Trojans	↑	↑	↑	↑	↑	↑
3. Code Injection	↑	↑	→	↑	↑	↑
4. Exploit Kits	↑	↑	↑	↑	↑	↑
5. Botnets	→	↑	↑	↑		
6. Physical Damage/Theft /Loss	↑	↑	↑	↑	↑	↑
7. Identity Theft/Fraud	↑	↑	↑	↑	↑	↑
8. Denial of Service	↑			↑		
9. Phishing	↑	↑	↑	↑	↑	↑
10. Spam	→		↑			
11. Rogueware/ Ransomware/ Scareware	↑					
12. Data Breaches	↑	↑		↑	↑	↑
13. Information Leakage	↑	↑	↑	↑	↑	↑
14. Targeted Attacks	↑				→	↑
15. Watering Hole	↑					

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing

Tabella 4 - Tabella riassuntiva dei trend relativi alle principali minacce cyber
Fonte: Trend Landscape Report, ENISA, 2013

1.3 Tipi di minacce

Le minacce a cui le PMI possono essere più esposte nel *cyber space* sono le stesse che incontrerebbero nel mondo reale, ma ovviamente il web per i criminali rappresenta una via di

sicuro più semplice e facilmente fruibile e moltiplica il numero di potenziali attaccanti a cui l'azienda si espone, rendendo anche le minacce tradizionali più subdole e difficili da scoprire.

Diventa indispensabile, di conseguenza, capire i loro interessi (diretti o indiretti), obiettivi, motivazioni (soldi e informazioni, rabbia) e strategie di attacco (attacchi mirati e non mirati, di massa e singoli). Quanto segue può essere considerato un elenco base, ma esaustivo delle tipologie di attaccanti, attacchi, rischi e vulnerabilità che le PMI potrebbero dover affrontare in ambito informatico e la cui conoscenza di sicuro costituisce un primo livello di protezione da questo tipo di minaccia.

1.3.1 Frodi

La frode consiste nell'accedere, senza averne il permesso, a sistemi informatici con lo scopo di ottenere gratuitamente, e quindi in maniera illecita, i servizi erogati dalla società vittima. Sono principalmente due le vie con cui l'attaccante può accedere a tali servizi, la prima, entrando in possesso attraverso diverse tecniche (phishing, *social engineering*) di credenziali di un amministratore o un dipendente della società, la seconda, entrando in possesso delle credenziali di un legittimo utente. Questa frode può anche essere perpetrata come passaggio intermedio per raggiungere un obiettivo più impegnativo. Questo tipo di azione illecita può avere anche come obiettivo intercettare o dirottare i dati passanti per i POS per rubare dati delle carte di credito o dirottare i pagamenti su un conto bancario controllato dall'attaccante.

Uno dei trend con maggiore crescita nell'ultimo periodo riguarda lo scam, tentativo di truffa nel quale il criminale richiede il pagamento di una piccola somma di denaro da anticipare alla vittima, in cambio di grossi guadagni, come per esempio finanziamenti esteri, vincite alla lotteria, eredità, ecc.[31]

1.3.2 Furto d'identità

Il furto d'identità, anche in ambito informatico, è una truffa con lo scopo di rubare l'identità di un'altra persona (o di un'azienda) al fine di ottenere risorse, informazioni o autorizzazioni illegittimamente.

In ambito aziendale questa minaccia prende forma in due differenti modi, il primo, più tradizionale, in cui un malintenzionato ruba l'identità di una persona interna all'azienda (dipendente, dirigente) al fine di ottenere informazioni preziose direttamente da un ignaro collega; in questo caso il furto d'identità è un passaggio intermedio per un obiettivo ulteriore. Invece nel secondo e più pericoloso modo, l'attaccante ruba l'identità dell'intera azienda (logo, progetti di produzione, catalogo) per utilizzare queste risorse in maniera illecita in un Paese straniero (Cina ed esempio) producendo gli stessi beni commercializzati dall'azienda vittima, e immettendoli nel mercato come merce contraffatta.

1.3.3 Furto di dati sensibili e di proprietà intellettuale

[31] Raggiro informatico famoso con il nome di "Truffa alla nigeriana".

Il furto di materiale sensibile e riservato è uno dei rischi maggiori per il mondo delle Piccole e Medie Imprese. Per le aziende il bene più prezioso sono il know-how e la proprietà intellettuale, cioè l'insieme dei beni immateriali frutto dell'attività creativa umana e che ritroviamo nelle PMI come risultato dell'inventiva dell'imprenditore, come ad esempio i progetti di architettura, le invenzioni industriali e i modelli di utilità, il design di vari beni, i marchi e le ricette senza i quali l'esistenza stessa dell'azienda non avrebbe senso e che in questi anni e soprattutto in questo periodo di crisi ricoprono una sempre maggiore rilevanza economica. È facile intuire come il furto ad un'azienda di moda di una nuova collezione non ancora lanciata sul mercato, o ad un'azienda farmaceutica della ricetta di un farmaco, ad uno studio di architettura del progetto per una gara di appalto costituiscano un danno economico enorme che potrebbe mettere in ginocchio l'azienda in questione.

Il furto di dati sensibili riguarda sia i dati interni all'azienda, (produzione del bene, novità, personale dipendente, informazioni finanziarie, ecc.) sia i dati dei clienti e dei fornitori (identità personali, numeri di carte di credito o conti bancari, credenziali di accesso al servizio offerto dalla società vittima, account e-mail, password ecc.). La top ten delle informazioni rubate nel 2013, vede, secondo Symantec, al primo posto i dati personali come nome, data di nascita, carta d'identità ed indirizzo abitativo, seguiti da dati medici, numeri di telefono, informazioni finanziarie, indirizzi e-mail, user e password e dati assicurativi. Questo genere di attacco ha un fortissimo impatto sul business aziendale, in caso di furto di dati interni infatti potrebbe esserci un blocco o un calo della produzione, in caso di furto di dati esterni, ad esempio di clienti, potrebbe esserci un calo delle vendite dovuto alla perdita di fiducia della clientela nei confronti della società, oltre che a potenziali danni legali per l'incuria nel conservare dati sensibili. Questo rappresenta di sicuro la minaccia più grave per una PMI, soprattutto in Italia, dove la perdita del marchio o del catalogo di produzione rappresenta un danno difficilmente riparabile.

1.3.4 Spionaggio

Lo spionaggio industriale è un'attività che ha come obiettivo principale quello di ottenere in maniera illecita informazioni aziendali e commerciali.

Le metodologie attraverso le quali avviene questo genere di attacchi prevedono generalmente un attacco diretto, attraverso attività di *social engineering* e/o l'installazione sui sistemi dell'azienda vittima di malware che permettono all'attaccante di controllarli. Questo genere di attacchi ha prevalentemente come mittente un'azienda concorrente che ha l'obiettivo di recuperare un gap produttivo o di mercato, ma ovviamente è necessario che venga coinvolto un esperto informatico o un dipendente infedele.

1.3.5 Sabotaggio

Il sabotaggio è quell'azione che ha lo scopo di rallentare o bloccare le attività della vittima attraverso l'intralcio delle normali operazioni come la distruzione di materiale o della strumentazione importante al business aziendale. Anche in questo caso esistono diverse

metodologie tecnologiche e sociali, e le figure coinvolte e gli obiettivi sono gli stessi dello spionaggio.

1.3.6 Attacchi dimostrativi

Questo tipo di attacchi è prevalentemente causato da singoli o gruppi di persone come protesta nei confronti della società vittima, accusata di un comportamento scorretto nei confronti degli utenti finali o dei privati cittadini. Prevalentemente attraverso attacchi di defacement o DDoS, hanno lo scopo di interferire con le normali attività lavorative dell'azienda e fare propaganda alla loro idea e alla loro rabbia.

1.3.7 Estorsione

L'estorsione informatica è un atto criminoso, perpetrato attraverso l'installazione illegale, da parte del criminale, di un malware di tipo ransomware, sul computer della vittima, senza la sua autorizzazione. Attraverso questo software il criminale blocca, da remoto, il computer della vittima oppure ne cripta i dati aziendali rendendone impossibile l'utilizzo. Alla vittima viene richiesto il pagamento di una somma di denaro al fine di sbloccare il PC o decriptare i dati presi in ostaggio. L'installazione del software malevolo avviene generalmente attraverso il click su link fraudolenti, inviati tramite posta elettronica (spam) o sui social network, o attraverso la semplice navigazione non attenta.

Questo tipo di attacchi ha avuto un considerevole aumento nell'ultimo anno, ben il 500%[32] con particolare interesse alle PMI come vittime preferenziali, specialmente in Russia e in generale in Europa.[33] Le somme richieste per il "riscatto" arrivano anche a 3.000-4.000 dollari, somme in molti casi pagate dalle vittime, che preferiscono pagare piuttosto che perdere i dati o dover denunciare l'attacco subito, con stime che si aggirano intorno ai 75 milioni di dollari all'anno di danni[34].

Di seguito, un esempio della schermata di *Cryptolocker*, che avvisa la vittima dell'avvenuta crittazione di tutti i suoi dati, e che chiede un riscatto per la loro restituzione in un tempo prestabilito.

---

[32] *Internet Security Threat Report 2014*, Symantec, in <http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf> (ultima consultazione 6-11-2014).

[33] "*Ransomware criminals attack SMEs using strong file encryption, ESET warns Summer surge in complex attacks*" di John E. Dunn, in <http://news.techworld.com/security/3470388/ransomware-criminals-attack-smes-using-strong-file-encryption-eset-warns/> (ultima consultazione 6-11-2014).

[34] *Europol, FBI, NCA and others disrupt the Gameover Zeus botnet — claim a 2 week window for users to get clean,* in <http://itsecurity.co.uk/2014/06/774/> (ultima consultazione 6-11-2014).

Figura 4 - Immagine della schermata di avviso del ransomware Cryptolocker
Fonte: CryptoLocker Virus, esempio tratto da Comodo.com[35]

Ne consegue che sono numerosi i rischi che il *cyber space* nasconde per le PMI, e che possono impattare su diversi aspetti della vita aziendale, non solo quelli strettamente legati agli strumenti informatici, ma anche e soprattutto sul business e sui beni aziendali più importanti: i dati, le persone e i servizi. I rischi per l'economia che derivano dal cyber crime sono numerosi e vanno dal mero furto di denaro da conto corrente o carta di credito, al danneggiamento della rete aziendale e dei macchinari del sistema produttivo, dal danno di immagine alla perdita di *safety*, dalla perdita della produzione a quella della proprietà intellettuale attraverso per esempio il furto di brevetti.

Difendersi dalle minacce in ambito cyber offre alle imprese un vantaggio in termini di competitività. Questo principio svolge un ruolo chiave nel miglioramento dei fattori economici di un Paese e si traduce in occupazione e crescita economica. Un cyber attacco ai danni delle PMI costituisce un vero e proprio attacco all' economia di un Paese.

Per questo una PMI non deve commettere l'errore di pensare di essere immune da cyber attacchi perché poco appetibile; la grandezza di una azienda non è un aspetto rilevante[36]. Anzi, possono essere facili prede per i cyber criminali che vogliono colpire più aziende, e per questo le PMI corrono oggi un rischio maggiore rispetto alle grandi imprese, di perdere informazioni confidenziali in seguito ad un attacco[37]. Le PMI italiane inoltre corrono un ulteriore rischio, più pesante di qualsiasi frode o perdita di dati, quello della perdita di brevetti e know-how che

[35] *CryptoLocker Virus. Best Practices to Ensure 100% Immunity*, 25-10-2013, di Kimberly Reynolds, in <https://blogs.comodo.com/it-security/cryptolocker-virus-best-practices-to-ensure-100-immunity/> (ultima consultazione 6-11-2014).

[36] Secondo il Rapporto Symantec 2014 le PMI costituiscono ben il 30% delle vittime di spear phishing.

rendono così importante e appetibile il *Made in Italy*, aspetto fondativo della nostra economia. In questo contesto la formazione del management delle PMI diventa la prima arma di difesa contro questo fenomeno.

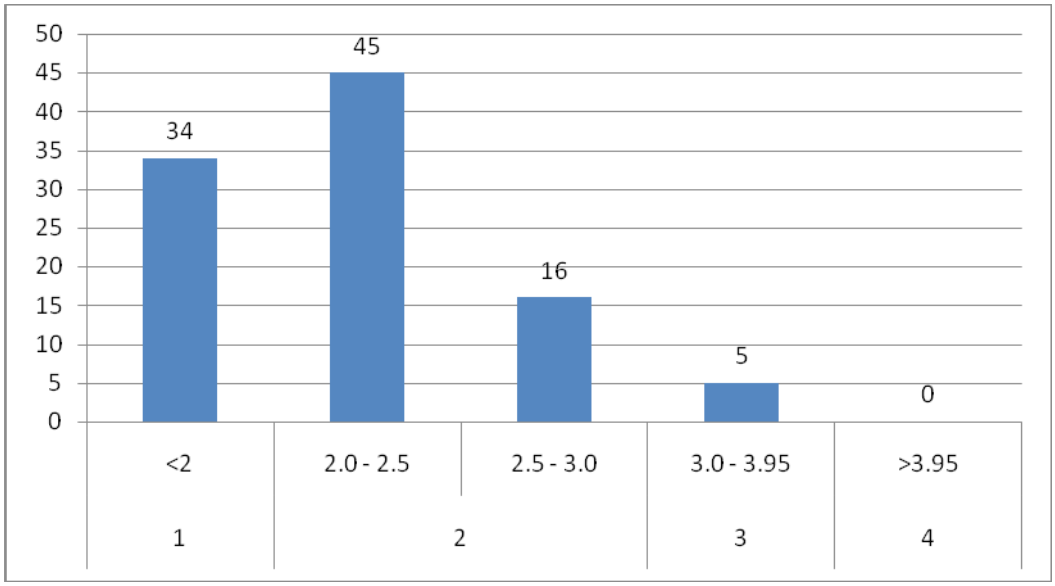


Figura 5 - Distribuzione del grado di maturità del risk management riguardo i rischi informatici
Fonte: Risk and Responsibility in a Hyperconnected World, World Economic Forum, 2014

Su 100 aziende coinvolte nello studio del World Economic Forum, *Risk and Responsibility in a Hyperconnected World*[38], emerge però che il *risk management* aziendale è poco maturo nella gestione del rischio in ambito informatico. Il rapporto divide in quattro livelli il grado di preparazione del *risk managment*, dal più basso "maturità nascente" (1) al più alto "robusto" (4) passando per gli intermedi "in sviluppo" (2) e "maturo" (3). Da questa indagine emerge infatti che nessuna azienda presa in esame ha un livello di *risk management* robusto e solo il 5% è risultato maturo. Ben il 34% è invece ancora al livello più basso, dimostrando la totale impreparazione di un terzo delle aziende. Il restante 60% circa ha un livello di preparazione in fase di sviluppo. Questo livello è a sua volta suddiviso in due sottolivelli, e il 45% del totale delle imprese è ancora nella fase iniziale dell'implementazione delle pratiche di sicurezza informatica. Nello studio non è specificata la dimensione delle aziende che costituiscono il campione, ma possiamo facilmente immaginare che il livello di maturità del *risk managment* di una industria sia direttamente proporzionale alle sue dimensioni, quindi relativamente alle PMI, il dato è assolutamente allarmante, e dimostra come sia necessaria ed urgente l'implementazione di piani di formazione sulle minacce cyber.

[37] Lo dimostra una ricerca condotta nel 2013 in Gran Bretagna da parte del dipartimento governativo degli affari e dell'innovazione, in <https://www.gov.uk/government/publications/cyber-essentials-scheme-overview> (ultima consultazione 6-11-2014).

[38] *Risk and Responsibility in a Hyperconnected World. Pathways to Global Cyber Resilience*, World Economic Forum, in <http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf> (ultima consultazione 6-11-2014).

Inoltre più è piccola la dimensione dell'impresa, minore è anche la sua capacità di identificare un attacco subito rispetto ad una impresa di maggiori dimensioni; per mancanza di reparti tecnici specializzati o semplicemente perché meno abituate a considerare la minaccia. Contro il 65% delle grandi imprese e il 43% delle medie, solamente il 22% delle piccole imprese ha una *policy* ICT formalmente definita. Inoltre un altro dato da sottolineare consiste nel prolungamento del tempo di *recovery* nel quale le aziende ripristinano i sistemi attaccati e riprendono la propria attività.

Spesso le PMI cadono nell'errore di considerarsi fuori dalla portata della criminalità informatica. Infatti in una ricerca[39] effettuata da Alliance su 1.000 PMI, più della metà degli intervistati ritiene di essere in grado di saper difendere i dati aziendali e dei propri clienti, ma non ha nessun tipo di politica di sicurezza aziendale che regoli per esempio l'uso di wireless non protette da parte dei dipendenti che usano dispositivi aziendali o che regoli le azioni da mettere in atto per rispondere ad un furto di dati finanziari o riguardante clienti. Ben l'85% ritiene che le grandi aziende siano l'unico obiettivo e che le PMI abbiano minori probabilità di essere attaccate dagli hacker. In realtà qualsiasi organizzazione facilmente violabile e proficua da sfruttare dal punto di vista economico, di dati o di brevetti, è obiettivo della criminalità informatica, che non fa certo nessun tipo di discriminazione sulla dimensione di un'impresa. Sempre dalla ricerca condotta da Alliance emerge che il 65% delle aziende intervistate conserva nei loro sistemi informatici dati riguardanti i clienti, e il 43% record finanziari. Ben il 33% conserva i dati sensibili di carte di credito e conti aziendali e il 20% conserva nei loro sistemi in rete anche dati riguardanti proprietà intellettuale e altri dati aziendali sensibili. Inoltre ben il 75% degli intervistati dichiara di non aver fornito più di tre ore di formazione o aggiornamento sulla sicurezza della rete aziendale o dei dispositivi mobili nell'ultimo anno e quasi al metà ha ammesso di non aver fornito nessun tipo di formazione.

Insomma, è chiaro che la percezione di consapevolezza della minaccia informatica è ancora molto bassa, soprattutto tra le PMI, che oggi rischiano più delle grandi imprese, dove si registrano in questi ultimi anni maggiori investimenti nelle politiche di sicurezza e dei relativi budget destinati, che spingono i criminali a cercare obiettivi più semplici, ma ugualmente redditizi.

1.4 Tipi di attacco

Le diverse tipologie di cyber attacco che possono essere perpetrate da parte di soggetti attaccanti ai danni delle aziende, per le finalità che abbiamo appena analizzato, possono dividersi in due diverse dicotomie:

- Attacchi on-line (la maggior parte degli attacchi, sia per numero sia per differenti tipologie, come ad esempio spam e phishing) e attacchi offline (causati spesso dall'errato comportamento dei dipendenti, sia volontariamente, per creare un danno all'azienda in caso di

[39] *National Small Business Study*, National *Cyber security* Alliance e Symantec, in <http://eagleintelligence.com/wp-content/uploads/2009/12/NCSA-SB-Study-Factsheet.pdf> (ultima consultazione 6-11-2014).

problemi interni; sia inconsapevolmente, tramite l'uso improprio delle macchine aziendali per usi personali).

- Attacchi mirati (nei quali l'attaccante colpisce un'azienda ben precisa, selezionata per sue specifiche caratteristiche, quali ad esempio la categoria merceologica o la zona geografica) e attacchi non mirati (nei quali l'attaccante colpisce una o più aziende che sono risultate vulnerabili alla minaccia messa a punto dal malintenzionato).

1.4.1 Hacking

L'Hacking è l'atto di accedere illecitamente ad un sistema per ottenere un alto grado di conoscenza ed un numero elevato di informazioni sul sistema stesso, sia sul suo funzionamento, sia dei dati che esso contiene, per poterlo adattare alle proprie necessità. Il termine hacking ha acquisito numerose sfumature durante l'arco di tempo in cui si sono sviluppati i sistemi informatici, acquistando connotati sia negativi, sia positivi.

L'uso delle tecniche e metodologie di hacking, con l'obiettivo di ottenere un guadagno, sia esso materiale e diretto, sia indiretto, rubando informazioni da rivendere o con lo scopo di danneggiare l'azienda vittima dell'attacco è propriamente detto cracking. La figura dell'hacker solitario e curioso che agisce dietro la spinta della sfida e degli interessi personali, lascia sempre di più il posto a gruppi di criminali organizzati che, attraverso azioni di hacking, perseguono scopi economici e di profitto.[40]

1.4.2 Spam

Spam è il termine che indica l'invio di messaggi indesiderati, generalmente di tipo commerciale, di norma attraverso e-mail. Il principale obiettivo dello spam è la pubblicità e la vendita di materiale illegale, falso e/o di provenienza illecita, fino ad arrivare a veri e propri tentativi di truffa. Generalmente lo spam per le aziende è considerato semplicemente una perdita di tempo, ma, in realtà il traffico internet generato dallo spam è circa il 70% di tutto il traffico e-mail[41], e causa diversi danni, soprattutto nelle sue evoluzioni, phishing e spear phishing. Dato confermato anche da Symantec che attesta il volume dello spam al 66% del traffico totale di e-mail per l'anno 2013 e che in media una e-mail ogni 196 contiene un malware.[42]

1.4.3 Phishing

[40] L'analista Lillian Ablon, autrice dello studio "*Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*", sottolinea come il cyber crime oggi sia un reato più redditizio e facile da compiere del traffico di stupefacenti e che ormai sia in mano a vere e proprie organizzazioni criminali, in <http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf> (ultima consultazione 6-11-2014).

[41] *More Than 70% of Email Is Spam*, Kaspersky Lab, in <http://usa.kaspersky.com/about-us/press-center/in-the-news/more-70-email-spam> (ultima consultazione 6-11-2014).

[42] *Internet Security Threat Report* 2014, Symantec, in <http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf> (ultima consultazione 6-11-2014).

Il phishing è un tentativo di truffa via internet attraverso il quale il malintenzionato cerca di convincere con l'inganno la vittima del raggiro a fornire dati personali sensibili, spesso attraverso l'invio di e-mail che simulano la grafica di siti postali o bancari, richiedendo le credenziali di accesso o il numero della carta di credito, per evitare l'incorrere di possibili problemi o sanzioni. All'interno di questa e-mail "esca" è presente un link che la vittima dovrebbe cliccare per risolvere il proprio problema, invece porta il malcapitato su un sito falso, nel quale inserire i propri dati personali consegnandoli così al malvivente. Il termine phishing deriva da fishing ("pescare" in inglese), e allude al tentativo di "pescare" dati personali, finanziari e password di un utente. Questo tipo di attacco sta registrando una crescita costante. Dal 2011 al 2012 ha infatti avuto un incremento del 59% in tutta Europa.[43]

Una nuova variante del phishing, che da qualche anno si sta diffondendo, specialmente nei Paesi di lingua anglofona, è il vishing. La truffa, effettuata però attraverso il telefono, è la stessa del phishing. Con l'inganno e tecniche di persuasione, il criminale cerca di farsi consegnare le credenziali di accesso ad esempio della Banca, fingendosi un operatore di *call center* o dell'assistenza. Questo nuovo tipo di truffa fa leva sulla maggiore fiducia che la vittima ripone verso una persona con cui ha un contatto diretto e più personale di una semplice e-mail e che sembra avere l'autorizzazione a richiedere informazioni sensibili.

Questa minaccia non è da sottovalutare, in quanto i dati Verizon[44] dimostrano che è più efficace di quanto non si possa pensare. Il grafico seguente infatti illustra che mediamente ogni 14 e-mail di phishing ricevute, una va a buon fine.

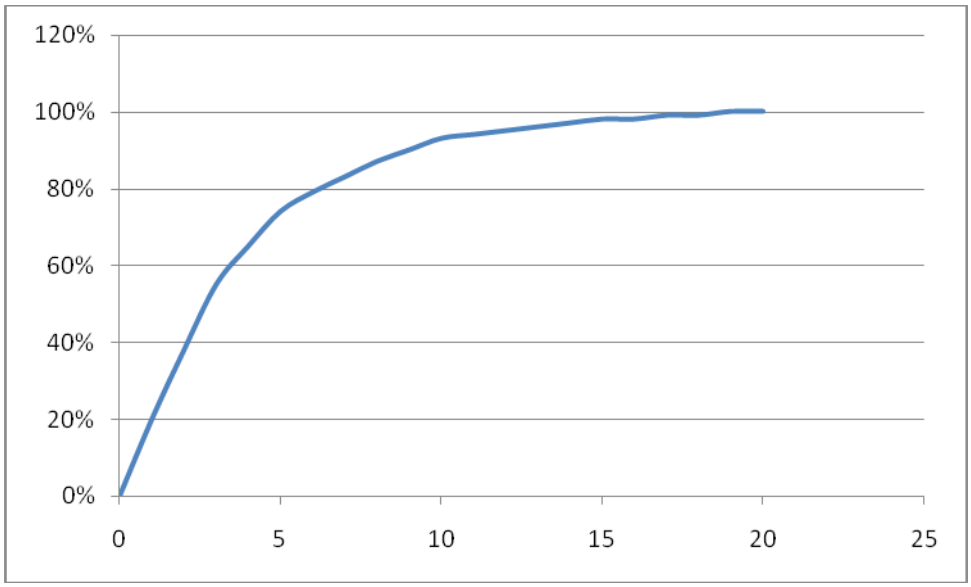


Figura 6 - Percentuale di successo di campagne di phishing
Fonte: Elaborazione da: Data Breach Investigation Report, Verizon, 2014

1.4.4 Spear phishing

[43] *The Year in Phishing*, Gennaio 2013, in <http://www.emc.com/collateral/fraud-report/on-line-rsa-fraud-report-012013.pdf> (ultima consultazione 6-11-2014).

[44] *2014 Data Breach Investigation Report*, Verizon, in <http://www.verizonenterprise.com/DBIR/2014/reports/rp_dbir-2014-executive-summary_en_xg.pdf> (ultima consultazione 15-11-2014).

Sostanzialmente è un'evoluzione del phishing. L'obiettivo finale rimane lo stesso, rubare dati sensibili della vittima. La differenza principale tra le due minacce è che lo spear phishing non invia e-mail casuali a una moltitudine di utenti, ma a differenza del phishing si concentra su poche vittime, calibrando con precisione l'attacco. Ad esempio, nel caso di una PMI, l'attaccante può inviare e-mail che simulino la grafica della Banca della vittima (rintracciabile tramite l'IBAN pubblicato sul sito web aziendale) oppure di un fornitore abituale. In questo caso il rischio corso è molto alto, in quanto possono essere concessi a malintenzionati dati riservati della propria azienda con potenziali gravi perdite economiche. Secondo il Rapporto Symantec 2014 le PMI costituiscono ben il 30% delle vittime di spear phishing.

1.4.5 Pharming

L'obiettivo del pharming è il medesimo del phishing, ovvero indirizzare la vittima verso un sito web fasullo appositamente realizzato per rubarne i dati personali. A differenza del phishing però, il pharming non richiede l'azione dell'utente, ma attraverso tecniche di intrusione ai danni dell'utente stesso o dell'ISP, il malintenzionato indirizza la vittima su un sito da lui controllato.

1.4.6 Defacement

Defacing (o defacement) è l'atto di cambiare illecitamente la homepage di un sito web o modificarne una o più pagine interne da parte di persone non autorizzate. È generalmente un atto vandalico e simbolico effettuato da attaccanti spesso alle prime armi come dimostrazione delle loro abilità e può essere utilizzato anche per diffamare o screditare la vittima. In ambito aziendale i danni causati da questo tipo di attacchi sono prevalentemente di immagine, in quanto un sito web può essere considerato come una "vetrina" verso i propri clienti e/o partner, e la sua deturpazione può avere un effetto negativo. In casi di siti web e-commerce il danno non è solo più di immagine, ma anche economico, sia per i mancati introiti per il periodo sotto attacco, ma anche per il futuro, potendo scoraggiare i potenziali clienti a inserire con fiducia i propri dati personali su un sito "bucato".

1.4.7 DoS

Un attacco Denial of Service (DoS) o Distributed Denial of Service (DDoS), "negazione di servizio" è un attacco effettuato da un malintenzionato verso un sito web o un sistema informatico, che ha l'obiettivo, appunto, di negare il servizio fornito dal sistema attaccato. Anche in questo caso, come per il defacement, il danno è prevalentemente di immagine (in caso di attacco del sito web), ma può tradursi in danni economici se il sistema attaccato è un server che gestisce tutte le operazioni aziendali (e-mail, contabilità, amministrazione, ecc.).

1.4.8 Malware

Con il termine malware (malicious software) "software dannoso" genericamente si identificano tutte le minacce software che possono colpire un PC. All'interno di questa famiglia, ricordiamo i virus, i worm, gli spyware, i trojan, le backdoor e tanti altri. Attraverso tecniche e metodologie diverse, l'obiettivo dei malware è quello di creare danni più o meno gravi alla macchina infetta e, in alcuni casi, di replicarsi alle macchine ad essa collegate, danneggiandole. In ambito aziendale, la perdita di dati importanti comporta spesso ritardi anche significativi nella filiera lavorativa, e in casi gravi anche l'impossibilità di continuare a erogare il servizio offerto.

Le principali difese da questo tipo di attacchi consistono nell'avere programmi antivirus e firewall ben configurati e sempre aggiornati, avere personale consapevole dei rischi e attento nell'uso quotidiano dei sistemi informatici e avere copie di backup soprattutto dei dati vitali per l'azienda. L'installazione di un malware può avvenire sia in modalità on-line, come per esempio cliccando link o scaricando allegati ricevuti via e-mail, sia off-line, attraverso per esempio l'uso di dispositivi USB infetti da parte di un dipendente.

Molti paragonano le infezioni informatiche alle epidemie di virus biologici. La principale similitudine tra i due è che, oltre danneggiare la vittima, in entrambi i casi, essa stessa diventa vettore dell'infezione, diffondendo la minaccia nella propria cerchia di prossimità. Ovviamente le infezioni biologiche si diffondono per prossimità fisica (contatto, aerea, ecc.) mentre le infezioni informatiche si diffondono per prossimità di interessi (contatti e-mail, cellulari, rapporti di fiducia sul posto di lavoro, ecc.). La seconda similitudine riguarda la possibilità che un virus rimanga latente per diverso tempo, per poi colpire anche vittime per cui non era specificatamente creato. Ancora dopo molto tempo dalla loro realizzazione e dal loro lancio, infatti, diversi virus informatici vengono rintracciati in giro per la rete, e infettano ciclicamente i sistemi, come per esempio avvenne per il caso Stuxnet[45] che anni dopo il suo lancio ha continuato ad infettare i sistemi di infrastrutture critiche in vari Paesi nel Mondo.

1.4.9 Botnet

Una botnet (robot network) "rete di robot" è una rete di computer, chiamati "zombie", collegati ad internet ed infettati da malware, che possono essere utilizzati, all'insaputa del legittimo proprietario della macchina, da malintenzionati che ne hanno ottenuto il controllo, per effettuare attacchi di tipo DDoS, spam o phishing.

I computer che fanno parte di reti aziendali sono i più interessanti per chi vuole utilizzare questo attacco, perché mediamente sono accesi per lunghi periodi di tempo senza essere riavviati, fanno parte di reti di numerosi computer che posso essere facilmente infettati e raramente l'utente finale si preoccupa della strana lentezza della macchina, dando erroneamente colpa alla vecchiaia della macchina, che invece è sintomo di un "lavoro" illecito della stessa.

1.4.10 *Social engineering*

[45] Per approfondimenti si veda: <http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99> (ultima consultazione 6-11-2014).

È l'insieme delle tecniche che sfruttano il comportamento umano al fine di ottenere informazioni. Questo metodo riesce a raggirare eventuali ostacoli che l'attaccante incontra quando sono messe in atto adeguate misure di sicurezza. Attraverso l'inganno e nascondendo la propria identità o fingendosi un'altra persona si riesce a ricavare informazioni che non si potrebbero mai ottenere facilmente in altro modo. Si sfruttano così debolezze del comportamento umano come la curiosità o l'empatia per poi arrivare all'attacco vero e proprio. Si sceglie di attaccare spesso dipendenti di basso livello, fingendosi superiori (interni o esterni) che necessitano di informazioni immediate, sfruttando la paura di incorrere in richiami in ambio lavorativo.

Le tecniche di attacco appena esposte non vengono usate singolarmente dagli attaccanti, ma il più delle volte l'attacco viene condotto attraverso l'uso combinato di più tecniche per ottenere più facilmente il risultato voluto.

1.5 Tipi di attaccanti

Il *profiling* degli attaccanti sta avendo in questi ultimi anni sempre più importanza, perché molteplici possono essere le motivazioni che si celano dietro ad un'azione criminale.

1.5.1 Crimine organizzato

Gruppi organizzati di criminali, spesso internazionali, che hanno come motivazione il mero profitto economico, e che hanno come obiettivi principali aziende e Banche. Colpiscono sia con attacchi mirati a singole vittime sia con attacchi di massa (phishing, botnet). Le PMI per il loro minore livello di protezione in ambito informatico costituiscono per questo tipi di criminali un bersaglio facile.

1.5.2 Insider

Singolo dipendente o ex dipendente che ha come intento principale quello di creare un danno alla sua (o ex) compagnia in maniera diretta (danneggiando i sistemi) o indiretta (vendendo le informazioni ad un concorrente) spinto da motivazioni quali rabbia verso i colleghi o la dirigenza, insoddisfazione personale, frustrazione sul posto di lavoro.

Il crimine organizzato e lo spionaggio industriale costituiscono le maggiori minacce per le PMI, soprattutto in Italia dove il *Made in Italy* e la produzione di prodotti di eccellenza possono essere messe in pericolo dal furto della proprietà intellettuale.

Bisogna sottolineare inoltre che, come evidenzia il CISCO Report in un suo grafico[46], possiamo considerare i cyber criminali divisi in una sorta di gerarchia a piramide, con al vertice alto i più capaci e innovatori in ambito di tecniche di attacco e codici, al centro coloro che sfruttano le infrastrutture di attacco già esistenti e/o rivendono tali strumenti, ed alla base quelli che possiamo considerare quasi non tecnici, ma criminali in questo settore per pura opportunità, che sono utenti dei programmi e delle infrastrutture messi in piedi da altri.

1.5.3 Spie industriali

Singoli individui con unica motivazione il profitto personale indiretto (vendita delle informazioni riservate di un'azienda ad un concorrente, o ricatto nei confronti della vittima per la non divulgazione dei segreti sottratti) e con obiettivi aziende e multinazionali.

1.5.4 Hacktivist

Gruppi di persone, con motivazioni etiche, civili e politiche ed obiettivi prevalentemente dimostrativi e che condividono ideali ed etiche proprie. Il termine è stato coniato per definire i protagonisti delle azioni di disobbedienza civile in rete e indica oggi le pratiche di coloro che, attraverso la rete, colpiscono principalmente Governi e multinazionali, accusati di comportamenti scorretti nei confronti dei cittadini o degli utenti. Gli attacchi più usati sono il defacement e il DoS, ma a volte possono verificarsi anche attacchi più gravi, rappresentazione delle forme dell'azione diretta condotte attraverso il mezzo informatico: i cortei si trasformano in DDoS, il volantinaggio nell'invio massivo di e-mail di partecipazione e di protesta e i graffiti vengono rappresentati dal defacement temporaneo di siti web. Questa tipologia di attaccante è meno interessato, di norma, a colpire le PMI, e quindi costituisce in teoria una minaccia minore, a meno che, la Piccola e Media Impresa non sia in stretti rapporti commerciali con una società bersaglio dell'azione dimostrativa degli hackivisti.

1.5.5 Wannabe lamer, script kiddie

Il cyber crime non è prerogativa solo di chi ha capacità tecniche elevate o particolari, ma, grazie alla sempre maggiore informatizzazione di tutti gli aspetti della vita quotidiana, anche il concetto di hacker ha subito uno sviluppo. Tra le diverse tipologie di profili hacker che possiamo distinguere, infatti, quelli maggiormente interessati alle PMI, e quindi più pericolosi rispetto al campo di studio di questo lavoro, possono essere racchiusi nei profili wannabe lamer e script kiddie. Sono i due profili che identificano gli hacker meno esperti e meno capaci, spesso giovani, che compiono azioni di gruppo per moda, come sfogo della loro rabbia, per dimostrare le loro capacità, senza una vera motivazione diretta nei confronti della vittima. Danneggiano i sistemi che colpiscono un po' per inesperienza, un po' per noia, come un atto di vandalismo. Colpiscono gli utenti finali e le PMI perché non hanno le competenze per puntare a obiettivi più grandi. Proprio la

[46] *Annual Security Report*, 2014, CISCO, pag.10, in <http://www.cisco.com/web/offer/gist_ty2_*asset*/Cisco_2014_ASR.pdf> (ultima consultazione 6-11-2014).

loro poca esperienza li rende potenzialmente molto pericolosi, perché possono arrecare danni molto gravi, per incapacità più che volontariamente. Colpiscono le PMI o gli utenti finali che hanno le difese più basse, quindi un approccio attento alle tematiche della *cyber security* aiuta in maniera significativa a contrastare questo genere di attaccanti.

1.6 Rischi

Dai tipi di attacchi e attaccanti sopraelencati ne conseguono per le aziende diversi tipi di rischi derivanti da vulnerabilità tecniche ed umane che analizzeremo in seguito. I rischi che il *cyber space* nasconde per le PMI, possono impattare su diversi aspetti della vita aziendale, non solo quelli strettamente legati agli strumenti informatici, ma anche e soprattutto sul business e sui beni aziendali più importanti: i dati, le persone e i servizi.

Con la perdita dei dati o della loro integrità si possono subire dalla semplice e mera perdita economica diretta (attraverso perdita di credenziali, spam, o estorsione e truffa), a danni derivanti dal furto della proprietà intellettuale ai danni di immagine e reputazionali. L'informazione infatti oggi ha spesso lo stesso valore economico del denaro, e si può tradurre in database clienti, dati finanziari aziendali, dettagli finanziari di clienti e fornitori, informazioni sui prezzi, progetti di prodotti o processi di produzione. Questo tipo di rischio è particolarmente strategico soprattutto per le PMI, non solo perché difficilmente stimabili, ma soprattutto perché possono riguardare il *core business* dell'azienda e creare danni difficilmente risanabili. Una grossa azienda o multinazionale, solida sul mercato, che produce un ampia gamma di prodotti, in caso di danno riguardante un singolo e specifico bene può, sia dal punto di vista economico che di produzione, cercare di gestire quel danno di sicuro più facilmente di una PMI che fonda tutto il suo business sulla produzione di un singolo bene. È facile immaginare come un attacco di questo tipo possa mettere in ginocchio una PMI e che tipo di impatto possa avere in termini di posti di lavoro ed economia locale.

La seconda tipologia di danni che le PMI possono subire a causa di un cyber attacco è quella relativa ai danni ad impatto fisico, cioè, quel tipo di attacchi che colpiscono l'integrità dei macchinari, dei sistemi, delle reti e degli strumenti di controllo, rallentando o bloccando di fatto la produzione e danneggiando il business aziendale o impedendo l'accesso al web e a tutti i sistemi informatici aziendali. Per ripristinare i sistemi è necessario un investimento economico e di tempo che aggrava ulteriormente il danno diretto dell'attacco.

La terza e ultima tipologia di danno riguarda i danni ad impatto sui servizi erogati o utilizzati da un'azienda che possono inficiare la qualità del bene prodotto o la sicurezza dei dipendenti o degli utenti.

1.7 Vulnerabilità tecniche

Ogni azienda presenta al suo interno delle vulnerabilità sia tecniche sia umane che, individuate, possono essere sfruttate dai cyber criminali per i loro intenti. Nella maggior parte dei casi le tecniche di attacco utilizzate sono diffusamente note e spesso semplici, sfruttano errori nella scrittura dei codici, la mancata installazione di patch di sicurezza dei programmi o dei sistemi utilizzati dalla vittima, il mancato aggiornamento degli antivirus e degli anti malware e l'errata o mancata configurazione degli apparecchi e delle reti aziendali o l'uso di password ripetitive o troppo semplici; tutte vulnerabilità che si potrebbero facilmente risolvere con un'adeguata preparazione dei responsabili tecnici e una maggiore conoscenza delle buone pratiche da parte di tutti gli utenti dei sistemi a rischio. Queste semplici pratiche renderebbero sicuramente più difficile l'ottenimento del risultato da parte degli attaccanti.

L'aspetto tecnologico, a livello aziendale, oggi è sempre più pervasivo e si compone di innovazioni sempre più veloci in ogni ambito. Queste due caratteristiche portano gli utenti ad utilizzare tecnologie non sempre mature e studiate al meglio pensando alla sicurezza, e con un bagaglio di conoscenze tecniche non sempre sufficiente ad un uso sicuro degli strumenti. La disponibilità di internet ormai costante, attraverso reti wireless, oltretutto spesso non protette o protette male, con password di default o troppo semplici, senza un'adeguata configurazione degli apparecchi e della rete interna e con l'uso di protocolli non sicuri come WEP e WPA al posto del più sicuro WPA2, ha permesso la nascita di molti strumenti fino a poco tempo fa impensati, che portano al seguito una quantità di nuovi problemi legati alla sicurezza dei dati e delle informazioni.

Il primo fattore di rischio è intrinseco ed è dato proprio dall'esposizione dei dispositivi on-line, dalla tipologia di connessione utilizzata e dalle connessioni in generale, che offrono la possibilità di diversi tipi di attacco. Ad esempio, nel corso degli ultimi anni sta prendendo piede, sia a livello di utilizzo privato, sia di utilizzo aziendale, il fenomeno del cloud computing, principalmente per questioni economiche. In breve, il cloud computing è la possibilità di utilizzare servizi IT attraverso il web. Questo permette in termini più semplici di avere a disposizione i propri file e i propri dati ovunque ci sia una connessione ad internet, e condividerli attraverso più piattaforme (PC di casa, dell'ufficio, smartphone, Smart TV ecc.), ma in termini più articolati, anche di sfruttare applicazioni basate su linguaggi web in condivisione con altre persone attraverso internet.

Infatti, proteggere le informazioni, che, come si sa, sono il vero "denaro" del *cyber space*, risulta molto più complicato se queste possono essere visualizzate, attraverso internet, da un legittimo proprietario che, ad esempio, visualizza i file del lavoro dal PC di casa perché deve lavorare fino a tardi per una scadenza impellente. È molto complicato infatti conciliare le esigenze di mobilità con le esigenze di sicurezza, perché così facendo le informazioni sono accessibili anche da un malintenzionato che, pur non avendo diritto a quelle informazioni, è abbastanza competente per ottenere lo stesso ciò che cerca, e spesso il suo compito è reso più semplice dalle errate configurazioni dei sistemi o dalla superficialità di chi li usa.

Questo tipo di attenzioni è da considerarsi obbligatorio sia per difendersi da attacchi esterni sia da attacchi realizzati da persone interne alla struttura, che possono, per le più svariate ragioni, voler danneggiare, rubare o rivendere dati a cui non dovrebbero avere accesso o effettuare operazioni ancora più dannose. A livello aziendale è quindi indispensabile avere "regole" che disciplinino l'uso dei dispositivi mobili, sia aziendali sia personali, impedendo, ad

esempio di collegarsi alle reti wireless libere e gratuite offerte dai locali commerciali, ristoranti o bar e di inserire dati aziendali sensibili durante la navigazione wireless non protetta (account bancari, password, credenziali aziendali).

Insieme al cloud computing un'altra delle problematiche più attuali riguarda i dispositivi mobili, come smartphone e tablet, la cui vendita ha ormai superato di gran lunga quella dei PC desktop e portatili tradizionali[47] e il cui uso è sempre più diffuso.

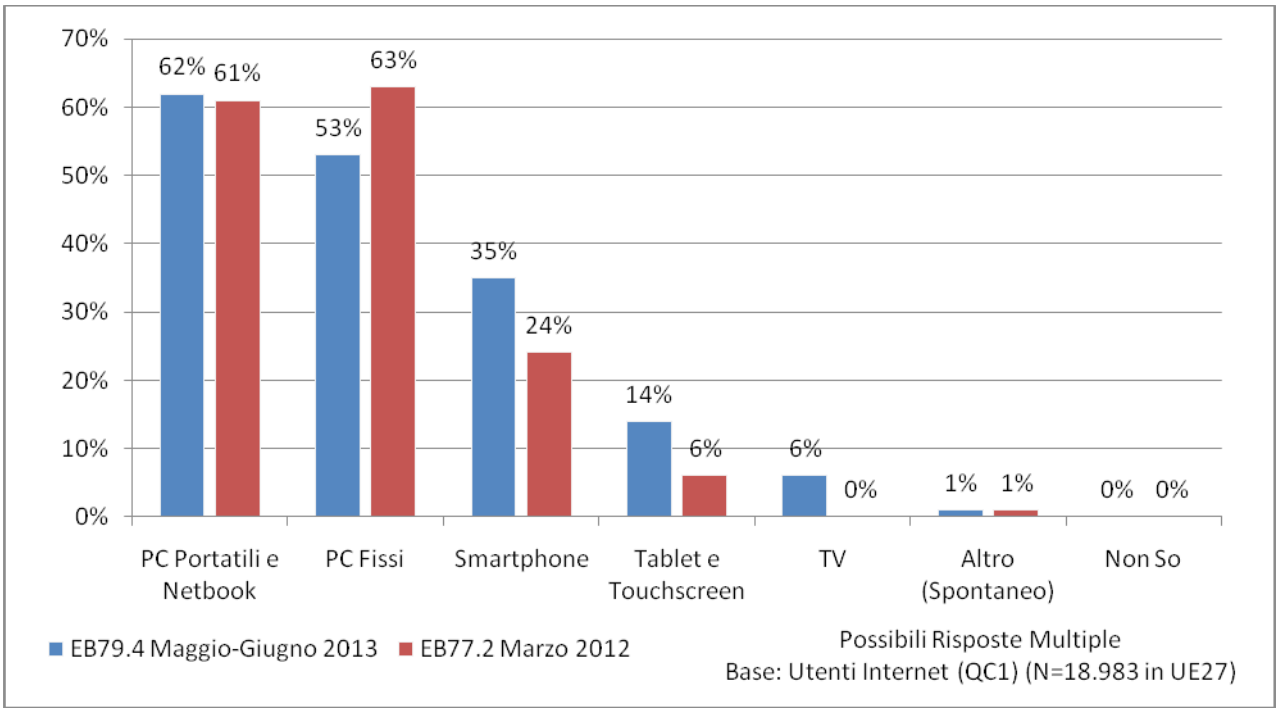


Figura 7 - Statistiche sull'uso dei dispositivi per l'accesso ad internet in Europa
Fonte: Speciale Eurobarometro 404 Cyber security Report, 2013

Il grafico sopra esposto presenta diversi spunti interessanti. Prima di tutto, il calo del 10% dell'uso di PC fissi, mentre rimane stabile l'uso del computer portatile, che si piazza al primo posto come dispositivo usato per accedere ad internet.

Il secondo dato interessante, è la comparsa delle Smart TV, che hanno iniziato a ritagliarsi la loro fetta di mercato come dispositivi per la fruizione di contenuti web, primo passo per l'Internet of Things (IoT)[48].

L'ultimo, ma più interessante dato è l'aumento dell'uso di tablet e touchscreen, che è più che raddoppiato, e l'11% in più di smartphone. Purtroppo il dato relativo alla diffusione dei dispositivi mobili non è incoraggiante se guardiamo le stime di Symantec, che nel suo report sottolinea come il 44% degli adulti non siano attenti alla sicurezza del loro dispositivo mobile (immaginiamo solo come possano essere poco attenti gli adolescenti, che rappresentano una

[47] Il mercato degli smartphone a livello mondiale ha raggiunto una nuova pietra miliare nel 2013 con un miliardo di unità vendute in un solo anno, per la prima volta, in crescita del 38% rispetto ai 725 milioni di unità vendute nel 2012. Per approfondimenti veda: *IDC Worldwide Quarterly Mobile Phone Tracker, January 2014*, in <http://www.idc.com/tracker/showproductinfo.jsp?prod_id=37> (ultima consultazione 6-11-2014).

[48] Per approfondimenti veda: *Internet of Things* di Hermann Kopetz, in <http://link.springer.com/chapter/10.1007/978-1-4419-8237-7_13> (ultima consultazione 6-11-2014).

percentuale tutt'altro che trascurabile degli utenti di smartphone e tablet). Questo tipo di disattenzione porta rischi quali: la perdita della privacy sull'uso del dispositivo, la lettura degli SMS o dei registri delle telefonate, tracciamento delle coordinate GPS, registrazione delle telefonate e dei messaggi, lettura delle e-mail, furto di video e foto, furto degli account dei social network e delle applicazioni installate.

Purtroppo l'elevata diffusione di questi apparecchi non solo attira l'interesse dei cyber criminali che aumentano i loro sforzi per sfruttare le vulnerabilità di questi sistemi, ma è controproducente anche sotto il punto di vista della sicurezza, in quanto sono estremamente difficili da proteggere. Le difficoltà principali sono:

- da parte dei produttori: la tecnologia ancora acerba e la progettazione non pensata per la sicurezza, il rilascio lento delle patch e degli aggiornamenti, la sicurezza degli *store* ufficiali;
- da parte degli utenti: la non completa consapevolezza nell'uso del dispositivo, i dati sensibili che vengono memorizzati su di essi con superficialità, la mancanza di attenzione riguardo gli aggiornamenti, la mancata installazione di antivirus e anti malware.

E queste solo per citare le più importanti. Le conseguenze sono evidenti e i rischi sono, oltre le infezioni di virus e malware, soprattutto frodi attraverso i social media e il phishing. Anche in questo settore il 2012 ha dato un'enorme accelerata, vedendo quintuplicarsi il numero di campioni malware per device mobili rispetto al 2011. Questo aumento è dovuto anche alla costante crescita di transazioni bancarie effettuate attraverso dispositivi mobili. Secondo Gartner infatti il volume delle transazioni mobili a livello globale crescerà mediamente del 42% all'anno tra il 2011 e il 2016[49]. A questo proposito, Kaspersky evidenzia come sia in evoluzione la minaccia riguardante trojan che colpiscono proprio i sistemi di mobile banking.[50]

[49] *Gartner Says Worldwide Mobile Payment Transaction Value to Surpass $171.5 Billion,* in <https://www.gartner.com/newsroom/id/2028315> (ultima consultazione 6-11-2014).

[50] *Kaspersky Mobile Malware Evolution: 2013,* 24-2-2014 di Cassie Bodnar, in <https://blog.kaspersky.com/mobile-malware-evolution-2013/> (ultima consultazione 6-11-2014).

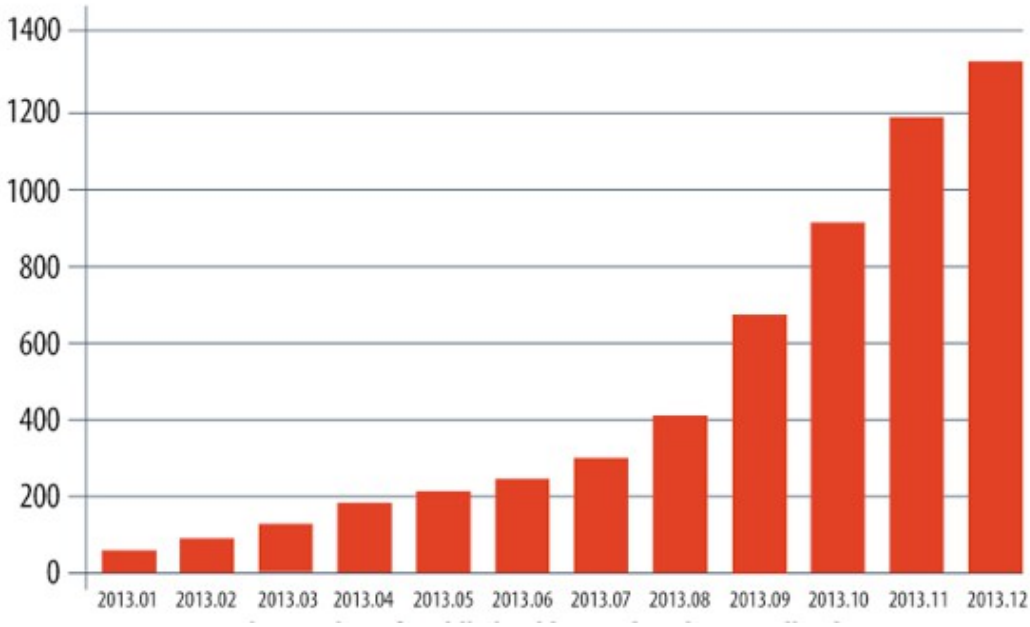


Figura 8 - Dati relativi all'aumento del numero di trojan che colpiscono le transazioni bancarie effettuate attraverso dispositivi mobili
Fonte: Mobile Malware Evolution, Kaspersky, 2013

Il grafico seguente, sempre di Kaspersky, evidenzia come Android sia il Sistema Operativo per dispositivi mobili più colpito dalla minaccia malware, con oltre il 98% di minacce rilevate. Da notare, il dato più interessante, è in realtà quello che non c'è. Cioè la totale assenza di iOS, il Sistema Operativo di Apple, ad ora apparentemente immune da questa minaccia.

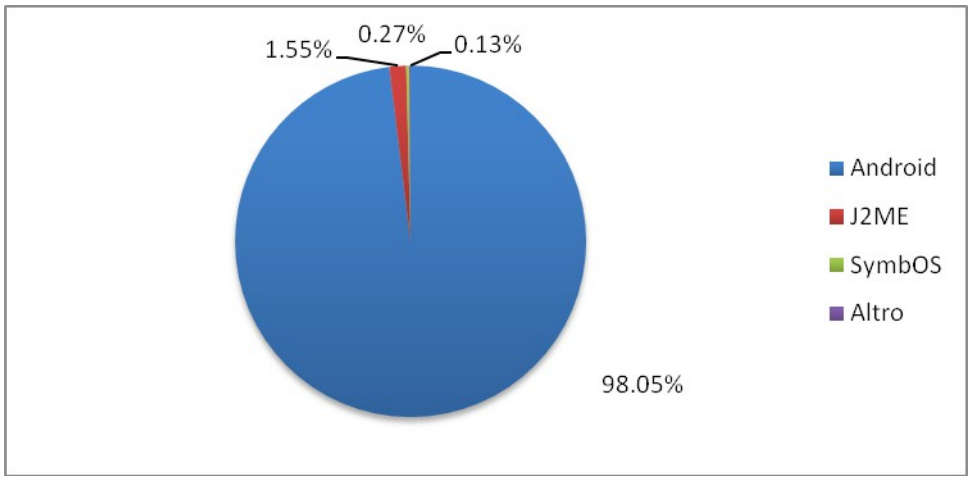


Figura 9 - Dati relativi alla percentuale di diffusione di malware per Sistema Operativo per dispositivi mobili
Fonte: Mobile Malware Evolution, Kaspersky, 2013

La diffusione dei dispositivi mobili inoltre contribuisce all'aumento della pratica del BYOD e la mancanza di sicurezza degli apparecchi rende immediatamente meno sicure anche le aziende, che, pur incentivando l'uso di dispositivi personali per accedere ai sistemi aziendali, in molti casi sottovalutano la necessità di standard di sicurezza più elevati per proteggere i propri dati sensibili, come ad esempio l'uso di VPN o criptazione dei dati.

Dall'indagine *IT Security Risks 2014* di Kaspersky Lab[51] emerge che un ulteriore rischio è l'aumento del furto fisico dei dispositivi mobili, con relativo pericolo di perdita di dati sensibili, materiale aziendale e accessi a servizi aziendali, il 25% delle aziende rispetto al 14% del 2011. Inoltre questo rischio è aggravato dal fatto che il dipendente che subisce il furto del proprio dispositivo lo denuncia alla società con un ritardo medio che va dai 2 ai 5 giorni, allungando pericolosamente i tempi di risposta a questa minaccia. La vulnerabilità in questi casi non è solo tecnica, ma soprattutto umana perché i dipendenti tendono a non avvisare in tempi rapidi i responsabili aziendali del furto avvenuto. Ben il 38% degli impiegati denunciano il furto del proprio dispositivo dopo 2 giorni, e il 9% addirittura dopo 5 giorni, mentre solo la metà dei dipendenti denuncia l'accaduto il giorno stesso, dato in discesa rispetto al dato del 2013 (60%).

Il dato più preoccupante è costituito da un 19% di aziende che hanno dichiarato di aver perso dati aziendali sensibili in seguito al furto del dispositivo mobile[52]. Parallelamente con l'aumento della diffusione dell'uso dei dispositivi mobili in ambito aziendale, aumentano anche i furti e i rischi relativi per le aziende, ma diminuisce il livello di allarme percepito dai dipendenti, in tutte le zone del Mondo prese in esame dall'indagine di Kaspersky, il numero di dipendenti che notificano tale sottrazione diminuisce col tempo[53]. Nonostante il costante aumento dei dispositivi mobili in ambito lavorativo, più della metà degli intervistati ammette di essere più preoccupato rispetto agli anni precedenti dei rischi legati al mobile e addirittura il 43% ritiene i rischi troppo elevati rispetto i vantaggi in termini di comodità.

Per quanto riguarda le PMI un altro fattore che concorre fortemente a rendere le aziende meno sicure è l'uso di sistemi operativi, programmi e applicazioni, sia client che server, non aggiornati e quindi poco sicuri. Ad esempio il mancato passaggio da Windows XP a versioni successive del Sistema Operativo Microsoft (spesso per mancanza di fondi aziendali per l'acquisto delle onerose licenze di utilizzo) è una vulnerabilità estremamente rilevante, soprattutto da aprile 2014 quando Microsoft ha deciso di terminare definitivamente il supporto a questo prodotto.

[51] Indagine rivolta ai professionisti della sicurezza informatica di aziende e organizzazioni a livello globale. *IT Security Risks Survey 2014: A Business Approach to Managing Data Security Threats*, Kaspersky Lab, in <http://media.kaspersky.com/en/IT_Security_Risks_Survey_2014_Global_report.pdf> (ultima consultazione 6-11-2014).

[52] Dati basati sul contributo di 3.900 responsabili della sicurezza IT di aziende e organizzazioni di tutte le dimensioni e di 27 Paesi in tutto il Mondo, di cui 198 hanno contribuito dall'Italia.

[53] In altre zone del Mondo si registrano tempi diversi, nel Nord America per esempio sono più lenti. Solo il 43% dei dipendenti segnala il furto lo stesso giorno in cui è avvenuto. In Asia invece si è registrato il cambiamento più significativo su un solo anno. Il 47% nel 2014 ha notificato la sottrazione del dispositivo nel giorno stesso, mentre nel 2013 la percentuale era del 74%.

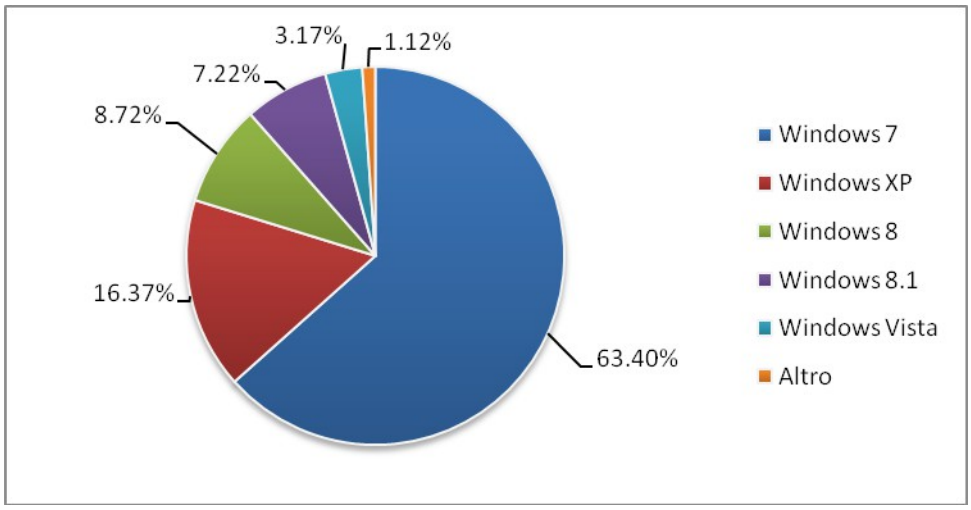


Figura 10 - Uso di Windows XP a giugno 2014, due mesi dopo la chiusura del supporto di sicurezza ufficiale Microsoft

Fonte: Windows usage & vulnerabilities, Kaspersky Security Network Report, 2014

Come illustrato da Kaspersky Lab, tra tutti gli utenti che hanno partecipato all'indagine[54] sull'uso di Windows, si evince che, a due mesi dal termine del supporto ufficiale Microsoft a Windows XP, oltre il 16% degli utenti utilizza ancora questo Sistema Operativo[55] che risale al 2001, quindi 13 anni fa, e che in ambito informatico corrisponde ad un lasso di tempo enorme. Questo dato è rilevante se si considerano le potenziali implicazioni per la sicurezza delle informazioni. Avere una versione non aggiornata di un Sistema Operativo così datato comporta maggiori rischi, derivanti dalla possibilità di sfruttare vulnerabilità non corrette, da parte dei cyber criminali. Il rapporto ha anche esaminato la percentuale di utenti che usano ancora Windows XP nei singoli Paesi e l'Italia è al quinto posto con il 20.31%, primo assoluto tra i Paesi occidentali, una percentuale significativa per quanto attiene la sicurezza informatica. Se consideriamo invece la percentuale degli utenti che hanno effettuato il passaggio al nuovo Sistema Operativo in questi mesi, analizzata per singoli Paesi, i leader sono Stati Uniti (16,27%), Canada (13,52%), Germania (11,17%), Regno Unito (10,79%) e Francia (10,31%). Gli outsider sono Italia (8,1%), Russia (5,14%) e India (2,91%).[56]

Oltre alle vulnerabilità che riguardano i sistemi operativi, anche l'uso poco attento di programmi come lettori PDF (Adobe Reader, Foxit Reader), suite di programmi per ufficio (Microsoft Office, LibreOffice, OpenOffice) raramente aggiornati, e servizi on-line (Facebook, Twitter e tutte le applicazioni offerte da Google) mette ogni giorno a serio rischio la sicurezza degli utenti.

---

[54] *Kaspersky Security Network Report: Windows usage & vulnerabilities Version 1.0*, agosto, 2014, in <https://securelist.com/files/2014/08/Kaspersky_Lab_KSN_report_windows_usage_eng.pdf> (ultima consultazione 6-11-2014).

[55] Dato confermato anche da Statcounter.

[56] *16.37% Users Still Run Windows XP*, Kaspersky Lab Statistics Say, agosto, 2014, in <http://www.kaspersky.com/about/news/virus/2014/16-37-per-cent-Users-Still-Run-Windows-XP-Kaspersky-Lab-Statistics-Say> (ultima consultazione 6-11-2014).

1.8 Vulnerabilità umane

Il fattore umano è senza dubbio un fattore fondamentale all'interno dell'intero sistema di sicurezza aziendale. Infatti molto spesso la prima breccia nella sicurezza di un sistema si ottiene non con strumenti tecnici, ma semplicemente sfruttando aspetti del comportamento umano codificati e standardizzati come: distrazione, superficialità, negligenza, altruismo, fiducia e curiosità, su cui molte tipologie di attacco poggiano le loro basi. Ad esempio il phishing, il pharming, e in generale gli attacchi con obiettivo la frode o il furto d'identità o di dati sensibili, si fondano sulla probabilità che l'operatore dall'altra parte del PC possa essere indotto a cliccare su link suggeriti, per semplice curiosità, perché crede di conoscere il mittente della e-mail o perché convinto di poter risolvere problemi sulla propria carta di credito.[57] La tecnica di *social engineering* è più complessa perché sfrutta telefono, e-mail, informazioni rilasciate sui social network e contatto fisico diretto per ottenere direttamente dal bersaglio l'informazione necessaria a proseguire l'attacco, effettuato poi attraverso strumenti tecnologici. È quindi necessario comprendere la mentalità dell'attaccante e l'atteggiamento che ha, le sue motivazioni, come raccoglie le informazioni sul bersaglio; in pratica un *profiling* dell'hacker e dell'etica che lo muove.

È di luglio di quest'anno il caso riguardante la richiesta da parte di Goldman Sachs[58] nei confronti di Google[59] di cancellare un'e-mail confidenziale contenente materiale aziendale classificato e dati della clientela, inviata per l'errore umano di un *contractor* della Banca d'investimenti, ad un indirizzo e-mail errato, gmail.com al posto di gs.com (il dominio aziendale Goldman Sachs). Un errore apparentemente così banale ha rischiato di compromettere dati sensibili e conseguentemente rapporti commerciali di alto profilo.

Un recente studio rivela come l'80% dei professionisti IT tra gli intervistati veda i dipendenti come l'anello più debole nella catena della sicurezza IT e dipinge un quadro del settore delle PMI inondato di minacce di sicurezza informatica.[60]

1.8.1 Vulnerabilità derivanti dall'uso dei social media

Questo tipo di vulnerabilità viene inserito all'interno di quelle "umane" poiché il rischio più elevato che gli utenti di internet corrono attraverso l'uso dei social network deriva non da errori di programmazione delle piattaforme usate, come Facebook, Twitter, LinkedIn ecc., ma soprattutto dall'errato uso di questi strumenti e da applicazioni malevole e plug-in esterni collegati ad essi e realizzati da cyber criminali, che reindirizzano gli utenti su siti malevoli o link fraudolenti,

[57] Ironicamente in ambito informatico si è coniato il termine PEBKAC che significa "Problem Exists Between Keyboard And Chair", ossia "Il problema sta fra tastiera e sedia" per indicare che problemi in ambito informatico spesso e volentieri sono causati dall'utente stesso.

[58] *Goldman says client data leaked, wants Google to delete email* di Jonathan Stempel, 2-7-2014, in <http://www.reuters.com/article/2014/07/02/us-google-goldman-leak-idUSKBN0F729I20140702> (ultima consultazione 6-11-2014).

[59] Il 26 giugno Google ha dichiarato che l'e-mail non poteva essere eliminata senza l'ordine del Tribunale. Il caso è Goldman, Sachs & Co. V. Google Inc. New York State Supreme Court, New York County, No. 156295/2014.

[60] *2015 State of SMB Cybersecurity,* CloudEntr by Gemalto, in <https://app.box.com/s/2mf328i6a7j0z2tbdv07?src=undefined> (ultima consultazione 15-11-2014).

ingannandoli pubblicizzando e invitando a cliccare su false applicazioni che riguardano giochi o video virali, piuttosto che la possibilità di sapere chi ha visitato il proprio profilo o di cambiare il colore del *template*. Infatti, nel 2012 grosse percentuali di spam e phishing si sono spostate proprio su questo tipo di piattaforma, rendendo sempre più insidiose e difficili da riconoscere queste minacce. Symantec, nel corso del 2013, ha confermato la nascita di nuove minacce che sfruttano la sempre maggiore popolarità dei social network. La connettività sociale in questi ultimi anni ha avuto una crescita senza precedenti, si stima infatti che il 71% degli adulti on-line abbia un account Facebook[61], social network che da solo è passato da un milione di utenti nel suo primo anno a oltre 1,15 miliardi oggi. I social network sono sempre più importanti per il business globale, soprattutto nel mercato della telefonia mobile, e quando uno nuovo raggiunge un adeguato livello di popolarità inevitabilmente scatena l'attrazione di sempre più utenti, e quindi di sempre più criminali, che inizieranno ad interessarsi ad esso e a trovare modi sempre nuovi per sfruttarlo per ottenere guadagni illeciti.

È importante quindi sottolineare che per affrontare questa minaccia crescente, più che strumenti tecnici, sia necessario aumentare gli sforzi nelle politiche di sensibilizzazione e di istruzione del cittadino all'uso corretto e prudente del web e dei social network, che di certo porterebbero ad un beneficio anche a livello aziendale, in quanto gli atteggiamenti potenzialmente scorretti che abbiamo con l'uso dei dispositivi mobili tendiamo poi a metterlo in pratica anche sul luogo di lavoro; ad esempio la superficialità con la quale usiamo dispositivi USB o gli smartphone, apriamo e-mail da mittenti sconosciuti o scarichiamo software pirata non sicuro.

CAPITOLO 2

IL CYBER CRIME IN PROSPETTIVA INTERNAZIONALE ED EUROPEA

2.1 Il cyber crime come minaccia a livello internazionale

A livello globale i rischi di vario tipo sono diventati sempre più importanti a causa dell'intensificazione della globalizzazione ed in questo scenario il cyber crime costituisce una minaccia sempre più pericolosa. Anche le conseguenze dei nuovi rischi sono divenute *cross-boundary*, e sono potenzialmente devastanti e imprevedibili. L'interconnessione globale rende più vulnerabile ogni sistema economico-produttivo nazionale. Come abbiamo visto, il cyber crime è un fenomeno che coinvolge tutti gli Stati del Mondo, soprattutto i più industrializzati e informatizzati.

[61] *The Internet Organised Crime Threat Assessment (iOCTA) 2014*, EUROPOL, in <https://www.Europol.europa.eu/sites/default/files/publications/Europol_iocta_web.pdf> (ultima consultazione 6-11-2014).

Esistono centinaia di differenti fonti che forniscono dati riguardo l'entità del fenomeno cyber crime, ma sono statistiche insufficienti e frammentate. Analizzando, ad ogni modo, i principali report di settore, i dati che emergono non sono affatto incoraggianti.

In un suo recente rapporto, redatto sulla base di interviste a 250 tra esperti del settore e dirigenti di azienda, il World Economic Forum avverte che, nei prossimi 6 anni, i cyber attacchi potrebbero generare perdite economiche fino a 3 mila miliardi di dollari, se non si riesce ad agire in modo efficiente per contrastare questo tipo di minaccia; che potrebbe, secondo lo stesso studio, portare anche ad un rallentamento dell'uso di soluzioni tecnologiche innovative nei prossimi anni.[62] Ben il 78% delle aziende intervistate ha infatti posticipato l'uso di soluzioni come il cloud computing proprio per il timore di essere vittima di un attacco hacker e di subire una perdita di dati sensibili. L'adozione invece di azioni proattive da parte di aziende e Governi, secondo lo studio del WEF, non solo porterebbe ad una limitazione del numero degli attacchi e della loro entità, ma addirittura potrebbe portare a generare un valore economico in termini di innovazioni tecnologiche ed informatiche, che, a sua volta, genererebbe all'economia globale un profitto tra i 9 mila e i 21 mila miliardi di dollari in un decennio.

Il costo annuo dei danni inflitti dalla criminalità informatica è difficile da stimare per diversi motivi: le aziende non condividono sempre informazioni a riguardo, spesso non ci si accorge nemmeno di essere stati attaccati, se non dopo mesi o anni, e in taluni casi può essere difficile stimare l'effettivo danno subito. In un tipo di reato, poi, dal carattere così transnazionale si dovrebbe prendere in considerazione il fatto che non esiste una legislazione a livello internazionale e quindi è anche difficile definire quale azione è considerata reato nei diversi Stati Nazionali per redigere delle stime internazionali attendibili.

Inoltre, i numerosi report, tutti stilati da società di sicurezza informatica private, soffrono il limite di non poter usufruire di dati completi a livello dei singoli Stati Nazionali; solo report ufficiali stilati dagli Stati potrebbero garantire una maggiore precisione sulle statistiche finali. Ad ogni modo danno un'indicazione della gravità e del trend che si registra in questi anni riguardo il fenomeno cyber crime. Tutti i report, infatti, sottolineano come il rischio di subire cyber attacchi sia in continuo aumento e come l'impatto sull'economia globale sia sempre più preoccupante e dovrebbe essere sufficiente a spronare PMI, società civile e Governi a prendere più seriamente in considerazione questa minaccia e a collaborare per limitarne i danni.

Secondo Kaspersky l'impatto sull'economia globale del cyber crime è tristemente destinato a moltiplicarsi negli anni, gli attacchi più temibili rimangono quelli verso le infrastrutture critiche, ma preoccupa anche il notevole aumento di reati nei confronti delle imprese come frode o furto di dati. Al Web Summit di Dublino di quest'anno, infatti, Eugene Kaspersky ha dichiarato che l'impatto della criminalità informatica sull'economia globale è stimato in un centinaio di miliardi di dollari, ma oggi questo valore dovrebbe considerarsi moltiplicato di molte volte[63].

---

[62] *Risk and Responsibility in a Hyperconnected World*, World Economic Forum, in <http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf> (ultima consultazione 6-11-2014).

[63] *On-line fraud costs global economy 'many times more than $100bn'*, The Guardian, 30-10-2013, in <http://www.theguardian.com/technology/2013/oct/30/on-line-fraud-costs-more-than-100-billion-dollars> (ultima consultazione 6-11-2014).

Più prudenti sono le stime di McAfee[64] e CISCO che valutano la forbice del costo annuale del cyber crime per l'economia globale tra i 375 e i 575[65] miliardi di dollari l'anno, potenzialmente anche un trilione di dollari, ma comunque in costante crescita dato gli ingenti e facili rendimenti, a fronte di rischi molto bassi per i criminali. McAfee segnala inoltre che le aziende tendono a sottostimare la gravità del rischio cyber e la sua velocità di crescita.

Il gap tra l'aumento delle capacità di attacco dei criminali e quelle di difesa delle aziende è in costante aumento[66], e questo problema diventa maggiore se parliamo di PMI, nelle quali per ovvi motivi il budget dedicato agli strumenti di difesa è inferiore rispetto a quello di una grande impresa e rispetto a quello che servirebbe per attuare delle policy di sicurezza quantomeno accettabili. Si è stimato inoltre che, nel solo 2013, c'è stata una perdita di oltre 800 milioni di record che porterebbe da sola ad uno costo per le imprese di 160 miliardi di dollari l'anno. Più di 3.000 aziende degli USA nel 2013 sono state vittime di cyber attacchi, nel Golfo Persico due sole Banche hanno perso quasi 50 milioni di dollari, una società britannica ha perso più di un miliardo di dollari e in Brasile milioni di dollari vengono sottratti ai clienti annualmente. Tra il 2011 e il 2013 i CERT[67] indiani hanno dichiarato che più di 300 mila siti web sono stati violati da cyber criminali.

Uno dei più ampi studi sull'impatto del cyber crime sugli utenti, il *Norton Cybercrime Report 2012*, stima che ogni anno in media il cyber crime colpisca direttamente oltre 500 milioni di vittime[68]. Le Nazioni più industrializzate subiscono la maggior parte delle perdite, data la loro maggiore informatizzazione, ma la situazione è destinata ad investire anche i Paesi meno sviluppati man mano che aumenterà la loro informatizzazione. Stati Uniti, Cina, Giappone e Germania registrano da sole 200 miliardi di dollari di perdite annue.

Il report presenta le stime medie dei costi a cui le aziende devono incorrere quando subiscono un attacco informatico, in sei nazioni analizzate: Stati Uniti, Germania, Giappone, Francia, Regno Unito e Australia. La differenza tra i dati nazionali potrebbe dipendere sia dalla frequenza e dalle precedenti esperienze di attacco, sia dall'importanza che ogni azienda attribuisce a questa specifica minaccia rispetto ad altre.

---

[64] *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II Center for Strategic and International Studies June 2014*, in <http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf> (ultima consultazione 6-11-2014).

[65] Anche la minore delle stime è comunque più alta delle entrate di molti Stati Nazionali.

[66] Secondo dati Gartner la spesa globale per prodotti e servizi di *cyber security* si aggira intorno ai 70 miliardi di dollari per il 2013, con un incremento del 16% rispetto all'anno precedente, mentre le stime del Ponemon Istitute indicano nelle perdite dirette e indirette causate dal cyber crime una stima di 500 miliardi i dollari, ben un 26% in più rispetto al 2012. È quindi evidente come gli investimenti economici in tema di sicurezza informatica non siano sufficienti a contrastare o quantomeno tamponare l'avanzata della minaccia rappresentata dal cyber crime.

[67] L'acronimo CERT è la denominazione storica per la prima squadra (CERT Coordination Center CERT-CC) presso la Carnegie Mellon University di Pittsburgh (Pennsylvania) nata nel 1988 in risposta al worm Morris, in <https://www.cert.org/about/> (ultima consultazione 10-11-2014).

[68] Stima realizzata su un campione di 13.000 utenti di 24 Paesi.

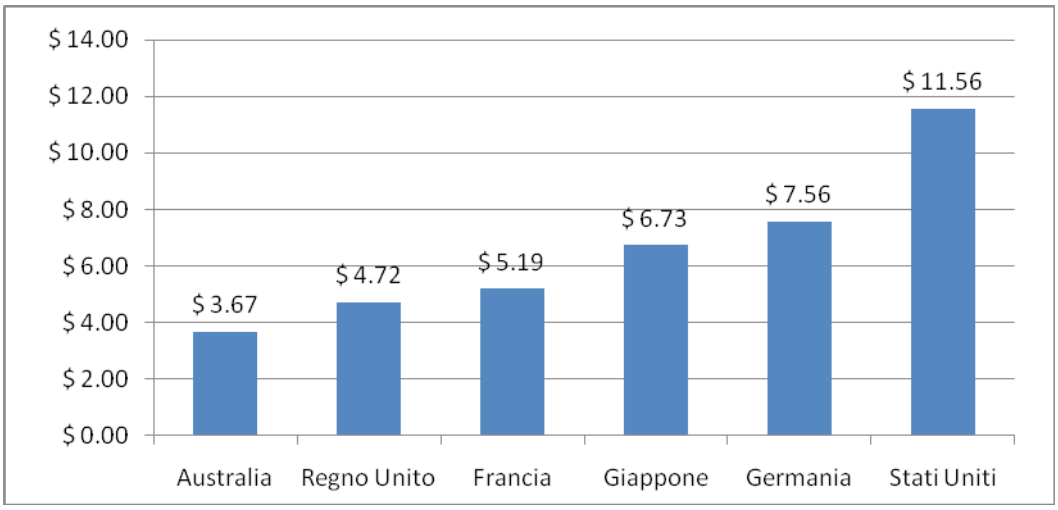


Figura 11 - Dati relativi al costo totale del cyber crime in sei nazioni, espresso in milioni di dollari
Fonte: Cost of Cybercrime Study Global Report, Ponemon Institute, 2013

Altri tipi di perdite, come abbiamo visto, sono molto più difficili da quantificare. Ad esempio le perdite da furto di proprietà intellettuale sono difficilmente stimabili nel breve periodo, ma costituiscono un costo enorme per le aziende soprattutto nel lungo periodo, non solo come perdita diretta, ma soprattutto in termini di costi di recupero, perdita del business e di posti di lavoro.[69] Il cyber crime ha un grave impatto anche in termini di occupazione all'interno di un Paese e il danno maggiore per le società è l'effetto che un attacco può avere sul business, come rapporti con i clienti, indennizzi da corrispondere o penalità contrattuali, costi di recupero dei danni di immagine, contromisure per mitigare le perdite, piani di *disaster recovery* e assicurazioni, danni reputazionali e in termini di competitività. Nei soli Stati Uniti si è registrata una perdita in termini di occupazione di almeno 200 mila posti di lavoro, mentre in Europa si stima che le perdite potrebbero aggirarsi intorno ai 150 mila posti; non solo lavoratori di società strettamente legate al mondo informatico, ma soprattutto dipendenti di aziende in difficoltà dopo ingenti perdite economiche.

E se consideriamo le PMI, i dati sono ancora più allarmanti, secondo *il Symantec Internet Security Threat Report 2014*, i cyber criminali starebbero concentrando le loro risorse negli attacchi nei confronti delle Piccole e Medie Imprese e starebbero diminuendo quelli nei confronti delle grosse aziende. Inoltre, il rapporto sottolinea come le metodologie più usate siano sempre più sofisticate e siano rappresentate soprattutto da phishing, *social engineering*, spesso in modo congiunto, e ransomware.[70]

I dati relativi all'impatto della criminalità informatica sull'occupazione e sulla violazione di proprietà intellettuale non sono facili da stimare, ma non sono certo da sottovalutare, e sono le

[69] Una società britannica ha ammesso di aver subito perdite per 1,3 miliardi dollari a causa di un furto di proprietà intellettuale e, successivamente, aver subito notevoli svantaggi nelle sue attività commerciali. *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II Center for Strategic and International Studies June 2014*, in <http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf> (ultima consultazione 6-11-2014).

[70] *Symantec Internet Security Threat Report 2014*, in <http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf> (ultima consultazione 6-11-2014).

variabili più gravi per l'economia di un Paese, soprattutto per quelli come l'Italia, dove le PMI sono il carattere fondativo dell'identità economica del territorio. Le perdite derivanti da furto di proprietà intellettuale si ripercuotono sul reddito, sulla produzione e sull'occupazione di un'azienda. Se consideriamo l'impatto economico della criminalità informatica, vediamo come il danno principale per le aziende consiste proprio nel furto di proprietà intellettuale[71], danni che iniziano nell'azienda ma che si ripercuotono come cerchi nell'acqua verso le economie locali, nazionali ed internazionali. Tutto questo agisce come un freno alla crescita aziendale, e del Paese nel suo complesso, impedendo la crescita delle economie nazionali e globale, così centrale in tutto il Mondo, soprattutto in questi anni di profonda crisi economica.

Anche se non sono di immediata valutazione, le perdite nel tempo a causa di questo tipo di violazione, non sono da sottovalutare, rispetto alla perdita di dati bancari ed economici, che sono più semplici da calcolare in caso di cyber attacco. Milioni di persone e aziende sono ormai vittime del furto di dati di carte di credito e di prelievi illegittimi sui propri conti correnti, tanto che sta diventando un fenomeno globale. Nel 2013, solo nel Regno Unito, una serie di attacchi su larga scala, con obiettivo soprattutto aziende, ha causato perdite per 850 milioni di dollari e in Australia di circa 100 milioni di dollari.[72]

Nel Regno Unito il National Cyber Crime Unit della National Crime Agency (NCA), ha lanciato una nuova campagna per aumentare la consapevolezza dei pericoli derivanti dalla non adeguata protezione on-line, chiedendo agli utenti di essere "*cyber streetwise*" e adottare misure di sicurezza per proteggere i propri dati. Secondo l'Office of National Statistics, infatti, ci sono state più di 10 mila vittime di virus informatici nel Regno Unito lo scorso anno, l'80% delle quali potevano essere evitate semplicemente aggiornando i programmi di sicurezza e in generale i software installati sul proprio PC.[73] L'obiettivo di questa nuova campagna è ridurre il numero di attacchi messi a segno attraverso messaggi di posta elettronica fraudolenti o l'uso di chiavette USB infette o la mancanza di attenzione nei download su internet e nell'aggiornamento dei programmi, che sono citati come i problemi più comuni tra gi utenti. La campagna inoltre sottolinea come a rischio non sono solo i risparmi degli utenti ma anche i loro dati personali. Le statistiche che hanno spinto a creare questa iniziativa, per la quale sono stati stanziati 860 milioni di sterline in cinque anni, sono quelle riferite alla percentuale di adulti che non installano o aggiornano software di sicurezza, pari al 40%.

Il trend immaginabile per il futuro, purtroppo, può essere solo in crescita, in quanto vi è un basso indice di rischio per gli hacker di essere catturati, una estrema facilità per il cyber criminale di perpetrare questo tipo di reato a fronte di un bassissimo rischio e di enormi guadagni. Studi di settore stimano che internet generi un volume di affari per l'economia globale che varia tra i 2.000 e i 3.000 miliardi di dollari l'anno e che, data l'elevata crescita dell'informatizzazione, costituisca un mercato in costante aumento. Di sicuro questo aspetto può agire da spinta alla crescita

[71] *2014 McAfee Report on the Global Cost of Cybercrime*, in <http://csis.org/event/2014-mcafee-report-global-cost-cybercrime> (ultima consultazione 6-11-2014).

[72] Dati McAfee-CSIS.

[73] *10 Steps to Cyber security Executive Companion CESG The Information Security Arm of GCHQ*, in <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/73128/12-1120-10-steps-to-cyber-security-executive.pdf> (ultima consultazione 6-11-2014).

dell'economia globale, se non fosse così vulnerabile. Il cyber crime rappresenta un'imposta sul valore di questa economia, stimata tra il 15% e il 20%, con un impatto sul PIL mondiale che va dallo 0,4% all'1,4%, con pesanti risvolti, ovviamente, sull'occupazione e sulla crescita, riducendo il tasso di investimento nell'innovazione da parte delle società.

Attraverso i dati fornitici per questa ricerca dal dott. Paolo Passeri, che da anni analizza i maggiori cyber attacchi che si verificano a livello globale, possiamo notare che il cyber crime rappresenta costantemente la principale motivazione che si cela dietro gli attacchi ai danni di attori pubblici e privati.

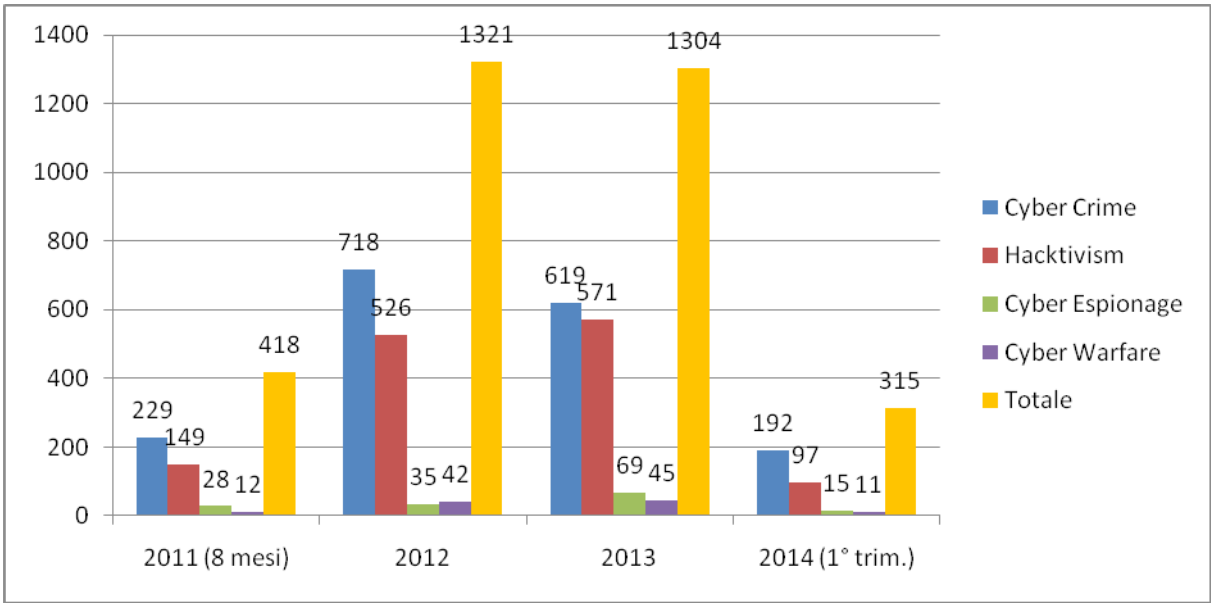


Figura 12 - Motivazione alla base dei maggior cyber attacchi nel Mondo, 2011-2014
Fonte: Elaborazione dei dati forniti per questa ricerca dal dott. Paolo Passeri, 2014

Un altro aspetto che caratterizza il fenomeno del cyber crime e che purtroppo lo rende così insidioso è che essendo fortemente legato alla tecnologia è un fenomeno con un alto potenziale di crescita, parallelo all'aumento della digitalizzazione di ogni aspetto della vita quotidiana ed economica e all'aumento esponenziale degli utenti internet.

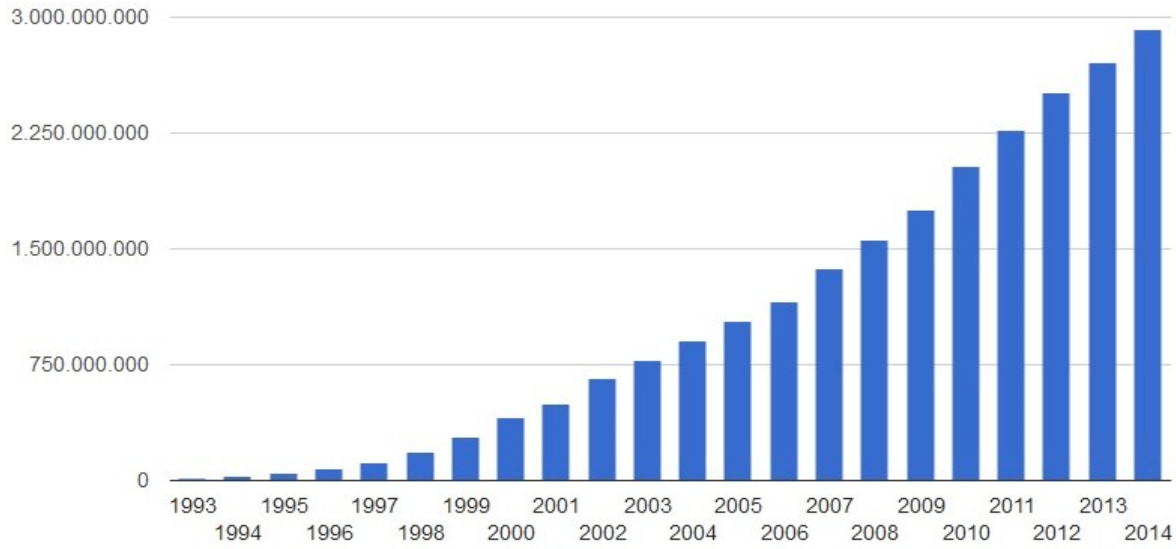


Figura 13 - Numero degli utenti internet globali
Fonte: Internet Live Stats[74], 2014

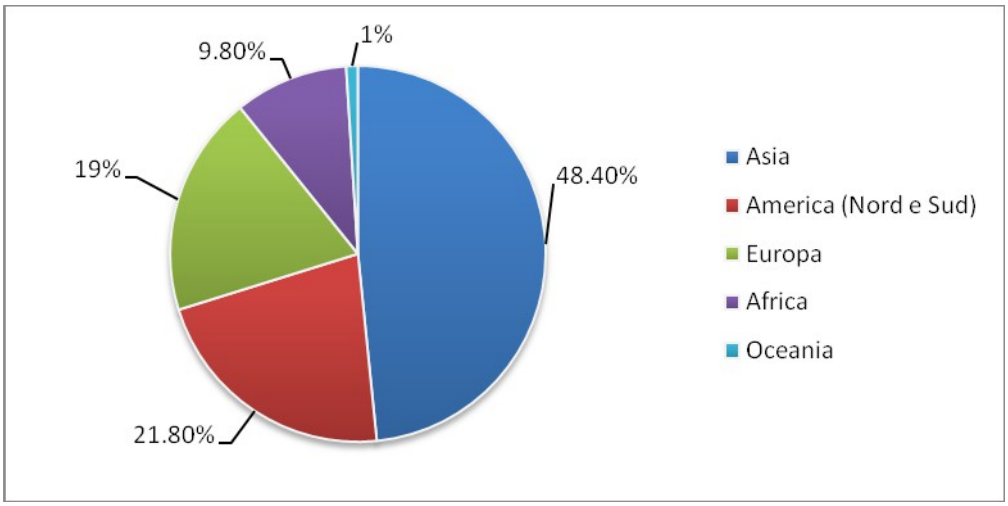


Figura 14 - Utenti internet per Continente a luglio 2013
Fonte: Internet Live Stats, 2013

Sono in aumento i reati contro i dispositivi mobili, smartphone e tablet, e i clienti che ne fanno uso; i crimini perpetrati attraverso i social media, sui quali moltissime aziende hanno un profilo pubblico; attacchi attraverso servizi di internet banking, attacchi contro aziende multinazionali da parte di hacktivist, che sfruttano l'enorme eco che il web garantisce a queste azioni dimostrative in tutto il Mondo. L'aumento esponenziale dei big data che vengono resi disponibili su internet aumenterà di conseguenza la possibilità e l'efficacia delle offensive cyber con l'obiettivo di rubare la nuova moneta di internet, l'informazione.

Secondo lo studio *The 2013 Cost of Cybercrime Study* realizzato dal Ponemon Institute, il costo del crimine informatico è aumentato del 78% rispetto a quattro anni fa, ma a preoccupare è anche il dato riguardante il tempo necessario per la risoluzione di un problema, che è aumentato del 130% nello stesso arco temporale. Al furto di dati sono imputabili le principali perdite, il 43%

[74] Internet users in the world, in <http://www.internetlivestats.com/internet-users/> (ultima consultazione 6-11-2014).

dei costi totali dovuti al cyber crime; mentre i danni al business e la perdita di competitività incidono per il 36%.

Sempre secondo la ricerca del Ponemon Institute[75], nell'ultimo anno, il costo totale medio per la violazione dei dati, a livello mondiale, è aumentato del 15%, raggiungendo i 3,5 milioni di dollari; e per ogni singolo record la percentuale è aumentata di oltre il 9% passando da 136 dollari a 145 dollari. L'importanza di questo dato consiste nel fatto che non sono dati ipotetici, ma stime fornite direttamente dalle aziende coinvolte nello studio[76] che hanno subito questi danni e che hanno registrato da un minimo di circa 2.415 a poco più di 100 mila record compromessi. Il costo medio più alto pagato per violazione è stato di 201 dollari per singolo record a danno delle aziende statunitensi e di 195 dollari per record a danno di quelle tedesche. In Germania e in Francia inoltre il report registra un investimento maggiore in attività di rilevamento e valutazione della violazione dei dati rispettivamente con uno stanziamento di, 1,3 milioni di dollari e 1,1 milioni di dollari.

A livello globale il cyber crime rappresenta un fenomeno sempre più serio, per le aziende, i cittadini e i Governi che incominciano a sviluppare strategie per contrastarlo.

In Australia, nel 2012, 5,4 milioni di cittadini sono stati vittime di reati informatici, con un costo stimato per l'economia di 1,65 miliardi di dollari. Ciò ha richiesto una risposta significativa per la sicurezza. La minaccia informatica è stata individuata come uno dei principali rischi nella strategia di sicurezza nazionale. A maggio 2014 è stato istituito a Camberra un nuovo *Cyber security* Centre (ACSC) che si avvale delle competenze dei migliori esperti di sicurezza informatica della Nazione, che costituirà il fulcro degli sforzi in tema di sicurezza informatica del Governo e aumenterà la capacità della Nazione di difendersi dagli attacchi informatici. L'ACSC comprende, in un unico luogo, i maggiori nuclei operativi dalla *Defense Intelligence Organisation* all'*Australian Security Intelligence Organisation*, dal Dipartimento di *Emergency Response Team Australia*, alla Polizia Federale Australiana e la Commissione Crimine australiano. Il centro analizzerà la natura e la portata delle minacce informatiche, e guiderà la risposta del Governo in caso di incidenti informatici. Il lavoro è svolto a stretto contatto con i settori delle infrastrutture critiche e delle imprese del Paese, per proteggere reti e sistemi nazionali creando una sorta di comunità epistemica, con l'obiettivo di far fronte a questo tipo di minacce. Il centro fornisce anche consulenza e supporto per lo sviluppo di strategie di prevenzione per contrastare le minacce informatiche.

Un altro interessante esempio di come può essere affrontato il cyber crime è rappresentato dalla strategia in tema di *cyber security* rilasciata dal Canada nel mese di ottobre 2010. Oltre a contenere direttive in tema di sicurezza e protezione dei sistemi in ambito governativo e delle infrastrutture critiche e a prevedere la collaborazione al di fuori del Governo federale sui sistemi informatici vitali, la strategia canadese contiene anche un aspetto innovativo

[75] *2013 Cost of Cyber Crime Study: Global Report*, Ponemon Istitute, in <http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf> (ultima consultazione 6-11-2014).

[76] Hanno partecipato 1.690 individui di 314 aziende, intervistati nel corso di un periodo di dieci mesi, che rappresentano i seguenti 10 Paesi: Stati Uniti, Regno Unito, Germania, Australia, Francia, Brasile, Giappone, Italia, India, Emirati Arabi Uniti e Arabia Saudita.

rispetto alle strategie delle altre Nazioni, cioè sostiene la programmazione di azioni per rafforzare l'istruzione e la consapevolezza della popolazione canadese circa le minacce informatiche e il corretto uso del web. La strategia prevede la collaborazione con gli altri Governi e con l'industria IT per garantire che i sistemi vitali per la sicurezza canadese, la prosperità economica e la qualità della vita siano protetti.

Sempre più Governi investono nella prevenzione in ambito informatico attraverso politiche di lotta al cyber crime, considerato un pericolo per l'economia nazionale. I funzionari della difesa indiani hanno dichiarato che l'India si prepara ad affrontare un'escalation di attacchi informatici pericolosi per la propria economia e che per questo dal 2012 è partito un piano per arruolare sino a 500 mila specialisti del cyber nel corso dei prossimi 5 anni[77]. L'India, inoltre, ha firmato un protocollo, non vincolante, con gli Stati Uniti per la cooperazione tecnica e operativa per contrastare le minacce informatiche[78].

Gli Stati Uniti, dal conto loro, si confermano una delle nazioni più interessate da questo fenomeno. Negli ultimi dieci anni, infatti, la consapevolezza americana circa la rilevanza della minaccia informatica proveniente da Nazioni, organizzazioni terroristiche, criminali e altri soggetti è cresciuta sino a portare alla formulazione di una delle prime strategie in ambito informatico. Nel mese di maggio 2011 la Casa Bianca ha presentato la sua strategia internazionale per il *cyber space* e nel novembre 2011, in base al *National Defense Authorization Act*, il Dipartimento della Difesa ha riferito che la Nazione si riserva il diritto di reagire militarmente per eventuali "attacchi informatici significativi diretti contro l'economia degli Stati Uniti, il Governo o l'apparato militare". Secondo stime non ufficiali il cyber crime transnazionale organizzato incassa 12 miliardi di dollari all'anno, con danni diretti ed indiretti per quasi 400 miliardi di dollari. A questo si aggiunge circa un trilione di dollari l'anno, frutto di spionaggio industriale (privato e governativo), sottrazione di proprietà intellettuale e dati sensibili. In questo scenario, nel corso del 2012, il Governo degli Stati Uniti ha creato *CyberCity*, un vero e proprio campo di addestramento per formare tecnici, un ambiente virtuale dove vivono 15 mila persone con i loro account e le loro abitudini sociali, con tutti i servizi come Banche, ospedali, centrali elettriche, bar, ristoranti, Università, PMI, zone WI-FI, ecc. La *CyberCity* ha una caratteristica particolare: è costantemente sotto attacco e di conseguenza difesa dagli hacker-soldati.[79] Il Presidente Obama ha dichiarato che la "*minaccia informatica è una delle sfide più gravi per la sicurezza economica e nazionale che abbiamo di fronte come Nazione"* e che "*la prosperità economica degli Stati Uniti nel XXI secolo dipenderà dalla sicurezza informatica*".

Recentemente nella città di New York, che nel 2013 ha registrato un forte aumento di violazioni di dati che hanno colpito soprattutto imprese e attività commerciali, è stata avviata una collaborazione tra FBI e *New York Police Department* (NYPD) e la *Metropolitan Transportation Authority* (MTA) per rispondere specificatamente ai reati finanziari commessi attraverso l'uso del mezzo informatico. Questa nuova *task force* si concentrerà sui crimini nella zona di New York,

---

[77] *India training half a million cyber security experts*, in <http://www.timeslive.co.za/scitech/2012/10/16/india-training-half-a-million-cyber-security-experts> (ultima consultazione 6-11-2014).

[78] *India to greenlight state-sponsored cyber attacks. Gov agencies will get the nod,* di Phil Muncaster, in <http://www.theregister.co.uk/2012/06/11/india_state_sponsored_attacks/> (ultima consultazione 6-11-2014).

[79] Per comprendere le migliori strategie di sicurezza informatica è necessario entrare nella mentalità dell'attaccante, per poterne prevedere ed ostacolare le mosse. L'aspetto psicologico e sociologico diventa essenziale.

collaborando anche con agenzie federali straniere, studiando tutti i reati finanziari, dai furti delle carte di credito ai casi di frode, ad attacchi sui sistemi di pagamento e piattaforme di *trading*. I reati informatici di natura finanziaria rappresentano i reati più comuni, ma anche quelli con maggior impatto sull'economia di un Paese. I reparti di sicurezza informatica di aziende private collaboreranno con la neonata *task force* condividendo informazioni su incidenti informatici. Questa collaborazione tra agenzie locali, federali ed internazionali è necessaria per contrastare una criminalità, come quella informatica, che ha come caratteristica peculiare quella di non avere confini e territorialità. L'*Internet Crime Complaint Center* (IC3) nel 2013 ha elaborato 262 mila denunce, che rappresentano più di 781 milioni di dollari di perdite.[80]

Secondo un sondaggio McAfee, su 1.000 aziende, quasi il 90% delle Piccole e Medie Imprese negli Stati Uniti non usano protezione dei dati riguardanti informazioni su clienti e società e meno della metà proteggono la posta elettronica aziendale per evitare truffe come il phishing. Il Centro Internazionale per gli Studi Strategici di Washington ha stimato che la criminalità informatica e il cyber spionaggio costano all'economia americana 100 miliardi di dollari l'anno e all'economia globale circa 300 miliardi di dollari. Le Piccole e Medie Imprese sono ancora all'oscuro della minaccia, infatti i due terzi ritengono i loro dati e dispositivi al sicuro da attacchi hacker, nonostante solo il 9% protegga gli smartphone dei loro dipendenti.

Negli ultimissimi anni, diversi Stati hanno iniziato a sviluppare politiche di sicurezza informatica, anche attraverso il sostegno alle PMI innovative impegnate direttamente in questo settore. Francia, Stati Uniti e Regno Unito promuovono opportunità per le PMI che si occupano di prodotti innovativi nel campo informatico e permettono loro di avere un ruolo attivo nel rendere il *cyber space* un luogo più sicuro.

Come già menzionato è necessario evidenziare che, allo stato attuale, la maggior parte dei report che forniscono dati e statistiche relative al fenomeno del cyber crime sono redatti da società informatiche di settore. Mancano invece molto spesso statistiche redatte da fonti ufficiali e nazionali. Questo sarebbe utile non solo per capire il reale impatto di questo fenomeno sull'economia a livello nazionale, ma anche per creare dei database internazionali che misurino, in base alle rispettive normative nazionali, i reati di cyber crime, per pianificare interventi di contrasto sia a livello locale che regionale che nazionale ed internazionale. I dati aggregati a livello globale spesso danno una minore percezione del fenomeno a livello locale. Il singolo cittadino, come una PMI, senza dei dati ufficiali di quanto questo fenomeno sia diffuso anche nella propria zona, potrebbe correre il rischio di sottovalutarne la reale pericolosità ed interpretare i dati globali come relativi al solo mondo delle grandi imprese multinazionali o confinato ai Paesi esteri come ad esempio gli Stati Uniti; o semplicemente ritenerlo distante dalla propria quotidianità e cadere nell'errore di considerarlo come un rischio che non lo riguarderà mai. Sarebbe utile avere quindi anche dei dati e delle stime ufficiali a livello nazionale da parte di ogni singolo Stato, da comparare poi a livello internazionale.

2.2 Il cyber crime come minaccia in Europa

[80] *2013 Internet Crime Report*, IC3, in <https://www.ic3.gov/media/annualreport/2013_ic3report.pdf> (ultima consultazione 6-11-2014).

In Europa la situazione non è di certo migliore, infatti, secondo le stime dell'Interpol, il cyber crime sarebbe un affare da 750 miliardi[81] di euro l'anno[82].

A livello europeo, la recente ricerca di Eurobarometro[83] conferma che i cittadini europei considerano la sicurezza informatica come un argomento che suscita enormi preoccupazioni; i dati rilevano che l'89% del campione dichiara di essere preoccupato della sicurezza delle proprie informazioni personali accessibili on-line e il 74% pensa che il rischio di essere vittima del cyber crime sia aumentato rispetto all'anno precedente. I dati più interessanti del rapporto indicano come il 10% degli utenti europei intervistati abbia la certezza di aver subito frodi on-line e il 6% di essere stato vittima di furto di identità.

La possibilità di poter diventare vittima di un criminale su internet è una paura che comincia ad essere considerata, ma nonostante ciò non diminuisce il livello di disinvoltura con il quale molti utenti condividono on-line le proprie informazioni personali senza curarsi di misure di prevenzione o sicurezza, permettendo in questo modo ai cyber criminali di avere facilmente accesso ad una considerevole quantità di dati personali. Inoltre il 50% del campione ammette di non aver cambiato nessuna password dei suoi servizi on-line nell'ultimo anno e il 52% si sente poco o male informato riguardo le minacce della criminalità informatica. Il 12% ha subito un blocco nell'accesso ad internet, ad un altro 12% è stato hackerato il proprio account di social network, mentre il 7% ha subito il furto della carta di credito.

Solo la metà degli europei mette in atto misure di protezione accettabili per affrontare questo tipo di criminalità.

Nel Regno Unito, nel 2013, il 93% delle grandi aziende e il 76%[84] delle Piccole e Medie Imprese ha denunciato un attacco di natura informatica[85] con costi che vanno da 110 mila a 250 mila sterline per le grandi aziende e tra 15 mila e 30 mila sterline per singola PMI.[86] È da considerare che le stime potrebbero essere in realtà molto più alte dato che le frodi segnalate sono di certo minori di quelle realmente avvenute, sia perché non sempre ci si accorge di aver subito una frode sia perché questa potrebbe essere in realtà non denunciata. La *Federation of small businesses* (FSB) inglese ha pubblicato un interessante studio sui costi dei crimini informatici

---

[81] *Opening Remarks by INTERPOL PRESIDENT KHOO BOON HUI.* At the 41ST EUROPEAN REGIONAL CONFERENCE (ISRAEL, TEL AVIV, 8 MAY 2012), in <http://www.interpol.int/content/download/14086/99246/version/1/file/41ERC-Khoo-Opening-Speech.pdf> (ultima consultazione 10-11-2014).

[82] Alla fine del 2012 un gruppo di cyber criminali ha lanciato un malware che, restringendo l'accesso ai computer infettati, ha fruttato addirittura circa 1 milione di euro per ogni attacco.

[83] Cyber Security Report Special Eurobarometer 404, in <ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf> (ultima consultazione 6-11-2014).

[84] 87% per il McAfee Report 2014.

[85] *2013 Information security breaches survey Technical Report*, in <https://www.pwc.co.uk/*asset*s/pdf/cyber-security-2013-technical-report.pdf> (ultima consultazione 6-11-2014).

[86] Se si prendono in considerazione le peggiori violazioni di sicurezza si può arrivare a costi che oscillano dalle 35.000 alle 65.000 sterline per le PMI, e dalle 450.000 alle 850.000 sterline per le aziende più grandi. A tal proposito si legga *SMEs face increased risk of cyber attack***,** in <http://www.prweb.com/releases/2014/09/prweb12147240.htm> (ultima consultazione 6-11-2014).

subiti dalle Piccole e Medie Imprese nel Regno Unito ed ha rivelato l'aumento del fenomeno[87]. Inoltre circa il 30% dei suoi membri è stato vittima di frode, oltre il 50% delle PMI inglesi è stato colpito da un malware, l'8% è stato vittima di hacking e circa il 5% ha subito violazioni di sicurezza. Per far fronte a questa problematica, il Centro Antifrode inglese, *Action Fraud*, ha sviluppato una sezione del proprio sito web, dedicata alla sensibilizzazione al problema e a offrire informazioni riguardo la prevenzione dagli attacchi e la protezione dei dati per le PMI, che riguardano i punti deboli delle aziende come clienti, fornitori, dipendenti e beni. All'interno del sito è presente una sezione per la denuncia on-line di tentativi di frode subiti.[88] Il rapporto evidenzia come proteggere le PMI dal cyber crime sia strategico anche per difendere le grandi aziende e quindi l'economia del Paese.

Secondo la stima della FSB, proiettando i dati relativi alle piccole imprese su scala nazionale, il costo della criminalità informatica è superiore a 18,8 miliardi di sterline.

Nel Regno Unito ci sono circa 4,8 milioni di PMI e, nonostante l'impatto della criminalità informatica e l'elevata frequenza di eventi dannosi, quasi il 20% non avevano preso alcuna contromisura per mitigare le minacce informatiche[89]. La *cyber security*, per il Governo britannico, è un argomento molto importante per la crescita di tutto il Regno Unito; il ministro James Brokenshire[90] ha commentato i risultati proposti dallo studio, stimolando l'azione e l'adozione di un approccio proattivo alla criminalità informatica. Il Governo britannico, inoltre, ha emanato il *Data Protection Bill*, che imporrà alle imprese di denunciare tutti gli incidenti informatici e le violazioni subite. Il forte sostegno del Governo e delle principali imprese è un fattore essenziale per sostenere la crescita di una cultura della sicurezza che potrebbe aiutare a ridurre gli effetti della criminalità informatica.

Un'altra interessante iniziativa del Governo britannico riguarda una nuova partnership con il mondo industriale, per condividere informazioni sulle minacce alla sicurezza informatica. La *Cyber security Information Sharing Partnership* (CISP) prevede la realizzazione di una piattaforma on-line attraverso la quale è possibile scambiarsi in tempo reale informazioni sulle minacce e le vulnerabilità.[91]

La Germania registra notevoli danni finanziari ed in termini di perdita di creazione di valore, di fiducia e derivanti dallo spionaggio industriale. Uno studio del Corporate Trust afferma che lo spionaggio industriale colpisce le industrie tedesche per circa 4 mila miliardi di euro all'anno. La più grande azienda di telecomunicazione tedesca, la Deutsche Telekom, dichiara di subire circa

---

87 *Cost of cybercrime for UK Small Businesses*, di Pierluigi Paganini in Security Affairs, in <http://securityaffairs.co/wordpress/14628/cyber-crime/cost-of-cybercrime-for-uk-small-businesses.html> (ultima consultazione 6-11-2014).

88 *ActionFraud is the UK's national fraud and internet crime reporting centre*, in <http://www.actionfraud.police.uk/> (ultima consultazione 6-11-2014).

89 Una recente ricerca ha scoperto che solo il 12% delle imprese intervistate ha investito in assicurazioni contro le minacce informatiche.

90 Minister of State for Security and Immigration.

91 *Government launches information sharing partnership on cyber security*, in <https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security> (ultima consultazione 6-11-2014).

450 mila attacchi al giorno e che questo numero è in continuo aumento; la sicurezza dei sistemi IT è un fattore che, senza dubbio, rallenta lo sviluppo economico e sociale della Germania.

Uno studio della BITCOM, considerando la totalità delle aziende tedesche, afferma che nel solo anno 2012 oltre il 39% delle aziende è stata vittima di un attacco informatico, come furto di dati, violazione di brevetti e proprietà intellettuale, spionaggio, frode, intercettazioni e danni ai sistemi.[92]

La gravità della situazione è confermata infatti anche dai dati relativi alle PMI tedesche, il 96% delle quali ha già avuto incidenti di sicurezza informatica e relativi danni.[93] Di conseguenza il *Federal Ministry of Education and Research* (BMBF - *Bundesministerium für Bildung und Forschung*) e il Ministero Federale degli Interni dal 2009 stanno supportando la ricerca nel settore della sicurezza dell'informazione e della comunicazione "*IT Security Research*" per lo sviluppo di nuove tecnologie in questo settore.

Le PMI utilizzano principalmente sistemi di sicurezza base, come firewall e antivirus, che spesso non sono sufficienti a garantire un adeguato livello di protezione. Il progetto "*SIEM für Klein und Mittelständische Unternehmen*" (SIMU)[94] sta quindi studiando come poter adattare alle PMI i sistemi di sicurezza più complessi, *Security Information and Event Management* (SIEM) utilizzati dalle grandi imprese e spesso economicamente non accessibili alle piccole aziende.

Sebbene i dati forniti nei vari report fin quei esaminati diano senza dubbio informazioni utili su come questo fenomeno si stia evolvendo nel tempo nei confronti di cittadini e aziende, nonostante la difficoltà nel quantificare l'entità e i danni che tale fenomeno comporta, ancora una volta bisogna considerare che sono per la maggior parte redatti da società private di sicurezza informatica e che non ci sono ancora stime ufficiali da parte dei vari Governi ed enti sovranazionali che possano dare un quadro più preciso e comparabile a livello internazionale.

2.3 L'attività dell'Unione Europea contro il cyber crime

Con la pubblicazione del documento "*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyber space*"[95] del 7 febbraio 2013, l'Unione Europea prende atto che il *cyber space* costituisce una dimensione sempre più importante a livello internazionale e vuole dare inizio ad una intensificazione delle sue azioni in questo campo, definendo ruoli, responsabilità e azioni necessarie, basate anche sulla tutela e sulla promozione dei diritti dei cittadini. Rendere il

[92] L'Ufficio federale di polizia criminale dichiara un aumento del 3,4% dei crimini informatici nel 2012, con un totale di 87.871 casi. I reati che comportano alterazione dei dati e sabotaggio di computer (+133,8%) stanno diventando un pericolo crescente.

[93] *Cybersecurity research to boost Germany's competitiveness*, in <http://www.bmbf.de/en/73.php> (ultima consultazione 6-11-2014).

[94] Parte del programma "PMI innovative" del BMBF.

[95] European Commission *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* 7/2/2013, in <http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf> (ultima consultazione 6-11-2014).

cyber space più sicuro e combattere l'analfabetismo digitale diventano priorità che l'UE non può più permettersi di ignorare. L'Unione Europea ha strutturato il suo sistema di *governance* attorno a tre pilastri.

Il primo pilastro, fondato nel 2005, è la Agenzia Europea della Sicurezza delle Reti e delle Informazioni (*European Network and Information Security Agency*, ENISA) che individua le cause e crea dialogo, *awareness* e fornisce informazioni e best practices ai Paesi Membri dell'UE.

Il secondo pilastro ha completato la protezione contro le minacce informatiche, mediante l'istituzione del *Centro Europeo sulla Criminalità Informatica* (EC3)[96], di cui parleremo in seguito.

Nell'ambito del terzo pilastro, lanciato nel 2010 con l'*Agenda digitale per l'Europa*[97], l'Unione Europea ha adottato una serie di leggi e iniziative che promuovono lo sviluppo di opportunità sociali ed economiche nel mondo digitale, come ad esempio la protezione della proprietà intellettuale, lo sviluppo di una copertura a banda larga, l'e-commerce e la firma elettronica. Anche il Parlamento Europeo, assistito dal Garante europeo della protezione dei dati, è un attore essenziale della *governance* in materia di sicurezza informatica dell'UE in quanto bilancia i tre pilastri.

Come accennato, il primo dei tre pilasti intorno al quale l'Unione Europea ha strutturato il suo sistema di *governance* è l'ENISA, costituita nel marzo del 2004.

L'Agenzia promuove all'interno della Comunità Europea lo sviluppo di una cultura della sicurezza per cittadini, imprese ed organizzazioni pubbliche, aiutando la Commissione Europea, gli Stati Membri e le aziende di settore ad evitare e affrontare problemi di sicurezza dell'informazione e delle reti. L'obiettivo dell'Agenzia è che il proprio sito costituisca un "hub" europeo per lo scambio di informazioni, best practices e conoscenze, nel campo della sicurezza delle informazioni. Dal 2007 ENISA si è occupata anche di promuovere lo sviluppo di politiche di sicurezza mirate per le PMI, data la loro notevole importanza a livello economico europeo.[98] Nel 2009 l'Unione Europea ha stabilito che gli Stati Membri dell'ENISA devono notificare annualmente, a partire dal 2011, gli incidenti subiti esclusivamente nel settore delle comunicazioni elettroniche.

La Commissione Europea ha invitato l'ENISA a condurre uno studio di fattibilità su un sistema di condivisione a livello europeo, per aumentare la consapevolezza della sicurezza IT e per colmare le lacune nella copertura di tali informazioni, soprattutto per i cittadini e le PMI. Nel suo recentissimo report *Annual Incident Reports 2013 Analysis of Article 13a annual incident reports*[99]

[96] La Commissione Europea ha annunciato la decisione di istituire un Centro europeo per la lotta alla criminalità informatica (EC3) all'interno de "*La strategia di sicurezza interna dell'UE in azione*", adottata il 22 novembre 2010, in <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:IT:PDF> (ultima consultazione 6-11-2014).

[97] *Digital Agenda for Europe* è una delle iniziative della strategia Europa 2020, che definisce gli obiettivi di crescita che l'Unione Europea si prefigge di raggiungere entro il 2020. L'Agenda Digitale propone di sfruttare le tecnologie dell'informazione e della comunicazione (TIC) per incentivare l'innovazione, la crescita economica e il progresso, in <http://ec.europa.eu/digital-agenda/digital-agenda-europe> (ultima consultazione 6-11-2014).

[98] *ENISA Deliverable: Information Package for SMEs*, in <http://www.enisa.europa.eu/act/rm/cr/risk-management-inventory/files/deliverables/information-package-for-smes/at_download/fullReport> (ultima consultazione 6-11-2014).

[99] *Annual Incident Reports 2013 Analysis of Article 13a annual incident reports September 2014*, in <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-

che riporta i dati relativi agli incidenti significativi del settore delle comunicazioni, segnalati a norma dell'Articolo 13 bis della Direttiva Quadro (2009/140/CE)[100], da parte delle autorità nazionali di regolamentazione (ANR) dei diversi Stati Membri dell'UE, ENISA effettua un'analisi aggregata degli incidenti che hanno comportato gravi interruzioni di servizio sul territorio europeo.[101]

Un'ulteriore iniziativa politica della Commissione Europea di particolare rilevanza è rappresentata dalla Comunicazione relativa alla protezione delle infrastrutture critiche informatizzate[102] che sottolinea come le infrastrutture critiche informatizzate siano fondamentali per la crescita economica e sociale dell'Unione e predispone un piano d'azione per rafforzarne la sicurezza e la resilienza e che ha contribuito ad accrescere il ruolo dell'ENISA a livello europeo sul piano tattico ed operativo.

L'*European Information Sharing and Alert System* (EISAS) infatti, rappresenta un sistema di condivisione delle informazioni e di allarme europeo, cerca di migliorare la cooperazione degli Stati Membri per raggiungere i cittadini e le PMI attraverso la raccolta, l'elaborazione e la diffusione delle informazioni di sicurezza rilevanti.[103] Si prefigge l'obiettivo di responsabilizzare i cittadini europei e le PMI al fine di sviluppare conoscenze e competenze per proteggersi dalle minacce in ambito cyber e implementare le capacità degli Stati Membri attraverso la cooperazione tra i CERT nazionali.[104] Il progetto, del 2012, coinvolge un campione di più di 1.500 persone tra cittadini e PMI di tutta Europa, dal quale emergono dati poco rassicuranti come la bassissima conoscenza dei principali vettori di attacco e come spesso si preferisca rivolgersi, in caso di difficoltà a livello IT, ad amici e familiari piuttosto che a professionisti del settore.

ENISA organizza e coordina anche esercitazioni a livello europeo per testare le capacità dei Paesi Membri nel rispondere ad un attacco di natura informatica.[105] Il 4 ottobre del 2012 si è

reports-2013/at_download/fullReport> (ultima consultazione 6-11-2014).

[100] La riforma del quadro normativo comunitario per le comunicazioni elettroniche, che è stata adottata nel 2009 ed è stata recepita dalla maggior parte dei Paesi dell'UE a maggio 2011, aggiunge l'articolo 13 bis della direttiva quadro. L'articolo 13 bis riguarda la sicurezza e l'integrità di reti pubbliche di comunicazione elettronica e servizi.

[101] Quest'anno, 19 Paesi hanno segnalato 90 incidenti rilevanti e 9 Paesi invece hanno segnalato incidenti non significativi.

[102] Commissione Europea, *Proteggere le infrastrutture critiche informatizzate. "Rafforzare la preparazione, la sicurezza e la resilienza per proteggere l'Europa dai ciberattacchi e dalle ciberperturbazioni"* COM (2009) 149, 30 marzo 2009, in <http://europa.eu/legislation_summaries/information_society/internet/si0010_it.htm> (ultima consultazione 20-11-2014).

[103] *EISAS - European Information Sharing and Alert System, A Feasibility Study 2006/2007*, in <http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/files/EISAS_finalreport.pdf> (ultima consultazione 6-11-2014).

[104] *EISAS Basic Toolset 1.0 Feasibility Study of Home Users' IT Security*, in <http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas-basic-toolset/at_download/fullReport> (ultima consultazione 6-11-2014).

[105] Il vice Presidente della Commissione Europea, Neelie Kroes ha dichiarato, in occasione della recente esercitazione: "La complessità e la quantità di incidenti di tipo cyber stanno aumentando ogni giorno e non possono essere contrastati se i singoli Stati lavorano da soli o se sono solo piccoli gruppi ad agire in maniera coordinata. Sono contenta che gli Stati Membri dell'Unione Europea e dell'EFTA stiano lavorando insieme alle Istituzioni Europee coordinate da ENISA. Solo questo tipo di sforzi comuni potranno proteggere la nostra società ed economia.", in <http://www.enisa.europa.eu/media/press-releases/biggest-ever-cyber-security-exercise-in-europe-today> (ultima

effettuata una simulazione di un cyber attacco su scala europea che per la prima volta ha visto anche la partecipazione di Banche e società di IT[106]. Quattrocento specialisti del settore privato e pubblico hanno affrontato 1.200 incidenti informatici per valutare la risposta e la cooperazione, se un vero e proprio attacco congiunto contro i siti web pubblici e le principali Banche europee si fosse effettivamente verificato. Nel mese di agosto del 2013, l'ENISA ha pubblicato un rapporto conseguente l'esercitazione, concludendo che la mancanza di trasparenza e di informazione sugli incidenti ha reso difficile capire l'impatto globale, le cause e le possibili interdipendenze della legislazione sulla sicurezza. Questo tipo di esercitazione si effettua ogni due anni.

Quest'anno è stata realizzata la più grande esercitazione europea mai effettuata nel suo genere. L'esercitazione, denominata *Cyber Europe 2014*[107], coordinata sempre dall'Agenzia Europea della Sicurezza delle Reti e delle Informazioni ha visto la partecipazione di più di 200 organizzazioni provenienti da 29 Stati europei, 26 Stati Membri dell'Unione e 3 dell'*European Free Trade Association* (EFTA), con il fine ultimo di collaudare le capacità di contrasto dei singoli Paesi alle minacce informatiche e la cooperazione a livello nazionale e internazionale tra settore pubblico e privato con la simulazione di oltre 2.000 differenti incidenti di *cyber security*, tra cui attacchi DDoS, defacement, pubblicazione di informazioni sensibili e attacchi a infrastrutture critiche come quelle energetiche e di telecomunicazioni.[108] Questa esercitazione ha visto anche la collaborazione di oltre 400 esperti provenienti dal settore pubblico e privato come Agenzie di *cyber security*, CERT, Ministeri, Operatori di telecomunicazioni, Compagnie del settore energetico, Istituzioni finanziarie e Internet Service Provider ed ha testato tra l'altro anche la cooperazione a livello europeo e le procedure di escalation[109]. I risultati di questa esercitazione verranno pubblicati nei prossimi mesi attraverso un report redatto da ENISA.

Sempre nell'ambito della sicurezza delle infrastrutture critiche si inserisce la Comunicazione "relativa alla protezione delle infrastrutture critiche informatizzate"[110] che ha ribadito il ruolo centrale dell'ENISA per quanto riguarda la protezione delle IC e ha invitato gli Stati Membri a realizzare un proprio CERT nazionale.

---

consultazione 6-11-2014).

[106] *Europe tests cyber security capabilities in simulation* di Andrew Wagaman, in <http://www.neurope.eu/article/europe-tests-cyber-security-capabilities-simulation-today> (ultima consultazione 6-11-2014).

[107] *Biggest ever cyber security exercise in Europe today*, ENISA, in <http://www.enisa.europa.eu/media/press-releases/biggest-ever-cyber-security-exercise-in-europe-today> (ultima consultazione 6-11-2014).

[108] L'Italia ha partecipato a questa simulazione con 10 Organizzazioni del settore pubblico e privato, per un totale di circa 50 esperti tecnici in materia di sicurezza informatica.

[109] Procedure Operative Standard Europee (EU-SOPs), un insieme di strumenti standard che comprende, la lista dei Punti di Contatto nazionali, *template* operativi, flussi di lavoro, *best practices* e guide su come gestire i grandi incidenti di tipo informatico.

[110] Commissione Europea, *Commissione relativa alla protezione delle infrastrutture critiche informatizzate "Realizzazioni e prossime tappe: verso la sicurezza informatica mondiale"* COM (2011) 163, 31 marzo 2011, in <http://ec.europa.eu/transparency/regdoc/rep/1/2011/IT/1-2011-163-IT-F1-1.Pdf> (ultima consultazione 20-11-2014).

All'interno delle istituzioni europee, il *Computer Emergency Response Team*, CERT-EU[111], è stato istituito alla fine del 2012, per rispondere alle crescenti minacce informatiche e per sostenere il lavoro dei CERT nazionali, la cui istituzione è fortemente voluta e raccomandata dall'Agenda Digitale europea. Il team è composto da esperti di sicurezza IT delle principali istituzioni UE (Commissione Europea, Segretariato generale del Consiglio, Parlamento Europeo, Comitato delle Regioni, Comitato economico e sociale) e collabora con gli altri CERT degli Stati Membri e con società di sicurezza IT specializzate e opera sotto la supervisione strategica di un comitato direttivo interistituzionale[112]. Sotto questo aspetto c'è ancora tanto da fare perché, a livello europeo, si sono incontrate notevoli difficoltà nella realizzazione di CERT nazionali effettivamente operativi e di sicuro questo costituisce un gap che è necessario colmare.

L'Unione Europea non ha un unico approccio alla sicurezza informatica; in generale, le responsabilità della sicurezza interna rimangono prerogativa dei singoli Governi nazionali; ma a rendere complesso l'implementazione di un sistema di protezione coordinato a livello europeo vi è la presenza di legislazioni differenti, e in taluni casi mancanti, tra una Nazione e l'altra[113]. La sicurezza informatica a livello UE è trattata da diverse organizzazioni e direttive, preposte ad arginare questo gap.

Nell'ambito del secondo pilastro infatti la Commissione Europea ha istituito un Centro Europeo di Criminalità Informatica, *European Cyber Crime Centre* (EC3) presso l'Europol a gennaio del 2013. Il centro è responsabile della condivisione delle informazioni, della sensibilizzazione e dell'assistenza nelle indagini sui crimini informatici ed è stato pensato per diventare il punto di riferimento nella lotta dell'Unione Europea contro la criminalità informatica e per rendere più rapida la risposta nei casi di crimini on-line. L'EC3 ha il compito di affrontare le seguenti aree di criminalità informatica:

- crimini commessi da gruppi organizzati in grado di generare grandi profitti criminali quali le frodi on-line;
- reati informatici che causano gravi danni alle vittime, quali lo sfruttamento sessuale dei minori;
- attacchi informatici contro le infrastrutture nevralgiche e i sistemi d'informazione dell'Europa.

L'EC3 può contare sulle infrastrutture esistenti dell'Europol, ma ha un organico ridotto rispetto ai compiti assegnatigli, come sostenere gli Stati Membri e l'Unione Europea nello sviluppo delle capacità operative e di analisi per le indagini sul cyber crime.

---

[111] CERT-EU About us, <http://cert.europa.eu/cert/plainedition/en/cert_about.html> (ultima consultazione 6-11-2014).

[112] Comunicato stampa Commissione Europea, 12 settembre 2012, *Un progetto pilota consente di rafforzare la sicurezza informatica delle istituzioni europee*, in <http://europa.eu/rapid/press-release_IP-12-949_it.htm> (ultima consultazione 6-11-2014).

[113] *The European Cyber security Strategy: Too Big to Fail?,* di Neil Robinson, in <http://www.rand.org/blog/2013/02/the-european-cyber-security-strategy-too-big-to-fail.html> (ultima consultazione 6-11-2014).

Dal primo settembre di quest'anno è operativa la *Joint Cybercrime Action Taskforce* (J-CAT), *task force* europea contro la criminalità informatica, che ha sede presso l'EC3 e che agisce in coordinamento con altre organizzazioni internazionali. La *task force* guidata da Andy Archibald, Deputy Director del *National Cybercrime Unit* della *National Crime Agency* del Regno Unito (NCA), è composta da esperti e funzionari di collegamento delle Forze dell'Ordine di Paesi Membri UE ed extraeuropei. Ad oggi questa *task force* è composta da Austria, Canada, Germania, Francia, Italia, Paesi Bassi, Spagna, Regno Unito, Irlanda e Stati Uniti, e sono coinvolte in questa iniziativa anche Australia e Colombia. L'intento di questa nuova struttura non è solo strategico, ma anche operativo, con l'obiettivo di combattere il crimine on-line in modo più efficace, coinvolgendo le polizie dei Paesi UE col fine di coordinare le attività investigative e adottare misure congiunte contro il cyber crime.

Per quanto riguarda le Forze dell'Ordine, Interpol ed Europol svolgono un importante ruolo di coordinamento e condivisione delle informazioni su questo tipo di criminalità a forte natura transnazionale. L'Interpol è la più grande organizzazione di polizia internazionale del Mondo, composta da 190 Stati Membri, ed ha il compito di assicurare che le polizie mondiali abbiano accesso ai servizi e agli strumenti necessari per poter realizzare il loro lavoro in modo efficiente, ed inoltre conduce progetti di formazione anche in ambito cyber. Nata nel 1923 a Vienna come *International Criminal Police Commission* è presente, in ogni Paese Membro dell'organizzazione, con un ufficio centrale di polizia internazionale, che collabora con le altre sezioni e con i corpi locali per la repressione della criminalità operante su scala internazionale. Non avendo propri agenti operativi, il ruolo dell'Interpol è puramente coordinativo.

Dal 1999 è operativa l'Europol, agenzia preposta al contrasto alla criminalità in tutta l'Unione Europea. Scopo principale di questa agenzia è quello di facilitare lo scambio di informazioni tra le polizie dei Paesi Membri raccogliendo e analizzando dati e segnalazioni e comunicando notizie sui reati agli enti competenti di ogni singolo Stato europeo, con lo scopo di agevolare e velocizzare le indagini. Nei confronti di un tipo di criminalità come quella informatica a forte caratterizzazione internazionale, è chiaro come il ruolo dell'Europol acquisisca una rilevanza strategica. Europol ha rilasciato nel 2014 una versione pubblica del suo *The Internet Organised Crime Threat Assessment* (iOCTA)[114], la cui finalità è fornire una analisi dell'impatto del cyber crime all'interno dell'UE, realizzando una previsione sui rischi futuri e sulle minacce emergenti.

Fondata nel 2001 e istituita come agenzia dell'Unione Europea nel 2005[115] anche l'*European Police College* (CEPOL)[116], supporta e promuove un approccio cooperativo tra gli Stati europei per combattere i maggiori crimini transnazionali, riunendo gli alti funzionari delle Forze di Polizia di tutta Europa. Organizza ogni anno negli Stati Membri corsi, seminari, conferenze e riunioni, che riguardano molteplici tematiche rilevanti per le attuali attività di polizia in Europa tra le quali il cyber crime.

---

[114] *The Internet Organised Crime Threat Assessment* (iOCTA) 2014, in <https://www.Europol.europa.eu/sites/default/files/publications/Europol_iocta_web.pdf> (ultima consultazione 6-11-2014).

[115] Decisione 2005/681/GAI del Consiglio, del 20 settembre 2005.

[116] Deriva dal francese "*Collège Européen de Police*".

Nel 2007 viene istituito l'*European Cyber-crime Training and Education Group* (ECTEG) i cui componenti provengono da Stati Membri dell'Unione Europea, Forze di Polizia, organismi internazionali, mondo accademico e industria privata e coordina la formazione sul cyber crime, sostenendo attività internazionali di formazione sulla criminalità informatica, condividendo conoscenze, competenze e soluzioni a problemi specifici, standardizzando metodi e procedure di formazione e collaborando con Università e partner privati di settore per estendere le conoscenze su questo fenomeno al di fuori dei confini nazionali.

A livello giudiziario la cooperazione europea è coordinata da Eurojust, unità istituita nel 2002[117], che assiste le autorità competenti degli Stati Membri quando devono affrontare gruppi criminali organizzati internazionali, potenziando l'efficienza dell'azione delle autorità nazionali. Lo staff di Eurojust è composto da circa 200 persone e da un rappresentante, designato tra pubblici ministeri, giudici o funzionari di polizia con pari prerogative, di ciascuno degli Stati Membri. La criminalità informatica è uno degli argomenti principali delle riunioni che periodicamente vengono tenute durante l'anno e che coinvolgono le autorità giudiziarie e investigative degli Stati Membri.

Nel 2010 viene inoltre costituito l'*European Union Cyber-crime task force* (EUCTF), composto da un gruppo di esperti rappresentanti di Europol, Eurojust e Commissione Europea, in collaborazione con i responsabili delle unità di criminalità informatica dell'Unione Europea per la lotta al cyber crime internazionale. Fornisce assistenza per la promozione di un approccio armonizzato dell'UE alla lotta contro la criminalità informatica.

Fulcro del terzo pilastro e presentata nel maggio del 2010 dalla Commissione Europea, l'Agenda Digitale, gestita da DG Connect[118], contiene 101 azioni, raggruppate intorno a sette aree prioritarie, con l'obiettivo di migliorare la capacità dell'Europa di prevenire, rilevare e rispondere ai problemi in abito informatico. Lo scopo di DG Connect è cercare di rafforzare la resilienza delle infrastrutture critiche, migliorarne la preparazione e promuovere una cultura della *cyber security* attraverso la centralizzazione delle informazioni, la creazione di partenariati tra il settore pubblico e privato, basandosi su un approccio comune e una prospettiva internazionale. Il suo compito è quello di garantire che le tecnologie digitali possano contribuire a realizzare la crescita di cui l'Unione Europea necessita.[119] L'Agenda Digitale ha tra i suoi pilastri fondamentali la sicurezza informatica perché è ritenuta una delle condizioni imprescindibili alla diffusione del mezzo informatico e di internet come strumento di sviluppo e mezzo attraverso il quale accrescere la competitività delle aziende europee. Per rendere la rete un valore aggiunto per le imprese, è necessario che il loro approccio verso il mondo digitale sia di fiducia, al fine di poter agire senza il rischio di subire danni gravi, che costituirebbero un freno alla crescita economica e ad un pieno uso della rete e delle molte opportunità che essa può offrire. Del resto continuano a valere le regole del mondo fisico reale, nel quale è prassi comune e consolidata informarsi dell'affidabilità di

[117] Con decisione 2002/187/GAI del Consiglio, modificata dalla decisione 2009/426/GAI del Consiglio, del 16 dicembre 2008.

[118] European Commission Directorate General for Communications Networks, Content & Technology.

[119] Per approfondimenti si veda: <http://ec.europa.eu/dgs/connect/en/content/mission-and-priorities> (ultima consultazione 6-11-2014).

un interlocutore nel lavoro (sia esso cliente o fornitore) o della sicurezza di un luogo prima di visitarlo, soprattutto se ci è sconosciuto. Queste regole di base, scontate se parliamo del mondo fisico, devono essere applicate ancora con maggiore accortezza quando si parla di mondo virtuale, essendo questo ancora più vasto, impervio, pericoloso e in continuo mutamento rispetto al mondo reale.[120]

L'Agenda Digitale europea ricopre un ruolo strategico in quanto si stima che la sua piena attuazione aumenterebbe del 5% il PIL europeo nell'arco dei prossimi otto anni, portando di conseguenza ad un aumento degli investimenti per l'innovazione del settore tecnologico che migliorerebbe di conseguenza le condizioni di sviluppo di tutti i settori sia pubblici sia privati, anche in termini di posti di lavoro. Il rischio è che, entro il 2020, senza un'azione comune europea, si possano perdere sino a 900 mila posti di lavoro, mentre se ne potrebbero creare molti di più attraverso la costruzione di nuove infrastrutture digitali, progetto che a lungo termine porterebbe fino a 3,8 milioni di posti di lavoro in tutta Europa.

L'Agenda Digitale europea prevede azioni di due tipi, quelle a carico della Commissione Europea, di tipo legislativo, che riguardano strategie e linee guida, e quelle a carico dei singoli Stati Membri che attraverso l'adeguamento alla normativa europea hanno il compito di applicare in concreto le indicazioni comunitarie.

La Commissione Europea in questi ultimi anni sta lavorando molto per raggiungere l'obiettivo di una efficace protezione dei dati, conciliando le necessità di privacy con i benefici di una rete globale "*aperta, innovativa, unificata*". Nel febbraio 2013 infatti la Commissione ha presentato la prima Cyberstrategy europea[121] che si concentra molto sul fenomeno del cyber crime, con l'obiettivo di attuare un piano di difesa dagli strumenti informatici a livello comunitario, sottolineando l'importanza di aumentare la resilienza di reti e sistemi, intensificando la lotta alla criminalità informatica attraverso la normativa in vigore, il rafforzamento degli strumenti di contrasto al fenomeno e promuovendo una politica di sicurezza informatica tra i Paesi Membri e in ambito internazionale per un *cyber space "open, safe and secure"*. Il documento sollecita gli Stati Nazionali ad elaborare piani strategici finalizzati al contrasto delle minacce cyber e sottolinea come la responsabilità della sicurezza del *cyber space* sia da condividere tra tutti i protagonisti della società globale dell'informazione, dai singoli cittadini, alle imprese, agli Stati Nazionali.

A tal fine è indispensabile la cooperazione in ambito internazionale che l'UE si presta a sviluppare insieme ad organizzazioni internazionali, settore privato e cittadini per la quale è stata prevista l'istituzione della piattaforma NIS pubblico-privato e promossa la partecipazione delle PMI.[122]

Tra gli obiettivi di maggior importanza si segnalano l'adozione di un quadro giuridico comune, il rafforzamento della cooperazione tra gli enti preposti al contrasto di questo fenomeno,

[120] "*People - including me - sometimes about talk about our "digital rights". But I don't think that's quite right. These are not digital rights, nor on-line rights: they are fundamental rights, and they apply just as much on-line as off. Whether it is privacy, or freedom of speech, or consumer protection. New technology can enhance our humanity: it should not override our human rights*". Neelie Kroes, *A secure on-line network for Europe Cyber security conference*, Bruxelles 28 febbraio 2014, in <http://europa.eu/rapid/press-release_SPEECH-14-167_en.htm> (ultima consultazione 6-11-2014).

[121] Elaborato dall'Alta rappresentante Catherine Ashton e dalla Commissione Europea.

[122] Piattaforma NIS, in <https://resilience.enisa.europa.eu/nis-platform> (ultima consultazione 20-11-2014).

l'incentivo alla creazione di partenariati pubblico-privato attraverso attività di formazione, il sostegno all'implementazione dei CERT nazionali e la promozione della cooperazione internazionale al di fuori dei confini europei, anche esortando gli Stati Membri alla ratifica della Convenzione sulla criminalità informatica, nota come Convenzione di Budapest[123], che dopo quattro anni di lavoro, è entrata in vigore il primo luglio 2004, e che costituisce il primo trattato internazionale sui reati commessi via internet e su altre reti informatiche. Con lo scopo di costruire una politica penale comune per la lotta alla cyber criminalità e di promuovere la cooperazione internazionale, affronta in particolar modo i temi della violazione del diritto d'autore, della frode informatica, della pedopornografia e della sicurezza della rete, prevedendo sanzioni più pesanti per i reati informatici, aumentando la responsabilità delle imprese, prevedendo maggiori tutele per i dati personali e prevedendo procedure appropriate, quali la perquisizione dei sistemi informatici, l'intercettazione dei dati e la possibilità per le Forze dell'Ordine di chiedere al *provider* il congelamento dei dati telematici per sei mesi. La Convenzione si muove sostanzialmente su tre direttrici e cioè: sulla definizione dell'ambito di applicazione delle misure processuali previste (Art. 14); sulla previsione di misure per l'acquisizione di dati informatici (Artt. 19, 20 e 21) e sulla previsione di misure coattive per ottenere tali dati da soggetti terzi (Artt.16, 17 e 18). Un aspetto rilevante è che l'ambito di applicazione di tale Convenzione comprende non solo i reati informatici puramente tecnici, ma anche i reati tradizionali realizzati attraverso il mezzo informatico, ed inoltre anche i reati che possono essere provati mediante prove elettroniche. L'importanza della cooperazione internazionale nel contrasto di questo tipo di fenomeno è oggetto anche del Protocollo addizionale alla Convenzione sulla criminalità informatica, relativo all'incriminazione per atti di natura razzista e xenofoba commessi a mezzo di sistemi informatici del gennaio 2003[124].

Le priorità della cyber strategia europea sono: sviluppare un livello di resilienza informatica, ridurre il crimine informatico, sviluppare risorse industriali e tecnologiche, sviluppare una politica coerente per contrastare le minacce promuovendo i valori dell'UE, e soprattutto stabilire i requisiti minimi comuni per la National Information Security che a livello nazionale costringerebbe gli Stati Membri a dotarsi di una strategia in tema di *cyber security*, a designare le autorità nazionali competenti in materia, ad istituire un ottimo funzionamento dei CERT, e spingere verso una reale cooperazione internazionale. La Commissione invita costantemente a creare un elevato livello di "NIS" in tutta l'Unione adottando pratiche di gestione del rischio e di condivisione delle informazioni sulla sicurezza delle reti affrontando quelle che sono le capacità nazionali. Il documento insiste in più punti sull'esigenza che tutti i Paesi europei si mettano al passo con un efficiente sistema di *cyber security*, dato che gli anelli deboli rendono fragile tutto il sistema Europa. Ogni Stato deve dotarsi di una normativa forte ed efficace per affrontare la criminalità informatica. Nella strategia europea di *cyber security* la Commissione Europea richiede

[123] *Convention on Cybercrime,* Budapest, 23.XI.2001, in <http://conventions.coe.int/Treaty/en/Treaties/PDF/Italian/185-Italian.pdf> (ultima consultazione 6-11-2014).

[124] *Protocollo addizionale alla Convenzione sulla criminalità informatica, relativo all'incriminazione di atti di natura razzista e xenofobica commessi a mezzo di sistemi informatici*, entrato in vigore il 1 marzo 2006, in <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ITA&CM=8&NT=189> (ultima consultazione 6-11-2014).

lo sviluppo di un piano di contingenza nazionale e la realizzazione periodica di esercitazioni volte a testare la risposta ad incidenti di sicurezza delle reti su larga scala e il successivo *disaster recovery*.

Contestualmente alla cyber strategia europea è stata presentata la proposta di Direttiva sulla sicurezza delle reti e dell'informazione che pone in capo agli Stati obblighi in materia di prevenzione, trattamento e risposta nei confronti dei rischi e degli incidenti, crea un meccanismo di collaborazione tra i Paesi Membri e stabilisce obblighi di sicurezza per gli operatori del mercato e le amministrazioni pubbliche.[125]

La visione dell'UE può essere realizzata solo attraverso una vera e propria partnership tra i vari soggetti interessati. Per affrontare le sfide future, gli Stati Membri non possono più aspettare e devono indicare le loro strategie nazionali in modo preciso, i ruoli, le responsabilità e i vari enti nazionali dedicati. La strategia non deve essere solo di facciata ma reale ed efficiente.

La cyber strategy europea si fonda sostanzialmente su tre pilastri, come rappresentato dal grafico sottostante, che devono collaborare tra di loro sia a livello comunitario che nazionale, ma data la complessità del fenomeno e la moltitudine degli attori coinvolti si rende necessaria innanzitutto un'efficace risposta a livello nazionale unita ad un forte coinvolgimento a livello europeo.

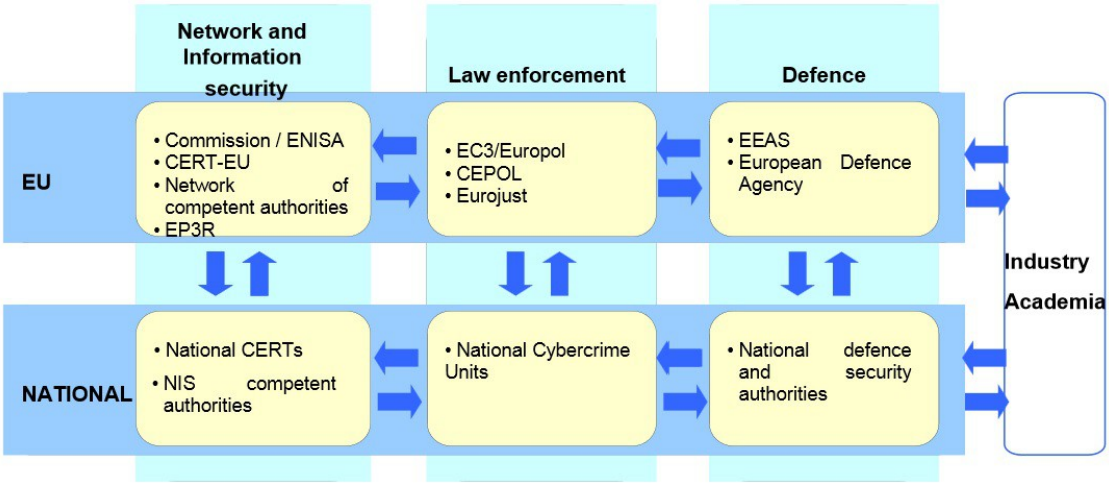


Figura 15 - Coordinazione tra le competenze e ripartizione tra i diversi attori
Fonte: Cybersecurity strategy of the European Union, 2013

A livello europeo infatti l'attuazione della strategia in ambito cyber crime ha il limite di subire i ritardi dei Paesi Membri nell'adeguamento alle direttive europee e la differenza tra questi di politiche messe in atto per contrastare tale fenomeno; tutto ciò rende difficile il raggiungimento degli obiettivi preposti, nonostante l'impegno dell'UE nei confronti della lotta al cyber crime.

Ulteriore impegno dell'UE nel contrasto al cyber crime è costituita dalla Direttiva 2013/40[126] del 12 agosto 2013 sugli attacchi contro i sistemi d'informazione, adottata in base

[125] Proposta di Direttiva del Parlamento europeo e del Consiglio recante misure volte a garantire un livello comune elevato di sicurezza delle reti e dell'informazione nell'Unione <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0048:FIN:IT:PDF> (ultima consultazione 20-11-2014).

[126] *Direttiva 2013/40/UE del Parlamento Europeo e del Consiglio del 12 agosto 2013 relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio*, in <http://eur-

all'Articolo 83 del Trattato di Lisbona sul funzionamento dell'Unione Europea, che dovrebbe essere recepita entro il 4 settembre 2015 e che si pone l'obiettivo di armonizzare i reati e le sanzioni previste per questo tipo di criminalità, imponendo agli Stati il limite minimo del massimo della pena quando il reato commesso è di grande entità e coinvolge più Paesi.

La Commissione inoltre ha inserito all'interno del programma Horizon 2020[127] la *cyber security* e temi riguardanti la privacy e il *trust* dei cittadini e delle aziende europee e ha definito una piattaforma pubblica, denominata piattaforma "NIS", Network and Information Security, che ha lo scopo di identificare le best practices per la *cyber security* e promuovere e incentivare nuove soluzioni ICT per migliorare la sicurezza e la gestione del rischio in ambito informatico. Approvata il 13 marzo di quest'anno dal Parlamento Europeo, la Direttiva sulla *Cyber security* prevede l'obbligo di comunicare i tentativi di violazione dei sistemi solo a società che possiedono, gestiscono o forniscono tecnologia per le infrastrutture critiche, non includendo però i provider di servizi globali. L'importanza delle PMI, nel sistema economico europeo, richiederebbe la loro inclusione nel sistema di obbligo di comunicazione dei cyber attacchi, dato che costituiscono la maggioranza delle imprese in Europa.

L'Agenda Digitale europea fonda le sue azioni sulla definizione di regole e sulla predisposizione di strumenti e piattaforme di supporto, senza implementare azioni per la misurazione e valutazione delle misure intraprese e delegando gli Stati Membri a questo, che, dal canto loro, registrano ancora notevoli ritardi nel recepimento delle azioni indicate. Ad eccezione dell'Azione 39 riguardante la realizzazione di simulazioni di attacchi informatici, numerose importanti azioni non sono ancora state implementate dai Paesi Membri. Per esempio l'Azione 38 che riguarda la realizzazione di *Computer Emergency Response Team* (CERT), negli Stati Membri, prevista inizialmente per il 2012, vede ancora diversi Paesi, compreso l'Italia, in ritardo nella loro implementazione. Ben 12 Paesi sono inadempienti per quanto concerne l'Azione 40 relativa alla realizzazione di *hotline* di allerta sui contenuti pericolosi, soprattutto verso i soggetti deboli, come i bambini (prevista per il 2013). L'Italia e altri 15 Paesi europei non hanno ancora recepito l'Azione 41, che riguarda la realizzazione di piattaforme nazionali di allerta, in realtà prevista per il 2012[128].

Il ritardo nell'avanzamento delle Azioni stabilite dall'Agenda Digitale riflette sicuramente la tendenza di molti Paesi europei a rimanere vincolati ad un approccio prevalentemente nazionale delle politiche e quindi alla lentezza nel recepimento delle Azioni stesse e ad un ritardo nell'unificazione delle policy di contrasto al fenomeno cyber crime. Risultano inoltre disparità anche nelle valutazioni delle risposte dei Paesi in quanto queste vengono effettuate dai Paesi stessi, rivelando divergenze nei metri di giudizio, da quelli più magnanimi a quelli più severi, ed impedendo di fatto una comparazione esatta tra gli Stati. Con queste premesse l'approvazione della Direttiva Europea che vincoli i Paesi Membri ad azioni congiunte e programmate risulta uno strumento senza dubbio utile alla lotta al cyber crime.

---

lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32013L0040> (ultima consultazione 6-11-2014).

[127] Attività "Innovation in SMEs" è un ponte tra le attività principali di Horizon 2020 (il supporto alla ricerca, progetti di sviluppo e innovazione) e la creazione di un ambiente per la crescita e l'innovazione delle PMI.

[128] *Sicurezza delle reti in Europa: il punto sui ritardi* di Nello Iacono, in <http://www.agendadigitale.eu/infrastrutture/718_sicurezza-delle-reti-in-europa-il-punto-sui-ritardi.htm> (ultima consultazione 6-11-2014).

L'aspetto però più importante è quello della sua operatività, in quanto, la messa in sicurezza delle reti e dei sistemi europei è strettamente vincolata all'adozione da parte di ogni singolo Paese Membro di tutte le Direttive approvate e all'adempimento di tutti i requisiti stabiliti dalla Commissione europea.

Le dichiarazioni del Commissario europeo per l'Agenda Digitale Neelie Kroes confermano infatti la necessità di una Direttiva forte e realmente vincolante che coinvolga in maniera decisa tutti i Paesi Membri, per non rendere vani gli sforzi fatti fin qui e per non mettere in pericolo il futuro digitale europeo. Il risultato dell'Agenda Digitale europea dipenderà molto dalla volontà dei singoli Paesi Membri di creare una rete efficiente che si occupi di sicurezza. L'importanza che questi temi hanno assunto a livello europeo è confermata anche dalla presenza di un nuovo Vice Presidente per il *digital single market* e da un Commissario.

Inoltre è utile considerare che un ulteriore ostacolo alla realizzazione di una strategia difensiva comune europea efficace in ambito cyber è costituito dalle differenze tra i singoli Paesi Membri, sia a livello di infrastrutture che di apparati giuridici e di difesa. A livello infrastrutturale il *digital divide* tra i diversi Paesi dell'Unione e in taluni casi anche all'interno dei Paesi stessi e la conseguente sicurezza di reti e informazioni, rende difficile il raggiungimento di un livello adeguato di difesa. In ambito legale gli Stati Membri non solo non hanno un comune approccio ad alcuni tipi di reati realizzati attraverso lo strumento informatico, ma hanno apparati giuridici completamente differenti, autonomi e in certi casi contrastanti. Questa situazione non permette facilmente l'unificazione delle misure giuridiche e legali adatte a raggiungere una risposta comunitaria alla minaccia informatica.

CAPITOLO 3

L'IMPATTO DEL CYBER CRIME IN ITALIA E RELATIVE CONTROMISURE

3.1 Stato attuale delle PMI in Italia

Come riportato nel primo capitolo il 99,9% del panorama economico italiano è composto da Piccole e Medie Imprese non finanziarie. Le sole micro imprese, con meno di dieci addetti, rappresentano in Italia il 95% del totale, con un peso in termini di occupazione dell'81%. Nella sua ultima Relazione annuale[129] il Garante per le Micro, Piccole e Medie Imprese riferisce che nel 2013 il saldo tra il numero di PMI nate e quelle che hanno cessato la loro attività è stato il peggiore degli ultimi anni, registrando infatti il maggior numero di fallimenti dell'ultimo decennio (oltre 10.000). In questo quadro di forte crisi il Garante sottolinea come performance particolarmente positive si sono registrate in casi in cui si sono realizzati fenomeni di aggregazione tra piccole imprese appartenenti a filiere trainate da aziende di medie dimensioni, soprattutto tra quelle che hanno puntato su export, tecnologia[130] e produzione di beni di alta qualità, caratteristica tipica del *Made in Italy*. Tra i trend più positivi in prospettiva futura il Garante segnala la crescita dell'uso di tecnologie digitali nel settore artigiano tra le imprese che hanno saputo fondere la tradizione con l'innovazione, e l'aumento delle start up innovative, soprattutto nate dai laboratori promossi tra Università ed imprese. Le imprese di medie dimensioni avendo una presenza più solida sul mercato e maggiore internazionalizzazione[131] rappresentano una grossa opportunità per le aziende subfornitrici all'interno delle filiere e una spinta verso la ripresa. A questo proposito l'e-commerce può essere uno strumento per incrementare il bacino di potenziali clienti favorendo l'export delle micro e piccole imprese che soffrono però di un livello di digitalizzazione ancora basso. La presenza sui mercati esteri infatti può essere un canale di opportunità per le PMI, soprattutto per quelle italiane specializzate nel settore manifatturiero tipico del *Made in Italy* che rappresentano la punta di diamante della nostra economia. Secondo i dati del Garante infatti l'Italia è tra i primi cinque Paesi esportatori di ben un quarto dei 5.500 prodotti in cui si può suddividere il commercio mondiale, e prima per 235 prodotti.[132]

---

[129] Relazione al Presidente del Consiglio articolo 17, comma 1, legge 11-11-2011 n. 180 *"Norme per la tutela della libertà d'impresa. Statuto delle Imprese"*, Roma, 06.02.2014, in <http://www.governo.it/backoffice/allegati/75045-9261.pdf> (ultima consultazione 7-11-2014).

[130] In primis filiera meccanica e farmaceutica.

[131] Sempre nel rapporto del Garante si specifica che gli ultimi dati Unioncamere-Mediobanca indicano che il 90% delle medie imprese italiane esporta i propri prodotti all'estero.

[132] Bonifazi Alberto, Giannetti Anna (2014), *Finanziare l'impresa con i fondi europei Strumenti e opportunità 2014-2020. Redazione e presentazione delle domande. Simulazioni pratiche*, IPSOA.

Le indicazioni espresse nel rapporto del Garante per le PMI sono sostenute anche dalla rilevazione[133] dell'Osservatorio sulla competitività delle PMI[134] (OPMI) promosso dal *Knowledge Center* della Sda Bocconi per il quale dal 2007 sino alla fine del 2013 delle 55.709 Piccole e Medie Imprese italiane che fatturavano dai 5 ai 50 milioni di euro, il 16% ha chiuso la propria attività. Tradotto in termini economici significa una perdita di ben 120 miliardi di euro di fatturato e 405 mila posti di lavoro in meno e 8.841 imprese scomparse. Il dato incoraggiante sta nel fatto che le 46.868 che non hanno chiuso in seguito alla crisi economica hanno registrato una crescita del 4,28% medio annuo, cioè del 26% cumulata. Tra queste, il 2,5%, cioè circa 1.165 PMI, è cresciuto, nonostante la crisi, del 12,4% annuo (77% di crescita cumulata) e risiedono per lo più nel Veneto, Emilia Romagna, Piemonte e Liguria e si concentrano in settori quali il manifatturiero (meccanica, alimentari e bevande e chimico-farmaceutico in testa) e il commercio all'ingrosso. Sono aziende soprattutto con anni di attività alle spalle di dimensioni maggiori e secondo il rapporto hanno realizzato questo risultato grazie alla loro capacità di internazionalizzarsi, di fare innovazione, di registrare marchi e brevetti. Altre quasi 9.000 PMI, secondo il rapporto, avrebbero tutte il potenziale per aumentare la loro redditività.

Le PMI italiane possono svolgere un ruolo chiave per la ripresa economica del Paese. È della stessa opinione Riccardo Luca, *Digital Champion* italiano che ha recentemente sottolineato l'importanza di investire nell'opera di digitalizzazione delle PMI italiane per sostenerne l'internazionalizzazione e l'utilizzo dell'e-commerce e quanto sia fondamentale per rilanciare l'economia che le PMI si riparino da rischi della rete. Un altro fattore strategico secondo Luna è quello culturale che va sostenuto per aumentare la consapevolezza del mezzo informatico. "*Negli anni '60 il boom economico è stato provocato anche dal maestro Manzi, che in tv ha insegnato agli italiani a leggere e a scrivere. Oggi servono nuovi maestri Manzi che insegnino agli italiani i pericoli ma soprattutto le opportunità della Rete*" è quanto ha dichiarato[135].

[133] *Empowering the knowledge of small and medium enterprises management*, Divisione ricerche Claudio Dematté Osservatorio sulla competitività delle PMI 10 luglio 2014 SDA Bocconi, in <http://www.sdabocconi.it/sites/default/files/upload/pdf/report_PMI_10_luglio_2014.pdf> (ultima consultazione 7-11-2014).

[134] La rilevazione analizza i bilanci delle 56.000 PMI italiane dal 2007 con fatturato compreso tra 5 e 50 milioni di euro che, pur costituendo solo il 6,1% delle imprese italiane, producono il 39% del Pil e occupano 2.291.000 persone. E individua 1.200 campioni.

[135] Luna: "*Le startup non bastano, per la ripresa servono PMI digitali*", in <http://www.corrierecomunicazioni.it/job-skill/30662_luna-le-startup-non-bastano-per-la-ripresa-servono-pmi-digitali.htm> (ultima consultazione 7-11-2014).

3.2 Il cyber crime come freno all'economia del Paese. Panoramica sull'impatto del cyber crime in Italia

In Italia il fenomeno del cyber crime è ancora sottostimato rispetto al reale impatto che ha sull'economia. Secondo i dati del PwC's 2014 Global Economic Crime Survey[136] una azienda italiana su quattro ha dichiarato di essere stata vittima di cyber crime, il rapporto ovviamente sottolinea come il dato sia di sicuro inferiore alla realtà in quanto questo tipo di criminalità non sempre è individuata dall'azienda e non sempre chi lo subisce è disposto a condividerlo.[137] Il rischio di subire questo tipo di attacchi viene percepito come maggiore rispetto agli anni precedenti da un'azienda su tre, mentre per quasi la metà delle aziende è rimasto stabile. I tipi di danni conseguenti un attacco informatico che preoccupano in particolar modo le aziende italiane campione della ricerca sono per il 65% danni reputazionali o di immagine, per il 64% danni relativi alla violazione di normative, per il 60% danni economici diretti dovuti a frode informatica, per il 59% l'interruzione di servizi dovuti ad attacchi hacker, e per il 58% il furto e la perdita di informazioni sensibili riguardanti gli utenti ed infine i danni relativi al furto di dati riservati aziendali per il 55%. È da notare inoltre come la percezione di questo tipo di minaccia sia afferibile a contesti esterni all'azienda, considerando spesso il cyber criminale come non appartenente al proprio ambiente, ma come un criminale che agisce da Paesi e posti lontani. Infatti la maggioranza delle aziende italiane intervistate considera il cyber crime come una minaccia proveniente dall'esterno dell'azienda, per il 23% rappresenta un rischio sia interno che esterno e solo il 7% lo considera un pericolo interno all'azienda stessa.

La situazione descritta dallo studio "Guadagnare dalle informazioni digitali"[138] condotto da Trend Micro sulla sicurezza informatica in Italia non è di certo rosea. Secondo tale studio infatti l'Italia sarebbe quinta tra i Paesi con il maggior numero di reti botnet attive nel primo trimestre del 2013 e in assoluto la terza al mondo per spam inviato, nonché ottava tra i Paesi colpiti da malware destinati al settore finanziario e dell'*on-banking*. È indicativo del fatto che la nostra nazione sia colpita in modo sostanziale dalle minacce informatiche il dato che riferisce che l'italiano sia la nona lingua al mondo più utilizzata per le e-mail di spam e rispetto al mondo del mobile ben quarta tra i Paesi con il maggior numero di App malevoli per piattaforme Android.

Secondo una ricerca condotta da Vanson Bourne, Emc Global Data Protection Index, che ha intervistato 3.300 *decision maker* IT di medie e grandi aziende di 24 Paesi, l'Italia si posiziona solo al quindicesimo posto per la maturità delle politiche per la protezione dei dati. Solo il 10% delle aziende in Italia è al passo coi tempi nella *data protection*, mentre negli ultimi 12 mesi ben l'80% delle imprese ha registrato un blocco nei sistemi informatici, che ha causato per il 38% a una

---

[136] *PwC's 2014 Global Economic Crime Survey Le frodi economico-finanziariein Italia: una minaccia per il business Settima edizione,* in <http://www.pwc.com/it/it/services/forensic/assets/docs/gecs-2014.pdf> (ultima consultazione 7-11-2014).

[137] La Global Economic Crime Survey 2014 ha realizzato oltre 5.000 interviste, per un totale di 95 Paesi coinvolti e per quanto riguarda l'Italia, hanno aderito alla ricerca 101 aziende.

[138] *Guadagnare sulle informazioni digitali* Verifica di sicurezza annuale 2013 di TRENDLABS, in <http://www.trendmicro.it/informazioni-sulla-sicurezza/ricerca/trendlabs-2013-annual-security-roundup/index.html> (ultima consultazione 7-11-2014).

perdita della produttività, per il 22% a un decremento del fatturato e per il 36% al ritardo nello sviluppo di un prodotto.

Le aziende italiane hanno così perso ben 9 miliardi di dollari a causa della perdita dei propri dati sensibili negli ultimi 12 mesi. Una cifra che sale a 14,1 miliardi di dollari se si sommano le perdite derivanti dalle interruzioni operative dei sistemi informatici[139].

L'Italia soffre della mancanza di studi, dati e statistiche ufficiali riguardo il fenomeno del cyber crime e gli unici studi disponibili sono frutto di statistiche redatte dal settore privato. L'associazione che stila ogni anno un rapporto sulla sicurezza ICT in Italia è il Clusit[140] che da anni ha tra i suoi obiettivi quello di diffondere la cultura della sicurezza informatica in Italia promuovendo, attraverso summit periodici, la condivisione delle informazioni in questo settore. Secondo il Rapporto Clusit 2014[141] il cyber crime è un fenomeno in rapida evoluzione e in preoccupante aumento. La gravità degli attacchi infatti è aumentata negli anni in modo significativo sia in termini meramente numerici sia in termini di valore dei dati sottratti e di conseguenze derivanti dai vari tipi di attacco. Diventa sempre più labile inoltre il confine tra cyber crime e hacktivism, in quanto gli strumenti tradizionalmente associati ad uno dei due mondi vengono usati in commistione per raggiungere lo stesso obiettivo ed aumentare le probabilità di successo di un attacco. Attraverso il *deep web* infatti sono facilmente fruibili tutti gli strumenti a disposizione dei cyber criminali che, per esempio, possono acquistare botnet per realizzare DDoS, tendenzialmente considerato un attacco tipico del mondo hacktivism, al fine di mascherare il reale intento dell'attacco come il furto di dati sensibili.

Un altro trend a livello internazionale evidenziato dal Rapporto Clusit è relativo alla tendenza da parte dei cyber criminali di attaccare più facilmente fornitori di beni e servizi e aziende appartenenti alla stessa filiera considerati l'anello debole[142], pur essendo soprattutto in Italia il cuore pulsante dell'economia, utilizzabile per arrivare al bersaglio principale, generalmente una azienda di medio grandi dimensioni. È di questi giorni la notizia relativa all'offensiva hacker contro il colosso americano dei prodotti per la casa *Home Depot* al quale sono stati sottratti 53 milioni di indirizzi e-mail, oltre alla violazione dei mesi scorsi di 56 milioni di informazioni finanziarie, carte di debito e carte di credito appartenenti a cittadini USA e canadesi, usando semplicemente le credenziali di un suo fornitore. Attraverso l'username e password di un *outsourcer* quindi gli hacker sono riusciti ad entrare nella rete di Home Depot, installare un malware creato appositamente per ingannare il software antivirus e diffondersi all'interno del network, accedendo così al database di indirizzi di posta elettronica e al registro dei pagamenti contenente i dati relativi alla transazioni, realizzando così il più grosso attacco informatico mai registrato[143]. Come abbiamo già esposto nel primo capitolo di questa ricerca, gli hacker

---

[139] Emc Global Data Protection Index in <http://www.emc.com/microsites/emc-global-data-protection-index/index.htm#infographic-italy> (ultima consultazione 8-12-2014).

[140] Nato nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano.

[141] *Rapporto Clusit 2014 sulla sicurezza ICT in Italia*, in <https://clusit.it/rapportoclusit/> (ultima consultazione 7-11-2014).

[142] Tendenzialmente sfruttandone le utenze privilegiate e le connessioni VPN.

[143] *The Home Depot Reports Findings in Payment Data Breach Investigation*, in <http://www.streetinsider.com/Press+Releases/The+Home+Depot+Reports+Findings+in+Payment+Data+Breach+Investigation/9986431.html> (ultima consultazione 7-11-2014). Si veda anche: *Home Depot Says Hackers Also Stole Email*

intravedono nelle PMI una scorciatoia molto proficua per colpire organizzazioni più grosse minimizzando gli sforzi dato che il livello della sicurezza informatica per motivi di budget e culturali è ancora basso nelle imprese di dimensioni più piccole.

Per quanto riguarda il panorama italiano, delle 438 aziende interpellate dallo studio, 81 delle quali fornitrici di tecnologia, la metà dichiara di voler aumentare il budget destinato alla sicurezza informatica, mentre un'altra metà lo manterrà invariato rispetto all'anno precedente e nessuna ha intenzione di diminuirlo. Per quanto riguarda le PMI, invece, il 43% di esse vorrebbero aumentare i budget dedicati alla sicurezza, quante poi, in base alle possibilità, riusciranno a farlo non è un dato quantificabile. Ciò nonostante il campione analizzato nel rapporto esprime quest'anno una maggiore propensione all'investimento nella sicurezza informatica, il 46,7% rispetto al 26,7% dichiarato nel 2013 e potrebbe rappresentare l'aumento del livello di maturità nei confronti di questa tematica. Infatti proprio le medie imprese risultano come le più propense ad aumentare i loro investimenti anche secondo l'opinione di fornitori di ICT security. In generale possiamo rilevare una dichiarazione di maggiore interesse nei confronti degli anni precedenti riguardo il tema dell'ICT security anche se tra le iniziative di maggior rilievo, che hanno in questi mesi impegnato le aziende nell'ambito della sicurezza ICT, tra le prime posizioni prevalgono azione di natura tecnica e ultime figurano le attività di formazione.

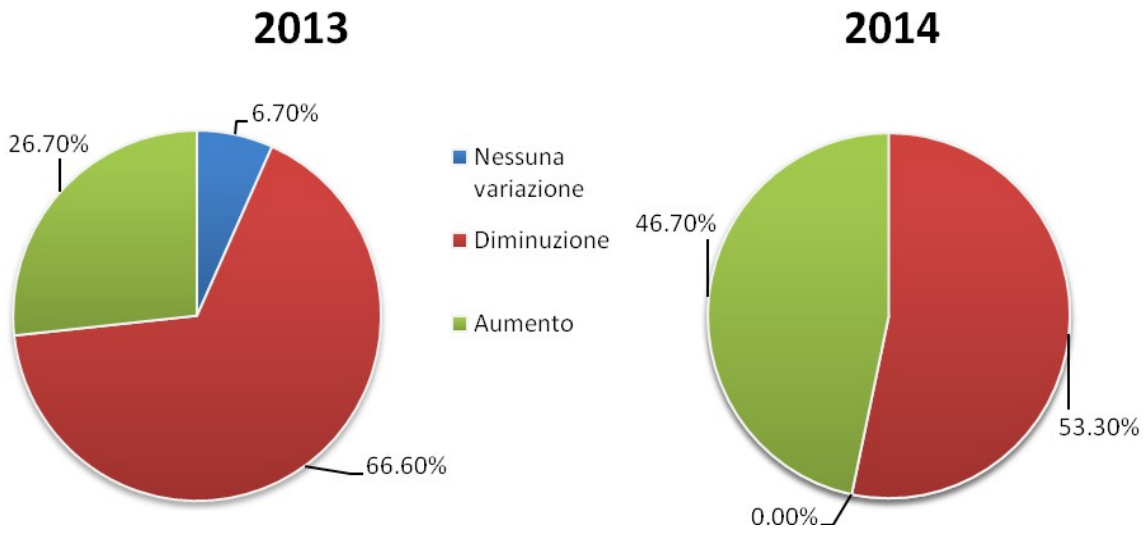


Figura 16 - Dichiarazione di investimento nella spesa informatica rispetto all'anno precedente
Fonte: Rapporto Clusit 2014

Il limite di cui soffre il Rapporto Clusit è che si riferisce all'analisi degli attacchi realizzati in Italia nel 2013. Il Rapporto infatti analizza solo 35 casi gravi che di certo non possono rappresentare la fotografia dello stato attuale dalla criminalità informatica in Italia per due ragioni fondamentali, la prima è riferibile alla reticenza delle aziende nel divulgare informazioni riguardanti eventuali attacchi subiti e alla difficoltà che ancora persiste nel saper rilevare il fatto che questi attacchi si siano verificati. Il secondo aspetto da considerare è che i casi gravi sono di

Addresses di Nicole Perlroth, The New York Times 6-11-2014, in <http://bits.blogs.nytimes.com/2014/11/06/home-depot-says-hackers-also-stole-email-addresses/?_r=0> (ultima consultazione 7-11-2014).

norma ascrivibili ad eventi riguardanti Governi, movimenti politici, forze di polizia ed enti istituzionali[144], infatti il dato che ne deriva è una maggioranza di attacchi hackitvism rispetto a quelli relativi al cyber crime (rispettivamente 83% e 17%). La natura stessa di questi due attacchi vizia la rilevazione in quanto di norma gli attivisti hanno tutto l'interesse affinché il loro attacco sia pubblico e usano strumenti che rendono evidente l'attacco stesso, mentre i cyber criminali tendono ad usare strumenti meno visibili per mantenere nascosto il loro attacco.

Questa analisi è di fatto confermata dai dati Fastweb contenuti nel rapporto che, pur riferendosi solo alla propria rete (circa 10% copertura nazionale[145]), rivela come il cyber crime sia la principale causa di attacchi con il 60% del totale, mentre il 24% è relativo al fenomeno di spionaggio industriale e solo i 16% ad hacktivism[146]. Questo dato è particolarmente preoccupante per le imprese in quanto bersaglio sia di attività di cyber crime sia di *cyber espionage* che hanno lo scopo di rubare o copiare progetti, dati sensibile e documenti.

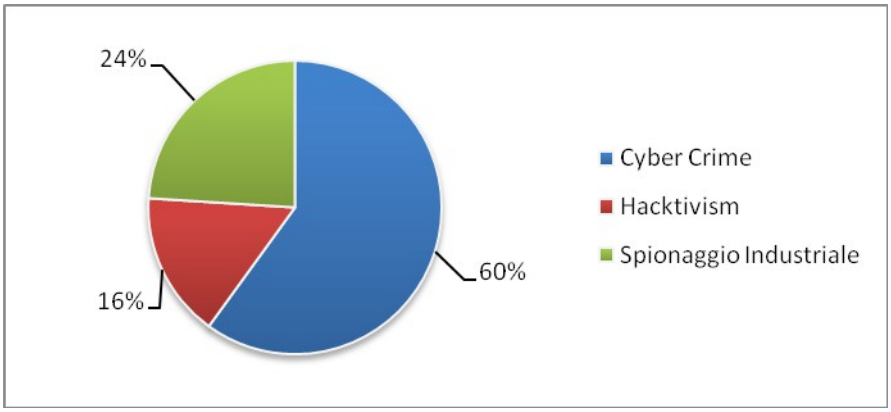


Figura 17 - Motivazione degli attaccanti
Fonte: Rapporto Clusit 2014, dati Fastweb

Per quanto attiene l'origine di questi attacchi Fastweb prende in considerazione, per ovvie ragioni riferibili alla assoluta inattendibilità del dato inerente al solo indirizzi IP finali di un attacco appartenenti ad una botnet, la localizzazione dei *Command and Control* cioè i server utilizzati come centri di controllo, che attiva alla richiesta del "botnet master" una connessione attraverso la quale il criminale può comandare i computer infetti e far transitare attraverso di loro l'attacco. Anche il *Command and Control* è uno strumento che può essere gestito a distanza, quindi la sua localizzazione non garantisce automaticamente la localizzazione dell'attaccante che potrebbe gestirlo da un altro Paese. Ad ogni modo questo dato è indicativo di come il cyber crime sia un

[144] Tra gli attacchi considerati dal Clusit figurano quelli DDoS realizzati contro obiettivi politici come quella del Presidente del Consiglio Matteo Renzi, movimenti come il Movimento 5 stelle e Casaleggio & Associati, istituzioni come il Ministero dell'Interno, Regioni, Forze dell'Ordine. Tra gli eventi di cyber crime il Rapporto cita Alpitour, il Tribunale di Milano e il CNR di Genova.

[145] *Dati Agcom: bene 3 Italia e Fastweb. Ed è boom per Lycamobile* di Andrea Biondi su Il Sole 24 Ore 7-10-2014, in <http://www.ilsole24ore.com/art/impresa-e-territori/2014-10-07/dati-agcom-bene-3-italia-e-fastweb-ed-e-boom-lycamobile-173237.shtml?uuid=ABdmQx0B> (ultima consultazione 8-11-2014).

[146] Dati rilevati su 200.000 indirizzi IP appartenenti all'Autonomous System dell'Internet Service Provider Fastweb SpA, che comprende sia quelli dei Clienti sia di Fastweb stessa.

fenomeno assolutamente transazionale. L'area del mondo con in assoluto il maggior numero di *Command and Controll* risulta essere l'Asia, seguita Europa e Medio Oriente.

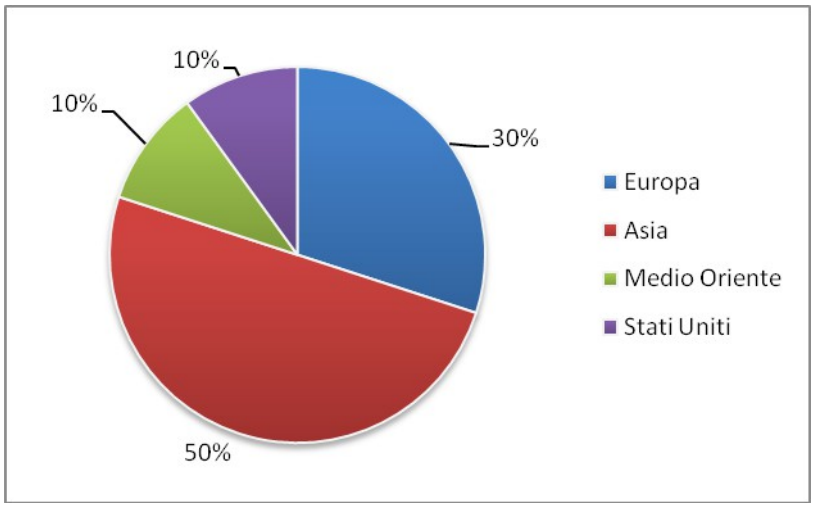


Figura 18 - Distribuzione centri Command & Control
Fonte: Rapporto Clusit 2014, dati Fastweb

Il fenomeno della criminalità informatica viaggia sicuramente ad una velocità maggiore rispetto allo sviluppo della consapevolezza dello strumento informatico da parte degli utenti, anticipando ed individuando precocemente i canali migliori da sfruttare per esercitare la loro attività e massimizzare i profitti. In questo contesto i social network e l'uso sempre maggiore dei dispositivi mobili rappresentano i nuovi veicoli privilegiati per effettuare gli attacchi di natura informatica. In Italia, infatti, secondo gli ultimi dati Audiweb di agosto di quest'anno sono 27,4 milioni gli italiani[147] attivi sulla Rete[148]. Questa rivoluzione sociale e tecnologica vede inoltre l'aumento sempre più consistente dei navigatori internet che usano dispositivi mobili (tablet e smartphone) rispetto al PC[149].

[147] Utenti unici.

[148] *Audiweb pubblica i dati dell'audience mobile e della total digital audience del mese di agosto 2014*, in <http://www.primaon-line.it/wp-content/uploads/2014/11/Audiweb_CS_TotalDigitalAudience_03112014.pdf> (ultima consultazione 7-11-2014).

[149] Sono, infatti, 15,5 milioni gli italiani tra i 18 e i 74 anni che ogni giorno si sono connessi in mobilità, mentre l'audience on-line da PC registra 10,5 milioni utenti unici.

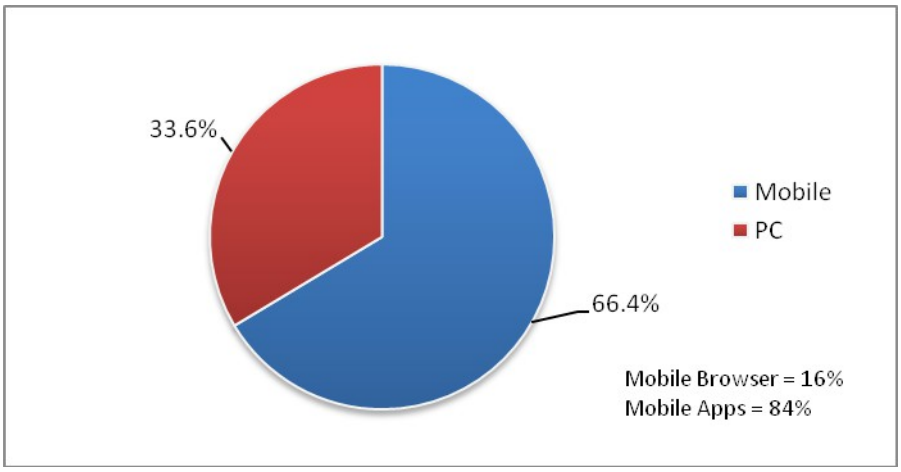


Figura 19 - Tempo di navigazione rispetto al dispositivo usato
Fonte: Dati Audiweb, agosto 2014

Di sicuro questo dato costituisce un'informazione importante per capire come stanno cambiando le abitudini degli italiani e di conseguenza dove si possono concentrare le maggiori minacce ed insidie, tali infatti non solo da influenzare investimenti e scelte strategiche, ma anche l'azione dei cyber criminali. Della percentuale relativa alla navigazione mobile è importante sottolineare come l'84% si riferisca all'uso di internet delle applicazioni, mentre la navigazione da browser è solo del 16%. A livello aziendale è importante sottolineare come la comodità di uso del dispositivo mobile abbia negli anni abbia aumentato i casi di *dual use*, cioè l'utilizzo del dispositivo sia per finalità lavorative che private.[150] Questo introduce numerosi altri problemi per le aziende, che devono gestire anche le vulnerabilità dei dispositivi mobili e il loro uso da parte degli utenti, tendenzialmente più disinvolti e disattenti, veicolo di attacchi sempre più mirati ed aggressivi. La vulnerabilità dei sistemi mobili sta portando i cyber criminali a realizzare attacchi sempre più sofisticati verso questi dispositivi che sono ormai veri e propri PC senza però essere spesso dotati di protezioni antivirus efficaci, il ché li rende più accessibili dall'esterno; durante una connessione wireless per esempio i dati che viaggiano da smartphone alla rete sono in chiaro, il ché permette di visualizzare password e tutto ciò che riguarda la connessione da qualsiasi criminale informatico che si spacci per *access point*. Inoltre molti utenti modificano il proprio dispositivo mobile eliminando i blocchi di fabbrica per sbloccare funzionalità di amministrazione avanzate (*root* di Android o *jailbreak* di iPhone) e installano software e giochi "craccati" scaricandoli da App Store non ufficiali, non comprendendo il reale pericolo di queste manovre.

Un altro trend che riguarda le abitudini degli utenti di internet sia privati che aziendali in Italia è rappresentato dal crescente uso dei social network e dei servizi cloud. Nell'indagine condotta da AIDiM, ANVED ed eCircle[151] già nel 2012 emergeva che il 75% delle 315 aziende italiane intervistate usavano i social media come piattaforma per comunicare i valori del *brand*, interagire con i clienti, catturare nuovi clienti con promozioni e attuare azioni di marketing e raccolta di feedback sui prodotti e i servizi. Il social più usato risultava Facebook seguito da

[150] Guardia di Finanza Nucleo Speciale Frodi Tecnologiche, 2014, in <http://www.aracneeditrice.it/scaricabili/interventoreda.pdf> (ultima consultazione 7-11-2014).

[151] "*Quanto è Social la tua Azienda?*", in <www.slideshare.net/kornfeind/quanto-social-la-tua-azienda> (ultima consultazione 7-11-2014).

LinkedIn, YouTube e Pinterest, senza dubbio è facile immaginare che questo trend abbia avuto in questi ultimi mesi una rapida evoluzione. I servizi cloud, dal canto loro, permettono alle aziende di utilizzare strumenti innovativi riducendo notevolmente i costi di gestione, soprattutto per quanto riguarda le PMI che hanno, rispetto alle grandi imprese, budget più limitati. I social network e i servizi cloud però contengono una quantità di dati tali da risultare molto appetibili ai criminali informatici i quali, soprattutto attraverso tecniche si *social engineering*, phishing e spam, sfruttano le vulnerabilità tecniche dei cloud e umane dei social per i loro attacchi.

Il fenomeno del cyber crime non è di certo un fenomeno da sottovalutare per il suo ampio impatto sull'economia di un Paese. Secondo l'ultimo studio di McAfee sui costi per l'economia del cyber crime a livello mondiale[152] il nostro Paese perde, in termini di danni diretti, circa 875 milioni di dollari all'anno che arrivano a ben 8,5 miliardi (pari allo 0,6 del PIL) se si considerano anche i danni di immagine e reputazionali e i costi derivanti da *recovery* e perdita di opportunità di business.

Secondo i dati della ricerca Websense *Exposing the Cybersecurity Cracks: A Global Perspective*[153] condotta dal Ponemon Institute[154] il 66% delle aziende italiane non reputa di avere tutte le competenze e gli strumenti per impedire l'eventuale perdita di dati sensibili. Il 54% degli intervistati inoltre dichiara di considerare la propria azienda non sufficientemente sicura contro i tipi di attacco informatico più evoluto e quasi la metà ammette di aver subito almeno un attacco di non poca rilevanza nell'anno precedente. Inoltre per il 70% degli intervistati i propri strumenti difensivi non permettono di individuare la cause primarie di un attacco e più della metà delle aziende che hanno subito una violazione non è in gado di identificare quali dati fossero stati sottratti.

Un altro importante aspetto che emerge da questa ricerca, condotta intervistando gli IT Manager che rappresentano la figura più competente in ambito aziendale per quanto riguarda la sicurezza informatica, è la difficoltà che si ha a livello dirigenziale nel percepire una eventuale perdita di dati come un danno economico, per ben l'80% degli attori coinvolti nella ricerca. Un ultimo dato rilevante riguarda il livello di conoscenza media del fenomeno che il professionista della sicurezza ritiene che il dirigente aziendale abbia, per la metà degli intervistati non sufficiente.

Il problema quindi ha soprattutto una fortissima connotazione culturale, infatti nonostante gli utenti italiani sul web siano quasi 37 milioni, equivalente a quasi il 60% della popolazione italiana[155], la conoscenza dei pericoli derivanti dallo strumento informatico è ancora molto bassa.

---

[152] *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II Center for Strategic and International Studies*, giugno 2014, in <http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf> (ultima consultazione 7-11-2014).

[153] *Exposing the Cybersecurity Cracks: A Global Perspective Part I Websense*, Inc. Ponemon Institute aprile 2014, in <https://www.websense.com/assets/reports/report-ponemon-2014-exposing-cybersecurity-cracks-en.pdf> (ultima consultazione 7-11-2014).

[154] La ricerca coinvolge circa 5.000 professionisti della sicurezza IT in tutto il mondo, con un'esperienza di circa 10 anni provenienti da 15 Paesi: Australia, Brasile, Canada, Cina, Francia, Germania, Hong Kong, India, Italia, Messico, Paesi Bassi, Singapore, Svezia, Regno Unito e Stati Uniti.

[155] Italy Internet Users, in <http://www.internetlivestats.com/internet-users/italy/> (ultima consultazione 7-11-2014).

Secondo i dati riportati da Eurobarometro[156] infatti il 61% degli italiani intervistati dichiara di non ritenersi ben informato sui rischi dei cyber reati contro il 52% della media europea. Il sondaggio rivela che la maggior parte dei cittadini europei si sente impreparato a proteggere le proprie informazioni on-line. Come possiamo leggere dalla figura seguente, il 33% dichiara di sentirsi informato nonostante questo sia un fattore difficilmente valutabile in modo adeguato. Semplici abitudini infatti come il cambio password faticano ancora ad entrare nella quotidianità degli utenti internet. Più della metà degli italiani secondo lo studio Eurobarometro dichiara infatti di non aver cambiato nessuna delle proprie password almeno nei 12 mesi precedenti.

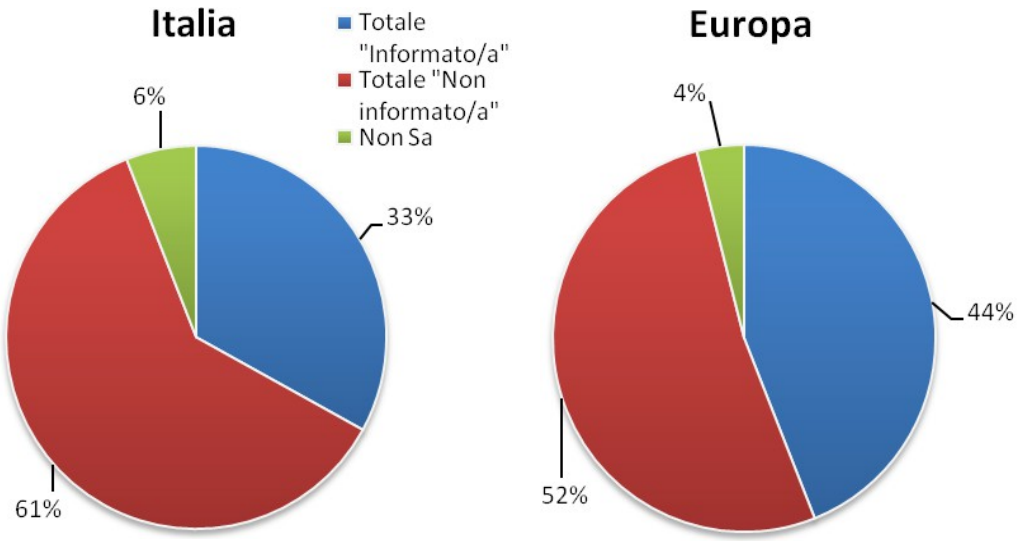


Figura 20 - Sondaggio sulla percezione dell'informazione riguardo i rischi dei cyber reati
Fonte: Speciale Eurobarometro 404 Cyber Security Report, 2013

[156] *Eurobarometer Special Surveys*, Cyber security Report, European Commission, in <http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_fact_it_it.pdf> (ultima consultazione 7-11-2014).

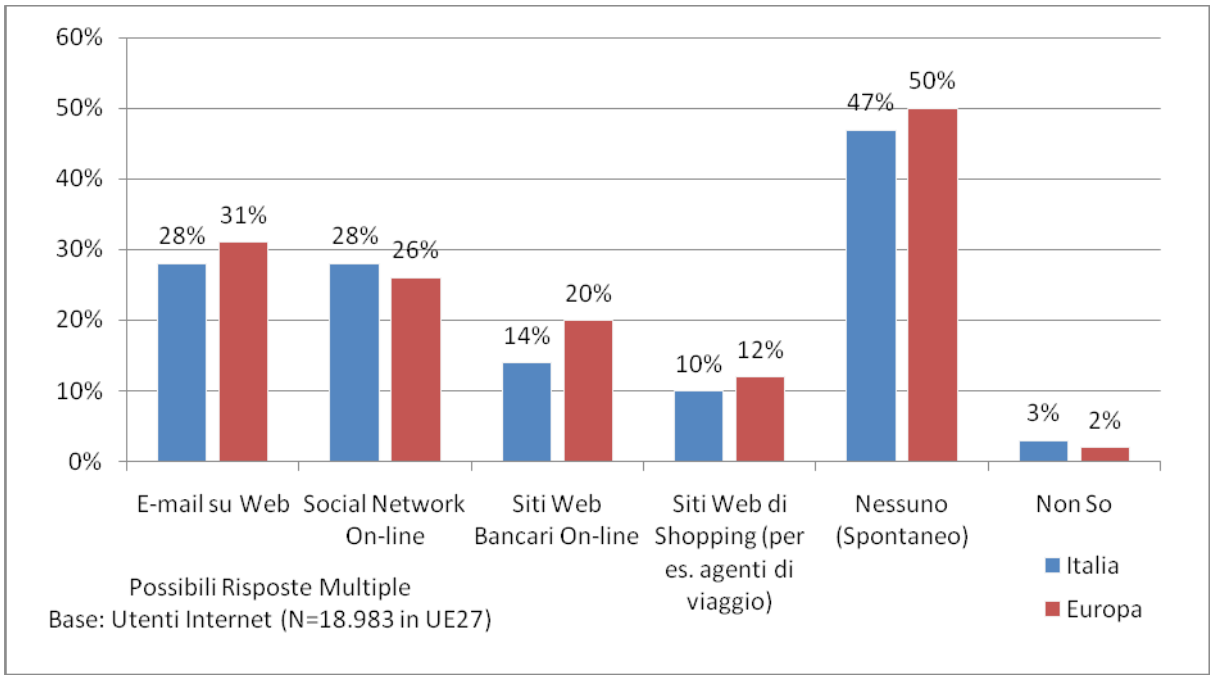


Figura 21 - Sondaggio sulle abitudini di cambio password nell'arco di 12 mesi
Fonte: Speciale Eurobarometro 404 Cyber Security Report, 2013

3.3 Le politiche italiane in ambito cyber security

La nuova fattispecie giuridica che sanziona i reati di tipo informatico viene introdotta per prima volta con modifiche al Codice penale e al Codice di procedura penale attraverso due leggi approvate negli anni novanta, la legge n°547 del 23 dicembre 1993, *Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica* e la legge n°269 del 3 agosto 1998, *Norme contro lo sfruttamento della prostituzione, della pedopornografia, del turismo sessuale in danno di minori*[157], la quale individua nella Polizia postale e delle comunicazioni l'organo preposto a condurre le attività occorrenti per il contrasto dei reati perpetrati attraverso il mezzo informatico[158].

Per quanto attiene alla delicata questione sulla protezione delle informazioni, il primo documento italiano inerente la loro tutela è la direttiva *Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni*[159] del 16 gennaio 2002, che afferma l'importanza strategica per il Paese di proteggere e tutelare le informazioni raccolte nei database della pubblica amministrazione, sollecitando le PA a testare il proprio livello di sicurezza informatica e mettere in atto tutte azioni necessarie per un livello adeguato di sicurezza. Tale disciplina è regolamentata anche dal Codice in materia di protezione dei dati personali approvato

[157] "*Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù*.", pubblicata nella Gazzetta Ufficiale n. 185 del 10 agosto 1998, in <http://www.camera.it/parlam/leggi/98269l.htm> (ultima consultazione 9-11-2014).

[158] Articolo 14.

[159] Emanata dal Ministero per le Innovazioni e tecnologie, in <http://www.gazzettaufficiale.it/eli/id/2002/03/22/02A03219/sg%20;jsessionid=nBvFj9k-8FcOCREFNlFaag__.ntc-as1-guri2a> (ultima consultazione 9-11-2014).

con decreto legislativo n°196 del 30 giugno 2003, che regolamenta il trattamento dei dati personali con obblighi previsti per le pubbliche amministrazioni.

Per promuovere gli interventi normativi, regolamentari e amministrativi in materia di sicurezza e tutela delle reti, il Gruppo di lavoro, istituito con Decreto interministeriale del 1 settembre 1999, diventa Osservatorio permanente per la sicurezza e la tutela delle reti e delle comunicazioni all'interno del Ministero dello sviluppo economico nel 2003 con un Decreto interministeriale. Ampliato in modo permanente, dalla presenza di rappresentanti del Ministero della difesa, del dipartimento per la funzione pubblica, del dipartimento per l'innovazione e le tecnologie e del Ministero delle attività produttive, questo Osservatorio risponde all'esigenza di monitorare l'evoluzione tecnologica e normativa dei diversi aspetti del settore delle telecomunicazioni con particolare riguardo al tema della sicurezza[160].

Organo che ricopre il ruolo importante di principale interlocutore nazionale con l'ENISA è l'Istituto superiore delle comunicazione e delle tecnologie dell'informazione (ISCOM)[161] organo tecnico scientifico del Governo all'interno del MISE la cui istituzione risale al 1907[162] e che si è evoluto negli anni al pari della tecnologia del settore delle telecomunicazioni e dell'informazione. Oggi l'Istituto si articola in quattro divisioni all'interno delle quali è suddiviso il personale composto da 112 unità altamente specializzate delle quali il 70% è rappresentato da tecnici ed ingegneri e supporta con attività di consulenza aziende del settore ICT, PA e utenti soprattutto nell'ambito dei sevizi alle imprese. Inoltre l'Istituto si occupa di organizzare le esercitazioni nazionali in tema di cyber security e partecipa a quelle paneuropee e quello congiunte UE-USA con lo scopo di valutare l'efficienza dell'*information sharing* tra settore pubblico e privato.

Uno dei primi rapporti pubblicati in tema di cyber security è rappresentato dal testo "*Protezione delle infrastrutture critiche informatizzate. La realtà italiana.",* pubblicato nel 2004 dal Gruppo di lavoro sulla protezione delle infrastrutture critiche informatizzate istituito nel 2003 dal Ministero per l'Innovazione e le tecnologie composto da rappresentanti di diversi Ministeri come quello dell'interno, delle Infrastrutture e delle Comunicazioni e del settore privato come Telecom Italia, ABI, Wind e Snam Rete Gas e che sottolinea l'importanza strategica per l'intero Paese della sicurezza delle infrastrutture critiche data la loro forte interdipendenza in ambito informatico, individuando quelle di maggior impatto per il sistema Paese[163], classificate poi nel 2008 dal decreto *Individuazione delle infrastrutture critiche informatiche di interesse nazionale* approvato dal

[160] Osservatorio permanente per la sicurezza e la tutela delle reti e delle comunicazioni, in <http://www.sviluppoeconomico.gov.it/index.php?view=article&catid=686%3Apresentazioni&id=2017543%3Aosservatorio-permanente-per-la-sicurezza-e-la-tutela-delle-reti-e-delle-comunicazioni-&format=pdf&option=com_content> (ultima consultazione 9-11-2014).

[161] Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione opera nell'ambito del Ministero dello Sviluppo Economico, Presentazione, in <http://www.isticom.it/index.php/presentazione (ultima consultazione 9-11-2014).

[162] Legge 111 del 24 marzo 1907 sull'ampliamento e il miglioramento dei servizi postali, telegrafici e telefonici.

[163] Nello specifico: infrastruttura elettrica, reti informatiche e di telecomunicazioni, infrastruttura per il trasporto del gas, rete ferroviaria e viaria, circuiti bancari e finanziari, ospedali, ed altre criticità infrastrutturali, impianti nucleari, navigazione satellitare e sistemi SCADA.

Ministero dell'Interno. Questo rapporto inoltre invita alla creazione di un CERT-PA di cui parleremo in seguito.

Il 2005 vede l'emanazione del decreto legislativo n°82 del 7 Marzo *Codice dell'amministrazione digitale* e la legge n°155 del 31 luglio "recante misure urgenti per il contrasto al terrorismo internazionale" detta Legge Pisanu, nome dell'allora Ministro dell'Interno. Il Codice è alla base del processo di digitalizzazione delle attività amministrative per un reale ammodernamento degli enti pubblici, attivando tecnologie digitali per la comunicazione telematica tra le PA e i cittadini e le imprese. La legge Pisanu invece attribuisce competenza al Ministero dell'Interno per la protezione delle infrastrutture critiche informatizzate[164] e identifica la Polizia Postale e delle comunicazioni come responsabile dell'applicazione delle leggi contro gli attacchi informatizzati contro le infrastrutture critiche ponendo sotto il suo controllo il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (CNAIPIC) istituito successivamente nel 2008[165]. Il CNAIPIC svolge attività di tutela dei sistemi telematici di istituzioni e PA, enti pubblici e privati e aziende operanti nei settori dei rapporti internazionali, della sicurezza, della difesa, della finanza, delle comunicazioni, dei trasporti, dell'energia, dell'ambiente, la cui attività si è ritenuta strategica per la tutela dell'ordine e della sicurezza pubblica nazionale dal Ministero dell'Interno. Il CNAIPIC e le singole infrastrutture critiche gestiscono i servizi di protezione informatica attraverso collegamenti telematici dedicati, realizzati sulla base di convenzioni stipulate con il dipartimento della pubblica sicurezza quindi attraverso una sala operativa attiva H24 7 giorni su 7. Il centro, attraverso il monitoraggio della rete e i rapporti di collaborazione con altri organismi di polizia e aziende dell'ICT security nazionali ed internazionali, realizza attività di intelligence sulla raccolta dei dati e delle informazioni utili per la prevenzione e le analizza in chiave comparativa per misurare l'evoluzione delle minacce in ambito cyber. In caso di un attacco alle IC il centro può contare sulla collaborazione di 20 compartimenti e 80 sezioni dell'articolazione periferica della Polizia Postale e delle Comunicazioni e di forze di polizia straniere ed internazionali come Interpol ed Europol. Secondo quanto previsto dalla convenzione di Budapest sul cyber crime, presso li CNAIPIC è attivo il punto di contatto italiano per le emergenze nell'ambito di attacchi informatici transnazionali. Il punto di contatto opera H24 7 giorni su 7 all'interno della rete *Hightechcrime* costituita in ambio G8 ed estesa al Consiglio d'Europa che collega 64 Paesi nel Mondo. Dati statistici[166] forniti dalla Polizia Postale e delle Comunicazioni mostrano che gli attacchi rilevati nell'anno 2013 sono stati 746, quasi il doppio rispetto all'anno precedente, gli *alert* diramati 786, le richieste di cooperazione all'interno dell'*Hightechcrime network*[167] 62, le indagini avviate 53, le persone denunciate 18 e quelle arrestate 9 e che sono stati realizzati ben 9121 monitoraggi.[168] Dal 2006 inoltre è attivo il portale del Commissariato di P.S. on-

[164] Articolo 7bis sulla sicurezza telematica.

[165] Decreto del Ministero dell'Interno del 9 gennaio 2008 in attuazione della legge 31 luglio 2005 n° 155.

[166] *Relazione annuale 2014 della Polizia Postale e delle Comunicazioni*, fornita per questa ricerca dal Vicequestore di Firenze, Dott.ssa Stefania Pierazzi.

[167] Ai sensi dell'Articolo 35 della Convenzione di Budapest.

[168] All'interno della II Divisione del Servizio Postale e delle Comunicazioni è operante anche il centro nazionale per il contrasto della pedopornografia on-line, CNCPO, istituito con legge n° 38 del 6 febbraio 2006. L'attività investigativa di tale centro riferita all'anno 2013 conta 28063 siti monitorati, 1641 siti inseriti in blacklist, 430 perquisizioni, 344 persone denunciate e 55 persone arrestate.

line[169] che ha lo scopo di diventare il punto specializzato di riferimento per gli utenti di internet e che ha ricevuto, nel 2013, 7.014 denunce.

Anche la Guardia di Finanza e l'arma dei Carabinieri hanno centri preposti al contrasto di questo tipo di criminalità, infatti il Nucleo speciale frodi telematiche della GdF, attivo dal 2001, svolge la sua attività soprattutto nel contrasto ai reati di natura finanziaria commessi in rete e collabora anche con l'Agenzia per l'Italia Digitale, mentre il servizio investigazioni scientifiche dell'arma dei Carabinieri si compone di 4 reparti e 29 sezioni e un Raggruppamento investigazioni scientifiche attivi nell'ambito della sicurezza informatica.[170]

Il processo nazionale di contrasto al cyber crime, fenomeno a carattere altamente transnazionale, porta l'Italia nel 2008 alla ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica.[171] L'anno successivo viene promosso dal Ministero per la Pubblica Amministrazione e per l'Innovazione il "Piano e-Gov 2012", con il fine di aumentare il livello di digitalizzazione del Paese e ridurre il *digital divide*.

Il cyber crime diventa a tutti gli effetti una delle minacce alla sicurezza nazionale più rilevanti con la *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico*[172] trasmessa dal Comitato parlamentare per la sicurezza della Repubblica (COPASIR) alle Camere il 15 luglio del 2010. La Relazione distingue le minacce del *cyber space* in cyber crime, *cyber terrorism*, *cyber espionage* e *cyber war*; proponendo per le successive politiche nazionali di contrasto in materia, il coinvolgimento trasversale di imprese e cittadini per incentivare partnership tra settore pubblico e privato e la cultura alla sicurezza informatica. La rilevanza di questa relazione consiste nel fatto che, per la prima volta, si annoveri tra gli scenari di rischio la *cyber threat* e che inviti il Governo ad adottare una struttura di coordinamento che gestisca in modo adeguato le politiche per il contrasto alle minacce informatiche e i maggiori aspetti inerenti la *cyber security*.

Dal 2011 al 2013 l'Italia in questo campo ha compiuto altri passi avanti nell'implementazione di azioni volte ad affrontare questo fenomeno. Tra queste annoveriamo l'*Attuazione della direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione* del 2011[173] che assegna al Nucleo interministeriale di situazione e pianificazione (NISP)[174] il compito di stabilire le procedure per l'individuazione delle infrastrutture critiche europee (ECI) e svolgere il

[169] Consultabile all'indirizzo: www.commissariatodips.it.

[170] Carabinieri indagini scientifiche, in <http://www.carabinieri.it/Internet/Arma/Oggi/RACIS/> (ultima consultazione 9-11-2014).

[171] Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, legge n° 48 del 18 marzo 2008.

[172] *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico*, COPASIR, 7 luglio 2010, in <http://www.senato.it/service/PDF/PDFServer/BGT/525461.pdf> (ultima consultazione 9-11-2014).

[173] Decreto legislativo n° 61, 11 aprile 2011, del Presidente della Repubblica.

[174] Istituito dal DPCM 5 maggio 2010, Organizzazione nazionale per la gestione di crisi, che aggiornava il Manuale nazionale per la gestione di crisi del 1994, basandosi sul NATO Crisis Responses System Manual e sul Manual of EU Emergency and Crisis Coordination.

ruolo di punto di contatto nazionale per la protezione delle ECI a livello europeo senza però prevedere alcun fondo finanziario per questi obiettivi.

Nel 2012 con il Decreto legge n°83 del 15 giugno 2012[175] l'Italia istituisce l'Agenzia per l'Italia Digitale (AgID) al fine di coordinare tutte le azioni di innovazione per incentivare l'uso delle tecnologie ICT in ambito PA, in linea con gli obiettivi dell'Agenda Digitale italiana[176] e l'Agenda Digitale europea. La realizzazione della rete a banda larga dell'Italia, l'infrastruttura ICT delle PA e lo sviluppo digitale sono alcune tra le azioni strategiche portate avanti dall'AgID con l'obiettivo di costituire un'opportunità di crescita economica per il Paese. Sempre all'interno dell'AgID dal gennaio 2014 è attivo il CERT-PA, uno dei CERT operativi in Italia, di cui si parlerà in seguito.

In ambito *cyber security* la legge 133 del 7 agosto 2012[177], riconosce al Dipartimento informazioni per la sicurezza (DIS) l'importante ruolo di coordinamento delle attività di intelligence per rafforzare la protezione e la sicurezza informatica nazionale.

Nel 2013, per la prima volta, l'Italia definisce "l'architettura istituzionale deputata alla sicurezza nazionale relativamente alle infrastrutture critiche materiali ed immateriali"[178] con il DPCM[179] del 24 gennaio, approvato dal Presidente del Consiglio dei Ministri rispondendo all'esigenza di dotarsi di un quadro legale per la sicurezza nel *cyber space*, individuando gli organi preposti al contrasto di eventuali pericoli da esso derivanti, delineando un modello organizzativo funzionale per la sicurezza informatica e fornendo definizioni utili e condivise sui principali aspetti della sicurezza in ambito cyber.

Il DPCM individua tre diversi livelli di intervento: livello strategico e politico (per l'elaborazione degli indirizzi strategici, affidati al Comitato interministeriale per la sicurezza della Repubblica); livello operativo, sostenendo e coordinando tutti gli organismi coinvolti (il Nucleo per la Sicurezza Cibernetica presieduto dal Consigliere Militare del Presidente del Consiglio); livello di gestione delle crisi (affidato al Tavolo interministeriale di crisi cibernetica).

Questo documento individua, inoltre, le strutture pubbliche nazionali deputate alla *cyber security*. Il Presidente del Consiglio, nello specifico, ha il compito di redigere un *Quadro strategico nazionale per la sicurezza dello spazio cibernetico* (QSN) ed un *Piano nazionale per la protezione cibernetica e la sicurezza informatica* (PN) adottato il 18 dicembre 2013 su proposta unanime del Comitato interministeriale per la sicurezza della Repubblica (CISR). Entrambi i documenti sono entrati in vigore il 27 gennaio 2014[180] e hanno lo scopo di definire gli strumenti e le procedure per contrastare le cy*ber threat* nei confronti delle reti di interesse nazionale.

Il QSN nello specifico è un documento politico programmatico e individua i profili e le tendenze evolutive delle minacce e delle vulnerabilità dei sistemi e delle reti di interesse

[175] Decreto convertito in legge 134 del 7 agosto 2012, detto decreto sviluppo.

[176] Stabilita con Decreto del Ministero dello Sviluppo economico del 1 marzo 2012. Le misure per l'effettiva realizzazione dell'Agenda, sono indicate nel Decreto legge 179 del 18 ottobre 2012 "*Ulteriori misure urgenti per la crescita del Paese".*

[177] Modifiche alla legge 3 agosto 2007 n° 124, concernente il sistema di informazione per la sicurezza della Repubblica e la disciplina del segreto, Art. 3.1.

[178] Art. 1.1

[179] Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale.

[180] Gazzetta ufficiale n° 41 del 19 febbraio 2014.

nazionale, specificando i ruoli e i compiti dei diversi soggetti pubblici e privati e gli strumenti e le procedure per prevenire e contrastare le minacce del *cyber space*[181]. Il cyber crime, il cui impatto è oggetto principale di questa ricerca, è una della quattro macrocategorie, trattate dal QSN, delle minacce del *cyber space*, insieme allo spionaggio, alla guerra e al terrorismo informatico e ritenuto rischio di massima priorità per il Paese. Il documento definisce, inoltre, le procedure per implementare le capacità italiane in ambito cyber attraverso sei indirizzi strategici e gli attori primari per la sicurezza informatica nazionale, definiti dal DPCM del 24 gennaio 2013[182], e undici indirizzi operativi. La concreta attuazione del QSN è demandata al *Piano Nazionale per la protezione cibernetica e la sicurezza informatica*, delineando gli obiettivi da raggiungere per tutti gli indirizzi operativi e sviluppando quelli strategici nell'arco del biennio 2014-15 sulla base di partnership pubblico-privato dalle quali dipende il successo delle politiche adottate. Il Piano purtroppo non stabilisce ancora un bilancio per la *cyber security* e non contiene riferimenti ai tempi di attuazione e le responsabilità per le azioni indicate. La strategia ufficiale nazionale di *cyber security* italiana è quindi costituita da questi due documenti, QSN e PN, che nonostante il ritardo rispetto alla media dei Paesi europei più avanzati, si pongono l'obiettivo di prevenire le future *cyber threats* e pongono le basi per un graduale progresso su questo fronte.

Il CERT nazionale[183], come da dichiarazione della Dott.ssa Rita Forsi, Direttore dell'Istituto superiore delle comunicazioni Ministero dello Sviluppo Economico-Dipartimento per le Comunicazioni (ISCOM) è operativo dal 5 giugno 2014. Il CERT, team di risposta alle emergenze di natura informatica, ricopre il ruolo di organizzazione responsabile per il monitoraggio degli incidenti informatici e per la gestione di tali incidenti, aiutando gli utenti nel ripristino delle attività precedenti la violazione. Per ridurre i rischi derivanti dagli attacchi informatici molti CERT forniscono ai loro utenti anche informazioni utili alla conoscenza del fenomeno. Il compito del CERT a livello nazionale è importante in quanto contribuisce alla sicurezza fisica ed economica del Paese identificando gli incidenti che potrebbero colpire infrastrutture critiche, informa gli *stakeholder* sulle minacce emergenti e dialoga con gli altri CERT sul territorio nazionale ed internazionale sia del settore pubblico che privato.

Per quanto riguarda lo stato attuale dei CERT in Italia, l'elenco disponibile sul sito dell'ENISA[184], riferito ai CERT operativi in ogni Paese dell'Unione, non risulta aggiornato in quanto riporta CERT non più attivi sul territorio italiano. Dall'elenco ENISA infatti risultano presenti nove CERT in Italia. Di questi, attraverso la consultazione dei siti internet e le telefonate realizzate ai

[181] Presidenza del Consiglio dei Ministri, QSN, in <http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/quadro-strategico-nazionale-cyber_0.pdf> (ultima consultazione 9-11-2014).

[182] Presidente del Consiglio dei Ministri, CISR, intelligence, Nucleo per la sicurezza cibernetica, NISP e CERT nazionale.

[183] Maggiori informazioni si possono trovare sul sito: <https://www.certnazionale.it/chi-siamo/>

L'identificazione di un CERT-GOV al Ministero delle sviluppo economico è stata introdotta con il Decreto legislativo 28 maggio 2012, n. 70 *Modifiche al decreto legislativo 1° agosto 2003, n. 259, recante codice delle comunicazioni elettroniche in attuazione delle direttive 2009/140/CE, in materia di reti e servizi di comunicazione elettronica, e 2009/136/CE in materia di trattamento dei dati personali e tutela della vita privata*, in < http://www.gazzettaufficiale.it/gunewsletter/dettaglio.jsp?service=1&datagu=2012-05-31&task=dettaglio&numgu=126&redaz=012G0091&tmstp=1338881263427> (ultima consultazione 10-11-2014).

[184] Consultabile all'indirizzo: <http://www.enisa.europa.eu/activities/cert//background/inv/certs-by-country-interactive-map> (ultima consultazione 10-11-2014)

numeri indicati si è potuto accertare che alcuni come il CERT-RAFVG Regione Friuli Venezia Giulia e il CERT-IT non sono più attivi e che il CERT delle Poste Italiane (PI-CERT) ha, a differenza di quanto si può leggere sul sito ENISA, sia la certificazione *FIRST* che la certificazione *Trusted introducer*, certificazioni che attestano il livello di maturità dei CERT e ne favoriscono il dialogo. Queste informazioni si sono potute reperire dagli elenchi aggiornati dei siti ufficiali delle due certificazioni. Per alcuni CERT vi è una mancanza di informazioni necessarie a comprendere l'attività che viene effettivamente svolta e il loro reale stato. Di seguito l'elenco aggiornato risultato della ricerca effettuata.

CERT	Data	Sito Web	Certificazione TI	Certificazione First	Stato
Servizio Base Provider Clienti PI-CERT	I° Trim. 2013	http://www.picert.it	Accreditato dal 1 Gen 2001	Membro	Attivo
Telecom Italia CERT - TS.SOC	2004	http://www.telecomitalia.com/CERT	Non accreditato	Non membro	Attivo
CERT-PA	II° Quad. 2014	http://www.cert-pa.it/	Non accreditato	Non membro	Attivo
CERT-Difesa	Non specificato	http://www.difesa.it/SMD/Staff/Reparti/II-reparto/CERT/ PAGINA NON TROVATA	Non accreditato	Non membro	Attivo
CERT IT Ricerca e Formazione	I° Trim. 1994	http://security.dsi.unimi.it PAGINA NON TROVATA	Non accreditato	Non membro	Non attivo
GARR-CERT	01/03/1999	http://www.cert.garr.it	Acceditato dal 3 Dic 2013	Non membro	Attivo
CERT ENEL Settore Energia	Non specificato	http://www.enel.it/attivita/servizi_diversificati/informatica/cert/ HOMEPAGE ENEL	Non accreditato	Non membro	Nessuna informazione a riguardo
CERT-RAFVG Regione Friuli Venezia Giulia	Non specificato	http://cert-rafvg.regione.fvg.it/ INDIRIZZO E-MAIL NON ATTIVO	Non accreditato	Non membro	Non attivo
SICEI-CERT Diocesi della Chiesa Cattolica	Non specificato	http://cert.chiesacattolica.it/	Non accreditato	Non membro	Attivo

Tabella 5 - Tabella riassuntiva del reale stato dei CERT italiani

Anche se c'è ancora molto da fare, lo sviluppo della cyber strategy in Italia nasce da una graduale presa di consapevolezza della necessità di dotarsi di strumenti adeguati a contrastare le minacce derivanti dal *cyber space*, di sicuro migliorabili nel tempo[185], ed in questo contesto la promozione di una maggiore cultura della sicurezza informatica tra cittadini, aziende e istituzioni è un passaggio fondamentale per il raggiungimento degli obiettivi prefissi.

3.4 Indagine empirica sull'impatto del cyber crime in Italia

[185] Per approfondimenti si veda: *Cybersecurity: Unione europea e Italia Prospettive a confronto* di Claudia Cencetti, 2014, Quaderni IAI, Edizioni Nuova Cultura.

È evidente come la sicurezza informatica sia ormai un argomento non solo attuale e di una certa entità, ma che necessiti di una conoscenza e studio aggiornato per cercare di contrastarlo. La mancanza di studi e statistiche nazionali ufficiali su tale fenomeno è stato uno degli aspetti che ha richiesto un approccio empirico per la realizzazione di questa ricerca. Per cercare quindi di avere una visione più completa dei vari aspetti e attori coinvolti quotidianamente nel contrasto e studio del cyber crime si sono realizzate interviste per analizzare lo stato attuale di questo fenomeno in ambito bancario e giuridico.

3.4.1 Settore bancario

Una delle realtà da sempre più consapevoli di queste problematiche è il settore bancario. A tal fine si è condotta un'intervista con la dott.ssa Monica Pellegrino, ICT Research Analyst presso ABI Lab[186], dalla quale è emerso che ABI Lab coordina un vero è proprio centro di *information sharing* e aggiornamento per le Banche italiane sulle principali minacce informatiche, l'Osservatorio Sicurezza e Frodi Informatiche[187], al quale partecipano oltre 40 Banche e 10 partner ICT specializzati in materia e che organizza incontri periodici finalizzati ad analizzare i principali trend in materia di frodi informatiche, sicurezza logica e gestione dell'identità di clienti e dipendenti. Inoltre, l'Osservatorio svolge le seguenti attività per le Banche italiane: monitoraggio dello scenario nazionale e internazionale; realizzazione di indagini di sistema e *survey* ad hoc; definizione di linee guida di sistema; analisi di soluzioni tecnologiche e modelli organizzativi per la prevenzione e contrasto delle principali minacce; analisi di policy interne in materia di sicurezza informatica; promozione e sviluppo di esperienze pilota e condivisione di best practices. In aggiunta, l'Osservatorio ha costituito una mailing list, denominata presidio.internet, estesa a oltre 300 referenti di Banche e alla Polizia Postale, attraverso la quale vengono fornite sia informazioni rilevanti su nuovi attacchi sia bollettini mensili sullo scenario della sicurezza informatica a livello nazionale e internazionale.

ABI Lab inoltre partecipa a diversi network internazionali, sia istituzionali sia operativi, allo scopo di essere aggiornati sui trend legati a frode e minacce informatiche. Inoltre, dalla *survey* annuale dell'Osservatorio Sicurezza e Frodi Informatiche, cui hanno partecipato per il 2014 25 organizzazioni bancarie rappresentative di circa il 77% del sistema in termini di dipendenti, è emerso che nel 2013 oltre il 70% del campione ha partecipato direttamente a community di *information sharing* ed ad iniziative associative per la collaborazione intersettoriale. Tra le diverse iniziative, si segnala anche la realizzazione della piattaforma di *information sharing* gestita dalla Polizia Postale e definita, insieme con ABI Lab, nell'ambito del progetto europeo di contrasto avanzato ai crimini informatici *On line Fraud Cyber Center and Expert Network* (OF2CEN)[188].

[186] Nato come un progetto nell'ambito del Settore Tecnologie e Sicurezza dell'Associazione Bancaria Italiana, ABI Lab si è costituito nel 2002 sotto forma di Consorzio e si è affermato oggi come il Centro di Ricerca e Innovazione per la Banca promuovendo la collaborazione tra Banche, aziende e istituzioni, in <http://www.abilab.it/consorzio/chi-siamo> (ultima consultazione 10-11-2014).

[187] Osservatorio Sicurezza e Frodi Informatiche, in <http://www.abilab.it/web/sicurezza-e-frodi-informatiche> (ultima consultazione 10-11-2014).

[188] Global Cybersecurity Center, On-line Fraud Cyber Centre and Experts Network (OF2CEN), in <http://www.gcsec.org/activity/research/on-line-fraud-cyber-centre-and-experts-network-of2cen> (ultima

A seguito della stipula della convenzione tra ABI e Polizia di Stato, firmata nel dicembre 2010 e finalizzata alla prevenzione dei crimini informatici nel settore bancario italiano, infatti, la collaborazione tra ABI, Banche e Polizia Postale e delle Comunicazioni è proseguita con diverse attività, tra cui la partecipazione congiunta al progetto europeo OF2CEN, finanziato dalla Commissione e coordinato dalla Polizia Postale. Il progetto, che si è concluso nell'ottobre 2013, ha visto la realizzazione di una piattaforma di *information sharing* per condividere dati relativi a transazioni anomale, con l'obiettivo di realizzare un canale di comunicazione sicuro con la Polizia Postale che possa facilitare il processo formale di segnalazione delle operazioni fraudolente. Alla piattaforma possono accedere, in modalità volontaria, tutte le Banche che abbiano preventivamente aderito alla convenzione con la Polizia Postale: inserendo le informazioni relative a transazioni fraudolente, ogni utente contribuisce ad alimentare il database gestito dalla Polizia, incrementando pertanto il livello di efficienza nello scambio di informazioni, che avviene con processi strutturati e sicuri, nonché l'efficacia e la rapidità dell'azione investigativa.

Per gli Istituti bancari l'attività di sensibilizzazione e informazione della clientela sui temi legati alle frodi e alle minacce informatiche, al fine di renderla consapevole dei rischi connessi a un uso negligente del web, è di importanza strategica non solo con lo scopo di aumentare l'adozione di misure tecnologiche e comportamentali opportune in ottica preventiva, ma anche per far conoscere le procedure da attuare verso la Banca e le Forze dell'Ordine in caso di anomalie.

Dalla *survey* dell'Osservatorio ABI Lab, è emerso inoltre che le Banche adottano i molteplici canali a loro disposizione per il dialogo con la clientela *Corporate* sulle tematiche di sicurezza, privilegiando naturalmente il portale di Internet Banking (100% del campione), ma anche le filiali (50%) e l'informativa contrattualistica (50%). Inoltre, a seguito dell'incremento degli attacchi informatici registrato negli ultimi tempi proprio nei confronti della clientela *Corporate*, ABI Lab ha realizzato nel 2013 in collaborazione con il Consorzio *Customer to Business Interaction* (CBI)[189] e con la Polizia Postale e delle Comunicazioni, un documento di raccomandazioni di tipo tecnologico e organizzativo, finalizzato a supportare le Banche nell'attività di sensibilizzazione della clientela *Corporate* per un utilizzo sicuro dei servizi di *Internet Banking*[190].

Dal Report 2014 dell'Osservatorio Sicurezza e Frodi Informatiche "*Sicurezza e frodi informatiche in banca. Come prevenire e contrastare le frodi su Internet e Mobile Banking*"[191],

consultazione 10-11-2014).

[189] Il *Consorzio Customer to Business Interaction (CBI)* è stato creato il 20 maggio 2008 in prosecuzione delle attività gestite dall'Associazione per il Corporate Banking Interbancario (ACBI), nata nel 2001. Il Consorzio CBI definisce in ambito cooperativo le regole e gli standard tecnici e normativi del "Servizio CBI", del "Servizio CBILL" e dei servizi di Nodo e gestisce l'infrastruttura tecnica di connessione tra i Consorziati, per realizzare, in via telematica, il collegamento ed il colloquio con la clientela, in ottica di interoperabilità a livello nazionale ed internazionale. Al Consorzio CBI aderiscono circa 600 Istituti Finanziari (95% del sistema bancario italiano, Poste Italiane e CartaLis), che ad oggi offrono il Servizio CBI in modalità competitiva ad oltre 950.000 imprese, in <http://www.cbi-org.eu/Engine/RAServePG.php/P/250110010404/T/Consorzio-CBI> (ultima consultazione 10-11-2014).

[190] Tali indicazioni, infatti, possono essere inviate dalle Banche alla clientela nelle modalità ritenute più opportune, ad esempio come allegato alla propria comunicazione in tema di sicurezza, come rielaborazione in base alle proprie esigenze, ecc.

[191] Il report contiene i risultati della *survey* condotta da ABI Lab sulle frodi via internet e mobile banking. Hanno risposto, per questa edizione, 25 organizzazioni, considerando banche, gruppi e *outsourcer* di servizi bancari; tuttavia, se si tiene conto del numero di singoli istituti associati ai rispondenti, il campione complessivo sale a 153 realtà

fornito per questa ricerca da ABI Lab, emerge che le operazioni fraudolente vengono rilevate in misura principale (44,2%) attraverso l'utilizzo di strumenti interni di monitoraggio delle transazioni anomale (sempre più presenti nelle Banche) o mediante disconoscimento delle operazioni da parte del cliente (39,2% dei casi) per il segmento *retail.* Nel 2013 il 95% dei singoli Istituti rappresentati nel rapporto ha rilevato episodi di furto di credenziali di accesso di *internet banking* a danno dei loro clienti *retail*, il dato sale al 100% se si considerano i clienti *corporate* su un campione di 18 Istituti rispondenti su 25.

In relazione alle transazioni fraudolente effettive l'analisi mostra una prevalenza di operazioni illecite di ricarica di carte prepagate andate a buon fine, pari al 58% del totale delle frodi effettive per il segmento *retail.* Il 39,4% delle operazioni che hanno comportato una perdita di denaro è invece rappresentata dai bonifici, mentre il restante 2,6% da ricariche telefoniche, sempre meno utilizzate per attività criminali, probabilmente per i limitati volumi economici associati a tale tipologia di operazione.

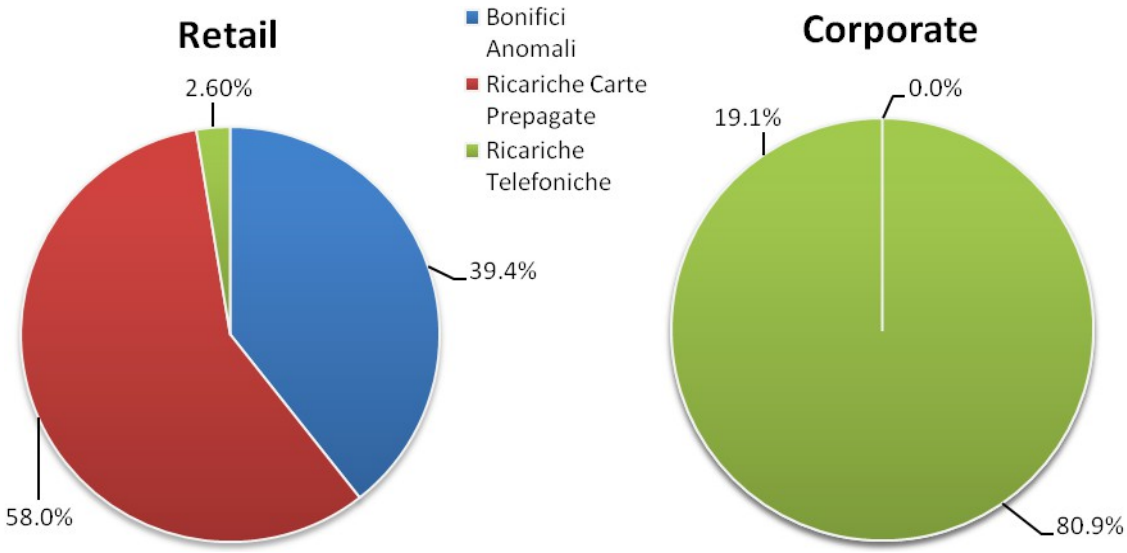


Figura 22 - Ripartizione percentuale delle tipologie di transazioni effettive
Fonte: Come prevenire e contrastare le frodi su Internet e Mobile Banking, ABI Lab, maggio 2014

I dati cambiano per il segmento *corporate* dove l'80,9% delle tipologie di transazioni effettive è rappresentato dai bonifici, che a livello generale sono la tipologia più frequentemente disposta via *Internet Banking* per il comparto imprese.

È interessante notare quale sia il rapporto tra le transazioni fraudolente effettive a danno dei clienti *corporate* e clienti *retail* e il conseguente volume economico di tali transazioni. A fronte di un minor numero di transazioni fraudolente (43,3%) il volume economico sottratto ai clienti *corporate* è 3 volte maggiore rispetto a quanto rilevato per il *retail*, rispettivamente pari al 74,4% e al 25,6% del totale.

bancarie. In termini di rappresentatività a livello di sistema, il campione rispondenti fa riferimento a circa il 77% dei dipendenti e dei conti *Retail* abilitati e a circa 1,9 milioni di account *Corporate* attivi. I dati riportati fanno riferimento al periodo temporale compreso tra il 1° gennaio e il 31 dicembre 2013 e sono distinti per segmento di clientela, *Retail* e *Corporate*.

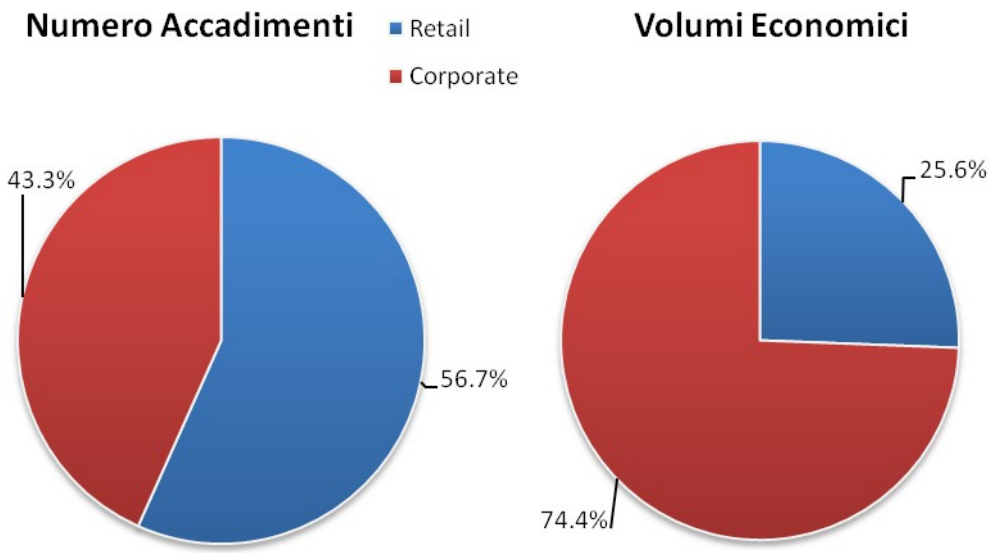


Figura 23 - Ripartizione totale delle transazioni effettive, suddivise per segmento
Fonte: Come prevenire e contrastare le frodi su Internet e Mobile Banking, ABI Lab, maggio 2014

3.4.2 Ambito giuridico

In seguito alla "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno"[192] tutti i reati di tipo informatico vengono seguiti dalla Procura distrettuale. Per questo motivo si è scelto di condurre delle interviste presso le Procure, al fine di capire meglio l'entità del fenomeno e come vengono trattate queste tipologie di reati. In seguito all'intervista con il Sostituto Procuratore Alberto Perduca della Procura della Repubblica di Torino e con il Sostituto Procuratore Andrea Cusani della Procura della Repubblica di Firenze, entrambi specializzati nei reati di tipo informatico, sono emersi aspetti di notevole interesse.

Senza dubbio oggi il web rappresenta un'opportunità enorme per il criminale, le transazioni economiche avvengono sempre di più attraverso internet e di conseguenza l'attività predatoria si è spostata sulla rete. Internet d'altro canto rappresenta anche un'enorme possibilità di mercato per le imprese, soprattutto per le PMI che possono abbattere i costi di molti servizi attraverso il web, infatti moltissime aziende di beni e servizi spostano sempre di più loro attività nella rete. Il phishing, per entrambi i magistrati intervistati, rappresenta oggigiorno la quasi totalità dei casi che arrivano sulle loro scrivanie relativi a fenomeni di cyber crime. Il phishing rappresenta un mezzo a rischio praticamente zero per chi decide di compiere reati di tipo economico. Il problema è che l'intera società, dal singolo cittadino all'azienda, Governi ecc, è indietro rispetto allo sviluppo della rete. Secondo il dott. Cusani uno dei problemi più grandi che si riscontra è un'enorme difficoltà nella collaborazione internazionale per il contrasto a questo tipo di fenomeno. La maggior parte dei reati di cyber crime infatti non proviene da attaccanti italiani o dal nostro territorio, ma da

[192] Articolo 11, legge n° 48/2008 pubblicata nella *Gazzetta Ufficiale* n. 80 del 4 aprile 2008 - Supplemento ordinario n. 79, in <http://www.parlamento.it/parlam/leggi/08048l.htm> (ultima consultazione 10-11-2014).

Paesi dell'est Europa come Bulgaria o Romania. In quei Paesi in seguito alla passata delocalizzazione delle imprese IT si sono sviluppate delle enormi competenze che poi sono state sfruttate dalla criminalità informatica. Per questo tipo di criminalità a forte carattere transazionale l'iter giudiziario, nel momento in cui si accerti che il reato è stato commesso attraverso un altro Paese, sarebbe quello di richiedere una rogatoria internazionale, la cui compilazione prevede costi molto alti in termini di risorse non solo economiche ma anche temporali. In questi casi, secondo una stima realistica, lo Stato a cui è stata rivolta la rogatoria risponde dopo 3 mesi, un periodo che per il tipo di reato considerato è già problematico ai fini della reperibilità e dell'acquisizione delle informazioni utili. I tempi medi per una rogatoria si attestano tra i 6 e i 9 mesi e possono allungarsi anche a più di un anno o addirittura non ricevere mai risposta. Anche un solo mese in questo campo rappresenta un periodo di tempo enorme considerando la volatilità dei dati informatici. Secondo il parere del dott. Cusani, a livello internazionale ed Europeo il gap di competenze, giuridico, tecnologico ecc. tra le Nazioni è un'ulteriore impedimento al contrasto di questo fenomeno. Vi sono ordinamenti diversi, uffici preposti diversi, procedure diverse, conciliare tutto ciò e rendere più celere possibile le indagini è difficilissimo. Eurojust, EC3 o altri strumenti a livello europeo sono certamente la giusta direzione di marcia nel contrasto al fenomeno, tuttavia risultano ancora fortemente legati ad un sistema di rapporti tra Paesi basato piuttosto su cortesi dichiarazioni di disponibilità alla cooperazione che su effettivi ed efficaci vincoli sia pure di tipo pattizio. L'intento è ammirevole, ma nella realtà ci si scontra con procedure che all'atto pratico rendono questo lavoro estremamente complesso e lento. "*È come rincorrere con una 500 un ladro che fugge a bordo di una Ferrari ultimo modello.*" Ha dichiarato a tal proposito il Magistrato. Largamente incerta è poi la collaborazione con Paesi con i quali non esistono accordi di cooperazione giudiziaria[193].

Dello stesso parere è il Sostituto Procuratore dott. Perduca di Torino il cui team si occupa dei reati di frode in generale e di tutti i reati informatici, previsti dall'ordinamento, che sono di competenza distrettuale. Per la Procura di Torino parliamo di circa 4.000 casi l'anno per i quali il tasso di esercizio dell'azione penale è molto basso. Su 4.000 casi, circa il 90% vengono archiviati. Prima ancora di essere assegnati ai giudici se ne archiviano almeno la metà e le motivazioni dell'archiviazione possono essere molteplici, di natura processuale, per esempio manca la querela, infatti molti di questi reati sono perseguibili a querela, o che la querela sia troppo generica o non contenga informazioni utili, oppure perché riguarda questioni civilistiche non trattate in sede penale, o anche perché molto spesso il cyber criminale è difficilmente rintracciabile. Ad ogni modo, soprattutto nei casi in cui sarebbe necessaria una rogatoria internazionale, quello che si opera è una mera analisi costi benefici e nonostante l'obbligatorietà dell'azione penale per questi casi non sempre si realizza un esercizio dell'azione penale.

[193] Nel contrasto ai reati informatici un ulteriore elemento da considerare è la difficoltà di determinare il Tribunale di competenza dato che è complesso determinare il luogo fisico in cui il reato si è compiuto. In sintesi, le generali regole di competenza previste dal codice vanno correlate alle singole fattispecie incriminanti e quindi è possibile che per i diversi reati informatici previsti dalla legge vengano in rilievo criteri di determinazione della competenza per territorio diversi tra loro. Per questa ragione il tema della determinazione della competenza territoriale in materia di reati informatici non può essere affrontato unitariamente. È probabile quindi che le prassi applicative delle diverse procure in tema di competenza possano essere diverse ed anche divergere sensibilmente.

Questo aspetto è di enorme rilevanza sociologica perché quello che emerge è come il confine tra norme procedurali scritte e prassi sia molto variabile e che sono gli operatori del diritto ad avere il compito di definire in larga misura il significato delle norme e la loro applicazione. La differenza tra prassi e procedura è un fenomeno frequente come lo è il superamento dell'obbligatorietà dell'azione in diversi ambiti penali. Quello che accade nell'ambito dei reati di natura informatica è il riferimento ad un mero principio di economia, al di là dell'obbligatorietà dell'azione penale, si effettua una prognosi di insuccesso in base ad una valutazione costi benefici.[194]

I reati informatici registrati nelle Procura di Torino variano dagli accessi non autorizzati a Facebook, o a social media in generale, che però non sono reati che aggrediscono il patrimonio, al furto d'identità digitale alle frodi on-line. Il Sostituto Procuratore Perduca afferma che si registra un vero e proprio stillicidio sui conti correnti a causa del phishing e dei prelievi on-line con varie tecniche rispetto ai quali si può fare ben poco, sia per la pochezza del singolo prelievo che magari è solo di qualche centinaio di euro, sia per la velocità della tipologia di reato nei confronti del quale è molto difficile investigare. Spesso i soldi vengono accreditati sul conto o sulla carta prepagata di qualcuno, che è stato identificato con delle generalità false, oppure intestata a persone irreperibili, che prestano la loro identità per far transitare i soldi. La classica truffa nel confronti delle aziende, soprattutto PMI, consiste di solito nell'accesso da parte degli hacker alla e-mail aziendale, e attraverso questa riescono a rubare l'elenco di clienti e fornitori; la truffa vera e propria consiste nel mandare una e-mail ai contatti rubati comunicando che l'impresa ha per esempio cambiato IBAN bancario, quindi i soldi vanno poi a finire su un conto appositamente creato dal cyber criminale. Il cliente paga credendo di versare l'importo all'azienda giusta, in realtà il conto corrente beneficiario è sito nei Paesi più improbabili. Di solito queste truffe avvengono attraverso e-mail di phishing nelle quali l'utente clicca un link malevolo, o in alcuni casi i criminali riescono a "craccarre" la password dell'account. Il problema consiste nel fatto che l'attacco può avvenire da qualsiasi parte del Mondo perché l'IP non è assolutamente indicativo. Per le forze di Polizia e la Magistratura diventa davvero difficile avviare un'azione di contrasto efficace.

Per quanto riguarda i reati inerenti la proprietà intellettuale, il classico caso riguarda l'ex dirigente o dipendente che si mette in proprio o viene licenziato, e ruba tutti i dati dell'azienda precedente per poi utilizzarne il pacchetto clienti o accedere alla banca dati dell'azienda. Nella quasi totalità dei casi sono insider che accedono ai sistemi perché agli account aziendali a loro assegnati non vengono revocati. I reati connessi ad attività di hacktivism sono pochissimi rispetto ad altri attacchi come il phishing e lo spear phishing, che rappresentano il vero problema a livello economico.

---

[194] Per approfondimenti si veda: *L'obbligatorietà dell'azione penale come un mito? Appunti sul caso italiano*, in M. Verga (a cura di), Centro Universitario per le Ricerche sulla Sociologia del Diritto, dell'Informazione e delle Istituzioni Giuridiche (CIRSDIG), in "Quaderno dei lavori 2007, Terzo Seminario Nazionale di Sociologia del Diritto, A.I.S. – Sezione di Sociologia del Diritto", Working Paper n. 25, 2007, pp. 121-136, in <http://www.cirsdig.it/Pubblicazioni/capraia.pdf> (ultima consultazione 11-11-2014); e Zanier M. (2009) *Tra il dire e il fare. Obbligatorietà dell'azione penale e comportamenti degli attori giuridici*, Macerata, EUM Edizioni Università di Macerata.

Secondo il parere del dott. Perduca, sarebbe necessario un sistema di prevenzione maggiore. Una volta che il reato è stato compiuto, soprattutto se economicamente di dimensioni non considerevoli, è difficile che l'apparato repressivo possa intervenire efficacemente, tenuto conto dei limiti di risorse, processuali, dei tempi, ecc. Il procedimento penale così come è concepito e articolato è uno strumento sovradimensionato in termini di costi e di tempi. Con una maggiore educazione e formazione si alzerebbe il livello di resistenza.

Come sappiamo, la Polizia Postale è l'organo più specializzato nel contrasto ai reati di natura informatica, ciononostante, spesso accade che il cittadino o l'impresa denuncino casi di questo tipo ad altre forze di Polizia come per esempio ai Carabinieri, più presenti sul territorio e di stazionamento anche nei paesi più piccoli. Non sempre però il carabiniere che accoglie la denuncia ha la formazione adatta per trattare questo tipo di reati, quindi accade che rimanda il caso alla Postale o che non metta in atto tutte le necessarie indagini nei giusti tempi. Dovrebbe essere previsto quindi anche un percorso di formazione base per tutte le Forze dell'Ordine preposte ad accogliere questo tipo di denunce, alzando di conseguenza il livello di preparazione media minima.

Attraverso la disponibilità del Sostituto Procuratore Perduca e del Sostituto Procuratore Riccaboni della Procura della Repubblica di Torino si è avuta la possibilità di visionare e riportare in questa ricerca un caso studio riguardante un reato di frode informatica a danno di una PMI del Piemonte.

Il caso preso in esame coinvolge una azienda specializzata nella produzione di cibo per animali. I clienti di questa media impresa sono per il 90% costituiti da imprese straniere. Quattro aziende dell'Asia, precisamente una di Hong Kong, una australiana, una giapponese e una della Thailandia, clienti della suddetta, ricevono una e-mail, apparentemente dalla azienda piemontese, riportante una fattura emessa nei loro confronti con gli esatti importi previsti, elemento che quindi non ha fatto assolutamente insospettire i contabili delle aziende. Questa e-mail riportava inoltre la comunicazione del cambio di IBAN da parte della azienda fornitrice, che ben 3 aziende su 4 hanno recepito senza realizzare alcun tipo di controllo ed effettuando quindi il bonifico verso il conto corrente dei cyber criminali. Uno solo dei quattro clienti, o per policy aziendale o perché insospettita dall'IBAN diverso da quelli italiani, ha effettuato un accertamento telefonico all'azienda di Cuneo per verificare l'effettivo cambio di IBAN permettendo così di scoprire la truffa in atto. A questo punto l'azienda piemontese contatta tutti i clienti informandoli di non avere effettuato nessun cambio di IBAN ed in questo modo scopre che 3 clienti avevano già ricevuto questa e-mail e pagato fatture per un totale di 200 mila dollari. A seguito della denuncia alle autorità competenti sono iniziate le indagini, ma risalire all'IP da cui era stata mandata questa e-mail truffa è stato impossibile. Accertare da dove è stata condotta una violazione informatica, come abbiamo visto, è difficilissimo. In questi casi qualche risultato lo si può ottenere attraverso la collaborazione delle Banche seguendo i trasferimenti di denaro. In seguito alla richiesta, da parte della azienda alla propria Banca, di reperire informazioni attraverso il sistema bancario internazionale infatti si è scoperto che i bonifici sono stati accreditati su 4 conti differenti in 2 Banche a Tbilisi in Georgia. Da questo tipo di accertamenti, di solito molto efficienti soprattutto tra Banche di Paesi evoluti a livello finanziario e che non appartengono alle *black list*, si può avere

risposta già dopo 24/48 ore e bloccare l'emissione o l'accredito di un bonifico in caso di un'indagine per truffa. Nel caso specifico la Georgia non fa parte del network bancario internazionale e quindi risponde dopo diversi giorni, ed è plausibile che siano state scelte proprio per questo motivo delle Banche georgiane.

Da questa informazione parte dall'Italia una rogatoria internazionale destinata alla Georgia, che di norma, tranne accordi specifici, va redatta nella lingua del paese di destinazione, in questo caso in georgiano, ma la Procura riscontrando enormi difficoltà nel trovare un traduttore si accorda con la Georgia per inviarla in lingua inglese. La Georgia risponde alla rogatoria in tempi abbastanza celeri, in tre mesi circa, ma invia alla Procura di Torino un fascicolo in Georgiano. Né da contatti con il Consolato e Ambasciata georgiani in Italia, né da richieste alle Università di Lingue, la Procura riesce a trovare un traduttore affidabile. Fortunatamente l'azienda piemontese era in contatto con un ragazzo che traduceva per loro le etichette dei prodotti destinati in Georgia e che riesce a tradurre la rogatoria dalla quale emerge che i conti correnti di destinazione sono intestati a tre uomini di colore di cui vengono allegati i documenti. La Georgia, in questo caso, è stata abbastanza celere nel rispondere alla rogatoria in quanto era già in atto una importante indagine su un'azione di riciclaggio di denaro sul loro territorio che confermava il rapido transito del denaro sui conti in questione. I documenti identificano i tre sospettati come di nazionalità sudafricana, inglese e guineana. Viene quindi richiesta da parte della Procura di Torino conferma alle autorità competenti da cui si riceve ad oggi risposta solo dall'Inghilterra, che afferma che il passaporto è falso, dalle altre due nazioni non si ha ancora risposta. Se la Procura non dovesse ricevere risposta dalla Guinea e dal Sudafrica, o se dovessero anche loro rispondere che i documenti in questione sono falsi, il procedimento si fermerebbe qui e si avrebbe una archiviazione contro ignoti.

È da notare in questo particolare caso che le aziende clienti hanno ricevuto non solo una e-mail con la stessa intestazione e riferimenti della ditta piemontese, ma che le fatture riportavano anche l'esatto importo che esse dovevano pagare, ciò significa che l'azienda italiana in questione aveva subito una violazione nei loro sistemi. Di questa intrusione l'azienda non aveva avuto evidenza e nulla è emerso in successivi controlli. L'azienda pare che, per non perdere o rovinare i rapporti commerciali con le aziende clienti in Asia, abbia raggiunto degli accordi per dividere in qualche modo le perdite subite.

Il dott. Riccaboni riporta, purtroppo, che casi come questo di frode informatica e violazione dei dati sensibili sono, in questi anni, in aumento. I cyber criminali si stano specializzando sempre di più in questo tipo di frode contro la quale purtroppo si può fare ben poco.

Gli unici casi per i quali è forse più probabile arrivare ad un risultato a livello investigativo riguardano i reati sulla manomissione degli ATM per la clonazione delle carte. Questo tipo di reato necessita della presenza fisica del criminale presso l'ATM e quindi attraverso telecamere, impronte o altro si riesce in molti casi ad arrivare ai criminali.

Recentemente la Procura di Torino ha ricevuto il caso riguardante un'azienda del settore chimico, molto simile a quello sopra esposto, con la differenza che la violazione iniziale è presumibilmente avvenuta ai danni dell'azienda cliente sita in India, che aveva ricevuto una e-mail di spear phishing riportante il cambio IBAN. I bonifici, per una cifra complessiva di 40.000 euro sono stati accreditati su un conto presso una Banca di Torino intestato ad un cittadino nigeriano.

Le perquisizioni e gli accertamenti svolti sui PC del sospettato hanno avuto esito negativo. Attraverso la collaborazione di Google e Yahoo, gestori dei servizi e-mail che il criminale ha usato per creare i falsi indirizzi, si è scoperto che le e-mail erano state inviate da dispositivo mobile. Le indagini sono tuttora in corso.

È evidente che il fenomeno del cyber crime costituisca un rischio da non sottovalutare per le PMI. È di questo parere anche Domenico Raguseo, Europe Security Systems Technical sales and Solution Manager di IBM, per il quale essere vittima di frodi "*non è una peculiarità delle grosse aziende per le quali un danno d'immagine può costituire sicuramente un danno maggiore rispetto alla PMI in termini assoluti, ma per una Piccola e Media Impresa un attacco di cyber crime può spesso minare la vita stessa dell'azienda. Prevenire, identificare e rispondere agli attacchi diventa*", per Raguseo, "*un bene intrinseco per le PMI, importanti quanto l'ossigeno per un essere umano. Prevenire è la fase più importante. Infatti gli attacchi sono sempre più sofisticati e con una durata sempre più lunga*." Diventa vitale anche saper identificare gli attacchi in quanto questi "*sono spesso disegnati e costruiti su misura di colui che si vuole attaccare".* Gli attaccanti hanno un enorme vantaggio perché conoscono bene la loro vittima e la tecnologia che usa, mentre chi si difende si deve difendere da tutto. Infine, "*non si può considerare l'attacco remoto, e limitare gli impatti e contenere eventuali attacchi è pertanto importante e possibile".*

CAPITOLO 4

FOCUS SULLA PROVINCIA DI LUCCA

4.1 Caratteristiche del territorio e delle PMI della Provincia di Lucca

Al fine di realizzare un focus che desse non solo degli indicatori del fenomeno cyber crime preso in questione, ma che potesse anche fornire informazioni di tipo qualitativo, utili a comprendere quali aspetti dell'*asset* aziendale siano minacciati di più dal cyber crime, quali siano le azioni messe in atto per prevenire eventuali danni e che livello di consapevolezza si sia acquisito in questi ultimi anni rispetto questo fenomeno, si è scelto di condurre una serie di interviste semistrutturate, non solo presso aziende rappresentative della zona presa in considerazione, ma anche con attori istituzionali coinvolti e Forze dell'Ordine preposte a combattere la criminalità di tipo informatico.

Esaminiamo ora qualche dato per comprendere meglio le caratteristiche del territorio. La provincia di Lucca è la terza più popolosa del territorio toscano con 372.244 abitanti[195] e conta 38.584 imprese attive sul territorio. Gli addetti per classe dimensionale nelle imprese sono suddivisi per il 57,1% in dipendenti di micro imprese (meno di 10 dipendenti), per il 23,4% in lavoratori nelle piccole imprese (tra i 10 e 49 dipendenti), per il 13,2% in addetti di medie imprese

[195] Popolazione presente nella Provincia di Lucca al Censimento 2001 - dato per Comune. *Elaborazioni Provincia di Lucca su dati ISTAT,* in <http://www.provincia.lucca.it/economia_occupazione/popolazione.php> (ultima consultazione 11-11-2014).

e per il 6,3% in dipendenti di imprese con più di 250 dipendenti. Il 93,7% degli addetti della Provincia di Lucca quindi risulta lavorare in Piccole, Medie e Micro Imprese[196].

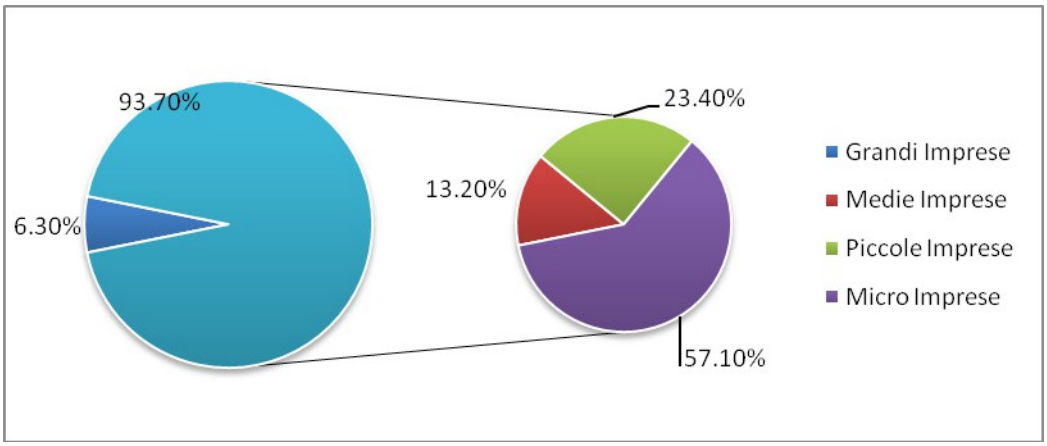


Figura 24 - Addetti per classe dimensionale anno 2011

Fonte: L'Italia delle Province, Servizio Studi e Ricerche Industry and Banking di Intesa Sanpaolo, 2014

La percentuale sopra riportata è leggermente maggiore dei dati nazionali, e rappresenta la realtà tipica del territorio del centro Italia. Dalle statistiche forniteci dal Servizio Studi e Ricerche Industry and Banking di Intesa Sanpaolo risulta che il valore economico delle esportazioni delle aziende della Provincia di Lucca sia il doppio delle importazioni e che il settore con la maggior percentuale di beni esportati è quello della carta[197] con il 23,9%, seguito da meccanica, altri mezzi di trasporto, cuoio e calzature, rispettivamente con il 17,2%, 13,7% e 9,1%. Il settore cartario e cartotecnico del distretto lucchese rappresenta quindi una realtà importante sul territorio, che comprende più di 100 aziende che hanno un fatturato pari a quasi 3.500 milioni di euro e più di 6.500 dipendenti, che arrivano a oltre 14.000 se consideriamo l'indotto. Il distretto detiene il controllo di circa l'80% della produzione nazionale di carta *tissue*, che rappresenta il 17% del dato europeo. Più dell'80% dell'esportazione di questo distretto è destinato ai mercati europei, mentre per il settore meccanico i dati sono più omogenei, 38,7% in Europa, 28,2% in America del nord e America del sud e 33% nel resto del Mondo.

Come si evince da questi dati, la Provincia di Lucca, rispetta in pieno la composizione tipica dell'*asset* industriale del nostro centro Italia. L'ampia presenza di Micro, Piccole e Medie Imprese ad alto know-how e l'elevato livello dei rapporti commerciali con l'estero rendono quindi questa zona appetibile per i criminali informatici.

4.2 Dati Consorzio Bancomat

[196] *L'Italia delle Province. Lucca Settembre 2014,* fornito per questa ricerca dal Servizio Studi e Ricerche Industry and Banking di Intesa Sanpaolo.

[197] Ritorna a crescere l'export del cartario di Capannori (+2,5% risultato del terzo trimestre 2013), *Monitor dei Distretti Toscana Trimestrale – n. 15 Intesa Sanpaolo gennaio 2014 Servizio Studi e Ricerche Industry and Banking* a cura di: Stefania Trenti, in <http://www.group.intesasanpaolo.com/scriptIsir0/si09/contentData/view/content-ref?id=CNT-04-00000001B77B2> (ultima consultazione 12-11-2014).

Il cyber crime risulta essere per il Consorzio Bancomat un rischio un po' borderline in quanto loro hanno notizia solo degli attacchi sulle apparecchiature ATM. Avendo l'apparecchiatura una connessione IP agganciata direttamente alla rete della Banca, l'attacco è volto non tanto alla cattura o all'interferenza dei dati della transazione, ma probabilmente più ad andare ad infettare la rete della Banca.

Il Consorzio registra gli attacchi e collabora con le Forze dell'Ordine e partecipa ai vari gruppi e sottogruppi tecnici per la realizzazione del Sistema informatizzato di prevenzione amministrativa delle frodi sulle carte di pagamento (Sipaf), ed è *National Member nell'European ATM Security Team* (EAST), un consorzio internazionale per la gestione degli ATM. All'interno del Consorzio Bancomat vi è un centro antifrode che effettua controlli su tutta la rete degli *stakeholder* e degli *shareholder*. Questo centro ha dei presidi stabili di monitoraggio puntuale delle frodi, quindi tutte le Banche e tutti i *service* segnalano attraverso delle applicazioni in tempo reale le eventuali manomissioni o gli eventuali tentativi di qualsiasi tipologia di frode che poi vengono caricate nei SIPAF.

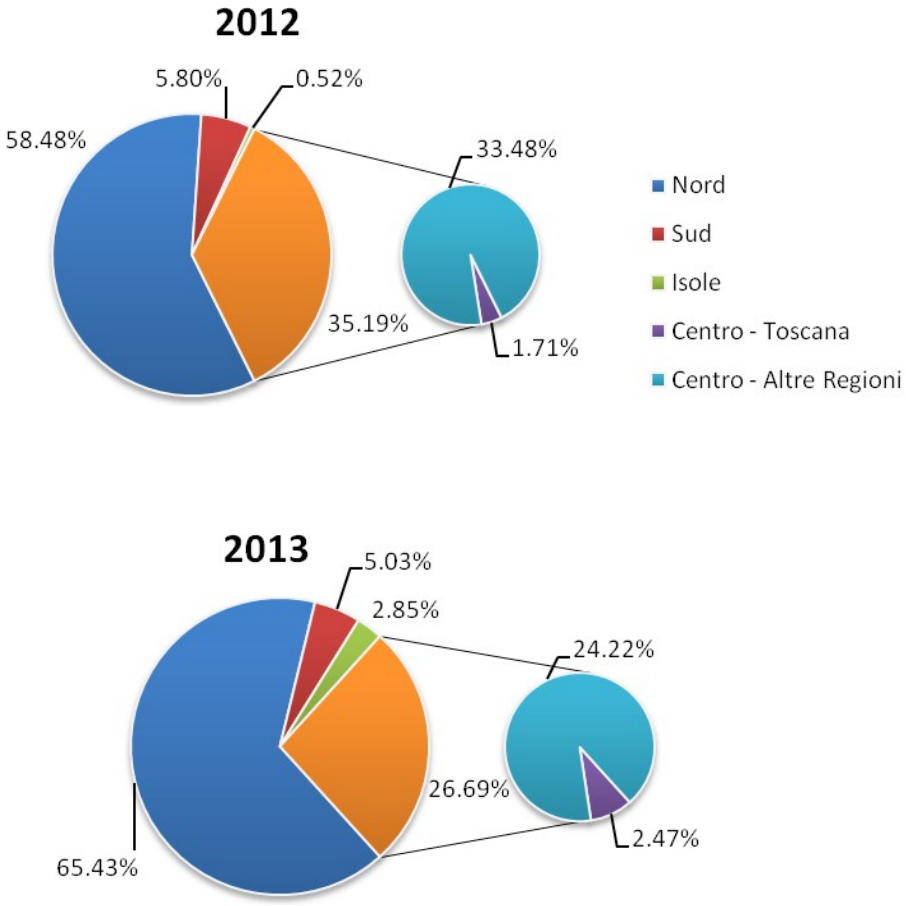


Figura 25 - Distribuzione percentuale delle manomissioni per aree geografiche
Fonte: Statistiche attacchi fraudolenti, Centro Antifrode Consorzio BANCOMAT

Essendo un circuito domestico abilitato a transitare solamente all'interno dei confini italiani il Consorzio Bancomat è solo marginalmente toccato dalla transnazionalità del cyber crime, nel

senso che la spendibilità delle carte può avvenire solo in Italia. Però le carte Bancomat condividono spesso lo stesso supporto con altri circuiti, tipo Visa, MasterCard ecc, quindi, una volta che lo strumento è compromesso c'è una perdita anche nel loro circuito.

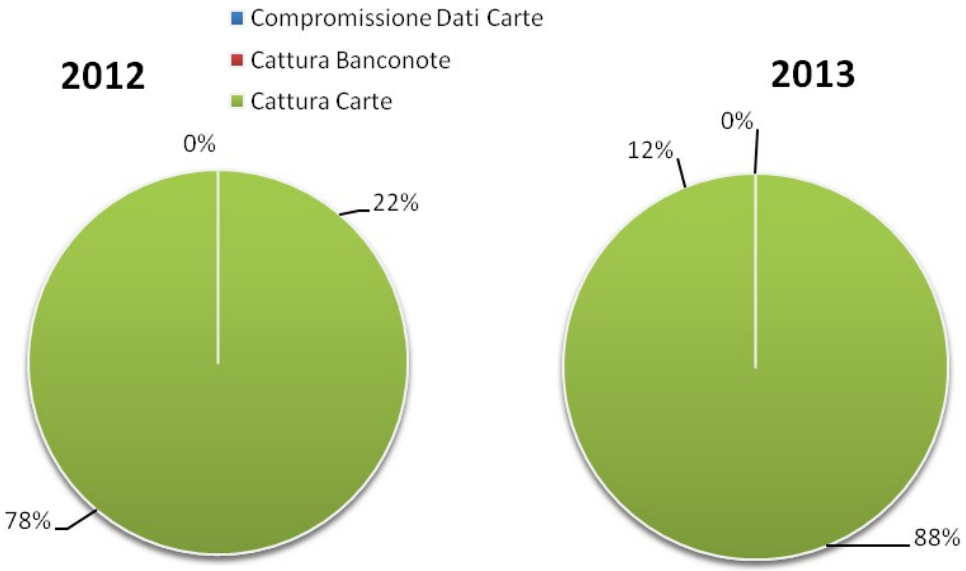


Figura 26 - Composizione degli attacchi nella Regione Toscana
Fonte: Statistiche attacchi fraudolenti, Centro Antifrode Consorzio BANCOMAT

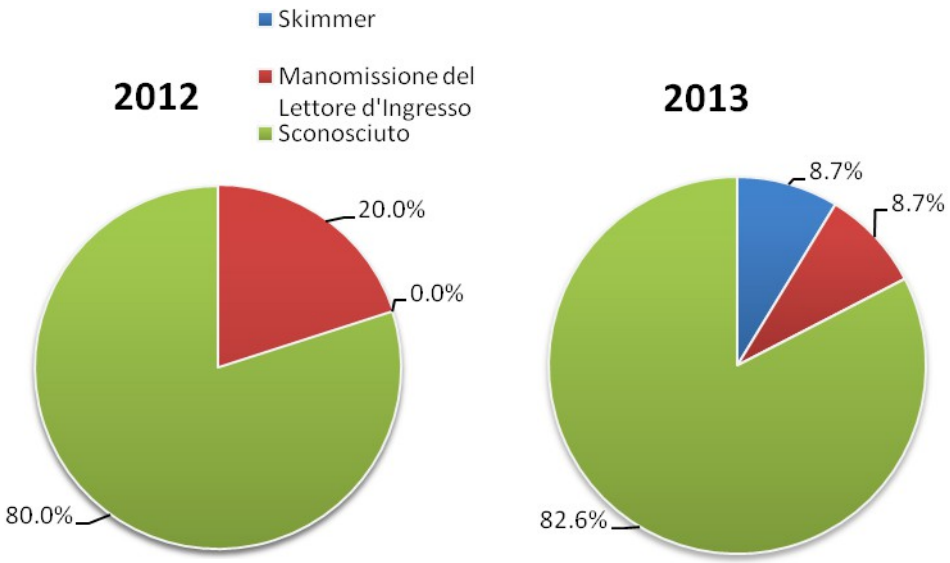


Figura 27 - Tipologia di manomissione, compromissione dei dati delle carte
Fonte: Statistiche attacchi fraudolenti, Centro Antifrode Consorzio BANCOMAT

In questo momento il circuito è sufficientemente tutelato dalla normativa attuale. il problema sorge per le transazioni definite *card not present*, quindi le transazioni fatte attraverso canale internet oppure *web like*, per le quali manca ancora tutto il supporto legale, la materia non è ancora chiara e ci sono dei gap che vanno assolutamente colmati.

4.3 Analisi delle interviste realizzate nel territorio della Provincia di Lucca

4.3.1 Intervista a rappresentanti delle Forze dell'Ordine

Per valutare l'entità del fenomeno cyber crime nella Provincia di Lucca si è scelto di condurre interviste mirate a due esponenti delle Forze dell'Ordine in Toscana, l'Ispettore Capo Franco Bozzi della Polizia di Stato presso la Procura della Repubblica presso il Tribunale di Lucca e il Vice Questore Aggiunto Stefania Pierazzi[198] della Polizia Postale e delle Telecomunicazioni di Firenze.

Come già esposto nel capitolo precedente, dal 2008, in seguito alla Ratifica della Convenzione di Budapest, tutti i reati di tipo informatico vengono seguiti a livello distrettuale[199], quindi in Toscana[200] dalla Procura di Firenze, dove confluiscono le denunce raccolte da tutte le Forze dell'Ordine, pur essendo la Polizia Postale la struttura più specializzata ad indagare su questo tipo di reato. Proprio per questo motivo si è deciso di condurre la prima intervista con la dott.ssa Pierazzi, al fine di capire il trend registrato in questi ultimi anni a livello investigativo sul territorio relativo a questo fenomeno. La dott.ssa Pierazzi ha dichiarato che i reati informatici sono in costante aumento, registrando una vera e propria escalation, nello specifico quello che in questi ultimi tre, quattro anni ha avuto un vero e proprio picco è stato il phishing, anche nella variante spear phishing, considerato non come un reato a sé stante, ma concomitante, per esempio, ad un accesso abusivo ad un sistema informatico con lo scopo di carpire dati e credenziali bancarie di un singolo o di una società di qualsiasi dimensione e di utilizzarli per fare transazioni. "*Questo trend non accenna a scendere, continua a svilupparsi in maniera costante nel tempo"* ha affermato la dott. Pierazzi.

Parallelamente all'aumento degli attacchi di tipo informatico è aumentata anche la propensione a rivolgersi alle autorità competenti. La dott.ssa Pierazzi, che si occupa di questo fenomeno da 15 anni, ha potuto notare, a tal proposito, una vera e propria evoluzione: "*I primi anni c'era molto pudore a denunciare questo tipo di reato […] poi con il tempo è diventato un reato sempre più comune e si sono resi conto che il fatto di aver subito un attacco non sminuisce la propria immagine, non fa venire meno la credibilità di un soggetto, o di una società. E allora, si sono manifestati di più ed oggi anche le grosse società denunciano questo tipo di reato. Di sicuro più di quanto succedesse in passato.*"

Una decina di anni fa infatti, la Polizia Postale venne a conoscenza di un attacco indirizzato a Google, che coinvolse diverse aziende fiorentine, dalla denuncia di un'unica piccola azienda di

[198] L'intervista integrale alla dott.ssa Pierazzi è allegata in appendice metodologica.

[199] Articolo 11, legge n° 48/2008 pubblicata nella *Gazzetta Ufficiale* n. 80 del 4 aprile 2008 - Supplemento ordinario n. 79, in <http://www.parlamento.it/parlam/leggi/08048l.htm> (ultima consultazione 10-11-2014).

[200] A livello distrettuale a Firenze si gestiscono le denunce di tutte le province della Toscana eccetto Massa-Carrara che è compresa nel distretto di Genova.

Prato, attraverso la quale si poté ricostruire l'entità dell'attacco e scoprire che erano state coinvolte molte altre aziende, anche di grosse dimensioni. Da quattro o cinque anni invece, si registra questa inversione di tendenza e, anche grazie al fatto che si incomincia a parlare di più di questo tipo di criminalità, le aziende stanno comprendendo che è un fenomeno appannaggio di tanti e questo dimostra anche, secondo quanto riportato nell'intervista, un buon livello di fiducia nei confronti delle Forze dell'Ordine da parte delle vittime. Il Vice Questore dichiara di aver trovato raramente chiusure nei loro confronti e che le vittime collaborano volentieri, accettando consigli, consulenze e fornendo liberamente i loro dati.[201]

A questo proposito, purtroppo, è necessario considerare anche che è vero che l'utente si affida più facilmente alle Forze dell'Ordine, ma purtroppo non si rende ancora conto delle problematiche relative alle investigazioni e all'azione penale riguardanti questo tipo di fenomeno, pensando di risolvere velocemente il danno subito in casi di frode come per esempio da piattaforme e-bay, subito.it ed altre similari, come emerge dall'intervista con l'Ispettore Bozzi. Anche la dott.ssa Pierazzi a tal proposito conferma questo dato e afferma che è molto difficile individuare chi ha realizzato l'attacco perché "*di norma i criminali sono molto preparati, quindi usano sistemi che permettono loro di non essere individuarti, basta usare un proxy e già si rendono irrintracciabili, o per lo meno sembra che l'acquisizione sia stata fatta usando un server che è all'estero e l'attività non dico che si ferma, ma quasi*."

Come già illustrato nei capitoli precedenti, il carattere internazionale del cyber crime rende più difficoltoso condurre le indagini. Spesso infatti gli attacchi provengono da Paesi non appartenenti alla Comunità europea, con i quali non ci sono rapporti di reciprocità e non sempre viene attivata una rogatoria internazionale, e, quando invece questo accade, i tempi sono comunque troppo lunghi rispetto alla volatilità dei dati che servono per compiere l'attività investigativa. Riguardo ciò la dott.ssa Pierazzi confida "*La velocità è fondamentale in questo tipo di reati. È difficilissimo. Se ci si muove subito è possibile fare qualcosa, altrimenti no."* Anche se a livello investigativo è presente la collaborazione internazionale bisogna poi considerare che per creare un fascicolo processuale a tutti gli effetti bisogna seguire delle procedure standard, come la rogatoria internazionale, che sono più farraginose ed allungano i tempi delle indagini.

Purtroppo i danni derivanti da questo tipo di attacchi non sono da sottovalutare. I casi raccolti dalla Polizia Postale di Firenze spaziano da phishing e spear phishing, dove il danno è puramente economico, alla sottrazione di dati, brevetti e pacchetti clienti, che costituiscono un danno quantificabile solo in un secondo momento. I dati ufficiali, forniti dal Compartimento della Polizia Postale di Firenze[202], relativi all'anno in corso, sono già di 711 denunce ricevute per truffa, 231 per accesso abusivo e 92 per frode informatica.

Dai dati forniti per questa ricerca dalla Cancelleria della Procura della Repubblica di Firenze, relativi ai casi pervenuti negli ultimi tre anni, non solo dalla Polizia Postale, ma anche dalle altre

[201] Dato confermato anche dal: *Cyber security Report* Special Eurobarometer 404, 2013, European Commission, pag.77, in <http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf> (ultima consultazione 6-11-2014).

[202] Si consideri che i casi denunciati alla Polizia Postale sono solo una parte di quelli realmente denunciati, perché molti possono essere presentati, ed a volte gestiti, anche da altre Forze di Polizia.

Forze dell'Ordine, come ad esempio Carabinieri e Guardia di Finanza, secondo gli Articoli 615 Ter cp[203], 615 Quater cp[204], 640 cp[205] e 640 Ter cp[206] emergono diversi aspetti interessanti.

PROCURA DELLA REPUBBLICA DI FIRENZE

Procedimenti Sopravvenuti	Anno Iscrizione 2012	2013	2014 (fino al 27/10/2014)	Totale complessivo
Noti Mod. 21	**1.723**	**1.817**	**2.404**	**5.944**
Art. 615 Quater cp	19	30	46	95
Art. 615 Ter cp	246	339	574	1.159
Art. 640 cp	1.233	1.144	1.258	3.635
Art. 640 Ter cp	225	304	526	1.055
Ignoti Mod. 44	**2.963**	**4.176**	**6.714**	**13.853**
Art. 615 Quater cp	50	47	41	138
Art. 615 Ter cp	991	1.701	2.940	5.632
Art. 640 cp	938	864	1.127	2.929
Art. 640 Ter cp	984	1.564	2.606	5.154
Totale complessivo	**4.686**	**5.993**	**9.118**	**19.797**

Tabella 6 - Procedimenti sopravvenuti contro noti ed ignoti secondo Artt. 615 Ter, 615 Quater, 640 e 640 Ter
Fonte: Dati forniti dalla Procura della Repubblica di Firenze, anni 2012, 2013 e 2014

PROCURA DELLA REPUBBLICA DI FIRENZE

[203] Art. 615 ter codice penale. Reato di accesso abusivo ad un sistema informatico o telematico "*Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni".*

[204] Art. 615 quater codice penale *"Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a un anno e con la multa sino a cinquemilacentosessantaquattro euro".*

[205] Art. 640 codice penale. Reato di frode "*Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da cinquantuno euro a milletrentadue euro*".

[206] Art. 640 ter codice penale. Reato di frode informatica "*Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032".*

Procedimenti	Anno Definizione				
Definiti	**2012**	**2013**	**2014**	**Pendenti al 27/10/2014**	**Totale complessivo**
Ignoti Mod. 44	**2.563**	**3.696**	**4.317**		**10.576**
Art. 615 Quater cp	28	64	36		128
Art. 615 Ter cp	715	1.457	1.758		3.930
Art. 640 cp	938	847	848		2.633
Art. 640 Ter cp	882	1.328	1.675		3.885
Noti Mod. 21	**1.532**	**1.930**	**2.051**	**131**	**5.644**
Art. 615 Quater cp	10	14	41	2	67
Art. 615 Ter cp	195	351	456	5	1.007
Art. 640 cp	1.129	1.223	1.099	124	3.575
Art. 640 Ter cp	198	342	455		995
Totale complessivo	**4.095**	**5.626**	**6.368**	**131**	**16.220**

Tabella 7 - Procedimenti definiti contro noti ed ignoti secondo Artt. 615 Ter, 615 Quater, 640 e 640 Ter
Fonte: Dati forniti dalla Procura della Repubblica di Firenze, anni 2012, 2013 e 2014

Dal 2012 ad oggi, come si può notare, i reati per frode informatica (Art. 640 Ter cp) sono passati dal costituire un terzo della totalità dei reati per frode, a costituirne oggi più della metà. Un altro dato osservabile è che, negli ultimi tre anni, mentre i reati per frode (Art. 640 cp) sono più o meno costanti, o registrano un lieve aumento, quelli relativi alla frode informatica invece registrano un notevole aumento. Soprattutto quelli contro ignoti, che sono arrivati a ben 2.606 casi. Questo divario enorme tra i procedimenti per frode informatica verso ignoti e quelli verso noti è sintomatico di questo tipo di criminalità, per la quale è difficilissimo risalire all'autore del reato. Questi dati, ovviamente, si riferiscono ai reati per cui è stata sporta una denuncia, e non considerano tutto il sommerso che riguarda casi che non sono stati denunciati o di cui la vittima non si è accorta. Per avere un quadro statisticamente più vicino alla realtà sarebbe opportuno, per questa tipologia di reato, realizzare delle indagini di vittimizzazione in ambito aziendale.

Per quanto riguarda le aziende, un altro elemento emerso dalle interviste, che rende difficile anche solo accorgersi di aver subito un reato di tipo informatico, è costituito dal fatto che i cyber criminali commisurano la cifra sottratta alla parte offesa, rendendo la movimentazione plausibile, tra le solite movimentazioni, e quindi non facilmente rilevata come transazione anomala dalle Banche o dalle aziende stesse. Gli importi sottratti infatti risultano adeguati al volume d'affari dell'azienda. Di norma dalle 30 alle 70 mila euro per una grossa società, ed anche solo da 500 euro in su per una PMI. Sono attacchi di cifre modeste, magari ripetuti nel tempo, giocando su falsi ordini, false fatture o modifica delle anagrafiche bancarie.

Un dato interessante, emerso sia dall'intervista con la dott.ssa Pierazzi, sia da quella con l'Ispettore Bozzi, riguarda la differenziazione della tipologia di attaccante per i reati puramente economici, come il phishing e la frode, e quelli inerenti le violazioni allo scopo di sottrarre dati riservati. Infatti, nella quasi totalità dei casi, la prima tipologia riguarda attacchi esterni all'azienda, mentre la seconda, il più delle volte, coinvolge persone interne all'azienda, dipendenti infedeli o ex dipendenti risentiti che rubano dati semplicemente per creare un danno o per rivendere queste informazioni a criminali esterni o mettersi in proprio, sottraendo know-how, pacchetti clienti,

progetti e brevetti. Tra questi ultimi la dott.ssa Pierazzi menziona un caso avvenuto anni prima nel quale ex dipendenti di un'azienda farmaceutica toscana sottrassero la ricetta di un farmaco non ancora brevettato costituendo un'altra società.

È evidente come entrambe le tipologie di rischi siano considerevoli per una PMI, per la quale una frode economica può sicuramente costituire un danno importante, soprattutto in questo periodo di crisi economica, e per le quali, basando il loro business molto spesso su brevetti, eccellenze, utilizzo esclusivo di un marchio e contatti commerciali specifici, una violazione di questi dati potrebbe mettere in serio pericolo la sopravvivenza dell'azienda stessa.

Purtroppo però la consapevolezza e la preparazione delle PMI è ancora molto bassa. Oggi sono le aziende più soggette al rischio e, soprattutto le micro e piccole imprese, spesso hanno PC obsoleti o non aggiornati a livello di hardware e software, pochi, se non addirittura nessun tecnico informatico preposto alla sicurezza, PC collegati ad internet con modem sempre connessi senza sistemi antivirus e firewall, o non aggiornati o non correttamente configurati.

La sicurezza informatica rappresenta di sicuro un grosso investimento economico per le PMI, dal punto di vista tecnico e di strumenti di protezione, ma dall'altra parte richiede anche l'attivazione di policy di sicurezza aziendale, effettuabili a basso costo o addirittura gratuite. *"Il più delle volte aspettano di subire il danno per poi correre ai ripari,"* afferma la dott.ssa Pierazzi, "*certe volte però ci sarebbero cose davvero così banali, tipo la variazione della password. Per esempio, se va via un dipendente, che magari gestiva l'amministrazione, sarebbe il minino cambiare subito le password e disattivare il suo account, ed invece non si fa nulla per mesi. A volte ci sono cose che non costerebbero nulla, basterebbe forse investire in una figura professionale che si occupi di queste cose, e raramente, se non nelle grandi aziende, si è strutturati in modo da avere ciò*". Un caso interessante, riferito dall'Ispettore Bozzi durante l'intervista rilasciata per questa ricerca, conferma quanto detto. Riguarda una PMI della zona di Lucca, che ha subito un attacco a causa di un malware di tipo ransomware contro i propri sistemi, attraverso il quale sono stati criptati gli archivi gestionali e chiesto un riscatto di circa 1.000 euro dai cyber criminali[207]. L'azienda in questione non aveva ovviamente un adeguato sistema di sicurezza ed in più effettuava backup non frequenti e peraltro sullo stesso hard disk. Data la difficoltà di poter avviare un'azione investigativa e penale che desse dei risultati certi, l'azienda ha scelto di cedere al ricatto e pagare[208]. Il consulente informatico dell'azienda in questione cerca di mettere in pratica qualche tipo di soluzione per il futuro, ma, prima che vengano attuate le nuove metodologie di sicurezza, l'azienda rimane vittima dello stesso tipo di reato, verosimilmente da parte degli stessi criminali, che richiedono questa volta una somma inferiore.

Si evince da questo caso innanzitutto la furbizia dei cyber criminali nel misurare la richiesta economica in modo tale da rende più conveniente pagare piuttosto che denunciare l'accaduto alle autorità competenti. Inoltre, data la facilità di azione, è plausibile che sia proficuo per il cyber criminale anche richiedere un importo basso, ma per più aziende, avendo questo tipo di attacchi un ROI molto alto. Altro fattore sconcertante di questa vicenda è che nonostante l'azienda avesse

[207] Che in questo caso specifico erano di nazionalità russa, territorio con in quale non c'è un'alta collaborazione per quanto attiene i reati di natura informatica.

[208] Tra l'altro l'azienda in questo caso ottiene, a seguito del pagamento del "riscatto", la decriptazione dei dati da parte dei criminali. Cosa che non sempre avviene.

già subito questo attacco, la capacità di mettere in atto procedure e sistemi di sicurezza per evitare di subirne un altro è stata praticamente nulla. Il livello di conoscenza e consapevolezza è ancora così basso che non riesce a portare neanche alla definizione delle più basilari azioni di prevenzione. Nei confronti del secondo attacco però l'azienda, avendo effettuato almeno il backup settimanale, ha deciso di non pagare più ed ha accettato di aver comunque perso i dati relativi agli ultimi giorni dopo l'ultimo backup.

Il fenomeno del cyber crime, ad ogni modo, è molto trasversale, come ci riferisce la dott.ssa Pierazzi; in base alle denunce, segnalazioni o deleghe che ricevono, non colpisce un tipo particolare di azienda ma è un fenomeno indiscriminato che colpisce qualsiasi società, non solo quelle del settore informatico o che producono beni altamente specializzati. Ormai anche le più piccole aziende hanno informatizzato almeno la gestione economica aziendale, spesso non considerando i rischi che possono correre a livello informatico. "*Qualche volta sembra davvero che non abbiano la percezione di quanto possano essere vulnerabili i loro sistemi*" è quanto riporta la dott.ssa Pierazzi "*qualche volta invece sono un po' più consapevoli ma aspettano comunque di subire un danno prima di mettere in atto delle contromisure."* Dalle interviste emerge, inoltre, che non esiste alcun tipo di condivisione delle informazioni tre le aziende in questo ambito. In occasione di seminari sull'uso del POS organizzati dalla Confcommercio di Firenze alcuni anni fa, la dott.ssa Pierazzi ci ha confessato di aver avuto la possibilità di constatare che i commercianti e le PMI erano davvero poco informati a riguardo e completamente vulnerabili.

Entrambi gli intervistati, alla domanda inerente il tipo di strumenti ritenuti più utili al contrasto di questo tipo di fenomeno, hanno sottolineato l'importanza strategica dell'aspetto culturale e del valore della formazione. Rappresentativo a tal proposito è quanto dichiarato dalla dott.ssa Pierazzi su cosa sia più utile alle PMI per difendersi da questa minaccia: "*La conoscenza umana. Assolutamente. Anche perché molto si basa sul social engineering. Uomo contro uomo. È vero che c'è una macchina di mezzo, ma c'è un uomo davanti a quella macchina. Io penso che sia fondamentale la preparazione dell'utente, del cliente, del dipendente. In primis la consapevolezza dei rischi che si corrono. Poi preparare anche l'ultimo dei propri dipendenti a fronteggiare determinati rischi, per non fare sciocchezze, come l'accesso a siti che possono essere dannosi, possono installare dei virus, una sorta di consapevolezza ed educazione del mezzo informatico, perché c'è la presunzione che questo mezzo sia facilmente gestibile. È fuorviante, perché ti dà la possibilità di fare tutto subito. Il sistema informatico è grandioso, veramente, ti permette di fare delle cose stupefacenti, io credo che sia davvero una cosa stupenda, però devi anche approcciarti con un po' di malizia e non affidarti ad occhi chiusi."*

4.3.2 Interviste presso le aziende

Parte fondamentale di questa ricerca è stato individuare delle aziende rappresentative del territorio lucchese, per condurre delle interviste che dessero gli strumenti necessari per comprendere lo stato attuale delle PMI nei confronti della sicurezza informatica, la consapevolezza riguardo il cyber crime e ciò di cui hanno bisogno per mitigare i rischi derivanti da esso. Date le caratteristiche della Provincia si è scelto di intervistare un'azienda ad alto know-how nell'ambito

dei macchinari per la lavorazione del marmo, due cartiere del distretto più importante della zona e due aziende dell'ambito IT.

La Giorgini Maggi è la più antica[209] azienda specializzata nella costruzione di macchine per la lavorazione del marmo, della pietra e del granito. Composta da circa 10 dipendenti e con circa 5 postazioni PC fisse, da sempre ha rapporti diretti con i propri clienti distribuiti in ogni parte del Mondo. L'azienda riceve, come un po' tutte le attività commerciali, numerose e-mail di spam, nell'ordine di una cinquantina al giorno e si affida ad una società esterna locale che fornisce loro il servizio e-mail e gestione del sito. Durante l'intervista è emerso un dato importantissimo riguardante un'esperienza di frode indirettamente subita. A giugno di quest'anno infatti la Giorgini Maggi aspettava un bonifico da un cliente greco, in genere molto puntuale, che quindi ricontatta per accertarsi che non ci siano problemi e scopre che in realtà il cliente aveva già effettuato il bonifico utilizzando però un IBAN diverso, ricevuto tramite e-mail dall'azienda toscana. L'e-mail in questione era stata realizzata molto bene, scritta in inglese corretto, con i riferimenti, grafica, colori e logo dell'azienda e comunicava il cambio di IBAN per le future fatturazioni. L'importo sottratto dai cyber criminali si aggirava intorno ai 4.000 euro, e fortunatamente il cliente, legato da un rapporto commerciale di lunga data, non ha interrotto i rapporti con l'azienda intervistata. Nello specifico non sappiamo se la violazione iniziale che ha permesso questa frode sia stata subita dall'azienda intervistata o dall'azienda greca, ad ogni modo un attacco di questo tipo può, oltre che causare un danno economico, minare anche il tessuto di rapporti di fiducia tra le PMI. Fortunatamente l'azienda da noi intervistata, da sempre, conserva i dati sensibili e i brevetti dei macchinari che producono su un computer separato dalla rete interna e senza accesso ad internet. Dall'evento di giugno, prima del quale la titolare non avrebbe mai pensato di poter essere vittima di un attacco di questo tipo, la Giorgini Maggi ha avviato una policy di cambio password alfanumeriche ogni 15 giorni, e vorrebbe fare ancora di più per la propria sicurezza informatica, ma lamenta di non ha ricevuto molto sostegno e informazioni a riguardo, soprattutto dalla società che gestisce loro le e-mail.

Questo tipo di frode, come abbiamo già visto dal caso studio illustrato nel capitolo precedente, è molto diffusa in questo periodo, ed è un tipo di attacco mirato più difficilmente riconoscibile rispetto al classico phishing (scritto in modo non corretto e abbastanza semplice da riconoscere). Questo tipo di frode è costruita solitamente molto bene, reca il nome del cliente o fornitore, relativo logo e dati di fatturazione e viene inviata ad un indirizzo e-mail ritenuto affidabile, quindi, senza un preciso controllo sul nuovo IBAN indicato o un accertamento telefonico dell'avvenuto cambio di conto, è facile che le aziende caschino nella trappola dei cyber criminali. È quanto mai importante aver rilevato questo evento tra le interviste svolte perché testimonia come questo tipo di criminalità non è affatto lontana dalla realtà delle micro imprese che compongono il tessuto economico del nostro territorio.

Successivamente sono state realizzate delle interviste presso due cartiere della zona, aziende di medio grandi dimensioni, anche loro con clienti sia italiani che internazionali. Le aziende

[209] La sua origine, infatti, risale al 1865. L'azienda Giorgini Maggi si trova nella zona dei marmi bianchi della Alpi Apuane famosa perché luogo dove Michelangelo intraprese l'attività di estrazione dei blocchi per la creazione dei suoi capolavori.

in questione, Industria cartaria Pieretti (IcP) e Lucart, sono aziende che affrontano il tema della sicurezza informatica da diversi anni ed hanno un reparto IT interno all'azienda, che si occupa anche della sicurezza informatica. Sono entrambe ben strutturate ed hanno policy di cambio password alfanumeriche obbligatoria ogni tre mesi.

La IcP, azienda con 110 dipendenti e clienti in 60 Paesi nel Mondo, Europa, Medio Oriente, Stati Uniti e Sud America, nel settore della carta sin dal 1924, ha un responsabile IT che si occupa della parte hardware, reti, connessioni, apparecchi, backup, connessioni, configurazioni; un responsabile software per la gestione dei software interni, ERP e vari prodotti, e un esperto in telecomunicazioni che gestisce il marketing. Tutte e tre le figure sono sotto la direzione del dott. Tiziano Pieretti, Amministratore Delegato dell'Azienda, con il quale si è svolta l'intervista. La IcP rappresenta di sicuro un esempio virtuoso nell'ambito della sicurezza informatica in quanto ha approntato un regolamento aziendale sul corretto uso del sistema informatico, congiuntamente ad un *Business Continuity Plan* che periodicamente viene aggiornato e verificato, è conforme alle richieste da parte della normativa riguardo la gestione dei dati personali[210] e ha maturato una sensibilità in materia di sicurezza che si pone anche oltre quelle che sono le normative, adottando policy piuttosto restrittive. Lo stesso dott. Pieretti a tal proposito dichiara che "*forse siamo l'estremo opposto rispetto alla media, noi siamo fin troppo attenti, ma se l'alternativa è l'altra penso sia meglio questa*".

Il danno che più temono è quello che un attacco potrebbe creare ai loro sistemi, come ad esempio fermare la produzione o danneggiare un server ERP che bloccherebbe l'intera azienda per giorni. Perdere un giorno o 12 ore per fare *disaster recovery*, tenere ferme le spedizioni, i trasporti, è un lusso che le aziende non si possono permettere.

La Lucart, azienda di grandi dimensioni[211] e anch'essa ben strutturata, conta tra le 300 e le 350 postazioni informatiche in Italia e almeno altre 200 circa in Francia, gestite tutte dal reparto IT sito vicino Lucca. L'azienda dichiara di aumentare costantemente ogni anno il budget dedicato alla sicurezza informatica, così come di aver ampliato il reparto IT negli ultimi anni. L'ICT Manager ritiene che il loro livello di protezione, per gli standard che si prefigge, sia ad oggi al 60%, però sono fiduciosi di colmare il restante gap in breve tempo. Oltre all'aumento di budget in questi anni sta crescendo anche la loro attenzione riguardo questi temi.

Da entrambe le interviste emerge che le policy di sicurezza un po' più restrittive non sempre vengono comprese e accolte positivamente da tutti i dipendenti. "*Come reazione per le limitazioni all'utilizzo del web registriamo un po' di tutto tra i dipendenti, c'è chi lo auspica, c'è chi ha capito, c'è chi invece borbotta perché non capisce*"ci rivela l'ICT Manager dott. Burresi.

"Ci sono due tipi di aziende" dichiara inoltre il dott. Pasquini durante l'intervista *"quelle che hanno già un certo tipo di cultura e quelle che aspettano di picchiare la testa*".

[210] La gestione dei dati, siano essi personali o sensibili (in funzione della gestione di adempimenti amministrativi del personale) all'interno di Industria cartaria Pieretti SpA viene effettuata seguendo quanto previsto dal Decreto legislativo 30 giugno 2003, n. 196 seguendo gli adempimenti previsti dal disciplinare tecnico in materia di misure minime di sicurezza (allegato B).

[211] Azienda con 1.400 dipendenti e con reparto IT gestito interamente in Italia. Le sedi in Italia sono 5 più due in Francia. L'IT è presente da 20 anni e attualmente è composto da 11-12 persone.

Le ultime due aziende intervistate sono società del settore IT, scelte per avere un parere tecnico relativo alla loro esperienza con altre aziende del territorio e non solo.

La Lucense è una Società Consortile per Azioni *no profit*, costituita a Lucca nel 1984 con la partecipazione di enti pubblici, istituti e fondazioni bancarie ed associazioni di categoria. La sua attività è finalizzata allo sviluppo del sistema economico territoriale, ma nel corso degli anni il mercato di riferimento di Lucense si è progressivamente allargato, fino ad assumere una dimensione nazionale e, per alcune attività, anche internazionale. Dal 2010 Lucense è Organismo di Ricerca e svolge attività di ricerca industriale, sviluppo sperimentale, trasferimento tecnologie e divulgazione. Lucense opera dal 1986 anche come player tecnologico nel settore delle ICT progettando e realizziamo siti e applicativi software per il web, applicazioni per dispositivi mobili e installazioni multimediali, sviluppando e gestendo reti e sistemi informatici. Dal 1995 sono Internet Service Provider con il marchio LUNET e forniscono servizi di hosting, connessioni internet in ponte radio e anche soluzioni di cloud computing. Il sig. Landucci, intervistato per questa ricerca, riferisce che negli ultimi due, tre anni sono in aumento le segnalazioni di e-mail di phishing ai danni delle aziende che hanno il dominio presso Lucense. Attraverso l'intervista è emerso che di recente un'azienda del settore calzaturiero ha rischiato di cadere vittima di spear phishing, in maniera molto simile ai casi studio analizzati nel capitolo precedente, in seguito ad un ordine ad un suo fornitore in Cina. Spesso la Lucense consiglia ai suoi clienti di cambiare periodicamente le password e mettere in atto almeno le policy minime di sicurezza, ma quello che rileva è una profonda difficoltà a livello culturale "*l'attenzione anche verso cose semplici come una password complessa sembra difficile da far entrare nelle abitudini aziendali*" confessa il sig. Landucci. La maggior parte delle volte in cui si verificano casi di DDoS o defacement infatti è perché si è lasciata la password di default "admin". Per questo si è preventivato di impostare per gli applicativi che realizza Lucense un cambio password obbligatorio ogni 90 giorni, mentre per il dominio di posta no perché non era una policy ben tollerata dai clienti. Conservando i dati sensibili di aziende all'interno dei loro server, Lucense ha attuato una policy di sicurezza abbastanza restrittiva prevedendo per esempio piani di backup storicizzati in base alle richieste del cliente su sistemi crittografati. Dall'intervista emerge che è capitato qualche episodio di defacement su alcune pagine di siti da loro ospitati, nulla di mirato con particolari fini, ma riconducibili ad hacker russi e iraniani, con basse capacità e come semplice esercizio di bravura. Ma casi come questi non costituisco per Landucci il vero pericolo per le PMI, che spesso si accorgono di eventuali defacement su loro pagine web anche dopo mesi; il vero pericolo è rappresentato da phishing e spear phishing che rischiano di creare un danno economico. Anche attraverso questa intervista emerge la bassa consapevolezza da parte delle PMI riguardo questo tipo di fenomeno.

Il cliente medio per Lucense, soprattutto in questo periodo di crisi economica, è poco propenso ad investire economicamente in sicurezza e preferisce correre il rischio di subire un danno derivante da un attacco informatico, sottovalutando i pericoli che ne derivano. Non è raro, da quanto riferito dal sig. Landucci, che per esempio studi di architettura non proteggano adeguatamente progetti in corso di realizzazione per bandi e gare d'appalto, "*non considerano quanto costerebbe se il dato venisse perso"*. Alcuni clienti di Lucense inoltre, si lamentano per la lentezza della loro connessione, incolpando il provider di scarse performance, non accorgendosi però che questa lentezza dipende invece da un uso non autorizzato della rete da parte di un

dipendente, che magari durante l'orario di lavoro scarica materiale non affidabile che potrebbe contenere virus che possono infettare i sistemi aziendali.

Alla domanda su cosa potrebbe essere utile per contrastare questo fenomeno, in linea con le altre interviste condotte, il sig. Landucci conferma la necessità di rinnovare seminari che coinvolgano le aziende e le associazioni di categoria, durante le quali affrontare anche gli aspetti pratici, con dimostrazioni ed esempi che illustrino alle aziende come sia relativamente semplice realizzare un attacco informatico. Lucense stessa in questi anni ha organizzato seminari su cloud e *disaster recovery*, con scadenze bimestrali o trimestrali, registrando un'affluenza relativamente bassa. "*Il seminario potrebbe essere una buona occasione per superare l'omertà e il bassissimo livello di condivisione di queste tematiche*" afferma infine il sig. Landucci.

La seconda azienda del settore IT intervistata è Tagetik, fondata nel 1986 e riconosciuta nel mercato delle soluzioni software per il *Corporate Performance Management* (CPM) e la *Business Intelligence* (BI) che negli ultimi anni ha registrato tra i più elevati e rapidi tassi di crescita nel suo settore. La Tagetik ha oltre 600 clienti nel Mondo, la maggior parte all'estero, Europa e oltreoceano, con diverse sedi in Italia, Europa e Stati Uniti. Da 5-6 anni è attivo anche il reparto cloud che ha visto raddoppiare il personale da 3 a 6 unità nell'ultimo anno. Il reparto IT, che si occupa della gestione dei sistemi informatici interni, è invece formato da 4 dipendenti.

Il dott. Santo Natale, responsabile del team cloud e il dott. Matteo Fava, IT manager riportano che le policy di sicurezza sono enormemente cambiate negli anni.

"*All'inizio era un'altra cosa, un'altra situazione. In quegli anni effettivamente infatti mi ricordo un tentativo riuscito, bucarono un server Windows attraverso il quale provarono ad attaccare un'altra azienda che ci chiamò dicendoci che c'era un nostro IP pubblico che tentava di attaccarli. Forse era il 2001.*" (Matteo Fava).

La Tagetik è un'azienda ben strutturata e molto attenta al tema della sicurezza informatica, ha policy di sicurezza interne abbastanza restrittive, che prevedono piani di *business continuity* e *disaster recovery* su server esterni, ed ha in programma di affidarsi ad un secondo servizio cloud per ridondare i dati che detengono. Effettuano attività di *penetration test* e *vulnerability assessment* periodicamente. Inoltre differenziano gli accessi ai dati, per utenti junior e senior oltre che per reparto aziendale. Il timore più grande infatti, come riferito dal dott. Fava, "*è rappresentato dalla possibilità che qualcuno possa entrare nei nostri server dove sono ospitati dati critici dei clienti, come bilanci di grossissime aziende non ancora pubblicati".*

All'interno del servizio cloud, che in questi anni sta riscuotendo un enorme successo commerciale, offrono un pacchetto che comprende il software da loro sviluppato, il server che lo ospita e naturalmente anche la sicurezza. Per questo il problema della sicurezza è fortemente considerato poiché costituisce un problema di business. Se un dato venisse compromesso ne verrebbe compromessa la reputazione dell'azienda. Il reparto cloud è certificato ISO/IEC 27001[212], e vive di policy più stringenti, e anche il resto dell'azienda beneficia di queste policy anche se con meno vincoli.

[212] ISO / IEC 27001 è lo standard più conosciuto della famiglia che fornisce i requisiti per un sistema di gestione della sicurezza delle informazioni (ISMS), in <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm> (ultima consultazione 15-11-2014).

Come tutti gli indirizzi IP pubblici su internet, dichiarano di registrare spesso tentativi di accesso non autorizzato anche se, finora, non hanno avuto evidenza di compromissione di macchine. "*Registriamo una frequenza abbastanza alta di tentativi di intrusione, spam, virus, e sugli IP pubblici abbiamo tentativi di scan molto frequenti, dal banale brute force sugli account FTP ai tentativi di accesso alle nostre e-mail con le password più comuni*". Proprio a giugno di quest'anno hanno rilevato la violazione di un loro account, notificato subito da Google e subito sospeso, e fortunatamente appartenente ad un utente con bassi privilegi e con accessi limitati.

La percezione che emerge è che la consapevolezza tra le PMI sia ancora molto bassa. "*Chi dice che è sicuro non sa di che cosa parla*" afferma il dott. Natale a tal proposito.

Spesso alcuni grossi clienti si lamentano dei troppi fattori di autenticazione. "*Nonostante noi lo facciamo davvero per la sicurezza del cliente a volte non viene percepito così e quindi ci sono delle resistenze […] Purtroppo la nostra forza di imporre policy di sicurezza è bassa, più che dare consigli non possiamo fare. Se l'utente si lamenta abbiamo le mani legate".*

Sia Natale che Fava riferiscono l'esigenza di sensibilizzare in modo trasversale gli utenti sui pericoli informatici, cosa che già loro tentano di fare, auspicando anche un maggior livello di condivisione a riguardo, "*non bisogna vedere la sicurezza solo come un costo ma anche come un investimento",* dichiarano.

Importante è la condivisione non solo delle informazioni, ma anche di obiettivi e metodi, in quanto un buon rapporto tra reparto IT e Consiglio di Amministrazione facilita l'attuazione di corrette policy di sicurezza, "*se l'IT non è supportato dal CDA non si va da nessuna parte*" dichiara Fava. Entrambi inoltre lamentano della mancanza di equilibrio di seminari e convegni a cui hanno partecipato, spesso troppo superficiali o troppo allarmistici.

Un'ultima intervista è stata infine realizzata presso l'Assindustria di Lucca, con il Direttore Claudio Romiti e il responsabile Daniele Chersi (Servizio economico) secondo i quali, in generale e soprattutto per le PMI, non vi è consapevolezza dei pericoli derivanti da un uso disinvolto del mezzo informatico. In questo periodo registrano un maggiore interessamento al cloud, soprattutto per un principio di economicità. Di norma però l'atteggiamento che notano è di rifiuto a considerare anche le più basilari policy di sicurezza, "*sino a quando non succede un pasticcio, non prendono in considerazione neanche il semplice cambio password* […] *Vi è un problema di cultura enorme. Il problema oltre che culturale, consiste anche nel fatto che nella maggior parte delle PMI manca una figura che si occupi specificamente di questi aspetti".*

Con scadenza più o meno annuale Assindustria organizza seminari a tema, come PEC, fatturazione aziendale, banda larga, registrando però una bassa affluenza da parte delle PMI.

La realizzazione di interviste semistrutturate, presso diversi attori istituzionali coinvolti ed aziende della zona presa in esame, ha permesso che emergessero quelli che possiamo definire i concetti chiave più utili per una corretta definizione di programmi ad hoc per le PMI ed il contrasto alla criminalità informatica.

Data la natura di questo fenomeno, l'esigenza di investire in formazione è l'aspetto primario emerso in tutte le interviste, insieme all'esigenza di abbattere le barriere culturali che

frenano la consapevolezza riguardo i rischi del cyber crime. Le vulnerabilità umane infatti sono da considerarsi più pericolose di quelle tecniche.

I casi che registrano un sensibile aumento in questi ultimi anni, inoltre, risultano essere quelli di tipo mirato, come lo spear phishing, molto pericoloso per le aziende anche perché il criminale calcola l'importo da sottrarre in modo da non permettere alle aziende, in molti casi, di accorgersi subito dell'accaduto.

È ritenuto necessario inoltre che non solo i reparti IT continuino ad essere informati su questo fenomeno, ma che lo siano anche gli amministratori, i titolari delle aziende e il CDA, al fine di mettere in atto contromisure e policy concertate.

La totale mancanza di condivisione e collaborazione tra le aziende inoltre suggerisce l'esigenza di creare dei network tra le aziende dello stesso settore o per dimensione al fine di aumentarne il dialogo e la diffusione di best practices.

Purtroppo la sicurezza viene ancora vista molto spesso come un costo e non come un valore, questo porta ovviamente a notare che mediamente il livello di sicurezza è direttamente proporzionale alla grandezza dell'azienda, a quanto questa sia strutturata e al budget e alle risorse impiegate per migliorare questo aspetto.

Proteggere le PMI italiane, fondamentali per la nostra economia e ad alto valore in termini di know-how, dovrebbe essere un obiettivo fondamentale soprattutto se consideriamo quello che emerge e cioè che sono spesso vittime del furto della loro eccellenza da insider più che da hacker esterni, di conseguenza è quanto mai necessaria una buona policy interna per mitigare questo rischio.

CONCLUSIONI

Per la sicurezza di una Nazione e della sua economia il contrasto al fenomeno sempre più vasto del cyber crime è una *issue* quanto mai primaria. Gli eventi di cyber crime sono sempre più diffusi e il loro impatto sull'economia mondiale è sempre più preoccupante.

Come abbiamo visto, l'Unione Europea, nel 2013 ha adottato la propria cyber strategy ed ha invitato gli Stati Membri a fare altrettanto. Nel 2014 anche l'Italia si è dotata di un *Quadro strategico nazionale per la sicurezza dello spazio cibernetico* registrando però ancora dei ritardi rispetto alla media europea nel recepimento di alcune direttive. Come si afferma nel report di UNODC[213], la maggior parte dei cyber attacchi è di carattere transazionale, ciò significa che è difficile contrastarli solo localmente. Si rende innanzitutto necessario articolare una risposta a livello globale attraverso regolamenti condivisi e percorsi di sviluppo tecnologico comuni. L'implementazione delle politiche di sicurezza informatica è prerogativa degli Stati Nazionali, ma è quanto mai importante, riguardo questo fenomeno, incentivare la cooperazione europea ed internazionale e le partnership nel settore pubblico e privato. Inoltre, non va dimenticato che il *cyber space* costituisce un'opportunità fondamentale per l'economia di un Paese, ma nasconde numerose insidie che è necessario conoscere e da cui bisogna imparare a difendersi.

La difficoltà nell'affrontare questo tipo di criminalità consiste soprattutto nell'asimmetria esistente tra gli strumenti e le conoscenze appannaggio dei cyber criminali, rispetto a quelle di chi si deve difendere o è preposto a contrastare questo fenomeno. I mezzi per condurre un cyber attacco, infatti, sono sempre più potenti e sempre più facilmente reperibili ed utilizzabili, e relativamente poco costosi. Le abilità necessarie ai criminali per condurre un attacco di tipo informatico sono sempre minori, basta davvero poco per potersi dotare degli strumenti e delle informazioni necessarie, e il *deep web*, in questo facilita le cose. La lotta al cyber crime necessita sicuramente di azioni legislative forti, meccanismi di *law enforcement*, di strumenti adeguati, e collaborazioni, ma il fattore più importante è la conoscenza.

Sia le Forze di Polizia, sia le aziende hanno il difficile compito, rispettivamente, di contrastare e di difendersi da tutte le tipologie di attacchi informatici conosciuti, mentre, sempre più spesso, accade che i criminali si specializzino in una determinata tipologia di attacco e raffinino le loro tecniche raggiungendo alti livelli di efficacia, sviluppandone sempre di nuove, spesso sconosciute a chi deve contrastare questo fenomeno. Si pensi all'evoluzione del phishing. Ormai siamo sempre meno in presenza di e-mail fraudolente scritte in modo scorretto e facilmente individuabili e aumentano sempre di più i casi di spear phishing, azioni mirate moto difficili da riconoscere. Gli esiti, dal punto di vista delle azioni repressive, sono incerti in questo campo, infatti il problema non è dovuto alla scarsità di denunce o dal personale non sufficiente, ma le motivazioni sono riferibili alla natura stessa del fenomeno, quindi risulta più efficace lavorare sulla prevenzione. Lo scenario emerso dalle interviste è che, questo tipo di crimine, soprattutto a livello investigativo e giudiziario, è moto difficile da perseguire e attualmente questo costituisce una situazione purtroppo idilliaca per i cyber criminali che posso continuare ad incrementare le loro capacità, i loro guadagni e la loro rete, diventando terreno fertile anche ad esempio per la criminalità organizzata o il terrorismo.

[213] *Comprehensive Study on Cybercrime*, UNODC, febbraio 2013, in <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf> (ultima consultazione 15-11-2014).

Un elemento che purtroppo non aiuta a ridurre il gap tra l'intensità di questo fenomeno e la reale capacità di difendersi da questi attacchi è dato dal fatto che la velocità di aggiornamento, specializzazione e quantità di risorse dedicate da parte dei cyber criminali saranno sempre maggiori rispetto alle azioni messe in campo dal singolo utente.

Diminuisce sempre di più con il tempo, inoltre, il confine tra i vari tipi di cyber attaccanti ed aumentano i rapporti tra la criminalità informatica e quella ordinaria che sfrutta la nuova tecnologia per ampliare le proprie attività illecite, collaborando direttamente con i cyber criminali o acquistando da loro strumenti e risorse necessari per compiere azioni criminali nel *cyber space*.

Dalle interviste emerge che le tipologie di reati commessi dai cyber criminali italiani rispecchiano tendenzialmente la classica truffa "all'italiana" perpetrata attraverso il mezzo informatico, come le truffe da false vendite, mentre le altre tipologie di reati più complessi sono soprattutto di origine russa, cinese ed africana.

Un altro fattore che rende più difficile la lotta a questo tipo di criminalità è la difficoltà di determinare una particolare tipologia di vittima, tutti i singoli utenti del web (cittadini, PMI, grandi imprese, Stati Nazionali) sono potenziali vittime.

In questo ambito è utile considerare l'aspetto psicologico alla base di questi reati, la percezione del rischio, infatti, tra la sicurezza fisica e la sicurezza informatica è completamente diversa e fortemente viziata dall'esperienza. Il furto fisico è ben percepito, quello virtuale meno, infatti nessuno di noi oggi lascerebbe mai la porta di casa aperta o il proprio portafoglio incustodito in un luogo pubblico, ma, dal punto di vista informatico, la propria vulnerabilità non viene avvertita a causa della tendenza a non considerare reale il virtuale. Sempre dal punto di vista psicologico, la neutralità del monitor abbatte le capacità di percezione degli effetti delle proprie azioni, sia dal punto di vista del criminale sia da quello della vittima. La desensibilizzazione che avviene attraverso l'uso del PC impedisce al cyber criminale di comprendere l'entità del danno arrecato alla vittima, le conseguenze di questo e l'esistenza della vittima stessa, che appare solo come un semplice indirizzo IP. Lo stesso processo avviene anche nell'utente, che abbassa le proprie difese nel web perdendo certi pudori e sottovalutandone la pericolosità, per esempio un click su un link ricevuto per e-mail, la condivisione di informazioni personali sui social, la facilità con cui si è predisposti a comunicare con persone sconosciute via chat o webcam, sono tutte azioni che difficilmente si compierebbero con leggerezza nel mondo reale. Inoltre la distanza fisica che intercorre tra il cyber criminale e la vittima amplifica questi aspetti.

Il fattore umano è un elemento assolutamente determinate in questo tipo di criminalità, che spesso sfrutta le debolezze umane per i propri scopi. I cyber criminali contano proprio sui piccoli errori umani per trarne vantaggio, come ad esempio convincere un utente a cliccare su un link in una e-mail di phishing che porterà ad infettare il suo PC, o a rivelare informazioni personali o aziendali riservate puntando sulla propensione a non verificare l'attendibilità di chi sta dall'altra parte del computer. La sicurezza informatica, infatti, non è uno stato da acquisire, ma una mentalità da adottare a 360 gradi nella vita privata e soprattutto all'interno della propria azienda o del proprio posto di lavoro. Solo così si possono ottenere risultati validi e duraturi nel tempo.

Per superare l'intangibilità dei danni arrecati e l'invisibilità delle vittime di questi reati, nell'ottobre del 2012 si è realizzato il primo caso di giustizia ripartiva in Italia in un processo ordinario, volta a far riconoscere al reo l'esistenza delle vittime e a ripagare la comunità non in

termini economici ma umani, nei confronti di un soggetto che aveva truffato più di 100 persone, resosi disponibile a servire alla mensa dei poveri in seguito ad un patteggiamento di una parte della pena[214].

Anche nell'ambito delle Piccole e Medie Imprese, il fattore umano gioca un ruolo fondamentale. La negligenza sul posto di lavoro infatti rappresenta una delle cause principali, insieme alle falle dei sistemi e agli attacchi hacker, di violazione dei dati aziendali che possono portare, oltre ad una perdita di business anche alla perdita di fiducia da parte della clientela, danno enorme per una PMI.

Le PMI spesso sottovalutano i pericoli derivanti dal cyber crime, dando la priorità al bilancio e non considerando i costi legati a questi rischi. La spesa ICT è vista come un male necessario perché si pensa che non abbia un impatto sul fatturato.

Oggi qualsiasi settore merceologico e aziendale è influenzato dall'ICT. La struttura del nostro sistema economico, a differenza di quello di altri Paesi europei, è fondato sulle PMI. Il know-how italiano è il nostro fiore all'occhiello e, mentre le grandi imprese cominciano a difendersi dal cyber crime e le Banche ci convivono da tempo, le PMI faticano ancora a mettere in atto adeguate contromisure. Anche se questi pericoli possono sembrare intangibili, i danni che producono non lo sono. Il tessuto connettivo industriale del nostro territorio non può essere considerato come un sistema chiuso, i rapporti commerciali, nazionali ed internazionali, e le comunicazioni telematiche tra le aziende, imprescindibili per la continuazione del business, possono essere veicolo di infezioni sempre più veloci e potenzialmente dannose per tutto il sistema economico. La sicurezza del sistema dipende dalla sicurezza di tutti. Una PMI potrebbe pensare di non essere un bersaglio appetibile per un cyber criminale, soprattutto se produce beni non legati all'ICT. In realtà proprio le aziende più piccole e vulnerabili costituiscono un facile bersaglio e il problema maggiore è che non ne sono consapevoli. Dalle interviste svolte è emerso che un atteggiamento molto diffuso tra le PMI è quello di preferire di pagare i danni conseguenti ad un attacco piuttosto che investire nel prevenirlo. È vero che il livello di consapevolezza sta lentamente aumentando, ma rimane ancora radicata l'idea che investire nella sicurezza informatica sia un costo troppo oneroso e quindi si sceglie di non farlo. Registriamo quindi una dichiarazione di percezione, alla quale però non seguono azioni proattive.

Bisogna considerare che non viene lesa solo l'azienda attaccata in modo diretto tramite una frode on-line, ma indirettamente anche tutto il sistema economico, il cittadino, il mercato, le istituzioni locali. In più, di fronte a questo reato, la vittima purtroppo non è adeguatamente tutelata. Come abbiamo visto dai casi di cronaca citati nei capitoli precedenti, le aziende più grandi sono colpite sempre di più attraverso fornitori, *outsources* e aziende della propria filiera.

L'affidabilità in termini di sicurezza informatica delle PMI italiane, soprattutto all'interno dei distretti industriali, potrebbe essere un elemento a loro favore nel processo che vede la delocalizzazione in Paesi dell'est, che però possono costituire un pericolo dal punto di vista della

[214] *Truffatore on-line servirà a tavola i poveri Primo caso di giustizia «riparativa» Il giudice: così si accorge delle vittime nel mondo reale*. Di Luigi Ferrarella. Corriere della Sera 7-10-2012, in <http://milano.corriere.it/milano/notizie/cronaca/12_ottobre_17/truffatore-pena-riparativa-poveri-mensa-2112290080980.shtml> (ultima consultazione 15-11-2014).

cyber security. Il terreno di sfida non può essere solo quello economico, in quanto un'azienda italiana non potrà mai abbassare i propri prezzi allo stesso livello di una concorrente dei Paesi in via di sviluppo, ma potrebbe puntare su una maggiore offerta in termini di affidabilità in ambito informatico, puntando sulla cyber security come valore aggiunto. Le imprese distrettuali potrebbero vedere così nelle PMI italiane anche una opportunità di investimento in termini di security.

La vera frontiera da abbattere è quella culturale, infatti molte azioni difensive possono essere messe in atto anche a costi limitati. Oltre alle policy di sicurezza interna è necessario incentivare la condivisione delle informazioni a più livelli. A livello preventivo, prima che si verifichi un attacco, condividere best practices ed informazioni sulle minacce con le aziende della filiera, le associazioni di categoria e Forze dell'Ordine può aiutare a mettere in atto delle prime contromisure. A livello operativo, durante o dopo un attacco, la condivisione con attori preferenziali come Forze dell'Ordine, Banche ecc. può avere il fine di aumentare la resilienza del sistema e mitigare i danni subiti.

Dall'analisi svolta sui report internazionali, sulle informazioni raccolte sul fenomeno del cyber crime, sulle normative emesse a livello europeo ed italiano nell'ambito della sicurezza informatica e soprattutto dall'indagine svolta attraverso le interviste ad attori istituzionali preposti a contrastare questo tipo di criminalità e alle aziende della Provincia di Lucca, emerge chiaramente che l'unica arma davvero efficace contro il cyber crime è la consapevolezza. Il problema non è solo tecnico ma soprattutto culturale.

Le azioni da mettere in campo per contrastare questo fenomeno devono essere volte a formare il più possibile l'utente e a favorire la condivisione delle informazioni. Questi due obiettivi possono essere raggiunti attraverso l'attuazione di due progetti.

Il primo progetto, con lo scopo di aumentare la conoscenza e l'informazione in questo settore su due diversi livelli aziendali, potrebbe riguardare l'organizzazione di seminari, workshop e corsi di formazione differenziati, rivolti a decisori non tecnici, cioè CDA e titolari delle imprese e al personale IT dell'azienda. Questa differenziazione permette di strutturare il seminario in modo che sia adeguato alla formazione di base dei partecipanti e alle loro funzioni all'interno dell'azienda. Realizzare seminari troppo tecnici per chi ha il compito di prendere delle decisioni per tutta l'azienda, oppure troppo generici per chi ha una formazione molto tecnica, rischiano di essere poco appetibili e di non formare adeguatamente l'utente. Corsi differenziati hanno il vantaggio di fornire, agli amministratori delle aziende, tutte le conoscenze di base, per comprendere i vari aspetti di questo fenomeno, necessarie a prendere le decisioni in maniera più consapevole e responsabile. Per il personale IT, invece, corsi più tecnici e specialistici possono aggiornarli sulle nuove minacce, soprattutto quelle emergenti o di nicchia, mantenendo alto il loro livello di formazione, che spesso è lasciato alla loro libera iniziativa. Questi due differenti percorsi formativi, a loro volta, possono essere organizzati, differenziandoli per settore merceologico o per dimensione dell'azienda. In questo modo, oltre alla formazione, si vuole favorire la condivisione tra le aziende e la nascita di network per la condivisione di esperienze ed informazioni. È

consigliabile che questi corsi vengano svolti con il sostegno delle associazioni di categoria e non da aziende private per evitare il timore da parte delle aziende di partecipare a corsi con il solo fine di sponsorizzare dei prodotti. Oltre agli aspetti teorici sarebbe molto importante puntare anche su simulazioni pratiche che mostrino ai partecipanti la facilità con la quale un cyber criminale può mettere a segno un attacco che mini la sicurezza dei dati aziendali.

Figura 28 - Progetto di Corsi di Formazione Differenziati

Un secondo progetto, complementare al primo, prevede la realizzazione di periodiche tavole rotonde tra attori specifici come rappresentanti delle PMI per settore merceologico, Questura, associazioni di categoria, Università, Procura ed esperti legali. Lo scopo di questo progetto è non solo quello di condividere le informazioni sui rischi emergenti in ambito cyber, ma anche quello di favorire l'individuazione di referenti per settore merceologico delle Piccole e Medie Imprese e soprattutto, con il tempo, permettere la nascita di una sorta di comunità epistemica, che alimenti il motore della conoscenza in questo settore e che possa diventare un esempio virtuoso di prevenzione al cyber crime. Rafforzando questo progetto, si potrebbero coinvolgere nel tempo anche le grandi aziende di tutto il centro Italia.

Figura 29 - Progetto di Istituzione di Tavole Rotonde Periodiche

Attraverso la realizzazione di questi due progetti si può arrivare alla creazione di una comunità epistemica che non solo ha il valore di promuovere una vera cultura della sicurezza, ma ha anche il vantaggio di non diventare mai obsoleta rispetto alle semplici best practices, e di adattarsi a qualsiasi tipo di evoluzione del fenomeno registrandone i cambiamenti e adattandosi ad essi.

INDICE DELLE FIGURE

INDICE DELLE TABELLE

METODOLOGIA

L'argomento della ricerca e gli obiettivi prefissati hanno richiesto due fasi di studio.

Nella prima fase di studio si è svolta un'analisi dei più recenti report sul fenomeno del cyber crime redatti dalle maggiori aziende di consulenza informatica (CISCO, Kaspersky, McAfee, Ponemon, TrendMicro, Clusit, ecc.) e disponibili on-line e gli ultimi report pubblicati da i più stimati enti superpartes (UNIDOC, ENISA, World Economic Forum, ecc). Attraverso questa analisi si sono voluti mettere in evidenza i dati riguardanti il cyber crime comuni a tutti i report per avere una raffigurazione il più possibile vicina alla realtà del fenomeno, soprattutto per quanto riguarda le PMI. Oltre ciò, nella prima fase sono state esaminate le principali normative a livello europeo e nazionale e gli enti preposti ad affrontare questo tipo di criminalità. Questo studio ha avuto lo scopo di riassumere la situazione normativa attuale all'interno della quale si configura la capacità di risposta degli Stati nazionali e dell'Italia nel contrasto al cyber crime. Inoltre attraverso una mirata attività di OSInt, attraverso le maggiori testate giornalistiche internazionali, sono stati studiati ed esposti casi concreti dei principali eventi di *cyber attack* a livello internazionale e di come alcuni Stati stanno affrontando questo tipo di criminalità. Infine, è emersa l'esigenza durante questa fase di realizzare una panoramica delle tipologie di attacchi, attaccanti, vulnerabilità e rischi attualmente presenti per dare una, se non esaustiva, quanto meno principale conoscenza di come questo fenomeno si è evoluto sino ad oggi e di cosa possa costituire un pericolo per le PMI. Questa sezione può essere infatti considerata una sorta di guida per le PMI al fenomeno del cyber crime attraverso rischi e vulnerabilità che interessano le aziende.

Durante la seconda fase di ricerca si sono svolte delle interviste semistrutturate di tipo qualitativo utili a definire ed illustrare la reale situazione dello stato attuale del fenomeno a livello locale e specificatamente nella Provincia di Lucca, focus dell'ultimo capitolo di questa ricerca. Per realizzare queste interviste si sono individuati degli interlocutori chiave. Si è anche testata l'efficacia di una semplice richiesta generica via e-mail di adesione alla ricerca che però, come spesso accade in questi casi, non ha avuto un alto riscontro. Nello specifico è stato esposto il progetto di ricerca al Direttore di Assindustria di Lucca, che ha diffuso alle aziende iscritte una circolare (allegato A) nella quale si annunciava la realizzazione della ricerca e si richiedeva la disponibilità ad essere contattati per informazioni utili ai fini della ricerca. In seguito a questo invio una sola azienda ha risposto chiedendo informazioni. L'azienda in questione poi ha acconsentito anche a rilasciare un'intervista per la ricerca. Maggior efficacia invece ha avuto il contattare personalmente attori riconosciuti come strategici ai fini della ricerca, come esponenti delle Forze dell'Ordine e Magistrati che hanno accolto positivamente la richiesta di collaborazione. Nello specifico l'intervista con il Vice Questore aggiunto della Polizia Postale di Firenze dott.ssa Pierazzi è riportata in questa sezione (allegato B) in quanto è stato possibile registrare la conversazione. Le Procure della Repubblica di Firenze e di Torino inoltre hanno fornito rispettivamente dati statistici e la visione di un caso studio da riportare all'interno della ricerca.

In seguito hanno accolto positivamente la possibilità di rilasciare interviste le aziende della zona di Lucca rappresentative dei settori merceologici più diffusi, Assindustria, ABI Lab, Consorzio

Bancomat e IBM. L’analisi di tutte le interviste svolte ha permesso di individuare i principali fattori chiave per l’implementazione di azioni per il contrasto al cyber crime.

Allegato A

27/2014/V/1 - Indagine sulla criminalità informatica

Riferimenti Internet:			
Numero	Data	Settore Merceologico	Argomento
27/2014	08/07/2014	Tutte le Aziende	Internet – Siti vari

UNICRI(1) sta svolgendo una Ricerca sulla criminalità informatica e i rischi per l'economia e le imprese a livello internazionale, europeo ed italiano, con un focus specifico sulla Provincia di Lucca. I risultati saranno presentati durante una conferenza e utilizzati per la progettazione di programmi di formazione.
Gli scopi della ricerca sono:

- identificare e analizzare i principali problemi legati alla criminalità informatica e sicurezza informatica a livello internazionale;
- identificare e analizzare i principali problemi legati alla criminalità informatica e sicurezza informatica e rischi per l'economia e le imprese a livello dell'UE e le relative contromisure;
- identificare e analizzare i principali problemi legati alla criminalità informatica e sicurezza informatica e rischi per l'economia e le imprese a livello italiano, con un focus sulle PMI;
- focus sulla provincia di Lucca e le sue piccole medie aziende, attraverso indagini sul campo."

Le aziende interessate a partecipare possono contattare direttamente:
Flavia Zappa

Referente:
Daniele Chersi

(1) UNICRI-*United Nations Interregional Crime and Justice Research Institute* di Torino.

Allegato B

Intervista Vice Questore dott.ssa Stefania Pierazzi

D: *Innanzitutto la ringrazio per aver accettato questa intervista. La Polizia Postale svolge un ruolo fondamentale per il contrasto al cyber crime e in base alla Legge 48 del 2008 tutti i reati di tipo informatico vengono trattati a livello distrettuale. Voi quindi ricevete i casi di tutta la Regione Toscana?*

R: Sì, se siamo noi a ricevere la denuncia, come Polizia Postale, la trasmettiamo alla distrettuale che di solito delega questo ufficio, ma può anche capitare che vengano trattate anche da altri uffici. Il dato complessivo di quanti reati sono sopravvenuti lo può fornire la Procura che ha i dati di tutta la Regione, mentre noi, a livello distrettuale abbiamo i dati di tutte le Provincie eccetto Massa, che è sotto Genova.

D: *Lei si occupa di questo fenomeno da 15 anni e quindi ha potuto notare la sua evoluzione. Cosa può dirci a riguardo?*

R: Sì, all'inizio era un fenomeno sottotono, infatti i primi anni c'era anche molto pudore a denunciare questo tipo di reato, e le Banche, per prime, tendevano, laddove avessero subito degli attacchi, a non manifestarlo all'esterno. Magari restituivano ai clienti quello che era stato loro sottratto però come fenomeno non lo rappresentavano mai, poi con il tempo è diventato un reato sempre più comune e si sono resi conto che il fatto di aver subito un attacco non sminuisce la propria immagine, non fa venire meno la credibilità di un soggetto, o di una società. E allora, si sono manifestati di più ed oggi anche le grosse società denunciano questo tipo di reato. Di sicuro di più di quanto succedesse in passato. Prima era molto difficile, lo venivamo a sapere o *de relato*, perché c'era stato qualche atto concomitante e quindi ne venivamo a conoscenza… faccio un esempio… vi fu un *e-mail bombing* di Google nel 2002-2003, un sacco di società fiorentine subirono l'attacco, e fecero da tramite per questo tipo di attacco indirizzato a Google. In realtà noi la denuncia la ricevemmo solo da una piccola società di Prato e da lì avemmo contezza del fenomeno su Firenze e Provincia. Era il caso di vari soggetti che si erano accordati in tutto il Mondo per intasare la posta elettronica di Google, alcuni di questi soggetti erano su Bologna, erano degli studenti di ingegneria che avevano bucato varie società di Prato e Firenze per compiere questo attacco. Però questo le società fiorentine non lo avevano denunciato, ce lo riferì una piccola azienda e da lì potemmo ricostruire il tutto. Oggi non è più così, lo rappresentano con maggiore facilità anche le grandi aziende. Anche la grossa azienda e i grossi marchi, qui a Firenze ne abbiamo di diversi, che possono aver avuto degli attacchi o dei tentativi di acquisizioni fraudolente lo hanno rappresentato, anche quando hanno avuto il solo sospetto di poter essere state vittima.

D: *Da quanti anni lei sta notando questa inversione di tendenza?*

R: Direi da 4-5 anni decisamente. Infatti, più se ne parla e più si fa capire che è un fenomeno che è appannaggio di tanti e che quindi lo si può dire. Poi perché la legge sulla privacy ha dato molti più oneri alle società sulla gestione dei dati e quindi a fronte di questa loro responsabilizzazione lo comunicano con più facilità.

D: *Che trend si è registrato rispetto ai fenomeni di cyber crime in questi ultimi anni nella zona di sua competenza?*

R: Come reati informatici in genere il trend è in aumento, notiamo una vera e propria escalation. In realtà quello che, in questi ultimi, anni ha avuto il picco è stato il phishing. Non è un reato a se stante, ma è la concomitanza di un accesso abusivo ad un sistema informatico e da lì parte tutta un'altra serie di reati che possono essere commessi. Il fenomeno del cosiddetto phishing è quello che ha avuto in questi ultimi anni una vera escalation. Il tentativo cioè di carpire dati e credenziali bancarie di un singolo o di una società piccola o grande che sia e di utilizzarli per fare transazioni. L'accesso abusivo più comune e più registrato è proprio questo. Sì, di questo si è avuto un'impennata negli ultimi 3-4 anni. Questo trend non accenna a scendere, continua a svilupparsi in maniera costante nel tempo.

D: *Nella zona di Lucca prevale il distretto delle cartiere, a cui appartengo la maggior parte delle PMI della Provincia, mi può confermare questo dato? E c'è una tipologia particolare di impresa vittima di questo fenomeno?*

R: Sì nella zona di Lucca è molto diffuso il distretto delle cartiere. Il fenomeno del cyber crime è comunque molto trasversale, attraverso i nostri dati empirici in base alle denunce, segnalazioni o deleghe che ricevo, direi che non colpisce una tipologia in particolare di azienda. È un tipo di fenomeno indiscriminato, arriva qui da noi la piccola azienda come la grossa società, contattata dalla propria Banca perché ha rilevato un bonifico anomalo, magari di una cifra considerevole di 70.000 euro verso X e la società in realtà non aveva autorizzato nessun bonifico. Quindi tendenzialmente registriamo la medio grossa società con importi di furti più elevati e società più piccole con importi più piccoli e anche il singolo cittadino con piccoli importi.

D: *Qual è l'entità economica di questo tipo di attacchi?*

R: È più facile che siano più attacchi di cifre non esagerate e commisurate alla parte offesa, per esempio una grossa società può subire un attacco da 35 o 40 mila euro, una società piccola attacchi per esempio da 1.500, 2.000 euro, ovviamente più di uno ripetuto nel tempo che incidono nella stessa misura. E le imprese così non si accorgono subito dell'attacco. Giocano per esempio su dei falsi ordini, false fatture, far indirizzare le fatture ad indirizzi diversi rispetto a quelli dei reali destinatari, sono importi anche non necessariamente altissimi, però abbastanza diffusi.

D: *È difficile individuare chi ha realizzato l'attacco?*

R: Sì, perché di norma i criminali sono molto preparati, quindi usano sistemi che permettono loro di non essere individuarti, basta usare un proxy e già si rendono irrintracciabili, o per lo meno sembra che l'acquisizione sia stata fatta usando un server che è all'estero e l'attività non dico che si ferma, ma quasi.

D: *Quindi è molto difficile anche capire la nazionalità dell'attaccante?*

R: Sì, esattamente, verosimilmente in qualche caso abbiamo individuato i soggetti e abbiamo avuto riscontro che i soldi sono poi rientrati in Italia. Però non è sempre così. E comunque riescono a far sparire le loro tracce in brevissimo tempo. Per esempio se io uso un *proxy* che fa sembrare che l'attività sia partita da qualsiasi Stato dell'Oceania, siamo di nuovo al punto di partenza.

D: *Qual è il livello di transnazionalità dei reati registrati nella zona di vostra competenza? Il carattere transazionale del cyber crime rende più difficoltoso condurre le indagini?*

R: Assolutamente. Il problema è ulteriore perché gli attacchi spesso vengono da Paesi che non sono della Comunità europea, quindi non sono così collegabili tramite Europol, che invece è uno strumento che utilizziamo. Quindi in quei casi, l'attacco provenendo da Paesi con i quali non ci sono accordi di reciprocità, dove non ci sono scambi o per lo meno acquisizioni di dati, si può richiedere una rogatoria internazionale. Però la Procura ovviamente fa una constatazione costi benefici, per 300 euro di frode una rogatoria internazionale che costa 5.000 non la attiva, è comprensibile, è buon senso questo, ma, ammesso e non concesso che viene attivata, i tempi sono talmente lunghi che per la volatilità dei dati che servono per fare l'attività investigativa, qualche volta, anche quando arrivi sul posto, non ci sono più i dati che ti servono, quindi sono dei reati, quelli transazionali davvero tra i più difficili da gestire.

D: *Vi è collaborazione a livello internazionale nelle indagini?*

R: In questi casi, le strade che possiamo seguire sono due. O tramite il nostro servizio di Polizia Postale che ha sede a Roma, che è l'omologo del sevizio di cooperazione internazionale, Interpol, tutti e due del Ministero, tutti e due dello stesso livello e parlano tra sé, e qualche volta quando c'è qualcosa di urgente ci rivolgiamo noi stessi a loro, e c'è collaborazione effettivamente, nel limite del possibile dell'acquisizione dei dati. Nel senso che possono darmi collaborazione nel fornirmi alcune informazioni, come nell'identificazione per esempio. Poi ci sono dei dati che comunque devono essere acquisiti secondo una procedura ben precisa, altrimenti non hanno valenza in sede processuale, quindi bisogna attivare una rogatoria internazionale ecc. Per esempio, se io sto monitorando un soggetto che si trova in un Paese straniero e voglio sapere qual è la sua identità, attraverso la collaborazione della Polizia locale riesco ad ottenere l'identificazione e quella mi è utile a livello investigativo. Diverso è ciò che posso poi usare in ambito processuale e allora in quel caso occorre l'attivazione di procedure standard come la rogatoria internazionale con un'acquisizione formale, e in quel caso i tempi sono dilatati e di conseguenza è comprensibile come non sia sempre fattibile. Nel caso della pura investigazione i tempi sono più rapidi, anche

perché spesso ci capita di chiamare il collega che fa il funzionario di collegamento nello Stato X e ti dà delle informazioni che servono per andare avanti nelle investigazioni, poi per creare un fascicolo processuale a tutti gli effetti bisogna seguire altre procedure e sono diverse e più farraginose.

D: *La differenza consiste quindi molto dall'entità dell'attacco.*

R: Sì, dipende sempre dalla Procura, capisco che per un cittadino che guadagna 100, 10 è molto, però la Procura ha delle spese che deve considerare, fa proprio una valutazione costi benefici, quindi, magari l'importo può non essere alto in taluni casi, ma si vede che verosimilmente può essere lo stesso soggetto che ha perpetrato il crimine, lo ha commesso più volte, quindi la Procura è spinta a muoversi, ma per importi non elevati e occasionali, è talmente tanto lunga e dispendiosa l'attività che non sempre la giustizia italiana se le può permettere.

D: *Ci sono gruppi italiani, particolarmente noti, che agiscono sul territorio?*

R: A noi riscontri con la criminalità internazionale organizzata e strutturata in Italia non ce ne sono capitati, ci possono essere stati gruppi ristretti che hanno messo in piedi delle attività. Però io faccio anche un'attività diversa, magari i colleghi dell'antimafia, DIA, hanno una visione di questo fenomeno sicuramente che va oltre, magari di criminalità organizzata internazionale che opera in questo modo. A noi è capitato magari di individuare gruppi di soggetti che sono delinquenti comuni, non particolarmente di livello, magari fini, abili, capaci, ma delinquenza comune. Fanno enormi danni a livello economico perché ne hanno la competenza, però la loro figura è piuttosto di basso profilo.

D: *Per quanto riguarda il tipo di danno che subiscono, per sua esperienza, le PMI in Toscana, è solo di tipo economico o avete registrato casi anche di perdita di proprietà intellettuale, danno di immagine o furto di dati?*

R: C'è un po' di tutto, però devo dire che il danno puramente economico avviene da soggetti estranei all'azienda, il più delle volte invece la sottrazione di dati e il danno, che poi viene quantificato in un secondo momento, come la sottrazione di brevetti, sottrazione di pacchetti di clienti, perché anche quello è un dato appetibile, dati di fatturazione alterati ecc., molto spesso arrivano da dipendenti infedeli o da ex-dipendenti avvelenati. Che magari poi anno creato una società per conto loro oppure semplicemente sono avvelenati nei confronti della società dalla quale sono usciti e avendo conoscenza degli accessi ecc., utilizzano queste informazioni per creare danni, diffondere brevetti, produrli a loro volta, impedire di avere contatti, fare da mediazione, come per esempio è capitato più di una volta "guarda questa società, lo stesso prodotto lo vendo io, ma il prezzo è inferiore". Perché le PMI basano il loro business su brevetti, eccellenze e soprattutto su contatti commerciali specifici, su utilizzo esclusivo di un marchio piuttosto che di un altro. Ecco, in questo caso il più delle volte, non vorrei dire il 100%, ma siamo lì, sono ex dipendenti. Raramente sono società concorrenti.

D: *Vi sono casi di furto di* know-how *e proprietà intellettuale dall'estero?*

R: Possono accadere. Un evento del genere però avviene per esempio perché magari dalla Cina qualcuno aggancia un soggetto che è qui in Italia e gli viene fatta un offerta. Oppure l'ex dipendente che si rimette in proprio e che si apre un certo canale e utilizza per sé quel bagaglio di conoscenze o di dati che è una sottrazione a tutti gli effetti.

D: *Difficile quindi da quantificare economicamente nel breve periodo.*

R: Sì, sicuramente, io purtroppo la parte civile la perdo, io conosco l'aspetto penale, so che Tizio ha fatto danno a Caio. Poi c'è il riscontro. Però poi l'attività civile che viene messa in piedi la perdo. A volte abbiamo qualche ritorno o conoscenza, ma il più delle volte non lo sappiamo.

D: *E le aziende di solito come reagiscono a questo tipo di attacchi?*

R: Se devo essere sincera, il più delle volte aspettano di avere il danno per poi correre ai ripari. Perché per loro la sicurezza informatica rappresenta un grosso investimento, soprattutto per le PMI. Costa tanto attuare una politica di prevenzione e di copertura totale a 360 gradi della propria struttura. Poi la tecnologia informatica cresce ad un livello esponenziale, quello che conosciamo oggi domani è già obsoleto, quindi l'aggiornamento è anche quello difficile e costoso. Anche se un'azienda ha approntato un buon sistema, si è organizzata bene, è talmente tanto frequente la necessità di aggiornarsi che non sempre tutti riescono a stare al passo. A volte si vede che aspettano un eventuale evento, corrono il rischio e un danno se eventualmente c'è si affronta dopo.

D: *Una sorta di analisi costo benefici, quindi.*

R: Sì, esattamente. Certe volte però ci sarebbero cose così davvero banali, tipo la variazione della password. Per esempio, se va via un dipendente, che magari gestiva l'amministrazione, sarebbe il minino cambiare subito le password e disattivare il suo account, ed invece non si fa nulla per mesi. A volte ci sono cose che non costerebbero nulla, basterebbe forse investire in una figura professionale che si occupi di queste cose, e raramente, se non nelle grandi aziende, si è strutturati in modo da avere ciò, e comunque anche le grandi aziende subiscono attacchi, basti vedere le Banche.

D: *A tal proposito, nella conversazione con l'Ispettore Bozzi, è emerso che ci sono Banche che hanno anche protezioni molto basse per esempio della loro rete WI-FI.*

R: Sì, si riesce in tempi brevissimi a carpire una quantità esagerata di dati. Non solo. Noi abbiamo il riscontro spesso degli attacchi che subiscono le Banche dalle denunce dei correntisti, cittadini comuni, attraverso il quale notiamo per esempio un trend. Per esempio in una quindicina di giorni vengono a denunciare più casi di clonazione di carte di credito, prelievi fraudolenti, sempre dalla

stessa Banca, quindi verosimilmente sono attacchi che subiscono quelle Banche o, se non direttamente loro, i sistemi che usano che magari non sono correttamente aggiornati e quindi sono altamente vulnerabili.

D: *Per quanto riguarda le grandi imprese molte hanno reparti appositamente strutturati e investono in questo settore e comunque subiscono degli attacchi. Immagino che per le PMI sia più difficile difendersi da questo tipo di criminalità*.

R: Sì, perché spesso hanno pochi dipendenti e magari uno stesso dipendente ha più mansioni tra cui questa. E questa cosa la subiscono sicuramente di più e quando poi si accorgono di aver subito un danno cercano di rimediare in qualche modo.

D: *C'è un buon livello di fiducia nei confronti delle Forze dell'Ordine da parte delle imprese o di chi subisce l'attacco per sua esperienza?*

R: Sì, devo dire che si affidano molto a noi. Spesso la ditta viene a denunciare l'attacco subito come per esempio casi in cui carpiscono l'elenco dei clienti, e noi suggeriamo l'accertamento da un perito o magari loro lo hanno già fatto fare da un consulente tecnico, ma comunque ci chiedono di fare una verifica perché se la facciamo noi si sentono più tranquilli e sicuri. E questo devo dire che è un aspetto davvero positivo, raramente ho trovato chiusure nei nostri confronti in questo campo, volentieri accettano consigli, consulenze, forniscono liberamente i loro dati, insomma c'è una buona collaborazione da questo punto di vista.

D: *Data la peculiarità di questo tipo di reato lei ritiene che la normativa esistente sia adeguata?*

R: Sì, capisco che è difficile per un legislatore pensare a tutte le fattispecie. Diciamo che finora siamo riusciti abbastanza bene a far rientrare tutti i fenomeni nelle varie fattispecie che il legislatore nel tempo ha creato. Perché laddove il legislatore inserisce, per esempio per quanto riguarda i sistemi economici, anche i sistemi informatici, allora ci dà la possibilità di applicare quella tipologia di reato a tutti i casi. Con questa aggiunta, che è stata fatta per diverse tipologie di reato, dalla truffa, che è diventata così frode informatica, dagli accessi abusivi, ma anche l'acquisizione della posta, laddove c'è scritto che la posta elettronica è equiparata a quella cartacea il legislatore mi dà possibilità di muovermi e di fare un'attività di investigazione.

D: *E questa integrazione è stata fatta per ogni singola fattispecie?*

R: Sì, ci sono i reati dal 615 cp in poi che sono quelli che riguardano i sistemi informatici e telematici. E poi via via vengono fatte delle modifiche e delle precisazioni che rendono adeguate le varie fattispecie.

D: *L'ultima Direttiva europea, che non è stata ancora recepita, riguarda solo i provider delle infrastrutture critiche, questo vi limita in qualche modo?*

R: Sì, non è ancora stata recepita. Devo dire che ci basiamo molto sulla collaborazione dei provider, che per noi è fondamentale. L'handicap è che spesso sono all'estero, però riusciamo lo stesso a ottenere i dati che ci servono perché comunque hanno uffici legali qui in Italia oppure forniscono comunque il dato. Come per esempio Google, che non è italiana, ma fa' da tramite con Google Italia e accetta le richieste formulate dalla Polizia italiana. Quindi anche se le società sono straniere riusciamo comunque a cooperare.

D: *E questo vale se l'entità del furto è considerevole o anche per piccole violazioni?*

R: No, in questo caso dipende solo dalla società di provider. Richiedono comunque un decreto dell'autorità italiana, giustamente, perché sono dati sensibili, e nel momento in cui si ha il decreto, loro lo considerano come emesso dalle loro autorità, quindi lo riconoscono e ci danno la possibilità di collaborare. Noi acquisiamo i dati anche da società straniere.

D: *Qual è il livello di informatizzazione delle PMI della zona di sua competenza?*

R: Abbastanza alto. Sì, anche le più piccole ormai hanno l'informatizzazione di tutto l'aspetto economico. E poi hanno i contatti con i clienti. La rete interna può esserci o non esserci, ma ormai il sistema informatico è una realtà di tutte le aziende. Ovviamente con livelli di dimestichezza diversi.

D: *Mi diceva che spesso aspettano di avere un attacco per poi eventualmente rimediare, per motivi economici. Qual è la percezione del rischio e della criminalità in ambito informatico?*

R: Qualche volta sembra davvero che non abbiano la percezione di quanto possano essere vulnerabili i loro sistemi. Magari si ha a che fare con la vecchia scuola, vecchio imprenditore con pochi dipendenti che non ha la minima confidenza con lo strumento. Qualche volta invece sono un po' più consapevoli ma aspettano comunque di subire un danno prima di mettere in atto delle contromisure.

D: *Vi sono mai capitati casi di piccole imprese, satelliti di altre più grandi, colpite per colpire la grande azienda?*

R: Per quel che ricordo non ci è mai capitato. O comunque a livello informatico. Può darsi che a livello economico questo avvenga, però non è un settore di cui mi occupo io. Forse la Guardia di Finanzia ha più prontezza di questi aspetti.

D: *È a conoscenza di eventuali attività o iniziative da parte delle PMI o di enti Istituzionali locali per aumentare la consapevolezza dei rischi per le aziende in ambito informatico?*

R: Qualche anno fa ne organizzò una la Confcommercio riguardo l'uso del POS. Fece dei seminari per allertare sui pericoli e mi si aprì un mondo, perché ebbi la possibilità di parlare direttamente

con i commercianti fiorentini che già digerivano male l'imposizione di usare il POS. Quando gli si rappresentavano tutti i rischi che potevano correre nel maneggiarli o nel farli maneggiare a terzi, come il semplice inganno del caso di un soggetto che si può spacciare manutentore del POS, e glielo si fa' maneggiare senza chiedere nessun tipo di verifica, ho potuto constatare che erano proprio a digiuno su queste tematiche. Lì ho visto che il piccolo commerciante non era proprio informato su questo punto di vista, era vulnerabile al massimo. Sicuramente le società più grandi o neo costituite hanno forse più consapevolezza e conoscenza di questo problema. A volte infatti si fa' pubblicare magari di proposito un articolo per alzare il livello di attenzione. Spesso il giornalista è compiacente con la necessità di istruire le persone e la cittadinanza e informarla su un fenomeno emergente. O per esempio in concomitanza con l'arrivo delle vacanze si fanno iniziative del genere, anni fa lo fece il prefetto di Pisa, principalmente indirizzato agli anziani, ma comprendente tutta una serie di attività di preparazione a fronteggiare determinati problemi con l'ATM, per usarlo con correttezza, sia per anziani che per persone più giovani.

D: *Queste iniziative hanno avuto un buon riscontro? Vi è stata nel tempo un'evoluzione della consapevolezza delle proprie vulnerabilità in ambito informatico da parte delle PMI?*

R: Spesso sì. Qualche volta comunque sono iniziative che partono da richieste o esigenze specifiche. Ad attacco avvenuto allora cerchiamo di capire qual è stato il problema. Spesso si fanno a posteriori e sono settoriali. Ha molta più resa se ci occupiamo settore per settore e investiamo più nella qualità che nella quantità. Ovviamente spesso c'è anche la non risposta, cioè soggetti che sottovalutano molto il fenomeno, lo credono lontano dalla loro attività e credono di essere sufficientemente sicuri e non si preoccupano di questi rischi. C'è a volte anche un po' di supponenza e diventano più disponibili solo dopo aver subito il danno e aver avuto qualche tipo di problema.

D: *Lei si riferisce quindi ad iniziative di categoria?*

R: Sì, la Confcommercio aveva fatto incontri di questo tipo, a volte anche altre associazioni, ma sporadicamente. C'è stato un Questore a Firenze anni fa che spesso organizzava incontri con tutte le associazioni di categoria e la Polizia e si discuteva di quello che erano i rischi a 360 gradi. Il collega della mobile magari rappresentava i rischi di truffe fatte in un certo modo, noi i rischi di natura informatica, ecc. Ci sono state anche delle iniziative di questo tipo.

D: *Che grado di condivisione esiste, tra le aziende e all'interno delle categorie di settore, delle informazioni inerenti i rischi in ambito cyber?*

R: Non credo ne abbiano. A me non si è mai verificato nessun caso in cui un'azienda si sia rivolta a noi dicendo "so che lo stesso problema l'ha avuto anche Tizio o Caio" o "so che l'ho avuto solo io e Caio no." Non mi è mai capitato di constatare che tra loro dialoghino molto, anzi. Forse per quanto riguarda l'aspetto strettamente economico di un settore come può essere quello bancario sì. Anche perché le associazioni bancarie promuovono questo tipo di condivisione. Ma le altre

categorie no, a Firenze per esempio c'è tutta la filiera del tessile, ma non vi è alcun tipo di condivisione.

D: *La caratteristica delle imprese italiane è proprio quella del Made in Italy. Avete avuto casi che riguardassero questo aspetto delle PMI?*

R: Più che furto di brevetti noi abbiamo avuto ultimamente casi di furto di immagine nel settore del turismo riguardanti aziende turistiche della zona. Le immagini di proprietà di alcune aziende turistiche, agriturismi ecc., certificate di loro proprietà, pubblicate nei loro siti, venivano poi rubate e pubblicate da terzi. La sottrazione di brevetti invece capitò tempo fa nei confronti di un'azienda farmaceutica. Un gruppo di ex dipendenti aveva costituito un'altra società e aveva iniziato a produrre un farmaco brevettato dall'azienda principale con relativa sottrazione di dati di clienti ecc. Un grosso danno.

D: *E nel comparto moda?*

R: Sì, è capitato tempo fa con una nota azienda di moda della zona, che però essendo ben strutturata ha un reparto che si occupa di questo, ha i suoi ispettori interni e fa' controlli a tappeto e laddove ha sentore di una violazione più che nel penale vanno nel civile. Perché in realtà la sottrazione del brevetto, a meno che non venga fatto con modalità che hanno rilevanza penale, ha di solito rilevanza civilistica, quindi a me non lo vengono a rappresentare. È più facile che questo dato lo abbia la Camera di Commercio. La Camera di Commercio può sapere di azioni che sono state attivate ecc. Da me possono venire se il brevetto è stato sottratto con un accesso abusivo, ma raramente avviene, per brevetti di grosso calibro, che vengano tenuti alla *mercé* di tutti o siano informatizzati.

D: *Avete registrato casi di attivismo?*

R: No, non li abbiamo registrati. Diciamo che Anonymous ha attaccato noi in qualche occasione. Cioè il Ministero degli Interni diffondendo poi dei dati. O effettuato defacement con la prima pagina in lingua araba, ma cose così, senza altri danni.

D: *Ci può illustrare un caso che l'ha colpita particolarmente in questi ultimi anni?*

R: Ricordo bene di un'azienda fiorentina che aveva subito il fenomeno del phishing mirato, ma per grossi importi, e siamo riusciti ad individuare dei soggetti rumeni, con la collaborazione della Polizia rumena. Ovviamente il problema fu' che loro avevano avuto la percezione di quello che era stato il danno subìto in ritardo, non sempre la Banca ti avverte, o quando lo fa' di solito il danno economico c'è già stato. Erano soggetti che avevano carpito, attraverso l'accesso ai database della Banca, le credenziali dell'azienda e si erano proprio impadroniti dei loro conti correnti e facevano transazioni *random*. Si parlava di cifre molto grosse e qualcuna è stato poi possibile stopparla, altre no perché essendo una medio grossa società le movimentazioni di grosse cifre non appaiono

strane. Non sempre la Banca ti chiede subito riscontro di quello che fai. Passa un po' di tempo, ma anche 15 giorni in questi casi sono preziosi perché quei dati non sono più recuperabili. In quel caso individuammo questi soggetti rumeni, la Romania fa parte della Comunità europea, quindi siamo riusciti a muoverci abbastanza velocemente. Ma è stato un caso abbastanza raro. Raramente l'azienda se ne accorge. Quando vai a muoverti e fare una attività investigativa non c'è più niente dove andare ad investigare. La velocità è fondamentale in questo tipo di reati. È difficilissimo. Se ci si muove subito è possibile fare qualcosa, altrimenti no.

D: *Che tipo di strumenti lei ritiene siano più necessari per contrastare questo tipo di fenomeno, secondo la sua esperienza?*

R: La conoscenza umana. Assolutamente. Anche perché molto si basa sul *social engineering*. Uomo contro uomo. È vero che c'è una macchina di mezzo, ma c'è un uomo davanti a quella macchina. Io penso che sia fondamentale la preparazione dell'utente, del cliente, del dipendente. In primis la consapevolezza dei rischi che si corrono. Poi preparare anche l'ultimo dei propri dipendenti a fronteggiare determinati rischi, per non fare sciocchezze come l'accesso a siti che possono essere dannosi, possono installare dei virus, una sorta di consapevolezza ed educazione del mezzo informatico, perché c'è la presunzione che questo mezzo sia facilmente gestibile. È fuorviante, perché ti dà la possibilità di fare tutto subito. Il sistema informatico è grandioso, veramente, ti permette di fare delle cose stupefacenti, io credo che sia davvero una cosa stupenda, però devi anche approcciarti con un po' di malizia e non affidarti ad occhi chiusi.

D: *L'uso dei social network infatti credo sia strategico in questo campo.*

R: Sì, infatti su quello facciamo molta attività nelle scuole perché i ragazzi non hanno assolutamente percezione di quelli che sono i rischi che corrono nel dare informazioni del tipo "oggi andiamo in vacanza e a casa non ci rimane nessuno" oppure "questo è il mio numero di telefono e abito qui" e farsi trovare un qualche malintenzionato sotto casa, perché poi questo è quello che succede. E la stessa cosa succede anche con le aziende.

BIBLIOGRAFIA

Ablon L., (2014) "*Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*", in <http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf> (ultima consultazione 6-11-2014)

AIDiM, ANVED, eCircle (2012), *Quanto è "Social" la tua Azienda?*, in <www.slideshare.net/kornfeind/quanto-social-la-tua-azienda> (ultima consultazione 7-11-2014)

Audiweb (2014), *Audiweb pubblica i dati dell'audiencemobile e della total digital audience del mese di agosto 2014*, in <http://www.audiweb.it/wp-content/uploads/2014/08/Audiweb_CS_TotalDigitalAudience_07082014.pdf> (ultima consultazione 7-11-2014)

Biondi A. (2014), *Agcom: bene 3 Italia e Fastweb. Ed è boom per Lycamobile*, in "Il Sole 24 Ore" 7 ottobre 2014, in <http://www.ilsole24ore.com/art/impresa-e-territori/2014-10-07/dati-agcom-bene-3-italia-e-fastweb-ed-e-boom-lycamobile-173237.shtml?uuid=ABdmQx0B> (ultima consultazione 8-11-2014)

Bodnar C. (2014), *Kaspersky Mobile Malware Evolution: 2013,* 24 febbraio, in <https://blog.kaspersky.com/mobile-malware-evolution-2013/> (ultima consultazione 6-11-2014)

Cabinet Office and The Rt Hon Francis Maude MP (2013), *Government launches information sharing partnership on cyber security*, 27 marzo, Keeping the UK safe in cyber space and National security, in <https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security> (ultima consultazione 6-11-2014)

Cencetti C., (2014), *Cybersecurity: Unione Europea e Italia Prospettive a confronto,* Quaderni IAI, Edizioni Nuova Cultura

Cheslow D. (2012), *Interpol Ups The War Against Cyber Crime*, in "Huffingtonpost", 5 agosto, in <http://www.huffingtonpost.com/2012/05/08/Interpol-cyber-crime_n_1499734.html> (ultima consultazione 6-11-2014)

CISCO (2014), *Annual 2014 Security Report*, pagina 10, in <http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf> (ultima consultazione 6-11-2014)

CloudEntr (2014), *2015 State of SMB Cybersecurity*, in <https://app.box.com/s/2mf328i6a7j0z2tbdv07?src=undefined> (ultima consultazione 15-11-2014)

Commissione Europea (2003), *Raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese, testo integrale dell'atto*, GU L 124 del 20 maggio 2003, in <http://europa.eu/legislation_summaries/enterprise/business_environment/n26026_it.htm> (ultima consultazione 1-11-2014)

Commissione Europea (2006), *La nuova definizione di PMI. Guida dell'utente e modello di dichiarazione. Pubblicazioni della direzione generale per le imprese e l'industria*, in <http://ec.europa.eu/enterprise/policies/sme/files/sme_definition/sme_user_guide_it.pdf> (ultima consultazione 1-11-2014)

Commissione Europea (2009), Proteggere le infrastrutture critiche informatizzate. *"Rafforzare la preparazione, la sicurezza e la resilienza per proteggere l'Europa dai ciberattacchi e dalle ciberperturbazioni*" COM (2009) 149, 30 marzo 2009, in <http://europa.eu/legislation_summaries/information_society/internet/si0010_it.htm> (ultima consultazione 20-11-2014)

Commissione Europea (2010), *La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura*, Bruxelles 22 novembre, in <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:IT:PDF> (ultima consultazione 6-11-2014)

Commissione Europea (2011), Commissione relativa alla protezione delle infrastrutture critiche informatizzate *"Realizzazioni e prossime tappe: verso la sicurezza informatica mondiale"* COM (2011) 163, 31 marzo 2011, in <http://ec.europa.eu/transparency/regdoc/rep/1/2011/IT/1-2011-163-IT-F1-1.Pdf> (ultima consultazione 20-11-2014)

Commissione Europea (2012), *Un progetto pilota consente di rafforzare la sicurezza informatica delle istituzioni europee*, Comunicato stampa 12 settembre, in <http://europa.eu/rapid/press-release_IP-12-949_it.htm> (ultima consultazione 6-11-2014)

Commissione Europea (2013), *A recovery on the horizon? Annual Report on European SMEs 2012/2013,* in <http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/performance-review/files/supporting-documents/2013/annual-report-smes-2013_en.pdf> (ultima consultazione 11-11-2014)

Commissione Europea (2013), Cyber Security Report Special Eurobarometer 404, *in <http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf > (ultima consultazione 6-11-2014)*

Commissione Europea (2013), *Enterprise and Industry 2013 SBA Fact Sheet ITALY*, in <http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/performance-review/files/countries-sheets/2013/italy_en.pdf> (ultima consultazione 6-11-2014)

Commissione Europea (2013), *Eurobarometer Special Surveys, Cyber security Report*, in <http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_fact_it_it.pdf> (ultima consultazione 7-11-2014)

Commissione Europea (2013), *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,* 7 febbraio, in <http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf> (ultima consultazione 6-11-2014)

Commissione Europea (2013), *Proposta di Direttiva del Parlamento europeo e del Consiglio recante misure volte a garantire un livello comune elevato di sicurezza delle reti e dell'informazione nell'Unione*, 7 febbraio, in <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0048:FIN:IT:PDF> (ultima consultazione 20-11-2014)

Commissione Europea (2014), *Implementation of the Digital Agenda for Europe. Actions under the responsibility of Member States. Dashboard,* in <http://daeimplementation.eu/dashboard2.php> (ultima consultazione 9-11-2014)

Consiglio d'Europa (2001), *Convention on Cybercrime,* Budapest, 23.XI.2001, in <http://conventions.coe.int/Treaty/en/Treaties/PDF/Italian/185-Italian.pdf> (ultima consultazione 6-11-2014)> (ultima consultazione 6-11-2014)

Consiglio d'Europa (2003), *Protocollo addizionale alla Convenzione sulla criminalità informatica, relativo all'incriminazione di atti di natura razzista e xenofobica commessi a mezzo di sistemi informatici*, 28 gennaio, in <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ITA&CM=8&NT=189> (ultima consultazione 6-11-2014)

Consiglio d'Europa (2008), *"Think Small First" A "Small Business Act" for Europe*, 25 giugno, in <http://europa.eu/rapid/press-release_IP-08-1003_en.htm> (ultima consultazione 6-11-2014)

COPASIR (2010), *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico*, 7 luglio 2010, in <http://www.senato.it/service/PDF/PDFServer/BGT/525461.pdf> (ultima consultazione 9-11-2014)

CSES (2012), *Evaluation of the SME Definition September 2012, Final Report Framework*, Center for Strategy & Evaluation Services, in <http://ec.europa.eu/enterprise/policies/sme/files/studies/evaluation-sme-definition_en.pdf> (ultima consultazione 6-11-2014)

CSIS (2014), *2014 McAfee Report on the Global Cost of Cybercrime*, giugno, in <http://csis.org/event/2014-mcafee-report-global-cost-cybercrime> (ultima consultazione 6-11-2014)

Decreto convertito in legge 134 del 7 agosto 2012, *Conversione in legge, con modificazioni, del decreto-legge 22 giugno 2012, n. 83, recante misure urgenti per la crescita del Paese*. (GU n. 187 del 11-8-2012)

Decreto del Ministero dell'Interno del 9 gennaio 2008 in attuazione della legge 31 luglio 2005 n° 155. *Individuazione delle infrastrutture critiche informatiche di interesse nazionale*

Decreto legislativo n° 61 11 aprile 2011, del Presidente della Repubblica. *Attuazione della Direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione*. (GU n. 102 del 4-5-2011)

Decreto legislativo 28 maggio 2012, n. 70 *Modifiche al decreto legislativo 1° agosto 2003, n. 259* (GU Serie Generale n.126 del 31-5-2012)

Decreto legge 179 del 18 ottobre 2012, *Ulteriori misure urgenti per la crescita del Paese*. (GU n.245 del 19-10-2012 - Suppl. Ordinario n. 194)

Department for Business, Innovation & Skills Cabinet Office (2014), *Cyber essentials scheme*: *overview*, in <https://www.gov.uk/government/publications/cyber-essentials-scheme-overview> (ultima consultazione 6-11-2014)

Di Corinto A. (2014), *Tutti i segreti del deep web,* in "Repubblica.it" 20 aprile, in <http://www.repubblica.it/tecnologia/2014/04/20/news/tutti_i_segreti_del_deep_web-84053410/> (ultima consultazione 11-11-2014)

Digital Agenda for Europe (2014), *A Europe 2020 Initiative*, in <http://ec.europa.eu/digital-agenda/digital-agenda-europe> (ultima consultazione 6-11-2014)

Direttiva 2013/40/UE del Parlamento Europeo e del Consiglio del 12 agosto 2013 relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio, in <http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32013L0040> (ultima consultazione 6-11-2014)

Dunn J.E. (2013), *Ransomware criminals attack SMEs using strong file encryption, ESET warns Summer surge in complex attacks*, in "Techworld", 24 settembre, <http://news.techworld.com/security/3470388/ransomware-criminals-attack-smes-using-strong-file-encryption-eset-warns/> (ultima consultazione 1-11-2014)

EC3 (2014)*, The Internet Organised Crime Threat Assessment (iOCTA) 2014*, in <https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web.pdf> (ultima consultazione 6-11-2014)

EISAS (2007), *European Information Sharing and Alert System A Feasibility Study 2006/2007*, in <http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/files/EISAS_finalreport.pdf> (ultima consultazione 1-11-2014)

EISAS (2011), *Basic Toolset 1.0 Feasibility Study of Home Users' IT Security*, in <http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas-basic-toolset/at_download/fullReport> (ultima consultazione 6-11-2014)

EMC (2013), *The Year in Phishing*, gennaio, in <http://www.emc.com/collateral/fraud-report/online-rsa-fraud-report-012013.pdf> (ultima consultazione 6-11-2014)

ENISA (2007) *Deliverable: Information Package for SMEs*, febbraio, in <http://www.enisa.europa.eu/act/rm/cr/risk-management-inventory/files/deliverables/information-package-for-smes/at_download/fullReport> (ultima consultazione 6-11-2014)

ENISA (2013), Threat *Landscape 2013 Overview of current and emerging cyber-threats,* 11 dicembre, in <https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats/at_download/fullReport> (ultima consultazione 6-11-2014)

ENISA (2014), *Annual Incident Reports 2013 Analysis of Article 13a annual incident reports September 2014*, in <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2013/at_download/fullReport> (ultima consultazione 6-11-2014)

ENISA (2014), *Biggest ever cyber security exercise in Europe today*, in <http://www.enisa.europa.eu/media/press-releases/biggest-ever-cyber-security-exercise-in-europe-today> (ultima consultazione 6-11-2014)

EUROPOL (2011), *Threat Assessment on Internet Facilitated Organised Crime (iOCTA) 2014*, 7 gennaio, in <https://www.europol.europa.eu/sites/default/files/publications/iocta_0.pdf> (ultima consultazione 6-11-2014)

Federal Ministry of Education and Research (2014)*, Cybersecurity research to boost Germany's competitiveness*, in <http://www.bmbf.de/en/73.php> (ultima consultazione 6-11-2014)

Garante PMI (2014), *Relazione al Presidente del Consiglio articolo 17, comma 1, legge 11-11-2011 n. 180 "Norme per la tutela della libertà d'impresa. Statuto delle Imprese"*, Roma 6 febbraio, in <http://www.governo.it/backoffice/allegati/75045-9261.pdf> (ultima consultazione 7-11-2014)

Gartner (2012), *Gartner Says Worldwide Mobile Payment Transaction Value to Surpass $171.5 Billion,* 29 maggio, in <https://www.gartner.com/newsroom/id/2028315> (ultima consultazione 6-11-2014)

GCHQ (2012), *10 Steps to Cyber Security Executive Companion CESG The Information Security Arm of GCHQ*, in <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/73128/12-1120-10-steps-to-cyber-security-executive.pdf> (ultima consultazione 6-11-2014)

Global Cybersecurity Center (2013), *On-line Fraud Cyber Centre and Experts Network (OF2CEN)*, in <http://www.gcsec.org/activity/research/online-fraud-cyber-centre-and-experts-network-of2cen > (ultima consultazione 10-11-2014)

Gori Umberto (2012) "*Riflessioni propedeutiche alla cyber intelligence"* in "*Information Warfare 2011. La sfida della Cyber Intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale"* a cura di Umberto Gori e Luigi Sergio Germani, Franco Angeli Editore

Guardia di Finanza (2014), *Intervento Comandante Reda Nucleo Speciale Frodi Tecnologiche*, in <http://www.aracneeditrice.it/scaricabili/interventoreda.pdf> (ultima consultazione 7-11-2014)

Iacono N. (2014), *Sicurezza delle reti in Europa: il punto sui ritardi,* in "Agenda Digitale", 13 marzo, in <http://www.agendadigitale.eu/infrastrutture/718_sicurezza-delle-reti-in-europa-il-punto-sui-ritardi.htm> (ultima consultazione 6-11-2014)

IC3 (2013), *2013 Internet Crime Report*, in <https://www.ic3.gov/media/annualreport/2013_ic3report.pdf> (ultima consultazione 6-11-2014)

IDC (2014), *Worldwide Quarterly Mobile Phone Tracker,* gennaio, in <http://www.idc.com/tracker/showproductinfo.jsp?prod_id=37> (ultima consultazione 6-11-2014)

INTERPOL (2012), *Speech Opening remarks by INTERPOL President Khoo Boon Hui* at the 41ST European Regional Conference. Israele, Tel Aviv, 8 maggio, in <http://www.Interpol.int/content/download/14086/99246/version/1/file/41ERC-Khoo-Opening-Speech.pdf> (ultima consultazione 6-11-2014)

ITsecurity (2014), *Europol, FBI, NCA and others disrupt the Gameover Zeus botnet — claim a 2 week window for users to get clean,* in <http://itsecurity.co.uk/2014/06/774/> (ultima consultazione 6-11-2014)

Kaspersky Lab (2014), *IT Security Risks Survey 2014: A Business Approach to Managing Data Security Threats*, in <http://media.kaspersky.com/en/IT_Security_Risks_Survey_2014_Global_report.pdf> (ultima consultazione 6-11-2014)

Kaspersky Lab (2014), *Security Network Report: Windows usage & vulnerabilities Version 1.0*, agosto, in <https://securelist.com/files/2014/08/Kaspersky_Lab_KSN_report_windows_usage_eng.pdf> (ultima consultazione 6-11-2014)

Kaspersky Security Network (2014), *16.37% Users Still Run Windows XP, Kaspersky Lab Statistics Say*, 19 Agosto, in <http://www.kaspersky.com/about/news/virus/2014/16-37-per-cent-Users-Still-Run-Windows-XP-Kaspersky-Lab-Statistics-Say> (ultima consultazione 6-11-2014)

Kroes N.(2014), *A secure on-line network for Europe Cyber security conference*, Brussels 28 febbraio, in <http://europa.eu/rapid/press-release_SPEECH-14-167_en.htm> (ultima consultazione 6-11-2014)

McAfee (2014), *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II Center for Strategic and International Studies,* giugno, in <http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf> (ultima consultazione 6-11-2014)

McDonald E. (2013), *On-line fraud costs global economy 'many times more than $100bn'*, in "The Guardian", 30 ottobre, in <http://www.theguardian.com/technology/2013/oct/30/online-fraud-costs-more-than-100-billion-dollars> (ultima consultazione 6-11-2014)

Mick J*., Anonymous Engages in Sony DDoS Attacks Over GeoHot PS3 Lawsuit*, in "Daily Tech" 4 aprile 2011 <http://www.daiytech.com/Anonymous+Engages+in+Sony+DDoS+Attacks+Over+GeoHot+PS3+Lawsuit/article21282.htm> (ultima consultazione 6-11-2014)

MISE (2003), *Decreto interministeriale 14 gennaio 2003 - Istituzione Osservatorio permanente per la sicurezza e la tutela delle reti e delle telecomunicazioni*, in <http://www.mise.gov.it/index.php/it/?option=com_content&view=article&idmenu=1620&idarea1=0&idarea2=0&idarea3=0&andor=AND&sectionid=0&andorcat=AND&MvediT=1&cattitle1=Decreti%20interministeriali&partebassaType=0&showMenu=1&showCat=1&idarea4=0&idareaCalendario1=0&page=15&id=2017545&viewType=0> (ultima consultazione 9-11-2014)

OPMI (2014), *Empowering the knowledge of small and medium enterprises management,* Divisione ricerche Claudio Dematté Osservatorio sulla competitività delle PMI, 10 Luglio 2014, SDA Bocconi, in <http://www.sdabocconi.it/sites/default/files/upload/pdf/report_PMI_10_luglio_2014.pdf> (ultima consultazione 7-11-2014)

Paganini P. (2013), *Cost of cybercrime for UK Small Businesses*, in "Security Affairs", 23 maggio 2013, in <http://securityaffairs.co/wordpress/14628/cyber-crime/cost-of-cybercrime-for-uk-small-businesses.html> (ultima consultazione 6-11-2014)

Parlamento Italiano (1998), *Legge 3 agosto 1998, n. 269, Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù* , *GU* n. 185 del 10 agosto 1998, in <http://www.camera.it/parlam/leggi/98269l.htm> (ultima consultazione 9-11-2014)

Parlamento Italiano (2008), Legge n° 48 del 18 marzo 2008 "*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno"* (GU n. 80 del 4 aprile 2008 - Supplemento ordinario n. 79), in <http://www.camera.it/parlam/leggi/08048l.htm> (ultima consultazione 1-11-2014)

Perlroth N. (2014), *Home Depot Says Hackers Also Stole Email Addresses*, in "The New York Times" 6 novembre, in <http://bits.blogs.nytimes.com/2014/11/06/home-depot-says-hackers-also-stole-email-addresses/?_r=0> (ultima consultazione 7-11-2014)

Polizia di Stato (2014), *Relazione annuale 2014 della Polizia Postale e delle Comunicazioni*, fornita per questa ricerca dal Vicequestore di Firenze, dott.ssa Stefania Pierazzi

Ponemon Institute (2013), *2013 Cost of Cyber Crime Study: United States*, in <http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf> (ultima consultazione 6-11-2014)

Ponemon Institute (2014), *Exposing the Cybersecurity Cracks:A Global PerspectivePart IWebsense*, aprile, in <https://www.websense.com/assets/reports/report-ponemon-2014-exposing-cybersecurity-cracks-en.pdf> (ultima consultazione 7-11-2014)

Presidenza del Consiglio dei Ministri, Dipartimento per l'Innovazione e le Tecnologie (2002) , *DIRETTIVA 16 gennaio 2002. Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni,* GU Serie Generale n.69 del 22-3-2002, in <http://www.gazzettaufficiale.it/eli/id/2002/03/22/02A03219/sg%20;jsessionid=nBvFj9k-8FcOCREFNlFaag__.ntc-as1-guri2a> (ultima consultazione 9-11-2014)

Presidenza del Consiglio dei Ministri (2013), *Quadro Strategico Nazionale per la Sicurezza dello spazio cibernetico*, dicembre, in <http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/quadro-strategico-nazionale-cyber_0.pdf> (ultima consultazione 9-11-2014)

PR Web (2014), *SMEs face increased risk of cyber attack*, 8 settembre, in <http://www.prweb.com/releases/2014/09/prweb12147240.htm> (ultima consultazione 6-11-2014)

PwC (2013), *Information Security Breaches Survey Technical Report,* in <https://www.pwc.co.uk/assets/pdf/cyber-security-2013-technical-report.pdf> (ultima consultazione 6-11-2014)

PwC (2014), *Global Economic Crime Survey. Le frodi economico-finanziariein Italia: una minaccia per il business Settima edizione,* in <http://www.pwc.com/it/it/services/forensic/assets/docs/gecs-2014.pdf> (ultima consultazione 7-11-2014)

Quadrio Curzio A. e Fortis M. (2002, a cura di), *Complessità e Distretti Industriali. Dinamiche, Modelli, Casi reali*, Il Mulino, Bologna

Reynolds K. (2013)*, CryptoLocker Virus. Best Practices to Ensure 100% Immunity***,** 25-10-2013, in Comodo <https://blogs.comodo.com/it-security/cryptolocker-virus-best-practices-to-ensure-100-immunity/> (ultima consultazione 6-11-2014)

Ricciardi A. (2010), *Le Pmi localizzate nei distretti industriali: vantaggi competitivi, evoluzione organizzativa, prospettive future*, in Quaderni di ricerca sull'artigianato N°54 Rivista di Economia, Cultura e Ricerca sociale dell'Associazione Artigiani e Piccole Imprese Mestre CGIA A cura del Centro Studi Sintesi, in <http://www.quaderniartigianato.com/wp-content/uploads/2011/05/Quaderni-N%C2%B054.pdf> (ultima consultazione 11-11-2014)

Robinson N. (2013), *The European Cyber Security Strategy: Too Big to Fail?*, in <http://www.rand.org/blog/2013/02/the-european-cyber-security-strategy-too-big-to-fail.html> (ultima consultazione 6-11-2014)

Stempel J. (2014)*, Goldman says client data leaked, wants Google to delete email*, in "Reuters" 2 luglio, in <http://www.reuters.com/article/2014/07/02/us-google-goldman-leak-idUSKBN0F729I20140702> (ultima consultazione 6-11-2014)

Street Insider (2014), *The Home Depot Reports Findings in Payment Data Breach Investigation*, PRNewswire 6 novembre, in

<http://www.streetinsider.com/Press+Releases/The+Home+Depot+Reports+Findings+in+Payment+Data+Breach+Investigation/9986431.html> (ultima consultazione 7-11-2014)

Symantec (2009), *National Small Business Study*, National Cyber Security Alliance e Symantec, in <http://eagleintelligence.com/wp-content/uploads/2009/12/NCSA-SB-Study-Factsheet.pdf> (ultima consultazione 6-11-2014)

Symantec (2014), *Internet Security Threat Report 2014 Volume 19*, aprile, in <http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf> (ultima consultazione 6-11-2014)

TimesLive (2012), *India training half a million cyber security experts*, 16 ottobre, in <http://www.timeslive.co.za/scitech/2012/10/16/india-training-half-a-million-cyber-security-experts> (ultima consultazione 6-11-2014)

TrendMicro (2013), *Guadagnare sulle informazioni digitali*. *Verifica di sicurezza annuale*,TrendLabs, in <http://www.trendmicro.it/informazioni-sulla-sicurezza/ricerca/trendlabs-2013-annual-security-roundup/index.html> (ultima consultazione 7-11-2014)

UNODC (2013) *Comprehensive Study on Cybercrime,* Febbraio, in <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf> (ultima consultazione 15-11-2014)

Vanson Bourne (2014), *Emc Global Data Protection Index*, in <http://www.emc.com/microsites/emc-global-data-protection-index/index.htm#infographic-italy> (ultima consultazione 8-12-2014)

Verga M. (a cura di), *L'obbligatorietà dell'azione penale come un mito? Appunti sul caso italiano*, Centro Universitario per le Ricerche sulla Sociologia del Diritto, dell'Informazione e delle Istituzioni Giuridiche (CIRSDIG), in "Quaderno dei lavori 2007, Terzo Seminario Nazionale di Sociologia del Diritto, A.I.S. – Sezione di Sociologia del Diritto", Working Paper n. 25, 2007, pp. 121-136, in <http://www.cirsdig.it/Pubblicazioni/capraia.pdf> (ultima consultazione 11-11-2014)

Verizon (2014), *2014 Data Breach Investigation Report,* in <http://www.verizonenterprise.com/DBIR/2014/reports/rp_dbir-2014-executive-summary_en_xg.pdf> (ultima consultazione 15-11-2014)

Wagaman A. (2012), *Europe tests cyber security capabilities in simulation*, in "NewEurope" 4 ottobre 2012, in <http://www.neurope.eu/article/europe-tests-cyber-security-capabilities-simulation-today> (ultima consultazione 6-11-2014)

Wagner K. (2013)*, More Than 70% of Email Is Spam*, Kaspersky Lab, in <http://usa.kaspersky.com/about-us/press-center/in-the-news/more-70-email-spam> (ultima consultazione 6-11-2014)

WEF (2012), *Risk and Responsibility in a Hyperconnected World. Pathways to Global Cyber Resilience*, in <http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf> (ultima consultazione 6-11-2014)
WEF (2014), *Global risks 2014 Ninth edition*, in <http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf> (ultima consultazione 6-11-2014)

Zanier M. (2009), *Tra il dire e il fare. Obbligatorietà dell'azione penale e comportamenti degli attori giuridici*, Macerata, EUM Edizioni, Università di Macerata

Zetter K. (2013), *Feds Arrest Alleged 'Dread Pirate Roberts,' the Brain Behind the Silk Road Drug Site* in "Wired" 10 febbraio 2013, in <http://www.wired.com/2013/10/silk-road-raided/> (ultima consultazione 6-11-2014)