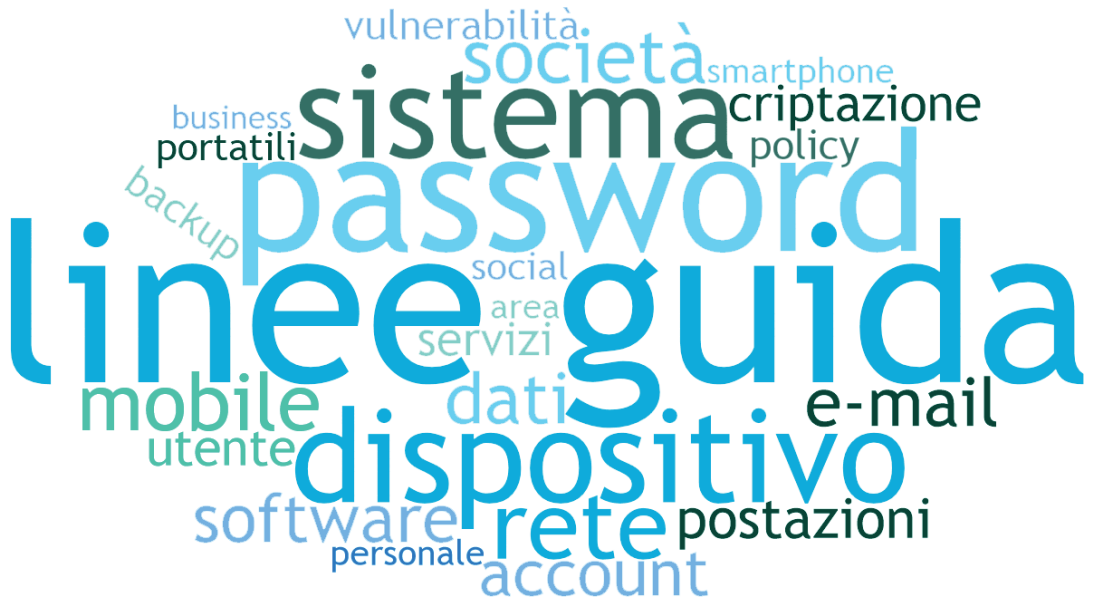
LINEE GUIDA PER LA SICUREZZA INFORMATICA NELLE PMI



United Nations Interregional Crime and Justice Research Institute

Fondazione Cassa di Risparmio di Lucca

United Nations
Interregional Crime and Justice
Research Institute

Linee guida per la sicurezza informatica nelle PMI

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

Disclaimer

Le opinioni espresse in questo studio rappresentano il punto di vista dell'autore e non riflettono necessariamente le posizioni dell'UNICRI, e in generale delle Nazioni Unite. Il contenuto della pubblicazione può essere citato o riprodotto purché la fonte sia specificata.
Il fatto che nel rapporto possano essere menzionate istituzioni o compagnie non significa che esse siano appoggiate o raccomandate dall'UNICRI, o che si esprima una preferenza rispetto ad altre entità che non sono menzionate.

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

Indice

Ringraziamenti 5

Executive summary 6

Lista degli acronimi 8

CAPITOLO 1 Panoramica sull'impatto del cyber crime in Italia: Primo semestre 2015 e trend 9

CAPITOLO 2 Indagine empirica sull'impatto del cyber crime in Italia: Interviste e casi studio 18

CAPITOLO 3 Linee guida per le PMI in tema di sicurezza informatica 28

Conclusioni 40

Indice delle figure 42

Metodologia 43

Bibliografia 44

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 Magistrato Giuseppe Corasaniti, il Sostituto Procuratore Vito Sandro Destito della Procura della Repubblica di Torino e l'avvocato Marco Tullio Giordano dello studio legale R&P di Milano, per la disponibilità a chiarire gli aspetti giuridico-normativi e procedurali di questo fenomeno. Inoltre si ringrazia il dott. Tanara e il dott. Bernardino Grignaffini di Certego per i dati fornitici.

Si ringraziano ancora tutte le aziende che hanno validato le linee guida redatte per le PMI, Fastweb nella figura del dott. Davide Del Vecchio, IBM nella figura del dott. Pier Luigi Rotondo, Kaspersky nella figura del dott. Giuseppe Vinucci, Microsoft nelle figure del dott. Andrea Piazza e del dott. Carlo Mauceli., la Lucense nella figura di Luca Landucci, la Lucart nella figura del dott. Alessandro Burresi e la Tagetik nelle persone di Matteo Fava e del dott. Santo Natale.

Un ringraziamento va inoltre alla dott.ssa Marilina Labia di Si.Camera, al dott. Tocci di Unindustria e a Rossano Rogani. Si ringrazia infine la dott.ssa Monica Pellegrino di ABI Lab, per i dati forniti e la collaborazione dimostrata.

Executive summary

La sicurezza informatica nel mondo delle Piccole e Medie Imprese (PMI) rappresenta una delle sfide più importanti per l'economia europea e nazionale. In quest'ottica è necessario mettere in atto una serie di azioni proattive per aumentare la sensibilità nei confronti di questo tema.

La presente ricerca costituisce il primo aggiornamento dello studio: "*La criminalità informatica e i rischi per l'economia e le imprese a livello italiano ed europeo*" pubblicato a dicembre 2014 da UNICRI, nel quale si è indagato sulla reale situazione in cui versano le PMI italiane in questo settore.

Le PMI, costituendo il 99,8% delle imprese europee e il 99,9% di quelle italiane, con un impatto in termini occupazionali di 86,8 milioni di persone occupate in tutta Europa, sono l'asse portante dell'economia nazionale ed europea, ma posso costituire al contempo un anello debole in termini di sicurezza. Come già emerso nella precedente ricerca quando una PMI viene attaccata non viene lesa solo la singola azienda, ma l'intero sistema Paese che si fonda in gran parte su questa realtà economica.

L'indagine svolta nel 2014 infatti evidenziava come il livello di percezione e conoscenza della minaccia informatica e le relative contromisure messe in atto da parte delle PMI siano ancora molto basse. Nel precedente studio è stata dedicata una sezione alle varie tipologie di minacce e attacchi di tipo informatico che le aziende si possono trovare ad affrontare e si sono realizzate numerose interviste ad enti istituzionali come le Procure e la Polizia Postale e principalmente a PMI, per indagare sulle loro reali esigenze e sulle lacune che hanno nei confronti della sicurezza informatica.

Questa prima integrazione si concentrerà su un aggiornamento dei dati e dei trend relativi al primo semestre 2015 inerenti il cyber crime, sull'analisi di casi studio sul territorio nazionale e sulla stesura di linee guida per la sicurezza informatica per le PMI, che si ritiene possano essere d'aiuto per colmare i gap emersi durante la precedente indagine. L'esigenza di dare un indirizzo che assista le PMI nell'individuazione e nella definizione delle proprie linee guida nasce dall'analisi dei risultati delle interviste qualitative condotte presso le aziende coinvolte durante la precedente ricerca.

Le linee guida stilate sono state poi sottoposte e validate da esperti del settore di aziende leader come Fastweb, IBM, Kaspersky e Microsoft e dai responsabili IT di tre delle aziende più strutturate e consapevoli tra quelle intervistate nel precede studio: Lucart,

Lucense e Tagetik. Il cyber crime è un fenomeno che non risparmia nessuna tipologia di azienda e nessuna zona d'Italia, quindi non può che richiedere non solo una risposta in termini di conoscenza e prevenzione da parte di ogni singola azienda, ma soprattutto una risposta a livello nazionale. A tal fine, in questa integrazione sono state inserite le opinioni a riguardo di esponenti delle istituzioni.

Lista degli acronimi

AIPSI	Associazione Italiana Professionisti Sicurezza Informatica
APT	*Advanced Persistent Threat*
BIS	*Department for Business and Innovation Skills*
BYOD	*Bring your own device*
C&C	*Command and Control*
CMS	*Content Management System*
DDL	Disegno Di Legge
DDoS	*Distributed Denial of Service*
EBA	*European Bank Authority*
EC3	*European Cybercrime Centre*
ENISA	*European Union Agency for Network and Information Security*
EU	*European Union*
IoT	*Internet of Things*
IT	*Information Technology*
MaaS	*Malware-as-a-Service*
PMI	Piccole e Medie Imprese
POS	*Point of Sale*
PwC	*PricewaterhouseCoopers*
UNICRI	*United Nations Interregional Crime and Justice Research Institute*
WEF	*World Economic Forum*

CAPITOLO 1

Panoramica sull'impatto del cyber crime in Italia: Primo semestre 2015 e trend

Il cyber crime è una minaccia sempre maggiore per i cittadini e l'economia a livello mondiale e rappresenta un'enorme fonte di guadagno per le organizzazioni criminali. Insieme al terrorismo e al crimine organizzato la criminalità informatica costituisce una delle priorità fondamentali per l'Agenda Europea sulla sicurezza[1]. Il nuovo rapporto[2] del World Economic Forum (WEF) sui rischi a livello globale conferma come gli attacchi cyber rimangano tra i maggiori rischi sia in termini di impatto sia di probabilità di verificarsi.

Mentre aumenta sensibilmente ogni anno il budget che le grandi aziende stanziano per il contrasto al cyber crime, le PMI fanno ancora molta fatica a percepirlo come un rischio reale per il loro business e la loro sopravvivenza sul mercato. Dati Gartner[3] rivelano che il 40% delle grandi aziende entro il 2018 avrà adottato sistemi di sicurezza utili a difendersi dagli attacchi informatici. Le piccole e medie imprese rappresentano invece obiettivi "facili" in quanto poco difese, inconsapevoli dei rischi, e spesso neanche in grado di rilevare la portata dei furti subiti. Inoltre le PMI che collaborano con grandi aziende per realizzare singole parti di progetti più complessi costituiscono una via più semplice per i cyber criminali per raggiungere l'obiettivo finale.

1 Communication from the commission to the European Parliament, The Council, The European economic and social committee and the committee of the region, The European Agenda on Security, Commissione Europea, Strasburgo, 28-04-2015, in <http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf> (ultima consultazione 09-06-2015)

2 The Global Risks 2015 10th Edition, World Economic Forum, in <http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf> (ultima consultazione 06-05-2015)

3 Cybersecurity: il 40% delle grandi aziende pronte ad attacchi cyber nel 2018, di Lorenzo Sorbini, Key4biz, 24-02-2015, in <http://www.key4biz.it/cybersecurity-40-delle-grandi-aziende-pronte-ad-attacchi-cyber-nel-2018/> (ultima consultazione 21-05-2015)

Considerando i trend di crescita di questo tipo di minaccia, è quanto mai necessario incominciare a sviluppare sistemi di prevenzione e sicurezza informatica più efficienti. I pericoli a livello aziendale sono costituiti non solo dai danni prodotti dall'attacco in sé, ma soprattutto dalle conseguenze che questi attacchi causano anche nel lungo periodo. Assistiamo infatti sempre più ad attacchi di tipo mirato come l'appropriazione dei dati sensibili, la cancellazione dei dati stessi o il furto di materiale coperto da copyright. Oggigiorno questo tipo di attacchi può interrompere l'attività di un'azienda per diversi giorni o mesi, diminuirne la reputazione o metterne in crisi l'esistenza stessa. Con l'aumento dell'uso di strumenti informatici da parte di ogni tipo di PMI, le aziende risultano più deboli e attaccabili da più fronti.

L'allarme su questo fenomeno arriva anche da fonti autorevoli come il direttore dell'European Cybercrime Centre (EC3) Troels Oerting[4], secondo cui le imprese hanno bisogno di prendere seriamente la criminalità informatica in quanto sono tutte suscettibili di subire cyber attacchi. La criminalità informatica inoltre è più forte e diffusa di quanto si possa pensare, dato che la maggior parte degli attacchi non viene ancora rilevata e denunciata. Le perdite dovute al cyber crime possono anche arrivare a diversi milioni di euro per le singole aziende. Solo le imprese che investono in processi, procedure e nelle tecnologie giuste potranno avere benefici nel lungo periodo in termini di sicurezza, di reputazione e di profitto.

Ormai è un dato di fatto che le PMI siano un bersaglio molto attraente per i cyber criminali e che purtroppo sottovalutino ancora troppo questa minaccia. Una recente ricerca del governo britannico afferma che più dei due terzi delle PMI non ha mai pensato di poter essere vittima del cyber crime[5]. La realtà invece sembra essere un'altra: da un report pubblicato da PwC/BIS[6] emerge che il 60% delle PMI prese in esame aveva subito una violazione informatica. Non importa quale sia il business di una PMI, ogni azienda è appetibile per un cyber criminale. Qualsiasi informazione di tipo commerciale, dati personali, indirizzi e-mail, know-how ecc. è vendibile al mercato nero per commettere frodi, per diffondere malware e per mettere in atto altri crimini.

Nel 2014 a causa di attacchi su larga scala sono stati compromessi un miliardo di record[7], quindi in media uno ogni tre utenti di internet. Molti di questi erano totalmente in chiaro e quindi facilmente sfruttabili. Gli attacchi automatizzati sono ormai a buon mercato e

4 Top 10 cyber crime stories of 2014, di Warwick Ashford, Computerweekly, 31-12-2014, in <http://www.computerweekly.com/news/2240236215/Top-10-cyber-crime-stories-of-201> (ultima consultazione 28-04-2015)

5 Misunderstanding cyber threats puts a third of SME revenue at risk, di Neil Ford, 27-02-2015, in <http://www.itgovernance.co.uk/blog/misunderstanding-cyber-threats-puts-a-third-of-sme-revenue-at-risk/> (ultima consultazione 30-04-2015)

6 2014 Information Security Breaches Survey, Department for Business, Innovation and Skills Cabinet Office, in <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/307297/bis-14-766-information-security-breaches-survey-2014-executive-summary-revision1.pdf> (ultima consultazione 30-04-2015)

7 Why SMEs are an attractive target for cyber criminals and what they can do about it, di Neil Ford, 02-03-2015, in <http://www.itgovernance.co.uk/blog/why-smes-are-an-attractive-target-for-cyber-criminals-and-what-they-can-do-about-it/> (ultima consultazione 21-05-2015)

facili da gestire. Essendo indiscriminati, non hanno interesse a colpire una particolare azienda o un sito specifico, ma sfruttano vulnerabilità note e hanno come principale obiettivo quello di colpire più vittime possibili.

Quando viene scoperta una nuova vulnerabilità, il tempo nel quale i criminali riescono a sfruttarla prima che venga patchata è brevissimo. Nell'ottobre 2014, ad esempio, Drupal ha annunciato che gli utenti che non avevano patchato la loro piattaforma *Content Management System* (CMS) entro sette ore dalla scoperta di un bug, dovevano considerare violato il loro sito. La velocità di risposta è un fattore di rischio maggiore per le PMI, che spesso non hanno le risorse per affrontare questi attacchi automatizzati e per attuare una politica di gestione delle patch e di aggiornamento dei software così rapidamente come le grandi aziende, che possono contare invece su reparti IT preparati e su azioni proattive come *penetration test* e *vulnerability assessment*.

Da una recente ricerca del governo britannico all'interno della campagna *Cyber Streetwise* emerge che le PMI inglesi mettono a rischio un terzo dei loro ricavi tra perdita di dati, danni finanziari e reputazionali, sottovalutando il pericolo rappresentato dal cyber crime. Le PMI prese a campione ritengono che le misure di sicurezza siano troppo costose e spesso non sanno da dove cominciare. È necessario quindi un supporto in questo senso per cercare di mitigare i danni causati dal cyber crime e per sostenere le PMI verso un'organizzazione consapevole e crescente del proprio *asset* di sicurezza.

Un recente report di HP[8] rivela che il 44% delle violazioni avvenute nel 2014 hanno sfruttato vulnerabilità note che risalivano a 2-4 anni prima. Inoltre la principale falla sfruttata dai cyber criminali è rappresentata, sempre secondo i dati di questo studio, da errori di configurazione che hanno esposto inutilmente le aziende ad attacchi. Questo è un dato che dimostra non solo quanto sia ancora bassa la conoscenza in questo settore, ma soprattutto quanta superficialità ancora persista nella manutenzione degli apparati informatici aziendali.

Il Websense Security Labs ha rilasciato il *Threat Report 2015*, che evidenzia come sempre più spesso i criminali creino minacce sempre più avanzate e sofisticate, adottando strumenti all'avanguardia già esistenti e non sviluppandoli da zero. Nel mondo del cyber crime vengono infatti scambiati, affittati e venduti codici e programmi che sono alla base di nuove minacce. Aumenta notevolmente la rete di scambio di questi strumenti, permettendo così a criminali anche non molto capaci di sfruttare questo mezzo per atti criminosi, *Malware-as-a-Service* (MaaS). Ad esempio nel 2014 il 99,3% dei *Command and Control* (C&C) usati per i malware era già stato utilizzato in precedenza, e nel 98,2% dei casi erano già stati utilizzati più di 5 volte. Sempre secondo questo studio l'81% delle e-mail scansionate da Websense sono state considerate malevole.[9]

8 HP Cyber Risk Report 2015, HP, in <http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/> (ultima consultazione 01-05-2015)

9 Websense Threat Report 2015, fare cybercrime è sempre più facile, Websense Security Labs, 13-04-2015, in <http://www.techfromthenet.it/201504101252/News-analisi/websense-threat-report-2015-fare-cybercrime-e-sempre-piu-facile.html> (ultima consultazione 22-04-2015)

Secondo il Guardian[10], le minacce cyber che avranno nel 2015 il maggior trend di ascesa saranno, a livello generale, le *Advanced Persistent Threat* (APT) e lo spam sempre più sofisticato. Proprio riguardo lo spam, il dato più interessante è che pur diminuendo in misura assoluta il volume, la sua sempre maggiore sofisticatezza rende più difficile ai programmi antispam filtrare questi messaggi, con il risultato che l'utente se ne vede ricevere di più nella sua casella di posta, dato confermato anche dall'ultimo *Internet Security Threat Report*[11] di Symantec.

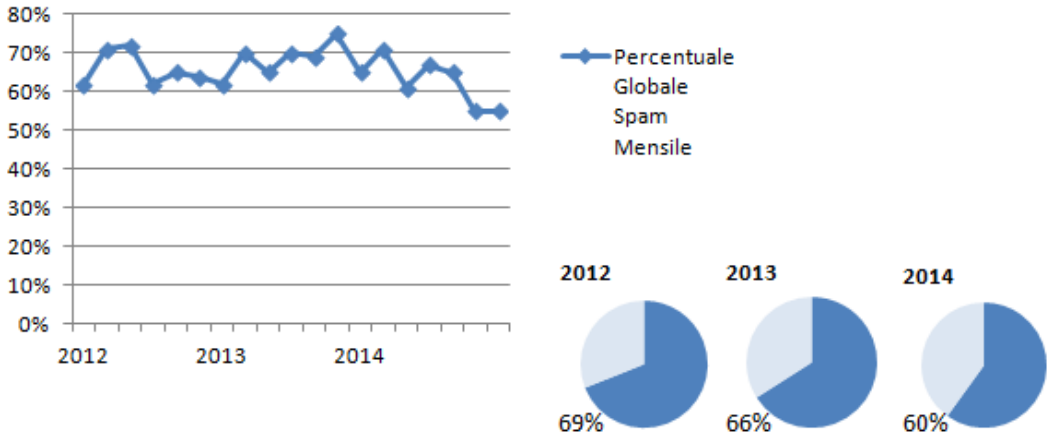


Figura 1 - Percentuale Globale Spam, 2012-2014
Fonte: Internet Security Threat Report, Symantec, 2015

Inoltre, anche il fenomeno del ransomware non accennerà a diminuire. Questo tipo di attacchi infatti nel 2014 è più che raddoppiato, passando da 4,1 milioni del 2013 agli 8,8 del 2014. Sul piano psicologico è un tipo di attacco molto redditizio perché, nel caso in cui non siano stati effettuati regolari backup conservati separatamente, l'utente pur di recuperare i propri dati è disposto a pagare il riscatto.

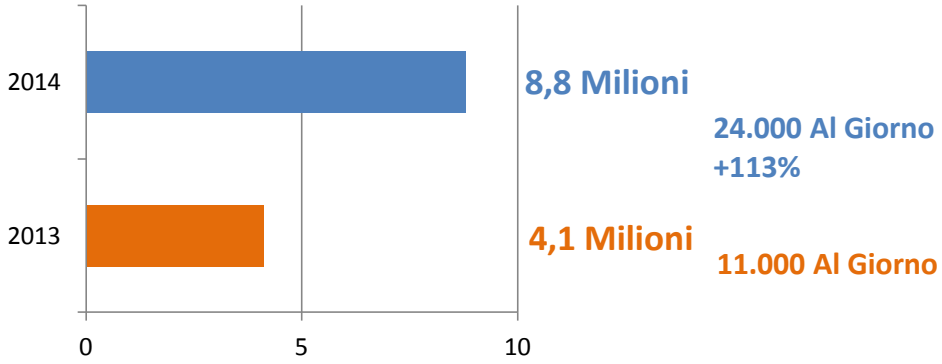


Figura 2 - Totale Ransomware
Fonte: Internet Security Threat Report, Symantec, 2015

10 How you could become a victim of cybercrime in 2015, The Guardian, 24-12-2014, in <http://www.theguardian.com/technology/2014/dec/24/cybercrime-2015-cybersecurity-ransomware-cyberwar> (ultima consultazione 10-04-2015)
11 Internet Security Threat Report, Symantec, Aprile 2015, in <https://know.elq.symantec.com/LP=1542> (ultima consultazione 22-06-2015)

Altro argomento interessante per i cyber criminali sarà, anche per il 2015, quello delle transazioni economiche on-line, sempre più diffuse, anche su smartphone e dispositivi mobili. Parlando di dispositivi mobili, il 2015 potrebbe essere l'anno che sfaterà il mito dell'inviolabilità dell'iPhone, lo smartphone di casa Apple; pur rimanendo Android la piattaforma preferita come bersaglio dei cyber criminali. Secondo BitDefender[12], che nel 2014 ha pubblicato una lista delle dieci maggiori truffe su Facebook, nel 2015 questo genere di azioni fraudolente tenderà ad aumentare, poiché il sempre maggiore bacino d'utenza dei social network è di grande interesse per i criminali. Il 2014 ha visto una netta inversione di tendenza riguardo le modalità di diffusione delle truffe attraverso i social network, registrando un drastico aumento degli scambi tra utenti reali di video e messaggi malevoli.

Anche il rapporto Clusit 2015 conferma che il cyber crime è un fenomeno in costante aumento e che costituisce la causa principale degli attacchi di natura informatica. Secondo l'analisi Fastweb contenuta nel rapporto, infatti, il 93% degli attacchi[13] sono riconducibili ad azioni di cyber crime.

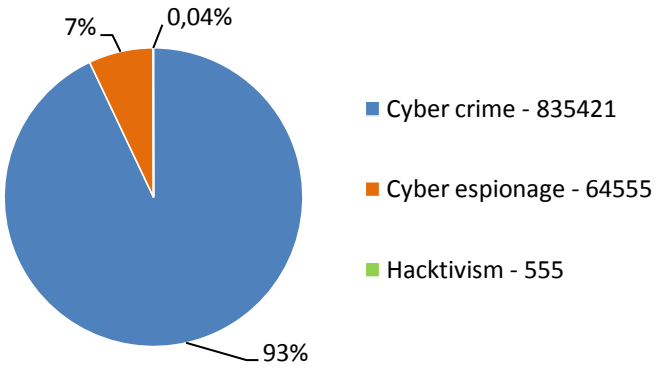


Figura 3 - Dati Fastweb relativi alle motivazioni di attacco
Fonte: Clusit, 2015

Il problema principale è che i rischi derivanti da un basso livello di prevenzione in materia di sicurezza informatica crescono più rapidamente della capacità di protezione dagli attacchi informatici. Pur aumentando in questi ultimi anni gli investimenti in sicurezza informatica, la quantità degli attacchi e il loro livello di gravità continuano ad aumentare. Il rapporto inoltre stima che i due terzi degli incidenti non siano neanche rilevati dalle vittime per mancanza di competenze e di strumenti adeguati.

Per quanto riguarda la previsione dei rischi per il 2015, il rapporto individua la criticità dei social network, la cui diffusione non solo come rete tra utenti privati, ma anche come vetrina per piccole e medie imprese e grandi aziende rende queste piattaforme appetibili

12 It's been a great year! Thanks to these Facebook scams for being a part of it..., The Guardian, 24-12-2014, in <http://www.theguardian.com/technology/2014/dec/24/facebook-scams-malware-naked-videos> (ultima consultazione 10-04-2015)
13 Dati relativi a circa 6 milioni di indirizzi IPv4 appartenenti all'AS Fastweb SpA (quindi sia quelli dei clienti che di Fastweb stessa) raccolti ed analizzati dal Security Operations Center

per la diffusione di malware e per effettuare frodi. Tra le altre tendenze per il 2015 si segnalano la fragilità dei sistemi *Point of Sale* (POS) presi sempre più di mira dai criminali per la facilità con la quale si possono sfruttare malware ad-hoc molto economici che possono essere usati dai criminali comuni per frodi economiche; la sempre maggiore criticità dei dispositivi mobili attraverso i quali è in costante aumento l'attitudine degli utenti a realizzare acquisti, il cosiddetto *m-commerce*, e infine la continua diffusione di ransomware come Cryptolocker.

Uno studio condotto da SecuRe Pay, il forum europeo sulla sicurezza del pagamento al dettaglio, afferma che, per gli anni per i quali si avevano dati a riguardo (2011 e 2012), si è registrato un aumento del 21,2% delle frodi su e-commerce. 94 milioni di euro sarebbero stati rubati infatti ad utenti che avevano effettuato acquisti on-line con carta di credito[14]. Una cifra così preoccupante da spingere l'*European Bank Authority* (EBA), a pubblicare delle linee guida che saranno in vigore dal prossimo agosto, come la verifica dell'identità dei clienti prima di procedere con la transazione on-line e fornire ai clienti un servizio di informazione e aiuto sul tema della sicurezza dei pagamenti on-line. Sempre secondo l'EBA le frodi "*card not present*" costituiscono il 60% dei complessivi 1,33 miliardi di euro frodati nel 2012[15]. Bisogna considerare inoltre che quasi la metà degli utenti frodati in seguito ad acquisti on-line non recuperano più il denaro perso[16].

Il 2014 ha confermato quello che si poteva immaginare con la rapida diffusione di smartphone e tablet e cioè che i criminali sfruttano sempre di più questi nuovi punti di attacco. Alcatel-Lucent's Motive Security Labs, in un report[17] pubblicato alla fine del 2014, stima che in tutto il mondo siano stati infettati da malware più di 16 milioni di dispositivi mobili al fine di realizzare azioni di spionaggio industriale e personale, per rubare informazioni e attaccare imprese, privati, banche e governi. Solo nel 2014 le infezioni dei dispositivi mobili sono aumentate del 25% (un incremento del 5% rispetto al 2013). La continua crescita dei malware per mobile è dovuta soprattutto all'uso del dispositivo da parte degli utenti senza le dovute precauzioni di sicurezza, soprattutto in ambito lavorativo, dove questo viene usato senza particolari differenze da quello privato. 6 dei 20 malware più diffusi sono spyware: cioè applicazioni utilizzate per spiare il proprietario del telefono tracciandone la posizione, monitorando le chiamate in entrata e in uscita e leggendo i messaggi di testo. Tra gli altri malware della top 20 ci sono applicazioni scareware che

14 Ecommerce: le frodi costano 794 milioni l'anno, di Marco Boscolo, Wired Italia, 30-12-2014, in <http://www.wired.it/economia/business/2014/12/30/pagamenti-online-frodi-valgono-794-milioni-lanno/?utm_content=buffer4be2c&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer> (ultima consultazione 05-03-2015)

15 New report on card fraud shows online fraud increased in 2012, European Central Bank, Press Release 25-02-2014, in <https://www.ecb.europa.eu/press/pr/date/2014/html/pr140225.en.html> (ultima consultazione 05-03-2015)

16 Acquisti online e frodi: il 44% degli utenti non recupera il denaro, La Stampa tecnologia, 24-12-2014, in <http://www.lastampa.it/2014/12/24/tecnologia/acquisti-online-e-frodi-il-degli-utenti-non-recupera-il-denaro-Ft9RDDFyPpYTbyoJi1J96J/pagina.html?utm_content> (ultima consultazione 20-03-2015)

17 Motive Security Labs malware report – H2 2014, Alcatel-Lucent's Motive Security Labs, in <https://resources.alcatel-lucent.com/asset/184652> (ultima consultazione 23-03-2015)

cercano di estorcere denaro affermando di aver criptato i dati del telefono, applicazioni che rubano informazioni personali dal dispositivo e applicazioni proxy web che consentono agli hacker di navigare in forma anonima sul web attraverso un telefono infetto a spese del proprietario. Questi dati sono allarmanti se consideriamo che il livello di consapevolezza dell'utente nell'uso del dispositivo mobile è ancora molto basso. Un recente studio condotto da Kaspersky Lab e B2B International[18] dimostra come quasi il 30% degli utenti non sappia neanche cosa sia un malware.

In questo scenario si inserisce lo scarsissimo livello di attenzione e consapevolezza degli utenti che spesso scaricano applicazioni e visitano siti poco sicuri con troppa disinvoltura. Il già citato rapporto Symantec afferma che il 17% delle applicazioni per Android (quasi un milione) contengono malware.

Il fattore umano rimane sempre il più decisivo, anche nei processi collegati all'uso di dispositivi mobili e ne rappresenta senza dubbio l'anello più debole. Una ricerca della *Carnegie Mellon University* di Pittsburgh[19] afferma che la già minima diffidenza dell'utente medio nei confronti di software di cui non si conosce con certezza la fonte, viene del tutto annullata se il download del file è collegato ad un incentivo economico anche irrisorio. I ricercatori della *Carnegie Mellon University* hanno condiviso in rete un programma che offriva un piccolo credito in denaro in cambio del download, e allo stesso tempo avvertivano dei potenziali rischi collegati al download di un software non certificato. Il risultato è stato che ben il 22% degli utenti che hanno effettuato il download ha scaricato il programma per un solo centesimo di dollaro, il 36% per 50 centesimi e il 42% del campione per un dollaro. Il risultato di questa ricerca non fa che confermare che la diffusione del cyber crime è senza dubbio facilitata dal comportamento umano. La scarsa consapevolezza dei pericoli derivanti dal web induce l'utente ad avere comportamenti che agevolano la diffusione dei virus e permettono di realizzare frodi o altri tipi di attacchi, comportamenti sui quali i criminali informatici fanno leva.

18 Indagine Kaspersky Lab: un utente su quattro non comprende i rischi delle minacce informatiche mobile, Kaspersky Lab, 27-02-2015, in <http://www.kaspersky.com/it/about/news/virus/2015/Indagine_Kaspersky_Lab_un_utente_su_quattro_non_comprende_i_rischi_delle_minacce_informatiche_mobile> (ultima consultazione 28-03-2015)

19 It's All About The Benjamins: An empirical study on incentivizing users to ignore security advice, di Nicolas Christin, Serge Egelman, Timothy Vidas e Jens Grossklags, INI/CyLab, Carnegie Mellon University, National Institute of Standards and Technology, ECE/CyLab, Carnegie Mellon University, IST, Pennsylvania State University, in <https://www.andrew.cmu.edu/user/nicolasc/publications/CEVG-FC11.pdf> (ultima consultazione 07-05-2015)

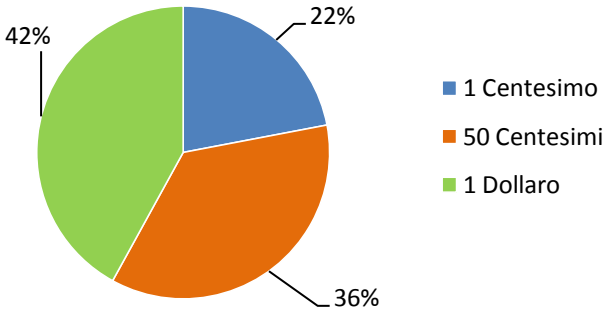


Figura 4 - Distribuzione dei download collegati ad un incentivo economico
Fonte: Carnegie Mellon University, Pittsburgh

Uno studio di Kaspersky Lab dimostra come più di un quarto degli utenti di dispositivi mobili ignori le pratiche minime di sicurezza, non considerando la sensibilità dei dati all'interno dei dispositivi stessi (rubrica, password di account e-mail o social network, informazioni bancarie, dati personali come foto e video, SMS). Lo studio conferma anche lo scarso utilizzo di software antivirus e protezioni minime come password o PIN e che i device Android sono i più vulnerabili, anche per la minore competenza degli utenti.

La criticità dell'elemento umano emerge anche dallo studio Ntt[20], il quale afferma che nei giorni seguenti i weekend o le festività si registra un aumento del 75% delle macchine infette, dato che sottolinea come l'utente costituisca un pericolo concreto per l'infrastruttura aziendale a causa dell'uso non differenziato dai dispositivi privati.

Un'indagine di Kaspersky Lab realizzata in tema di B*ring Your Own Device* (BYOD)[21] evidenzia come il 62% dei datori di lavoro e dei dipendenti usino abitualmente dispositivi privati in ambito lavorativo, spesso senza efficaci misure di protezione. Il 92% degli intervistati infatti archivia dati aziendali sensibili su smartphone e tablet usati sia in ambito lavorativo che privato. Il 60% dei dipendenti ritiene che sia responsabilità dell'azienda attivare o meno sistemi di protezione. Per quanto riguarda le PMI risulta ancora molto bassa la percentuale di lavoratori e titolari che ritengono i pericoli informatici una minaccia reale e concreta, mentre quasi il 60% delle grandi aziende è seriamente allarmato dal fenomeno del cyber crime.

Contrariamente a quanto si possa pensare, il phishing rimane ancora uno dei metodi di attacco più diffusi e usati. Nonostante sia forse la tecnica di attacco informatico più conosciuta dalla maggior parte delle persone, ancora oggi gli utenti che cliccano su e-mail di phishing costituiscono percentuali altissime. Purtroppo i dati su questo fenomeno non sono

20 Cybersecurity, così Intelligence e imprese possono collaborare, di Michele Pierri, 16-03-2015, in <http://www.formiche.net/2015/03/16/cybersecurity-minniti-ruffinoni/> (ultima consultazione 20-03-2015)
21 Consumer Security Risk Survey 2014: Multi-device threats in a multi device world, Kaspersky Lab, Luglio 2014, in <http://media.kaspersky.com/en/Kaspersky_Lab_Consumer_Security_Risks_Survey_2014_ENG.pdf> (ultima consultazione 28-05-2015)

affatto incoraggianti, soprattutto per quanto riguarda il cyber spionaggio, che risulta essere in costante crescita. Gli 80mila incidenti di sicurezza analizzati nel *Data Breach Investigation report* di Verizon[22] hanno portato a perdite di dati per un danno economico di più di 400 milioni di dollari per le aziende coinvolte. Il phishing si conferma una delle tecniche più usate nonostante si tratti di una tecnica di social engeneering di vecchia data, ma nei confronti della quale non ci si protegge ancora abbastanza, soprattutto per quanto riguarda il fattore umano. Nonostante anni di esperienza, non si riesce ancora a non cedere alla tentazione di cliccare su link malevoli. I dati Verizon confermano che questo trend è in crescita: la percentuale degli utenti che clicca su una e-mail di phishing è salito dal 10% dello scorso anno al 23%, ancora più sconfortante è il dato che vede l'11% degli utenti aprire anche gli allegati contenuti nelle e-mail, che contengono malware. Lo studio di Verizon dimostra quanto sia altamente proficuo per un cyber criminale usare tecniche di phishing, dato che una campagna di appena 10 messaggi di posta elettronica produrrebbe una probabilità superiore al 90% che almeno un utente cada vittima dell'attacco. In base ad un esperimento effettuato dai ricercatori di Verizon si è potuto stimare che quasi il 5% degli utenti cliccano su una e-mail di phishing già nella prima ora di invio della e-mail stessa. Questo ci suggerisce che con un'adeguata formazione dell'utente, il fattore umano può diventare un sensore più efficace di qualsiasi strumento tecnologico nel rilevare una e-mail di phishing. Dati di una indagine di Intel Security, effettuata su 19 mila utenti di 144 Paesi, rivelano che solo il 3% è riuscito a riconoscere tutte le e-mail di phishing e l'80% invece non è riuscito ad identificarne nemmeno una[23].

22 2015 Data Breach Investigations Report, Verizon, in <http://www.verizonenterprise.com/DBIR/2015/> (ultima consultazione 25-05-2015)

23 Il 97% di chi naviga su Internet non sa riconoscere il phishing, Il secolo XIX Tech, 23-05-2015, in <http://www.ilsecoloxix.it/p/magazine/2015/05/23/AR7IpzXE-phishing_internet_riconoscere.shtml> (ultima consultazione 05-05-2015)

CAPITOLO 2

Indagine empirica sull'impatto del cyber crime in Italia: Interviste e casi studio

La sicurezza informatica è un tema che necessita una conoscenza approfondita di tutti gli aspetti che riguardano il cyber crime. La mancanza di studi e statistiche nazionali ufficiali su tale fenomeno è stato uno degli aspetti che ha suggerito un approccio empirico per la realizzazione della precedente ricerca. Per dare continuità a questo studio si è scelto di realizzare interviste a livello nazionale che riguardassero altri aspetti strategici in questo settore, al fine di studiare quegli indicatori del fenomeno del cyber crime che possano fornire informazioni di tipo qualitativo, utili a comprendere l'evoluzione delle minacce, le azioni da mettere in atto per prevenire eventuali danni e il livello di consapevolezza rispetto questo fenomeno.

Dati ABI Lab

Una delle realtà da sempre più attente a queste problematiche è il settore bancario. A tal fine, si è analizzato il Report 2015 dell'Osservatorio Sicurezza e Frodi Informatiche "*Sicurezza e frodi informatiche in banca. Come prevenire e contrastare le frodi su Internet e Mobile Banking*"[24], fornito per questa ricerca dalla dott.ssa Monica Pellegrino di ABI Lab.

Il settore finanziario e bancario è senza dubbio uno dei settori più appetibili per i cyber criminali, non soltanto per la sottrazione di somme di denaro in modo fraudolento, ma anche per il patrimonio informativo che le banche gestiscono. Nell'era digitale assume

24 Il report contiene i risultati della survey condotta da ABI Lab sulle frodi via internet e mobile banking. Hanno partecipato a questa edizione 45 banche, 4 outsourcer e aziende specializzate

un'importanza sempre maggiore il valore dell'informazione e del dato. Dall'analisi svolta da ABI Lab emerge che nel 2014 l'80% del campione ha rilevato casi di frode identitaria nei confronti della propria clientela retail, e il 66,7% invece relativo alla clientela corporate. Un dato in linea con quelli che saranno i casi studio analizzati in questo capitolo riguarda invece la tipologia di operazioni fraudolente commesse dai cyber criminali, tra le quali il bonifico bancario costituisce per i clienti retail la modalità maggiormente utilizzata per effettuare operazioni non autorizzate. Il report inoltre registra un aumento dell'uso di operazioni di ricarica di carte prepagate da parte dei frodatori. Per i clienti corporate il bonifico, invece, soprattutto quelli verso conti in istituti bancari stranieri[25], è l'unica modalità usata per trasferire somme di denaro anche ingenti. Un dato rilevante è che, seppur le frodi nei confronti della clientela retail sono maggiori in confronto a quella corporate, il maggior volume economico associato alle operazioni non autorizzate, ben il 72,3%, riguarda il segmento corporate. Per quanto riguarda i vettori di attacco, il report rileva che il crimeware continua ad essere quello più utilizzato per realizzare frodi, soprattutto nei confronti delle imprese, verso le quali vengono realizzati attacchi più mirati. Nello specifico si registra un aumento delle transazioni fraudolente realizzate durante una sessione del cliente legittimo (*Man-in-the-Browser*) corrispondente al 60% degli attacchi per quanto riguarda le imprese, oltre a casi di phishing e azioni con tecniche combinate.

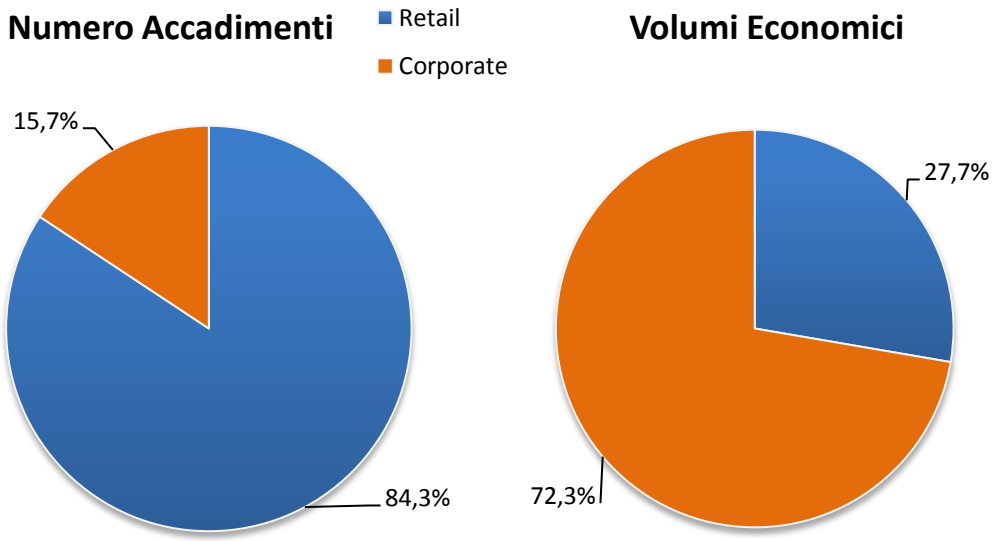


Figura 5 - Ripartizione totale delle transazioni effettive, suddivise per segmento
Fonte: Sicurezza e Frodi Informatiche in Banca, ABI Lab, Giugno 2015

25 A testimonianza di come sempre più spesso le organizzazioni criminali abbiano un coordinamento e una rete extra-nazionale e siano al contempo consapevoli della maggiore difficoltà che si può riscontrare nel bloccare tempestivamente operazioni indirizzate verso beneficiari di altri Paesi

Si.Camera e Unindustria: esperienze a confronto

Gli istituti che hanno i maggiori contatti diretti con le aziende sono il sistema camerale e le associazioni di categoria. A tal proposito sono stati coinvolti la dott.ssa Labia (Si.Camera) e il dott. Tocci (Unindustria) per indagare sulla situazione delle PMI a livello nazionale in tema di sicurezza informatica.

Molto si sta facendo in questi ultimi anni per la lotta al cyber crime, ma per quanto riguarda le PMI ciò che è prioritario è una forte attività di prevenzione e formazione. Manca però una distribuzione capillare di iniziative organizzate e coordinate a livello nazionale di formazione e sostegno nell'ambito del cyber crime, destinate alle PMI. È quanto hanno confermato anche la dott.ssa Labia, Responsabile dell'area Proprietà intellettuale e Anticontraffazione e dell'area filiere e sviluppo dei territori di Si.Camera e il dott. Tocci, funzionario area legale e appalti di Unindustria di Roma. Le iniziative realizzate sinora infatti sono solo a livello locale. Secondo la dott.ssa Labia il grado di conoscenza del cyber crime è ancora molto basso come lo è anche il livello di attenzione tra le imprese "*senz'altro il livello di informatizzazione e consapevolezza sta crescendo in questi ultimi anni, ma è ancora piuttosto basso. Più sensibili appaiono le imprese operanti nelle filiere del Made in Italy. Siamo dinanzi ad una questione importante ed urgente, che impatta sulla vita aziendale e sulla competitività dell'impresa nel suo complesso. È un tema squisitamente di cultura imprenditoriale. Sensibilizzazione, formazione, accompagnamento 'one to one' le azioni da mettere in campo. Occorre far crescere le professionalità che operano all'interno delle imprese, a partire dagli amministratori, coinvolgendole in un percorso di affiancamento individuale, ma anche di networking.*"

Di parere concorde è il dott. Tocci il quale rileva nella sua attività che il livello di attenzione varia a seconda della dimensione dell'azienda, le grandi aziende sono molto attente, le piccole meno. Inoltre per il dott. Tocci in Italia manca ancora "*una cultura del dato come risorsa strategica d'impresa e non ci si dota quindi degli strumenti adatti ad impedire fenomeni di cyber crime che minano il know-how e il business delle PMI.*" Questo aspetto è infatti quanto mai cruciale nell'implementazione della cultura della sicurezza. L'uso dello strumento informatico per la sottrazione e la contraffazione di prodotti, brevetti e marchi sta diventando un aspetto sempre più sensibile.

Il parere di due società IT italiane

Nell'ambito dei nuovi scenari di attacco, dove lo scopo dei cyber criminali non è solo quello di creare un danno immediato, ma soprattutto ottenere il controllo dei sistemi della vittima per attacchi più sofisticati, è stata realizzata un'intervista presso Certego, realtà innovativa nata nel 2013 con sede a Modena e specializzata nell'erogazione di servizi di sicurezza IT gestita e di contrasto al cyber crime. Certego infatti ha sviluppato una piattaforma in grado di identificare la presenza di anomalie nel traffico di rete e

nell'esecuzione dei processi applicativi all'interno dei sistemi, analizzando e identificando l'eventuale presenza di attacchi informatici.

Dall'analisi effettuata sui dati forniti da Certego, raccolti attraverso il loro servizio di Breach Detection, Investigation & Response[26], si può notare come all'interno delle reti da loro monitorate[27] solo nei primi 5 mesi del 2015 siano stati rilevati ben 278 attacchi "veri positivi" che hanno superato le barriere difensive costituite dalle principali tecnologie di IT Security (firewall, antivirus, intrusion prevention systems, ecc.). Inoltre, un dato importante da valutare è che ben un terzo degli attacchi rilevati sono classificati come critici, che mettono quindi a serio rischio il business o l'operatività di un'azienda e richiedono un intervento immediato.

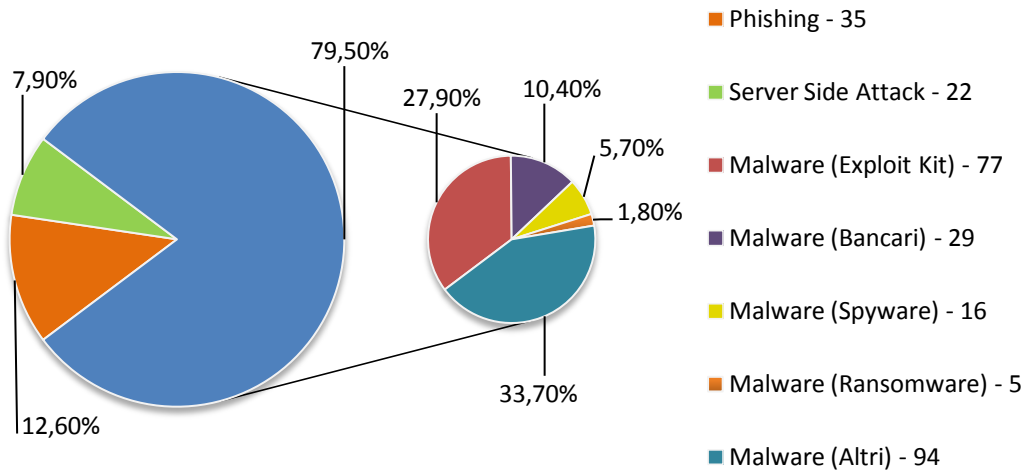


Figura 6 - Distribuzione degli attacchi relativi alla rete monitorata da Certego
Fonte: Certego, 2015

Come si evince dal grafico, il 12,5% del totale degli attacchi andati a buon fine è rappresentato da phishing, cioè e-mail che hanno superato le barriere tecniche dei filtri antispam, riuscendo ad ingannare i destinatari. Il 79,5% delle minacce rilevate comprende tutte le tipologie di malware, compresi ransomware, spyware, exploit kit di programmi come ad esempio Adobe Reader, Java Runtime e Adobe Flash. Anche in questo caso attacchi andati a buon fine, cioè che hanno superato le barriere dei software antivirus e che sono stati installati dall'utente. Il restante 8% è relativo agli attacchi di tipo *server-side*, ovvero che hanno come obiettivo le risorse di un server o di un'applicazione.

Un'importante osservazione del dott. Roberto Tanara, Lead Consultant di Certego, è che "*per macro categorie il profilo di distribuzione delle minacce che abbiamo osservato sulle PMI non si discosta molto da quello delle grandi aziende, il che conferma che il cyber crime ha natura comunque opportunistica nelle operations su larga scala, senza distinzione tra piccole realtà e grandi organizzazioni.*" Il CEO di Certego, dott. Bernardino Grignaffini

26 Con un numero medio di sistemi monitorizzati ogni giorno pari a 15.000 circa tra client, server e mobile
27 Relativa ai clienti PMI della zona centro-nord Italia

aggiunge *"In tal senso, anche i piccoli dovrebbero avere le stesse preoccupazioni dei grandi, pur con meno risorse a disposizione."*

Per quanto riguarda i tempi di *remediation* non tutte le imprese sono poi così attente anche dopo la segnalazione, Certego registra ancora casi in cui sensibilità e reattività sono molto basse.

Data la mancanza in Italia di statistiche complete ed esaustive sull'entità del cyber crime e dei tempi e costi relativi, il dott. Tanara e il dott. Grignaffini sottolineano l'importanza di promuovere la cultura dei dati, creando ad esempio una piattaforma di condivisione di dati anonimizzati che rilevino una situazione il più possibile vicina alla realtà.

Il basso livello di attenzione delle PMI italiane nei confronti dei pericoli del cyber crime è un aspetto diffuso in tutte le regioni. Rossano Rogani, membro dell'Associazione Italiana Professionisti Sicurezza Informatica (AIPSI) ci confessa che, parlando delle PMI, il livello di informatizzazione e di consapevolezza sul fenomeno del cyber crime è ancora molto basso nel suo territorio. *"In alcuni casi possiamo trovare le stesse carenze anche nelle grandi aziende."* Rogani inoltre rileva che nella sua zona si registra in quest'ultimo periodo un trend in aumento di casi di ransomware (soprattutto Cryptolocker) e attacchi a siti web. Per questi ultimi osserva che la cultura della sicurezza informatica è ancora molto bassa anche tra le web agency, che li realizzano senza molta attenzione alla security, rendendoli facili bersagli per i cyber criminali. Negli ultimi due mesi Rogani ha assistito più di 20 PMI vittime di ransomware, secondo il suo parere è un fenomeno molto serio e per il quale la prima cosa da fare è educare e formare il personale al buon uso dei sistemi informatici, ma purtroppo nella zona non sono ancora presenti iniziative di formazione a livello istituzionale.

Ambito giuridico-legale: opinioni ed esperienze a confronto

Per capire meglio cosa si trova ad affrontare una PMI dopo aver subito un attacco, abbiamo ascoltato il parere dell'avvocato Marco Tullio Giordano, esperto nel settore del diritto penale delle nuove tecnologie presso lo studio legale R&P di Milano. Il trend che registra l'avvocato Giordano in questi ultimi mesi è un aumento sensibile di casi riguardanti eventi di *Man-in-the-Middle* e di spionaggio industriale. L'attacco *Man-in-the-Middle* è un tipo di attacco silente nel quale l'attaccante si inserisce nei sistemi della vittima (o del suo interlocutore) e per un lungo periodo di tempo ne studia le abitudini informatiche, leggendo e modificando le comunicazioni tra le due parti e nascondendo la sua presenza ad entrambi.

Nello specifico l'avvocato Giordano ci fornisce il caso studio di un'azienda manifatturiera del nord Italia con un basso livello di presenza su internet in quanto il suo prodotto non è diretto all'utente finale ma ad una clientela business molto specifica. L'azienda in questione riceve una e-mail da un fornitore asiatico con la quale viene invitata ad effettuare i successivi bonifici su un nuovo conto, aperto per agevolare i clienti europei, presso una banca inglese. La società italiana effettua nell'arco di tre mesi bonifici per un

totale di 600.000 euro. Per sentirsi maggiormente sicuro, in una situazione mai avvenuta prima, il CFO dell'azienda effettua i bonifici al numero di conto fornito dai cyber criminali inserendo come beneficiario il nome dell'azienda fornitrice asiatica. I criminali cercano, a questo punto, di approfittare del nominativo non corrispondente all'intestatario del conto per richiedere nuovamente l'importo del bonifico asserendo che non era andato a buon fine. A questo punto l'azienda si accorge che qualcosa non andava. A seguito di accertamenti viene a conoscenza della truffa e si rivolge ad uno studio legale specializzato in fattispecie di questo tipo. Inizialmente si ipotizzano irregolarità in fase di apertura conto presso la banca inglese, ma questa si rifiuta di dare informazioni sul titolare del conto per tutelarne la privacy. Dopo verifica tramite richiesta dal fornitore asiatico si viene a scoprire che il conto risulta intestato a terzi. "*Le disposizioni europee tutelano i pagamenti fatti a soggetti diversi dal titolare del conto, una vera aporia del sistema*"[28] ci dichiara l'avvocato Giordano "*purtroppo c'è poco da fare, bisognerebbe intervenire a livello europeo*". Manca quindi l'obbligo di attivare un *alert* quando la banca riceve una transazione economica con beneficiario difforme dal titolare del conto, almeno per cifre superiori ad una certa entità. A seguito della denuncia e della richiesta da parte dello studio legale italiano, la banca inglese restituisce alla società vittima l'importo rimanente sul conto, chiudendolo, ammettendo di fatto l'illecito commesso, senza però fornire ulteriori dettagli utili per l'investigazione. Lo studio dell'avvocato Giordano tenta ogni strada, consultando anche uno studio legale londinese, ma data la normativa le probabilità di recuperare la somma persa sono quasi nulle.

In questo caso i criminali si sono inseriti nelle comunicazioni tra le due società per diverso tempo, monitorando le comunicazioni, bloccando le e-mail autentiche dal fornitore asiatico verso l'azienda italiana, e inviando a loro volta e-mail false ma estremamente ben realizzate, simulandone l'invio da parte del fornitore asiatico.

A causa del danno subito, questa azienda italiana ha di fatto perso gli utili previsti per il prossimo anno e ha chiuso il reparto di ricerca e sviluppo. Il feedback che l'avvocato Giordano ha dai propri clienti è di abbandono e frustrazione in quanto lamentano di non essere mai state allertate sui pericoli derivanti dal crimine informatico da parte di nessuna associazione di categoria a cui sono iscritti. "*Un ulteriore aspetto critico è costituito dal fatto che, data la bassa percentuale d'esercizio dell'azione penale, può accadere che le forze dell'ordine non accolgano le denunce o le chiudano dopo pochissimo tempo facendo sentire la vittima definitivamente abbandonata dalle istituzioni, questo è un messaggio che non deve passare."* Anche se l'esercizio dell'azione penale per questo tipo di crimine è molto bassa a causa dell'elevata transnazionalità del fenomeno, non si dovrebbe cadere nell'errore di far sentire le vittime abbandonate dalle istituzioni e soprattutto si dovrebbe puntare ad una

28 Per approfondimenti si rimanda a: Art. 74 del Payment Service Regulation 2009 (PSR) in vigore nel Regno Unito e del corrispondente Art. 24 della L. 11/2010, c.d. Testo Unico Bancario e a: Attuazione del Titolo II del Decreto legislativo n. 11 del 27 Gennaio 2010 relativo ai servizi di pagamento (Diritti ed obblighi delle parti), Banca d'Italia, Eurosistema

maggiore formazione delle forze dell'ordine che si trovano ad accogliere imprese e cittadini vittime del cyber crime.

Il livello di conoscenza di questo fenomeno è talmente basso che l'avvocato Giordano ci riferisce casi di aziende che inizialmente avevano pensato di essere state truffate dal fornitore stesso, ignorando totalmente l'esistenza di questo tipo di criminalità informatica. "*Le associazioni di categoria dovrebbero promuovere in modo più capillare eventi di formazione su questo tema. Anche solo con l'invio di circolari a livello bancario e da parte di associazioni di categoria si potrebbero quanto meno limitare i casi come questo e si alzerebbe il livello di attenzione.*" È plausibile, da quanto riferitoci dall'avvocato Giordano, che i cyber criminali studino quali sono le banche con diligenza minima e mancanza di ulteriori parametri di controllo per realizzare la frode. "*Quello che serve è l'informazione prima che si verifichino casi di questo tipo e un raccordo internazionale a livello istituzionale dopo, per centralizzare le indagini*". I tempi per questo tipo di casi infatti attualmente sono troppo lunghi, mediamente ci si accorge dell'accaduto dopo alcuni mesi e ne passano altri per capire cosa fare da parte delle aziende colpite. Le cifre sottratte alle imprese in questi casi sono cifre importanti, che spesso minano la sopravvivenza delle aziende stesse.

"*Un altro trend che registriamo in questo settore sono i casi di spionaggio industriale".* Sono spesso casi di dipendenti che si mettono in proprio o cambiano azienda e rubano dati e know-how, sfruttando i loro livelli di accesso o forzando i sistemi informatici. Un caso recente, seguito dall'avvocato Giordano, ha riguardato un insider di un'azienda italiana accusato di aver trasferito know-how e database clienti presso la sua nuova azienda estera, che ha poi contattato i clienti offrendo gli stessi prodotti ad un quarto del prezzo. L'azienda italiana in questione ha dovuto porre alcuni dipendenti in cassa integrazione. "*Nei confronti di questi casi però è possibile fare qualcosa in più."*

Di opinione concorde è il Sostituto Procuratore della Procura della Repubblica di Torino dott. Vito Destito "*Rispetto ad altri fenomeni di criminalità informatica, migliori risultati – quantomeno sotto il profilo investigativo, l'identificazione del responsabile e l'esercizio dell'azione penale – sono stati ottenuti nei casi di insider aziendale. Il fenomeno è quello del dirigente, progettista o comunque soggetto legato da rapporto di lavoro ad una determinata società o ditta che, nell'interrompere il rapporto con il primo soggetto economico ed intraprenderne uno nuovo (alle dipendenze di altro ente, se non addirittura in proprio) 'trafughi' dati aziendali. Il fenomeno si ricollega alla criminalità informatica in quanto l'accesso per finalità proprie ed incompatibili con quelle dell'ente che gli consentiva l'accesso, costituisce accesso abusivo a sistema informatico (in relazione ad un dissenso quantomeno tacito e presunto) seppure il soggetto che effettuato l'accesso fosse dotato delle relative credenziali."*

In un caso illustratoci dal Procuratore Destito un progettista di un'azienda piemontese, del settore manifatturiero che realizza componenti idrauliche, ha trafugato e trasferito ad una società tedesca, che l'avrebbe poi assunto, tutti i progetti della società italiana per cui aveva lavorato, sottraendone l'intero know-how aziendale.

In un secondo caso, sempre fornitoci dal Procuratore Destino, un quadro del settore commerciale ha sottratto progetti riguardanti macchinari per la lavorazione delle lamiere, a favore di una società inglese che ha aperto una controllata in Italia. Il questo caso il commerciale "*dei progetti non avrebbe neppure potuto disporne (tanto che, in questo caso viene contestato il reato di cui all'art. 621 c.p., ovvero di notizie destinate a rimanere segrete di cui il soggetto sia venuto abusivamente in possesso e non quello di cui all'articolo successivo relativo alla comunicazione di notizie delle quali il soggetto legittimamente disponeva). Ciò sarebbe stato reso possibile da una 'cattiva' ripartizione degli accessi ai dati aziendali. Il commerciale non avrebbe dovuto poter accedere ai dati progettuali dell'azienda, cosa che è, invece, accaduta per uno scarso livello di sicurezza informatica interna che non garantiva una suddivisione degli accessi per 'gradi', a seconda dei dati sui quali il soggetto poteva e doveva operare in relazione alle mansioni svolte*."

Da quanto ci riferisce il Procuratore Destito, in casi di questo genere, molto spesso è la stessa ditta querelante ad indirizzare le indagini in una direzione ben precisa, spesso avvalendosi di consulenti informatici, aziendali e finanche di investigatori privati. Le indagini effettuate dalla Procura di Torino iniziano quindi con l'esame della documentazione informatica, che dimostrerebbe il *fumus* di reato secondo la persona offesa, a cui segue una perquisizione informatica presso la ditta per la quale l'insider ha intrapreso la sua nuova attività (e anche al suo domicilio) volta ad acquisire i dati informatici utilizzati. Si effettua poi l'esame comparativo dei dati e dei relativi progetti o banche dati (ad es., banalmente, l'elenco clienti) trasferito solitamente ad un consulente, che ricostruisce come e in che misura la seconda ditta utilizzi i dati trafugati alla prima. Molto spesso tali consulenze richiedono sia competenze tecniche-ingegneristiche-meccaniche, sia competenze informatiche.

Secondo il parere dell'avv. Giordano e del suo collega avv. Giuseppe Vaciago "*la redazione di apposite policies di comportamento e l'emanazione di un regolamento sull'utilizzo degli strumenti informatici aziendali risulta quanto mai consigliabile, tanto per prevenire episodi di questo genere, quanto per avere una base documentale dalla quale partire per effettuare un'investigazione interna in caso di condotte illecite attraverso le tecniche più idonee di digital forensics*.[29]"

In questi ultimi anni si sta cercando di focalizzare sempre di più l'attenzione sul cyber crime anche in ambito giuridico. Molto si è fatto, ma tanto si dovrà ancora fare. In questo settore uno dei primi PM ad occuparsi di cyber crime e uno dei pochi ad aver avuto risultati investigativi molto importanti alla Procura della Repubblica di Roma è il Magistrato Giuseppe Corasaniti[30] che dal 2012 si occupa, presso la Procura Generale della Corte di Cassazione, di

29 La sicurezza informatica, un asset aziendale strategico, di Giuseppe Vaciago e Marco Tullio Giordano, Rivista 231 (02-2015) pag. 273

30 Sostituto Procuratore Generale della Procura generale della Repubblica presso la Corte Suprema di Cassazione. Studioso tra i più esperti di problemi giuridici della comunicazione e dell'informatica e di Diritto informatico. Membro del gruppo 24/24 per il Consiglio d'Europa che garantisce assistenza alle richieste estere provenienti dai magistrati

dirimere i contrasti tra PM in questa materia. Purtroppo il trend per quanto riguarda i crimini informatici è in costante aumento sin dagli anni '90 e ciò dipende "*dalla reperibilità dei tools in rete e dalla relativa facilità d'uso. Nel frattempo è molto migliorata la cooperazione internazionale e certamente un allargamento dei Paesi aderenti alla Convenzione di Budapest del 2001 è essenziale"* ci riferisce il Magistrato Corasaniti che aggiunge "*si sta lavorando per aggiornare la Convenzione del Consiglio d'Europa, che è pur sempre del 2001 come impianto di fondo, va implementato il tracking on-line e soprattutto un sistema di ricerca per il cloud che da eccezione sta divenendo la regola."* Ovviamente l'alto livello di transnazionalità di questo tipo di reati pone molti problemi all'esercizio dell'azione penale, come emerge dai dati del precedente rapporto pubblicato da UNICRI[31] e molto potrebbe essere ancora fatto come "*migliorare gli strumenti di cooperazione internazionale che già esistono e che sono definiti dalla Convenzione del 2001, ad esempio definendo con più precisione le regole della competenza giurisdizionale. Di recente la Corte di Cassazione italiana ha stabilito, dirimendo un contrasto tra Tribunali, che in Italia il giudice competente è quello dove si trova l'attaccante. È un criterio preciso che potrebbe essere esteso a livello internazionale. Non dimentichiamo che la stessa nozione di 'sistema informatico' che oggi è riconosciuta nella Convenzione come nozione unitaria si deve ad una posizione precedente della Corte di Cassazione italiana del 1999."* Per quanto attiene la normativa vigente "*come tutte le normative di legge deve essere adeguata all'evolversi della tecnologia, ma il modello comincia a dare effetti positivi. Bisogna superare le diffidenze e fidarsi di un modello di cooperazione pubblico/privato nell'interesse collettivo.*"

È stato chiesto inoltre al Magistrato Corasaniti cosa ne pensasse della realizzazione di un quadro di assistenza, sostegno ed informazione per le PMI in ambito cyber crime, una sorta di linee guida che aiutino qualsiasi tipologia di PMI ad essere maggiormente consapevole di ciò che può fare per difendersi da questo tipo di criminalità. "*Si tratta di uno strumento essenziale. Le PMI rappresentano un perno centrale del sistema dell'economia in UE e sono anche interessate in quanto potenzialmente le migliori vittime del crimine informatico. Finora c'è stata una certa sottovalutazione, ma credo che da qualche tempo le cose stiano cambiando, ed è crescente l'interesse per le PMI alle problematiche del cyber crime, problematica che le coinvolge anche sotto l'aspetto della responsabilità delle persone giuridiche, prevista dalla Convenzione del 2001 ed in Italia dal D.lvo 231/2001. Un modello organizzativo adeguato ed efficace è infatti essenziale per prevenire il cyber crime*."

L'*information sharing* tra le aziende su questo tema, come è emerso anche dalle interviste condotte nello studio precedente, è ancora molto bassa, quasi nulla. L'opinione del Magistrato è che si potrebbe migliorare "*progettando una cooperazione on-line più organica, settore per settore, distinguendo tra frodi, furti di identità ed attacchi ai sistemi. La politica di sicurezza si costruisce condividendo le informazioni."*

Inoltre per cercare di mitigare questo fenomeno, sarebbe utile secondo il Magistrato "*predisporre, come negli USA, portali di informazione specifica e di assistenza alle vittime e*

31 La Criminalità informatica e i rischi per l'economia e le imprese a livello italiano ed europeo, UNICRI, 2014, in <http://www.unicri.it/in_focus/files/Criminalita_informatica_def.pdf> (ultima consultazione 04-07-2015)

rendere possibile la denuncia on-line con link specifici e assistenza in caso di infezioni da malware" e una "*sensibilizzazione più estesa a livello internazionale, e qui sottolineo il ruolo delle Nazioni Unite, e a livello interno con la creazione di una Conferenza di cooperazione che sia presente a livello internazionale, nella quale pubblico e privato svolgano le loro osservazioni e sviluppino le loro proposte, e soprattutto condividano le proprie esperienze, sia quelle negative che quelle positive."*

CAPITOLO 3

Linee guida per le PMI in tema di sicurezza informatica

Nella ricerca "*La criminalità informatica e i rischi per l'economia e le imprese a livello italiano ed europeo*" sono state realizzate numerose interviste a livello locale, a forze dell'ordine, istituzioni e aziende della zona di Lucca. Attraverso queste interviste sono emersi non solo quali siano i maggiori rischi che le aziende corrono quotidianamente e quali siano i tipi di attacco più frequenti, ma soprattutto il loro livello di conoscenza e preparazione di fronte alle minacce informatiche, quali siano i loro gap, cosa dovrebbero implementare e di cosa sentono di aver bisogno per contrastare i rischi derivanti dal cyber crime.

Il primo aspetto che abbiamo registrato è rappresentato dal fatto che le aziende vittima di un attacco spesso si trovano in una situazione di impreparazione, che le porta a non avere chiaro neanche a chi potersi rivolgere non solo per affrontare le conseguenze dell'attacco subito, ma soprattutto per porre in atto azioni affinché questo non si ripeta. Alcune si rivolgono alle forze dell'ordine come la polizia postale, molte solo ai consulenti, spesso locali, a cui hanno affidato la gestione del sistema informatico.

Non sempre però le vittime si accorgono di essere state violate. Le aziende che hanno subito un qualche tipo di attacco informatico o che hanno un minimo di consapevolezza dei rischi che corrono, spesso non sanno cosa fare per proteggersi da questa minaccia e credono erroneamente che le azioni che potrebbero mettere in atto siano solo ed esclusivamente di tipo tecnico e che siano economicamente impegnative. Quello che manca alle PMI del nostro territorio è principalmente un quadro di assistenza all'implementazione della loro sicurezza informatica che comprenda non solo aspetti tecnici quali antivirus, firewall ecc., ma soprattutto uno schema di policy da adottare per costruire un *framework* da modificare, adattare e implementare negli anni in base all'evolversi di questo tipo di minaccia.

Da questo scenario e dall'analisi dei gap esistenti si è pensato di costruire uno schema di linee guida che possa essere il più possibile esaustivo, ma al contempo facilmente

comprensibile e soprattutto adattabile alle diverse tipologie di PMI presenti sul nostro territorio. A tal fine si è pensato di dividere le linee guida in base alle possibili aree presenti in un'azienda, in modo tale che ogni singola PMI sappia quali linee guida poter adottare in funzione della presenza o meno di quell'area all'interno della propria struttura.

All'interno delle aree, le linee guide sono state elencate in ordine di urgenza, e comprendono azioni proattive da adottare sia sotto il profilo tecnico sia sotto il profilo comportamentale, attraverso delle policy semplici ed economiche che possano mitigare uno degli aspetti più critici per le aziende, il comportamento umano. Proprio in virtù della enorme diversità tra una PMI e l'altra e delle evidenti innumerevoli eccezioni, un approccio top down risulta inutile, vano e poco congeniale per ottenere il risultato che ci si prefigge. Non sono le aziende che si devono adattare alle linee guida, ma sono in realtà le linee guida che si devono adattare alle aziende. Dopo un'attenta autovalutazione sarà la PMI stessa ad adattare le linee guida alla propria realtà aziendale.

La sicurezza non deve essere vista come uno stato da raggiungere, ma piuttosto come un processo che coinvolga costantemente tutte le azioni in ambito IT, che diventi parte integrante dei processi aziendali e che possa svilupparsi, modificarsi e implementarsi nel tempo, in base agli sviluppi delle minacce. La cultura aziendale si incrementa solo se si incrementa la cultura individuale di ogni singolo dipendente.

Per creare un documento completo e condiviso abbiamo sottoposto le linee guida redatte alla validazione di esperti di aziende leader in questo settore come: Davide Del Vecchio, Security Operations Center Manager di Fastweb, Pier Luigi Rotondo, Security IT Architect di IBM, Gianfranco Vinucci, Head of Support & Services/Technical Manager di Kaspersky Lab Italia, Carlo Mauceli, Chief Technology Officer e Andrea Piazza, National Security Advisor di Microsoft e gli IT Manager delle aziende coinvolte nella precedente ricerca, Lucart, Lucense e Tagetik, che hanno contribuito grazie alla loro esperienza a rendere il documento più completo ed esaustivo. Inoltre Fastweb, IBM, Kaspersky e Microsoft hanno rilasciato per questo aggiornamento, attraverso i loro esperti di sicurezza, opinioni sui principali aspetti che riguardano l'attuale situazione delle PMI in ambito informatico.

Interviste ad esperti del settore

È stato chiesto a Fastweb, IBM, Kaspersky e Microsoft quali siano, secondo la loro opinione, i problemi maggiori della lotta al cyber crime. Tutti concordano che la mancanza di sensibilità e consapevolezza sono i principali scogli che si incontrano. Nello specifico il dott. Piazza ritiene che uno dei problemi maggiori sia "*lo squilibrio di consapevolezza tra chi attacca e chi difende. Questo vale sia per le grandi aziende che per le PMI. Il livello di sofisticazione degli attacchi al giorno d'oggi è tale che persino aziende con budget estremamente elevati e team di sicurezza dedicati sono state oggetto di attacchi veramente*

rilevanti e di difficile individuazione. Questo si traduce in possibili impatti economici molto seri, che vanno dal danno d'immagine, al furto di proprietà intellettuale, alle richieste di risarcimento danni da parte dei clienti." Il dott. Mauceli specifica che "*la superficie di attacco complessivamente esposta dalla nostra civiltà digitale cresce più velocemente della nostra capacità di proteggerlo".* Il dott. Vinucci aggiunge che "*siamo di fronte a veri e propri gruppi organizzati di professionisti che mirano ad ottenere informazioni di valore e puntano a vittime di alto livello, compresi i governi. Purtroppo accade spesso che all'interno delle aziende non ci siano competenze abbastanza forti per contrastare questo tipo di campagne mirate e che non si riesca a tenere il passo con i cyber criminali. Le conseguenze di ciò purtroppo sono considerevoli per le vittime, prima fra tutte la perdita delle informazioni sensibili quali ad esempio la proprietà intellettuale che può compromettere reti corporate, interrompere processi di business e cancellare dati."*

Le PMI costituisco una realtà differente sia dagli utenti privati che dalle grandi aziende. Questa differenza porta ovviamente a sviluppare dei vantaggi e degli svantaggi peculiari nel contrastare questo tipo di fenomeno. Chiarissimo è al riguardo il dott. Del Vecchio, secondo il quale il ridotto budget a disposizione e la scarsa sensibilità all'argomento costituisco senza dubbio i maggiori svantaggi per una PMI che al contempo può contare però su una maggiore flessibilità rispetto ad una grande azienda grazie "*alla minore burocrazia e alla possibilità di agire direttamente per correggere i problemi".* Indipendentemente dalla dimensione di un'azienda, vi sono delle best practices che dovrebbero essere osservate come semplici pratiche quotidiane per la protezione degli *asset* aziendali. È l'opinione del dott. Rotondo, secondo il quale "*così come periodicamente controlliamo la sicurezza della nostra autovettura, l'efficienza dell'impianto frenante, lo stato di usura dei pneumatici, allo stesso modo dovremmo fare per i nostri strumenti informatici. Una PMI paga indubbiamente i costi di accesso a soluzioni tecnologicamente avanzate di sicurezza delle informazioni.*" Il pericolo purtroppo è che le PMI sottovalutano molto questo fenomeno. "M*olte PMI pensano che le loro dimensioni non le rendano appetibili agli occhi dei criminali informatici e che non abbiano dati sufficientemente interessanti per essere presi di mira. In realtà questo non è vero. Gli imprenditori, infatti, dovrebbero tenere conto del fatto che quando effettuano i pagamenti con carta di credito, archiviano le informazioni di un cliente o elaborano piani per la creazione di nuovi prodotti, sono in possesso di informazioni preziosissime per i criminali informatici. Una PMI senza protezione è un 'bersaglio facile' e anche se il guadagno che un criminale informatico riesce ad ottenere da ciascuna vittima sarà più basso di quello che otterrebbe attaccando una grande azienda, richiede uno sforzo minimo e questo spinge i criminali ad attaccare con successo numerose PMI. Le grandi aziende generalmente hanno le risorse necessarie per far fronte alle perdite derivanti da un attacco informatico, che possono ammontare anche a milioni di dollari, a seconda del tipo di attacco. Si tratta di costi relativi ai dati persi dei clienti, al tempo trascorso offline e alle spese necessarie al ripristino dell'infrastruttura. Per le piccole imprese, invece, un attacco di questo tipo e i conseguenti danni economici possono essere sufficienti a causare un fallimento*".

A rischio infatti non sono solo i budget aziendali, ma anche i piani industriali e di sviluppo, il know-how di un'azienda e l'economia dell'intero sistema Paese. Una PMI dovrebbe interrogarsi su quanto conosce realmente sul cyber crime, su cosa sta facendo per proteggere il proprio business e su come fare a proteggere i propri dati e i propri *asset* vitali. È prioritario quindi aumentare il grado di conoscenza e consapevolezza del cyber crime, che purtroppo è ancora molto basso. "*Partire dalla sensibilizzazione di chi utilizza strumenti informatici. Occorre spiegare loro come riconoscere ed evitare i comportamenti a rischio. Aprire un file allegato ad una e-mail che non aspettavamo, scaricare del software del quale non si è in grado di valutare con assoluta certezza la genuinità e la fonte, utilizzare sui social le stesse password dei sistemi aziendali, ignorare i messaggi con il quale il nostro sistema ci informa che ci sono aggiornamenti di software disponibili, conservare il disco di backup nella stessa borsa dove conserviamo il nostro computer. Sono tutti comportamenti a rischio, dei quali non tutti sono consapevoli. E qui parliamo veramente di pratiche di base per le quali non ci sono assolutamente scuse. Occorre informare che nella migliore delle ipotesi le PMI rischiano di perdere per sempre informazioni vitali per la continuità del business aziendale, con ricadute dirette sulla capacità di rimanere sul mercato. Un'azienda può non essere più in grado di risollevarsi da un attacco di cyber crime ben assestato*" questo è quanto riferitoci dal dott. Rotondo. Il dott. Vinucci di Kaspersky sottolinea inoltre l'importanza di investimenti maggiori in campagne educative sulla sicurezza informatica, per evidenziare le minacce rivolte alle PMI e le misure che esse possono adottare per ridurre i rischi derivanti da questo tipo di criminalità, infatti "*il problema è che la maggior parte delle imprese (come le persone in generale) tendono ad ascoltare gli avvertimenti e i consigli solo dopo essere stati colpiti da un disastro. Spesso la realtà è quindi l'insegnante più efficace. È solo quando la propria società viene hackerata, oppure quando un'altra azienda nota viene colpita e si diffonde la notizia, che le aziende acquisiscono maggiore conoscenza e consapevolezza dei crimini informatici. A fare notizia sono gli attacchi alle grandi imprese e questo fa spesso pensare alle aziende di piccole dimensioni di non essere obiettivi interessanti per i criminali informatici."* Oltre a delle campagne di sensibilizzazione, secondo il dott. Piazza purtroppo potrebbe rendersi necessario imporre l'adozione di specifiche misure come "*l'obbligo di segnalare le compromissioni, di formare il personale, di adottare specifiche misure di sicurezza, e di prevedere in azienda un responsabile della sicurezza IT*".

Sulla necessità di incentivare il grado di condivisione tra le aziende e le istituzioni sulle informazioni inerenti i rischi in ambito cyber attraverso obblighi concorda anche il dott. Del Vecchio di Fastweb. Il dott. Vinucci sottolinea che "*i criminali informatici operano in un ambiente senza confini, quindi abbiamo bisogno di combatterli creando relazioni aperte e di lavoro tra i settori pubblico e privato, così come tra le nazioni. La collaborazione e la condivisione delle informazioni sono due delle armi più potenti che abbiamo in questa lotta, quindi incoraggiare la fiducia e la trasparenza nel settore è di fondamentale importanza*".

Il rischio nell'affrontare un tipo di criminalità come il cyber crime è quello di non stare al passo con un fenomeno che si evolve così rapidamente. Per questo è necessario predisporre delle azioni di prevenzione mirate. Si è chiesto agli esperti quali siano le più urgenti. Secondo Kaspersky "*in primo luogo, le piccole e medie imprese devono rendersi conto che la minaccia rappresentata dalla criminalità informatica è reale. Il governo ha una responsabilità fondamentale nel garantire che le imprese nel loro complesso capiscano questo. In termini di misure specifiche per le PMI, direi che il punto di partenza per qualsiasi azienda è quello di valutare i rischi: quali sono gli asset aziendali (proprietà intellettuale, dati dei clienti, ecc.), chi vuole attaccare la società e con quali mezzi potrebbe cercare di farlo. Valutati questi aspetti, l'azienda ha bisogno di tracciare una strategia per ridurre i rischi. La tecnologia è importante (anti-malware, firewall, crittografia, ecc.), ma non è sufficiente. L'azienda deve anche definire le policy e le procedure che riducono il rischio di esposizione. Per esempio, la segmentazione della rete per rendere più difficile la diffusione dell'attacco. Inoltre, è essenziale sensibilizzare i dipendenti, infatti, molti attacchi oggi hanno inizio proprio a causa di qualche imprudenza dei dipendenti che in modo inconsapevole mettono a repentaglio la sicurezza dell'azienda. È quindi importante cercare di evitare possibili danni causati dagli 'umani' e proteggere allo stesso tempo gli asset digitali dell'azienda. È importante vedere la sicurezza come un processo."* Microsoft a riguardo aggiunge un concetto fondamentale e cioè "*definire nei percorsi scolastici un rafforzamento dell'istruzione informatica e delle specializzazioni legate alla cyber security, prevedendo forti partnership tra il mondo privato e quello universitario: è necessario mettere sul mercato un maggior numero di esperti in questo ambito che abbiano esperienza concreta sul campo*". L'istruzione delle future generazioni gioca un ruolo fondamentale nel bilanciare l'attuale divario tra le competenze di chi attacca e chi è preposto a difendere i sistemi informatici.

Per una minaccia che si evolve così rapidamente è importante altresì cercare di prevedere quali possano essere gli sviluppi futuri. Si è chiesto quindi quali siano a loro avviso i trend che bisogna aspettarsi nell'ambito della sicurezza informatica per le PMI. Per Microsoft "*il 2014 è stato il peggiore dal punto di vista degli attacchi e il 2015 sta mostrando ulteriori peggioramenti della situazione. In questo momento non si può ipotizzare un'inversione di tendenza. Gli attacchi saranno in crescita, avranno impatti più pesanti, colpiranno fasce di popolazione più ampie, che hanno meno familiarità con gli strumenti informatici. Credo sia da prevedere un'espansione degli attacchi sugli strumenti mobile e sugli strumenti legati al fenomeno dell'Internet of Things (IoT)*." "*Sempre di più*" aggiunge il dott. Rotondo di IBM "*vedremo attacchi mirati commissionati da concorrenti oppure da nuove aziende, situate anche in aree geografiche molto lontane, che manovrano per entrare nel mercato anche utilizzando tecniche di criminalità informatica*. *L'automazione dell'attacco consente di prendere di mira una grande quantità di obiettivi e di potenziali vittime. Con la tecnica del watering-hole per esempio vengono compromessi siti web o altre risorse condivise da un determinato gruppo di utilizzatori con malware appositamente configurati per attacchi specifici al gruppo. Catturate le credenziali, i nuovi malware sono in grado di*

riutilizzarle in automatico per proseguire nell'attacco. L'anno che si è appena concluso si è caratterizzato per attacchi Advanced Persistent Threat (APT), basati su malware già noti in passato ma riutilizzati secondo schemi di attacco articolati, mirati a specifiche entità o organizzazioni. Gli attacchi APT basano il loro successo su un accurato studio del bersaglio, preventivo ma che spesso continua anche durante l'attacco, l'impiego di tool e malware sofisticati, e la lunga persistenza nel tempo utilizzando tecniche di offuscamento ed evasione per rimanere inosservati e continuare così a perpetrare quanto più possibile il proprio effetto." Una prospettiva che potrebbe costituire un pericolo enorme per una azienda è, secondo l'opinione del dott. Del Vecchio, il diffondersi di "*azioni di ricatto in cambio dello sblocco di tutta l'operatività aziendale".* Infine il dott. Vinucci di Kaspersky cita come possibili trend in sviluppo quelli relativi all'aumento dei ransomware, dei *Distributed Denial of Service* (DDoS) e inoltre, specificatamente per le PMI, "*gli attacchi 'stepping stone' - in cui un fornitore viene preso di mira come un mezzo per ottenere l'accesso a informazioni che possono aprire le porte a un obiettivo più grande, o più importante - continueranno ad emergere come una grave minaccia per le PMI.*[32] *Il panorama delle minacce è costituito da attacchi casuali (di quelli che affrontiamo tutti noi come individui) e attacchi mirati alle imprese o gruppi di imprese (che operano in un determinato settore di mercato). Purtroppo, le PMI sono soggette a entrambi i tipi di attacco. Mancano le competenze in-house di una grande azienda e gli obiettivi chiave delle PMI sono sensibili ai 'trucchi' del social engineering che consentono ai criminali di rubare la loro identità e accedere ai conti bancari e ai dati confidenziali: in altre parole viene utilizzato lo stesso modus operandi usato per ingannare le persone, ma in una PMI le conseguenze sono più gravi. È per questo che la formazione è una parte essenziale di una strategia di sicurezza aziendale."*

Già dal primo studio condotto da UNICRI sull'impatto del cyber crime sull'economia e le PMI è emersa l'importanza fondamentale di sostenere le aziende con un quadro di assistenza ed informazione specifico per loro in ambito cyber crime. A questo proposito tutti gli intervistati concordano sulla necessità ed importanza di un progetto di questo tipo. *"Sono assolutamente d'accordo, sia con piani di formazione al personale, che con aggiornamenti periodici del fenomeno cyber crime, da sempre estremamente mutevole"* ci dichiara il dott. Rotondo di IBM "*i fenomeni cyber crime che abbiamo osservato in questi ultimi mesi erano inimmaginabili solo qualche anno fa. Dal punto di vista architetturale avevamo dei meccanismi di sicurezza che consideravamo come garanzia di sicurezza totale. Alcuni di questi meccanismi sono stati sovvertiti e resi obsoleti. Al tempo stesso sono convinto che tra qualche anno saremo di fronte a schemi di attacco che ora non riusciamo nemmeno ad ipotizzare. Un qualsiasi quadro di assistenza, sostegno ed informazione per le PMI deve*

32 Abbiamo già visto alcuni esempi di questo tipo di attacco. Per esempio, nel 2011, alcuni criminali si sono infiltrati nelle reti informatiche di alcune aziende che operano nel porto di Anversa e questo ha permesso loro di controllare i movimenti dei container e contrabbandare droga. Per approfondimenti si legga: "Police warning after drug traffickers' cyber-attack", di Tom Bateman, 16-10-2013, in <http://www.bbc.com/news/world-europe-24539417> (ultima consultazione 22-06-2015)

tenere conto di tutto questo, rivedendo periodicamente le soluzioni proposte e sensibilizzando le PMI sul fatto che il cyber crime muta per adattarsi ai meccanismi di difesa che le organizzazioni adottano."

"*È un'idea estremamente positiva,*" aggiunge Kaspersky. "*Sappiamo che le PMI spesso hanno budget IT limitati e quindi non hanno la possibilità di affidarsi a consulenti di sicurezza dedicati. Sappiamo anche che le PMI sono sempre più un bersaglio dei criminali informatici, che ostacolano o danneggiano il loro business. Anche se non sono l'obiettivo finale, le piccole e medie imprese sono sempre più prese di mira dai criminali informatici come anelli di una catena, un anello debole per ottenere l'accesso ai sistemi on-stream di un partner. La criminalità informatica è una questione importante che non accenna a diminuire. Anzi in realtà, nel corso degli ultimi anni è andato peggiorando. È di vitale importanza che le imprese di tutte le dimensioni - ma in particolare le piccole e medie imprese che costituiscono una così grande parte delle imprese totali - abbiano accesso al supporto, alla formazione e alle informazioni che possono contribuire a migliorare le loro difese*."

Linee guida per le PMI

Di seguito uno schema riassuntivo delle linee guida[33] redatte pensando alle esigenze delle PMI, emerse soprattutto dalle interviste empiriche condotte nel precedente studio. Tali linee guida infatti nascono dalla necessità di fornire un vademecum il più completo possibile, che possa essere utile alle PMI per capire cosa possono fare per la sicurezza dei loro dati, del loro business, del loro know-how e della loro infrastruttura aziendale. Le linee guida sono state redatte pensando alle principali aree presenti in un'azienda. Dopo un breve test di autoanalisi, ogni PMI può cercare le linee guida in base alla presenza o meno di quell'area nella propria struttura. Ad esempio, una piccola società come uno studio professionale può non avere i reparti di produzione e di conseguenza e quindi non seguire le linee guida ad essi relative e fare riferimento solo a quelle per esempio dell'area amministrazione e commerciale dove vi sono policy relative alla tutela dei dati sensibili. Inoltre, con l'aiuto di un consulente informatico, se non si dispone di un reparto IT interno, è necessario valutare le azioni da implementare relative all'area informatica, nella quale sono stati raggruppati gli aspetti più strettamente tecnici, come ad esempio i piani di backup, importantissimi per proteggersi da minacce come quelle del Criptolocker. Pensiamo per esempio ad uno studio di commerciasti nel periodo di consegna delle documentazioni relative ai propri clienti, oppure ad uno studio di architetti dove è cruciale che i progetti per gare di appalto siano conservati in aree sicure della rete aziendale, possibilmente non collegate ad internet. Ovviamente ci sono policy comuni a più aree aziendali, come per esempio la gestione sicura delle password e la formazione per il riconoscimento di e-mail fraudolente. Infatti ormai sono sempre meno le e-mail di phishing scritte in modo scorretto e facilmente individuabili e aumentano sempre di più i casi di spear phishing, azioni mirate molto più difficili da

33 Il testo completo delle linee guida per le PMI verrà fornito previa richiesta ad UNICRI

riconoscere. Riconoscere una e-mail fraudolenta da una reale è qualcosa su cui il personale va costantemente informato e aggiornato. Semplici accorgimenti, come passare per esempio il cursore del mouse sopra il nome del mittente, permettono di verificare che l'indirizzo e-mail coincida con quello visualizzato e non sia in realtà un altro contraffatto ad arte per indurre in errore l'utente. Un esempio di quanto sopra riportato è rappresentato nella figura successiva.

Figura 7 - Esempio di come riconoscere una e-mail di phishing

Come possiamo vedere nell'esempio in figura 7, l'e-mail truffa è stata inviata da un indirizzo di posta @infas.it e non dalla compagnia telefonica Wind, come invece vuole far credere. Inoltre ci sono molti altri indizi, come ad esempio gli errori di punteggiatura e la richiesta di scaricare un file .html sul nostro computer. Tutti questi indizi permettono all'utente di capire che l'e-mail non è autentica, di segnalarla come spam e cestinarla. L'obiettivo di questa e-mail può essere duplice, innanzitutto sottrarre i dati delle carte di credito, e poi infettare il PC per farlo diventare parte di una botnet oppure criptarne i dati per chiedere un riscatto in denaro.

Come si può notare dallo schema riassuntivo delle linee guida si sono identificate sei principali aree aziendali:

- Area amministrazione
- Area commerciale
- Area ricerca e sviluppo
- Area logistica
- Area produzione
- Area informatica

Linee guida per le PMI[34]

Area amministrazione

- Gestione degli account del personale amministrativo
  - Gestione sicura delle password
  - Uso degli indirizzi di posta certificati PEC
- Reparto risorse umane
- Protezione dei dati sensibili riguardanti il personale aziendale
- Uso di dispositivi mobili aziendali (es. smartphone e laptop)
- Uso dei social network
- Gestione degli accessi fisici del personale aziendale

Area commerciale

- Gestione degli account del personale commerciale
  - Gestione sicura delle password
- Gestione dei database clienti e fornitori
  - Protezione dei dati sensibili riguardanti clienti e fornitori
- Gestione della sicurezza nei rapporti con i fornitori
- Fatturazione
  - Protezione dei dati relativi alla fatturazione
- Uso di dispositivi mobili aziendali (es. smartphone e laptop)

Area ricerca e sviluppo

- Gestione degli account del personale di ricerca e sviluppo
  - Gestione sicura delle password
- Protezione del know-how, della proprietà intellettuale e dei beni aziendali (es. brevetti, progetti, cataloghi)
  - Programmazione di un piano di backup e di disaster recovery costante
  - Utilizzare sistemi di criptazione dei dati su tutte le postazioni fisse, laptop, dispositivi mobili e dispositivi esterni (es. HD e chiavette USB)
- Uso di dispositivi mobili aziendali (es. smartphone e laptop)

34 Le linee guida presentate sono state realizzate grazie alla consulenza del dott. Daniele De Nicolò e alla validazione di Fastweb, IBM, Kaspersky, Microsoft e degli IT Manager di Lucart, Lucense e Tagetik

Area logistica

- Gestione degli account del personale logistico
  - Gestione sicura delle password
- Magazzini e movimentazioni di materiali e prodotti
- Uso di dispositivi mobili aziendali (es. smartphone e laptop)

Area produzione

- Gestione degli account del personale di produzione
  - Gestione sicura delle password
- Protezione dei sistemi informatici delle linee produttive automatizzate
- Uso di dispositivi mobili aziendali (es. smartphone e laptop)

Area informatica

- Analisi dell'ecosistema informatico aziendale
- Gestione del sistema informatico
  - Gestione delle postazioni informatiche
  - Sicurezza della rete
  - Gestione degli account aziendali
  - Programmazione di un piano di backup e di disaster recovery costante
  - Cancellazione sicura dei dati dai supporti non più utilizzati (es. HD, DVD/nastri di backup, supporti USB) anche se in fase di smaltimento
  - Politica di criptazione dei dati
  - Gestione dei social network
  - Gestione dei siti pubblici aziendali e dell'e-commerce (se presente)
  - Cosa fare in caso si sia subito un attacco

Figura 8 - Linee guida per la sicurezza informatica nelle PMI

Attraverso l'analisi di queste aree ogni PMI può ritrovare la sua migliore collocazione e quindi è facilitata nel recepire le linee guida più adatte alla propria struttura. Per ogni area sono stati identificati gli *asset* aziendali più importanti e per ognuno di essi sono state evidenziate, cercando di ordinarle per urgenza, delle buone pratiche che aiutino a gestire e mitigare al meglio i potenziali rischi.

Tra queste policy possiamo vedere ad esempio la protezione dei dati sensibili, sia riguardanti il personale aziendale (nomi, informazioni personali e bancarie ecc.) sia relative a clienti e fornitori (nominativi, partita IVA, IBAN, storico fatture ecc.) oppure la gestione del cloud, strumento che suscita sempre più interesse in ambito aziendale, per i vantaggi che può portare soprattutto alle PMI, come l'abbattimento di alcuni costi di gestione e manutenzione delle apparecchiature informatiche. Per aiutare le aziende ad una più consapevole scelta dell'uso del cloud, l'European Union Agency for Network and Information Security (ENISA) ha pubblicato di recente l'*ENISA's security guide and online tool for SMEs when going Cloud*[35], nel quale sono raccolte le 11 maggiori opportunità che i servizi cloud offrono e i maggiori 11 rischi che comportano, oltre a 12 domande che le PMI dovrebbero farsi durante la fase di scelta dell'adozione di soluzioni cloud.

Nella redazione delle linee guida si è data particolare attenzione non solo agli aspetti tecnici, ma anche a quelli comportamentali, dato che la maggior parte delle minacce contano sull'errore umano e possono essere veicolate anche attraverso apparentemente innocue immagini allegate ad un'e-mail[36].

35 Cloud Security Guide for SMEs. Cloud computing security risks and opportunities for SMEs, ENISA, Aprile 2015, in <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/security-for-smes/cloud-security-guide-for-smes> (ultima consultazione 24-06-2015)

36 How to hack a computer using just a image, The Hacker News, di Swati Khandelwal, Giugno 2015, in <http://thehackernews.com/2015/06/Stegosploit-malware.html> (ultima consultazione 2-6-2015)

Conclusioni

L'impatto del cyber crime sull'economia mondiale è sempre più preoccupante. L'asimmetria tra gli strumenti e le conoscenze in possesso dei cyber criminali e quelle di chi si deve difendere o è preposto a contrastare questo fenomeno rappresenta una delle maggiori difficoltà nell'affrontare questo tipo di criminalità. Inoltre la rapida e sempre più economica diffusione in rete dei *tools* malevoli e la loro facilità d'uso permettono anche a chi non ha alte conoscenze tecniche l'accesso alla criminalità informatica. Un'ulteriore minaccia alla sicurezza delle PMI è rappresentata dall'utilizzo sempre più diffuso da parte dei cyber criminali di software legittimi al posto di malware per ottenere l'accesso ai sistemi aziendali. Questo comporta due principali fattori di rischio per le piccole e medie imprese. In primis la maggiore difficoltà da parte dei software antivirus di riconoscere questi programmi come una minaccia. Il secondo fattore di rischio è costituito dalla maggiore velocità con cui gli attaccanti riescono a sfruttare questi software non dovendo programmare malware da zero, ma avendo già una base su cui sviluppare il loro attacco.

Per contrastare un fenomeno così transnazionale come il cyber crime è necessaria una risposta a livello globale, attraverso regolamenti condivisi. Inoltre è fondamentale rafforzare la cooperazione europea ed internazionale attraverso strumenti di collaborazione, meccanismi di *law enforcement* e azioni legislative specifiche per la lotta al cyber crime. A tal proposito si ritiene fondamentale per un'analisi più capillare del fenomeno riportare casi studio, in modo tale che, da ciò che accade, si possa trarre *lesson learned* per capire cosa c'è ancora da fare, come farlo e studiare nuove misure di contrasto e prevenzione. La sicurezza deve essere considerata un obiettivo comune da tutti gli attori coinvolti, sia pubblici che privati, tra i quali devono prevalere logiche collaborative coordinate ed efficaci.

Sostenere le PMI in questo ambito è di vitale importanza per l'economia di una nazione. Attraverso la diffusione di report, articoli e studi su questo argomento la sensibilità nei confronti di questa minaccia sta lentamente aumentando, ma la conoscenza di ciò che all'atto pratico si dovrebbe fare per difendersi risulta ancora troppo bassa. Le start-up, per esempio, sono una realtà molto delicata, sono aziende giovanissime, per la maggior parte del settore IT o comunque con una forte informatizzazione, ma con budget e risorse limitate. Proprio queste realtà spesso considerano secondari gli aspetti relativi alla loro sicurezza e vanno sostenute e considerate un volano per l'economia del sistema Paese. Le piccole aziende commettono spesso il pericoloso errore di pensare che essendo apparentemente troppo piccole e insignificanti rispetto alla grandi aziende non attirino l'interesse dei criminali informatici. In realtà i fattori che i criminali informatici considerano sono semplicemente la presenza di soldi o dati da rubare e la facilità di violare un obiettivo, e le PMI purtroppo soddisfano entrambi questi requisiti. Nell'attuale era digitale la sicurezza informatica e il corretto uso del web e dello strumento informatico da parte di ogni singolo

cittadino, ma soprattutto da parte delle aziende, deve necessariamente essere un elemento da considerare come prioritario. Quello che serve alle aziende è un approccio metodico per la conoscenza e la valutazione dei rischi di natura informatica al fine di creare una gestione sempre aggiornata della propria sicurezza.

Le linee guida presentate in questo rapporto vogliono costituire un passo verso una più adeguata conoscenza, da parte delle PMI, dei rischi che corrono quotidianamente nel *cyber space.* Una PMI dovrebbe interrogarsi su quanto sa realmente sul cyber crime, su cosa sta facendo per proteggere il proprio business e i propri dati e come fare per migliorare il suo livello di sicurezza. Il progetto di UNICRI è quello di diffondere e illustrare queste linee guida all'interno di progetti di formazione per le PMI. Ogni linea guida sarà illustrata e motivata alle aziende spiegando loro cosa possono fare autonomamente e cosa invece fare con l'aiuto di aziende specializzate. Il rischio infatti è che la PMI possa vedere queste istruzioni come qualcosa di astratto e non alla propria portata. È importante quindi illustrare alle PMI la corrispondenza che esiste tra il crimine informatico e il crimine comune attraverso esempi della quotidianità, per cercare di contrastare la bassa percezione di rischio che si ha nei confronti di questo fenomeno. L'obiettivo è quello di rendere più concreto e tangibile un rischio ancora considerato così astratto e lontano dalla realtà.

Il problema nel contrastare la criminalità informatica è principalmente culturale e il primo passo è formare il più possibile l'utente e fornirgli uno schema di gestione delle azioni da mettere in atto per la propria sicurezza informatica. È importante che l'utente superi la convinzione che la sicurezza costituisca un costo troppo elevato da sostenere, in quanto molte soluzioni che innalzano sensibilmente la sicurezza aziendale possono essere implementate anche con investimenti minimi. Inoltre un altro falso mito da sfatare è che la sicurezza sia un costo a fondo perduto, mentre in realtà si possono ottenere notevoli ritorni economici e di immagine soprattutto puntando sull'affidabilità e nel diventare più competitive anche in termini di sicurezza. La vera tassa da pagare non è il costo della sicurezza informatica, ma quello della sua mancanza, che può comportare costi di gran lunga maggiori degli investimenti necessari, come i casi studio riportati hanno evidenziato.

Indice delle figure

Figura 1 - Percentuale Globale Spam, 2012-2014 12
Figura 2 - Totale Ransomware 12
Figura 3 - Dati Fastweb relativi alle motivazioni di attacco 13
Figura 4 - Distribuzione dei download collegati ad un incentivo economico 16
Figura 5 - Ripartizione totale delle transazioni effettive, suddivise per segmento 19
Figura 6 - Distribuzione degli attacchi relativi alla rete monitorata da Certego 21
Figura 7 - Esempio di come riconoscere una e-mail di phishing 35
Figura 8 - Linee guida per la sicurezza informatica nelle PMI 38

Metodologia

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

Nella prima fase si è svolta un'analisi dei repot pubblicati nel 2015 sul fenomeno del cyber crime, redatti dalle maggiori aziende di consulenza informatica (Kaspersky, Verizon, Symantec, Clusit, ecc.) e gli ultimi report pubblicati dai più stimati enti superpartes (ENISA, World Economic Forum, ecc.). Attraverso questa analisi si sono voluti mettere in evidenza i dati riguardanti il cyber crime relativi ai trend del 2015, soprattutto relativi alle PMI.

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 nazionale e con approfondimenti tramite casi studio. Per realizzare queste interviste si sono individuati degli interlocutori chiave.

La terza fase del progetto ha visto la redazione di linee guida di supporto alle PMI, realizzate in base agli esiti delle interviste condotte nel primo rapporto UNICRI sulla criminalità informatica e i rischi per l'economia e le PMI. Tali linee guida sono state poi sottoposte alla validazione di aziende come Fastweb, IBM, Kaspersky e Microsoft, da sempre impegnate nello sviluppo di soluzioni a sostegno delle PMI e alla mitigazione di questo tipo di minaccia.

Bibliografia

Alcatel-Lucent's Motive Security Labs (2014), *Motive Security Labs malware report – H2 2014*, in <https://resources.alcatel-lucent.com/asset/184652> (ultima consultazione 23-03-2015)

Ashford W. (2014), *Top 10 cyber crime stories of 2014*, in Computerweekly, 31-12-2014, in <http://www.computerweekly.com/news/2240236215/Top-10-cyber-crime-stories-of-201> (ultima consultazione 28-04-2015)

Bateman T. (2015), *Police warning after drug traffickers' cyber-attack*, 16-10-2013, in <http://www.bbc.com/news/world-europe-24539417> (ultima consultazione 22-06-2015)

Boscolo M. (2015), *Ecommerce: le frodi costano 794 milioni l'anno*, in Wired Italia, 30-12-2014, in <http://www.wired.it/economia/business/2014/12/30/pagamenti-online-frodi-valgono-794-milioni-lanno> (ultima consultazione 05-03-2015)

Christin N. (2015), *It's All About The Benjamins: An empirical study on incentivizing users to ignore security advice*, di Nicolas Christin, Serge Egelman, Timothy Vidas e Jens Grossklags, INI/CyLab, Carnegie Mellon University, National Institute of Standards and Technology, ECE/CyLab, Carnegie Mellon University, IST, Pennsylvania State University, in <https://www.andrew.cmu.edu/user/nicolasc/publications/CEVG-FC11.pdf> (ultima consultazione 07-05-2015)

Clusit (2015), *Rapporto 2015 sulla sicurezza ICT in Italia*

Commissione Europea (2015), *Communication from the commission to the European Parliament, The Council, The European economic and social committee and the committee of the region, The European Agenda on Security*, Strasburgo, 08-04-2015, in <http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf> (ultima consultazione 09-06-2015)

Department for Business, Innovation and Skills Cabinet Office (2014), *2014 Information Security Breaches Survey,* in <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/307297/bis-14-766-information-security-breaches-survey-2014-executive-summary-revision1.pdf> (ultima consultazione 30-04-2015)

ENISA (2015), *Cloud Security Guide for SMEs. Cloud computing security risks and opportunities for SMEs,* Aprile 2015, in <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/security-for-smes/cloud-security-guide-for-smes> (ultima consultazione 24-06-2015)

European Central Bank (2014), *New report on card fraud shows online fraud increased in 2012*, Press Release 25-02-2014, in <https://www.ecb.europa.eu/press/pr/date/2014/html/pr140225.en.html> (ultima consultazione 05-03-2015)

Ford N. (2015), *Misunderstanding cyber threats puts a third of SME revenue at risk*, 27-02-2015, in <http://www.itgovernance.co.uk/blog/misunderstanding-cyber-threats-puts-a-third-of-sme-revenue-at-risk/> (ultima consultazione 30-04-2015)

Ford N. (2015), *Why SMEs are an attractive target for cyber criminals and what they can do about it*, 02-03-2015, in <http://www.itgovernance.co.uk/blog/why-smes-are-an-attractive-target-for-cyber-criminals-and-what-they-can-do-about-it/> (ultima consultazione 21-05-2015)

Giordano M. e Vaciago G. (2015), *La sicurezza informatica, un asset aziendale strategico*, in Rivista 231 (02-2015) pag. 273

HP (2015), *Cyber Risk Report 2015,* in <http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/> (ultima consultazione 01-05-2015)

Il secolo XIX Tech (2015), *Il 97% di chi naviga su Internet non sa riconoscere il phishing*, 23-05-2015, in <http://www.ilsecoloxix.it/p/magazine/2015/05/23/AR7IpzXE-phishing_internet_riconoscere.shtml> (ultima consultazione 05-05-2015)

Kaspersky Lab (2014), *Consumer Security Risk Survey 2014: Multi-device threats in a multi device world*, Luglio 2014, in <http://media.kaspersky.com/en/Kaspersky_Lab_Consumer_Security_Risks_Survey_2014_ENG.pdf> (ultima consultazione 28-05-2015)

Kaspersky Lab (2015), *Indagine Kaspersky Lab: un utente su quattro non comprende i rischi delle minacce informatiche mobile*, 27-02-2015, in <http://www.kaspersky.com/it/about/news/virus/2015/Indagine_Kaspersky_Lab_un_utente_su_quattro_non_comprende_i_rischi_delle_minacce_informatiche_mobile> (ultima consultazione 10-05-2015)

Khandelwal S. (2015), *How to hack a computer using just a image*, The Hacker News, Giugno 2015, in <http://thehackernews.com/2015/06/Stegosploit-malware.html> (ultima consultazione 02-06-2015)

La Stampa tecnologia (2014), *Acquisti online e frodi: il 44% degli utenti non recupera il denaro*, 24-12-2014, in <http://www.lastampa.it/2014/12/24/tecnologia/acquisti-online-e-frodi-il-degli-utenti-non-recupera-il-denaro-Ft9RDDFyPpYTbyoJi1J96J/pagina.html> (ultima consultazione 20-03-2015)

Pierri M. (2015), *Cybersecurity, così Intelligence e imprese possono collaborare*, 16-03-2015, in <http://www.formiche.net/2015/03/16/cybersecurity-minniti-ruffinoni/> (ultima consultazione 20-03-2015)

Sorbini L. (2015), *Cybersecurity: il 40% delle grandi aziende pronte ad attacchi cyber nel 2018*, Key4biz, 24-02-2015, in <http://www.key4biz.it/cybersecurity-40-delle-grandi-aziende-pronte-ad-attacchi-cyber-nel-2018/> (ultima consultazione 21-05-2015)

Symantec (2015), *Internet Security Threat Report*, Aprile 2015, in <https://know.elq.symantec.com/LP=1542> (ultima consultazione 22-06-2015)

The Guardian (2014), *It's been a great year! Thanks to these Facebook scams for being a part of it...*, 24-12-2014, in <http://www.theguardian.com/technology/2014/dec/24/facebook-scams-malware-naked-videos> (ultima consultazione 10-04-2015)

The Guardian (2014), *How you could become a victim of cybercrime in 2015*, 24-12-2014, in <http://www.theguardian.com/technology/2014/dec/24/cybercrime-2015-cybersecurity-ransomware-cyberwar> (ultima consultazione 10-04-2015)

Verizon (2015), *2015 Data Breach Investigations Report*, in <http://www.verizonenterprise.com/DBIR/2015/> (ultima consultazione 25-05-2015)

Websense Security Labs (2015), *Websense Threat Report 2015, fare cybercrime è sempre più facile,* 13-04-2015, in <http://www.techfromthenet.it/201504101252/News-analisi/websense-threat-report-2015-fare-cybercrime-e-sempre-piu-facile.html> (ultima consultazione 22-04-2015)

World Economic Forum (2015), *The Global Risks 2015 10th Edition*, in <http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf> (ultima consultazione 06-05-2015)