Le best practice in materia di cyber-security per le PMI

di Stefano Mele

Abstract

Qual è il miglior modo per affrontare, nell'attività quotidiana delle piccole e medie imprese italiane, le minacce provenienti dal cyber-spazio? Stefano Mele – esperto di diritto delle tecnologie, privacy e sicurezza delle informazioni e già autore de I principi strategici delle politiche di cybersecurity – approfondisce questo tema, sia da un punto di vista legale che di policy, delineando alcune best practice in materia di cyber-security per le PMI.

Partendo dall'osservazione, supportata dai numerosi studi disponibili, che tali imprese rappresentino il principale asse portante e il vero motore economico dell'Europa - e dell'Italia, dove il settore risulta essere il più ampio – e che operino spesso a stretto contatto con molti degli operatori pubblici e privati classificabili come infrastrutture critiche nazionali, l'autore evidenzia il costante incremento delle attività di spionaggio elettronico nel settore. Tali azioni sono principalmente volte a sottrarre know-how e informazioni riservate al fine di minare la competitività – e quindi la sicurezza economica – del Paese. Da tali riflessione, e dal riferimento puntuale e continuo alle legislazioni attualmente presenti, l'autore offre una panoramica sulle misure di sicurezza informatica e le informazioni utili ad arginare questo genere di minaccia.

Profilo dell'autore

Stefano Mele è avvocato specializzato in Diritto delle tecnologie, Privacy e Sicurezza delle informazioni, nonché Coordinatore dell'Osservatorio InfoWarfare e Tecnologie emergenti dell'Istituto Italiano di Studi Strategici Niccolò Machiavelli. È inoltre consulente per organizzazioni nazionali ed estere in materia di cyber-intelligence, cyber-terrorism e cyber-warfare, nonché docente di queste materie presso numerosi Istituti di formazione e di ricerca sia nazionali che esteri.

Introduzione

Nell'ultimo decennio le politiche comunitarie volte a favorire la competitività delle piccole e medie imprese (PMI) hanno visto un notevole incremento. Le oltre 20 milioni di PMI presenti all'interno dei confini dell'Unione Europea rappresentano, infatti, circa il 99,8% del numero totale delle imprese, costituendo pertanto in maniera indiscutibile l'asse portante della crescita e

Questo articolo è pubblicato nell'ambito delle iniziative della sezione Il mondo dell'intelligence nel sito del Sistema di informazione per la sicurezza della Repubblica all'indirizzo www.sicurezzanazionale.gov.it.

dell'occupazione nel nostro quadrante. Basti pensare che circa 86,8 milioni di europei lavorano presso una PMI e il 57,6% della ricchezza dell'Unione dipende da queste realtà imprenditoriali[1].
Contestualmente, il settore delle PMI in Italia – il più grande dell'Unione Europea per numero di imprese – è attualmente dominato da quasi 3,5 milioni di microimprese (che occupano meno di 10 dipendenti), nonché da un valore complessivo di PMI che tocca quasi i 3,7 milioni, ovvero il 99,9% del numero totale di imprese presenti sul nostro territorio. Ben 12 milioni di italiani, infatti, lavorano presso una PMI, producendo il 68% della nostra ricchezza[2].

Anche solo dalla semplice lettura di questi dati, si può ben comprendere quanto la sicurezza delle informazioni utili al business di questo settore sia un elemento quanto mai fondamentale per la sua stabilità e soprattutto per la sua crescita. Sicurezza che passa – ormai in maniera inevitabile – principalmente attraverso la disciplina della sicurezza informatica e delle informazioni.
Occorre evidenziare, infatti, che la digitalizzazione delle informazioni, anche riservate, il loro conseguente accentramento, nonché soprattutto la scarsa percezione dei pericoli derivanti dall'utilizzo delle tecnologie informatiche, hanno fatto sì che lo spionaggio elettronico costituisca – da dieci anni a questa parte – una delle principali minacce alla sicurezza nazionale e alla competitività economica dei sistemi Paese.

Cercare di arginare questo genere di rischi, dunque, anche attraverso una corretta sensibilizzazione delle PMI in merito alle problematiche e ai rimedi in materia di sicurezza informatica e delle informazioni, rappresenta un'esigenza legata non più soltanto alla tutela del know-how italiano e/o all'eventuale protezione dei dati personali trattati dall'azienda, ma costituisce ormai un'azione volta soprattutto al contrasto alle attività criminali e al mantenimento della sicurezza nazionale e della competitività economica del Paese.

La sicurezza informatica e delle informazioni come impegno comune

Il legislatore italiano già da tempo si è preoccupato di dettare delle regole giuridiche vincolanti volte a individuare alcune misure minime di sicurezza da attuare nei casi in cui la qualità delle informazioni contenute nei sistemi informatici di un'azienda renda giuridicamente necessaria la loro protezione. È questo il caso dell'art. 31 del Codice in materia di protezione dei dati personali[3], che pone come regola generale quella secondo cui i dati personali oggetto di trattamento debbano essere "custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico,

[1] European Commission, *A Recovery on the Horizon? Annual Report on European SMEs 2012/2013*, 2013, in <http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/performance-review/files/supporting-documents/2013/annual-report-smes-2013_en.pdf> (ultima consultazione: 2014-06-09).

[2] European Commission, *Enterprise and Industry: 2013 SBA Fact Sheet – Italy*, 2013, in <http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/performance-review/files/countries-sheets/2013/italy_en.pdf> (ultima consultazione: 2014-06-09).

[3] Decreto legislativo n. 196 del 30 giugno 2003, *Codice in materia di protezione dei dati personali*, in <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248> (ultima consultazione: 2014-06-09).

alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta". Peraltro, il successivo art. 34 esplicitamente afferma che il trattamento dei dati personali attraverso l'utilizzo di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B)[4] al Codice, almeno le seguenti misure minime di sicurezza:

a) autenticazione informatica
b) adozione di procedure di gestione delle credenziali di autenticazione
c) utilizzazione di un sistema di autorizzazione
d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici
f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi
g) *[soppressa]*
h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Oltre a quanto previsto dal legislatore italiano, occorre evidenziare, tuttavia, come siano ormai numerosi i documenti contenenti standard e best practice, validate e riconosciute a livello internazionale dalla comunità di esperti del settore, che hanno come scopo proprio quello di esplicitare i requisiti e i controlli utili a un corretto processo di gestione della sicurezza informatica e delle informazioni. Lo standard ISO/IEC 27001[5], il framework COBIT[6] e il NIST SP 800-53 (Rev. 4)[7] rappresentano senz'altro i più importanti documenti per un approccio a questa materia completo, di respiro internazionale e soprattutto costantemente aggiornato.

Peraltro, non può di certo sorprendere che anche i governi di tutto il mondo abbiano ormai posto la cyber-security come argomento prioritario all'interno della propria agenda politica e che, dall'analisi comparata delle cyber-strategy attualmente pubbliche, si possa evincere come uno dei pilatri strategici condivisi a livello internazionale sia proprio quello volto a incrementare i livelli di

---

[4] Decreto legislativo n. 196 del 30 giugno 2003, *Codice in materia di protezione dei dati personali*, Allegato B – Disciplinare tecnico in materia di misure minime di sicurezza, in <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1557184> (ultima consultazione: 2014-06-09).

[5] Per approfondimenti, ISO/IEC 27001, *Information Security Management*, in <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm> (ultima consultazione: 2014-06-09).

[6] Per approfondimenti, COBIT 5, in <http://www.isaca.org/cobit/pages/default.aspx> (ultima consultazione: 2014-06-09).

[7] Per approfondimenti, NIST Special Publication 800-53, Revision 4 – Security and Privacy Controls for Federal Information Systems and Organizations, in <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf> (ultima consultazione: 2014-06-09).

sicurezza, affidabilità e resilienza delle reti e dei sistemi informatici[8]. Ciò soprattutto perché in molti di questi Paesi la protezione dei sistemi informatici critici per la sicurezza nazionale è demandata e gestita direttamente da soggetti privati e non dai governi.
Di conseguenza, ciò ha comportato, soprattutto in area americana/anglosassone, lo sviluppo e la pubblicazione di documenti[9] governativi volti a indicare al settore privato le misure di sicurezza ritenute più idonee per proteggere i sistemi informatici e le informazioni ivi contenute[10].

Anche l'Italia, attraverso il Decreto del Presidente del Consiglio dei Ministri del 24 gennaio 2013[11], ha posto in evidenza – tra le altre cose – come la sicurezza informatica e delle informazioni sia un compito di tutti, tanto dei governi quanto delle società private. L'art. 11 del DPCM, infatti, evidenzia proprio il ruolo chiave svolto in quest'ambito dagli operatori del settore privato, chiedendo a coloro che "forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico, [così come a] quelli che gestiscono infrastrutture critiche di rilievo nazionale ed europeo, il cui funzionamento è condizionato dall'operatività di sistemi informatici e telematici" di "adottare le best practices e le misure finalizzate all'obiettivo della sicurezza cibernetica, definite ai sensi dell'art. 16-bis, comma 1, lett. a), del Decreto legislativo n. 259/2003, e dell'art. 5, comma 3, lett. d), del presente Decreto"[12].

Le best practice in materia di cyber-security per le piccole e medie imprese

La messa in sicurezza dei sistemi informatici e delle informazioni in essi contenute raramente può essere vista come un processo sintetizzabile in pochi principi, men che mai quando l'obiettivo è

[8] Mele S., *I principi strategici delle politiche di cyber-security*, Sistema di Informazioni per la Sicurezza della Repubblica, 2013, in <http://www.sicurezzanazionale.gov.it/sisr.nsf/il-mondo-intelligence/principi-strategici-delle-politiche-di-cyber-security.html> (ultima consultazione: 2014-06-09)..

[9] Per approfondimenti, The National Institute of Standards and Technology (NIST), *Preliminary Cybersecurity Framework*, 2013, in <http://www.nist.gov/cyberframework/index.cfm> (ultima consultazione: 2014-06-09).; UK Government Communications Headquarters (GCHQ), *10 Steps to cyber security: executive companion*, 2012, in <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/73128/12-1120-10-steps-to-cyber-security-executive.pdf> (ultima consultazione: 2014-06-09).; UK Government Communications Headquarters (GCHQ), *10 Steps to Cyber Security: Advice Sheets*, 2012, in <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/73129/12-1121-10-steps-to-cyber-security-advice-sheets.pdf> (ultima consultazione: 2014-06-09).; French Network and Security Agency (ANSSI), *40 essential measures for a healthy network guide*, 2013, in <http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_v1-2-1_en.pdf> (ultima consultazione: 2014-06-09).

[10] Questa iniziativa, tuttavia, seppure indubbiamente lodevole, pare aver avuto purtroppo scarsi risultati, soprattutto negli Stati Uniti. Per approfondire, *President's Council of Advisors on Science and Technology (PCAST)*, *Report to the President on Immediate Opportunities for Strengthening the Nation's Cybersecurity* 2013, in <http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_cybersecurity_nov-2013.pdf> (ultima consultazione: 2014-06-09).

[11] Decreto del Presidente del Consiglio dei Ministri del 24 gennaio 2013, *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale* 2013, in <http://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg;jsessionid=QI0W7ckcZt5e7NUAX7Rj3Q__.ntc-as1-guri2a> (ultima consultazione: 2014-06-09).

[12] Confronta l'art. 11, comma 1, lett. *b)*, del Decreto del Presidente del Consiglio dei Ministri del 24 gennaio 2013, *cit.*.

quello di renderli anche comuni per le esigenze di protezione di una categoria così trasversale e variegata com'è quella delle piccole e medie imprese in Italia. Ciononostante, alcune regole primarie ed essenziali possono essere comunque delineate e poste alla base di un corretto approccio a questo genere di attività.

Le seguenti 15 best practice, dunque, devono essere considerate come assolutamente basilari e ad altissima priorità per qualsiasi piccola e media impresa. Esse sono:

1. Creare una lista di applicazioni considerate affidabili e la cui installazione risulti indispensabile per la produttività aziendale, impedendo l'installazione di qualsiasi altra applicazione.
2. Configurare in maniera sicura tutto l'hardware e il software presente all'interno del parco dei dispositivi aziendali, sia fissi che mobili (come, a esempio, server, workstation, router, switch, computer portatili, smartphone aziendali, ecc.).
3. Svolgere un'efficace ed effettiva politica di correzione delle vulnerabilità sia del sistema operativo, che delle applicazioni, entro un arco temporale ristretto e comunque non superiore alle 48 ore dalla pubblicazione di ciascun aggiornamento di sicurezza (patch).
4. Disattivare l'account di amministratore locale e contestualmente limitare il più possibile il numero degli utenti con i privilegi di 'amministratore/root' sia a livello locale, che di dominio, obbligando, inoltre, questi ultimi a usare account de-privilegiati per le operazioni quotidiane (come la lettura di email e la navigazione in Internet).
5. Configurare gli *account* degli utenti affinché abbiano i privilegi minimi richiesti per eseguire le attività loro assegnate e, di conseguenza, possano prendere visione e utilizzare esclusivamente le informazioni e le risorse condivise dell'azienda utili allo svolgimento della propria attività lavorativa.
6. Impostare per tutti gli utenti una politica di autenticazione attraverso password complesse (non meno di 8 caratteri, alfanumeriche, con l'inserimento di almeno una lettera maiuscola e un carattere speciale), obbligandone la modifica ogni 3 mesi e impedendo l'utilizzo almeno delle 5 password precedentemente utilizzate.
7. Predisporre un'efficace difesa del perimetro della rete aziendale attraverso strumenti informatici – software e/o hardware – volti ad analizzare e proteggere in tempo reale il traffico di rete proveniente sia dall'interno che dall'esterno dell'azienda, al fine di ricercare anomalie, attacchi e/o tentativi di accesso non autorizzati (firewall e network-based intrusion detection/prevention system).
8. Utilizzare su tutto il parco dei dispositivi aziendali – sia fissi, che mobili – sistemi di analisi, identificazione e protezione in tempo reale degli accessi degli utenti, dello stato dei sistemi informatici, dei programmi in esecuzione e del loro utilizzo delle risorse (antivirus, workstation firewall e host-based intrusion detection/prevention system).
9. Implementare specifici sistemi di protezione e stringenti politiche di sicurezza per l'utilizzo delle e-mail e soprattutto degli eventuali file allegati, al fine di diminuire il rischio d'infezione attraverso malware.
10. Impiegare sistemi automatizzati di analisi e filtro dei contenuti web, al fine di impedire la visualizzazione e la navigazione di siti Internet inappropriati e/o potenzialmente pericolosi per la sicurezza dei sistemi.

11. Predisporre un sistema centralizzato di raccolta, archiviazione e analisi in tempo reale dei file di log, sia quelli generati dai sistemi informatici, che quelli originati dalle attività di rete (file da conservare per almeno 6 mesi, come per legge[13]).
12. Prevenire l'uso non autorizzato e la trasmissione di informazioni aziendali riservate attraverso specifiche politiche di data loss prevention.
13. Adottare una politica di utilizzo e controllo quanto più stringente possibile in merito all'utilizzo in azienda dei supporti di memoria rimovibili (le cosiddette "chiavette USB", hard disk esterni, unità CD-ROM esterne, memory card, ecc.).
14. Attuare un'efficiente politica di backup e di disaster recovery volta a prevenire eventuali perdite di dati e ad aumentare il livello di resilienza dei sistemi informatici.
15. Avviare al più presto programmi di formazione del personale sull'utilizzo degli strumenti informatici aziendali, sulla sicurezza informatica e delle informazioni, nonché sulla privacy e la protezione dei dati personali.

Conclusioni

Come evidenziato all'interno del nostro Quadro strategico nazionale[14], "la protezione dello spazio cibernetico è un processo più che un fine" e "la continua innovazione tecnologica introduce inevitabilmente nuove vulnerabilità". È quindi di fondamentale importanza che la sicurezza dei sistemi informatici delle PMI non sia intesa come un mero costo, bensì come un vero e proprio investimento. Un processo in continua evoluzione e aggiornamento volto anzitutto a tutelare il business di quelle aziende che – nei fatti – costituiscono la vera ossatura e il motore dell'industria e dell'economia italiana.

[13] Garante per la protezione dei dati personali, *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*, 2008, in <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1577499> (ultima consultazione: 2014-06-09).

[14] Presidenza del Consiglio dei Ministri, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, 2014, in Sistema di Informazione per la Sicurezza della Repubblica, <http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/quadro-strategico-nazionale-cyber.pdf> (ultima consultazione: 2014-06-09).