

## **Testare la capacità di protezione del proprio sistema per la sicurezza**

***In uno scenario IT profondamente cambiato e in evoluzione, dove i confini della rete sono sempre più confusi e le risorse sono sempre più "liquide", dove cloud, virtualizzazione, mobilità e consumerizzazione aumentano la complessità dell'infrastruttura, predisporre una protezione efficace dell'azienda e dei suoi asset diventa un compito quanto mai arduo.***

***Come è possibile essere certi che, pur avendo investito pesantemente e con attenzione nella sicurezza dei dati, si sarà in grado di resistere alle minacce provenienti dal cyberspazio?***

***In realtà molte imprese non lo sono, anzi hanno spesso la certezza del contrario e non sanno nemmeno valutare se gli investimenti effettuati sono corretti e commisurati al costo di una violazione della sicurezza.***

***Il white paper analizza la caratteristiche dei servizi offerti da IBM per il test di penetrabilità della rete o penetration test. Saranno anche presentati i risultati di alcune ricerche realizzate dal Ponemon Institute sul costo della perdita dei dati.***

Transazioni commerciali, processi decisionali, proprietà intellettuali sono alcuni esempi delle grandi quantità di dati che ogni impresa deve proteggere per salvaguardare la propria sopravvivenza e garantirsi il successo.

È per questo che diventano sempre più stringenti le normative in tema di sicurezza dei dati: ingannevolmente catalogate come "privacy", tali normative non servono a proteggere la riservatezza di chi si mette già a nudo sui social network, ma forniscono, soprattutto alle imprese, un'indicazione e direttive sull'importanza di proteggere i loro asset, brevetti compresi, che nel terzo millennio sono di fatto digitali.

La compliance alle normative è però vista quasi esclusivamente come un obbligo dalle imprese, che non affrontano il problema con un'adeguata strategia, non avendo la certezza di essere realmente protette. I servizi di penetration test forniscono informazioni accurate sul rischio che una rete aziendale possa essere violata e con essa i suoi asset digitali. Ancora pochi sono coloro che ne comprendono l'utilità, convinti di essere protetti, avendo destinato un budget alla sicurezza.

L'opera di sensibilizzazione da parte del Garante della Privacy e, più recentemente, dell'Agenzia per il Digitale, hanno certamente reso le imprese più consapevoli

"dell'insicurezza" nella quale si trovano a operare, ma manca ancora una reale conoscenza del fenomeno e, soprattutto, manca una cultura della sicurezza in azienda.

Lo dimostra, per esempio, il Rapporto 2014 del Clusit, nota associazione di professionisti della sicurezza nata in seno all'Università Statale di Milano. Gli esperti del Clusit hanno classificato i principali incidenti pubblici verificatisi su scala mondiale negli ultimi tre anni, rilevandone una percentuale estremamente bassa in Italia (3%). Un dato eccessivamente discostato dalla media internazionale. Perché per gli italiani vale sempre il proverbio: "I panni sporchi vanno lavati in famiglia". In altre parole, non avviene la condivisione delle informazioni sugli attacchi di sicurezza. Una sorta di "omertà" che, pur comprendendo i timori in termini di immagine, risulta invece controproducente per le stesse imprese, penalizzando l'opera di prevenzione.

L'importanza della condivisione è sottolineata sia dal recentemente istituito CERT italiano, che a fine 2013 ha annunciato il "Piano per la protezione cibernetica e la sicurezza

informatica", sia dall'Unione Europea, che ha costituito la Piattaforma europea su Network e Information Security (NIS).

I suddetti timori sono poi infondati, perché è comunque possibile mettere a disposizione le informazioni in maniera anonima. Sempre il Rapporto Clusit riporta infatti i dati provenienti dal monitoraggio della rete di Fastweb, che mostrano uno scenario preoccupante: la sicurezza delle aziende italiane continua a scendere, pure a fronte di un incremento o mantenimento dei budget e mentre cresce il mercato della sicurezza informatica e continua a registrarsi una richiesta di figure professionali in quest'ambito superiore alla disponibilità.

## **Il costo della perdita dei dati**

A determinare questa paradossale situazione contribuisce in massima parte l'incapacità da parte della classe dirigente di comprendere il costo per l'azienda della perdita di un dato. Intanto, il dato non viene "rubato" ma copiato. A essere compromessa è la sua riservatezza e buona parte del costo dipende dall'utilizzo che il cybercriminale può farne. Per esempio, l'anno scorso un'azienda d'abbigliamento italiana ha subito un furto di dati, ma se ne è accorta solo mesi dopo, quando in alcuni negozi cinesi sono stati messi in vendita capi uguali ai bozzetti della nuova collezione.

Altro aspetto che incide sul valore della perdita è legato al settore economico in cui opera l'impresa. Kris Lovejoy, General Manager, IBM Security Services Division. Spiega: "Una violazione dei dati può comportare un danno enorme per l'impresa che la subisce, e va ben oltre gli aspetti finanziari. In gioco ci sono infatti la fidelizzazione dei clienti e la reputazione del marchio". Per esempio, un incidente di sicurezza per una banca mette certamente in discussione il rapporto di fiducia che è alla base della relazione con la clientela.

Ancora troppi imprenditori e dirigenti hanno bisogno di comprendere in quali modi i dati aziendali possono essere compromessi e come ciò possa pregiudicare l'attività della loro impresa. Si tratta di un aspetto fondamentale, perché senza questa comprensione e senza stimare il valore da assegnare ai dati, non è possibile calcolare quale budget sia adeguato riservare alle risorse per la prevenzione, il rilevamento e la risoluzione di un incidente. In altre parole, tornando al rapporto del Clusit, non comprendendo il fenomeno e l'importanza della sicurezza, rapportata ai propri dati, si rischia di investire tanto, poco o troppo poco e, soprattutto, nella direzione sbagliata.

Secondo la ricerca "Cost of Data Breach Study" condotta a livello mondiale dal Ponemon Institute e sponsorizzata da IBM, nell'ultimo anno il costo totale medio per la violazione dei dati a livello mondiale è aumentato del 15%, raggiungendo i 3,5 milioni di dollari.

Altro dato rilevato interessante è che il costo sostenuto per ogni record perso o rubato, contenente informazioni riservate e sensibili, è aumentato di più del 9%, toccando i 145 dollari.

La ricerca del Ponemon ha coinvolto manager che erano in grado di calcolare il valore dei propri dati. Erano altresì in grado di misurare la loro esposizione al rischio. Ci sono procedure che aiutano le imprese a effettuare un'analisi del rischio e, quindi, il valore del dato, ma, come è ovvio, solo i business manager possono assegnare un costo alla perdita di ciascun dato. Per questo è importante che il responsabile della sicurezza possa contare sulla collaborazione di tutti i dirigenti aziendali.

Idealmente, nella formazione culturale sulla sicurezza è opportuno coinvolgere tutti i dipendenti. Gli incidenti malevoli interni, il più delle volte, sono dovuti a disattenzione delle politiche di sicurezza definite. Con una forza lavoro più consapevole si può abbassare significativamente il rischio.

Per contro, in Italia, come un'ulteriore ricerca di Ponemon dimostra (Exposing the

Cybersecurity Cracks) e come confermato dal rapporto Clusit, la maggior parte delle imprese non solo si accorge molto tardi di aver subito un attacco, ma spesso non è in grado di risalire all'origine dell'attacco. Non sapere come si sia subito una violazione è estremamente grave, perché non è possibile impedire che questa si ripeta.

Lo scenario si fa ancora più tetro, se si considera che molte tecniche usate per gli attacchi utilizzano ancora vulnerabilità per le quali esiste da tempo una soluzione, che non viene adottata perché prevede l'aggiornamento di qualche sistema informatico. Talvolta, l'applicazione delle cosiddette patch non viene effettuata consapevolmente, perché ci sono impedimenti tecnici o, magari, perché si valuta che l'operazione abbia delle controindicazioni più costose del danno causato dalla violazione.

Questo, però, riporta al punto precedente: occorre poter valutare con precisione tale valore per una scelta consapevole. Purtroppo, molto spesso, l'applicazione delle patch viene continuamente rimandata perché si sottovaluta il problema e ci si trova a rincorrere le richieste del business, cieco alle problematiche di information security.

In ogni caso, anche nelle imprese in cui si sono fatti importanti investimenti in sicurezza, spesso non c'è una reale certezza di riuscire a bloccare gli attacchi. Anzi, sempre secondo i dati di Ponemon, la maggior parte dei responsabili per la sicurezza ammettono di non avere la certezza di riuscire a fermare tutti gli attacchi e, anzi, una buona fetta dei suddetti sospetta di subire diverse violazioni alla sicurezza.

Prima di investire il budget per la sicurezza in maniera sbagliata, è opportuno valutare una soluzione che possa identificare le vulnerabilità della sicurezza nell'ambiente ICT aziendale, arrivando a supportare le imprese nel determinare una roadmap delle attività, in modo da prevenire la violazione dei dati e la compromissione della rete.

Una soluzione che possa testare la resistenza del sistema per la sicurezza aziendale.

### **Test di penetrabilità per ridurre la vulnerabilità di rete: il servizio di IBM**

IBM Infrastructure Security Services fornisce tale soluzione. Più precisamente si tratta di un servizio di penetration testing, che effettua simulazioni controllate e sicure per rilevare le tecniche utilizzate per attacchi segreti e ostili e identificare i sistemi vulnerabili.

Tali servizi verificano l'efficacia dei controlli di sicurezza esistenti e quantificano i rischi concreti, fornendo alle imprese una roadmap dettagliata per la sicurezza che definisce la priorità dei punti deboli riscontrati nell'ambiente di rete.

In altre parole, una vera e propria simulazione d'attacco, al termine della quale gli esperti di IBM potranno fornire indicazioni specifiche e consigli su come ridurre i rischi, aumentare la disponibilità del sistema e rispettare le normative vigenti in termini di sicurezza.

I test di penetrabilità aiutano a identificare le vulnerabilità presenti sulla rete e mostrano in che modo gli aggressori possono arrivare a danneggiare il business, permettendo ai responsabili della sicurezza di migliorare le operazioni per la protezione della rete.

I servizi offerti verificano l'efficacia dei controlli esistenti e quantificano i rischi concreti, eseguendo simulazioni controllate e sicure che rilevano attività ostili e segrete.

IBM fornisce un'analisi di sicurezza tecnica e strategica che aiuta la creazione di infrastrutture di sicurezza adattabili, le quali rispettano i requisiti di business, riducono costi, complessità e migliorano la protezione globale.

Uno degli aspetti fondamentali in questo tipo di approccio riguarda la determinazione delle priorità, in funzione delle vulnerabilità identificate. Nei servizi di penetrabilità forniti da IBM, viene delineata una vera e propria roadmap della sicurezza. Quest'ultima definisce le priorità dei rischi rilevati e dei settori carenti, specificando le procedure di correzione per prevenire la compromissione della rete e verificare che gli aggiornamenti di sistema siano applicati correttamente.

La metodologia del test di penetrabilità include:

- Rilevamento ed esame preliminare dei dispositivi e dei servizi di rete, che prevede un'accurata ispezione degli host e dei servizi online.
- Attacco interno o perimetrale, che sfrutta le principali vulnerabilità.
- Sfruttamento remoto, cioè un ulteriore e sempre più sofisticato tentativo di penetrazione nella rete e violazione di dati riservati o importanti.
- Conclusioni e risultati finali di analisi, che prevede la realizzazione e consegna di report dettagliato in cui vengono presentate le conclusioni e i consigli attuabili.

Come evidenziato dai responsabili degli IBM Infrastructure Security Services, tali servizi di penetrabilità favoriscono a rispettare costantemente la normativa pubblica e quelle di settore, come la PCI DSS (Payment Card Industry Data Security Standard).

Un punto di forza nell'offerta di servizi forniti IBM è l'esperienza dei consulenti qualificati, che possono inoltre contare su una vasta base di conoscenza. Questi applicano tecniche di indagine manuale e utilizzano strumenti avanzati per identificare le vulnerabilità e illustrarne le modalità di sfruttamento.

Proprio tali competenze sono il miglior biglietto da visita per i servizi di penetrabilità: I consulenti sulla sicurezza IBM sono divenuti molto esperti nelle attività di supervisione della sicurezza aziendale, consulenza di sicurezza, indagine per conto di enti governativi, procedimenti legali.

Di fatto gli stessi consulenti svolgono attività di ricerca e sviluppo e si avvalgono del supporto diretto da parte del team di R&D IBM X-FORCE: le attività di quest'ultimo consentono a IBM di fornire soluzioni di sicurezza end-to-end. Soluzioni che sono personalizzabili per adattarsi alle caratteristiche di ciascun cliente.

Per ulteriori informazioni relative a IBM Infrastructure Security Services – penetration testing: [ibm.com/services/it/security](http://ibm.com/services/it/security).

IBM fornisce inoltre un supporto finanziario: [ibm.com/financing/it](http://ibm.com/financing/it)

BOX1 (o pezzo a parte se non si riesce a impaginare come box)

### **Ricerca Ponemon: Cost of Data Breach**

Secondo la nona edizione della ricerca "Cost of Data Breach Study", condotta a livello mondiale dal Ponemon Institute e pubblicata a Maggio 2014, il costo totale medio per la violazione dei dati a livello mondiale è aumentato del 15% in un anno, raggiungendo i 3,5 milioni di dollari.

Di seguito riportiamo i principali risultati ricavati dallo Studio Global Cost of Data Breach:

- Il costo sostenuto per ogni record perso o rubato, contenente informazioni riservate e sensibili, è aumentato di più del 9%, toccando i 145 dollari.
- Le violazioni più onerose si sono verificate negli Stati Uniti e in Germania, con un costo rispettivamente di 201 e 195 dollari per record compromesso. Le violazioni dei dati meno costose sono state in India e Brasile, rispettivamente pari a 51 e 70 dollari.
- Le cause principali cui addebitare le violazioni dei dati variano da paese a paese e possono influire sul costo della violazione. I paesi nella regione Araba e la Germania hanno avuto un maggior numero di violazioni dei dati causate da attacchi malevoli o di organizzazioni criminali. L'India ha avuto il maggior numero di violazioni dei dati causate da anomalie di sistema o di processo. L'errore umano è

stato la causa più comune nel Regno Unito e in Brasile.

- Le violazioni dei dati più onerose sono state quelle causate da attacchi malevoli o di organizzazioni criminali. Gli Stati Uniti e la Germania hanno sostenuto i costi più elevati.
- L'approccio alla sicurezza è stato essenziale per ridurre il costo della violazione dei dati. In media, le aziende che hanno dichiarato di avere un solido livello di sicurezza sono riuscite a ridurre il costo addirittura di 14 dollari per record.
- L'integrazione della gestione della business continuity ha ridotto il costo della violazione dei dati, in media, di quasi 9 per record.
- La nomina di un Chief Information Security Officer (CISO) alla guida di un team di gestione della violazione dei dati ha ridotto il costo di una violazione di oltre 6 dollari.
- I Paesi che hanno perso il maggior numero di clienti in seguito a una violazione dei dati sono stati la Francia e l'Italia. Le aziende nella Regione Araba e in Brasile hanno subito la perdita di clienti minore.
- La probabilità per un'azienda di subire una violazione dei dati che coinvolga 10 mila o più record riservati è del 22% nell'arco di due anni. I Paesi che hanno la maggiore probabilità di subire una violazione dei dati sono India, Brasile e Francia.

Come già emerso nei precedenti studi Cost of Data Breach, la causa più comune per una violazione dei dati risulta l'attacco malevolo da parte di soggetti interni all'azienda o di un'organizzazione criminale.

L'obiettivo della ricerca, come spiega Larry Ponemon, presidente e fondatore del Ponemon Institute, è quello di aiutare le imprese a indirizzare i propri investimenti in sicurezza, ma anche di fornire un orientamento sulla probabilità che le imprese hanno di subire una violazione dei dati e sui possibili interventi per ridurre le conseguenze finanziarie.

In questa nona edizione è stato anche chiesto alle figure professionali coinvolti nelle aziende quali sono le preoccupazioni maggiori sugli incidenti di sicurezza, quali investimenti stanno effettuando e l'eventuale esistenza di una strategia al riguardo.

Di seguito sono riportati alcuni dei risultati chiave:

- Le minacce più grandi per le aziende partecipanti sono il malware e i tentativi di accesso subiti. Secondo lo studio, queste due minacce sono in aumento.
- Solo il 38% delle aziende ha una strategia di sicurezza per proteggere la propria infrastruttura IT. Una percentuale più elevata (45%) ha in essere una strategia di sicurezza per proteggere il proprio patrimonio di informazioni.
- Codice maligno e probe subiti hanno registrato il massimo aumento. Le aziende stimano che dovranno confrontarsi con una media di 17 codici maligni e 12 probe subiti ogni mese. Gli incidenti legati agli accessi non autorizzati sono rimasti sostanzialmente invariati e le aziende stimano che dovranno confrontarsi con una media di 10 incidenti di questo tipo ogni mese.
- La maggior parte delle aziende (50%) ha scarsa o nessuna fiducia rispetto all'adeguatezza degli investimenti effettuati in risorse umane, processi e tecnologie per affrontare le minacce potenziali ed effettive.
- Idealmente, le aziende vorrebbero investire 14 milioni di dollari nei prossimi 12 mesi per realizzare la propria strategia di sicurezza. Tuttavia, nell'arco dei prossimi 12 mesi, le aziende prevedono di disporre in media di circa metà di tale cifra, ovvero 7 milioni di dollari, da investire in strategia di sicurezza.

BOX all'interno del BOX1 (o nel pezzo a parte)

### **La metodologia**

Lo studio annuale di Ponemon "Cost of Data Breach Study" è basato sulla raccolta di informazioni dettagliate sulle conseguenze finanziarie causate dalla violazione di dati. Ai fini di questa ricerca, viene considerata "violazione dei dati", un incidente in cui dati sensibili, protetti o riservati vengono persi o rubati e messi a rischio.

Per la ricerca è definito record compromesso quello che identifica il soggetto le cui informazioni sono state perse o rubate in una violazione dei dati.

Il Ponemon Institute ha condotto 1.690 interviste con professionisti dell'IT, della compliance e della sicurezza delle informazioni, in rappresentanza di 314 organizzazioni, nei 10 Paesi seguenti: Stati Uniti, Regno Unito, Germania, Australia, Francia, Brasile, Giappone, Italia, India e, per la prima volta, la regione araba (un insieme di organizzazioni degli Emirati Arabi Uniti e dell'Arabia Saudita).

Tutti gli intervistati sono figure che, per ruolo, conoscono le violazioni dei dati subite dalle rispettive organizzazioni e i costi associati alle relative risoluzioni. Tutte le organizzazioni partecipanti hanno subito violazioni dei dati, da un livello minimo di circa 2.400 record compromessi a poco più di 100mila.

I dati in valore sono stati espressi in dollari, convertendo le valute dei vari paesi coinvolti in quella degli Stati Uniti.

### **BOX2**

#### **Lo studio The State of Advanced Persistent Threats**

Il Ponemon Institute ha pubblicato anche lo studio The Economic Consequences of an APT Attack, sponsorizzato da Trusteer, una società IBM.

Questo rapporto fa parte di una ricerca più vasta, dal titolo "The State of Advanced Persistent Threats", pubblicato nel dicembre 2013. La ricerca originale, condotta tra 755 professionisti della sicurezza IT statunitensi, conferma i risultati dello studio The Cost of Data Breach, nel quale gli attacchi mirati di organizzazioni criminali sono considerati dalla maggior parte degli intervistati la più grande minaccia per la rispettiva organizzazione.

Un altro fatto avvalorante è la rilevazione che i danni in termini di reputazione rappresentano la componente o conseguenza più onerosa degli attacchi criminali, in particolare quelli che comportano il furto o l'uso improprio del patrimonio di informazioni.

Gli intervistati di questo studio stimano che il costo medio di un'azienda per ristabilire la propria reputazione sia pari a 9,4 milioni di dollari.