TD SYNNEX

La Babele delle nuove tecnologie di sicurezza

Orientarsi in un mondo in continua evoluzione

12 Luglio 2024

Webinar

Andrea Pezzoni – Security Presales Specialist – TD SYNNEX

Nuove tecnologie, nuovi acronimi e concetti

TD SYNNEX

Il mondo della Cyber Security sta affrontando una crescita senza eguali

Negli anni passati, il concetto di Cyber Security, spesso, ruotava intorno all'antivirus e al firewall.
Sono ancora sufficienti?
Cosa dobbiamo conoscere per affrontare i rischi alla sicurezza del dato?

Si fa presto a dire Cybersecurity

Cosa si nasconde dietro un concetto così vasto

La cybersecurity è un insieme di processi, procedure consigliate e soluzioni tecnologiche in grado di proteggere la tua rete e i tuoi sistemi critici dagli attacchi digitali. (Microsoft)

La cybersecurity è l'arte di proteggere reti, dispositivi e dati da accessi non autorizzati o da usi criminali e la pratica di garantire la riservatezza, l'integrità e la disponibilità delle informazioni (American Cyber Defense Agency)

La cybersecurity è la prassi di proteggere i sistemi, le reti e i programmi dagli attacchi digitali. (Cisco)

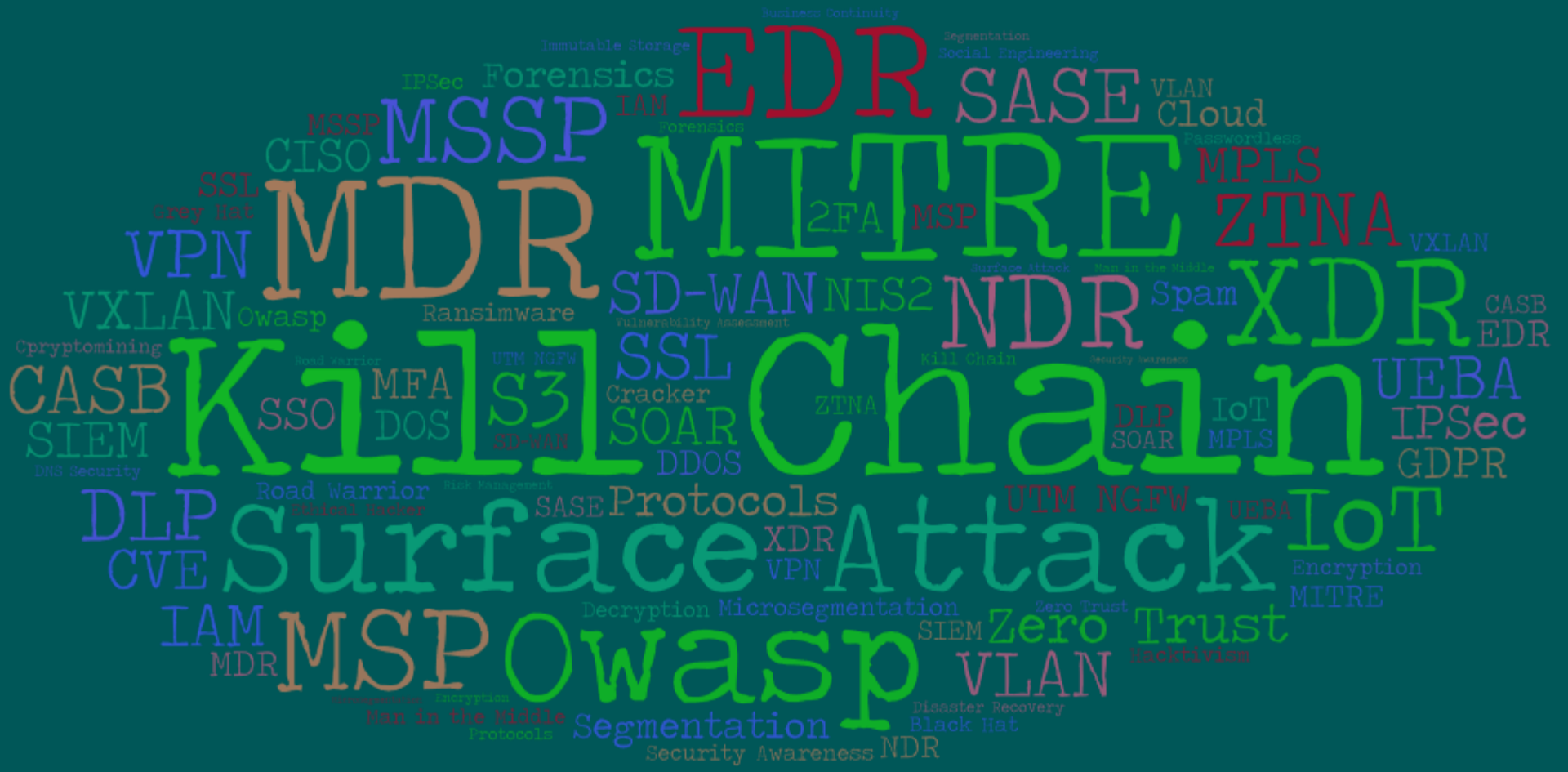
La sicurezza informatica è il modo in cui individui e organizzazioni riducono il rischio di attacchi informatici. (National Cyber Security Centre)

Per cybersecurity si intende qualsiasi tecnologia, misura o pratica per prevenire i cyberattacchi o attenuarne l'impatto. (IBM)

CyberSecurity Pillars

- Analisi e Compliance
- Processi e Procedure
- Persone
- Reti e Applicazioni
- Dispositivi
- Identità
- Dati
- Monitoraggio

TD SYNNEX


Business Continuity
Immutable Storage
Segmentation
Social Engineering
IPSec
Forensics
EDR
SASE
VLAN
IAM
Cloud
MSSP
Forensics
Passwordless
CISO
MSSP
MITRE
MPLS
SSL
Grey Hat
MDR
2FA
MSP
ZTNA
VPN
VXLAN
Surface Attack
Man in the Middle
SD-WAN
NIS2
NDR
Spam
XDR
CASB
VXLAN
Owasp
Ransimware
Vulnerability Assessment
EDR
Cpryptomining
SSL
Kill Chain
Security Awareness
CASB
MFA
S3
Cracker
UEBA
Road Warrior
UTM NGFW
Kill Chain
SSO
DOS
SOAR
ZTNA
DLP
IoT
IPSec
SIEM
SD-WAN
MPLS
DDOS
GDPR
DNS Security
Road Warrior
Risk Management
DLP
SASE
Protocols
UTM NGFW
UEBA
IoT
Surface
Attack
CVE
XDR
VPN
Encryption
MITRE
IAM
Decryption
Microsegmentation
Zero Trust
SIEM
Zero
Trust
MDR
MSP
Owasp
VLAN
Hacktivism
Encryption
Disaster Recovery
Man in the Middle
Segmentation
Black Hat
Protocols
Security Awareness
NDR

Analisi e Compliance

CISO
DPO
ISO
GDPR
NIS2
Assessment/Vulnerability Assessment
Penetration Testing (network and application)

Esame sistematico di un sistema o di un prodotto informatico per determinare l'adeguatezza delle misure di sicurezza, identificare le carenze di sicurezza, fornire dati in base ai quali prevedere l'efficacia delle misure di sicurezza proposte e confermare l'adeguatezza di tali misure dopo l'attuazione. (NIST)

Un metodo di test in cui i si prendono di mira i singoli componenti binari o l'applicazione nel suo complesso per determinare se le vulnerabilità interne o intercomponenti possono essere sfruttate per compromettere l'applicazione, i suoi dati o le sue risorse ambientali. (NIST)

Processi e Procedure

Backup
Disaster Recovery
RTO/RPO
Business Continuity
Remediation Plan
Policies
Least Privilege Approach

Recovery Time Objectives: Il tempo complessivo in cui i componenti di un sistema informativo possono essere in fase di recupero prima di avere un impatto negativo sulla missione o sui processi aziendali dell'organizzazione.
Recovery Point Objectives: Il momento in cui i dati devono essere recuperati dopo un'interruzione. (NIST)

Un principio di sicurezza secondo il quale un sistema deve limitare i privilegi di accesso degli utenti (o dei processi che agiscono per conto degli utenti) al minimo necessario per svolgere i compiti assegnati. (NIST)

Persone

Awareness
Phishing/Spear Phishing/Smishing/Vishing
Clone Phishing/Quishing/Whaling o Whale Phishing
Social Engineering
Shoulder surfing Attack
USB Drop
Juice Jacking

Processo di apprendimento che pone le basi per la formazione, modificando gli atteggiamenti individuali e organizzativi per rendersi conto dell'importanza della sicurezza e delle conseguenze negative del suo fallimento. (NIST)

Ingannare le persone per indurle a rivelare informazioni personali sensibili affermando di essere un'entità affidabile in una comunicazione elettronica. (NIST)

Un attacco USB drop è un tipo di attacco informatico in cui una chiavetta USB, in genere precaricata con malware, viene lasciata fisicamente in un luogo con l'intento che un individuo ignaro la raccolga e la colleghi a un computer. (OSI Beyond)

Il Juice jacking è un exploit di sicurezza in cui una stazione di ricarica USB infetta viene utilizzata per compromettere i dispositivi che vi si collegano. (Techtarget)

Reti e Applicazioni

Surface Attack
Next Generation Firewall
VPN
Segmentazione
Micro-Segmentazione
Web Hijacking
DNS Redirection
ZTNA – Zero Trust
CNAPP
DevSecOps -> SecDevOps
ATP
IOC

Un insieme di concetti e idee progettati per ridurre al minimo l'incertezza nell'applicazione di decisioni di accesso accurate e con il minimo privilegio per richiesta nei sistemi e nei servizi informativi a fronte di una rete considerata compromessa. (NIST)

Un indicatore di compromissione (IOC) è la prova che qualcuno potrebbe aver violato la rete o l'endpoint di un'organizzazione. Questi dati forensi non indicano solo una potenziale minaccia, ma segnalano che un attacco, come un malware, credenziali compromesse o esfiltrazione di dati, si è già verificato. (Microsoft)

Dispositivi

CVE/CVSS
Antivirus/Antimalware
EDR/XDR/MDR
Disk Encryption
RMM
Asset inventory
System Hardening

CVE: Un dizionario di nomi comuni per le vulnerabilità dei sistemi informatici pubblicamente note.
CVSS: Common Vulnerability Scoring System (NIST)

EDR: registra e memorizza i comportamenti a livello di sistema degli endpoint, utilizza varie tecniche di analisi dei dati per rilevare i comportamenti sospetti del sistema, fornisce informazioni contestuali, blocca le attività dannose e fornisce suggerimenti per il ripristino dei sistemi interessati. (Gartner)
XDR: piattaforma unificata di rilevamento e risposta agli incidenti di sicurezza che raccoglie e correla automaticamente i dati provenienti da più componenti di sicurezza proprietari. (Gartner)
MDR: servizio di cybersecurity che combina la tecnologia con l'esperienza umana per identificare rapidamente e limitare l'impatto delle minacce eseguendo attività di threat hunting, monitoraggio e risposta. (Crowdstrike)

Identità

Identity Management
SSO
MFA
Passwordless
Token
CASB

Un sistema di autenticazione che richiede più di un fattore di autenticazione distinto per il successo dell'autenticazione. L'autenticazione a più fattori può essere eseguita utilizzando un autenticatore multifattoriale o una combinazione di autenticatori che forniscono fattori diversi. I tre fattori di autenticazione sono: something you know, something you have, and something you are (NIST)

Punti di applicazione dei criteri di sicurezza on-premises o basati sul cloud, collocati tra i consumatori di servizi cloud e i fornitori di servizi cloud per combinare e interporre i criteri di sicurezza aziendali durante l'accesso alle risorse basate sul cloud. (Gartner)

Monitoraggio

SIEM

Applicazione che offre la possibilità di raccogliere dati sulla sicurezza dai componenti del sistema informativo e di presentarli come informazioni utilizzabili attraverso un'unica interfaccia. (NIST)

SOAR

Gli strumenti SOAR consentono a un'organizzazione di definire le procedure di analisi e risposta agli incidenti in un formato di flusso di lavoro digitale. (Gartner)

Log Server

IOC

Continuos Vulnerability Assessment

SOC/NOC

SOC: Security Operation Center

NOC: Network Operation Center

NDR

Categoria di tecnologie di sicurezza informatica che utilizza metodi non basati sulla firma, come l'intelligenza artificiale, l'apprendimento automatico e l'analisi comportamentale, per rilevare attività sospette o dannose sulla rete e rispondere alle minacce informatiche. (IBM)

TD SYNNEX

“There are only two types of companies in the world: those that have been breached and know it and those that have been breached and don’t know it.”

Ted Schlein

Sitografia

https://www.cisa.gov/news-events/news/what-cybersecurity
https://www.cisco.com/c/it_it/products/security/what-is-cybersecurity.html
https://www.microsoft.com/it-it/security/business/security-101/what-is-cybersecurity
https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security
https://csrc.nist.gov/glossary
https://www.osibeyond.com/blog/usb-drop-attacks-cause-cybersecurity-incidents/
https://www.techtarget.com/searchsecurity/definition/juice-jacking
https://www.crowdstrike.com/cybersecurity-101/managed-detection-and-response-mdr/
https://www.gartner.com/en/information-technology/glossary
https://www.ibm.com/topics/ndr

TD SYNNEX

Q&A

Your Opinion Counts!

Scarica la presentazione cliccando sul codice QR

PROSSIMI APPUNTAMENTI

19 LUGLIO: Attori Criminali, Trend delle minacce, politiche di sicurezza.

26 LUGLIO: Cyber Kill Chain.

TEAM SECURITY: security.it@tdsynnex.com
SPEAKER: andrea.pezzoni@tdsynnex.com