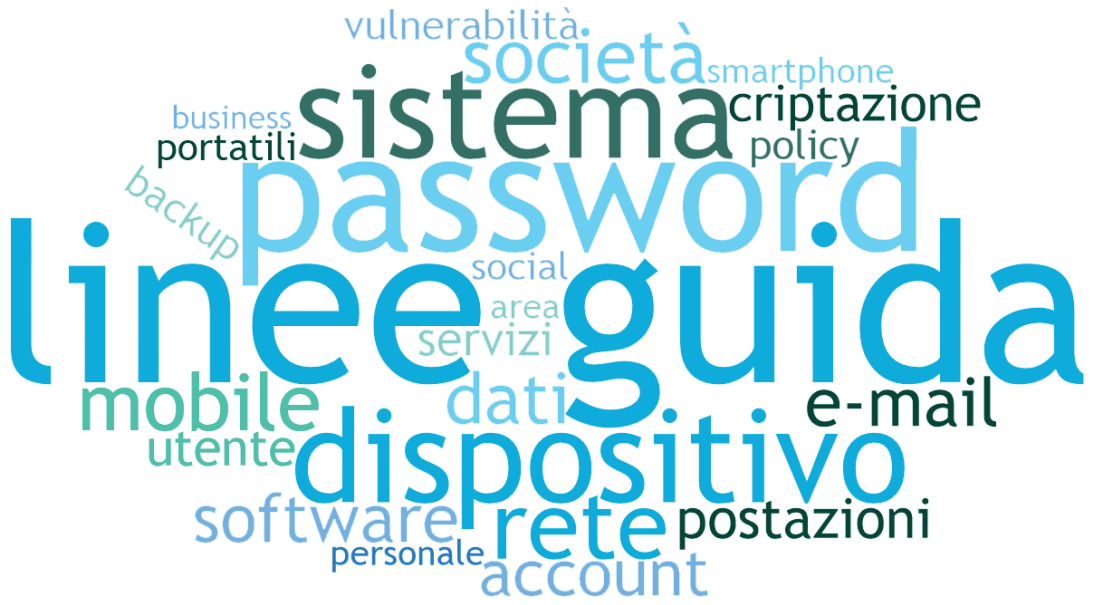
LINEE GUIDA PER LA SICUREZZA INFORMATICA NELLE PMI



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

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.

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.

Le PMI, costituendo il 99,8% delle imprese europee e il 99,9% di quelle italiane, con 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.

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

[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,

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.

Le PMI sono un bersaglio molto attraente per i cyber criminali ma purtroppo sottovalutano ancora troppo questa minaccia. **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.

I pericoli a livello aziendale sono costituiti non solo dai danni prodotti dall'attacco in sé, ma soprattutto dalle conseguenze che questi attacchi causano nel lungo periodo. Assistiamo infatti sempre più ad attacchi mirati come l'appropriazione dei dati sensibili, la cancellazione dei dati stessi o il furto di materiale coperto da copyright.

La criminalità informatica 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.**

Nel 2014 a causa di attacchi su larga scala sono stati compromessi **un miliardo di record**[3], quindi in media uno ogni tre utenti di internet. Molti di questi erano totalmente in chiaro e quindi facilmente sfruttabili.

Il fenomeno del ransomware non accenna a diminuire. Questo tipo di attacchi 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, l'utente pur di recuperare i propri dati è disposto a pagare il riscatto.

Alcatel-Lucent's Motive Security Labs[4] 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).

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] *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)

[4] *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)

Il phishing rimane ancora uno dei metodi di attacco più usati. Nonostante sia forse la tecnica di attacco informatico più conosciuta, ancora oggi gli utenti che cliccano su e-mail di phishing costituiscono percentuali altissime. **Gli 80mila incidenti di sicurezza analizzati nel *Data Breach Investigation report* di Verizon[5] hanno portato a perdite di dati per un danno economico di più di 400 milioni di dollari per le aziende coinvolte.** 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.

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 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.

Non sempre però le aziende si accorgono di essere state violate e spesso non sanno come proteggersi, credendo erroneamente che le azioni da mettere in atto siano solo di tipo tecnico e che siano economicamente impegnative.

Quello che manca alle PMI è principalmente un quadro di assistenza all'implementazione della loro sicurezza informatica che comprenda non solo aspetti tecnici, ma soprattutto uno schema di policy da implementare negli anni in base all'evolversi del cyber crime. **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.**

Le linee guida stilate sono state validate da esperti del settore di 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.

[5] *2015 Data Breach Investigations Report*, Verizon, in <http://www.verizonenterprise.com/DBIR/2015/> (ultima consultazione 25-05-2015)

MICROSOFT "*La superficie di attacco complessivamente esposta dalla nostra civiltà digitale cresce più velocemente della nostra capacità di proteggerlo".*

KASPERSKY *"Le piccole e medie imprese devono rendersi conto che la minaccia rappresentata dalla criminalità informatica è reale. 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".*

IBM "*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".*

FASTWEB *"Un quadro di assistenza, sostegno ed informazione per le PMI in ambito cyber crime più che utile, è necessario".*

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

unicri
United Nations Interregional Crime and Justice Research Institute

Linee guida per la Sicurezza Informatica nelle PMI[6]

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.

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

[6] 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