Minacce Informatiche nel 2024

Nel contesto dell'era digitale, le **minacce informatiche** rappresentano una delle sfide più complesse per le aziende. Non si tratta più soltanto di proteggere i dati, ma di garantire la continuità operativa di intere organizzazioni in un panorama globale sempre più interconnesso. Il **Threat Landscape 2024** di ENISA, l'Agenzia Europea per la Cybersecurity, traccia una panoramica dettagliata delle **minacce informatiche** attuali, analizzando tendenze, attori malevoli e soluzioni per la difesa.

Dal report emerge come ormai la cybersecurity non è più solo una preoccupazione tecnica, ma una parte fondamentale della strategia aziendale. Con l'aumento degli attacchi informatici e la loro crescente sofisticazione, le aziende devono essere pronte a difendersi in un contesto che cambia rapidamente.

Panoramica delle Minacce Informatiche

Nel 2024, le **minacce informatiche** sono aumentate sia in termini di volume che di sofisticazione. Attacchi come il **ransomware**, il **malware** e i **Distributed Denial of Service (DDoS)** stanno colpendo duramente settori critici come la sanità, la finanza e la pubblica amministrazione. Secondo ENISA, le **minacce informatiche** principali che le aziende devono affrontare includono ransomware, malware, attacchi di ingegneria sociale, violazioni di dati e attacchi alla supply chain.

Breakdown of analysed incidents by threat type (July 2023 till June 2024), ENISA

Le 7 Principali Minacce

Informatiche del 2024

1. Ransomware: Una delle Maggiori Minacce Informatiche

Il ransomware rimane una delle **minacce informatiche** più gravi per le aziende e continua a essere uno dei principali vettori di attacco nel 2024, con tecniche sempre più raffinate e dannose. L'evoluzione di questi attacchi ha portato a un aumento delle strategie di doppia e tripla estorsione, in cui gli attaccanti non solo criptano i dati delle vittime, ma minacciano anche di rilasciarli pubblicamente o di attaccare nuovamente se il riscatto non viene pagato. Gli attacchi ransomware hanno colpito in particolare settori come i servizi sanitari e finanziari, dove i dati sensibili e le operazioni critiche sono bersagli perfetti per estorsioni di alto profilo.

Dal punto di vista tecnico, gli attacchi ransomware spesso sfruttano vulnerabilità nei sistemi legacy o approfittano di credenziali compromesse. I vettori di accesso iniziali più comuni includono phishing mirato (spear phishing), exploit di vulnerabilità note e accesso ottenuto tramite broker di accessi iniziali (IAB). Una volta dentro la rete, gli attori malevoli utilizzano tecniche avanzate di **Living Off The Land (LOTL)** per sfruttare strumenti di sistema legittimi, evitando di essere rilevati dalle soluzioni di sicurezza tradizionali.

Mitigazione del Rischio Ransomware

Per difendersi da questo tipo di attacchi, le organizzazioni devono implementare una serie di misure preventive:

- **Backup regolari e testati**: Gli attacchi ransomware puntano a compromettere i dati, quindi backup frequenti e separati dalla rete principale sono fondamentali.
- **Segmentazione della rete**: Suddividere la rete in segmenti separati riduce l'impatto potenziale di un

attacco e limita la capacità degli attaccanti di muoversi lateralmente all'interno della rete.
- **Autenticazione multifattore (MFA)**: Limitare l'accesso agli asset critici utilizzando autenticazioni multiple, impedendo così agli attori malevoli di accedere ai sistemi solo con credenziali compromesse.

2. Malware: L'Ascesa del Malware-as-a-Service (MaaS)

Il malware resta uno dei metodi più comuni di attacco, ma il panorama si è evoluto significativamente. L'ascesa di modelli di business come il **Malware-as-a-Service (MaaS)** ha abbassato la barriera d'ingresso per i cybercriminali meno esperti, che possono acquistare e distribuire malware personalizzati su misura per le loro vittime.

Questi software malevoli sono progettati per compromettere la riservatezza, l'integrità e la disponibilità dei sistemi attaccati. Esempi di malware comuni includono **trojan bancari**, **spyware** e **worm**, tutti progettati per sottrarre dati sensibili o propagarsi all'interno delle reti aziendali.

Tecniche di Difesa Contro il Malware

- **Monitoraggio continuo**: Implementare soluzioni di **endpoint detection and response (EDR)**, che forniscono una visibilità avanzata su ciò che accade su ogni endpoint della rete.
- **Patching tempestivo**: Il malware spesso sfrutta vulnerabilità conosciute nei sistemi software. È essenziale implementare una gestione rigida delle patch per chiudere queste falle prima che possano essere sfruttate.
- **Threat intelligence**: L'utilizzo di servizi di threat intelligence in tempo reale può aiutare a identificare e mitigare potenziali minacce prima che colpiscano.

3. Ingegneria Sociale: Il Fattore Umano Come Vettore di Attacco

Nonostante le difese tecnologiche avanzate, il fattore umano rimane uno degli anelli deboli della sicurezza informatica. Le tecniche di **ingegneria sociale**, come il phishing, lo spear phishing e gli attacchi **Business Email Compromise (BEC)**, sfruttano l'errore umano per accedere a informazioni sensibili. Questi attacchi possono ingannare i dipendenti a divulgare credenziali o a eseguire azioni dannose come trasferimenti di denaro non autorizzati.

Prevenzione degli Attacchi di Ingegneria Sociale

- **Formazione e sensibilizzazione**: È essenziale educare continuamente i dipendenti sui rischi degli attacchi di ingegneria sociale, inclusi i segnali di phishing e altre tecniche di manipolazione.
- **Simulazioni di attacchi**: Le simulazioni regolari di phishing aiutano a preparare i dipendenti a riconoscere le minacce reali, migliorando la resilienza dell'organizzazione.

4. Minacce alla Disponibilità: Gli Attacchi DDoS e la Resilienza della Rete

Gli attacchi **Denial of Service (DoS)**, in particolare i **Distributed Denial of Service (DDoS)**, continuano a rappresentare una grave minaccia per le aziende, interrompendo i servizi e causando danni finanziari e reputazionali significativi. Questi attacchi sovraccaricano i sistemi con richieste illegittime, impedendo agli utenti legittimi di accedere ai servizi.

Difesa Contro gli Attacchi DDoS

- **Infrastrutture scalabili**: Utilizzare servizi di mitigazione DDoS basati su cloud che possano assorbire e

neutralizzare il traffico malevolo prima che raggiunga l’infrastruttura aziendale.
- **Architetture di rete distribuite**: La distribuzione dei servizi su una rete globale di data center può ridurre l’impatto di un attacco DDoS, permettendo di deviare il traffico malevolo verso nodi meno vulnerabili.

5. Violazioni dei Dati: Difendere il Patrimonio Informativo

Le minacce ai dati, comprese le violazioni e le fughe di dati, sono tra le problematiche più critiche per le aziende nel 2024. Le violazioni dei dati non solo espongono informazioni sensibili, ma possono anche portare a pesanti sanzioni normative, in particolare nell’Unione Europea, dove il GDPR impone requisiti stringenti sulla protezione dei dati.

Misure per Proteggere i Dati dalle Minacce Informatiche

- **Crittografia dei dati**: Assicurarsi che tutti i dati sensibili, sia in transito che a riposo, siano adeguatamente crittografati per prevenire l’accesso non autorizzato.
- **Gestione rigorosa delle autorizzazioni**: Implementare controlli di accesso basati sui ruoli (RBAC) per limitare l’accesso ai dati sensibili solo al personale autorizzato.

6. Manipolazione dell’Informazione: Il Cyber Espionaggio e l’Interferenza Straniera

Il 2024 ha visto un aumento delle campagne di **manipolazione delle informazioni**, spesso utilizzate come strumento di disinformazione e interferenza elettorale. Queste campagne sono spesso condotte da attori statali e mirano a

destabilizzare società o manipolare opinioni pubbliche a fini politici.

Contromisure per la Manipolazione dell’Informazione

- **Monitoraggio dei media e dei social media**: Implementare strumenti che rilevino rapidamente attività di disinformazione e che possano rispondere in modo proattivo con contro-narrative.
- **Collaborazione intersettoriale**: Lavorare con altre organizzazioni e agenzie governative per identificare e mitigare rapidamente queste minacce.

7. Attacchi alla Supply Chain: La Debolezza nei Sistemi Esterni

Gli attacchi alla supply chain sono emersi come una delle minacce informatiche più insidiose nel 2024. Questi attacchi mirano a compromessi nelle componenti software o hardware utilizzate da più organizzazioni. Un esempio notevole è il caso di compromissioni in progetti open-source, come **XZ Utils**, che ha visto l’introduzione di backdoor attraverso il social engineering verso i manutentori del progetto.

Difesa Contro gli Attacchi alla Supply Chain

- **Verifica delle forniture**: Implementare un processo rigoroso di verifica dei fornitori per garantire che i componenti software e hardware provengano da fonti affidabili.
- **Monitoraggio continuo delle vulnerabilità**: Mantenere un’attenzione costante sugli aggiornamenti dei software e sulle vulnerabilità potenzialmente sfruttabili nella catena di fornitura.

Attori delle Minacce

ENISA identifica quattro principali categorie di attori delle minacce:

- **Attori collegati agli Stati**: Questi gruppi, ben finanziati e con risorse significative, operano spesso per finalità di spionaggio o sabotaggio su larga scala.
- **Cybercriminali**: Gruppi che operano principalmente per profitto finanziario, utilizzando attacchi opportunistici per massimizzare il danno economico.
- **Attori del Settore Privato Offensivo (PSOA)**: Aziende private che sviluppano e vendono cyberarmi avanzate.
- **Hacktivisti**: Gruppi motivati da cause politiche o sociali, che utilizzano attacchi informatici per promuovere il cambiamento.



EU breakdown of number of threats by threat group, ENISA

Il **Threat Landscape 2024** di ENISA mette in evidenza un panorama delle minacce in continua evoluzione, dove le tecnologie avanzate e le tattiche di attacco sempre più sofisticate richiedono un approccio proattivo e multilivello alla sicurezza informatica. Le aziende devono adottare misure integrate che includano tecnologie all’avanguardia, formazione costante del personale e strette collaborazioni con enti governativi e fornitori. Solo così sarà possibile affrontare con successo le sfide che la cybersecurity continuerà a presentare nel futuro prossimo. Solo con un approccio integrato sarà possibile mitigare l’impatto delle **minacce informatiche** sul lungo termine.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/minacce-informatiche-2024/