Macrosoft
Vzdelávanie s trvalým efektom

Macrosoft s.r.o.
Štefánikova 47
811 04 Bratislava

tel: 02/ 55 410 308,
0948 88 40 88
e-mail: macrosoft@macrosoft.sk

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

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 tak, aby pokrývali identifikované riziká a eliminovali nežiaduce udalosti.

- UPOZORNENIE - Kurz je možné absolvovať iba prezenčnou formou. Online forma kurzu v tomto prípade nie je možná. Je možné kurz realizovať u Vás vo firme a zohľadniť individuálne špecifiká oblastí, ktoré potrebujete pokryť.
- Kurz prepája technické princípy konceptov zabezpečenia OS Windows, Server, domény Active Directory s manažérskymi rozhodnutiami v podniku.

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

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

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

Macrosoft s.r.o.
Štefánikova 47
811 04 Bratislava
tel: 02/ 55 410 308,
0948 88 40 88
e-mail: macrosoft@macrosoft.sk

- 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