X-Force

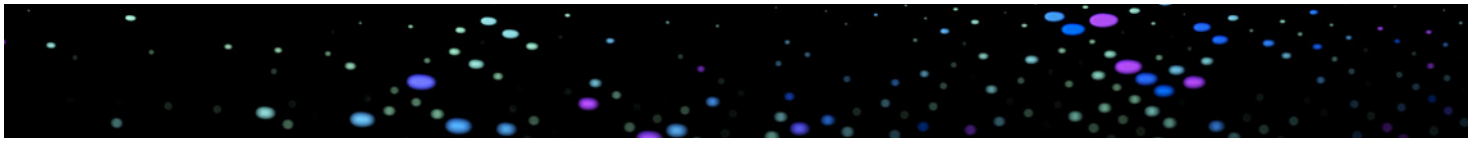
2021 IBM Security X-Force Insider Threat Report

IBM Security X-Force Threat Intelligence

Special Intelligence Report Q2 2021

IBM

Indice



Introduzione

Lo scenario delle minacce informatiche è in continua evoluzione: sia chi attacca che chi si difende è continuamente a caccia di innovazioni, nuove tecnologie e nuove procedure. Le organizzazioni, dal canto loro, spendono complessivamente circa 60 miliardi di dollari all'anno per proteggere i propri asset e per reperire professionisti in grado di prevenire e rispondere agli attacchi. La spesa generale per la sicurezza è aumentata di un ulteriore 10% nel 2021.[1]

Le organizzazioni concentrano gran parte della loro attenzione e del loro budget al contrasto agli attacchi esterni, sottovalutando spesso le minacce interne, ovvero quelle che provengono dall'azienda stessa. Le minacce interne, molte delle quali si rivelano poi non malevoli o accidentali, sono però anch'esse potenzialmente devastanti in termini di furti di dati, perdite finanziarie, furti di proprietà intellettuale e danni alla reputazione aziendale. In un sondaggio del 2020, l'Istituto Ponemon ha stimato che per porre rimedio alle minacce interne, indipendentemente dalla fonte dell'incidente, le organizzazioni hanno speso in media 644.852 dollari.[2] La cifra comprende i costi di monitoraggio e indagine sui presunti eventi interni, nonché le spese legate alla risposta, al contenimento, all'eliminazione del problema e al ripristino della situazione corretta.

Nel contesto del presente documento, IBM Security X-Force definisce un insider come segue:

— Insider accidentale: un dipendente o fornitore terzo negligente.[3]

— Insider malevolo: un dipendente o fornitore terzo con intenti malevoli o criminali.

1. https://www.infosecurity-magazine.com/news/global-cybersecurity-spending-to/
2. https://securityintelligence.com/posts/gaining-insight-into-the-ponemon-institutes-2020-cost-of-insider-threats-report/
3. Un insider negligente è colui o colei che causa in modo accidentale un incidente che danneggia la riservatezza, l'integrità o la disponibilità di dati o sistemi all'interno di un'organizzazione. Si escludono qui gli incidenti di tipo phishing/ingegneria sociale.

Mediante l'utilizzo di dati riservati ed esclusivi raccolti da indagini reali in risposta a incidenti, X-Force ha analizzato una serie di incidenti presumibilmente derivanti da minacce interne, sia accidentali sia malevole, che hanno colpito delle organizzazioni fra il 2018 e il 2020. In abbinamento con il reporting open-source degli attacchi più noti in materia di minacce dall'interno, questo documento esaminerà i risultati più importanti derivanti da tali dati, tra cui:

— Come viene scoperta la maggior parte degli attacchi interni.

— Il ruolo del livello di accesso negli attacchi interni.

— Le migliori prassi per mitigare le minacce dall'interno.

Risultati principali della ricerca

Il 40% degli incidenti è stato rilevato mediante avvisi generati da uno strumento di monitoraggio interno.

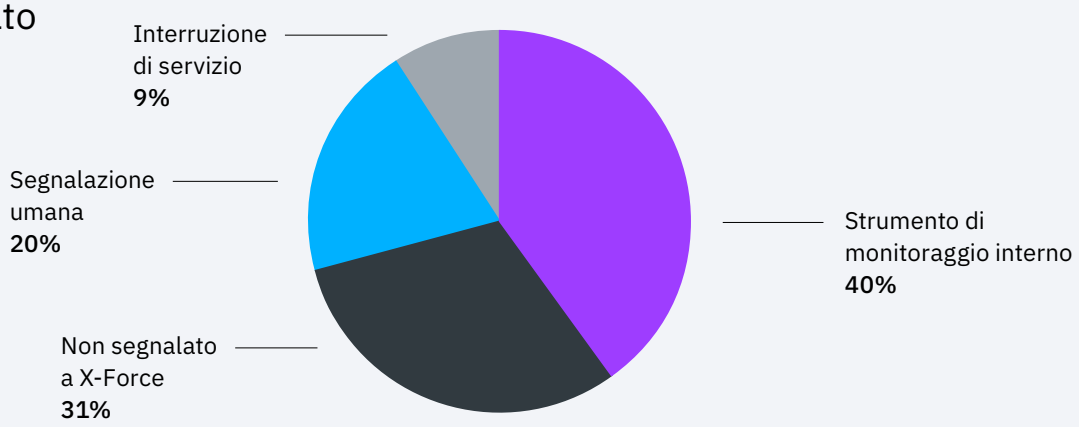
Il 40% degli incidenti ha riguardato un dipendente dotato di accesso privilegiato agli asset aziendali.

Nel 100% degli incidenti in cui l'insider aveva certamente o probabilmente accesso amministrativo, tale modalità di accesso privilegiato ha ricoperto un ruolo cruciale nell'incidente stesso.

Come si scoprono gli attacchi relativi a minacce interne

Le minacce interne sono solitamente costituite da attacchi nei quali gli utenti legittimi dotati di un determinato livello di accesso agli asset aziendali sfruttano tale accesso, in modo malevolo o involontario, con conseguente danno all'organizzazione. La minaccia può provenire da un dipendente attuale o un ex dipendente, così come da un fornitore terzo che disponga dell'accesso per svolgere una determinata funzione professionale.

Come è stato scoperto l'attacco interno



Secondo un'analisi delle minacce interne alle quali X-Force ha risposto dal 2018 in poi, il 40% di tali incidenti è stato rilevato mediante avvisi generati da uno strumento di monitoraggio interno. La segnalazione umana, come ad esempio un dipendente che avvisi la propria organizzazione di un'attività anomala, ha costituito il 20% degli incidenti individuati, mentre nel 9% dei casi i team di sicurezza sono stati avvisati da un'interruzione del sistema.

Nel 2020 Cost of Insider Threats: Global Report, stilato dall'Istituto Ponemon e sponsorizzato da ObserveIT e IBM, si stima che strumenti quali User Behaviour Analytics (UBA), Privileged Access Management (PAM), Security Information and Event Management (SIEM) e programmi come la condivisione di threat intelligence, unitamente alla formazione e alla sensibilizzazione degli utenti, abbiano fatto risparmiare alle organizzazioni in media 3 milioni di dollari per quanto riguarda la riduzione o l'eliminazione dei rischi interni.[4]

Risparmio sui costi: 3 milioni di dollari

Si stima che strumenti quali UBA, PAM, SIEM e programmi come la condivisione di threat intelligence, unitamente alla formazione e alla sensibilizzazione degli utenti, abbiano fatto risparmiare alle organizzazioni in media 3 milioni di dollari per quanto riguarda la riduzione o l'eliminazione dei rischi interni.[4]

4. https://securityintelligence.com/posts/gaining-insight-into-the-ponemon-institutes-2020-cost-of-insider-threats-report/

Mancanza di prove e incognite nella ricerca X-Force

Per quanto concerne gli incidenti interni per i quali la modalità di scoperta è stata “non segnalato a X-Force” o “mancanza di prove”, ai team X-Force preposti alla risposta agli incidenti non sono state fornite sufficienti informazioni per poter definire le modalità di rilevazione. Questo si verifica in quanto a molte organizzazioni manca spesso visibilità sull’ambiente di base e sul modo in cui opera. Per rilevare qualsiasi attività anomala in un sistema è fondamentale conoscere come si presenta l’attività standard, cosicché gli eventi atipici possano essere individuati più facilmente e con sicurezza. Nel 2019, IBM ha sponsorizzato un report SANS[5] dedicato allo scenario delle minacce avanzate mirate alle organizzazioni. Lo studio ha indicato che:

— Il 48% delle aziende considera la carenza di visibilità nella propria infrastruttura come la principale lacuna di sicurezza.

— Il 35% ritiene di non disporre della capacità di rilevare gli utilizzi impropri da parte di soggetti interni all’azienda.

— Il 47% delle aziende ammette di non comprendere le modalità di funzionamento dell’attività di base all’interno delle proprie reti.

6. https://www.ibm.com/account/reg/it-it/signup?formid=urx-39989

Confronto tra accesso privilegiato e amministrativo

Nel corso dell'analisi degli incidenti legati a minacce dall'interno, X-Force ha classificato due diverse tipologie di utenti.

Definiamo **utente con privilegi** chi, all'interno dell'organizzazione, ha accesso a dati sensibili. Può trattarsi di proprietà intellettuali, dati sui clienti o informazioni relative alle risorse umane. Fra tali utenti possono figurare anche coloro in grado di accedere a dati sensibili sull'azienda come, ad esempio, dati su fusioni e acquisizioni o altre informazioni di natura legale.

Definiamo invece utenti con **accesso amministrativo**, detti anche amministratori o admin, coloro che dispongono di un accesso privilegiato ai sistemi IT all'interno della rete. In teoria, queste tipologie di accesso non dovrebbero sovrapporsi. Tuttavia, X-Force ha rilevato che agli utenti finali viene spesso fornito un diritto di accesso eccessivo negli ambienti IT in cui operano.

Gli insider dotati di accesso amministrativo differiscono da quelli con accesso a dati sensibili dell'ambiente aziendale. Comprendono dipendenti e fornitori con accesso all'ambiente IT dell'organizzazione e rappresentano un rischio particolare per un'organizzazione in base ai loro privilegi elevati nella rete.

Esempi di ruoli dotati di accesso privilegiato

- Funzioni nelle risorse umane
- Dirigenti
- Ruoli nell'amministrazione finanziaria
- Ruoli legali
- Ruoli di ricerca
- Altri ruoli con accesso alla proprietà intellettuale dell'organizzazione, ad asset particolarmente importanti per l'azienda o ai dati sui clienti

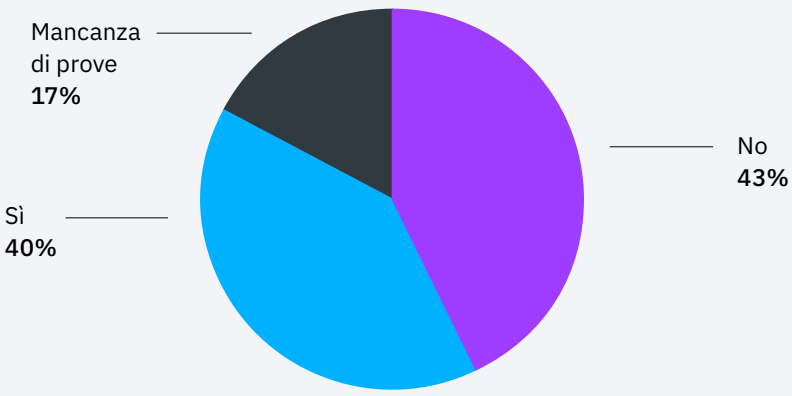
Esempi di ruoli dotati di accesso amministrativo

- Amministratori dei server
- Amministratori IT
- Servizio clienti
- Fornitori IT terzi
- Altri ruoli in grado di modificare configurazioni e/o impostazioni dei sistemi IT

Chi controlla i controllori?

Gli insider che tipicamente causano incidenti sono coloro che dispongono di accesso privilegiato? La risposta è semplice e breve: sì.

L'insider aveva accesso privilegiato ai dati?



Secondo le analisi di X-Force, il 40% degli incidenti provocati da insider ha riguardato un dipendente con accesso privilegiato agli asset sensibili dell'azienda. Ai fini della ricerca, X-Force ha classificato come accesso privilegiato quello di cui dispone chi lavora in reparti comprendenti IT, risorse umane, finanza, sicurezza o funzioni dirigenziali.

In un ulteriore 17% dei casi, non è stato chiaro se l'insider disponesse di accesso privilegiato ai dati sensibili, il che ci suggerisce che il numero di incidenti causati da utenti con accesso privilegiato potrebbe essere addirittura più elevato.

I soggetti dotati di accesso elevato ad asset critici, come le condivisioni di rete, le apparecchiature per la sicurezza, i sistemi e-mail, i dati di identificazione personale (Personally Identifiable Information, PII) relativi a dipendenti e/o clienti, le proprietà intellettuali e i dati finanziari possono costituire un rischio notevolmente più alto rispetto a chi dispone di privilegi più ridotti.

È ragionevole ritenere che gli incidenti causati accidentalmente da insider con accesso privilegiato finiscano per costare alle organizzazioni più di quelli provocati da insider accidentali dotati di un livello di accesso inferiore. Gli incidenti che coinvolgono insider malevoli dotati di livelli più elevati di accesso privilegiato sono quelli che determinano i costi più onerosi; inoltre, gli attacchi provocati da tali utenti possono sfociare in violazioni dei dati su larga scala. Nel 2018, ad esempio, un agente immobiliare australiano di un'agenzia locale di alto profilo venne scoperto ad accedere a database riservati poco prima di lasciare il posto di lavoro. L'agente aveva manipolato le note relative alle previsioni di vendita nel sistema, riducendo il grado di interesse dei potenziali clienti. In più, confessò di aver sottratto oltre 200 record di clienti per utilizzarli nella nuova agenzia per la quale avrebbe lavorato. L'attacco interno, secondo le stime, costò all'agenzia colpita 30 milioni di dollari in termini di potenziali vendite immobiliari.[6]

Uno dei metodi migliori per prevenire incidenti correlati al livello di accesso degli insider è di adottare il principio del privilegio minimo, facendo sì che gli utenti dispongano unicamente del livello di accesso essenziale per poter svolgere le proprie funzioni all'interno dell'organizzazione. Ciò può essere attuato mediante una soluzione di gestione degli accessi privilegiati (PAM), che può essere configurata con il modello Zero Trust.[7,8] Tale modello prevede che a chiunque sia dotato di un account utente venga concesso il livello minimo di privilegi, riducendo così le possibilità che un insider ottenga accessi non desiderati a dati o asset. Tale strategia diviene ancora più determinante nel cloud, dove risiedono più dati a cui devono poter accedere richiedenti sia umani che non umani a fini operativi.

Dal 2020 Cost of Insider Threats: Global Report emerge che solo il 39% delle organizzazioni ha adottato una qualche forma di gestione degli accessi privilegiati.[9] In più, ha mostrato che l'adozione di un PAM ha consentito un risparmio sui costi di 3,1 milioni di dollari, evidenziando in tal modo l'efficacia di tali misure.

39%

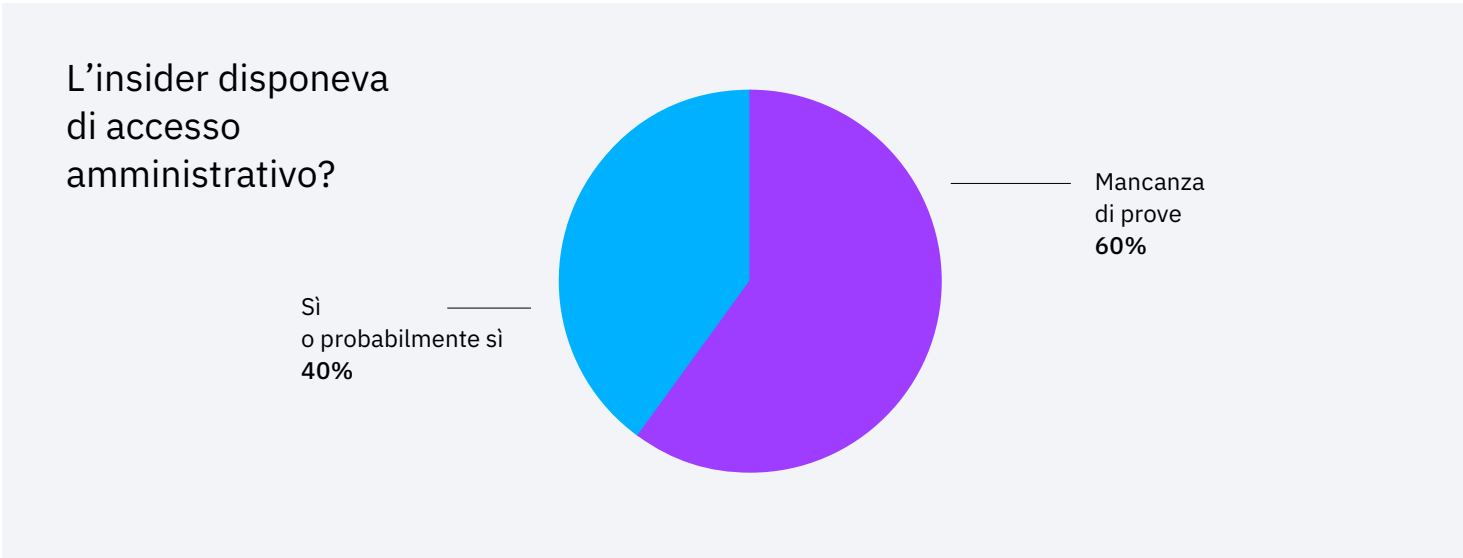
Il 39% delle organizzazioni ha adottato una qualche forma di PAM.[9] Tale soluzione ha consentito un risparmio sui costi di 3,1 milioni di dollari.

6. https://indaily.com.au/news/2018/10/23/harris-director-resigns-from-top-real-estate-post/
7. https://www.ibm.com/it-it/security/identity-access-management/privileged-access-management
8. https://www.ibm.com/it-it/security/zero-trust
9. https://www.ibm.com/it-it/security/digital-assets/services/cost-of-insider-threats/

L’uso improprio dell’accesso amministrativo costa molto alle aziende

Sono stati rilevati numerosi casi pubblici di insider che avevano usato impropriamente i propri poteri di utenti amministratori nelle organizzazioni a fini illeciti, tra cui vendetta, guadagno economico e altri intenti malevoli. Nel febbraio 2020 Volodymyr Kvashuk, ex tecnico di Microsoft, fu riconosciuto colpevole di aver usato il proprio accesso privilegiato per sottrarre all’azienda asset digitali per un valore di oltre 10 milioni di dollari.[10] Il diritto di accesso amministrativo di Kvashuk alla piattaforma di vendite retail della cui gestione era responsabile ha reso possibile il furto.[11] In particolare, Kvashuk aveva usato indirizzi e-mail e account di prova funzionanti di alcuni colleghi per offuscarne l’attività, tra cui l’esfiltrazione di buoni regalo digitali. Queste e altre risorse sottratte venivano vendute su Internet per profitto personale, utilizzato in seguito dal dipendente per acquistare una casa del valore di 1,6 milioni di dollari e un’auto Tesla da 160.000 dollari.[12]

L’uso improprio dell’accesso amministrativo in cifre



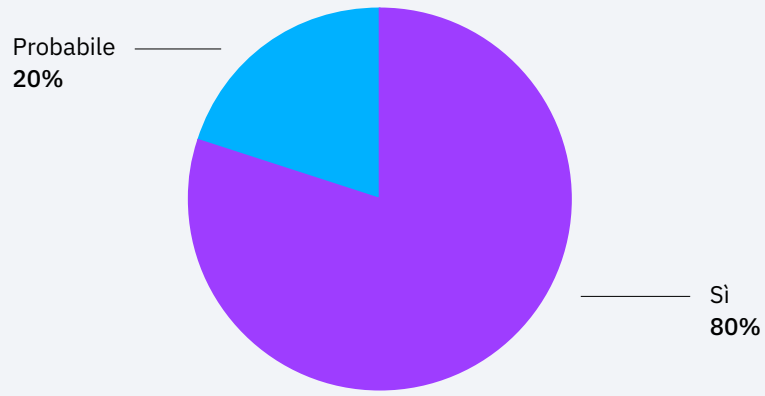
Nel 40% degli incidenti a cui X-Force ha risposto tra il 2018 e il 2020, l’insider aveva certamente o probabilmente accesso alla rete in qualità di amministratore. Se il ruolo specifico dell’utente non è stato chiarito dal cliente, gli analisti X-Force hanno determinato il tipo di accesso interno in base ai dettagli dell’incidente.

10. https://www.justice.gov/usao-wdwa/pr/former-microsoft-software-engineer-sentenced-nine-years-prison-stealing-more-10-million
11. https://apnews.com/article/seattle-retail-sales-james-robart-13f5a86053533b40034246ef37ecad8d
12. https://www.redmond-reporter.com/news/former-microsoft-employee-convicted-of-18-federal-felonies/

Tali incidenti hanno implicato, tra l'altro, l'esfiltrazione di dati, l'esposizione e la cancellazione di dati sensibili e l'installazione di software non autorizzati. Nello specifico, alcune organizzazioni hanno perduto petabyte di log cancellati dai server, sofferto di fughe di codici sorgente nonché subito onerose interruzioni di servizio per mano di un insider dotato di accesso amministrativo.

Ma il dato più interessante è che nel 100% degli incidenti nei quali l'insider aveva certamente o probabilmente accesso amministrativo, tale modalità di accesso ha ricoperto un ruolo nell'incidente stesso (vedere grafico sottostante).

L'accesso elevato alla rete ha svolto un ruolo cruciale nell'incidente interno?



In altre parole, se l'insider non avesse avuto accesso amministrativo, l'incidente avrebbe probabilmente avuto un impatto di gran lunga inferiore sull'organizzazione o, in molti casi, non si sarebbe verificato affatto. X-Force ha risposto a numerosi incidenti interni nei quali erano stati cancellati dai server database e log di importanza critica. Se l'insider non avesse avuto accesso amministrativo a tali sistemi, l'evento non si sarebbe verificato.

Raccomandazioni

X-Force ritiene che il numero di incidenti interni sia sottostimato nei dati forniti da terzi. È probabile che si verifichino e vengano trattati internamente dalle organizzazioni molti più incidenti di questo tipo di quanti ne vengano rivelati all'esterno, per timore di incorrere in responsabilità e danni alla reputazione aziendale.[13]

La ricerca e i dati di X-Force evidenziano l'esigenza di rendere le potenziali minacce dall'interno una componente importante nei programmi di sicurezza informatica, dato l'impatto che tali incidenti possono avere sulle aziende. In particolare, IBM Security raccomanda quanto segue in merito alle minacce dall'interno:

Le strategie "defense in depth" sono efficaci nel rilevamento delle minacce interne.

Tradizionalmente, un approccio multilayer alle tecnologie e ai processi implementati dalle organizzazioni è considerato uno strumento valido per affrontare le minacce esterne. Gli studi di X-Force indicano come molti di questi strumenti, tra cui le soluzioni SIEM (Security Information and Event Management), siano stati decisivi anche nel rilevamento di attività relative a minacce dall'interno.

Capire quale sia la "normalità" nel proprio ambiente.

Il modo migliore per rilevare le azioni sospette da parte di qualsiasi tipo di aggressore è comprendere quale tipo di attività sia da considerarsi normale nella propria rete. Conoscendo a fondo l'attività di base è più facile rilevare i comportamenti anomali e reagirvi prontamente in modo efficace. Questa funzionalità può essere fornita da una robusta soluzione UBA (User Behaviour Analytics) in grado di adattarsi nel tempo alle modifiche dell'ambiente.

Verificare regolarmente gli accessi amministrativi.

X-Force ha scoperto che molti degli incidenti che coinvolgevano amministratori erano probabilmente dovuti a privilegi eccessivi per gli utenti. Per gli accessi amministrativi, specialmente su server di tipo mission-critical, va attuato un rigido controllo di modifiche e processi. Consigliamo di considerare soluzioni tecnologiche che registrino e forniscano accesso amministrativo temporaneo a sistemi e funzioni sensibili.

13. https://www.darkreading.com/edge/theedge/fbi-encounters-reporting-an-insider-security-incident-to-the-feds-/b/d-id/1340016

Separare i team di sicurezza informatica e quelli di amministrazione IT.

L'esperienza di X-Force dimostra che un approccio equilibrato alla gestione dell'indipendenza e della governance dei team di sicurezza e amministrazione contribuisce a ottenere un grado di sicurezza più elevato. Consente inoltre ai team amministrativi di disporre della flessibilità e della creatività necessarie per ottimizzare la propria esplorazione e scoperta delle minacce, fornendo all'azienda una sufficiente supervisione e vigilanza per ridurre al minimo i rischi interni alla squadra di lavoro.

Creare profili di rischio per i ruoli organizzativi sensibili.

Poiché l'accesso elevato è risultato influente in numerosi casi di incidente interno a cui X-Force ha risposto, raccomandiamo alle aziende di considerare la creazione di profili di rischio per le posizioni all'interno dell'organizzazione che abbiano accesso sensibile o amministrativo a sistemi e/o dati. L'implementazione di una soluzione PAM (Privileged Access Management), basata su un modello Zero Trust, determina privilegi di accesso minimi per gli utenti ed è in grado di ridurre al minimo l'impatto degli incidenti interni.

Aggiornare il manuale di risposta agli incidenti includendo le minacce dall'interno.

Per questi incidenti non è sufficiente una formazione generica. Benché la maggior parte dei manuali di risposta agli incidenti comprenda casi di attacchi da parte di avversari esterni, è bene che le organizzazioni prendano in considerazione l'idea di aggiungere scenari che comprendano anche minacce dall'interno, siano esse malevole o involontarie. Consigliamo di rivolgersi a un partner in grado di aiutare a sviluppare piani di risposta agli incidenti e manuali specifici per gli attacchi, così da essere preparati e poter rispondere meglio agli attacchi informatici.

Formazione continua dei dipendenti.

I programmi di formazione annuale di molte organizzazioni comprendono procedure etiche, insieme alla formazione dedicata all'ingegneria sociale. Molti degli incidenti interni a cui X-Force ha risposto sono stati scoperti da altri dipendenti, anziché dalle tecnologie. Nell'ambito delle proprie attività annuali dedicate all'etica aziendale e alla formazione sull'ingegneria sociale, le organizzazioni devono includere istruzioni su come segnalare un presunto incidente interno. Una formazione basata sui ruoli rivolta ai dipendenti con privilegi di accesso può inoltre contribuire a renderli consapevoli dei segnali che possono indicare un comportamento anomalo.

Usare servizi affidabili di threat intelligence.

Ai clienti si presenta spesso la sfida di creare, gestire e rendere operativa la threat intelligence. È bene cercare una soluzione che offra l'aggregazione, l'automazione e le integrazioni necessarie per rendere la threat intelligence operativa su larga scala.

I servizi Managed Detection and Response offrono protezione 24 ore su 24.

I servizi di sicurezza MDR (Managed Detection and Response) sono essenziali per fornire prevenzione, rilevamento e rapide risposte alle minacce dall'interno. Risulta quindi fondamentale disporre di soluzioni che vadano oltre la prevenzione tradizionale, con AV di nuova generazione che consentano indagini e interventi basati sui comportamenti e una gestione continuativa delle policy.

Scopri come IBM Security aiuti i clienti a proteggere gli ambienti più complessi e critici dalle minacce esterne e interne.

Ulteriori informazioni su IBM Security

IBM Security

IBM Italia S.p.A.
Circonvallazione Idroscalo
20054 Segrate (Milano)
Italia

Prodotto negli Stati Uniti d'America
Maggio 2021

IBM