CORSO MFA PER ACTIVE DIRECTORY: PROTEGGERE WINDOWS, RDP E ACCESSI PRIVILEGIATI ON-PREMISES

Durata: 2 ore

NEXSYS
LEARN IT, TRANSFORM IT

PROGRAMMA

MODULO 1: MFA E SUPERFICI DI AUTENTICAZIONE ON-PREMISES

1.1 I percorsi di autenticazione in Active Directory

- Logon interattivo su workstation e server Windows
- Connessioni RDP e accessi amministrativi
- UAC, SMB, PowerShell Remoting e applicazioni legacy
- Ruolo di Kerberos, NTLM, LDAP e RADIUS
- Autenticazione iniziale e riutilizzo di sessioni e ticket

1.2 Perché la protezione MFA può essere incompleta

- Limiti dell'MFA applicata solo ai servizi cloud
- Credenziali valide e movimenti laterali
- Come individuare i percorsi di autenticazione non protetti

MODULO 2: TECNOLOGIE MICROSOFT PER LA PROTEZIONE DEGLI ACCESSI

2.1 Windows Hello for Business

- Autenticazione passwordless con PIN, biometria e TPM
- Integrazione con Active Directory e Kerberos
- Accesso alle risorse aziendali e scenari RDP
- Limiti di copertura e autenticazioni alternative con password

2.2 Altri strumenti Microsoft

- Smart card e autenticazione con certificati
- Microsoft Entra MFA con NPS Extension
- MFA sugli accessi tramite Remote Desktop Gateway
- Remote Credential Guard e protezione delle credenziali RDP
- Scenari che richiedono controlli MFA aggiuntivi

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO MFA PER ACTIVE DIRECTORY: PROTEGGERE WINDOWS, RDP E ACCESSI PRIVILEGIATI ON-PREMISES

Durata: 2 ore

MODULO 3: ARCHITETTURE MFA E SOLUZIONI PER ACTIVE DIRECTORY

3.1 Modelli di implementazione

- Credential Provider e agent sui sistemi Windows
- MFA su console, RDP e operazioni amministrative
- Integrazioni RADIUS e gateway di accesso
- MFA sulle autenticazioni Kerberos/NTLM
- Proteggere l'accesso al sistema e proteggere l'autenticazione sul dominio: le differenze

3.2 Soluzioni disponibili a confronto

- AuthLite: secondo fattore integrato in Active Directory
- Cisco Duo: Windows Logon, protezione della riga di comando e delle autenticazioni AD
- Silverfort: MFA e controllo delle autenticazioni AD
- UserLock: protezione e controllo degli accessi Windows
- Criteri di confronto: copertura, granularità delle policy, integrazione, disponibilità e complessità

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO MFA PER ACTIVE DIRECTORY: PROTEGGERE WINDOWS, RDP E ACCESSI PRIVILEGIATI ON-PREMISES

Durata: 2 ore

MODULO 4: LABORATORIO PRATICO, MFA SU WINDOWS E ACTIVE DIRECTORY

4.1 Verifica delle autenticazioni Windows

- Logon su workstation con Windows Hello for Business
- Accesso alle risorse di dominio
- Autenticazioni che usano ancora la password
- Individuazione dei percorsi privi di MFA

4.2 MFA sugli accessi RDP con un Credential Provider

- Architettura di un Credential Provider MFA (in laboratorio: Duo Windows Logon)
- Installazione e configurazione su Windows Server
- Abilitazione dell'MFA per le connessioni RDP
- Test con notifica push e push verificata
- Verifica degli accessi approvati e rifiutati
- Limiti della protezione basata sul Credential Provider

4.3 MFA sulle autenticazioni di dominio

- Come si intercettano le autenticazioni Kerberos/NTLM supportate
- Modalità di monitoraggio e analisi dei log
- Policy MFA applicate a gruppi pilota
- Test di autenticazioni protette ed escluse
- Limiti legati ai ticket Kerberos e alle sessioni già autenticate
- Comportamento fail-open e fail-closed

4.4 Verifica della copertura MFA

- Lettura dei log
- Analisi delle autenticazioni non protette
- Compilazione della matrice di copertura

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO MFA PER ACTIVE DIRECTORY: PROTEGGERE WINDOWS, RDP E ACCESSI PRIVILEGIATI ON-PREMISES

Durata: 2 ore

MODULO 5: PROGETTAZIONE, ROLLOUT E GESTIONE OPERATIVA

5.1 Strategia di implementazione

- Assessment preliminare degli accessi Active Directory
- Account e sistemi prioritari
- Implementazione graduale per gruppi pilota
- Protezione degli account amministrativi e degli accessi remoti
- Estensione progressiva dell'MFA

5.2 Continuità operativa ed eccezioni

- Fail-open e fail-closed: quando usarli
- Account di servizio e accessi non interattivi
- Account locali e autenticazioni offline
- Account di emergenza e procedure di bypass
- Disponibilità del servizio MFA e procedure di rollback

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO MFA PER ACTIVE DIRECTORY: PROTEGGERE WINDOWS, RDP E ACCESSI PRIVILEGIATI ON-PREMISES

Durata: 2 ore

NEXSYS
LEARN IT, TRANSFORM IT

OVERVIEW DEL CORSO

In molte aziende l'MFA protegge Microsoft 365 e i servizi cloud, mentre i logon su Windows, le sessioni RDP e gli accessi amministrativi al dominio dipendono ancora dalla sola password. Il corso mappa i percorsi di autenticazione di un ambiente Active Directory on-premises e confronta le tecnologie per proteggerli: Windows Hello for Business, smart card, Microsoft Entra MFA con NPS Extension, Remote Desktop Gateway e le soluzioni di terze parti basate su Credential Provider o sul controllo delle autenticazioni di dominio.
Nei 45 minuti di laboratorio si verifica dove l'MFA manca davvero e la si applica agli accessi RDP e alle autenticazioni AD. Si chiude con una matrice di copertura e una strategia di rollout per gruppi pilota, con la gestione delle eccezioni e della continuità operativa.

A CHI È RIVOLTO IL CORSO?

Il corso è rivolto a:

- Amministratori di sistema e di Active Directory che devono estendere l'MFA a logon Windows, RDP e accessi privilegiati
- Security engineer e team IT security che devono capire quali autenticazioni di dominio restano scoperte
- IT manager e responsabili infrastruttura che devono scegliere le tecnologie e pianificare il rollout
- Consulenti e system integrator che progettano progetti MFA on-premises per i clienti

COSA SAPRAI FARE ALLA FINE DEL CORSO?

Al termine del corso i partecipanti saranno in grado di:

- Mappare le superfici di autenticazione di un ambiente Active Directory e individuare i percorsi senza MFA
- Distinguere cosa copre Windows Hello for Business e quando servono controlli MFA aggiuntivi
- Valutare gli strumenti Microsoft: smart card, Entra MFA con NPS Extension, RD Gateway e Remote Credential Guard
- Confrontare architetture diverse per copertura, granularità e complessità
- Applicare l'MFA agli accessi RDP e alle autenticazioni di dominio, conoscendone limiti e possibili bypass
- Pianificare un rollout progressivo e documentare la copertura MFA reale

CONTATTI

info@nexsys.it

www.nexsys.it