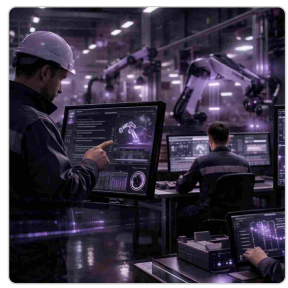
AUTOMAZIONENEWS.IT (WEB)

Minacce cyber: si espande la superficie di attacco, con tecniche piu' automatizzate e mirate a ident



La tua email
La password verrà inviata via email.
Home Process Automation Safety e Cybersecurity Minacce cyber: si espande la superficie di attacco, con tecniche più automatizzate...
Minacce cyber: si espande la superficie di attacco, con tecniche più automatizzate e mirate a identità digitali
Un´analisi sull´evoluzione delle minacce cyber da parte di Relatech, a partire dai dati del suo Risk Operations Center, rileva una crescita della superficie di attacco digitale e un aumento importante delle minacce informatiche.
Minacce cyber: si espande la superficie di attacco, con tecniche più automatizzate e mirate a identità digitali
Print
Credits: Relatech
Relatech ha presentato un´analisi aggiornata dell´evoluzione delle minacce cyber che colpiscono oggi imprese e organizzazioni. La crescente digitalizzazione dei processi aziendali, la diffusione di infrastrutture Cloud, l´interconnessione di sistemi e dispositivi e l´aumento dei servizi digitali esposti su Internet stanno estendendo rapidamente la superficie di attacco a disposizione dei cybercriminali.
In questo scenario, caratterizzato da attacchi sempre più automatizzati e mirati, diventano sempre più centrali il monitoraggio continuo delle infrastrutture digitali e la capacità di individuare tempestivamente attività sospette.
Il quadro globale: cosa dicono gli ultimi report sulla cybersecurity
Il quadro è confermato anche dai principali osservatori del settore. Secondo il Rapporto Clusit sulla sicurezza ICT in Italia, gli attacchi informatici continuano a crescere sia a livello globale sia nel nostro Paese.
Analogamente, l´ENISA Threat Landscape evidenzia come ransomware, phishing e compromissione delle credenziali rappresentino i principali vettori di attacco.
Il Data Breach Investigations Report (DBIR) di Verizon sottolinea come una quota significativa delle violazioni informatiche sia legata proprio all´abuso di credenziali e identità digitali compromesse.
I dati del Risk Operations Center di Relatech: +44% di attacchi in sei mesi
Queste tendenze trovano riscontro anche nei dati raccolti dal Risk Operations Center di Relatech attraverso il quale l´azienda monitora e analizza quotidianamente migliaia di eventi cyber provenienti dalle infrastrutture digitali dei propri clienti. L´analisi, basata sugli eventi rilevati negli ultimi sei mesi, offre una fotografia concreta dell´evoluzione recente delle minacce cyber.
Nel periodo analizzato gli attacchi rilevati sono aumentati del 44%, passando da circa 32.000 episodi nell´agosto 2025 a oltre 46.000 nel gennaio 2026.
La parola all´esperto: la visione di Relatech sulla cybersecurity
"Gli attacchi cyber non sono più eventi isolati, ma processi strutturati attraverso cui gli attaccanti individuano vulnerabilità nelle infrastrutture esposte", dichiara Andrea Ferrazzi, Cybersecurity & Cloud Business Unit Director di Relatech.
"In questo contesto le organizzazioni devono rafforzare la propria postura di sicurezza adottando modelli basati su monitoraggio continuo, analisi avanzata delle minacce e capacità di risposta rapida agli incidenti. La capacità di anticipare e rilevare tempestivamente le anomalie diventa oggi un fattore decisivo per proteggere infrastrutture, dati e continuità operativa".
Relatech Cloud Security: protezione continua 24/7
All´interno di questa strategia di protezione opera Relatech Cloud Security, la business unit del Gruppo dedicata alla protezione delle infrastrutture digitali e dei dati aziendali. L´area integra competenze in cybersecurity, Cloud e IT infrastructure, offrendo servizi gestiti e soluzioni personalizzate progettate per rafforzare la resilienza cibernetica delle organizzazioni.
Tra le attività rientrano servizi di monitoraggio e gestione della sicurezza attraverso centri operativi SOC (Security Operation Center) e NOC attivi 24/7, oltre all´integrazione di piattaforme tecnologiche progettate su misura per proteggere gli ambienti digitali aziendali.

Le tecniche di attacco più diffuse secondo il framework MITRE ATT&CK

L´analisi degli eventi gestiti dal SOC di Relatech, classificati secondo il framework internazionale MITRE ATT&CK, consente di individuare con precisione le principali tecniche utilizzate dagli attaccanti .

Fra le tecniche più diffuse emerge in particolare il credential access , che rappresenta circa il 30% degli eventi rilevati. Seguono i tentativi di initial access (24,4%), attraverso cui gli attaccanti cercano di ottenere il primo accesso alle infrastrutture della vittima.

Un ulteriore 11% degli eventi riguarda attività di command and control , indicative di tentativi di mantenere il controllo dei sistemi compromessi e stabilire canali di comunicazione con infrastrutture esterne.

Credenziali compromesse e phishing: le principali cause degli incidenti

Tra gli eventi più frequentemente rilevati figurano attività di scanning delle infrastrutture esposte, tentativi di accesso non autorizzato tramite credential attack e numerose operazioni riconducibili a tecniche di brute force e password spraying , utilizzate dagli attaccanti per individuare credenziali valide e ottenere un primo punto di ingresso nelle reti aziendali.

Le analisi del SOC indicano inoltre che la compromissione delle credenziali di accesso rappresenta la principale causa degli incidenti osservati, spesso ottenuta attraverso campagne di phishing o tentativi automatizzati di accesso alle credenziali sfruttando configurazioni deboli o sistemi esposti su Internet.

Privilege escalation e lateral movement: quando l´attacco si espande

Parallelamente, il SOC ha rilevato anche numerosi eventi riconducibili alle fasi successive del ciclo di attacco, tra cui privilege escalation, lateral movement e command and control . Questi indicatori segnalano tentativi da parte degli attaccanti di espandere progressivamente la propria presenza all´interno delle reti compromesse e mantenere il controllo dei sistemi.

Tags