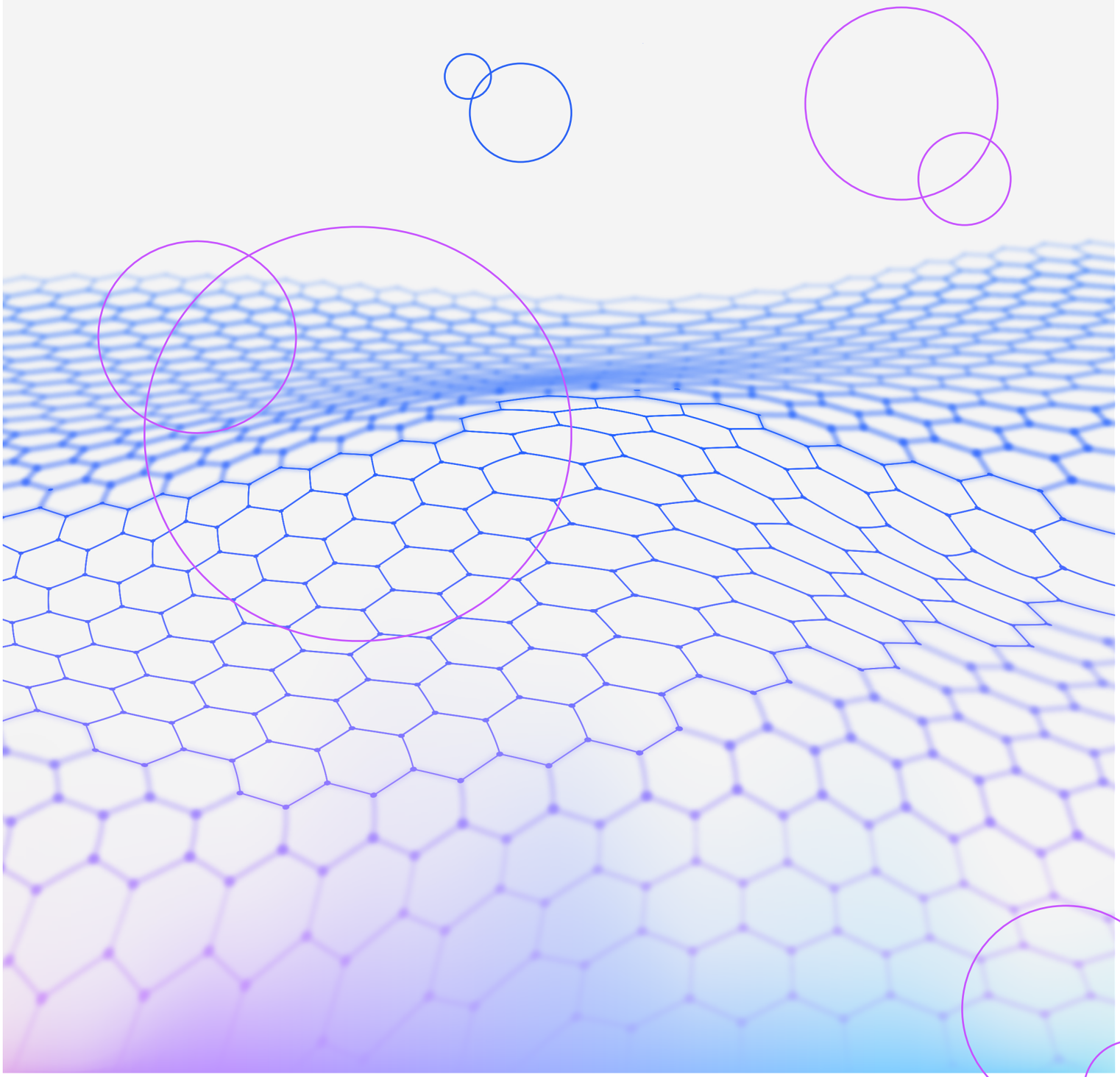
IBM Cyber Academy

Creare insieme le competenze
per un paese digitale sicuro



Indice

La formazione è la chiave per aprire le porte del progresso

Negli ultimi anni governi, imprese e cittadini si sono trovati a dover fronteggiare eventi dirompenti e imprevisti, di varia natura – economici, geopolitici, fisici - che hanno messo a dura prova la loro capacità di rimanere resilienti. Dalle situazioni sfidanti hanno sicuramente imparato a non affidarsi a decisioni basate sui cambiamenti di scenario dell'ultimo minuto e ad avvalersi delle evidenze per immaginare i prossimi "shock", per anticiparli e affrontarli con strategie proattive pensate da ora.

Cosa serve per operare in un contesto di questo tipo, in cui l'intensità e la velocità degli eventi richiedono forza e rapidità per poterli affrontare al meglio? E come, in un'economia sempre più digitale e interconnessa, sviluppare e attuare strategie che promuovano la resilienza cyber, considerando che viviamo in un mondo in cui le piattaforme tecnologiche sostengono ogni secondo dell'operatività delle imprese e della nostra vita quotidiana, per comunicare, lavorare, collaborare, acquistare?

Le nostre ricerche, i dati, le conversazioni quotidiane con interlocutori del mondo politico, economico, accademico e imprenditoriale ci portano a identificare, semplificando, due fattori determinanti: utilizzare le migliori e più affidabili tecnologie disponibili e, soprattutto, essere capaci di rispondere alle minacce con un capitale umano adeguatamente formato e dotato di un protocollo d'azione ben definito e rodato.

Per questo motivo, uno degli impegni maggiori di IBM Italia nel 2024 è quello di supportare la formazione in tema di cybersecurity, AI generativa e quantum computing anche attraverso partnership pubblico-private che promuovano la resilienza delle imprese e dell'intero Sistema Paese, ma anche competitività e crescita.

Con questo ambizioso obiettivo, apriamo a Roma l'IBM Cyber Academy, un luogo in cui assieme ai migliori esperti IBM di cybersecurity, AI e della Ricerca sarà possibile conoscere le tecnologie di frontiera, costruire le competenze e sviluppare i talenti per rispondere più rapidamente agli attacchi, allineare le priorità cyber tra settore pubblico e privato e formare leader capaci di rendere le proprie imprese resilienti per affrontare le sfide future.

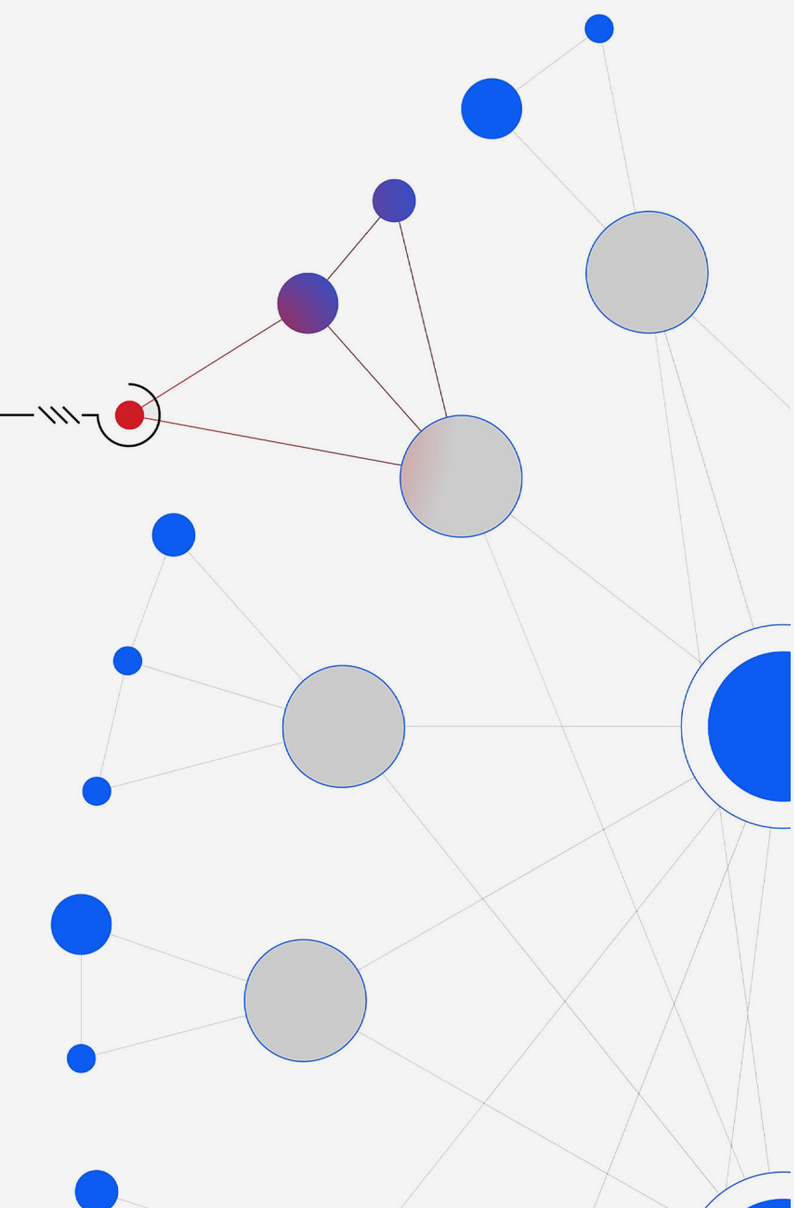
Stefano Rebattoni,
Presidente e AD di IBM Italia

In Europa l’identità digitale è sotto attacco

IBM X-Force Treath Intelligence Index: si allungano i tempi di ripristino dalle violazioni

La sicurezza informatica è diventata una priorità per le imprese di ogni settore. Il fenomeno cybercrime non solo non rallenta, ma accelera, si acuisce ulteriormente e si allungano i tempi di ripristino dalle violazioni subite, come dimostrato dall’impatto medio di ogni incidente, sempre più alto. Secondo il rapporto CLUSIT di ottobre 2023 l’Italia rimane nel mirino degli hacker.

La conferma di questi trend arriva dal report IBM X-Force Threat Intelligence Index 2024 che evidenzia l’emergere di una crisi globale in materia di identità digitale dovuta al fatto



L’Europa è stata la regione più bersagliata nel 2023 con il 32% degli incidenti globali, passando dal secondo posto del 2022 al primo

che è raddoppiato lo sfruttamento delle identità digitali degli utenti da parte dei criminali informatici con l’obiettivo di danneggiare le imprese di tutto il mondo. Secondo IBM X-Force i criminali informatici hanno individuato l’opportunità di accedere alle reti aziendali, utilizzando account validi, anziché effettuare una compromissione.

~74%

degli attacchi osservati ha riguardato infrastrutture critiche

Tra gli aspetti più rilevanti emersi nel report si nota che quasi un attacco su tre osservato a livello mondiale ha preso di mira l'Europa (32%), un numero mai raggiunto prima d'ora in una singola area analizzata

I paesi più colpiti:

27%
Regno Unito
15%
Germania
14%
Danimarca
11%
Portogallo
8%
Italia

In tutta Europa, X-Force ha osservato un aumento del 66% degli attacchi causati dall'uso di account validi rispetto all'anno precedente: i principali punti deboli registrati sono le identità digitali e le e-mail, entrambi sfruttati nel 30% delle violazioni di account validi e phishing.

E questa crisi legata alle identità a livello globale è destinata a peggiorare : "l'ingresso facile" per gli aggressori è più complesso da rilevare e comporta una risposta costosa da parte delle aziende.

Secondo X-Force, gli incidenti più gravi causati da criminali informatici che utilizzano account validi richiedono ai responsabili della sicurezza misure di risposta più complesse del 200% rispetto all'incidente medio, oltre alla necessità di distinguere tra attività di utenti legittimi e malintenzionati sulla rete.

Inoltre, viene evidenziato che l'AI generativa sarà un'area di attenzione che dovrà essere protetta nel prossimo futuro.

Le aziende devono acquisire la consapevolezza che l'infrastruttura sottostante esistente rappresenta una via di accesso ai loro modelli di AI, che non richiede tattiche innovative da parte dei cybercriminali per essere presa come bersaglio, evidenziando la necessità di un approccio olistico alla sicurezza nell'era dell'AI generativa.

IBM X-Force ha elaborato anche alcune raccomandazioni per le aziende. Innanzitutto, le organizzazioni dovrebbero prendere in considerazione l'integrazione di soluzioni per ridurre i danni che un incidente in materia di sicurezza dei dati potrebbe potenzialmente causare, riducendo il raggio d'azione dello stesso, ovvero l'impatto potenziale dell'evento in seguito alla compromissione di particolari utenti, dispositivi o dati. Altre azioni importanti riguardano la necessità di eseguire stress-test degli ambienti e preparare un piano regolarmente aggiornato e che includa una risposta inter-organizzativa. Oltre ad adottare l'AI in modo sicuro, preservando i dati di addestramento sottostanti all'intelligenza artificiale, proteggendo i modelli, il loro utilizzo e la loro logica. È fondamentale salvaguardare anche l'infrastruttura più ampia che interagisce con i modelli di AI.

L'Europa ha subito la percentuale più elevata di incidenti:

43%
settore energia
37%
settore finanziario e assicurativo

IBM XForce 2024

Vai al link --->

IBM Cost of a Data Breach Report: AI e automazione per identificare e contenere gli attacchi cyber

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 della 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 cybercriminali stessi a dichiararli e a chiedere un riscatto.

Ogni minuto è prezioso

Secondo il report, le organizzazioni intervistate che hanno adottato 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 veloci nel 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.

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, nel 2023, per la prima volta, il report 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 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. Il report ha evidenziato che il 33% delle violazioni è stato scoperto dai responsabili della sicurezza, il 40% da una terza parte neutrale, come ad esempio le forze dell'ordine e il 27% viene pubblicato direttamente dagli aggressori durante l'attacco.

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.

> I responsabili della sicurezza devono focalizzarsi sulle aree di maggior attenzione degli hacker in modo da prevenire le loro azioni e fermarli prima che raggiungano gli obiettivi. Gli investimenti impiegati per rilevare le minacce e per definire risposte rapide, grazie all'AI e all'automazione, sono fondamentali per mitigare gli attacchi.

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:

3,55 Milioni di euro

Il costo medio complessivo delle violazioni di dati

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).

235 Giorni

Necessari per identificare e contenere una minaccia informatica

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 vettori più costosi

Sono 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).

1,56 Milioni di euro

Di costi di violazione risparmiati

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, esistono ampi spazi di miglioramento per ridurre ulteriormente costi e tempi di rilevazione e gestione delle violazioni.

Violazione dei dati in tutti gli ambienti IT

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).

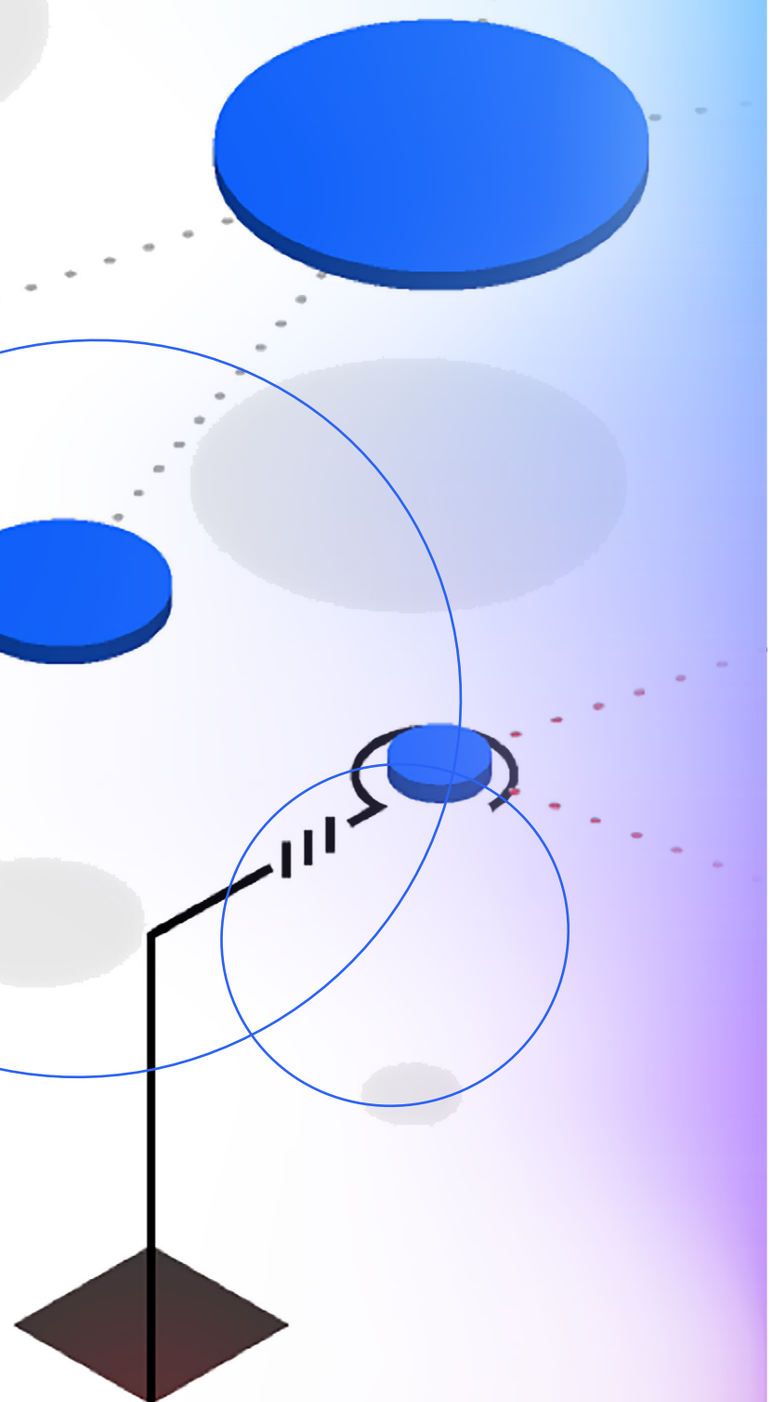
Dati analizzati nello studio riguardanti i principali vettori di attacco sono:

15%
Social engineering
un costo medio di 3,49 milioni di euro

14%
Phishing
un costo medio di 3,63 milioni di euro

12%
Credenziali rubate o compromesse
un costo medio di 3,40 milioni di euro

Preparare i governi agli shock futuri



Un piano d’azione per sviluppare la cyber resilience in un mondo di incertezza

L’IBM Institute for Business Value (IBV) e l’IBM Center for The Business of Government, in collaborazione con la National Academy of Public Administration e il Centro Studi Americani, propongono misure concrete per aiutare i governi ad affrontare gli shock informatici attuali e futuri.

Negli scorsi anni i governi hanno avuto modo e tempo per imparare a gestire situazioni di grande crisi, come quella causata dalla pandemia, e le relative conseguenze. Hanno sicuramente imparato a non affidarsi a decisioni basate sui cambiamenti di scenario dell’ultimo minuto e oggi sono in grado di guardare più consapevolmente al futuro, immaginando quali potrebbero essere i prossimi “shock”, per anticiparli ed essere pronti ad affrontarli. Nello scenario attuale è sempre più probabile che eventi con conseguenze impattanti e negative, gli “shock” appunto, si verifichino sempre più spesso. Possono manifestarsi più o meno velocemente, a livello regionale o globale, variando per portata e natura, ma sicuramente richiedono strategie proattive e tempestive.

I governi per essere resilienti e poter perseguire i propri obiettivi anche nell’incertezza potrebbero trarre significativi vantaggi dallo sviluppo di insight. Per farsi trovare pronti, sarà necessario dare priorità alla leadership e agli investimenti, oltre a definire e orchestrare strategie, con capacità fondamentali per essere meglio preparati alle sfide che potranno presentarsi in futuro nei più diversi ambiti.

I governi hanno quindi un ruolo fondamentale nel favorire la collaborazione tra i principali stakeholder per identificare i rischi informatici, accrescere la capacità di risposta e di rimanere resilienti di fronte a questi rischi. Le istituzioni oggi hanno anche un importante ruolo di leadership per guidare il cambiamento verso un futuro più resiliente nel contesto degli obiettivi dei loro programmi di governo.

Dallo studio emergono alcuni passi fondamentali per supportare i governi a livello globale a sviluppare e attuare strategie di cybersecurity che promuovano la resilienza attraverso una partnership tra pubblico e privato.

I principali sono:

Aumentare i talenti specializzati in cybersecurity

Per affrontare il divario crescente tra domanda e offerta di professionisti di cybersecurity, i partecipanti alle roundtable hanno indicato, in cima alla lista delle priorità da perseguire, l'importanza di aumentare i talenti competenti in sicurezza informatica. Come sottolineato da diversi partecipanti, la carenza di competenze informatiche riguarda un'ampia gamma di discipline, tra cui l'analisi, la progettazione e lo sviluppo di software, la threat intelligence, il penetration testing, l'auditing e la consulenza, la digital forensic e la crittografia.

Migliorare la collaborazione per rispondere più rapidamente agli attacchi

Nonostante i recenti progressi nel migliorare il coordinamento tra pubblico e privato, l'aumento della cooperazione tra i criminali cyber continua a essere una minaccia costante.
Infatti, gli aggressori cyber legati a governi ostili e associazioni criminali, stanno sviluppando infrastrutture e servizi da utilizzare per scopi fraudolenti. Inoltre, stanno anche adottando rapidamente nuove tecnologie per penetrare nelle reti e vanificare gli sforzi per contenere le minacce, che spesso dipendono dal coordinamento tra entità con standard, obiettivi e priorità diverse.

Allineare le priorità di cybersecurity tra settore pubblico e privato

I partecipanti hanno evidenziato numerose idee per la cooperazione tra industria e governo al fine di migliorare la sicurezza informatica su vasta scala, identificando le sfide comuni e condividendo le migliori pratiche. In questo senso, si dovrebbe promuovere l'assunzione di professionisti cyber provenienti da diversi contesti. È inoltre importante concentrarsi maggiormente sull'innovazione in sicurezza, vedendola come un vantaggio competitivo, e sostenere approcci zero trust, basati sul presupposto che la sicurezza informatica sia sempre a rischio di minacce, interne ed esterne.

Inoltre, è importante investire sulla consapevolezza delle problematiche informatiche all'interno delle istituzioni e della pubblica amministrazione. È quindi necessario migliorare gli standard, le metriche e i dati relativi alla cybersecurity per rafforzare la comprensione delle minacce e promuovere gli investimenti pubblici e privati volti a contrastarle e contenerle.

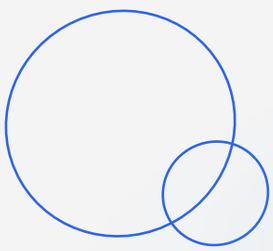
Formare leader resilienti ai rischi cyber, in grado di affrontare il futuro

La dipendenza globale dall'open technology rappresenta tutto quello che fa progredire le comunità, in particolare la connettività sociale, le comunicazioni e la collaborazione. Questi fattori sono determinanti per il benessere nazionale e internazionale, e allo stesso tempo, la sua dipendenza dalle tecnologie lo rende bersaglio privilegiato dei criminali informatici. Le attuali misure di sicurezza funzionano in parte, ma in troppi casi sono insufficienti.

Studiare modi per sostenere le istituzioni democratiche contro gli attaccanti cyber

Gli attacchi cyber sono progettati per influenzare il sostegno e il coinvolgimento dei cittadini nei processi elettorali, legislativi o normativi, cercando di manipolare l'opinione pubblica o di minare le norme di comportamento democratico. Sebbene l'obiettivo primario di queste campagne, palesi od occulte, sia quello di seminare confusione sociale nel breve termine, i partecipanti hanno riconosciuto che, a lungo termine, questi sforzi potrebbero riuscire a influenzare stabilmente l'opinione pubblica.

A causa delle complessità rappresentate da queste sfide informatiche soprattutto rispetto alle forme di governo più rappresentative, i partecipanti non concordavano univocamente sui modi più efficaci per difendersi da questa crescente minaccia e hanno chiesto di approfondire la ricerca sulle misure in grado di contrastare le minacce informatiche alla democrazia.




Nel mondo delle
minacce cyber, non puoi
Prevedere tutto, ma puoi
Prepararti.

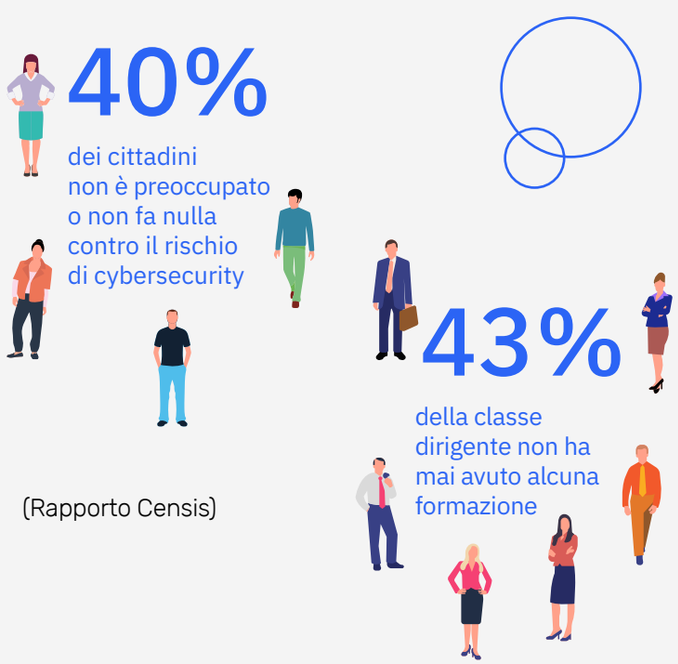
IBM Cyber Academy: un luogo di innovazione e formazione a Roma

La crescente complessità delle minacce digitali richiede una costante attenzione e preparazione da parte delle organizzazioni, che devono essere pronte a fronteggiare attacchi sempre più sofisticati. Nel contempo, le competenze in questo ambito sono sempre più specializzate e difficili da trovare. In questo contesto, IBM propone la nuova Cyber Academy a Roma, un centro dedicato all'informazione, alla consulenza personalizzata e alla formazione per le aziende italiane pubbliche e private.

Lo scopo di questa iniziativa è quello di mettere a disposizione un luogo dove: istituzioni, amministrazioni pubbliche, aziende private di tutte le dimensioni, studenti di scuole secondarie superiori e università possano:

- acquisire o aumentare la propria consapevolezza
- formarsi e formare le proprie organizzazioni
- costruire quelle competenze necessarie per un paese digitale più sicuro

Considerato che



(Rapporto Censis)

Come? Attraverso simulazioni e formazione: Cyber Theatre, Expert Labs, Garage, Design Thinking e altre metodologie guidate dagli esperti IBM di Cybersecurity, di Data & AI e della Ricerca. Tra le iniziative anche sessioni di intelligenza artificiale, di governance dell'AI, della gestione dei dati e sulle ultime tecnologie di crittografia.

2200

le persone che possono essere formate in un anno

La struttura potrà, inoltre, facilitare la collaborazione tra diverse aziende del settore, secondo le necessità e i requisiti del mercato.

Il centro può contare sulle competenze del Laboratorio di Ricerca IBM di Zurigo e della Sistemi Informativi Srl, una società del gruppo IBM, che ha investito in competenze digitali a Rieti in collaborazione con la Regione Lazio.

Cyber Theatre: il circuito di addestramento per rispondere alle emergenze

Nel cuore della Cyber Academy c'è il Cyber Theatre, un laboratorio interattivo, capace di far vivere in modo immersivo ed emozionale l'esperienza di un'intromissione malevola, andando a ricreare un attacco informatico reale per testare le capacità di risposta in situazioni complesse ed impreviste. Una vera e propria "palestra" di cybersecurity, pensata come un asset per la formazione nel campo della risposta alle emergenze, che consentirà di acquisire o potenziare la propria consapevolezza in tema di sicurezza.

Attraverso le simulazioni e le esercitazioni sarà possibile immergersi in scenari che permettono di analizzare le tematiche di cybersecurity da più punti di vista: dalla comprensione del rischio alla capacità di leadership necessaria per affrontare le situazioni che potrebbero presentarsi, dalla gestione della comunicazione al dettaglio delle soluzioni tecnologiche, fino al test dei processi, delle tecnologie e delle competenze delle persone coinvolte. Tutto ciò approfondendo le metodologie di attacco, ma anche gli impatti e le potenzialità delle nuove tecnologie quali il Quantum Homomorphic Encryption e la Gen AI applicata alla gestione dei rischi di sicurezza.

Gli scenari del Cyber Theatre includono esercitazioni che guardano con una particolare attenzione alle dinamiche regolamentari italiane e alle necessità che enti governativi e aziende di tutte le dimensioni si trovano ad affrontare nella gestione degli incidenti, nel reporting e nel percorso verso la trasformazione digitale e il ri-disegno dei loro processi secondo i principi zero trust e threat modeling.

Si tratta di un training che permette alla leadership delle imprese di provare in maniera realistica - mettendo i partecipanti sotto stress per emulare il più fedelmente possibile una

12

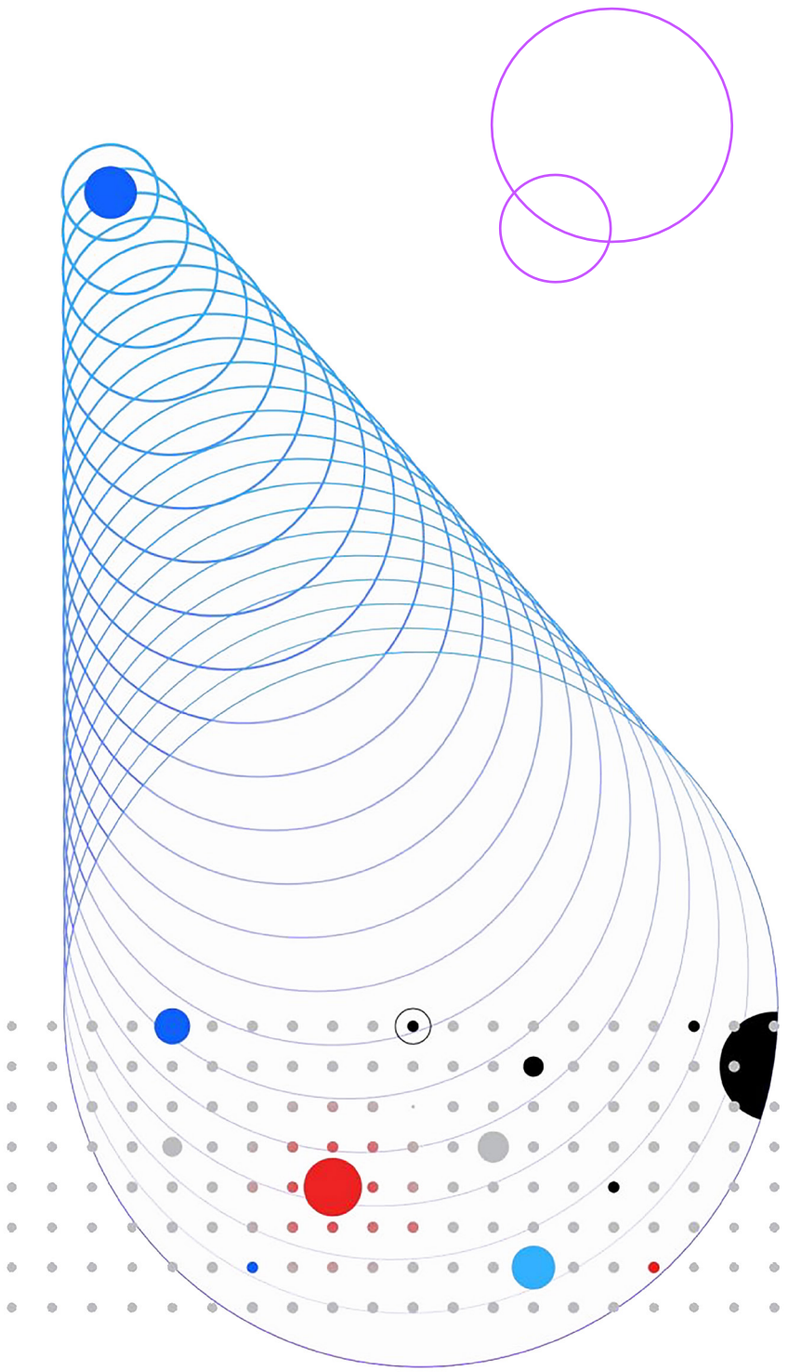
postazioni dove i CxO potranno esercitarsi per battere un nemico visibile solo per i suoi effetti: l'interruzione o il sabotaggio di sistemi critici per il normale funzionamento dell'azienda

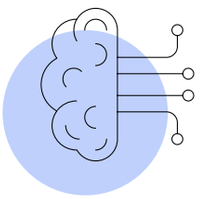
situazione reale - in che modo un attacco possa influenzare tutti coloro che operano in seno all'azienda colpita, e testare così il proprio livello di preparazione e i possibili impatti su clienti e processi interni che una crisi cibernetica potrebbe aprire, prima che questa possa creare danni all'organizzazione.

Il Cyber Theatre permetterà anche di vivere un'esperienza immersiva e interattiva tramite l'integrazione delle tecnologie di un Security Operations Center con le modalità di simulazione sopracitate, permettendo quindi sia a team tecnici che a team misti (tecnici e business) di lavorare direttamente sui prodotti e ampliare la propria conoscenza e le proprie competenze specifiche sulle tecnologie di cyber security. Questo con l'obiettivo di supportare attivamente l'impegno delle organizzazioni pubbliche e private verso l'up-skilling e il re-skilling delle risorse IT e di security.

Gli scenari infatti daranno la possibilità di iniziare percorsi di formazione che potranno poi essere riconosciuti ai fini dell'accrescimento delle competenze, dando quindi ulteriore strumento agli enti pubblici e privati per migliorare le competenze di sicurezza.

Queste esperienze mirano ad ampliare la preparazione nel campo della sicurezza informatica e a costruire la nuova Cybersecurity Culture tenendo sempre a mente che nel mondo, continuamente in evoluzione, della cybersecurity non si può prevedere tutto, ma ci si può preparare per poter affrontare le situazioni più critiche.





“Security for AI” e “AI for Security”

Il dibattito pubblico sull’utilità dell’intelligenza artificiale come volano del progresso e della trasformazione di aziende e amministrazioni pubbliche è ora più che mai attuale. L’AI generativa e in particolare i Foundation Model, rappresentano un cambiamento di passo notevole sulle capacità offerte da questa tecnologia e sulla sostenibilità economica dei progetti di AI.

I Foundation Model di fatto cambiano l’equazione economica dei progetti di AI riducendo i costi di aziende e amministrazioni per l’allenamento dei modelli su task specifici. Nascendo, di fatto, pre addestrati su una quantità innumerevole di informazioni, tali modelli sono facilmente adattabili (fine-tuning) a esigenze specifiche di aziende con costi marginali. Inoltre, le potenzialità della generazione di contenuti trova spazio in notevoli casi d’uso: dal marketing creativo, alla produzione di codice software, al customer-care, solo per citare alcuni.

Queste potenzialità dell’AI aprono comunque a nuove preoccupazioni per la sicurezza di tutte le organizzazioni. I modelli di AI di fatto aumentano la superfice di attacco delle aziende e quindi diventano un asset da proteggere in un cyberspace costantemente sotto attacco. Questo è testimoniato da quanto emerge da un’indagine recentemente condotta dall’Institute of Business Value di IBM su 200 dirigenti apicali, che ha rilevato che il 64% sente l’urgenza di dover accelerare l’adozione dell’AI generativa, ma l’84% considera i rischi legati alla cybersecurity come il principale ostacolo a questo tipo di progresso, identificando nella sicurezza la priorità numero uno per i casi d’uso dell’AI generativa. L’AI va protetta perché violabile con tecniche nuove e sempre più sofisticate, inoltre, si prevede che gli hacker adotteranno l’AI generativa per perpetrare i loro attacchi con la stessa velocità, scalabilità e capacità di sofisticazione che essa offre alle aziende.

L’introduzione di AI generativa richiede quindi nuovi approcci per proteggere i modelli di AI. E su questa problematica IBM si impegna ad offrire un’AI non solo pronta all’uso ed economicamente vantaggiosa, ma anche sicura by design e protetta da possibili attacchi futuri. L’ Adversial Robustness Toolbox è lo strumento sviluppato da IBM con un approccio open innovation che protegge i modelli dai principali attacchi quali avvelenamento dei dati di traning, l’estrazione (furto del modello attraverso query) o l’elusione (modifica del comportamento del modello cambiando l’input). In particolare IBM ha recentemente presentato l’IBM Framework for Securing AI, che aiuta le organizzazioni a definire meglio le priorità degli approcci difensivi più importanti per proteggere le loro iniziative di AI generativa dai possibili attacchi. Più le aziende comprendono quali tipi di aggressione contro l’AI sono possibili, più possono migliorare la loro preparazione costruendo strategie di difesa efficaci.

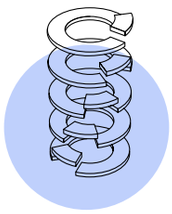
L’AI sicura diventa quindi uno strumento per lo sviluppo delle aziende e per IBM anche uno strumento per migliorare i propri prodotti di sicurezza. Infatti, con l’AI è possibile gestire attività ripetitive come per esempio la classificazione della severità degli incidenti in base a fattori di rischio, rendendo il team di analisti di sicurezza più produttivo nell’affrontare le notevoli sfide della gestione sicura della IT.

L’AI generativa integrata nei SOAR consentirà la creazione di piani di ripristino degli incidenti aumentando la resilienza delle aziende agli attacchi informatici. Non solo. Sebbene i primi casi d’uso dell’AI generativa nell’ambito della sicurezza si concentrino sul front-end, basandosi su modelli comportamentali, inizia ad essere utilizzata anche per monitorare le anomalie nell’accesso ai dati o l’utilizzo anomalo di credenziali, risparmiando tempo prezioso nel rilevare e risolvere i problemi. Le possibilità di attuare modelli di sicurezza predittiva su larga scala stanno diventando più tangibili, portandoci dalla prevenzione delle minacce alla previsione.

Proteggere i modelli di intelligenza artificiale e sfruttare l’intelligenza artificiale per una sicurezza più efficiente ed efficace sono le due traiettorie di sviluppo delle soluzioni di IBM Security.

Cybersecurity in the era of generative AI

Vai al link --->



Quantum Safe

L'informatica quantistica ha il potenziale per creare immensi vantaggi commerciali e per tutta la società: entro la fine del decennio, le soluzioni di calcolo quantistico potrebbero avere un impatto sulle strategie informatiche di tutti i settori.

Il quantum computing modificherà profondamente il modo in cui pensiamo all'informatica e anche il modo in cui proteggiamo la nostra economia digitale attraverso la crittografia.

Lo sviluppo di capacità di crittografia "quantum-safe" è fondamentale per mantenere la sicurezza e l'integrità dei dati per le applicazioni critiche. L'era dei quanti si svilupperà nel tempo, ma i leader delle aziende, della tecnologia e della sicurezza hanno l'urgenza di sviluppare subito una strategia e una tabella di marcia per la sicurezza quantistica. Infatti, l'informatica quantistica rappresenta un grande rischio per i classici protocolli di crittografia informatica che rendono oggi possibili tutte le transazioni digitali.

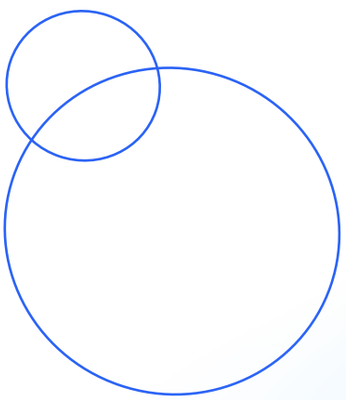
I computer quantistici stanno diventando tecnologicamente così avanzati che presto potrebbero decifrare gli attuali protocolli di sicurezza più utilizzati al mondo (come quelli RSA, basati sulla fattorizzazione di numeri complessi ed enormi). Di fatto, qualsiasi comunicazione classicamente crittografata che potrebbe essere intercettata è a rischio, potenzialmente già esposta all'esfiltrazione, con l'intenzione di raccogliere quei dati una volta che le soluzioni di decrittografia quantistica saranno praticabili. Queste tattiche sono definite attacchi "harvest now, decrypt later".

Anche se alcuni dati sono irrilevanti o perdono rapidamente il loro valore per gli hacker, i dati relativi alla sicurezza nazionale, alle infrastrutture, alle cartelle cliniche, al capitale intellettuale e altro ancora potrebbero mantenere o aumentare il loro valore nel tempo. È importante che i dati delle imprese, e dei loro clienti, rimangano riservati per sempre.

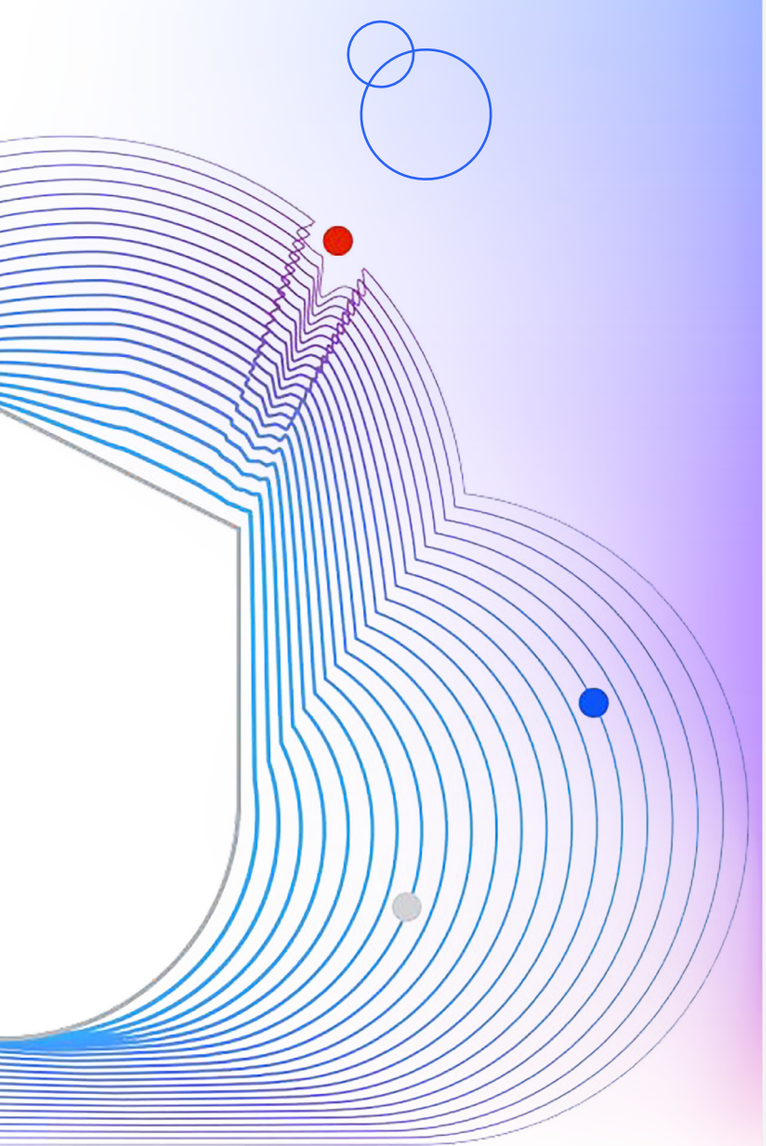
La minaccia che il quantum computing rappresenta per la crittografia è così grave che nel 2022, il governo degli Stati Uniti ha pubblicato nuovi requisiti e linee guida che invitano le agenzie federali ad avviare la transizione verso la sicurezza quantistica.

Il National Institute of Standards and Technology (NIST) ha selezionato per la standardizzazione quattro algoritmi quantum-resistant, 3 dei quali sono stati sviluppati da IBM Research insieme a partner accademici e industriali.

Alcuni settori hanno già iniziato a pianificare il passaggio a protocolli quantum-safe. E anche singole organizzazioni si stanno muovendo in questa direzione. Il tema potrà essere affrontato all'interno dell'IBM Cyber Academy, per accrescere la consapevolezza su questa tipologia di rischio e condividere le soluzioni e le competenze che IBM può mettere in campo a supporto dell'evoluzione verso il quantum-safe.



Soluzioni e prodotti



IBM QRadar Security Suite

IBM Security QRadar Suite include tutte le principali tecnologie di rilevamento, investigazione e risposta delle minacce. È dotata di un'unica interfaccia utente, modernizzata, integrata con l'intelligenza artificiale e l'automazione avanzata, progettate per offrire maggiore velocità, efficienza e precisione nell'utilizzo dei principali tool di analisi.

La suite include strumenti EDR/XDR, SIEM, SOAR e una nuova funzionalità sviluppata nativamente in cloud di gestione dei log, il tutto basato su un'interfaccia utente comune, insight condivisi e workflow connessi, con i seguenti elementi di progettazione principali:

- Esperienza di analisi unificata

  frutto della collaborazione con centinaia di utenti, la suite integra un'interfaccia intuitiva e modernizzata per tutti i prodotti per aumentare notevolmente la velocità e l'efficienza dell'intera attività di analisi. Inoltre, integra funzionalità di AI e di automazione che hanno dimostrato di velocizzare l'analisi e il triage degli avvisi del 55% in media nel primo anno, migliorando cosi la velocità e l'accuratezza delle operazioni SOC.

- Sviluppata su tecnologia aperta, integrazioni precostruite

  Qradar Suite è una piattaforma basata su standard che pemette quindi di accorpare sia tecnologie IBM che di terze parti grazie ad oltre 900 integrazioni che consentono di connettere tool e dati che provengono da diversi strumenti di sicurezza.

La IBM QRadar Suite include i seguenti moduli:

QRadar Log Insight

una nuova soluzione cloud nativa per le soluzioni di gestione dei log e osservabilità della sicurezza che fornisce la raccolta semplificata dei dati, la ricerca in meno di un secondo e l'analisi rapida.

QRadar EDR e XDR

consente alle aziende di proteggere i propri endpoint da minacce precedentemente sconosciute, minacce zero-day, utilizzando l'automazione e centinaia di modelli comportamentali e di apprendimento automatico per rilevare le anomalie nel comportamento e rispondere agli attacchi in tempo quasi reale. Sfrutta un approccio unico che monitora i sistemi operativi dall'esterno, evitando manipolazioni o interferenze.

QRadar SOAR

consente alle organizzazioni di automatizzare e orchestrare i flussi di lavoro di risposta agli attacchi e garantire che i processi specifici vengano seguiti in modo coerente, ottimizzato e misurabile. Include 300 integrazioni precostruite e offre playbook pronti da utilizzare per rispondere a oltre 180 normative globali sulla privacy e sulla violazione dei dati.

QRadar SIEM

con un'architettura riprogettata per l'ingestione dei dati altamente efficiente, la ricerca rapida e l'analisi su larga scala Basato su Red Hat OpenShift, QRadar SIEM è progettato per essere un sistema aperto, che consente una maggiore interoperabilità con cloud e strumenti di diversi fornitori. Utilizza l'open source e gli standard aperti per le principali funzioni, incluse le regole di rilevamento e il linguaggio di ricerca, consentendogli di lavorare in modo trasversale rispetto agli stack tecnologici e di sicurezza delle aziende.

QRadar SIEM applica più livelli di intelligenza artificiale e automazione per migliorare la qualità degli avvisi e l'efficienza degli analisti di sicurezza. Queste funzionalità di intelligenza artificiale sono state pre-addestrate su milioni di avvisi e perfezionate ulteriormente per tenere conto delle unicità di ciascun cliente.

DataSecurity

Per la protezione dei dati IBM mette a disposizione un framework di sicurezza end-to-end che copre diverse funzionalità tra cui:

IBM discovery and classify

una soluzione per la discovery e classificazione automatica dei dati sensibili per qualsiasi tipo di repository e tipologia di dato (strutturato, non strutturato, on premis o in cloud). Si tratta di una soluzione completamente agentless e può essere svolta sia sui dati a riposo che sui dati in movimento. La soluzione sfrutta AI e machine learning per addestrare il sistema a identificare i dati oggetto della ricerca, garantendo una maggiore accuratezza del risultato.

IBM Guardium Data Protection

la soluzione per il monitoraggio e tracciamento in real time degli accessi ai dati sensibili; è in grado di utilizzare degli algoritmi di machine learning per compiere analisi approfondite per individuare anomalie, analizzare il rischio e identificare le possibili minacce sia interne sia esterne. Guardium Data Protection mette a disposizione anche il modulo di Vulnerability Assessment per la scansione dei database per rilevare eventuali vulnerabilità e suggerire azioni correttive.

È in grado di rilevare vulnerabilità come patch mancanti, password deboli, privilegi configurati in modo errato, condivisione di account, ecc.

IBM Polar Security

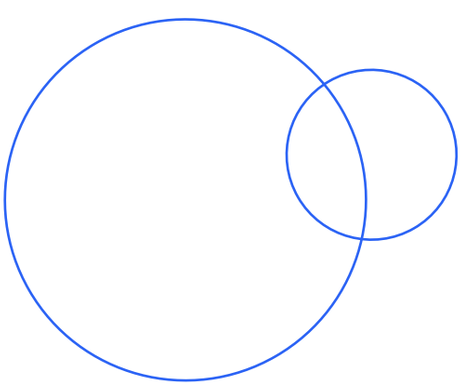
Una soluzione in SaaS di Data Security Posture Management (Cloud Data Security). Fornisce visibilità su dove si trovano i dati sensibili nel cloud, chi vi ha accesso, come vengono utilizzati e qual è la postura di sicurezza (rischi e vulnerabilità) dei data store in cui sono memorizzati. Le piattaforme supportate sono molteplici, tra cui: data-store su cloud provider (AWS, Google, Azure) Sorgenti dati nativi, buckets e applicazioni native SaaS (Google Drive, Slack, JIRA, Microsoft 365 etc.).

Randori

La piattaforma Randori permette di rilevare la superficie esterna di attacco di un'organizzazione mettendo in evidenza quelli che sono i target più "appetibili" per un attaccante. Simula il comportamento degli aggressori per fornire alle organizzazioni una visione chiara e continua del loro rischio. Implementa processi di ricognizione di tipo black box, non invasivi, e basati su informazioni pubbliche, prioritizzando i target che potrebbero essere sfruttati dagli attaccanti.

La piattaforma offre anche strumenti di red teaming automatizzato, permette di testare regolarmente le difese ed esercitare i piani di detection e reponse in condizioni reali. Questo fornisce ai team di sicurezza non solo evidenza su dove potrebbe colpire l'aggressore, ma la prova dell'impatto e dei danni che potrebbero derivare se lo ricevessero.

Attraverso l'utilizzo di Randori, le aziende sanno esattamente dove concentrare i loro sforzi, hanno una visione continuamente aggiornata della loro potenziale superficie d'attacco, semplificano e migliorano la resilienza della propria infrastruttura grazie anche alle integrazioni disponibili con l'ecosistema delle soluzioni di sicurezza esistenti, strumenti SIEM, SOAR e di Vulnerability Management.



Servizi di rilevamento e risposta alle minacce basati sull'AI

I servizi Threat Detection and Response Services (TDR) forniscono monitoraggio 24x7, indagini e correzione automatica degli avvisi di sicurezza rilevati da tutte le tecnologie presenti negli ambienti cloud ibridi, compresi gli strumenti di sicurezza e gli investimenti già previsti, nonché le tecnologie cloud, on-premise e operative (OT).

Vengono forniti dal team di analisti della sicurezza di IBM Consulting tramite la piattaforma di servizi di sicurezza avanzati di IBM, che applica più livelli di intelligenza artificiale e intelligence
sulle relative minacce provenienti dalla vasta rete di sicurezza dell'azienda, aiutando così ad automatizzare la gestione dei messaggi e risolvere rapidamente le eventuali minacce.

Affiancati da una serie di tecnologie di sicurezza basate sull'intelligenza artificiale, che supportano migliaia di aziende in tutto il mondo, sono in grado di monitorare miliardi di potenziali eventi di sicurezza al giorno. Il tutto sfruttando modelli di intelligenza artificiale che apprendono continuamente dai dati dei clienti del mondo reale, comprese le risposte degli analisti della sicurezza, e che sono progettati per chiudere automaticamente gli avvisi a bassa priorità e falsi positivi in base a un livello di sicurezza definito dall'azienda stessa.

Per supportare il continuo miglioramento delle capacità delle operazioni di sicurezza, i TDR Services comprendono l'accesso ai servizi di risposta agli incidenti X-Force di IBM, oltre alla possibilità di includere ulteriori servizi di sicurezza proattivi di IBM X-Force, quali ad esempio i test di penetrazione, simulazione avversaria o gestione delle vulnerabilità.

IBM Security Verify

Il report X-Force Threat Intelligence Index 2024 evidenzia l'emergere di una crisi globale in materia di identità digitali dovuta al fatto che è raddoppiato lo sfruttamento delle identità digitali degli utenti da parte dei criminali informatici con l'obiettivo di danneggiare le imprese di tutto il mondo.

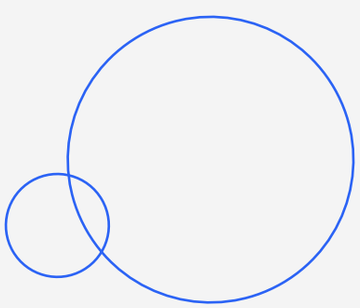
Secondo IBM X-Force i criminali informatici hanno individuato nello sfruttamento di account validi la strada più facile l'accesso malevolo alle reti aziendali e l'Italia si colloca tra i cinque paesi europei più colpiti.

Tutto ciò mette ancora maggiore enfasi sulla necessità per le aziende di rivedere e organizzare al meglio la propria strategia di Identity & Access Management (IAM).

La famiglia IBM Security Verify fornisce soluzioni, in cloud e on-premise, per gestire in modo completo l'identity fabric ed indirizzare al meglio la risposta alle nuove minacce.
Governance delle identità digitali, modalità di autenticazione avanzata e senza password, orchestrazione delle identità, gestione degli accessi privilegiati sono alcuni degli scenari che possono essere indirizzati con le soluzioni IBM Security Verify.
Ad essi si aggiungono la gestione accurata e corretta dei consensi, strumenti per la creazione di esperienze di registrazione semplici, la possibilità di realizzare arricchimenti progressivi dei profili utente che caratterizzano oggi le sfide più importanti di un sistema di Consumer IAM (CIAM).

Considerando gli ultimi trend in ambito di identità digitali, garantire la continua visibilità sulle autorizzazioni e sul loro utilizzo è fondamentale, così come adottare funzionalità come l'Adaptive Access che, sfruttando algoritmi di Intelligenza Artificiale, fornisce una valutazione in tempo reale del rischio rilevando possibili accessi malevoli e permettendo l'attuazione di policy di accesso ad hoc.

Un settore sicuramente emergente è inoltre l'Identity Threat Detection and Response (ITDR) che ha come obiettivo la protezione dagli attacchi basati sulle identità (come phishing, password spray, credential stuffing).
Le funzionalità di ITDR fornite da IBM Security Verify consentono alle organizzazioni di identificare e correggere in modo proattivo attacchi alle identità grazie all'applicazione di algoritmi di intelligenza artificiale in continua evoluzione.



Formazione e corsi

I percorsi di formazione certificati

Rispondere a un incidente informatico è una responsabilità di tutta l'azienda, è quindi fondamentale che tutti i dipendenti siano formati per essere pronti a fronteggiare e gestire questi eventi.

La IBM Cyber Academy offre alle aziende del settore pubblico e privato la possibilità di mettere alla prova, e aumentare, le proprie competenze di cybersecurity.

Sarà infatti possibile approfondire le tematiche di cybersecurity con l'ausilio degli esperti che spiegheranno in dettaglio come migliorare l'appoccio aziendale e personale – la cultura di sicurezza - ma anche come usare gli strumenti necessari per potersi avvicinare al mondo della sicurezza informatica. Grazie a esperienze immersive, è poi possibile ampliare l'offerta di training con attività che possono fornire chiare indicazioni su come comportarsi quando si fronteggia una minaccia e come gestire le crisi.

Infatti, quando si tratta di minacce cyber non è sempre possibile prevedere quando si verificheranno, ma ci si può preparare, acquisendo nuove competenze e specializzandosi per minimizzare gli impatti che questo tipo di incidenti possono avere su processi e applicazioni critiche di ogni organizzazione.

All'interno dell'IBM Cyber Theatre nella IBM Cyber Academy le sessioni di training comprendono un laboratorio interattivo, capace di far vivere in modo immersivo ed emozionale l'esperienza di un'intromissione malevola, andando a ricreare lo stress di un attacco informatico reale per testare le capacità di risposta in situazioni complesse e impreviste. Al termine del laboratorio sarà possibile ottenere il certificato di partecipazione, scaricabile dalla piattaforma SkillsBuild di IBM.

La formazione potrà essere poi ulteriormente arricchita grazie a numerosi corsi gratuiti messi a disposizione sulla piattaforma skillsbuild.org, tra cui: "Cybersecurity Fundamentals", "Generative AI in Cybersecurity", "Fortinet Certified Fundamentals", "Fortinet Certified Associate", "VetsinTech Cybersecurity". Alla fine di ciascun corso, ogni partecipante potrà scaricare il certificato nominativo con validità internazionale ad arricchimento del proprio curriculum professionale.

IBM SkillsBuild

Vai al link --->

LUBE: un programma Digital Security per garantire continuità di business e protezione del brand in ogni momento

Incremento degli investimenti in security e digitalizzazione per assicurare continuità operativa di fronte alle nuove sfide di mercato: questo l'approccio che il Gruppo LUBE - da oltre 50 anni protagonista del settore dell'arredo cucina – ha adottato realizzando il programma Digital Security assieme ai partner tecnologici IBM e Var Group. Gruppo LUBE è una vera e propria eccellenza del Made in Italy con 675 dipendenti e 4 stabilimenti produttivi, 1.650 punti di vendita in oltre 80 paesi al mondo.

Per proteggere il proprio brand e mettere a disposizione dei propri clienti prodotti e servizi di primaria qualità, LUBE ha adottato un approccio proattivo alla sicurezza, scegliendo un programma di Digital Security, basato su tecnologia IBM, realizzato in partnership con Var Group, facendo leva sulle competenze della divisione digital security Yarix.

Nell'ambito del percorso di Digital Security questo approccio evoluto alla sicurezza consente di analizzare in modalità intelligente l'intero traffico di rete, permette di controllare in modo continuativo l'intero sistema informatico e mette in sicurezza i dati aziendali, prevenendo i sempre più frequenti attacchi, inclusi quelli alla supply chain che costituiscono i rischi maggiormente diffusi e in crescita nel panorama del crimine informatico.

Il progetto, realizzato da Var Group, poggia su elementi strategici come il servizio di monitoraggio e gestione eventi fornito dal Security Operation Center (SOC) di Yarix e la tecnologia IBM QRadar, Security Information and Event Management (SIEM).

Grazie al lavoro di consulenti che operano H24, 7 giorni su 7, e alle capacità evolute di analytics, la soluzione adottata consente di rilevare in tempo reale i primi segnali di rischio.

IBM Lube

Vai al link --->

Intesa Sanpaolo è già nel percorso Quantum Safe

La collaborazione tra IBM e Intesa Sanpaolo (ISP) sul tema quantum-safe, iniziata a fine 2022, è nata dalla necessità di ISP di iniziare a proteggersi rispetto a un futuro computer quantistico, disponibile su larga scala, che potrebbe mettere a rischio l'attuale crittografia a chiave pubblica. ISP era consapevole della necessità di passare a una crittografia sicura dal punto di vista quantistico e voleva capire fino a che punto l'uso della crittografia quantum-safe fosse fattibile e maturo, quali potessero essere gli impatti potenziali e la complessità per la futura adozione.

Durante il progetto, ISP e IBM hanno lavorato insieme eseguendo diversi test con le librerie crittografiche di IBM Research su due dei quattro algoritmi di crittografia post-quantistica selezionati dal National Institute for Standards and Technology (NIST) per il processo di definizione della standardizzazione futura: CRYSTALS-Kyber per la crittografia generale e CRYSTALS-Dilithium per le firme digitali. Nell'ultimo anno, tali librerie sono diventate parte del prodotto IBM Quantum Safe Remediator, che permette di implementare modelli quantum-safe basati sulle migliori pratiche e comprenderne l'impatto potenziale sui sistemi e sulle risorse dovute all'adozione di soluzioni quantum-safe.

I test sono stati eseguiti utilizzando l'ambiente IBM Cloud, dove ISP ha potuto sperimentare diverse applicazioni degli algoritmi di crittografia quantum-safe, in gran parte supportati da componenti open-source. In particolare, il test ha riguardato un'applicazione Java Chat "business-like" di ISP, che utilizza elementi del protocollo KEMTLS. Questo protocollo sfrutta i meccanismi di incapsulamento delle chiavi (KEM) come elemento costitutivo per lo scambio di chiavi e l'autenticazione. L'algoritmo utilizzato è CRYSTALS-Kyber. I risultati dei test sono stati riassunti in un rapporto finale che definisce i possibili passi successivi per l'adozione della tecnologia in altri casi d'uso.

Sperimentando i modelli di crittografia quantum-safe, ora disponibili attraverso IBM Quantum Safe Remediator, il cliente è stato in grado di raggiungere un elevato grado di maturità nella comprensione dell'impatto di una futura migrazione alla crittografia quantum-safe. Questo può essere considerato uno dei primi passi del percorso quantum-safe su scala aziendale.

IBM Intesa Sanpaolo

Vai al link --->

Stampato su
carta riciclata