# LA SFIDA DELLA **CYBERSECURITY** PER LE IMPRESE ITALIANE

© Cifotart



*LA CYBERSECURITY È UN ARGOMENTO DI STRETTA ATTUALITÀ. NON PASSA GIORNO SENZA LEGGERE DI ATTACCHI CONDOTTI VERSO AZIENDE O ORGANIZZAZIONI GOVERNATIVE. NESSUNA ORGANIZZAZIONE, PICCOLA O GRANDE CHE SIA, PUÒ RITENERSI IMMUNE DALLA POSSIBILITÀ DI ATTACCHI INFORMATICI. È PERTANTO NECESSARIO PRENDERE COSCIENZA DI QUESTO FENOMENO E COSTRUIRE DELLE INFRASTRUTTURE E DELLE PROCEDURE CHE MINIMIZZINO QUESTI RISCHI E, QUALORA POSSIBILE, LI EVITINO. BEN SAPENDO CHE QUALUNQUE POLICY DOVRÀ ESSERE MONITORATA E ADEGUATA AI RISCHI CHE COSTANTEMENTE EVOLVONO E SI MODIFICANO*

di STEFANO SALVADEO
*CEO, Grant Thornton Financial Advisory Services Srl*

e di NICOLA SEGUINO
*IT Partner, Grant Thornton Financial Advisory Services Srl*

Negli ultimi mesi abbiamo assistito a un incremento di notizie su attacchi informatici verso aziende ed enti pubblici e, addirittura, verso Stati sovrani.

Su vari siti specialistici si possono trovare diverse analisi, interessanti o meno, su questo fenomeno, sulle motivazioni dell'incremento della vulnerabilità e sull'incapacità delle organizzazioni colpite di reagire immediatamente diminuendo le conseguenze negative dell'attacco subito.
Addirittura, nella recente campagna presidenziale americana, la *Cybersecurity* è entrata con forza nel dibattito tra i due candidati, tra accuse incrociate a livello mondiale.
Nel presente articolo si intende affrontare il tema della *Cybersecurity* dal punto di vista delle imprese che si trovano a dover

gestire questo rischio, cercando di dare un contributo concreto al dibattito e fornendo qualche spunto per ulteriori riflessioni.

***Cybersecurity:* cos'è?**

Iniziamo con il definire cos'è la *Cybersecurity*.
*Cybersecurity* è l'insieme di tecnologie, processi e pratiche volte a proteggere reti, computer, programmi e dati da attacchi, danni o accessi non autorizzati. In un contesto informatico, il termine sicurezza implica la *Cybersecurity*.
Garantire la sicurezza informatica richiede sforzi coordinati in tutto il sistema informativo. Elementi di sicurezza informatica sono:

- la sicurezza delle applicazioni;
- le informazioni di sicurezza;
- la sicurezza della rete;
- il ripristino di emergenza *(disaster recovery/business continuity)*;
- la formazione per l'utente finale.

Uno degli elementi più problematici della sicurezza informatica è la rapida e continua evoluzione dei rischi. L'approccio tradizionale è stato quello di concentrare la maggior parte delle risorse sui componenti di sistema più cruciali e sulla protezione contro le più grandi minacce note, lasciando senza protezione componenti e rischi apparentemente meno pericolosi. Tale approccio è insufficiente in un contesto come quello attuale. La minaccia cambia più velocemente di quanto faccia la nostra idea del rischio.

**La valutazione del rischio**

Il NIST (*National Institute of Standards and Technology*, ovvero l'ente americano preposto alla gestione delle tecnologie) ha recentemente pubblicato linee guida aggiornate nel suo quadro di valutazione del rischio che raccomandano una migrazione delle strategie verso le valutazioni di monitoraggio continuo e in tempo reale.
Di conseguenza, data l'ampiezza del suo ambito di applicazione, la *Cybersecurity* in primo luogo non può che basarsi su logiche di prevenzione, riduzione e trasferimento del rischio, e su processi di *Risk Governance* applicati però ad un dominio caotico, dai confini e dalle dinamiche sempre mutevoli, che va pertanto presidiato costantemente (24 ore su 24, 7 giorni su 7) da personale qualificato dotato di metodologie di *Risk Management* e con strumenti adeguati (ad esempio *tool* di analisi comportamentale, *big data analytics*, intelligenza artificiale, etc.), capaci di operare in tempo reale.

In secondo luogo, per definire puntualmente la componente esogena del rischio, ovvero la probabilità che una minaccia esterna si realizzi, è necessario impiegare metodologie e strumenti di *Cyber Intelligence* capaci di osservare, tramite un monitoraggio continuo, l'esterno e l'interno con altrettanta attenzione, e di correlare i due domini.
Anche in questo caso si tratta di sviluppare competenze sofisticate e di costruire processi nuovi, diversi rispetto alle prassi consolidate, considerando che oggi – nel migliore dei casi – le organizzazioni sono strutturate solo per osservare ciò che avviene nell'ambito di propri confini prestabiliti (i quali peraltro stanno ormai diventando sempre meno definiti, a causa delle nuove tecnologie).

In terzo luogo è necessario definire, e costantemente aggiornare il proprio modello di minaccia *(Threat Modeling)*, ovvero individuare quali rischi dovranno essere mitigati e quali sono le vulnerabilità della propria impresa, per cercare di sistematizzare le modalità di intrusione da parte degli *hackers* più probabili al fine di identificare le opportune politiche di mitigazione.

Anche questa attività di *Threat Modeling* non può che essere continuativa e deve integrarsi sia con i processi di *Risk Management* che di *Cyber Intelligence*.
I requisiti di affidabilità comprendono, per esempio, sicurezza, attendibilità, *performance*, resilienza e capacità di sopravvivenza a una serie di potenziali situazioni avverse. Adottare politiche efficaci in favore dell'affidabilità è importante solo nella misura in cui i requisiti siano sufficientemente completi e definiti, e possano essere accuratamente valutati.

Negli ultimi anni, in Italia e in Europa, il Legislatore e gli operatori stanno recependo le disposizioni in materia di *Cybersecurity* che sono state adottate anche in altri Paesi, in primo luogo negli Stati Uniti, dove un organismo appositamente creato, il NIST si occupa ogni anno di pubblicare le linee guida sulla disciplina dell'ingegneria dei sistemi in funzione della sicurezza.
Queste includono la protezione della proprietà intellettuale in forma di dati, informazioni, metodi, tecniche e tecnologie usate per creare un sistema adeguato.
Le attività di ingegneria della sicurezza dei sistemi si basano sulla combinazione della consolidata ingegneria delle infrastrutture e su principi, *concept* e tecniche di sicurezza per promuovere, adattare e integrare i relativi principi e pratiche all'ingegneria dei sistemi. Tali attività sono svolte in modo sistematico e coerente per ottenere una serie di risultati in ciascuna fase del ciclo di vita del sistema, compresi concezione, sviluppo, produzione, utilizzo, supporto e disinstallazione.
In Italia tali principi sono recepiti nel *Framework* Nazionale di *Cybersecurity* redatto dal CIS. Il suddetto documento ha molti punti in comune con il *Framework* di *Cybersecurity* del NIST, ma è stato ben tarato sulla realtà produttiva Italiana, fatta in particolare di piccole-medie imprese. Da ricordare che il *Framework* non è uno standard di sicurezza, bensì un quadro di riferimento nel quale possono essere inquadrati gli *standard* e le norme di settore esistenti e future.

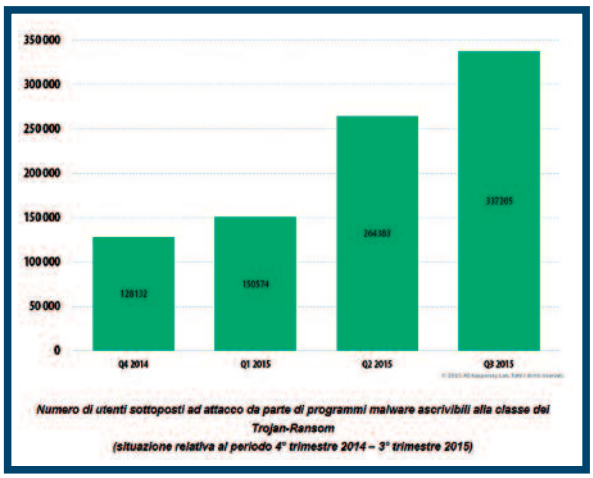
**Chi è a rischio di attacchi?**

Negli ultimi 10 anni abbiamo continuato a connettere qualsiasi dispositivo a internet e abbiamo incominciato a basare tutti i nostri affari su computer e reti interconnesse, quasi sempre senza pensare a renderli sicuri a causa di una percezione falsata del rischio data da due principali pensieri:

*«Perché dovrebbero attaccare proprio me?»* e *«Tanto non è mai successo»*.
Alla prima domanda è facile dare una risposta: i *cyber* criminali attaccano tutti, indiscriminatamente, con *script* di attività completamente automatizzate. Non si è attaccati solo se si hanno informazioni "preziose". Ogni informazione per loro è preziosa, ogni risorsa informatica può essere sfruttata per generare reddito sotto forma di *bitcoin*, per effettuare attacchi DDoS[1], inviare *spam* o rubare credenziali, identità e informazioni che solo in un secondo momento saranno vagliate oppure anche solo rivendute.

Alla seconda obiezione è ancora più semplice dare una risposta, in quanto non solo noi tutti veniamo continuamente attaccati ma anche tutte le nostre aziende vengono regolarmente compromesse.
Chi può affermare di non aver mai avuto un computer infettato da un *malware* nella rete della propria azienda? Quello che un tempo si chiamava *virus* e faceva apparire *popup* più o meno strani, oggi si chiama *malware* e, mentre fa qualsiasi cosa pur di nascondersi, con ancor più efficacia, sottrae qualsiasi dato in nostro possesso.
È così che la scena italiana durante il 2015 riflette ciò che si è visto anche nel resto del mondo: la crescita esponenziale dei *malware* e soprattutto quelli di tipo *ransomware*, ad esempio *Cryptolocker* e simili.
Questi eventi hanno scatenato grossi dibattiti sull'importanza della sicurezza informatica e su quanto sia necessario, ormai, che ogni azienda investa risorse specifiche in questo campo. Inoltre, sono sempre presenti le minacce rappresentate dagli attacchi di tipo DDoS, mirati all'interruzione dei servizi *online* (recente il blocco di Dyndns e di tutta la costa orientale degli Stati Uniti); tutte le aziende che offrono tali servizi possono essere possibili vittime di tali attacchi.

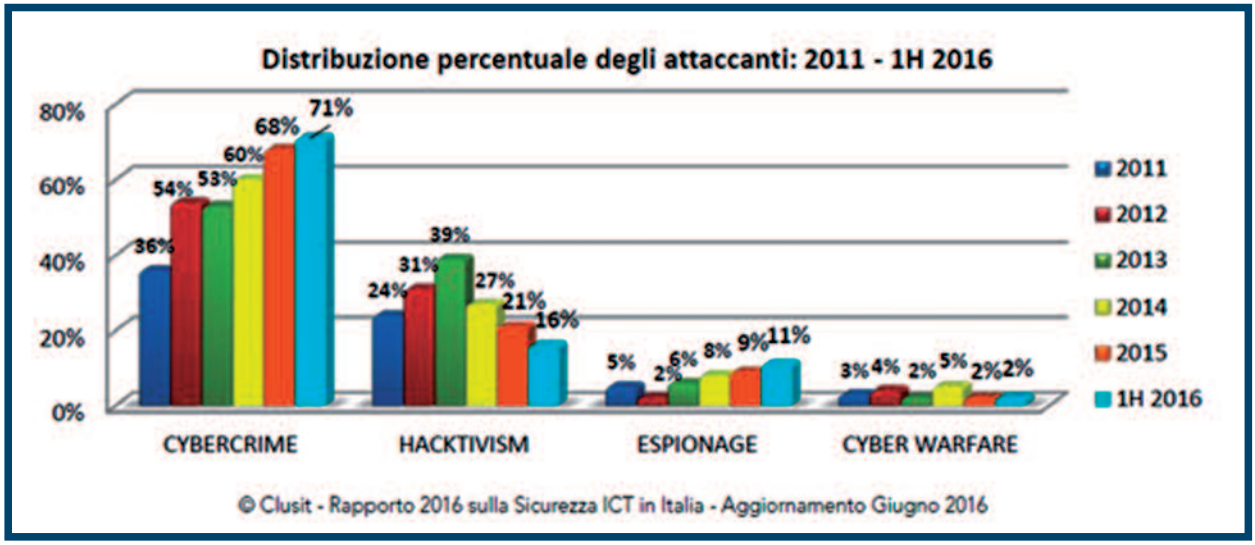
Complessivamente, nel corso del 2015, i *Trojan-Ransom* sono stati rilevati su 753.684 utenti (vedi grafico in basso). Il *ransomware*, quindi, sta divenendo un problema sempre più serio e allarmante.
A livello mondiale, nel corso del terzo trimestre 2016, una consistente porzione degli utenti della Rete (20,2%), anche per una sola volta, è risultata sottoposta ad attacchi informatici provenienti dal *web* e imputabili alla classe dei *malware*. Va tenuto presente che tali dati rappresentano solo una frazione, per quanto significativa, del totale degli attacchi gravi presumibilmente andati a buon fine nel corso del terzo trimestre di quest'anno. Tale campione, infatti, presenta ragionevolmente delle lacune, dovute al fatto che alcuni ambienti sono particolarmente efficaci nel minimizzare la diffusione pubblica di informazioni relative agli attacchi che subiscono, e risultano pertanto qui sotto-stimati. Inoltre, mentre ad oggi negli Stati Uniti è in vigore una normativa che obbliga le vittime a fare *disclosure* a seguito di un *data breach*, così non è nella maggior parte delle altre nazioni (Italia inclusa); di conseguenza gli attacchi noti contro bersagli americani risultano essere la maggioranza. Infine, alcuni tipi di attacchi (i più subdoli e silenziosi, per esempio quelli legati allo spionaggio industriale o ad attività di *Information Warfare*) sono compiuti nell'arco di periodi piuttosto lunghi e dunque, sempre che diventino di dominio pubblico, emergono solo ad anni di distanza.



*Numero di utenti sottoposti ad attacco da parte di programmi malware ascrivibili alla classe dei Trojan-Ransom*
*(situazione relativa al periodo 4° trimestre 2014 – 3° trimestre 2015)*

Non vi è alcun dubbio che la consapevolezza pubblica stia sensibilmente crescendo, riguardo al problema di sicurezza IT in questione, ma appare ben evidente come gli utenti privati e le organizzazioni stesse non facciano ancora abbastanza per combattere una simile minaccia. Secondo il rapporto CLUSIT 2016, in Italia, solo nel primo semestre ci sono stati 521 attacchi gravi di pubblico dominio. Questa è solo la punta dell'iceberg, sia perché la maggior parte di tali aggressioni non diventano di dominio pubblico, sia perché spesso le conseguenze più gravi si evidenziano ad anni di distanza (per esempio nel caso di furto di proprietà intellettuale con finalità di spionaggio economico, o di compromissione preventiva di sistemi critici per ragioni geopolitiche).

**Come affrontare il rischio**
Alcune regole pratiche e basiche possono limitare la probabilità di compromissione dei nostri sistemi e delle proprie credenziali, riducendo l'impatto di potenziali azioni fraudolente:
- fare *backup* periodici dei propri dati[2];
- diffidare di *email* non attese, o provenienti da mittenti sconosciuti o non credibili, specie se invitano ad aprire un allegato o cliccare su un *link*;
- attivare sull'*antivirus* la funzione di navigazione sicura e verifica dei *link*;
- attivare su tutti i *browser* le funzioni di navigazione sicura e verifica dei *link*;
- usare la massima cautela nell'aprire allegati, attendere comunque sempre che l'*antivirus* ne completi la scansione;
- mantenere aggiornato il Sistema Operativo e tutto il *software* applicativo, abilitando i meccanismi di aggiornamento automatico e verificandone periodicamente il corretto funzionamento;
- verificare il corretto funzionamento dell'*antivirus*, in particolare relativamente agli aggiornamenti delle signature che devono essere quotidiani e andare sempre a buon fine




in quanto alcuni *malware* cercano di sovvertire il meccanismo di aggiornamento dell'*antivirus*;
- di fronte a chiari segnali di *phishing*, segnalare il fenomeno attraverso gli strumenti messi a disposizione dai *browser*.

Le grandi organizzazioni dovrebbero inoltre implementare strategie più articolate per evitare o limitare attacchi *Corporate*, come ad esempio:
- sensibilizzare i collaboratori sull'esistenza di attacchi mirati a specifiche organizzazioni, particolarmente convincenti e perpetrati attraverso schemi di *spear phishing* o *watering-hole*;
- utilizzare servizi di *IP address reputation* che consentano il blocco selettivo di IP, siti e URL ritenuti pericolosi;
- bloccare, laddove consentito dai *firewall* perimetrali, il traffico verso le reti di anonimizzazione, in quanto questo limita il meccanismo di comunicazione di molti *malware*;
- addestrare il personale a riconoscere tentativi di *phishing*, anche attraverso simulazioni.

Il Regolamento Generale sulla Protezione dei Dati (GDPR, *General Data Protection Regulation*), Regolamento UE 2016/679, adottato nell'aprile scorso dalla Commissione Europea, e che entrerà in vigore nel mese di maggio 2018, richiederà di fatto, alle aziende, di notificare all'apposita autorità di regolamentazione le fughe di dati subite; tale provvedimento contempla, tra l'altro, l'applicazione di considerevoli sanzioni, in caso di mancata protezione dei dati personali.

Il GDPR è un Regolamento con il quale la Commissione Europea intende rafforzare e unificare la protezione dei dati personali entro i confini dell'Unione Europea (UE). Affronta anche il tema dell'esportazione di dati personali al di fuori dell'UE.

Queste sono alcune tra le principali novità introdotte dal GDPR per le imprese:
- le aziende pubbliche e private con un numero maggiore di 250 dipendenti dovranno nominare al loro interno un *Data Protection Officer* (DPO), un responsabile per la protezione dei dati con il compito di garantire il pieno rispetto della normativa;
- le sanzioni per le aziende che violeranno le disposizioni del GDPR saranno aumentate: fatti salvi i minimi di legge, si potrà arrivare fino al 4% del fatturato annuo dell'impresa;
- in caso di violazioni dei dati personali *(data breach)* al proprio interno, per esempio accessi non autorizzati, l'azienda dovrà notificare il fatto all'Autorità e ai propri utenti entro un periodo prestabilito dal momento della scoperta della violazione;
- le società dovranno rispondere al requisito del p*rivacy impact assessment*, effettuando una valutazione complessiva dell'impatto della normativa all'interno della propria impresa;
- dovrà essere applicato il principio generale del *privacy by design*, ossia la necessità di prevedere specifiche misure tecniche e organizzative a protezione dei dati, dal momento della progettazione di un prodotto e di un servizio;
- dovrà essere riconosciuto agli interessati il diritto all'oblio, cioè la possibilità di decidere quali informazioni personali far circolare (specialmente *online*), dopo un periodo di tempo, eccetto specifiche esigenze (es. obblighi di legge);
- dovrà essere garantito agli interessati il diritto alla portabilità del dato: ossia la facoltà di trasferire, ad esempio, i propri dati da un soggetto giuridico a un altro.

**Conclusione**

Il compito fondamentale della *Cybersecurity* è la protezione e la tutela della missione delle organizzazioni/aziende dai rischi derivanti dal *cyberspace* e dai sistemi informativi.
Tutte le organizzazioni sono esposte a una moltitudine di rischi di varia natura.
La connettività aumentata ha moltiplicato il rischio di attacchi informatici da parte degli *hacker*.
È quindi fondamentale che le imprese si dotino di *best practice* al loro interno, nonché verifichino i loro sistemi informatici anche dal punto di vista della sicurezza esterna.
Solo un approccio proattivo e continuativo potrà minimizzare gli effetti negativi di questo fenomeno. Fenomeno che potrà essere controllato e gestito, ma non del tutto eliminato.

(1) *Variante di attacco DoS. Il DoS è un attacco informatico che mira a esaurire le risorse di un sistema informatico (sia esso locale, sia di rete).*
(2) *Non essendo possibile allo stato delle cose decriptare i dati, il ripristino da un backup è al momento l'unica strada perseguibile nel caso in cui si dovesse cadere vittima di un crypto-ransomware.*