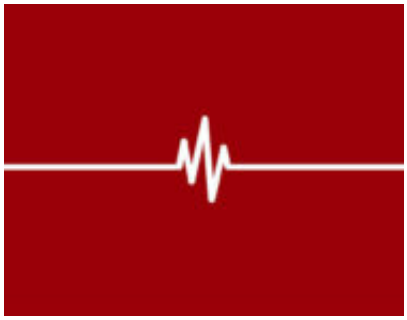
Red Team Regeneration

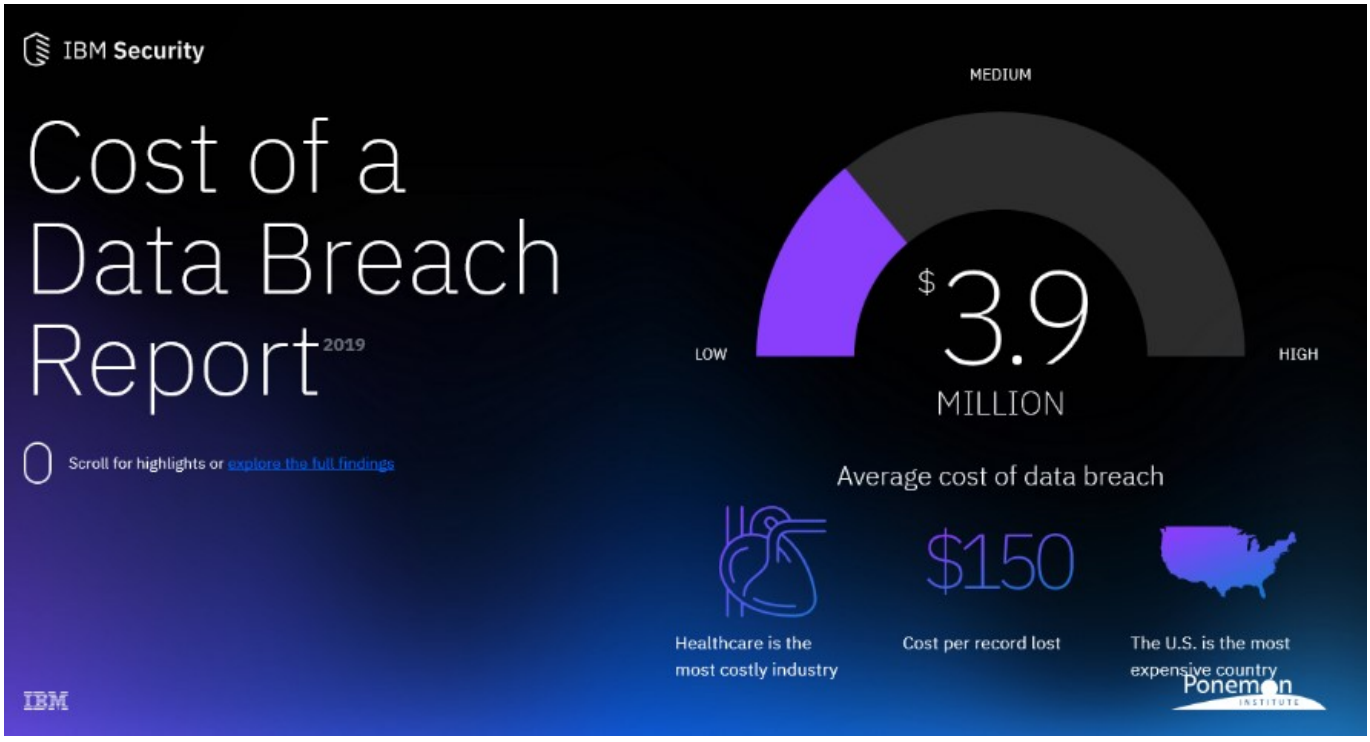
Author : Massimiliano Brolli

Date : 1 Ottobre 2019



Di recente è stato pubblicato il rapporto annuale "Cost of data breach" sviluppato da **Ponemon Istituite** in collaborazione con **IBM Security**, che riporta il costo medio che le aziende sostengono per singolo data-breach.

Ad oggi un data-breach si attesta a 3.9 milioni di dollari dove, **nel campione italiano analizzato di 11 aziende, la media si aggira su 3,1 milioni di euro** circa.



Dal report viene inoltre riportato che il costo non risulta distribuito nel periodo "strettamente successivo" all'incidente di sicurezza **ma viene distribuito anche nei due anni successivi.**

Quanto riportato da IBM Security fa comprendere come **il fenomeno data-breach possa influenzare in modo sensibile il cammino di ogni azienda**, oltre a comportare perdite ingenti (dirette e indirette) trainate anche da quello che potrebbe essere il "miglioramento delle politiche di sicurezza" e del "sistema controllo interno" a valle dell'incidente informatico.

La visione del NIST sui Security Assessment

Prima di addentrarci nell'esame di quali potrebbero essere i potenziali miglioramenti, citerei il NIST ***(National Institute of Standards and Technology)*** ovvero l'ente "supremo" che tutti noi riteniamo fonte di "ispirazione" e "autorevolezza" in termini di tecnologia, standard e metodologia.

Nella **Special Publication 800-115, denominata *"Technical Guide to Information Security Testing and Assessment",*** nel capitolo 2.3 viene riportato:

> *I Test di sicurezza non forniscono una valutazione completa della sicurezza di un sistema, e spesso hanno un ambito ristretto a causa delle risorse e delle limitazioni di tempo. I pirati informatici, d'altra parte, possono prendere tutto il tempo di cui hanno bisogno per sfruttare e penetrare un sistema.*

Inoltre, sempre il NIST riporta che i "*Security Assessment possono indicare le principali debolezze tecniche presenti sul sistema, consentono di comprendere la postura dell'organizzazione rispetto ai processi di sicurezza informatica*" che devono essere costantemente attuati.

Qualche semplice considerazione

Premesso che tutti siamo d'accordo nel dire che i processi di *Patching management*, *hardening* e Sviluppo sicuro **devono essere garantiti e presidiati da chi disegna, sviluppa, colluda ed esercisce i sistemi**, comincerei col porre una domanda che probabilmente alle volte dimentichiamo di farci, in preda all'operatività che regna sovrana nel settore degli addetti ai lavori:

qual è l'obiettivo principale della Sicurezza informatica?

Far in modo che possano essere garantite riservatezza, integrità e disponibilità dei dati contenuti in un sistema informatico. Ma sintetizziamo meglio... far in modo che si possano evitare gli accessi indebiti ai sistemi... ma di meglio, in chiave moderna, nel 2019...
fare in modo che i data-breach non ci siano!

La chiave di volta

Analizzando con attenzione il fenomeno, viene spontaneo chiedersi **se risulti corretto il posizionamento delle attività di Red Team nei processi aziendali di oggi** o se possa esserci un "modello" alternativo, più efficace, che possa anche essere misurato in termini di abbattimento del rischio "economico" e "d'impresa" dovuto soprattutto **alla rimozione preventiva dei data-breach, prima che questi possano essere sfruttati da un ipotetico "nemico".**

La ***Data Breach Prevention*** è una tipologia di *Security Assessment* che consente di effettuare un'analisi del sistema finalizzata a rilevare, nei punti di esposizione più "critici", la presenza di vettori di attacco capaci di generare un'esfiltrazione di dati sensibili. Generalmente questa attività viene svolta da rete internet **in puro ethical-hacking**, in quanto la potenziale esfiltrazione viene generata **concatenando diversi requisiti e carenze di sicurezza presenti sul sistema,** cosa che oggi le macchine (le attività di *Vulnerability Assessment*, nello specifico) non possono fare.

I principali punti di forza sono:

1. rilevare i data-breach potenziali prima che questi vengano utilizzati;
2. rimuovere in tempi brevi il primo "Gate" di innesco del vettore di attacco, in modo da

rimuovere eventuali accessi indesiderati;
3. analizzare le architetture perimetrali, facendo implementare qualora non presenti, *Security Gateway* e *Intrusion Prevention System,* aumentando la capacità di rilevazione di eventi anomali da parte del Security Operation Center.

Ricordiamoci però che la rilevazione dei data-breach potenziali risulta **direttamente proporzionale alla capacità di sperimentazione dell'hacker etico.** Inoltre, minore sarà la complessità nei processi da agire, maggiore sarà la sua concentrazione nel vincere la "sfida" (la parte a lui più congeniale per natura) ovvero violare il sistema e fornire le risultanze del vettore di attacco rilevato essendo consapevole di aver vinto la sfida.

Questo perché il "White Hat Hacker" (il tester di sicurezza) non sta facendo altro che simulare un'attività di attacco. **L'unica cosa che differisce è "l'ampiezza temporale",** in quanto tale ampiezza risulterà "definita" e non potenzialmente "infinita" come nel caso dei "Black Hat Hacker".

Qualora il Red Team avesse il mandato di svolgere attività di **Data Breach Prevention** con continuità, dandogli modo di sperimentare e analizzare al meglio le superfici di attacco (evitando di imbrigliarlo in processi documentali e non attuali), potrà essere misurato attraverso:

- numero di data-breach potenziali rilevati rispetto al numero di security assessment condotti;
- ritorno economico in termini di spesa del Red Team stesso (risparmio sotteso in termini di data-breach potenziali abbattuti);
- numero di Architetture perimetrali revisionate.

Inoltre, tutto questo potrebbe consentire di migliorare anche l'indotto e quindi:

- definire particolari contratti (in caso di utilizzo di fornitori) a "incentivo" in forma "variabile" a valle della rilevazione dei data-breach potenziali, come stimolo per i pen-tester arruolati nel Red Team stesso;
- incrementare l'*effort* del Red Team fino a raggiungere il giusto compromesso tra il suo costo e il risparmio sotteso in termini di data-breach abbattuti.

Conclusioni

La sicurezza informatica ha sempre insegnato che **le migliori idee e strategie sono sempre state avviate dopo un grande fallimento,** anche se su questo occorrerebbe una riflessione da parte di tutti.

Occorre entrare nell'ordine di idee che **la Security da sola non può evitare che i data-breach ci siano,** perché sarebbe come sostenere che, se esiste una funzione legale in azienda, non ci saranno più cause intentate ai danni della stessa.

> *La sicurezza informatica infatti è una Responsabilità condivisa, solo se tutti avranno la giusta "consapevolezza al rischio" e garantiranno l'adozione dei processi di sicurezza*

informatica con costanza e precisione, gli incidenti di sicurezza potranno essere ridotti.

Il Red Team può svolgere una attività di "carotaggio" importante, anche se per un tempo limitato, fornendo grandi benefici in termine di abbattimento del rischio; ma per fare questa scelta occorre **abbandonare le convinzioni del passato e vedere tutto da un'angolazione differente,** sia rispetto alla tradizionale cybersecurity sia nei confronti della normale operatività quotidiana.

Risulta quindi necessaria **una completa "rigenerazione" (non parlo di miglioramento)** di questa attività, consentendo ai tester di dedicarsi a "emulare" il comportamento di un reale nemico, garantendogli in quel tempo "limitato" di mettere in campo le cose a lui più congeniali come **sperimentazione, curiosità e passione.**

I controlli sui processi invece dovranno essere svolti da attività parallele **più congeniali alla logica di "Auditor" che da Red Team**, consentendo di migliorare la "postura" dell'organizzazione a livello di adozione, da parte delle linee tecniche, dei processi di sicurezza definiti.

Articolo a cura di **Massimiliano Brolli**