Cinque passi falsi comuni per la sicurezza dei dati da evitare

Scopri come migliorare la tua postura di sicurezza

IBM Security

Indice

La sicurezza dei dati dovrebbe essere una delle principali priorità per le aziende.

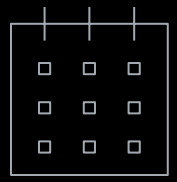
Anche se lo scenario IT diventa sempre più complesso e decentralizzato, è importante comprendere che molte delle violazioni alla sicurezza si possono prevenire. Sebbene gli obiettivi e le sfide di sicurezza possano cambiare da azienda a azienda, spesso le organizzazioni commettono gli stessi errori quando iniziano ad affrontare la sicurezza dei dati. Inoltre, diversi leader aziendali, spesso accettano questi errori come normale pratica di business.

Ci sono diversi fattori esterni e interni che possono contribuire al successo degli attacchi informatici, tra cui:

- Erosione dei parametri di rete
- Più possibilità di attacco a causa di ambienti IT complessi
- Le crescenti richieste che i servizi cloud attuano nei confronti delle practice di sicurezza
- La natura sempre più sofisticata dei crimini informatici
- Skill shortage
- Mancanza di consapevolezza da parte dei dipendenti circa i rischi relativi alla sicurezza dei dati

8.19 milioni di dollari

Costo medio di una violazione dei dati negli Stati Uniti nel 2019[1]



245 giorni

Tempo medio per identificare e contenere una violazione dei dati negli Stati Uniti[1]

Quanto sono forti le tue pratice relative alla sicurezza dei dati?

Diamo uno sguardo ai cinque passi falsi più comuni – ed evitabili – in termini di sicurezza dei dati che rendono le organizzazioni vulnerabili ai potenziali attacchi e cerchiamo di capire come evitarli.

Accelerare la conformità

Centralizzare la sicurezza

Stabilire l’ownership

Valutare le vulnerabilità

Assegnare priorità alle attività

Passo falso 1

L’incapacità di andare oltre la conformità

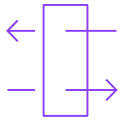
Conformità non necessariamente significa sicurezza. Le organizzazioni che concentrano tutte le loro risorse limitate nell’essere conformi a una certificazione o a un controllo potrebbero diventare compiacenti. Numerose importanti violazioni dei dati sono avvenute in organizzazioni che sulla carta erano completamente conformi. I seguenti esempi ci mostrano come la focalizzazione verso la conformità possa diminuire l’effettiva sicurezza:

Copertura incompleta
Le aziende spesso si affannano per cercare di affrontare le politiche di accesso obsolete e le errate configurazioni del database prima del controllo annuale. Le valutazioni dei rischi e delle vulnerabilità dovrebbero essere attività continue.

Sforzo minimo
Molte aziende adottano soluzioni di sicurezza dei dati solo per adempiere ai requisiti legali o dei business partner. Un atteggiamento del tipo “facciamo in modo di implementare uno standard minimo e torniamo al lavoro” può andare contro le buone practice di sicurezza. La sicurezza efficace dei dati è una maratona, non uno sprint.

Urgenza affievolita
Le aziende possono diventare più compiacenti a gestire i controlli nel momento in cui le normative come SOX (Sarbanes-Oxley Act) e il GDPR (General Data Protection Regulation) entrano in vigore. Ma, anche se con il passare del tempo, i leader potrebbero prestare meno attenzione alla privacy, alla sicurezza e alla protezione dei dati regolamentati, i rischi e i costi associati alla mancata conformità rimangono.

1.4



al giorno

1.4 violazioni dei dati sanitari stimati al giorno nel 2019, nonostante la legge HIPAA (Health Insurance Portability and Accountability Act)[2]

Omissione di dati non regolamentati
Gli asset, come ad esempio la proprietà intellettuale, possono mettere l’organizzazione a rischio in caso di perdita o condivisione con personale non autorizzato. Concentrarsi esclusivamente sulla conformità può portare le organizzazioni di sicurezza a sottovalutare e non proteggere a sufficienza i dati importanti.

Soluzione

Riconoscere e accettare che la conformità è un punto di partenza, non l’obiettivo

Le organizzazioni di sicurezza dei dati devono stabilire dei programmi strategici che proteggano in modo coerente i dati critici di business, rispetto al semplice rispondere ai requisiti di conformità.

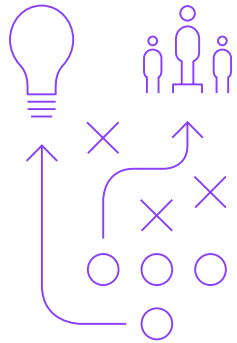
I programmi di protezione e sicurezza dei dati dovrebbero includere queste pratiche principali:

- **Rilevare e classificare i dati sensibili** in cloud e on-premise.
- **Valutare il rischio** con analytics e insight contestuali
- **Proteggere i dati sensibili** attraverso la crittografia e le politiche di accesso flessibili.
- **Monitorare l’accesso ai dati e i modelli** di utilizzo per scoprire rapidamente le attività sospette.
- **Rispondere alle minacce** in tempo reale.
- **Semplificare la conformità** e il reporting.

L’elemento finale può includere le responsabilità legali correlate alla conformità normativa, le possibili perdite che un’azienda potrebbe subire e i potenziali costi di tali perdite oltre alle multe per la mancata conformità.

Infine, sarebbe opportuno valutare il rischio nel suo insieme e il valore dei dati che si desidera proteggere.

Vedere la conformità come un’opportunità per innovare e innalzare gli standard di sicurezza per supportare il business.



Passo falso 2

L’incapacità di riconoscere l’esigenza di una sicurezza dei dati centralizzata

Senza obblighi di conformità più ampi che riguardano la sicurezza e la privacy dei dati, i leader dell’organizzazione possono perdere di vista l’esigenza di una sicurezza dei dati coerente, che riguardi tutta l’azienda.

Per le aziende con ambienti ibridi multicloud che cambiano e crescono di continuo, possono esserci nuovi tipi di data source ogni settimana o ogni giorno, e causare un’ampia dispersione di dati sensibili.

I leader delle aziende che stanno ampliando e aumentando le loro infrastrutture IT, possono non riuscire a riconoscere il rischio insito nella loro mutevole superficie di attacco. Possono non avere un’adeguata visibilità e controllo, man mano che i dati sensibili si spostano in un ambiente IT sempre più complesso e variegato. La mancata adozione di controlli per la protezione, la sicurezza e la privacy dei dati end-to-end – soprattutto all’interno di ambienti complessi – può trasformarsi in una distrazione molto costosa.

L’attuazione di singole soluzioni di sicurezza, può causare ulteriori problemi. Ad esempio, le organizzazioni con un security operations center (SOC) e una soluzione security information and event management (SIEM), potrebbero trascurare i sistemi non alimentandoli con insight raccolti dalle soluzioni di data security. Allo stesso modo, la mancanza di interoperabilità tra il personale, i processi e i tool di sicurezza, può impedire il successo di qualsiasi programma dedicato alla sicurezza.

La crittografia, la gestione della business continuity, l’integrazione della sicurezza nei processi di sviluppo software (DevSecOps) e la condivisione di threat intelligence possono contribuire a ridurre i costi per la violazione dei dati. [1]

Soluzione

Sapere dove risiedono i dati sensibili, inclusi i repository cloud-hosted e on-premise

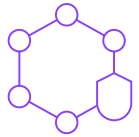
La protezione dei dati sensibili dovrebbe andare di pari passo con gli sforzi più ampi di sicurezza. Oltre a sapere dove risiedono i dati sensibili, è necessario conoscere anche quando e come viene effettuato l'accesso – anche se queste informazioni cambiano rapidamente. Inoltre, si dovrebbe lavorare per integrare le politiche e gli insight sulla protezione e sulla sicurezza dei dati nel programma generale sulla sicurezza, per consentire la comunicazione strettamente allineata tra tecnologie. Può essere utile in questo processo una soluzione per la sicurezza dei dati che operi in piattaforme e ambienti eterogenei.

Quindi, quando è il momento giusto per integrare la sicurezza dei dati con altri controlli di sicurezza, come parte di una pratica di sicurezza più olistica? Di seguito alcuni indicatori che suggeriscono che l'organizzazione è pronta per questo passaggio successivo:

Rischio di perdita di dati importanti
Il valore dei dati proprietari, sensibili e personali dell'organizzazione è così importante, che la sua perdita potrebbe causare un danno significativo alla sostenibilità del business.

Implicazioni normative
La tua organizzazione raccoglie e memorizza i dati con requisiti legali, come numeri delle carte di credito, altre informazioni di pagamento o dati personali.

La protezione dei dati sensibili dovrebbe andare di pari passo con gli sforzi più ampi di sicurezza.



Mancanza di controllo sulla sicurezza
La tua organizzazione è cresciuta a tal punto che è difficile tenere traccia e proteggere tutti gli endpoint di rete, incluse le istanze cloud. Ad esempio, hai un'idea chiara di dove, come e quando i dati vengono memorizzati, condivisi e consultati in cloud e on-premise?

Valutazione inadeguata
L'organizzazione ha adottato un approccio frammentato nel quale non esiste una chiara comprensione di quanto venga investito in tutte le attività riguardanti la sicurezza. Ad esempio, ci sono processi in atto per valutare precisamente il ROI in termini di risorse distribuite per ridurre il rischio legato alla sicurezza dei dati?

Se riconosci una qualsiasi delle situazioni qui descritte nella tua organizzazione, è il caso di prendere in considerazione l'acquisizione di soluzioni e competenze di sicurezza necessarie per integrare la sicurezza dei dati nella più ampia pratica di sicurezza esistente.

Passo falso 3

L’incapacità di definire chi ha la responsabilità dei dati

Anche quando sono consapevoli della necessità della sicurezza dei dati, molte aziende non hanno nessuno che sia specificamente responsabile della protezione dei dati sensibili. Questa situazione emerge spesso quando avviene un incidente di sicurezza dei dati o di audit e l’organizzazione è sotto pressione per scoprire chi sia veramente responsabile.

I top executive potrebbero rivolgersi al CIO (chief information officer) che potrebbe rispondere “Il nostro compito è far sì che i sistemi siano in esecuzione. Rivolgetevi a qualcuno dello staff IT.” I dipendenti IT potrebbero essere responsabili di numerosi database in cui risiedono i dati sensibili, eppure manca un budget dedicato alla sicurezza.

Generalmente, i team guidati dai CISO (chief information security officer) non sono direttamente responsabili dei dati che passano in tutta l’azienda. Possono dare consigli ai vari manager LOB (line-of-business) in un’azienda, ma in molte società, nessuno è esplicitamente responsabile dei dati stessi. Per un’organizzazione, i dati sono uno degli asset più importanti. Eppure, senza una responsabilità di ownership, la protezione adeguata dei dati sensibili si trasforma in una sfida.

Il

74%

delle organizzazioni intervistate sostiene che la carenza di competenze in materia di sicurezza informatica ha influito sull’organizzazione.[3]

“Nel 2018, il 67.9% delle aziende intervistate ha dichiarato di avere un CDO (chief data officer). Tuttavia, il ruolo rimane mal definito.”[4]

NewVantage Report
Big Data and AI Executive Survey 2019,
Executive Summary of Findings

Leggi lo studio →

Soluzione

Assumere un CDO o DPO dedicato alla sicurezza dei dati critici e sensibili

Negli ambienti IT complessi, è fondamentale tener conto dei dati nelle seguenti ubicazioni:

Condivisi in unità di business

Ubicati in infrastrutture di multicloud ibrido

Memorizzati su dispositivi mobili

Un CDO (chief data officer) o un DPO (data protection officer) possono svolgere questi compiti. In realtà, le aziende con sede in Europa o che svolgono attività di business con soggetti di dati dell'Unione Europea, devono rispondere agli obblighi del GDPR che richiedono di avere un DPO. Questo requisito preliminare riconosce che i dati sensibili – in questo caso le informazioni personali– hanno un valore che si estende al di là della LOB che utilizza tali dati. Inoltre, il requisito sottolinea che le aziende hanno un ruolo ben preciso in termini di responsabilità degli asset di dati. Tenere in considerazione i seguenti obiettivi e responsabilità nello scegliere un CDO o DPO:

Competenze tecniche e strategia di business
Valutare il rischio e creare un business case pratico che i leader di business non tecnici possano comprendere riguardo agli investimenti di sicurezza appropriati.

Implementazione strategica
Stabilire un piano a livello tecnico che applichi dei controlli in termini di rilevamento, risposta e sicurezza dei dati, per fornire protezione.

Compliance leadership
Conoscere i requisiti di conformità e sapere come associare tali requisiti ai controlli di sicurezza dei dati in modo che il business sia conforme.

Monitoraggio e valutazione
Monitorare lo scenario delle minacce e misurare l'efficacia del programma di sicurezza dei dati.

Flessibilità e scalabilità
Sapere quando e come adattare la strategia di sicurezza dei dati, ad esempio l'espansione dell'accesso ai dati e le politiche di utilizzo nei nuovi ambienti, integrando gli strumenti più avanzati.

Divisione del lavoro
Stabilire le aspettative con i provider di servizi cloud riguardo agli SLA (service-level agreements) e alle responsabilità associate al rischio per la sicurezza dei dati e alla remediation.

Piano di risposta alla violazione dei dati
Infine, essere pronti ad avere un ruolo chiave nel definire un piano strategico di mitigazione e risposta alle violazioni.

In sostanza, il CDO o DPO dovrebbe promuovere la collaborazione per la sicurezza dei dati tra i vari team e in tutta l'azienda, visto che ognuno ha bisogno di collaborare per proteggere in modo efficace i dati aziendali. Questa collaborazione può aiutare il CDO o DPO a supervisionare le protezioni e i programmi di cui ha bisogno l'organizzazione per riuscire a proteggere i dati sensibili.

Passo falso 4

L’incapacità di affrontare le vulnerabilità conosciute

Le violazioni di alto profilo nelle aziende spesso derivano da vulnerabilità conosciute, che non sono state risolte anche dopo il rilascio delle patch. La mancata risoluzione delle vulnerabilità conosciute anche dopo rilascio delle patch mette a rischio i dati dell’organizzazione, in quanto i criminali informatici cercano attivamente questi punti di ingresso facili.

Tuttavia, numerose aziende hanno difficoltà a implementare rapidamente le patch a causa del livello di coordinamento richiesto tra gruppi operativi, di sicurezza e IT. Inoltre, le patch spesso richiedono dei test per verificare che non interrompano un processo o introducano una nuova vulnerabilità.

Negli ambienti cloud, a volte è difficile sapere se a un componente acquisito di un’applicazione o di un servizio deve essere applicata la patch. Anche se viene trovata una vulnerabilità in un servizio, gli utenti spesso non hanno controllo sufficiente sul processo di correzione del provider di servizi.

Il

51%

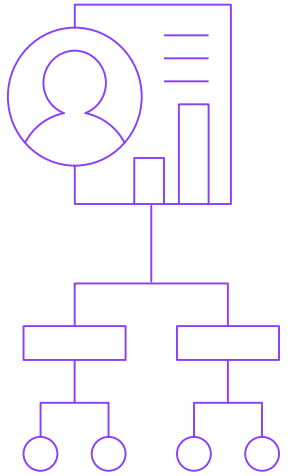
delle violazioni registrate nel 20219 è stato causato da attacchi malevoli. Gli attacchi malevoli sono la causa principale più diffusa e costosa delle violazioni.[1]

Soluzione

Stabilire un programma efficace per la gestione delle vulnerabilità, con la tecnologia appropriata per supportarne la crescita

La gestione delle vulnerabilità implica generalmente alcuni dei seguenti livelli di attività:

- Garantire condizioni base e un inventario accurati per gli asset di dati.
- Condurre valutazioni e scansioni frequenti delle vulnerabilità in tutta l'infrastruttura, inclusi gli asset cloud.
- Assegnare priorità alle azioni di correzione delle vulnerabilità, considerando anche la probabilità che la vulnerabilità venga sfruttata e l'impatto che l'evento avrebbe sul business.
- Includere la reattività e la gestione delle vulnerabilità nello SLA, con provider di servizi di terze parti.
- Offuscare i dati personali o sensibili laddove possibile. La crittografia, la tokenizzazione e la redazione sono tre opzioni per il raggiungimento di questo scopo.
- Adottare una gestione adeguata delle chiavi crittografiche, garantendo che tali chiavi siano memorizzate in modo sicuro e che venga eseguito un ciclo adeguato per garantire la sicurezza dei dati crittografati.



Persino all'interno di un programma di gestione delle vulnerabilità maturo, nessun sistema può essere perfetto. Partendo dal presupposto che le intrusioni possono avvenire anche negli ambienti meglio protetti, i dati hanno bisogno di un altro livello di protezione. La giusta serie di funzionalità e tecniche di crittografia dei dati può aiutare a proteggere i dati dalle minacce nuove ed emergenti.

Passo falso 5

L’incapacità di assegnare priorità e utilizzare il monitoraggio dell’attività dei dati

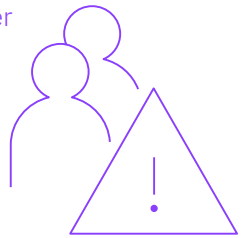
Il monitoraggio dell’accesso e dell’utilizzo dei dati è una parte essenziale di qualunque strategia di sicurezza dei dati. Un leader aziendale deve sapere chi, come e quando le persone accedono ai dati. Questo monitoraggio dovrebbe valutare anche se le persone hanno diritto all’accesso, se il livello dell’accesso è corretto e se rappresenta un rischio elevato per l’azienda.

Le identificazioni di utenti con privilegi sono una causa diffusa delle minacce interne.5 Un piano di protezione dei dati dovrebbe includere il monitoraggio in tempo reale per rilevare gli account di utenti con privilegi che vengono utilizzati per attività sospette o non autorizzate. Per evitare possibili attività malevoli, è necessario che la soluzione metta in atto le seguenti attività:

- Bloccare e mettere in quarantena le attività sospette in base alle violazioni di policy.
- Sospendere o chiudere le sessioni in base a comportamenti anomali.
- Utilizzare flussi di lavoro predefiniti specifici a livello normativo in tutti gli ambienti di dati.
- Inviare avvisi utili ai sistemi operativi e di sicurezza IT.

Il costo medio globale per una minaccia interna è

11.45 milioni di dollari. [6]



Tenere in considerazione le informazioni relative alla conformità e alla sicurezza dei dati e sapere come e quando rispondere alle potenziali minacce può essere difficile. Con gli utenti autorizzati che effettuano l’accesso a data source multiple, inclusi database, file system, ambienti mainframe e ambienti cloud, il monitoraggio e il salvataggio dei dati da tutte queste interazioni potrebbero apparire troppo complessi. La sfida consiste nel monitorare, acquisire, filtrare, elaborare e rispondere in modo efficiente a un elevato volume di attività di dati. Senza un piano adeguato, la tua organizzazione potrebbe ritrovarsi con un numero superiore di informazioni sull’attività rispetto a quello che può effettivamente elaborare e, di riflesso, sminuire l’importanza del monitoraggio dell’attività dei dati.

Soluzione

Sviluppare una strategia di protezione e rilevamento dei dati completa

A tal fine, quando si intraprende un percorso per la sicurezza dei dati, è necessario valutare e adattare gli sforzi di monitoraggio in modo da affrontare i rischi e i requisiti. Questa attività coinvolge spesso l'adozione di un approccio a fasi che consenta lo sviluppo e la scalabilità delle best practice in tutta l'azienda. Inoltre, è fondamentale confrontarsi con gli stakeholder IT e di business chiave all'inizio del processo, per comprendere gli obiettivi di business a breve e a lungo termine.

Tali confronti consentono anche di acquisire la tecnologia che sarà necessaria per supportare le iniziative chiave. Ad esempio, se l'azienda prevede di aprire dei nuovi uffici in una nuova ubicazione usando una combinazione tra repository di dati in cloud e on-premise, la strategia di sicurezza dei dati dovrebbe valutare in che modo il piano influirà sulla posizione che ha l'organizzazione in termini di conformità e sicurezza dei dati. Se, ad esempio, i dati aziendali saranno soggetti a nuovi requisiti di conformità e di sicurezza dei dati, come il GDPR, il CCPA (California Consumer Privacy Act), l'LPGD (Brazil's Lei Geral de Proteção de Dados) e così via.

Sarebbe opportuno anche assegnare delle priorità e concentrarsi su una o due origini che presumibilmente hanno i dati più sensibili. Accertarsi che le politiche di sicurezza dei dati siano chiare e dettagliate per tali source, prima di estende le pratiche al resto dell'infrastruttura.

Il costo totale medio di una violazione dei dati è stata

il 95% più alta

nelle organizzazioni prive di automazione della sicurezza nel 2019. [1]

5.16 milioni di dollari **senza automazione.** [1]

2.65 milioni di dollari **con piena automazione.** [1]

Sarebbe opportuno anche valutare una soluzione automatizzata di monitoraggio dell'attività dei file o dei dati, con analytics completa, che si concentri sui rischi chiave e sui comportamenti insoliti degli utenti con privilegi. Sebbene sia fondamentale ricevere degli avvisi automatizzati quando una soluzione di monitoraggio dell'attività dei file o dei dati rileva un comportamento anomalo, è necessario anche saper intraprendere delle azioni non appena vengono rilevate anomalie o deviazioni dalle politiche di accesso ai dati. Le azioni di protezione dovrebbero includere il blocco o il mascheramento dei dati dinamici.

Nello sviluppare i piani di protezione e monitoraggio dell'attività dei dati, spesso è utile valutare le seguenti domande:

- Quali sono le mie due data source sensibili principali?
- Quali sono le successive cinque, fino a dieci, data source a cui devo assegnare la priorità, in base al volume di dati sensibili?
- Alcuni endpoint o asset cloud sono associati a dati con rischio elevato?
- I dati sensibili vengono liberamente spostati da/a ambienti cloud, ibridi e on-premise?
- A quali utenti dovrei garantire accesso a data source e a quali condizioni?
- Quali account con privilegi o utenti ad alto rischio devono essere disattivati o richiedono un'analisi più attenta?
- La mia soluzione di sicurezza dei dati supporta il monitoraggio delle attività in tempo reale e le funzionalità di protezione dei dati automatizzate?
- Il monitoraggio in tempo reale esistente, tiene traccia dei dati contenuti nei file che risiedono nei data source come i database SQL (Structured Query Language), le distribuzioni Hadoop, le piattaforme NoSQL (Not only SQL) e così via?
- La mia soluzione di monitoraggio tiene conto degli archivi dati che riguardano tutti gli ambienti ibridi multicloud e mi consente di generare report personalizzati che vanno alle giuste persone al momento giusto?
- Dispongo delle funzionalità di monitoraggio con filtro e di analytics dei rischi necessarie per assegnare in modo efficace le priorità ai rischi, alle vulnerabilità e agli sforzi di remediation?

Quanto più si riescono a monitorare con precisione i requisiti di protezione e le priorità, tanto più efficace sarà la soluzione nel consentire di applicare le risorse di detection e risposta disponibili.

Cos’altro aggiungere

Come è possibile evitare di commettere questi passi falsi comuni riguardanti la sicurezza dei dati, soprattutto a fronte della diffusione di ambienti ibridi multicloud in un numero crescente di aziende? Si comincia riconoscendo il problema e preparando l’organizzazione ad adottare un approccio proattivo e olistico nei confronti della protezione dei dati, indipendentemente da dove essi risiedono.

Se il business presenta un ambiente IT complesso e ibrido, non è possibile adottare un approccio isolato per affrontare la sicurezza dei dati. È necessario aggiungere strategie di protezione dei dati che riguardino l’intera infrastruttura di dati e che supportino tutti i tipi di dati.

Tra gli interventi immediati che è possibile intraprendere per proteggere i dati più importanti dell’organizzazione troviamo:

- Creazione di una strategia di sicurezza dei dati che supporti gli obiettivi tecnologici e di business a breve e a lungo termine dell’organizzazione
- Implementazione della strategia con strumenti, processi e persone adeguati
- Pianificazione delle risorse per garantire che il programma di conformità e sicurezza dei dati si adatti effettivamente alle esigenze dell’organizzazione man mano che vengono adottate tecnologie moderne

La piattaforma di protezione dei dati IBM Security Guardium è progettata per aiutare le organizzazioni ad avere un approccio più intelligente e adattivo nei confronti della protezione dei dati critici, ovunque essi si trovino. Scopri perché può essere la soluzione adatta alla tua organizzazione.

Per ulteriori informazioni, visita il sito ibm.com/guardium.

>4 settimane

La maggior parte delle organizzazioni riconosce il valore offerto da Guardium in meno di un mese. [7]

Perché scegliere IBM Security?

IBM Security offre una delle più avanzate ed integrate serie di prodotti e servizi per la sicurezza aziendale. Il portfolio, supportato da esperti di ricerca e sviluppo IBM X-Force® noti in tutto il mondo, fornisce security intelligence per aiutare le organizzazioni a proteggere a 360 gradi il proprio personale, le infrastrutture, i dati e le applicazioni. Offre soluzioni per la gestione delle identità e degli accessi, sicurezza del database, application development, gestione dei rischi, gestione dell'endpoint, network security e tanto altro. Queste soluzioni consentono alle organizzazioni di gestire in modo efficace i rischi e di implementare la sicurezza integrata per il mobile, cloud, social media ed altre architetture di business aziendale.

IBM rappresenta una delle più vaste organizzazioni di ricerca, sviluppo e delivery di soluzioni per la sicurezza al mondo e monitora più di

60 miliardi

di eventi di sicurezza al giorno in più di 130 paesi.

IBM detiene oltre 3700 brevetti sulla sicurezza

IBM Italia S.p.A.
Circonvallazione Idroscalo
20090 Segrate (Milano)
Italia

La home page di IBM Italia si trova all'indirizzo:
ibm.com

Questo documento è aggiornato alla data iniziale della pubblicazione e può essere modificato da IBM senza necessità di preavviso. Non tutte le offerte sono disponibili in ogni paese in cui opera IBM.

1 "Cost of a Data Rreach report 2019." *IBM Security.* databreachcalculator.mybluemix.net/executive-summary

2 "Healthcare Data Breach Statistics." *HIPAA Journal. www.hipaajournal.com/healthcare-data-breach-statistics*

3 Jon Oltsik. "The Life and Times of Cybersecurity Professionals 2018." *Enterprise Strategy Group and Information Systems Security Association International*, aprile 2019. www.esg-global.com/hubfs/pdf/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Apr-2019.pdf

4 NewVantage Report, "Big Data and AI Executive Survey 2019 Executive Summary of Findings." *NewVantage Partners,* 2019. newvantage.com/wp-content/uploads/2018/12/Big-Data-Executive-Survey-2019-Findings-Updated-010219-1.pdf

5 Sue Poremba. "Why Privileged Account Management Is Key to Preventing Insider Threats." *Security Intelligence,* 20 giugno, 2018. securityintelligence.com/why-privileged-access-management-is-key-to-preventing-insider-threats

6 "Cost of Insider Threats: Global Report 2020." *Ponemon Institute*, 2020. www.ibm.com/security/digital-assets/services/cost-of-insider-threats/#

7 "Ponemon Report: Client Insights on Data Protection with Guardium." *Ponemon Institute,* Agosto 2019. www.ibm.com/account/reg/us-en/signup?formid=urx-40683

60031860-ITIT-00