IBM Italia
Audizione su Comunicazione UE
« La politica di cyberdifesa dell'UE «

Roma, 3 Maggio 2023

Scenario di cybersecurity

La fotografia che il gruppo di ricerca IBM X Force, che monitora più di 150 miliardi di eventi di sicurezza al giorno in tutto il mondo, ci evidenzia come gli attaccanti continuino a innovare i loro malware con focus sulle strutture cloud e Linux. Il ransomware e lo sfruttamento delle vulnerabilità rappresentano tra le sfide più importanti da gestire per le varie organizzazioni gravando inoltre sulle relative catene di approvvigionamento.

Notiamo come la quota di incidenti legati al ransomware sia diminuita solo leggermente (4 punti percentuali) nel 2022 rispetto all'anno precedente, i difensori quindi hanno avuto comunque più successo nel rilevare e prevenire i ransomware.

Nonostante questo, gli aggressori continuano a evolversi, infatti il report mostra che il tempo medio per completare un attacco ransomware è sceso da 2 mesi a meno di 4 giorni. Mentre il phishing è stato il vettore di attacco più comune nell'ultimo anno, IBM Security X-Force ha osservato un aumento nel numero degli attacchi causati dallo sfruttamento di vulnerabilità dei software non aggiornati: è questo il punto di ingresso preferito dai cybercriminali, causa della maggior parte degli attacchi ransomware.

Nel report si osserva come i cybercriminali vendano l'accesso alle backdoor esistenti per 10.000 dollari, rispetto ad esempio ai dati delle carte di credito rubate, che oggi possono essere venduti per meno di 10 dollari.

Nell'immagine a fianco, sono riportati alcuni dati significativi a livello mondiale.

In Italia la situazione è ancora complessa secondo il 2022 Cost of Data Breach Study (condotto da Ponemon Institute, promosso e analizzato da IBM), il tempo medio necessario per identificare un attacco è 181 giorni e 69 giorni per il contenimento ed il costo medio di una violazione dei dati è di 3,4 milioni di euro rendendo se necessario ancora più evidente le conseguenze sull'economia reale di un attacco cyber.

Alcune tra le sfide dei responsabili della sicurezza

27% degli attacchi è finalizzato all'estorsione	**58%** dei tentativi di phishing è indirizzato a ricercare le password degli utenti (più ricercate delle carte di credito)	**21%** degli incidenti ha visto l'implementazione di backdoors come obiettivo principale degli attaccanti a seguito di una violazione riuscita
70% delle organizzazioni ha subito almeno un attacco informatico attraverso l'utilizzo di un virus che ha sfruttato una falla informatica del sistema	**$4.35M** costo medio di una violazione dei dati a livello mondiale	**#1** l'industria manifatturiera è stata quella più attaccata nel 2022 nel mondo

Fonti: 2023 IBM X -Force Threat Intelligence Report, 2022 The State of Attack Surface Management Report, 2022 IBM Security Cost o f a Data Breach Report

Lo scenario di cybersecurity che abbiamo di fronte è estremamente complesso in quanto all'aumento della tipologia e della complessità degli attacchi si assiste alla forte crescita di nuove applicazioni e servizi in digitale da parte delle aziende e delle organizzazioni in generale.

Tutto questo in presenza di una limitazione di budget aziendali e una scarsità di risorse di competenze di cybersecurity sul mercato a livello mondiale.

E' quindi fondamentale avere una chiara definizione di quali sono gli assett, applicazione e i dati critici da proteggere per attuare una strategia di difesa efficace.

Si deve affrontare il tema della complessità dei software di sicurezza presenti nelle aziende che negli anni hanno spesso affrontato i vari problemi tecnici, aggiungendo strumenti software di sicurezza adatti solamente ad affrontare il tema specifico.

Questo crea complessità e aggravio sui costi, quindi è necessario lavorare sulla capacità di integrazione di questi software attraverso piattaforme open che favoriscono la loro integrazione e soprattutto una vista coerente e integrata dei rischi che un'organizzazione potrebbe correre in ogni istante.

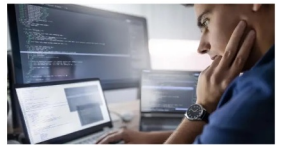
Questa razionalizzazione e integrazione deve essere accompagnata dal miglioramento dei processi di gestione della sicurezza e ad esempio di un incidente di sicurezza ed attraverso un continuo investimento sulle competenze di cybersecurity sia degli utenti che dei team di sicurezza aziendali.

Gli scenari di Cyber Security richiedono una governance integrata

Fattori Principali

Maggiori rischi

Velocità della digitalizzazione



Budget limitati

Complessità e carichi di lavoro dei team

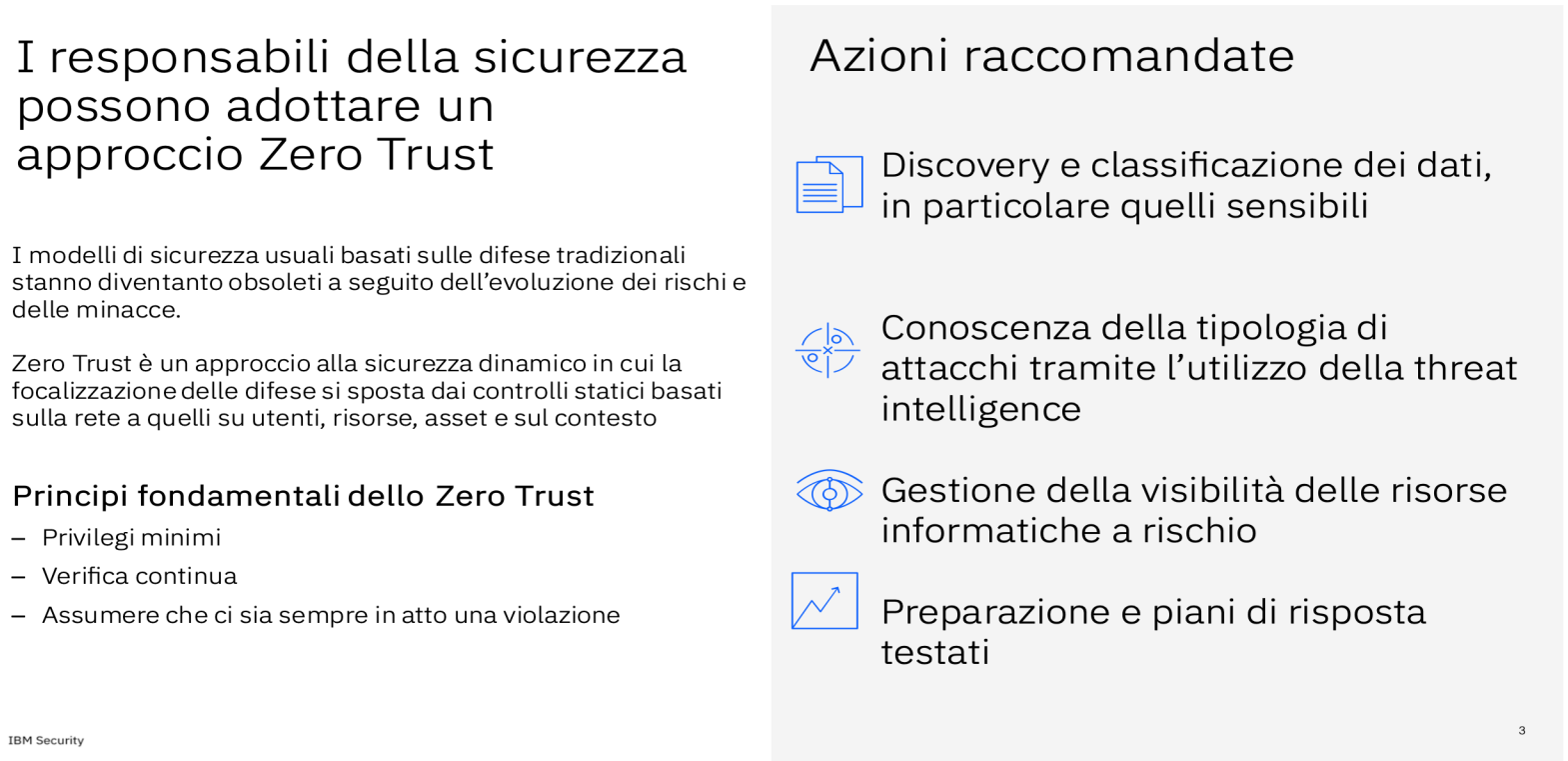
Strategia di sicurezza

Razionalizzazione dei tool e capacità di integrazione degli stessi

Miglioramenti dei processi e delle competenze

Quindi per gestire una tipologia di aggressione che cambia in continuazione e migliora le tecniche di attacco, trovando sempre nuovi modi per non essere rilevati, impone a chi si difende di adottare una strategia di sicurezza proattiva e basata sulle minacce.

E' importante quindi adottare una metodologia di "Zero Trust", ovvero un approccio fondato su una architettura informatica e dei servizi volti ad avere accesso alle applicazioni con privilegi minimi, effettuare sempre una verifica di chi accede e perché e supporre sempre che ci sia una violazione in atto.



Rimane importante cominciare ad investire sul futuro ed in particolare anticipando le problematiche dell'adozione di sistemi Quantum Computing che avranno un impatto sulla crittografia attuale mettendo potenzialmente rischio tutta l'infrastruttura di dati e comunicazioni attuali.

In Italia la consapevolezza sulla cybersecurity è sicuramente aumentata, soprattutto nelle aziende più grandi, ma la struttura del tessuto industriale e produttivo fatto di piccole e medie aziende e la frammentazione di tante piattaforme di interesse nazionale (sanità, scuola,) ci fa capire come questa cultura debba essere ancora compresa e soprattutto incentivata per favorire gli investimenti in tecnologie e capitale umano che sono necessari.