Macrosoft

Macrosoft s.r.o.

Štefánikova 47

811 04 Bratislava

tel: 02/55 410 308, 0903 28 68 38

e-mail: macrosoft@macrosoft.sk

web: www.macrosoft.sk

OSNOVY KURZOV V PDF

Pripravené pre okamžité stiahnutie

Aktualizované: 21.05.2026

Kybernetická bezpečnosť

Kategória obsahuje prehľad tém a štruktúru výučby jednotlivých kurzov.

Windows Server - Bezpečnosť serveru a domény Active Directory

Kurz 1

Objavte bezpečnostné mechanizmy, ktoré môžete uplatniť vo svojej firemnej doméne. Vysvetlíme Vám základné princípy informačnej bezpečnosti, pojmy bezpečnostných štandardov, ktoré následne aplikujete na zabezpečenie svojich Windows Serverov. Osobitne sa budeme venovať bezpečnostný...

Terminológia základných pojmov informačnej bezpečnosti a ich prepojenie s opatreniami v praxi

- Terminológia základných pojmov informačnej bezpečnosti a ich prepojenie s opatreniami v praxi

Riadenie, manažment informačnej bezpečnosti s ohľadom na prostredie Windows, Windows Server a Active Directory

- Riadenie, manažment informačnej bezpečnosti s ohľadom na prostredie Windows, Windows Server a Active Directory

Bezpečnostné mechanizmy systému Windows Server

- diskusia o službách a prvkoch systému Windows, ktoré môžu prestavovať vektory útokov bezpečná inštalácia a konfigurácia systému Windows

Základné koncepty bezpečnosti Windows Server

- aktualizácia operačného systému aktualizovanie kritických aplikácií antivírusová ochrana fyzická ochrana servera

Skupinová politika ako nástroj na bezpečné jednotné prostredie

- zásady pri nastavovaní hesiel v doméne pravidlá používania a distribúcie hesiel, politika hesiel a zamkýnanie účtov lokálna vs doménová skupinová politika samostatná aplikácia skupinovej politiky na vlastný server podľa medzinárodných štandardov

Aktualizácie Windows

- diskusia o rizikách spojených s (ne)aktualizovanými systémami možnosti využitia služby WSUS (software update service)/WSUS server

Firewall

- základný koncept brány firewall a jej implementácia vo Windows Server softvérové a hardvérové riešenia, ich výhody, nevýhody a využitie zásady správnej konfigurácie, umiestnenie servera do DMZ

Používateľské účty a skupiny používateľov

- rozdiel medzi doménovým a lokálnym účtom typy skupín a ich využitie (zopakovanie) prehľad stratégií prideľovania prístupových práv RBAC + zásady bezpečnosti pri zdieľaní súborov

Koncept vzdialenej súkromnej siete – VPN

- možnosti implementácie vzdialenej siete podľa úrovne bezpečnosti koncepty a scenáre použitia protokolov VPN sietí: PPTP, IPSec, OpenVPN a iné... scenáre využitia a účelnosti

Záverečné zhrnutie

- diskusia o možných ďalších opatreniach na zvýšenie bezpečnosti lokálnej siete záver

Bezpečnosť Windows/Server v kontexte ISO/IEC 27001 a 27002

Kurz 2

Bezpečnosť Active Directory v súlade s požiadavkami noriem ISO/IEC 27001 a 27002. Získate zručnosti v zosúladení existujúceho stavu zabezpečenia Vašej podnikovej domény s normami ISMS. Budete schopní samostatne analyzovať, vyhodnotiť a navrhnúť opatrenia vo Vašej firemnej sieti t...

Zopakovanie základov informačnej bezpečnoti

- Hravou formou si zopakujeme základné pojmy, nevyhnutnú terminológiu z informačnej bezpečnosti, aby sme mohli nadviazať na pokročilé požiadavky noriem. Základné legislatívne akty slovenskej právnej úpravy v tejto oblasti.

Základné princípy normy ISO/IEC 27001

- Základné princípy normy ISO/IEC 27001

Riadenie informačnej bezpečnosti podľa ISO/IEC27001

- v kontexte podnikovej domény postavenej na Active Directory a LAN počítačovej siete. Využívame druhú, najnovšiu revíziu normy 27001 z roku 2013.

Postup aplikácie odporúčaní podľa normy ISO/IEC27002

- Postup aplikácie odporúčaní podľa normy ISO/IEC27002

Politiky informačnej bezpečnosti

- tvorba, skúmanie

Riadenie aktív

- zodpovednosti, vlastníctvo aktív, prijateľné používanie, vrátenie, klasifikácia informácií, označovanie informácií, riadenie médií, likvidácia a prenos médií

Riadenie prístupu

- do domény, informačného systému, všeobecne – prístupy, registrácia a deaktivácia používateľov s ohľadom na práva a povinnosti GDPR a slovenskej právnej úpravy, riadenie privilégií, riadenie utajených autentizačných údajov, skúmanie prístupových práv, riadenie prístupov k systémom a aplikáciám, bezpečné prihlasovanie, praktické ukážky v OS Windows, nastavenie politík pre súlad s touto požiadavkou normy, riadenie a manažment hesiel v kontexte s redundanciou a zastupiteľnosťou, privilegované programy

Kryptografia teoreticky aj prakticky

- nebudeme skúmať matematické postupy ale z pohľadu manažmentu sa budeme venovať kryptografickým opatereniam, správe kľúčov a jednotlivé opatrenia si ukážeme v prostredí MS Windows.

Fyzická bezpečnosť a bezpečnosť prostredia

- perimeter fyzickej bezpečnosti, riadenie fyzických priestorov, zabezpečenie kancelárií, prostriedkov, ochrana pred hrozbami fyzického prostrednia, práca v bezpečnostnej zóne, umiestnenie zariadení a ich ochrana, proces zakúpenia aktíva/zariadenia až po jeho bezpečnú likvidáciu, ako riadiť bezpečnosť aktív mimo organizácie

Prevádzková bezpečnosť

- manažment konfigurácie, dokumentácia prevádzkového postupu, riadenie zmien, segregácia prostredí, opatrenia proti škodlivému kódu, zálohovanie v dennej praxi administrátorov, monitoring a ochrana auditného záznamu, jednotné časové nastavenia

Komunikačná bezpečnosť

- riadenie bezpečnosti na úrovni siete, bezpečnosť sieťových služieb, oddelenie sietí, prenos informácií, zmluvy o výmene informácií, výmena elektronických správ, postupy riadenia systémových zmien

Riadenie incidentov informačnej bezpečnosti

- zodpovednosť a postupy, informovanie o udalostiach informačnej bezpečnosti, posúdenie udalostí informačnej bezpečnosti a rozhodnutia o nich, legislatívne a technické aspekty bezpečnostných incidentov, odporúčaný postup čo robiť pri bezpečnostnom incidente, ponaučenie z incidentov

Kontinuita informačnej bezpečnosti

- plánovanie a vyhodnotenie kontinuity, kedy je vhodná redundancia, kde má a nemá zmysel uvažovať redundantné zdroje a prostriedky, vyhodnotenie kontinuity na základe histórie podniku a súčasných trendov

Bezpečnostné mechanizmy Active Directory

Kurz 3

Ste administrátor Active Directory? Chcete vylepšiť Vašu bezpečnostnú stratégiu tak, aby bola odolná voči súčasným typom útokov? Na rozšírenom kurze o pokročilých bezpečnostných mechanizmoch AD Vám predstavíme nové možnosti, ktorými možno zlepšiť zabezpečenie AD infraštruktúry pr...

Bezpečnostné mechanizmy systému Windows Server - opakovanie

- GPO – možnosti, odkiaľ čerpať námety Windows Firewall (a jeho úskalia v prípade použitia antimalvérových produktov s podobnou funkciou) Windows Defender a ostatné antimalvérové nástroje

Resuscitácia AD

- Dôležité miesta v doméne, ktoré je potrebné kontrolovať a monitorovať

Bezpečné DNS

- Využitie DNS proxy a rozličné scenáre ochrany DNS. Nastavenie bezpečnej replikácie DNS záznamov.

Bezpečná sieť

- Cez ktoré protokoly potrebujú naši používatelia komunikovať?

Firewall pre klientov, servery, radiče AD

- Nastavenie pravidiel prostredníctvom GPO

Používateľské účty a skupiny používateľov

- Prečo každý nemusí byť Domain User?

Model vrstvenia

- Ako ochrániť administrátorské konto pred „šikovným“ používateľom? Využitie vybraných skupín v AD

Problematika lokálneho administrátora

- Nástroj Local Admin Password Solution – áno alebo nie? Ochrana procesu LSASS

Čo všetko môžu naši používatelia?

- Čítanie z LDAP, resp. čítanie databázy AD Čítanie a parsovanie skupinových politík Spúšťanie programov, exfiltrácia

Ako získať večný život?

- Perzistencia na pracovnej stanici, serveri Perzistencia v AD Odhaľovanie perzistencie základnými ale aj sofistikovanými postupmi

Záverečné zhrnutie

- diskusia o možných ďalších opatreniach na zvýšenie bezpečnosti domény záver

Upozornenie

- Jedná sa o rozšírený kurz – oproti štandardnému kurzovému dňu je na tento kurz vyčlenených
- 6 hodín
- . V prípade záujmu je možné prispôsobiť témy kurzu na mieru a prispôsobiť ho potrebám konkrétnej inštitúcie (napr. pre účely školenia IT oddelení, Manažérov informačnej bezpečnosti a pod.)

Kybernetická bezpečnosť II. - pokročilí

Kurz 4

Tento špecializovaný technický kurz sa zameriava na analýzu sieťovej bezpečnosti na jednotlivých vrstvách OSI modelu. Účastníci získajú praktické znalosti o sieťových útokoch, obranných mechanizmoch a implementácii bezpečnostných riešení najmä na Cisco zariadeniach. Kurz kombinuj...

Sieťové modely a útoky

- OSI & TCP/IP Bezpečnosť podľa hladín OSI modelu Layer 2 druhá hladina Rozdelenie tipy útokov Mac address flooding VLAN hopping VLAN double tagging DHCP starvation DHCP spoofing ARP spoofing SPANNING tree attack CDP reconnaissance

Návrhy a sieťové bezpečnostné riešenia

- Bezpečnostná metóda: Port security Bezpečnostná metóda: DHCP snooping Dynamic ARP inspection PortFast and BPDU Guard

Layer 3 tretia hladina

- Basic Cisco IOS firewall: Acess listy Standard Extended Odporúčania NAT Static NAT Dynamic NAT PAT (NAT overload) Ako pracuje logika nat, routing a ACL na Cisco? Výhody a nevýhody NAT

Zariadenia vyšších hladín 4-7

- ESA WSA AAA

Cvičenia

- Základy práce s Wireshark-om Snifovanie CDP Snifovanie TELNET Skenovanie siete nMAP a iné nástroje

Kybernetická bezpečnosť I. - základy

Kurz 5

Tento kurz poskytuje účastníkom základné znalosti z oblasti kybernetickej bezpečnosti s dôrazom na praktické aplikácie a súčasnú legislatívu. Kurz kombinuje teoretické základy s praktickými príkladmi a reálnymi scenármi, čím pripravuje účastníkov na efektívnu implementáciu bezpeč...

Smernica NIST 2

- Základné vysvetlenie Čo to pre nás znamená Zákon o kybernetickej bezpečnosti Zákon 69/2018 Najznámejšie útoky Symptómy hacknutia

Data privacy / Súkromie údajov

- Kto všetko zbiera o nás údaje? Ochrana osobných údajov Dávaš si pozor, čo zdieľaš? Na čo si dávať pozor Kryptovanie údajov na disku Vymazávanie dát

Spôsoby ochrany

- Hardware Software školenia rozdelenie firewallov Model viacnásobnej ochrany

Monitoring siete

- Čo nám chodí po sieti ICMP SNMP NETFLOW

Overenie bezpečnosti siete

- Penetračné testy – čo to je?

Svetové a národné bezpečnostné autority

- CSIRT, SK-CERT

Sieťová bezpečnosť

- Rozdelenie zraniteľností Rozdelenie a popísanie hrozieb Rozdelenie útokov podľa typov Tvorba hesiel Sila hesiel Útoky na heslá

Bezpečnosť bezdrôtových sietí

- Rozdelenie WIFI Odporúčania Verejné wifi Odporúčania Bluetooth Odporúčania Domáce wifi Zraniteľnosť WIFI video1