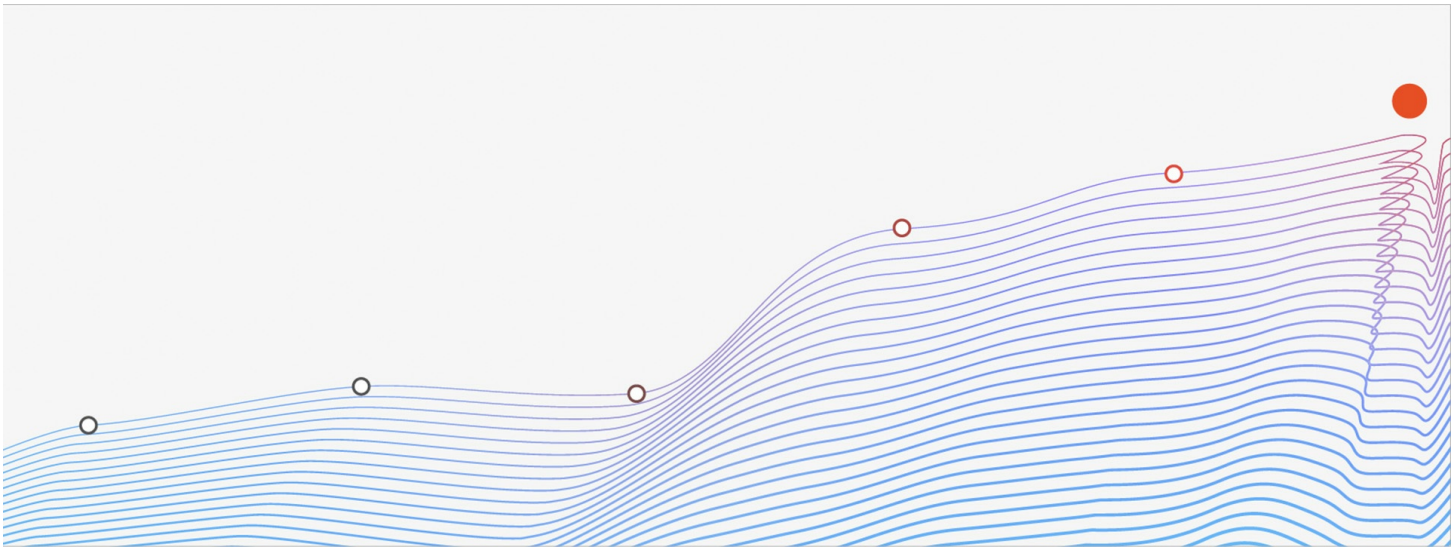
IBM Italy News Room

IBM Cost of a Data Breach Report 2023: intelligenza artificiale e automazione per identificare e contenere i cyberattacchi nelle aziende

In Italia, il costo complessivo delle violazioni di dati è pari a 3,55 milioni di euro, in crescita rispetto ai 3,03 milioni di euro nel 2021. I giorni per identificare e contenere una minaccia informatica sono 235, in leggero calo rispetto ai 250 giorni impiegati in precedenza

L'AI e l'automazione hanno ridotto, per le aziende italiane, i cicli di vita delle violazioni di 112 giorni e i costi delle violazioni di dati di 1,56 milioni di euro



Italy, 24 luglio 2023 – IBM (NYSE: IBM) Security ha rilasciato il **Cost of a Data Breach Report** [1], evidenziando che il costo medio globale di una violazione dei dati ha raggiunto 4,45 milioni di dollari nel 2023 - massimo storico per il report - in aumento del 15% negli ultimi 3 anni. A livello globale, i costi di rilevamento sono aumentati del 42% rispetto allo stesso periodo dell'anno precedente.

Quest'anno vi è una distinzione tra la gestione dell'aumento dei costi e quella della frequenza delle violazioni: il report ha rilevato, a livello globale, che il 95% delle organizzazioni intervistate ha subito più di una violazione ed è propenso a imputare ai clienti (57%) i costi degli attacchi subiti piuttosto che incrementare gli investimenti in sicurezza (51%).

Il Cost of a Data Breach Report 2023 si basa su un'analisi approfondita delle violazioni dei dati di 553 organizzazioni su base mondiale, effettuata tra marzo 2022 e marzo 2023. La ricerca, finanziata da IBM Security e condotta da Ponemon Institute, è giunta alla 18a edizione.

Globalmente, tra i risultati chiave del report IBM 2023 vi sono:

- **L'AI velocizza il rilevamento degli attacchi** - L'AI e l'automazione hanno impattato maggiormente sulla velocità di identificazione e contenimento delle violazioni. Le aziende che fanno uso esteso dell'AI e dell'automazione hanno rilevato gli attacchi con 108 giorni di anticipo (ovvero 214 giorni contro 322 giorni) rispetto alle organizzazioni che non hanno adottato queste tecnologie.

- **Il costo del silenzio** - Le vittime di ransomware che si sono rilvolte alle forze dell'ordine hanno risparmiato in media 470.000 dollari di costi per violazione rispetto a quelle che hanno scelto di non denunciare l'attacco, che corrispondono al 37% del totale delle organizzazioni colpite.

- **Inefficienza nel rilevamento degli attacchi** - Quando gli attacchi vengono rilevati in autonomia dai responsabili sicurezza delle organizzazioni, i costi sostenuti per far fronte ai danni subiti sono inferiori (di circa 1 milione di dollari) rispetto a quando sono i cyber criminali stessi a dichiararli e a chiedere un riscatto.

"*Il tempo è la nuova valuta nella sicurezza informatica sia per chi protegge l'azienda sia per i cybercriminali. Come indica il report, un rilevamento precoce e una risposta rapida possono ridurre significativamente l'impatto di una violazione*", ha dichiarato Chris McCurdy, General Manager, Worldwide IBM Security Services. "*I responsabili della sicurezza devono focalizzarsi sulle aree di maggior successo degli hacker in modo da prevenire le loro azioni e fermarli prima che raggiungano i loro obiettivi. Gli investimenti impiegati per rilevare le minacce e per definire risposte rapide, grazie all'AI e all'automazione, sono fondamentali per mitigare al meglio gli attacch*i".

Ogni minuto è prezioso

Secondo il report di quest'anno, le organizzazioni intervistate che hanno adottano adeguate misure di sicurezza, soluzioni di intelligenza artificiale e automazione, hanno impiegato in media 108 giorni in meno per rilevare un attacco rispetto a quelle che non hanno fatto gli stessi investimenti, oltre ad aver registrato un significativo risparmio economico. Infatti, chi integra nei propri sistemi di sicurezza AI e automazione risparmia oltre 1,8 milioni di dollari (cifra record) sui costi di violazione dei dati.

Allo stesso tempo, gli hacker sono mediamente più velocinel completare un attacco ransomware. Per molte aziende c'è ancora margine di miglioramento nell'ambito della sicurezza: il 40% infatti non ha ancora adottato tecnologie di AI e automazione pertanto ha l'opportunità di migliorare la velocità di rilevamento e di risposta agli attacchi.

"Codice sconto" per il ransomware

Alcune delle organizzazioni analizzate sono restie a coinvolgere le forze dell'ordine durante un attacco ransomware, in quanto hanno la percezione che ciò complichi la situazione. In realtà, quest'anno, per la prima volta, il report di IBM ha analizzato in modo più approfondito la questione provando il contrario. Per le organizzazioni intervistate che non hanno coinvolto le forze dell'ordine il ciclo di vita delle violazioni è durato mediamente 33 giorni in più, rispetto a quello sperimentato da coloro che hanno scelto di rivolgersi alle stesse. Inoltre, chi non si è rivolto alle forze dell'ordine ha pagato in media 470.000 dollari in più per le violazioni rispetto a chi non lo ha fatto.

I responsabili della sicurezza difficilmente intercettano le violazioni in autonomia

Secondo il Threat Intelligence Index 2023 di IBM, lo scorso anno i responsabili sicurezza delle aziende sono stati in grado di bloccare una percentuale più alta di attacchi ransomware. Tuttavia, gli hacker continuano a trovare il modo di eludere i sistemi di difesa delle organizzazioni. Il report ha evidenziato che il 33% delle violazioni è stato scoperto dai responsabili della sicurezza, il 27% è stato rivelato dallo stesso aggressore, mentre il 40% da una terza parte neutrale, come ad esempio le forze dell'ordine.

Le organizzazioni che hanno scoperto in autonomia di essere state violate hanno registrato costi inferiori di quasi 1 milione di dollari rispetto a quelle contattate direttamente dagli hacker (5,23 milioni di dollari contro 4,3 milioni di dollari). Le violazioni comunicate dai cybercriminali hanno inoltre avuto un ciclo di vita più lungo di quasi 80 giorni (320 contro 241) rispetto a quelle di chi ha identificato la violazione internamente. I significativi risparmi in termini di costi e di tempo che derivano dall'individuazione precoce dimostrano che investire in queste strategie può ripagare nel lungo periodo.

Lo spaccato italiano

Il Report 2023 è stato condotto anche a livello italiano su **24** realtà del territorio, da cui emergono interessanti spunti sulla situazione del Paese:

- **Il costo medio complessivo delle violazioni di dati è pari a 3,55 milioni di euro**, in crescita rispetto ai 3,03 milioni di euro nel 2021 e ai 3,40 milioni di euro del 2022. Nell'ultimo decennio, il costo medio per ogni violazione dei dati è cresciuto del 55% (da 95 euro nel 2013 a 147 euro nel 2023).

- **In media, i giorni necessari per identificare e contenere una minaccia informatica sono 235** (ci vogliono in media 174 giorni per identificare una violazione e 61 giorni per contenerla). Si tratta di 15 giorni in meno rispetto alla media italiana del 2022 (250 giorni). Questo dato è particolarmente interessante se si considera il dato pre-covid del 2019, che era di 283 giorni - 213 per identificare e 70 per contenere.

- I principali vettori di attacco sono: **social engineering** (15% delle violazioni di dati analizzate nello studio, un costo medio di 3,49 milioni di euro); **phishing** (14% delle violazioni, un costo medio di 3,63 milioni di euro); e **credenziali rubate o compromesse** (12% delle violazioni, un costo medio di 3,40 milioni di euro).

- I vettori più costosi sono invece: **insider malintenzionati** (6% delle violazioni di dati analizzate nello studio, un costo medio di 4,17 milioni di euro) e **compromissione delle e-mail aziendali** (10% delle violazioni, un costo medio di 3,64 milioni di euro).

- **L'intelligenza artificiale e l'automazione** hanno avuto il maggiore impatto sulla velocità di identificazione e contenimento delle violazioni nelle aziende intervistate. In Italia, le organizzazioni che hanno fatto un uso estensivo dell'AI e dell'automazione hanno registrato un ciclo di vita della violazione dei dati più breve di 112 giorni rispetto alle organizzazioni che non hanno utilizzato queste tecnologie (199 giorni contro 311 giorni). Di fatto, le organizzazioni analizzate che hanno utilizzato l'AI e l'automazione anche per la sicurezza informatica hanno registrato, in media, costi di violazione dei dati inferiori di quasi 1,56 milioni di euro (2,97 milioni di euro) rispetto alle organizzazioni che non hanno utilizzato queste tecnologie (4,53 milioni di euro) - il maggiore risparmio sui costi identificato nel report. Tuttavia, poiché quasi il 38% delle organizzazioni in Italia non ha ancora integrato l'AI e l'automazione nei propri sistemi di sicurezza informatica, le organizzazioni hanno ancora notevoli opportunità per aumentare la vel

- **Violazione dei dati in tutti gli ambienti** – Quasi il 41% delle violazioni dei dati analizzati ha comportato la perdita di dati in più ambienti, tra cui cloud pubblico, cloud privato e on-premise, dimostrando che i cybercriminali sono stati in grado di compromettere più ambienti evitando il rilevamento. Le violazioni dei dati che hanno avuto un impatto su più ambienti hanno anche portato a costi di violazione più elevati (3,72 milioni di euro in media).

- **Il vantaggio di DevSecOps** – Le organizzazioni di tutti i settori che hanno adottato in maniera significativa l'approccio DevSecOps hanno sostenuto un costo medio per violazione dei dati inferiore di 162.408 euro rispetto a quelle che l'hanno integrato in maniera limitata o nulla.

Ulteriori fonti

- ***Cost of a Data Breach Report 2023*** completo disponibile a questo link.

- Ulteriori informazioni sui risultati principali del report sono contenute in questoblog IBM Security Intelligence.

- Per iscriversi al webinar dedicato al Cost of a Data Breach Report di IBM Security, che si terrà**martedì 1 agosto 2023, alle 17:00,** cliccare qui.

- Contattare il team IBM Security X-Force per una consulenza personalizzata dei risultati attraverso il link: https://ibm.biz/book-a-consult.

- Per ulteriori informazioni sul report, visitare il sitoCost of a Data Breach Action Guide.

Informazioni su IBM Security

IBM Security aiuta a proteggere le aziende e le amministrazioni mondiali con un portafoglio integrato di prodotti e servizi di

sicurezza, che includono funzionalità dinamiche di automazione e AI. Tali soluzioni, supportate dalla ricerca IBM Security X-Force®, consentono alle organizzazioni di prevedere le minacce, proteggere i dati e rispondere con velocità e precisione agli attacchi, senza compromettere gli ambienti digitali. Con i propri esperti di sicurezza in tutto il mondo, IBM è richiesta da migliaia di organizzazioni come partner per valutare, implementare e gestire le trasformazioni delle strategie di sicurezza informatica. IBM gestisce una delle organizzazioni di ricerca, sviluppo e delivery di servizi di cybersecurity più grandi al mondo, monitora oltre 150 miliardi di eventi di sicurezza al giorno in oltre 130 paesi ed ha ottenuto più di 10.000 brevetti relativi alla sicurezza informatica in tutto il mondo.

Per maggiori informazioni:
Paola Piacentini, *IBM external Relations Leader*
email: paola_piacentini@it.ibm.com.
tel. + 39 335 1270646

[1] Il Cost of a Data Breach Report 2023, condotto da Ponemon, è finanziato e analizzato da IBM Security.
