

Studio IBM Security: le violazioni degli account dei dipendenti sono state quelle più costose nell'ultimo anno

I cambiamenti imposti dalla pandemia hanno spinto all'utilizzo di tecnologie che garantissero continuità operativa, ma il disallineamento nella preparazione del capitale umano ha provocato una breccia nella sicurezza delle aziende. L'Italia di poco più veloce rispetto alla media globale con 203 giorni in media per intercettare un attacco e 65 per contenere una violazione. L'adozione dell'intelligenza artificiale e di soluzioni per automatizzare i processi di sicurezza, uniti a maggiore formazione, possono ridurre in maniera significativa i costi.

CAMBRIDGE, Mass., 29 luglio 2020 - IBM Security ha annunciato i risultati del suo studio annuale che esamina l'impatto finanziario delle violazioni di dati sulle organizzazioni. Secondo il report, ogni violazione costa in media all'azienda impattata 3,86 milioni di dollari a livello globale e 2,90 milioni di euro in Italia. L'analisi approfondita delle violazioni di dati subite da oltre 500 organizzazioni in tutto il mondo, di cui 21 italiane, rivela che la violazione dei dati dei dipendenti è quella più gravosa e che l'80% di questi attacchi ha portato all'esposizione di informazioni di identificazione personale (Personal Identifiable Information, PII) dei clienti, causando costi ingenti per le aziende.

Se da un lato le tecnologie forti e mature hanno reso le organizzazioni sempre più resilienti, l'accesso ai dati sensibili attraverso il lavoro a distanza e le operazioni commerciali basate sul cloud, uniti alla mancanza di una adeguata formazione, hanno reso le organizzazioni più vulnerabili. Un altro [studio recente di IBM](#) ha rivelato che oltre la metà dei dipendenti che non lavorano da casa abitualmente, ma lo hanno fatto a causa della pandemia, non ha ricevuto linee guida aggiornate, volte a gestire in totale sicurezza le informazioni di identificazione personali dei clienti (PII). A fronte dei rischi di immagine e dei costi che le organizzazioni devono affrontare quando tali violazioni vengono perpetrate, gli investimenti in innovazione e capitale umano rappresentano i fattori più rilevanti per mitigare tali impatti e per garantire i migliori risultati anche in termini di sicurezza informatica.

Il report [Cost of a Data Breach 2020](#), richiesto da IBM Security e condotto da Ponemon Institute. è stato realizzato attraverso 3.200 interviste a responsabili della sicurezza di organizzazioni che hanno subito una violazione di dati nel corso dell'ultimo anno^[1]. Quella del 2020 è la 15^ edizione.

Principali risultati dello Studio 2020:

- **Il furto delle credenziali è fonte di spesa** le organizzazioni che hanno subito attacchi alle proprie reti aziendali attraverso l'uso di credenziali rubate o compromesse hanno speso quasi 1 milione di dollari in più rispetto alla media globale, raggiungendo i 4,77 milioni di dollari per violazione. Lo sfruttamento delle vulnerabilità di terze parti risulta la seconda voce di costo (4,5 milioni di dollari).
- **Le tecnologie smart abbattono del 50% i costi legati al furto di dati** le imprese che hanno implementato le più avanzate tecnologie di sicurezza, basate su intelligenza artificiale, capacità di analisi e orchestrazione automatizzata per identificare e rispondere agli attacchi, hanno sostenuto meno della metà dei costi di violazione di dati rispetto a quelle non dotate di tecnologie evolute (2,45 milioni di dollari contro 6,03 milioni di dollari, in media).
- **Attacchi Nation-State - Le violazioni peggiori:** nel periodo analizzato, le violazioni nation-state hanno causato la voce di costo più importante, determinando una spesa media di 4,43 milioni di dollari nel caso di furto di dati e superando i costi generati degli attacchi perpetrati da criminali informatici per finalità economiche.

"La capacità di mitigare gli attacchi informatici vede in netto vantaggio le organizzazioni che hanno investito nelle tecnologie più evolute", ha affermato Wendi Whitmore, Vice President, IBM X-Force Threat Intelligence. "Se da un lato il business nel mondo digitale sta crescendo a ritmi sostenuti, dall'altro persiste la carenza di esperti di sicurezza informatica. Inoltre, chi opera in questo ambito è sovraccarico di lavoro a causa della necessità di proteggere una moltitudine di dispositivi, sistemi e dati. Occorre dunque formare in cybersecurity e automatizzare alcuni processi per fornire risposte più rapide e risolutive in caso di attacco e garantendo efficienza in termini di costi".

Credenziali dei dipendenti e configurazione errata dei server cloud - Principali vulnerabilità

Il furto e la compromissione delle credenziali, oltre alle configurazioni errate dei server cloud, rappresentano le vulnerabilità più comuni, che causano quasi il 40% dei cyberattacchi. Lo studio rivela che nel 2019 oltre [8,5 miliardi di record](#) sono risultati vulnerabili e gli hacker, in 1 caso su 5, hanno sfruttato e-mail e password non adeguatamente protetti per sferrare i propri attacchi. Oggi le organizzazioni sono impegnate nella messa a punto di nuove strategie di sicurezza e nell'adozione un approccio a *Zero Trust*, che impone di rivedere i criteri di autenticazione e di accesso degli utenti.

Il report 2020 ha evidenziato che gli hacker hanno sfruttato proprio gli errori di configurazione dei server cloud per violare le reti quasi nel 20% dei casi, generando un aumento dei costi di oltre mezzo milione di dollari e portando a 4,41 milioni di dollari la spesa complessiva media, che si attesta quale terza voce di costo.

Le aziende Smart dispongono di tecnologie di sicurezza avanzate

Il report evidenzia il crescente divario tra i costi delle violazioni di dati sostenuti dalle aziende che investono nelle tecnologie di frontiera in ambito sicurezza e quelli delle aziende in ritardo su questo fronte: le prime vantano un risparmio di 3,58 milioni di dollari. Il divario di costo è cresciuto di 2 milioni di dollari, rispetto alla differenza di 1,55 milioni di dollari registrata nel 2018.

La piena adozione di tecnologie in grado di automatizzare i processi di sicurezza incide sulla velocità e l'efficienza di risposta di un'azienda a una violazione, contribuendo a diminuire i costi. Il report ha rilevato che intelligenza artificiale, machine learning, analytics e altri tool per automatizzare la sicurezza permettono alle aziende di rispondere più velocemente - del 27% - rispetto alle aziende che non hanno ancora adottato tali misure e che, pertanto, impiegano 74 giorni in più per identificare e contenere un attacco.

La preparazione nella risposta agli incidenti (Incident Response, IR) continua a impattare in modo significativo sulle conseguenze economiche di una violazione. Le aziende che non dispongono di un team di sicurezza dedicato e che non testano i propri piani sostengono una spesa media di 5,29 milioni di dollari, mentre le aziende che hanno adottato entrambe le misure, ed effettuano esercitazioni e simulazioni per testare i propri piani IR, spendono 2 milioni di dollari in meno in caso di violazione. Preparazione e prontezza consentono di conseguire un ROI significativo nell'area della cybersecurity.

Attacchi collegati ad attività governative

Nonostante rappresentino solo il 13% delle azioni malevoli, gli attacchi collegati ad attività governative sono quelli più dannosi, secondo il report, dimostrando che a quelli di natura finanziaria (53%), seppur di maggior numero, non consegue la maggiore perdita economica. Tattiche altamente sofisticate, durata e tipologia delle azioni perpetrare con l'obiettivo di sottrarre dati di alto valore, spesso inducono le vittime degli attacchi a scendere a compromessi, con un conseguente aumento dei costi di recovery, che si attesta mediamente a 4,43 milioni di dollari.

Altre evidenze del Report 2020:

- **Il lavoro a distanza determinerà un aggravio di costi** – La diffusione di modelli di lavoro ibridi rende gli ambienti meno

controllati. Lo studio ha rilevato che il 70% delle aziende che hanno adottato il telelavoro durante la pandemia si aspetta un aggravio dei costi causati dalla violazione di dati.

- **I CISO sono stati ritenuti responsabili delle violazioni, nonostante il potere decisionale limitato** il 46% degli intervistati ha dichiarato di ritenere il CISO / CSO responsabile delle violazioni effettuate, nonostante solo il 27% abbia affermato che il CISO / CSO abbia potere decisionale in termini di policy e tecnologie. Secondo il report, la nomina di un CISO è stata associata alla possibilità di risparmiare 145.000 dollari rispetto al costo medio di una violazione.
- **La maggior parte delle aziende assicurate contro i rischi informatici chiede risarcimenti per le spese di terzi** lo studio ha rilevato che le violazioni di dati subite da organizzazioni che hanno sottoscritto polizze assicurative contro i cyber risk hanno speso quasi 200.000 dollari in meno rispetto alla media globale di 3,86 milioni di dollari. Di fatto, tra le organizzazioni che hanno stipulato un'assicurazione contro il cyber risk, il 51% l'ha utilizzata per coprire le spese di consulenza e i servizi legali di terzi, mentre il 36% delle organizzazioni l'ha utilizzata per risarcire le vittime di attacchi. Solo il 10% delle polizze hanno coperto i costi sostenuti a causa di ransomware o estorsioni.
- **Trend per area geografica e settore:** mentre gli Stati Uniti si confermano il Paese con i più elevati costi di violazione dei dati, con una media di 8,64 milioni di dollari, il report ha inoltre rilevato che il settore healthcare ha registrato i costi medi più elevati, pari a 7,3 milioni di dollari, con un aumento di oltre il 10% rispetto all'edizione 2019 dello studio.

Per l'Italia, queste le principali evidenze:

In Italia il costo medio complessivo delle violazioni di dati è pari a 2,90 milioni di euro, in diminuzione del 4,9% rispetto al 2019; mentre, il costo medio relativo al furto o alla perdita di un singolo dato è pari a 125 euro, con una flessione del 3,8% rispetto al 2019.

Il 52% delle violazioni di dati è causato da attacchi malevoli e il tempo medio per identificare una violazione di dati è passato da 213 a 203 giorni, contro la media globale di 207 giorni. Inoltre, il tempo medio per contenere una violazione è passato da 70 a 65 giorni, contro i 73 mediamente necessari a livello globale.

In particolare, gli italiani impiegano mediamente:

- 229 giorni per identificare un attacco malevolo e 80 per contenerlo
- 180 giorni per identificare un errore umano e 49 per contenerlo
- 168 giorni per identificare una falla nei sistemi e 49 per contenerla

Tra i settori maggiormente colpiti al 1° posto troviamo quello finanziario, seguito da quello farmaceutico e dal terziario.

Le principali cause sono dovute agli attacchi malevoli (52%), agli errori umani (29%) e alle falliche dei sistemi (19%). La spesa media complessiva generata da ciascuna causa è pari a 3,20 milioni di euro (attacchi malevoli); 2,62 milioni di euro (falliche di sistema); 2,53 milioni di euro (errori umani)

Un numero crescente di organizzazioni ha adottato tecnologie avanzate per automatizzare la sicurezza: 56% nel 2020, contro il 49% del 2019.

La velocità e l'efficienza di risposta di un'azienda a una violazione ha un grande impatto sui costi: in Italia identificare un attacco in meno di 100 giorni fa registrare un costo medio di 2,18 milioni di euro, mentre impiegando oltre 100 giorni, il costo medio si assesta intorno ai 3,62 milioni di euro. Contenere un attacco entro i 30 giorni, invece, richiede una spesa di 2,23 milioni di euro, contro i 3,57 milioni oltre i 30 giorni.

Ciò significa che poter contare su team dedicati, predisporre e testare piani di sicurezza, adottare le più innovative tecnologie in questo ambito consente alle aziende di essere più efficienti nel prevenire e contrastare gli attacchi, ridurre i costi e conseguire ROI in tempi minori nell'area della cybersecurity.

Informazioni sullo studio

Il rapporto annuale sul costo di una violazione dei dati si basa sull'analisi approfondita delle violazioni dei dati reali nel periodo compreso tra agosto 2019 e aprile 2020.

L'analisi tiene conto di centinaia di fattori di costo, tra cui attività legali, normative e tecniche dovute a perdite di valore del brand, clienti e produttività dei dipendenti.

Studio Cost of Data Breach 2020: link per scaricare copia del report <http://ibm.com/databreach>

Webinar sul report Cost of Data Breach 2020, in programma: mercoledì 12 agosto 2020, h 11:00 ET. Link per iscriversi <https://ibm.biz/BdqhMf>

IBM Security

IBM Security offre uno dei portfolio più completi e integrati di prodotti e servizi per la protezione aziendale. Il portfolio, supportato dal team di ricerca di fama mondiale IBM X-Force®, consente alle organizzazioni di gestire con efficacia il rischio e difendersi dalle minacce emergenti. IBM dirige una delle organizzazioni di ricerca, sviluppo e delivery di soluzioni di sicurezza più grandi al mondo, monitora 70 miliardi di eventi di security al giorno in più di 130 Paesi e ha ottenuto oltre 10.000 brevetti di sicurezza. Per maggiori informazioni, visita il sito www.ibm.com/security, seguì @IBMSecurity su Twitter o visita il [blog di IBM Security Intelligence](#).

[1] Il Report analizza le violazioni di dati avvenute tra Agosto 2019 e aprile 2020.

Per ulteriori informazioni: Claudia Ruffini, External Relations, IBM Italia cla@it.ibm.com +39 335 6325093



Global Infographic (427 KB)