Közigazgatási Kibervédelmi Eszköztár

NKI White Paper

NEMZETI KIBERVÉDELMI INTÉZET

Tartalom

Bevezetés 3

Humán eredetű kockázatok 5

Felhasználói tudatosság 9

Elektronikus levelezés (e-mail) 13

Belső hálózati infrastruktúra védelme 17

Káros kódok elleni védelem 23

Vagyontárgyak (Data, HW, SW, Supply Chain) 27

Elavult eszközpark 31

Vezeték nélküli hálózatok biztonsága 35

Távoli munkavégzés 37

Magántulajdonú eszközök (BYOD) 41

Fizikai biztonság 45

Bevezetés

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézete (a továbbiakban: NKI) az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.) alapján, illetve „a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól” szóló 185/2015. (VII. 13.) Korm. rendelet alapján nem kötelező érvényű állásfoglalásokat, ajánlásokat adhat ki.

Jelen „Fehér Könyv” célja, hogy segítséget nyújtson a felhasználóknak, az informatikai üzemeltetőknek és vezetőknek, annak érdekében, miként növelhetik a meglévő biztonsági szintet, csökkenthetik a kockázatoknak való kitettséget, illetve milyen elvárt magatartásformát javasolt követniük.

A „Fehér Könyv” összeállítása során az NKI incidenskezelési tevékenysége során feldolgozott magas, vagy kritikus kockázati besorolású incidensek vizsgálati eredményei kerültek felhasználásra. A legmagasabb kockázati besorolású incidensek körébe olyan célzott támadások szerepelnek, melyeknek a célpontjai a közigazgatási szervek, különböző minisztériumok, valamint azok háttérintézményei. Az NKI szakértői ezen incidenseket alapul véve határozták meg azoknak a fenyegetéseknek a körét, melyek szerepet kaptak a kiadásra kerülő Fehér Könyvben. Ezeket a fenyegetéseket egyenként megcélozva a szakértők javaslatokat, jól bevált gyakorlatokat gyűjtöttek, melyek – az NKI reményei szerint – segítséget nyújthatnak mind a felhasználók, mind az informatikai üzemeltetők és döntéshozók, illetve az Informatikai Biztonsági Felelősök számára, hogy az üzletileg fontos rendszerek, adatok és eszközök biztonsága az elvárt szinten tartható legyen.

A „Fehér Könyvben” egyenként felsorakoztatásra kerülnek az NKI által összegyűjtött fenyegetések, majd az adott fenyegetéshez tartozó, különböző szintű biztonsági kontrollokra vonatkozó javaslatok. A könnyebb azonosítás érdekében az eltérő szintek különböző piktogramokkal lettek megjelölve, ezzel is segítve az irat követhetőségét. Az adatok olvashatóságát és feldolgozását az egyes fejezetek felosztása oly módon is segíti, hogy a fő fejezetek minden esetben páratlan oldalra esnek, így támogatva a könnyebb tájékozódást a dokumentumban. Emiatt, illetve az olvashatóság miatt javasolt a dokumentum „füzet elrendezésű” kinyomtatása, amennyiben papíron is szeretné az olvasó a dokumentumot forgatni.

Jelen dokumentumban megfogalmazott különböző szintű biztonsági javaslatok, valamint eljárások segítségül szolgálhatnak a biztonsági szabályrendszer alapjainak lefektetésében, és a szükséges biztonsági beállítások felülvizsgálatában is.

A Közigazgatási Kibervédelmi Eszköztár egy élő, folyamatos frissítés alatt álló ajánlásgyűjtemény. A dokumentummal, annak formájával, tartalmával kapcsolatos észrevételeket, javaslatokat, a cert@govcert.hu e-mail címen fogadják kollégáink.

Humán eredetű kockázatok

A legtöbb kormányzati intézményben, illetve gazdasági társaságokban is előfordulhatnak meggondolatlan, de akár elégedetlen/rosszindulatú belső munkavállalók is. Tekintettel arra, hogy e felhasználók már rendelkeznek – a legtöbb esetben a szükségesnél több – jogosultsággal a rendszerben, tevékenységük akár akarattal, akár akaratlanul is, a legnagyobb veszélyt jelenthetik a szervezet számára, ezért a belső felhasználók képzése, tudatosítása és az elvárt helyes magatartás különböző biztonsági kontrollokkal történő kikényszerítése alapvető érdeke minden szervezetnek.

Felhasználói javaslatok

- **Ismerjük meg és alkalmazzunk a jóváhagyott eljárásrendeket:** Az Informatikai Biztonsági Szabályzat megalkotása során a szakemberek törekedtek a használhatóság és a biztonság egyensúlyának fenntartására. A korlátozó szabályok a biztonsági szint növelése érdekében kerültek bevezetésre, betartásukkal a szervezet egészének informatikai biztonsága nő, ezzel párhuzamosan csökken az egyes fenyegetésekkel szembeni kitettség.

- **Tanúsítsunk biztonságtudatos magatartást, jobb kérdezni, mint egy hibás művelettel jelentős kárt okozni a szervezetnek:** Ha nem vagyunk biztosak abban, hogy a folyosón talált USB kulcsot be lehet-e dugni a hivatali számítógépbe, inkább kérdezzük meg a kollégákat, vagy az üzemeltetést, ezzel lehet, hogy jelentős kárt előzünk meg.

- **Korlátozzunk a munkavégzéssel közvetlenül nem összefüggő tevékenységet; a munkahelyi számítógépen vagy a munkahely által biztosított laptopon ne böngésszünk a munkavégzéssel nem összefüggő weboldalakat:** Egy gyors pillantás a legfrissebb hírekre még senkinek sem ártott, azonban egy gyors kattintás egy éppen lejáró nyereményjátékra már igen. Internetezzünk tudatosan, a céltalan böngészést pedig hagyjuk a szabadidőre.

- **Gondolataink interneten történő megosztása során kerüljük az érzékeny, vagy a munkahelyre hátrányos információk megosztását:** Egy meggondolatlanul publikált gondolatot akár arra is fel lehet használni, hogy további belső információkat szerezzen meg egy rosszindulatú támadó, de a nyilvánosság számára elérhetően megfogalmazott kritika is árthat a szervezet jó hírének. Fontoljuk meg, milyen gondolatokat teszünk közzé a munkahelyünkkel kapcsolatban.

- **Legkisebb jogosultság elve:** A felhasználói hozzáférések szigorú felügyelete és a jogosultságok beállítása oly módon történjen, hogy az egyes felhasználók munkájukat a lehető legkevesebb jogosultság megadásával tudják ellátni.

- **Data Leak Prevention (DLP) rendszerek alkalmazása:** A védendő, bizalmas adatok, „kiszivárogtatásának" megelőzésére céljából speciális, erre a célra készített rendszerek alkalmazása javasolt, melyek a felhasználói tevékenység nyomon követésével, mintázatok és anomália detekció segítségével generálnak riasztásokat a gyanús tevékenységekről (pl.: a felhasználó e-mail útján számos üzenetet továbbít meghatározott címre).

- **Access Based Enumeration bevezetése:** Az Access Based Enumeration technológia engedélyezése által az SMB/CIFS alapú megosztást kiszolgáló operációs rendszer eleve nem jeleníti meg azon könyvtárakat, melyekhez a felhasználó nem rendelkezik jogosultsággal. Ez a megoldás, pl.: projektek esetén meggátolja, hogy a felhasználó a mappák elnevezéséből adódóan olyan információhoz jusson, melyhez egyébként nem volna joga.

- **Anomália alapú detekció bevezetése:** Az anomália alapú vizsgálatot végző rendszerek alkalmazkodó (ún. adaptív) tanulásukat követően biztosítják a rendellenes események felderítését (pl.: felhasználó olyan könyvtárakban másol/módosít adatot, ahol még sosem dolgozott), mely ennek köszönhetően a belső szivárogtatások megelőzésére is alkalmazható.

- **Privilegizált felhasználók fokozott felügyelete:** A rendszerben jelen lévő, speciális privilégiumokkal rendelkező – tipikusan üzemeltető rendszergazda – felhasználók tevékenységének monitorozására és rögzítésére kifejlesztett alkalmazások használata (pl.: speciális naplózás, tevékenység követés, vagy akár a munkamenet vizuális rögzítése) segíti a magas jogosultsági szinttel való visszaélések felderítését.

- **Többfaktoros hitelesítés használata:** A használt munkaállomások, valamint egyéb bejelentkezési felületek esetén – legalább a privilegizált felhasználók számára – többfaktoros hitelesítés használata javasolt annak érdekében, hogy egy esetleges biztonsági incidens kivizsgálása esetén egyértelműen meghatározható legyen az adott tevékenységhez köthető valós személy (pl.: naplóállományban szerepel a felhasználónév, de nem eldönthető minden kétséget kizáróan, hogy nem csak megszemélyesítésről volt-e szó).

- **Identity Management (IDM) rendszerek bevezetése:** A felhasználói fiókok és egyéb hozzáférések megfelelő helyen, megfelelő időben, és jogosultság mértékében való központosított, átlátható kezelése érdekében kifejezetten erre a célra szánt, vállalati szintű identitáskezelést támogató szoftver használata javasolt azon rendszerek esetében, ahol több, kiemelt jogosultsággal rendelkező felhasználói fiók is felvételre került.

- **Csoporttagság alapú jogosultságok:** Az egyéni felhasználói fiókokhoz rendelt jogosultságok helyett kizárólag a szakmai irányelvekkel egyeztetett módon, csoporttagság alapú – ez által könnyedén átlátható és naplózható – jogosultságok használata célszerű.

- **Részletes naplózás:** A humán eredetű kockázatok minimalizálása, valamint az esetleges biztonsági incidensek utólagos kivizsgálása érdekében részletes – hosszabb távú - naplózás bevezetése javasolt (pl.: e-mail forgalom, felhasználói tevékenység, fájlszerverek naplói, tartományi- és egyéb szolgáltatások, valamint szakrendszerek ki/bejelentkezései és tevékenységei stb.).

- **Naplóelemző szoftverek bevezetése:** Az összegyűjtött naplóállományok elemzése és vizualizációja érdekében speciális, erre a célra kifejlesztett naplóelemző szoftverek használata javasolt, melyek képesek szemmel jól áttekinthető, vagy akár egyszerűen visszakereshető módon megjeleníteni a felhasználói tevékenységet (pl.: a fájlszerver eredendően „feldolgozhatatlan" logsoraiban felhasználónév és idő vonzatában könnyedén megjeleníthető a pontos fájlművelet szintű tevékenység).

Eljárásrendek

- **Hozzáférés kontroll:** Biztosítani kell, hogy az egyes hálózati eszközökhöz, megosztásokhoz csak azok férjenek hozzá, akiknek az valóban indokolt, a felesleges hozzáférési jogosultságokat pedig haladéktalanul meg kell szüntetni az esetleges visszaélések megakadályozása érdekében. Javasolt továbbá a hozzáférési jogosultságok folyamatos figyelemmel kísérése, az erre vonatkozó nyilvántartások folyamatos frissítése. A hozzáféréseket központilag, átlátható módon szükséges biztosítani úgy, hogy az egy esetleges felmérés/audit során is könnyedén visszaellenőrizhető legyen.

- **Távmunka:** Otthoni munkavégzés esetén a távoli hozzáférést és a távolról elérhető szolgáltatások listáját külön szükséges meghatározni.

- **Folyamatos biztonsági ellenőrzés:** A begyűjtött, naplóelemző rendszer által összesített és prezentált jelentések rendszeres áttekintése.

- **Adatok bizalmasságának biztosítása:** A meglévő rezsimintézkedések elemzése és felülvizsgálata abból a szempontból, hogy azok a rendszerekhez, szoftverekhez és elérhető adatokhoz a legszigorúbb hozzáférési feltételeket definiálják.

- **Kiemelt üzemeltetői jogú hozzáférések leválasztása, monitorozása, auditálása:** A rendszerekben jelenlévő jogosultságokról teljes körű, lehetőleg mátrix jellegű jogosultsági nyilvántartást kell vezetni és naprakészen tartani. A szervezetbe belépő, és/vagy új szerepkörbe kerülő felhasználók jogosultságait a munkavégzéshez elégséges, legkisebb szintű hozzáférést biztosító jogosultságokkal kell beállítani. A jogosultságok nyilvántartásának ki kell terjednie az egyes alkalmazások, rendszerek által használt technikai felhasználók jogosultságainak számbavételére is. A felhasználókat csoportokba kell sorolni, és lehetőség szerint csoportházirendek szerint kezelni. Az egyes felhasználói csoportokhoz, beleértve a technikai és adminisztrátori csoportokat is, jelszópolitikát kell kialakítani a jelszavak komplexitására és érvényességi idejére vonatkozóan. A hozzáférések igénylésére, engedélyezésére, módosítására, visszavonására az egyes rendszerek felett adatgazda szerepet betöltők bevonásával adminisztratív szabályokat kell bevezetni, és dokumentálni kell a jogosultságkezelés folyamatát. A jogosultságokat kezelő technikai munkatársaknak vissza kell jelezniük a módosítások elvégzéséről a feladatvégrehajtást elrendelő, és a felhasználó felé. A felhasználó köteles a vonatkozó szabályzatokat megismerni, illetve a rendszer használatba vételekor megváltoztatni a jelszavát, amelyet később nem oszthat meg sem a rendszer adminisztrátoraival, sem más felhasználókkal.

- **Az incidenskezelésben részt vevő, IT biztonsággal megbízott munkatársak azonosítása:** Azonosítani kell az informatikai biztonsággal kapcsolatos feladatokban résztvevő munkatársakat, az általuk betöltött szerepkörök feladatait és hatásköreiket (RACI mátrix) majd azokat rögzíteni kell a vonatkozó munkaköri leírásokban.

- **Személyi biztonsági feltételek megteremtése:** Az elektronikus információs rendszerek védelme szempontjából, a bennük kezelt adatok természetétől függően különböző feltételeknek kell megfelelniük a rendszereket használó és üzemeltető felhasználóknak. Nem minősített adatokat kezelő elektronikus információs rendszerek esetében ajánlott a felhasználókkal titoktartási nyilatkozatot aláíratni, tőlük hatósági erkölcsi bizonyítvány benyújtását kérni, továbbá a gazdasági döntések meghozatalában, és előkészítésében résztvevő munkavállalók esetében éves rendszerességgel vagyonnyilatkozat és összeférhetetlenségi nyilatkozat megtételét megkövetelni. A személyi biztonsági feltételek meglétét az elektronikus információs rendszerhez hozzáférést kapó, a szervezettel nem munkavállalói jogviszonyban lévő külsős felhasználók esetében is meg kell követelni. Külsős munkavállalót ne hagyjunk felügyelet nélkül.

- **Rendszeres biztonsági szint értékelés:** Az elektronikus információs rendszereket bizalmassági, sértetlenségi és rendelkezésre állási elvárásaik alapján biztonsági szintbe kell sorolni. Az elvárt és valós biztonsági szint közötti különbségek feltárásának érdekében biztonsági szint értékelés keretében fel kell mérni az adott időpillanatban a tényleges biztonsági szintet, és intézkedési tervet kell létrehozni a nemmegfelelőségek kezelésére.

Felhasználói tudatosság

A biztonságtudatosság a felelős és körültekintő, a belső szabályoknak és normáknak megfelelő munkavégzésnél kezdődik. Minden munkavállaló számára, aki hozzáfér a szervezet informatikai hálózatához, fontos hogy megfelelő alapképzés kerüljön biztosításra. Ideális esetben a munkavégzés megkezdése előtt sor kerül egy belső biztonsági képzésre, majd ezt követően kerül sor az Információbiztonsági Szabályzat oktatására. Az IBSZ-t a munkaviszony során időszakosan oktatni, az abban foglaltak betartását ellenőrizni szükséges.

Felhasználói javaslatok

- **Az Informatikai Biztonsági Szabályzatban foglalt szabályok ismerete és betartása:** A használhatóság és a biztonságosság közti törékeny egyensúly felett az IBSZ rendelkezései őrködnek, ha ezeket nem tartjuk be, a biztonság sérülhet.

- **Részvétel az Informatikai Biztonsági Felelős által tartott (biztonsági) képzéseken:** Az ilyen jellegű képzések az esetleges incidensek megelőzését szolgálják, illetve felfrissítik a meglévő ismereteket, hogyan lehetséges a hatékony, ám biztonságos munkavégzés.

- **Biztonságtudatos munkavégzés:** Munkánk során, ha szokatlan, nem üzemszerű működést tapasztalunk, jelezzük azt az üzemeltetőnek, mintsem mi legyünk egy biztonsági esemény kiindulópontja.

Technikai Kontrollok

- **Gyakorlatok:** Pszichológiai megtévesztő (social engineering) vizsgálatokkal felmérhető a munkatársak biztonságtudatos magatartása. A vizsgálatok keretében ellenőrizhető, hogy egy megtévesztő tevékenységgel milyen információk tudhatóak meg a felhasználóktól, valamint magatartásukkal (pl.: jelszavak és szenzitív információk tárolása) hogyan nyújthatnak segítséget egy célzott támadás esetén. A vizsgálatot követően tudatosító előadás megtartása javasolt.

- **Bring Your Own Device (BYOD) szabályainak kialakítása:** Napjainkban elterjedt, hogy a munkáltató engedélyezi a felhasználók számára a saját, magántulajdonú eszközök használatát munkavégzés céljából. Ezen eszközöknél jelentős figyelmet kell arra fordítani, hogy azokat kizárólag biztonságos módon használja a felhasználó. Minden esetben intézkedést kell kialakítani a megfelelő jelszóhasználatra és alkalmazáshasználatra, valamint az eszközök operációs rendszereinek biztonságos kialakítására.

- **Felhőhasználat:** A szervezet által felügyelt felhő szolgáltatással biztosítható az otthoni munkavégzés, valamint szabályozható a felhasználók számára megismerhető információk köre. A felhőszolgáltatás – távoli asztal kialakításával – lehetőséget biztosít, hogy a munkavállaló ne a saját számítógépén dolgozzon, így – megfelelően szabályozott környezettel – csökkenthető az adatszivárgás lehetősége. A felhőszolgáltatás segítségével nincs szükség minden munkatárs számítógépére célszoftvert (pl.: irodai szoftvercsomag, grafikai programok) vásárolni, elegendő azokat a munkavégzést biztosító kiszolgálóra feltelepíteni.

- **Jelszókezelő rendszerek használata:** A jelszókezelő alkalmazásokban a felhasználók biztonságosan tárolhatják a bejelentkezési adataikat. A megfelelő jelszóválasztásról és az alkalmazás használatáról képzés megtartása, vagy használati útmutató kiadása javasolt.

- **Képzés és számonkérés:** A rendszerek és alkalmazások használatáról bevezetéskor és jelentősebb fejlesztés esetén oktatás megtartása szükséges. A felhasználók és üzemeltetők számára eltérő képzés megtartása javasolt, amelyet követően a – rendszert érintő – biztonságtudatos felhasználást számon kérő teszt kitöltése segíthet a megértés felmérésében.

- **Menedzsment – IBF – Fejlesztő – Felhasználó együttműködés:** Alkalmazásfejlesztés során folyamatos egyeztetés szükséges a szervezet és a fejlesztők között. Egy fejlesztés során az Informatikai Biztonsági Felelős által meghatározott biztonsági feltételekhez és a felhasználók által kívánt funkciókhoz a fejlesztőnek rugalmasan alkalmazkodnia kell, amely során felmerülő költségeket a szervezet felső vezetésével egyeztetnie kell.

- **Privát élet / munkahelyi feladatok elválasztása:** A védelmi rendszereket úgy kell kialakítani, hogy a szervezet által biztosított eszközöket a felhasználók kizárólag, indokolt esetben használják magáncélra, így csökkenthető az információszivárgás kockázata. Meg kell határozni, hogy kommunikációs célra milyen alkalmazásokat vagy rendszereket használhatnak a felhasználók.

- **Tudatosító képzések:** A munkavállalókat munkaviszonyuk létesítésekor, majd ezt követően rendszeresen tudatosító képzésben kell részesíteni. A képzésnek ki kell terjednie az IBSZ és más biztonsági szabályzók valamint az elvárt, biztonságtudatos magatartásformák ismertetésére, illetve korábbi incidensekkel kapcsolatos tapasztalatok megosztására.

- **Eseti tudatosító képzések:** Nagyobb hatású incidenseket, vagy kampányokat követően a felhasználók és biztonsági szakemberek részére eseti tudatosító képzés megtartása lehet indokolt, mely során bemutatásra kerül az incidens, és a résztevők megismerik az incidens kezelése során szerzett tapasztalatokat.

- **Felhasználói kompetenciák ismerete:** A szervezetnek ismeretekkel kell rendelkeznie arról, hogy a rendszert használó egyes személyek milyen mértékű informatikai, illetve információ-biztonsági ismeretekkel rendelkeznek. Ennek tükrében kell kialakítani a megfelelő védelmi intézkedéseket. Elengedhetetlen a rendszer használatával érintett személyek rendszeres továbbképzése, akár belső, akár külső szakemberek segítségével.

Elektronikus levelezés (e-mail)

Az elektronikus levelezés és a hozzá kapcsolódó infrastruktúra a hivatali munkavégzés terén napjaink egyik legkiterjedtebb módon használt munkaeszköze. Legtöbb esetben ezen keresztül tartjuk a kapcsolatot a munkatársakkal, de a feladatokat is leggyakrabban e-mail útján kapjuk meg. Sajnos, mivel az elektronikus üzenet mostanra az egyik legelterjedtebb céges kommunikációs formává vált, a legtöbb munkavállalót fenyegető veszélyt is ez a megoldás hordozza. Az internetes levelezés védelme a hivatali infrastruktúra védelmének első, legfontosabb vonala.

Felhasználói javaslatok

- **A hozzáférésekhez használt jelszavak indokolatlan átadása tilos!** A „Lépj be a gépembe, itt a jelszavam” kijelentést követően a biztonsági esemény kivizsgálásakor már ez hangzik el: „Nem én léptem be, hanem a kollégám.” - ezt pedig már nehéz bizonyítani, inkább kerüljük el az ilyen helyzeteket!

- **Rendszeresen változtassunk meg a jelszavainkat, és ne használjunk „újrahasznosított” jelszavakat:** A régi jelszó majdnem olyan rossz, mint az egyszerűen kikövetkeztethető jelszó. Kerüljük ezeket!

- **Ismeretlen feladótól származó levélben érkezett csatolmányt csak abban az esetben nyissunk meg, ha meggyőződtünk a feladó személyéről és jó szándékáról:** A szervezetek informatikai rendszerét ért támadások leggyakrabban az elektronikus levélben küldött káros mellékletek felhasználó általi megnyitásával kezdődnek. Legyünk körültekintőek!

- **Amennyiben a levél, vagy csatolmánya gyanús, rossz nyelvezetű, szokatlan megfogalmazású, általános címzésű vagy sürgető hangvételű, fokozott óvatossággal járjunk el:** Az adathalász levelek, vagy káros kódot tartalmazó e-mailek legtöbbször tartalmaznak valami furcsaságot. Vegyük ezeket észre, és ne dőljünk be nekik!

- **Hiperhivatkozásokra (linkekre), furcsa csatolmányokra csak alapos körültekintést követően kattintsunk:** A hiperhivatkozások különösen veszélyesek, mert lehet, hogy nem is a keresett portálra, hanem egy káros kódot tartalmazó (meghamisított) oldalra irányítanak, ami a látogatást követően ezt a kódot fel is telepíti a gépünkre, vagy illetékteleneknek továbbítja a gyanútlanul begépelt személyes vagy pénzügyi adatainkat.

- **Gyanús, ismeretlen csatolmányú/szövegezésű levelet semmilyen formában ne küldjünk tovább kollegáknak:** Amennyiben egy beérkező levelet valamilyen okból gyanúsnak találunk, ne továbbítsuk azt senkinek sem, hanem azonnal értesítsük az üzemeltetést, vagy járjunk el a biztonsági szabályzatban foglaltaknak megfelelően.

- **Látszólag ismert feladótól érkező, szövegezésében vagy témájában gyanús levelek is lehetnek károsak**: A támadók gyakran élnek a megszemélyesítés, megtévesztés eszközeivel.

- **Többrétű levélszemét elleni (anti-spam) technológia bevezetése:** Az általános anti-spam megoldások mellett akár két különböző gyártó termékének, egymástól elkülönített módon történő alkalmazása is célszerű lehet, úgy, hogy az egyik megoldás a levélforgalomba ténylegesen be tudjon avatkozni, eltávolítva a káros leveleket (pl.: egy alapvető anti-spam rendszer a klasszikus káros levelek kiszűrésére), valamint „mögötte" üzemel egy, a spam szűrőtől elszeparált rendszer a célzott támadások kivédésére.

- **Futtatható állomány mellékletek korlátozása:** A gyakran használt – sok esetben leginkább veszélyt rejtő – futtatható állományok levélmellékletként való továbbításának tiltása, vagy erre vonatkozó korlátozás bevezetése ajánlott.

- **Belső levélforgalom védelme:** Javasolt a peremvédelmi eszközök (ún. „mail gateway") alkalmazásán túl antivírus megoldás implementálása a leveleket kiszolgáló adatbázis szerveren is, mely által a rendszerbe már korábban bejutott káros kódok is kiszűrésre kerülhetnek, amint definíciós állományuk/mintázatuk elterjed, publikálásra kerül.

- **Sender Policy Framework (SPF) rekord használata:** A szervezet tartományát (domain) felhasználó, hamisított e-mail forgalom kiszűrése céljából javasolt a megfelelő, lehető legszigorúbb SPF rekord beállítása a DNS szervereken. Ez által pontosan definiálásra kerül, mely kiszolgálók küldhetnek elektronikus üzeneteket a szervezet nevében, lehetőséget adva a fogadó levelezőszerver oldalán történő, kézbesítést megelőzően végrehajtott ellenőrzésre, így elkerülhető, hogy a szervezet nevében rosszindulatú személyek hamisított elektronikus leveleket küldjenek.

- **Domain Keys Identified Mail (DKIM) beállítása:** A DKIM protokoll nyilvános kulcsú titkosítás használatával a levelező kiszolgáló a levél fejlécében elhelyezett digitális aláírással látja el a levelező szerver által kiküldött leveleket. A kiszolgáló publikus kulcsát a feladó névtartományának (domain) névszervere szolgáltatja, DNS rekordként.

- **Fordított névfeloldás (reverse DNS lookup) ellenőrzése:** A megbízható levélforgalom működése érdekében a szervezet e-mail kiszolgálóinak rendelkeznie kell nem csak „A”, hanem „PTR” DNS rekordokkal, ez által egy megadott IP címről pontosan visszaellenőrizhető annak FQDN-je. Egyúttal a saját weboldalon is megkövetelhető a „PTR” rekordok visszaellenőrzése.

- **Open relay kiszolgálás tiltása:** A használt levelezőszerverek kizárólag hitelesítést követően, ismert feladóktól/entitásoktól fogadjanak levelet továbbküldés céljából. Ezzel a megoldással elkerülhető, hogy támadók a szervezet kiszolgálóin keresztül jogosulatlanul küldjenek káros vagy kéretlen leveleket.

- **SSL technológia használata:** A külön biztonsági mechanizmusokkal nem rendelkező protokollok (pl.: IMAP4, POP3, SMTP, WEB felület) védelme érdekében szükséges az SSL/TLS szolgáltatások használata, külső, elismert tanúsítványszolgáltató által kibocsájtott tanúsítványok alkalmazásával.

- **Elavult protokollok mellőzése:** A levelezés biztonságos elérése érdekében mindenképp javasolt az elavult (pl.: SSLv2, SSLv3, TLS1.0) protokollok mellőzése.

- **Web elérés korlátozása:** Az e-mailek megjelenítését lehetővé tévő Web interfész használatát a lehetőségek mentén célszerű korlátozni (pl.: Geo-IP alapú tiltás).

- **Részletes naplózás:** A vállalati levelezés tekintetében javasolt az esetleges biztonsági incidensek utólagos kivizsgálásának támogatása érdekében részletes – hosszabb távú – naplózás bevezetése (pl.: sikerességtől függetlenül a felhasználók ki-bejelentkezése, tevékenységük metaadatai, forrás IP címük, stb.).

- **Biztonságos levelezés:** Gondoskodni kell az SPF rekord (Sender Policy Framework) bevezetéséhez szükséges körülmények kialakításáról és bevezetéséről az e-mail fejlécek meghamisításának megelőzésének érdekében.

- **Bizalmasság garantálása:** Biztosítani szükséges, hogy az érzékeny információkat tartalmazó levelezés kizárólag titkosított (PGP) kommunikáció alkalmazásával kerüljön végrehajtásra, vagy a csatolt melléklet titkosított formátumban kerüljön továbbításra, aminek jelszava másik csatornán (pl.: SMS üzenetben) kerüljön elküldésre.

- **Tudatosító kampányok:** Javasolt az adathalászattal és az e-mail veszélyeivel kapcsolatos rendszeres tájékoztató, tudatosító kampányok megtartása.

- **Hozzáférések felülvizsgálata:** A munkavégzéshez szükséges legkisebb jogosultságokat biztosító hozzáférések kialakítása kívánatos egy biztonságos rendszer kialakításakor. A szervezeti változások miatt bekövetkező hozzáférési adatmódosulásokat, a változások életbelépése előtt érvényesíteni kell a rendszerben a felmerülő humán kockázatok csökkentése érdekében, például az elbocsátásra kerülő munkavállaló jogosultságait még a vele való (munkaviszony megszűnés) közlés előtt vissza kell vonni. A hozzáféréseket rendszeres időközönként ellenőrizni kell, biztosítandó, hogy továbbra is csak a szükséges mértékű engedélyeket tartalmazzák.

- **Intézményi levelezés használatára vonatkozó szabályzat elkészítése:** A lehető legpontosabban szükséges meghatározni, hogy az egyes munkavállalók milyen feltételek mellett vehetik igénybe a levelezés szolgáltatást, valamint ki az, aki rendelkezhet kívülről is elérhető címmel, illetve ki az, aki küldhet levelet a szervezeten kívülre. Az elektronikus levelekkel kapcsolatos mérőszámokat (maximális címzettek száma, méretkorlát, csatolmányok mérete, formája, darabszáma, e-mail törzsének formája [szöveg, html], stb.) is ajánlott meghatározni.

- **Inaktív fiókok törlése, archiválása:** A szabályzásban meg kell határozni, hogy mennyi a fiók zárolását megelőző maximális inaktivitási idő, milyen időtartamot követően kerül a postafiók archiválásra és törlésre, illetve ki kell alakítani az intézményi szintű archiválási szabályrendszert is.

- **Naplózás:** A biztonsági incidensek utólagos kivizsgálása érdekében a szolgáltatással kapcsolatos naplóállományok külön kiszolgálón, archiválható módon történő gyűjtése és tárolása javasolt.

- **Szolgáltatói és belső tanúsítványok kezelése, kezelésének rendje:** A belső és külső hálózati adatforgalmat (pl.: smb kapcsolatokat, levelező protokollokat, webalkalmazások elérését) titkosított kapcsolaton keresztül érdemes megvalósítani. A titkosításhoz használt tanúsítványokat egy belső tanúsítvány kiadó (Certificate Authority) alkalmazásával, illetve annak a rendszer tanúsítványtárjaiba való felvételével lehet könnyen központilag kezelni, valamint megújítani. A belső tanúsítványtárak kezeljék a rendszerben használt szoftverek és eszközök gyártói tanúsítványait is, így hatékonyabban kikényszeríthető, hogy csak a tanúsított alkalmazások kerülhessenek a szerverekre, illetve a munkaállomásokra.

- **Rendszeres biztonsági szint értékelés:** Az elektronikus információs rendszereket bizalmassági, sértetlenségi, valamint rendelkezésre állási elvárásaik alapján biztonsági szintbe kell sorolni. Az elvárt és valós biztonsági szint közötti különbségek feltárásának érdekében biztonsági szint értékelés keretében fel kell mérni az adott időpillanatban a tényleges biztonsági szintet, majd intézkedési tervet javasolt létrehozni a nemmegfelelőségek kezelésére.

Belső hálózati infrastruktúra védelme

A nagy kiterjedésű belső hálózati infrastruktúra védelme fokozott kihívások elé állítja az informatikai szakembereket. Egyrészt a hálózathoz kapcsolt végfelhasználói- és más aktív eszközök számossága miatt, másrészt a különböző, földrajzilag elkülönült telephelyek biztonságos, illetve magas rendelkezésre állású összeköttetéseinek biztosítása érdekében. Érdemes megfontolni, hogy az egyes hálózati szegmensekben (telephelyek, vagy célrendszerek, kiszolgálók hálózatai) található felhasználóknak, szolgáltatásoknak szükséges-e elérniük egy másik szegmensben lévő felhasználót vagy szolgáltatást.

Felhasználói javaslatok

- **Csak azokat a hálózati erőforrásokat használjuk, amelyek a munkánkhoz feltétlenül szükségesek:** Több szervezetnél is előfordulhat az a helytelen gyakorlat, miszerint egy munkatárs digitális profiljához több olyan erőforrás is biztosításra kerül, melyek nem szükségesek az adott felhasználó munkájához.

- **Ne csatlakozzunk ismeretlen és/vagy nyílt (nem titkosított) WiFi hálózatokhoz:** Előfordulhat, hogy a szomszéd irodaházból sugárzott jel erősebb és bárki számára elérhető, illetve azon keresztül akár az Internet is korlátozások nélkül elérhető, de ugyanakkor ez egy gondosan álcázott csapda is lehet. Az ilyen csapdákban rejlő veszélyeket azzal kerülhetjük el, hogy csak olyan hálózatokhoz csatlakozunk, amit a munkáltató a munkavégzéshez biztosít.

- **Saját eszközt az intézmény hálózatára kizárólag engedéllyel, a megadott módon és helyen csatlakoztassunk:** Az ilyen esetekre vonatkozó különleges szabályok legtöbbször az Informatikai Biztonsági Szabályzatban (IBSZ) találhatóak.

Technikai Kontrollok

- **Hálózatok szegmentálása:** Javasolt a szervezeti hálózati struktúra szétbontása úgy, hogy funkciójuk és biztonsági kockázatuk alapján elkülöníthető alhálózatok kerüljenek kialakításra (pl.: kliensek, szerverek, DMZ, biztonsági rendszerek, clusterek belső kommunikációi stb.).

- **Alhálózatok közti forgalom szabályozása:** A szeparációt követően szabályozni szükséges a létrejött alhálózatok egymás közti forgalmát, a lehető legkevesebb indokolt forgalom átengedésével. Erre általánosan használt megoldás a hozzáférés-jogosultsági listák (Access Control List - ACL) alkalmazása.

- **IDS/IPS rendszerek alkalmazása:** Az infrastruktúra belső hálózatának védelme érdekében IDS/IPS rendszerek alkalmazása ajánlott, melyek szignatúráik alapján képesek felismerni a gyakori támadások mintázatait. E rendszerek IDS esetén riasztani, míg IPS esetén közbeavatkozni - ez által a forgalmat tiltani - is képesek. Az eszközök szabályrendszerét rendszeresen frissíteni kell, illetve az ismertté vált új támadás típusok, kampányok kapcsán közzétett IoC-k (Indicators of Compromise) alapján új szabályok létrehozása ugyancsak indokolt lehet.

- **Nyitott szolgáltatások rendszeres ellenőrzése:** Célszerű rendszeresen ellenőrizni az egyes szervereken, munkaállomásokon, valamint egyéb IT eszközökön aktuálisan nyitott állapotban lévő portokat, illetve a feltelepített szolgáltatásokat, ezen kívül javasolt ezek indokoltságának ellenőrzése figyelembe véve az ismertté vált esetleges sérülékenységeket.

- **Internet irányából elérhető szolgáltatások korlátozása:** Az internetről – tipikusan közvetlenül/NAT port-forwarding által – elérhető szolgáltatások minimalizálása, továbbá pontos ismerete úgyszintén fontos. E szolgáltatások (bár sok esetben indokoltak és szükségesek) közvetlen veszélyt rejtenek az egyes sérülékenységek sikeres kihasználása esetén. A szolgáltatásokat biztosító kiszolgálók (pl.: webszerver) megerősítése, az ún. „hardening" ajánlásoknak való megfelelő konfigurálása csökkentheti a kitettséget.

- **Demilitarizált zóna (DMZ) használata:** A kívülről közvetlenül elérhető szolgáltatásokat speciális - tipikusan két tűzfal közé „szorított" - demilitarizált zónába javasolt implementálni. Ezzel további hálózati forgalomkorlátozás képezhető, arra a nem szerencsés esetre, amennyiben egy támadó sikeresen bejut valamely szolgáltatást kiszolgáló szerverre.

- **Biztonságos VPN technológia beállítása:** A belső infrastruktúrához való távoli hozzáférést - a szervezet munkatársai, valamint esetleges egyéb harmadik fél részére - javasolt titkosított adatkapcsolaton át, ismert gyártó által készített VPN szolgáltatás használatával biztosítani, kiemelt figyelmet fordítva annak magas szintű biztonsági beállításaira. Ekképpen a hálózatok közti forgalom teljes egészében titkosításra kerül, így védve annak tartalmát.

- **„Egykapus" Internet/hálózati forgalom:** A szervezet irányából ki- és befelé haladó Internet alapú, valamint egyéb hálózati forgalmat javasolt egyetlen (egyúttal magas rendelkezésre állást biztosító, redundáns), jól ellenőrizhető és „védhető" ponton kiengedni. Ez által biztosítható a központi, átlátható védelem, valamint az összes hálózati forgalom, a meglévő biztonsági eszközökkel történő átvizsgálása.

- **Port Security alkalmazása:** A fixen egy, vagy maximum néhány eszköz által használt hálózati csatlakozások esetén javasolt konfiguráció szintjén akadályt gördíteni az elé, hogy idegen eszközt tudjanak az intézmény vezetékes hálózatára csatlakoztatni. A hálózati eszközök (switchek) esetén az ezt biztosító funkciót Port Security-nek nevezik, amely idegen MAC cím (eszköz egyedi fizikai címe) érzékelése esetén akár tilthatja is az adott portot, adminisztratív beavatkozást kikényszerítve annak újbóli használatba vételéhez.

- **Hálózati eszközök maximális biztonsága:** A hálózat biztonsága érdekében javasolt az egyes tűzfalak, routerek, switchek, valamint egyéb hálózati eszközök konfigurációja esetén azok biztonsági szintjének növelése, valamint az általános biztonsági követelményeknek való megfeleltetése, akár gyártó ajánlásait felhasználva. Különböző privilégium szintekhez kötődő jelszavak és fizikai védelem alkalmazása is a védelem hatékony módszere lehet.

- **Részletes naplózás:** A belső hálózati infrastruktúra tekintetében az esetleges biztonsági incidensek utólagos kivizsgálása érdekében részletes – hosszabb távú – naplózás bevezetése (pl.: tűzfal sikeres/sikertelen kapcsolatok, hozzájuk tartozó metaadatok [időtartam, átvitt byte-ok, IP címek és portok], proxy log, DHCP log, stb.) alapvető követelménynek számít.

- **WiFi képes nyomtatók helyes beállítása:** Üzembe helyezéskor módosítani szükséges a nyomtatók alapértelmezett beállításait, kiemelt figyelmet kell fordítani a hozzáférések megfelelő definiálására. Vezeték nélküli kapcsolatra képes nyomtatók esetében kockázatot jelenthet az – általában számjegyből álló – alapértelmezett jelszó használata, mivel az visszafejtve egy támadó megismerheti a nyomtatón kinyomtatott dokumentumok tartalmát.

Eljárásrendek

- **Port biztonság:** A hálózaton jelen lévő munkaállomások, szerverek és egyéb IT eszközök, valamint azok nyitott szolgáltatásainak (portjainak) ellenőrzését rendszeresen végre kell hajtani, folyamatos sérülékenység-kontrollt kell végezni.

- **Naprakész és a biztonsági követelményeknek megfelelő beállítások:** Gondoskodni kell arról, hogy a tűzfalak, a routerek és switchek konfigurációja a biztonsági követelményeknek eleget tegyen. A konfigurációt dokumentáltan, és a szakemberek által ellenőrzött, jóváhagyott módon kell megvalósítani. A már nem aktuális konfigurációt is meg kell őrizni az érvényességi időtartamának megőrzése mellett.

- **Naplózás:** A biztonsági incidensek utólagos kivizsgálása érdekében az említett naplóállományokat külön kiszolgálón, archiválható módon gyűjteni szükséges.

- **Az incidenskezelésben részt vevő, IT biztonsággal megbízott munkatársak azonosítása:** Azonosítani kell az informatikai biztonsággal kapcsolatos feladatokban résztvevő munkatársakat, az általuk betöltött szerepkörök feladatait és hatásköreiket (RACI mátrix) majd azokat rögzíteni kell a vonatkozó munkaköri leírásokban.

- **Kiemelt üzemeltetői jogú hozzáférések leválasztása, monitorozása, auditálása:** A rendszerekben jelenlévő jogosultságokról teljes körű, lehetőleg mátrix jellegű jogosultsági nyilvántartást kell vezetni és naprakészen tartani. A szervezetbe belépő, és/vagy új szerepkörbe kerülő felhasználók jogosultságait a munkavégzéshez elégséges, legkisebb szintű hozzáférést biztosító jogosultságokkal kell beállítani. A jogosultságok nyilvántartásának ki kell terjednie az egyes alkalmazások, rendszerek által használt technikai felhasználók jogosultságainak számbavételére is. A felhasználókat csoportokba kell sorolni, és lehetőség szerint csoportházirendek szerint kezelni. Az egyes felhasználói csoportokhoz, beleértve a technikai és adminisztrátori csoportokat is, jelszópolitikát kell kialakítani a jelszavak komplexitására és érvényességi idejére vonatkozóan. A hozzáférések igénylésére, engedélyezésére, módosítására, visszavonására az egyes rendszerek felett adatgazda szerepet betöltők bevonásával adminisztratív szabályokat kell bevezetni, és dokumentálni kell a jogosultságkezelés folyamatát. A jogosultságokat kezelő technikai munkatársaknak vissza kell jelezniük a módosítások elvégzéséről a feladatvégrehajtást elrendelő, és a felhasználó felé. A felhasználó köteles a vonatkozó szabályzatokat megismerni, illetve a rendszer használatba vételekor megváltoztatni a jelszavát, amelyet később nem oszthat meg sem a rendszer adminisztrátoraival, sem más felhasználókkal.

- **Jogosultság nyilvántartás, általános jelszópolitika, kiemelt felhasználói jelszavak, technikai felhasználói jelszavak, csoportházirendek kezelésének általános szabályai:** A kiemelt üzemeltetői-, adminisztrációs-, gyökér-, privilegizált hozzáférési joggal rendelkező felhasználók vonatkozó hozzáférését külön kell kezelni a felhasználói jogosultsággal végzett feladataik ellátása során használt felhasználói profiljaiktól. A rendszerelemek és beállítások módosítását lehetővé tevő műveleteket a vonatkozó hozzáférések monitorozásával követni szükséges, és később ellenőrizhetővé kell tenni. A műveleteket rendszeresen belső audit keretében, és alkalmanként, elsősorban biztonsági incidensekhez kapcsolódva ellenőrizni kell.

- **Tanúsítványkezelés, szolgáltatói és belső tanúsítványok kezelésének rendje:** A belső hálózati adatforgalmat, levelező protokollok forgalmát és webalkalmazások elérését titkosított kapcsolaton keresztül érdemes megvalósítani. A titkosításhoz használt tanúsítványokat egy belső tanúsítvány kiadó (Certificate Authority) alkalmazásával, és annak a rendszer tanúsítványtárjaiba való felvétellel lehet könnyen központilag kezelni és megújítani. A belső tanúsítványtárak kezeljék a rendszerben használt szoftverek és eszközök gyártói tanúsítványait is, így hatékonyabban kikényszeríthető, hogy csak a tanúsított alkalmazások kerülhessenek a szerverekre és munkaállomásokra.

- **Informatikai katasztrófaterv, üzletmenet folytonossági terv készítése:** Üzletmenet folytonossági tervet kell készíteni, amelynek számba kell vennie a szervezet működéséhez feltétlenül szükséges anyagi, infrastrukturális és humán erőforrásokat, és a zavartalan működés szükséges tartalékot. Az Informatikai üzletmenet folytonossági tervnek koherens egységet kell képeznie a szervezet üzletmenet folytonossági tervével, biztosítva a folyamatok ellátásához szükséges, kellően redundáns IT infrastruktúrát, tartalék eszközöket, tartalék IT szolgáltatási útvonalakat. Az IT üzletmenet folytonossághoz szorosan csatlakozó informatikai katasztrófatervnek tartalmaznia kell az akadályok elhárításához szükséges intézkedések számbavételét, eljárásrendjét.

- **Rendszerek biztonsági osztályba sorolása:** Az Ibtv. előírásainak megfelelően az adat- és alkalmazásgazdák bevonásával a megfelelő és kívánatos bizalmasság, sértetlenség és rendelkezésre állási követelmények meghatározásával biztonsági osztályba kell sorolni az információs rendszereket. Meg kell határozni a maximális, még elfogadható adatvesztés mértékét (helyreállítási pont kijelölése), a maximális szolgáltatási időkiesés és elégséges szolgáltatási szint üzletmenet folytonossági és kapcsolódó tervekben rögzíthető adatait.

- **Mentési rend, újraindítási rend:** Mentési rendet kell készíteni a mentendő rendszer- és felhasználói adatok köréről, ütemezéséről, a vonatkozó időablakok meghatározásáról, és a visszatöltési tesztek alkalmáról, végrehajtásának módjáról. Újraindítási rendet kell készíteni a rendszer és egyes elemeinek újraindítási sorrendjéről, továbbá az újraindítási tesztek alkalmáról, végrehajtásának módjáról.

- **Rendszeres biztonsági szint értékelés:** Az elvárt és valós biztonsági szint közötti különbségek feltárásának érdekében rendszeres biztonsági szint értékelés keretében fel kell mérni az adott időpillanatban a tényleges biztonsági szintet, és intézkedési tervet kell létrehozni a nemmegfelelőségek kezelésére.

- **Rendszerkapcsolódási pontok felmérése, IP, portok számbavétele; mi minősül legális forgalomnak:** Fel kell tárni a rendszer egyes elmei közötti fizikai és logikai kapcsolatokat, és grafikusan is értelmezhető formában, folyamatosan aktualizáltan tárolni, így átlátható hálózati topológiát és végpont nyilvántartást vezetni.

- **Hálózati topológia és végpont nyilvántartás:** Fel kell mérni, hogy a szervezetben használt rendszerek mely más, belső és/vagy külső rendszerekhez mely interfészeken, hálózati kapcsolatokon, protokollokon, portokon, milyen hitelesítésen, tanúsítványokon keresztül és milyen üzeneteket forgalmazva kapcsolódnak egymáshoz. A kapcsolódási pontokról nyilvántartást kell vezetni, és legális forgalomként tűzfalszabályokon keresztül nevesítve is monitorozni. A nem legális forgalmat ki kell vizsgálni.

- **Szoftver és hardver karbantartási szabályok és időablakok meghatározása és a folyamatok dokumentálása:** A rendszerben található hardver és szoftver elemekhez, beleértve az operációs rendszereket, egyes alkalmazásokat, és alkalmazás csomagokat karbantartási eljárásrendet, frissítési rendet (patch management) és időablakokat kell meghatározni és dokumentálni kell a végrehajtási folyamatokat

- **Belső ntp és névszolgáltatás, biztonságos külső DNS szolgáltató használata:** A hálózaton belső időkiszolgálót (ntp) kell üzemeltetni, hogy az eszközök időállapota és a naplófájlokban rögzített események konzisztensek maradjanak. A hálózati eszközök nyilvántartásához belső DNS szolgáltatót kell használni, a külső kapcsolódáshoz pedig biztonságos DNS szolgáltatót kell igénybe venni. A DNS szolgáltatás alkalmas lehet az ártalmas weboldalak elkerülésére is.

Káros kódok elleni védelem

A káros kódok, vírusok, férgek, trójaiak és hátsó ajtók azért jelentenek nagy fenyegetést a szervezetre, mert rosszindulatú tevékenységüket többnyire leplezetten, a felhasználók és technikai szakemberek tudta nélkül, de azok nevében és jogosultságával folytatják. Felfedezésükre, azonosításukra nem létezik általános érvényű megoldás, felismerésüket továbbá az is nehezíti, hogy kis méretük és gyors módosíthatóságuk a minta alapú azonosítást is nehézzé teszik. Káros kódokat – akár e-mail útján – bárki akaratán kívül is letölthet az Internetről, vagy megfertőzheti a munkahelyi hálózatot egy gondosan előkészített USB eszközről.

Felhasználói javaslatok

- **Ne nyissuk meg a gyanúsnak tűnő hivatkozásokat és fájlokat:** Gyanúra ad okot például a kettős kiterjesztés használata (.doc.exe), vagy azok a hivatkozások, amik a levél szövegében másképp jelennek meg, mint amik valójában (például: fontos szervezeti hivatkozás szerepel a levél törzsében– de ha az egér mutatóját a link felé helyezzük a gonosz.oldal.com jelenik meg.)

- **Munkahelyi gépbe magántulajdonú, vagy ismeretlen forrásból származó eszközöket csak engedély birtokában, előzetes ellenőrzést követően helyezzünk be:** A magántulajdonú eszközök fokozott biztonsági kockázatot jelentenek, ezért még töltés céljából se csatlakoztassuk azokat a munkahelyi számítógéphez!

- **Ismeretlen, gyanús alkalmazásokra vagy felugró ablakokra ne kattintsunk, kérdéses esetben kérjünk szakmai segítséget:** Több csaló oldal használ felugró ablakokat, amik azt sugallják, hogy valami rossz dolog történt (vírustámadás, szerzői jogsértés), melynek elhárításához azonnali beavatkozás szükséges. Ne dőljünk be az ilyen oldalaknak, ha mégis ilyen üzenet jelenik meg, értesítsük az üzemeltetést!

- **Munkahelyi eszközön ne használjunk más forrásból vagy letöltésből származó szoftvert:** Nem minden szoftver megbízható, ami az internetes letöltő oldalakon található. Egyes szoftverek tartalmazhatnak hátsó ajtókat vagy férgeket is. A munkahelyi számítógépekre és mobil eszközökre kizárólag a munkahely által biztosított szoftvereket telepítsünk.

- **Központilag menedzselt antivírus megoldás:** A káros kódok elleni védelem alapja az egyes kliensek, szerverek és egyéb hosztok védelme vállalati üzemeltetésre alkalmas, központilag menedzselhető, célszerűen a vásárlás idejében piacvezető szintű antivírus termékkel.

- **Megemelt biztonsági konfiguráció:** Az implementált vírusvédelmi alkalmazás szoftver konfigurációjának részletes személyre szabása, szem előtt tartva a lehető legmagasabb biztonsági szintet, valamint gyanús esetekben legalább a karantén lehetőségének alkalmazását.

- **Hálózati forgalomelemzés/Sandboxing:** A – célszerűen egy ponton kivezetett – Internet és egyéb hálózati forgalom elemzése olyan „in-line" módon bekötött eszközökkel valamint proxyval, melyek képesek a károsnak ítélt forgalom elemzésére és tiltására, akár Sandbox vizsgálókörnyezetet alkalmazva.

- **Viselkedés alapú azonosítás:** A viselkedés alapú vizsgálatot végző rendszerek alkalmazkodó (ún. adaptív) tanulásukat követően biztosítják a rendellenes események felderítését (pl.: felhasználó olyan könyvtárakban másol, módosít adatot, ahol még sosem dolgozott), ez által a különböző, felhasználó nevében futó káros kód által folytatott tevékenységekre is fény derülhet.

- **Szigorított szoftverkörnyezet alkalmazása:** A nem engedélyezett szoftverek futtatásának ellenőrzésére javasolt az infrastruktúrában használt környezet átkonfigurálása úgy, hogy az alkalmazza a lehető legszigorúbb, szoftverek futtatására vonatkozó beállításokat. E környezetek pontosan, akár nevesített gyártó vagy konkrét állományok (pl.: „EXE" / „DLL" fájlok) tekintetében is megszabják, hogy kizárólag mi futhat a munkaállomáson.

- **Kötelező újratelepítés:** A fertőzéssel kapcsolatban beazonosított munkaállomások esetében, az incidens kivizsgálását követően javasolt a merevlemezről az összes adat végleges eltávolítását (wipe) követő újratelepítés, valamint a munkaállomáson tárolt és megtartani kívánt adatok részletes vizsgálata a visszahelyezés előtt.

- **Rendszeres, időzített teljes vizsgálat:** A szervezetnél rendszeresített antivírus megoldás rendszeres, ütemezett futtatásának beállítása annak érdekében, hogy az időközben napvilágra került definíciós állományok alapján egy teljes ellenőrzés formájában ismételten ellenőrizze a munkaállomásokon tárolt állományokat.

- **VDI munkakörnyezet:** Azon munkakörök esetén, melyek a virtualizációs technológia alkalmazását lehetővé teszik (pl.: tipikusan azonos szoftvert tömeges módon használó környezetek), a munkakörnyezet átalakítása központilag menedzselt, fürtözött, virtuális-gép alapú kliens környezetre (ún. VDI), melynél lehetőség adódik, hogy a felhasználók olyan, személyre szabott virtuális gépet használjanak, amely a munkamenet végén alapállapotába visszaáll. E technológia, valamint az alapállapotra visszaállítás által az esetlegesen kliensen lévő káros kód is törlődik.

- **Eszközök folyamatos frissítése:** Kiemelt fontosságú az IT infrastruktúrában jelen lévő kiszolgálók, kliensek és egyéb aktív eszközök rendszeres frissítése, kiemelt figyelmet fordítva a biztonsági csomagokra, valamint az esetleges 0-day sebezhetőségekre kiadott gyártói javításokra.

- **Vírusvédelem:** Gondoskodni kell olyan automatizált, központilag menedzselt antivírus rendszer alkalmazásáról, amely folyamatosan figyeli a munkaállomásokat, szervereket, valamint mobil eszközöket, s egyúttal megteszi a szükséges védelmi intézkedéseket a kártékony szoftverek megjelenése esetén.

- **Adathordozók használata:** Biztonsági szabályzatban szükséges rögzíteni a mobil adathordozók használatával kapcsolatos szabályokat, a karantén vagy „dirty PC” alkalmazásával kapcsolatos eljárásrendeket, illetve bejövő adatok vírusvédelmi ellenőrzésével kapcsolatos eljárásokat.

- **Eljárások meghatározása:** Szabályzat szinten javasolt előírni a találatok (TRUE vagy FALSE positive) kezelésével kapcsolatos eljárásrendeket (karantén, törlés, továbbítás elemzésre). Külön-külön eljárásrend kidolgozása célszerű a munkaállomásokra és a központi kiszolgálókra.

- **Közösségi alapú ellenőrzés:** A szervezet informatikai rendszerének biztonsági osztályának megfelelően meg kell határozni, hogy az alkalmazott védelmi megoldások közösségi alapú ellenőrzés funkciója, a felfedezett minták közösséggel történő megosztása, vagy a felhő alapú ellenőrzés engedélyezhető-e, és ha igen, milyen esetleges korlátok között.

Vagyontárgyak (Data, HW, SW, Supply Chain)

Az Asset Management nem új kihívás az üzemeltetők és technikai szakemberek számára, ennek ellenére a biztonságtudatos vagyonkezelés még nem épült be a mindennapi eljárásrendek közé. A szervezetek rendelkezésére álló adatvagyon, a jelentős beruházási igénnyel járó hardver eszközpark és az informatikai szolgáltatás portfólió folyamatos rendelkezésre állása olyan szervezeti érdek, melyet nem lehet fél vállról venni. A vagyontárgyak beszerzésétől kezdődően (ellátási lánc biztonság) a használatbavételen át a kivonásig számos fontos biztonsági kontroll van, melyet nemcsak célszerű, de határozottan javasolt is követni, azoknak megfelelni.

Felhasználói javaslatok

- **Nem „vesszük kölcsön” a munkahelyi eszközöket:** Bár a munkahely által biztosított eszközök a magánéletben is hasznosnak tűnnek, azokat kizárólag a munkáltató tudtával és engedélyével használjuk magáncélra. Sérülés, hiba, kár esetén sokkal nehezebb lesz elmagyarázni, miért is volt szükség az eszköz magáncélú használatára.

- **„Gondos gazda” bánásmód:** „Közös lónak túros a háta”, de ha nem óvjuk a munkahelyi eszközöket, azok gyorsabban és hamarabb amortizálódnak, azonnali pótlásuk pedig jellemzően nem megoldott. Az ilyen esetekben pedig az eszköz hiánya a munkavégzést hátráltatja.

- **Nem adjuk kölcsön (gyerek, családtag) a munkahely által biztosított eszközöket:** A munkavállaló részére biztosított (mobil) eszközök a munkavégzést támogatandó kerültek kiadásra, nem azért, hogy ez ilyen eszközzel nem rendelkező családtagunk élvezhesse a technológia vívmányait. Eltulajdonítás, sérülés esetén igen kellemetlen elmagyarázni, hogy miért is volt az adott eszköz a családtagnál, kerüljük el az ilyen helyzeteket!

- **A munkáltató által biztosított titkosítási algoritmus felelős, belső szabályzók szerinti használata:** A munkáltató, adatainak és eszközeinek védelme érdekében titkosítási eljárásokat, programokat telepíthet egyes eszközeire, vagy központi kiszolgálóira. Ezzel nem a munkavállaló munkavégzését kívánja megnehezíteni, hanem az a célja, hogy elkerülje, hogy illetéktelenek érzékeny, belső adatokhoz férjenek hozzá. Tartsuk be a megkívánt eljárásrendet, védjük a céges adatokat!

Technikai Kontrollok

- **Eszközleltár:** Javasolt egy, a szervezet egészét átfogó eszközleltár alkalmazás implementálása, mely a kliensekre telepített ügynökök segítségével pontos és naprakész információkat szolgáltat a szervezet tulajdonában álló eszközökről és szoftverekről.

- **Karbantartás:** Az eszközök teljes életciklusa során, a beszerzésétől a kivonásig gondoskodni kell a karbantartásról és a fogyó- vagy pótalkatrészek biztosításáról. Ezekkel a járulékos költségekkel a költségvetés szintjén éves rendszerességgel szükséges tervezni.

- **Adatbiztonság:** Az adatok biztonságának garantálása a rendelkezésre állásnál kezdődik, de biztosítani szükséges továbbá a bizalmasságot, a sértetlenséget és a letagadhatatlanságot is. Míg a rendelkezésre állás egyszerűbb technikai megvalósítással (RAID, mentőrendszer) biztosítható, a többi feltétel teljesítéséhez akár kriptográfiai eljárások alkalmazása is szükséges lehet.

- **Biztonságos fejlesztés:** Fejlesztés során folyamatosan figyelemmel kell követni a felhasznált technológia fejlesztési szabályait, valamint a nemzetközi biztonságos fejlesztési metodológiákat. Publikált sérülékenység esetén a fejlesztési dokumentációkat át kell nézni, és intézkedni kell a biztonsági rés kijavítására, védelmi eljárások alkalmazására.

- **Kriptográfia és titkosítás:** A szervezet által használt adathordozók eszköz szintű titkosítása ajánlott. Egy esetleges elvesztés esetén, az eszközön tárolt információhoz kizárólag annak tulajdonosa férhet hozzá, így megakadályozható az érzékeny információk illetéktelenek általi megismerése.

Eljárásrendek

- **Eszközleltár:** Fontos a hálózathoz tartozó, illetve a hálózaton kívüli eszközök pontos feltérképezése. A hálózatához kizárólag olyan gépek csatlakozzanak, amelyek szerepelnek a belső eszközök listáján, és hogy azok az eszközök, amelyek már nem képezik a hálózat részeit, ne tartalmazzanak olyan adatokat, amelyek kapcsán visszaélésekre nyílik lehetőség.

- **Szoftverleltár:** A belső hálózaton kizárólag ellenőrzött forrásból származó szoftverek kerüljenek felhasználásra, figyelve egyúttal a vonatkozó verziószámokra is. A szoftverek használatának nyomon követése folyamatos feladat.

- **Biztonsági osztályba sorolás:** A rendszerben szereplő adatokat, információkat osztályozni kell, és meg kell valósítani az ehhez igazodó, adott esetben többszintű titkosítást, különös tekintettel a szenzitív adatokat tartalmazó mobileszközökre.

- **Tanúsítványkezelés, szolgáltatói és belső tanúsítványok kezelésének rendje:** A belső hálózati adatforgalmat, levelező protokollok forgalmát és webalkalmazások elérését titkosított kapcsolaton keresztül érdemes megvalósítani. A titkosításhoz használt tanúsítványokat egy belső tanúsítvány kiadó (Certificate Authority) alkalmazásával, és annak a rendszer tanúsítványtárjaiba való felvétellel lehet könnyen központilag kezelni és megújítani. A belső tanúsítványtárak kezeljék a rendszerben használt szoftverek és eszközök gyártói tanúsítványait is, így hatékonyabban kikényszeríthető, hogy csak a tanúsított alkalmazások kerülhessenek a szerverekre és munkaállomásokra.

- **Adathordozók kezelése:** Az elektronikus információs rendszer tekintetében elsősorban elektronikus, másodsorban papír alapú adathordozók kezeléséről szükséges intézkedni. Az elektronikus adathordozók esetében meg kell határozni, az adathordozók használatára jogosultak körét, és az egyes adathordozók hordozhatóságának szintjét, megőrzési idejét. Például mentéseket tartalmazó adathordozót tilos kivinni a szervezet telephelyéről, és zárt lemezszekrényben kell tárolni. Tiltani kell a magántulajdonú pendrive használatát a szervezet információs rendszereit elérő hozzáférési pontokon. Az információs rendszerekből származó adatokat titkosított adathordozókon lehet csak tárolni és szállítani.

- **Eszközbeszerzési szabályok:** Az eszközbeszerzési folyamatot le kell szabályozni és a résztvevő munkavállalók számára javasolt kötelezővé tenni a szervezet személyi biztonsági feltételeinek való megfelelést. Az eszközbeszerzésnél ajánlott figyelembe venni a hardver és szoftver licencek, támogatási szerződések szükségességét, érvényességi idejüket, valamint azok folyamatos rendelkezésre állását is biztosítani kell. Az adatok felhasználásával a fenntartás mikéntjét is tervezni szükséges. A licenceket teljes élettartamuk alatt menedzselni érdemes. Amennyiben a beszerzendő eszközök új ismeretanyag birtoklását követelik meg a szervezet munkavállalóitól, úgy a szükséges képzéseket is be kell tervezni a beszerzés mellé.

- **Licence kezelés:** Az elektronikus információs rendszer hardver, szoftver, alkalmazás, és támogatási licenceit és szerződéseit érvényességi idejükkel együtt nyilvántartva folyamatosan kell vezetni. Az új, vagy meglévő licencek meghosszabbítását a szervezet beszerzési eljárásának betartásával és időigényének figyelembevételével kell megindítani, hogy ne fordulhasson elő olyan időállapot, amikor valamely rendszerelem működése nem biztosítható.

- **Konfigurációmenedzsment:** Az elektronikus információs rendszer elmeinek beállításait az egyes időpontokhoz kötődő formában menteni kell, hogy egy korábbi időállapotba visszaállítható legyen az érintett rendszerelem. Ezzel a megoldással biztosítható a konfiguráció változás nyomon követhetősége. Az egyes változásokat, módosításokat megjegyzésekkel kell ellátni. Az elektronikus információs rendszerben használt operációs rendszerek, rendszerelemek, csomagok és alkalmazások verzióról nyilvántartást kell vezetni. A verziószámok nyilvántartása a sérülékenységek azonosításában is segítséget nyújt.

- **Hálózati topológia és végpont nyilvántartás:** Fel kell mérni, hogy a szervezetben használt rendszerek, mely más, belső és/vagy külső rendszerekhez mely interfészeken, hálózati kapcsolatokon, protokollokon, portokon, milyen hitelesítésen, tanúsítványokon keresztül és milyen üzeneteket forgalmazva kapcsolódnak egymáshoz. A kapcsolódási pontokról nyilvántartást kell vezetni, és legális forgalomként tűzfalszabályokon keresztül nevesítve is monitorozni. A nem legális forgalmat ki kell vizsgálni.

Elavult eszközpark

Az elavult eszközök használata több ok miatt is kockázatos lehet a szervezetre nézve. A felhasználók például nehezen tolerálják a lassú, munkavégzésre alig alkalmas eszközöket, és hajlamosak inkább saját, magántulajdonú eszközeiken elvégezni a munkát, mely eszközökön viszont nem érvényesülnek a szervezet által meghatározott biztonsági beállítások. Másrészt, az elavult eszközök, szoftverek frissítése, a javítócsomagok telepítése nem minden esetben lehetséges, vagy a gyártói támogatás hiánya, vagy a patch management korlátai miatt. A nem frissített rendszerek pedig az idő előrehaladtával egyre nagyobb veszélyt jelentenek a szervezetre.

Felhasználói javaslatok

- **Kerüljük a magántulajdonú eszközök használatát (hacsak az nem támogatott a munkáltató által), még akkor is, ha a munka azokkal gyorsabban és hatékonyabban végezhető el:** A magántulajdonú eszközök olyan veszélyeket hordozhatnak, melyekről az üzemeltetésnek nincs tudomása, ennek megfelelően azokra nem is tud felkészülni.

- **Amennyiben sérülést vagy balesetveszélyes állapotot tapasztalunk az eszközön, függesszük fel annak használatát:** Ne használjunk hibásan működő, sérült, balesetveszélyes készülékeket, az ilyeneket azonnal jelentsük az üzemeltetésnek.

- **Jelentsük a rendellenes, szokatlan működést:** Egyes eszközök még alkalmasak lehetnek a használatra, ám épp elavultságuk miatt fokozottan kitettek egy esetleges támadásnak. A rendellenes, szokatlan működés egy kezdődő támadás jele is lehet, ezért célszerű az ilyen jelenségeket az üzemeltetéssel megosztani.

Technikai Kontrollok

- **Elavult eszközök cseréje:** Az olyan eszközöket, melyek már nem képesek biztonságos, naprakész és frissített programok futtatására, ki kell vonni az üzemeltetési körből. Ez épp úgy vonatkozik a végfelhasználói számítógépekre, mint a célhardverekre, vagy a hálózati eszközökre is. Az eszközpark fiatalítása során külön figyelmet kell szentelni arra, hogy a cserében nem érintett eszközök (nem amortizálódott eszközök) képesek legyenek az újonnan beszerzett eszközökkel együttműködni (kompatibilitás).

- **Patch management, javítócsomagok kezelése:** A frissítéskezelés problémakörére megoldást nyújthat a központilag kialakított, vállalati szintű, kötelező érvényű és riportálható patch management rendszer implementálása, mely gondoskodik az infrastruktúrában használt szoftverek tényleges naprakészségéről.

- **Asset Management Software:** Az infrastruktúrában jelen lévő szerverek, kliensek és egyéb IT eszközök pontos, naprakész nyilvántartására az erre a célra létrehozott Asset Management szoftverek lehetnek alkalmasak, melyek az operációs rendszerekre telepíthető ügynök komponense által képesek akár az eszközökről önmagukról történő, napi szintű jelentés készítésre.

- **Hálózati topológia és eszközök felmérése:** Az információs rendszerek tekintetében nagy szerepe van a hálózati topológia naprakészen tartásának. A topológiával megállapítható, hogy egy eszköz kiesése mely eszközöknél, kapcsolatoknál okozhat fennakadást.

- **Sérülékeny rendszerek felderítése és kizárása**: Javasolt a rendszerek összetevőinek frissítése, az eszközök publikált sérülékenységeinek folyamatos figyelemmel követése. Jelentős, nem javítható sérülékenységek esetén az eszköz használatát mellőzni kell, más eszközzel szükséges pótolni. A hálózatok szegmentálásával – egy esetleges sérülékenység esetén – megelőzhető a hálózat többi részének kompromittálódása.

- **Amortizációs csere:** A gyártó által a továbbiakban nem támogatott szoftver és hardver elemeket a rendszerből el kell távolítani, azokat naprakész, korszerű megoldással kell pótolni.

- **Biztonsági javítások:** javasolt az ún. „Patch management” kialakítása, amelynek keretében biztosítani kell a védelmi eszközök és szoftverek naprakészségét. A kisebb karbantartásokhoz előzetesen meghatározott időablakot, a nagyobb műveletekhez a karbantartás folyamatának rögzítése érdekében rendszerbeavatkozási tervet kell készíteni. A rendszerbeavatkozási tervnek tartalmaznia a végrehajtás módjának leírását lépésről lépésre, az elvárt működés tesztelésének leírását, a hibás működés esetén a kiinduló állapot visszaállítási módját, és az egyes folyamatrészek felelőseinek elérhetőségét.

- **Rendszeres biztonsági szint értékelés:** Az elektronikus információs rendszereket bizalmassági, sértetlenségi és rendelkezésre állási elvárásaik alapján biztonsági szintbe kell sorolni. Az elvárt és valós biztonsági szint közötti különbségek feltárásának érdekében biztonsági szint értékelés keretében fel kell mérni az adott időpillanatban a tényleges biztonsági szintet, és intézkedési tervet kell létrehozni a nemmegfelelőségek kezelésére.

- **Eszközbeszerzési szabályok:** Az eszközbeszerzési folyamatot le kell szabályozni és a résztvevő munkavállalók számára javasolt kötelezővé tenni a szervezet személyi biztonsági feltételeinek való megfelelést. Az eszközbeszerzésnél ajánlott figyelembe venni a hardver és szoftver licencek, támogatási szerződések szükségességét, érvényességi idejüket, valamint azok folyamatos rendelkezésre állását is biztosítani kell. Az adatok felhasználásával a fenntartás mikéntjét is tervezni szükséges. A licenceket teljes élettartamuk alatt menedzselni érdemes. Amennyiben a beszerzendő eszközök új ismeretanyag birtoklását követelik meg a szervezet munkavállalóitól, úgy a szükséges képzéseket is be kell tervezni a beszerzés mellé.

- **Konfigurációmenedzsment:** Az elektronikus információs rendszer elmeinek beállításait az egyes időpontokhoz kötődő formában menteni kell, hogy egy korábbi időállapotba visszaállítható legyen az érintett rendszerelem. Ezzel a megoldással biztosítható a konfiguráció változás nyomon követhetősége. Az egyes változásokat, módosításokat megjegyzésekkel kell ellátni. Az elektronikus információs rendszerben használt operációs rendszerek, rendszerelemek, csomagok és alkalmazások verzióról nyilvántartást kell vezetni. A verziószámok nyilvántartása a sérülékenységek azonosításában is segítséget nyújt.

- **Hálózati topológia és végpont nyilvántartás:** Fel kell mérni, hogy a szervezetben használt rendszerek, mely más, belső és/vagy külső rendszerekhez mely interfészeken, hálózati kapcsolatokon, protokollokon, portokon, milyen hitelesítésen, tanúsítványokon keresztül és milyen üzeneteket forgalmazva kapcsolódnak egymáshoz. A kapcsolódási pontokról nyilvántartást kell vezetni, és legális forgalomként tűzfalszabályokon keresztül nevesítve is monitorozni. A nem legális forgalmat ki kell vizsgálni.

- **Szoftver és hardver karbantartási szabályok és időablakok meghatározása és a folyamatok dokumentálása:** A rendszerben található hardver és szoftver elemekhez beleértve az operációs rendszereket, egyes alkalmazásokat, és alkalmazás csomagokat karbantartási eljárásrendet, frissítési rendet (patch management) és időablakokat kell meghatározni és dokumentálni kell a végrehajtási folyamatokat.

Vezeték nélküli hálózatok biztonsága

A vezeték nélküli hálózatok a mozgás szabadságát biztosítják a felhasználók részére, miközben folyamatos Internet elérést biztosítanak. A nagy szabadságnak viszont van árnyoldala is: rosszindulatú személyek hamis hozzáférési pontokat hozhatnak létre, aminek segítségével a teljes átmenő forgalom (ideértve a jelszavakat és bizalmas adatokat is) lehallgatható. A vezeték nélküli hálózatokhoz való hozzáférés jelenleg csak nagyon kisszámú esetben oldható meg biztonságosan. A nyíltan, azonosítás nélkül elérhető hálózatokhoz való, munkavégzés céljából történő csatlakozás semmilyen esetben sem tekinthető helyes és követendő magatartásnak.

Felhasználói javaslatok

- **A munkahely által biztosított (mobil) eszközökkel ne csatlakozzunk nyilvánosan elérhető hozzáférési pontokhoz:** A publikus hálózatokat nagyon egyszerű lehallgatni, az ezeken keresztül továbbított adatokat elmenteni és azokkal visszaélni.

- **Kerüljük a reptéri, vagy gyorséttermek, vendéglátóhelyek által biztosított hálózatokhoz való csatlakozást:** Ezek a hálózatokhoz való csatlakozás fokozott veszélyekkel jár, a rosszindulatú támadók gyakran használják az ilyen hálózatokat jogosulatlan adatszerzésre.

Technikai Kontrollok

- **Megfelelő autentikáció használata:** A vezeték nélküli hálózatok kialakításánál törekedni kell arra, hogy a hálózathoz való csatlakozásra kizárólag az arra illetékes felhasználóknak legyen joga. Amennyiben van lehetőség személyhez kötött autentikációs eljárás (enterprise) használatára, azt szükséges használni. A titkosítási eljárások során biztonságos protokoll használata szükséges.

- **Szeparált hálózat használata:** Szervezeten belül el kell különíteni a munkatársak által használt és a vendégek részére biztosított vezeték nélküli hálózatokat. A belső hálózat elérését meg kell szüntetni a vendég hálózatból, lehetőség szerint önálló internetes kijárat biztosítása szükséges.

- **Naplózás:** A felhasználók által végzett tevékenységeket folyamatosan naplózni szükséges, amelyet rendszeresen (akár alkalmazással folyamatosan) elemezni javasolt, és a gyanús tevékenységet ki kell vizsgálni. Az eszközökön beállított szabályokat – a naplóállományok megtekintésével – rendszeresen felül kell vizsgálni.

– **Megtévesztő hozzáférési pontok azonosítása:** A támadók gyakran használnak olyan eszközöket, amelyek a szervezet vezeték nélküli hálózati nevével megegyező azonosítót sugároznak, így elérve azt, hogy a hálózati forgalmazást megismerhessék. Fejlettebb eszközök képesek a hasonló, de nem a szervezet által üzemeltetett eszközöket felismerni, valamint riasztás küldeni az üzemeltetők részére.

– **Eszközök fizikai védelme:** Az eszközök elhelyezésénél törekedni kell arra, hogy egy támadó fizikálisan ne férhessen hozzá. Fizikai hozzáférés esetén az eszköz lehallgathatóvá válhat, valamint a konfigurációs állományok módosítására is lehetőség nyílhat.

Eljárásrendek

- **WiFi használata:** A vezeték nélküli készülékek csak indokolt mértékben legyenek jelen a hálózaton, egyúttal e készülékek azonosítóit és a készülékeket használók személyi körét egyértelműen rögzíteni kell.

- **Rendszeres biztonsági szint értékelés:** Az elektronikus információs rendszereket bizalmassági, sértetlenségi és rendelkezésre állási elvárásaik alapján biztonsági szintbe kell sorolni. Az elvárt és valós biztonsági szint közötti különbségek feltárásának érdekében biztonsági szint értékelés keretében fel kell mérni az adott időpillanatban a tényleges biztonsági szintet, és intézkedési tervet kell létrehozni a nemmegfelelőségek kezelésére.

- **Rendszerkapcsolódási pontok felmérése, IP címek, portok számbavétele; mi minősül legális forgalomnak:** Fel kell tárni a rendszer egyes elmei közötti fizikai és logikai kapcsolatokat, és grafikusan is értelmezhető formában, folyamatosan aktualizáltan tárolni, így átlátható hálózati topológiát és végpont nyilvántartást vezetni.

Távoli munkavégzés

A távoli (otthoni) munkavégzésnek nemcsak a munkáltatói oldalon jelentkeznek előnyei, hanem a munkavállalói oldalon is, azonban, az előnyök mellett olyan korlátozások is megjelennek, amivel a legjobban felkészült munkáltató is csak nehezen birkózik meg. A belső biztonsági eljárásrendek otthonra történő kiterjesztésétől kezdve az otthoni (magántulajdonú) eszközök védelmén át a kommunikációs csatornák biztonságával bezárólag nagyon sok olyan új támadási felület nyílik, amiknek a védelme egy irodai munkavégzés során viszonylag könnyen megoldható, ám a távoli munkavégzés során új eljárásrendek és szabályok alkotását teszi szükségessé.

Felhasználói javaslatok

- **Publikus vezeték nélküli hálózatot ne használjunk munkavégzésre:** A publikus hálózatokat nagyon egyszerű lehallgatni, az ezeken keresztül továbbított adatokat elmenteni és azokkal visszaélni.

- **Ne adjunk hozzáférést a szervezeti adatokhoz a családtagjaink számára:** Az otthoni munkavégzéshez biztosított eszközökön tárolt adatok ugyanúgy védendő adatok, mint a munkahelyi környezetben tárolt adatok!

- **Ha szünetet tartunk, zároljuk a számítógépet:** Az otthoni munkavégzéshez biztosított eszközöket is zárolni kell, ha szüneteltetjük a munkavégzést.

- **A hivatali eszközre ne töltsünk le, telepítsünk nem munkával összefüggő tartalmakat, alkalmazásokat:** Az otthoni munkavégzéshez biztosított eszközök nem szórakoztató elektronikai eszközök, azok nem saját tulajdonú gépek, ennek megfelelően csak a munkavégzéshez szükséges, munkáltató által biztosított alkalmazásokat lehet használni.

- **Ha idegen, harmadik személy tartózkodik az otthoni munkavégzés helyszínén, ne engedjünk neki betekintést a hivatali adatokba:** Ha idegen személy (szerelő, postás, családtag vendége) tartózkodik az otthoni munkavégzés helyszínén, úgy helyezzük el az eszközt, hogy az idegen személy ne tekinthessen rá a képernyőre (a tükröződést is figyelembe véve). Ha ez nem megoldható, szüneteltessük a munkavégzést.

- **Eszközök titkosítása:** Tanácsos a távoli munkavégzés céljából hazavitt notebookok és egyéb eszközök kötelező teljes lemeztitkosítása a szakmai körökben biztonságosként elismert eljárással vagy szoftverrel.

- **Frissítéskezelés:** Célszerű a távoli munkavégzésre használt eszközök bevonása a patch management infrastruktúrába úgy, hogy azok képesek legyenek a szervezet számára előírt módon és időben történő frissítéskezelésre, függetlenül attól, hogy éppen nem részei a belső infrastruktúrának.

- **VPN / Távelérés kialakítása:** Javasolt a felhasználók távoli munkavégzését támogató, magas biztonsági szintű, leginkább többfaktoros hitelesítést megkövetelő titkosított VPN csatorna, vagy egyéb, hasonló irányelveknek megfelelő megoldás kialakítása (pl.: távoli asztali kapcsolat / virtuális környezet jellegű).

- **Távoli törlés megvalósítása:** A távmunkavégzésben részt vevő eszközök esetén biztosítani szükséges, hogy – a mellett, hogy a tárolt adatok titkosítva is vannak –, biztonsági incidens esetén azok tartalmát távolról törölni lehessen.

- **Többfaktoros hitelesítés használata:** A távoli elérések során többfaktoros hitelesítés használata javasolt annak érdekében, hogy egy esetleges biztonsági incidens kivizsgálása esetén egyértelműen meghatározható legyen az adott tevékenységhez köthető valós személy (pl.: naplóállományban szerepel a felhasználónév, de minden kétséget kizáróan nem eldönthető, hogy nem csak megszemélyesítésről volt-e szó).

- **Részletes naplózás:** A távoli munkavégzéssel kapcsolatos kockázatok minimalizálása, valamint az esetleges biztonsági incidensek utólagos kivizsgálása érdekében részletes – hosszabb távú - naplózás bevezetése (pl.: Távoli kapcsolatok be-kijelentkezései, időtartama, forrás címe, az elért erőforrások naplózása/hálózati szintű információk, stb.) javasolt.

- **Távoli hozzáférés:** Távoli elérés kizárólag indokolt esetben alakítható ki. Amennyiben szükséges, akkor a privát csatornát (VPN) titkosítással is védeni szükséges.

- **Magántulajdonú eszközök:** A felhasználók által a munkahelyi környezetben használt magántulajdonú, külsős eszközök tiltása, vagy kizárólag kontrollált módon történő engedélyezése. Ez lehet pendrive, külső meghajtó, vagy más számítógépnek minősülő készülék: notebook, laptop, tablet, illetve egyéb eszközök.

- **Kiemelt üzemeltetői jogú hozzáférések leválasztása, monitorozása, auditálása:** A rendszerekben jelenlévő jogosultságokról teljes körű, lehetőleg mátrix jellegű jogosultsági nyilvántartást kell vezetni és naprakészen tartani. A szervezetbe belépő, és/vagy új szerepkörbe kerülő felhasználók jogosultságait a munkavégzéshez elégséges, legkisebb szintű hozzáférést biztosító jogosultságokkal kell beállítani. A jogosultságok nyilvántartásának ki kell terjednie az egyes alkalmazások, rendszerek által használt technikai felhasználók jogosultságainak számbavételére is. A felhasználókat csoportokba kell sorolni, és lehetőség szerint csoportházirendek szerint kezelni. Az egyes felhasználói csoportokhoz, beleértve a technikai és adminisztrátori csoportokat is, jelszópolitikát kell kialakítani a jelszavak komplexitására és érvényességi idejére vonatkozóan. A hozzáférések igénylésére, engedélyezésére, módosítására, visszavonására az egyes rendszerek felett adatgazda szerepet betöltők bevonásával adminisztratív szabályokat kell bevezetni, és dokumentálni kell a jogosultságkezelés folyamatát. A jogosultságokat kezelő technikai munkatársaknak vissza kell jelezniük a módosítások elvégzéséről a feladatvégrehajtást elrendelő, és a felhasználó felé. A felhasználó köteles a vonatkozó szabályzatokat megismerni, illetve a rendszer használatba vételekor megváltoztatni a jelszavát, amelyet később nem oszthat meg sem a rendszer adminisztrátoraival, sem más felhasználókkal.

- **Személyi biztonsági feltételek megteremtése:** Az elektronikus információs rendszerek védelme szempontjából, a bennük kezelt adatok természetétől függően különböző feltételeknek kell megfelelniük a rendszereket használó és üzemeltető felhasználóknak. Nem minősített adatokat kezelő elektronikus információs rendszerek esetében ajánlott a felhasználókkal titoktartási nyilatkozatot aláíratni, tőlük hatósági erkölcsi bizonyítvány benyújtását kérni, továbbá a gazdasági döntések meghozatalában, és előkészítésében résztvevő munkavállalók esetében éves rendszerességgel vagyonnyilatkozat és összeférhetetlenségi nyilatkozat megtételét megkövetelni. A személyi biztonsági feltételek meglétét az elektronikus információs rendszerhez hozzáférést kapó a szervezettel nem munkavállalói jogviszonyban lévő külsős felhasználók esetében is meg kell követelni. Külsős munkavállalót ne hagyjunk felügyelet nélkül.

- **Rendszeres biztonsági szint értékelés:** Az elektronikus információs rendszereket bizalmassági, sértetlenségi és rendelkezésre állási elvárásaik alapján biztonsági szintbe kell sorolni. Az elvárt és valós biztonsági szint közötti különbségek feltárásának érdekében biztonsági szint értékelés keretében fel kell mérni az adott időpillanatban a tényleges biztonsági szintet, és intézkedési tervet kell létrehozni a nemmegfelelőségek kezelésére.

- **Rendszerkapcsolódási pontok felmérése, IP, portok számbavétele; mi minősül legális forgalomnak:** Fel kell tárni a rendszer egyes elmei közötti fizikai és logikai kapcsolatokat, és grafikusan is értelmezhető formában, folyamatosan aktualizáltan tárolni, így átlátható hálózati topológiát és végpont nyilvántartást vezetni.

Magántulajdonú eszközök (BYOD)

A nagyobb cégeknél egyre elterjedtebb a magántulajdonú eszközök, munkavégzés céljából történő használatának az ellenőrzött körülmények közti engedélyezése. A hangsúly az ellenőrzött körülményeken van, hiszen a magántulajdonú eszközök esetében is meg kell határozni egy minimális biztonsági szintet, amelynek az adott eszköznek meg kell felelnie, különben nem alkalmazható munkavégzésre. Bár a BYOD (Bring Your Own Device) alapjában véve nem ellentétes a biztonsági szabályokkal, engedélyezése során nagyon körültekintően kell eljárni, és pontosan meg kell határozni azokat a feltételeket, amelyek mellett a magántulajdonú eszközök használata engedélyezhető.

Felhasználói javaslatok

- **Saját tulajdonú eszközünk szoftvere mindig legyen frissített és naprakész:** Az elavult, nem frissített szoftverek sokkal sérülékenyebbek, mint a legújabb biztonsági javítással rendelkező termékek.

- **Eszközünkön biztosítsuk a munkáltató által megkövetelt biztonsági szintnek való megfelelést:** Ez azonban nem jelenti azt, hogy önkéntes alapon nem lehetne szigorúbb beállításokat is alkalmazni az eszközön.

- **Amennyiben a magántulajdonú eszközök használata engedélyezett a munkahelyen, legyünk körültekintőek, milyen alkalmazásokat telepítünk az eszközünkre:** Sok alkalmazás hordoz magában beépített hátsó kapukat, kihasználható biztonsági réseket. Kizárólag megbízható forrásból származó, ellenőrzött alkalmazásokat telepítsünk, azokat tartsuk mindig naprakészen.

- **Magántulajdonú eszközökkel kapcsolatos szabályzó ismerete:** Mielőtt elköteleznénk magunkat egy eszköz megvétele és munkavégzés céljából történő használata mellett, ismerjük meg a munkáltató BYOD szabályzatát, eljárásrendjeit.

- **Karantén kiépítése:** Amennyiben a BYOD vállalati szinten engedélyezésre kerül, gondoskodni kell a magántulajdonú eszközök karanténba helyezésének lehetőségéről is, például MDM (Mobile Device Manager) rendszerek alkalmazásával.

- **Biztonságos szoftverkörnyezet:** Magántulajdonú eszköz kizárólag abban az esetben kerülhet be a vállalati rendszerbe, amennyiben az naprakész és jogtiszta szoftverekkel rendelkezik. A nem jogtiszta vagy elavult alkalmazások veszélyesek lehetnek a vállalat egészére nézve.

- **„Egyenrangú" antivírus védelem:** A szervezet hálózatára léptetett magántulajdonú eszköz esetén biztosítani kell, hogy az a vállalati antivírus megoldás központi menedzsmentjébe bevonható legyen, vagy azzal tudásban és beállításokban egyenértékű terméket használjon (pl.: egyetlen gyengén védett kliens ne tudja zsarolóvírus által megsemmisíteni a közös meghajtókon tárolt anyagokat).

- **Adatbiztonság:** Amennyiben egy BYOD engedélyezett eszköz meghibásodik, a rajta tárolt hivatali adatokat a szervezet üzemeltetésének kell eltávolítania, mielőtt a munkavállaló eszközét elviszi szervizeztetni. Biztosítani kell az eszköz távoli felügyeletének, a rajta tárolt adatok távoli törlésének lehetőségét, valamint technikai eszközökkel ki kell kényszeríteni az adathordozók eszköz szintű titkosítását is.

- **Magántulajdonú eszközhálózat kialakítása:** Javasolt a munkahelyi hálózati infrastruktúrától elkülönült, szigorúan ellenőrzött és biztonsági eszközökkel védett vezeték nélküli hálózat kialakítása, mely kizárólag a BYOD eszközöket szolgálja ki.

- **Megfelelősség-ellenőrzés:** A BYOD eszközök által hordozott kockázatok csökkentése érdekében célszerű a központi menedzsmentet, eszköz profilok kezelését, eszköz ön-regisztrációt, és egészségi állapot ellenőrzését segítő, támogató technológiák bevezetése.

- **Adminisztratív szabályzás:** Figyelembe véve, hogy a BYOD-dal kapcsolatos biztonsági követelményeknek való megfelelés nem minden esetben kényszeríthető ki technikai eszközökkel, a szervezetnek mindenre kiterjedő, világos szabályzókat dolgoznak ki, melyeket a BYOD policy alá eső munkavállalók tudomásul vesznek és elfogadnak.

- **Nyilvántartás:** A szervezet naprakész nyilvántartást vezet azokról a munkavállalókról, és az eszközeikről, akik részére a BYOD engedélyezett. Ezeket az eszközöket a munkáltató időszakosan ellenőrizheti.

- **Beépített eszközök:** Eljárásrend szinten célszerű meghatározni a BYOD szabályzás hatálya alá eső készülékek funkcióinak (kamera, GPS, WiFi és más, vezeték nélküli kapcsolatok) tiltását vagy engedélyezését.

- **Elvárt biztonsági szint meghatározása:** A BYOD szabályzás hatálya alá eső készülékek tekintetében a BYOD szabályozás térjen ki a minimálisan elvárt biztonsági szint meghatározására: jelszó politika, automatikus képernyőzár, titkosítás, távmenedzsment, távoli törlés, megbízható alkalmazások telepítése.

- **Felelősségi körök elhatárolása:** A BYOD szabályzat érthetően és egyértelműen fogalmazza meg a szabályzat hatálya alá eszközökkel kapcsolatos felelősségi köröket, az esetleges kártérítés és kompenzáció lehetőségeit. A munkáltató például anyagi eszközökkel hozzájárulhat az elvárt biztonsági szint nyújtására képes eszköz megvásárlásához, cserébe a munkavállaló elfogadja és magára nézve kötelezőnek ismeri el a szabályzatban részletezett korlátozásokat.

- **Engedélyezett eszközök, alkalmazások listája:** A munkáltató naprakész és a munkavállalók részére hozzáférhető listát vezet a BYOD szabályzás alá vonható eszközökről (gyártó, típus, évjárat) és alkalmazásokról (gyártó, kiadó, fő verzió, elérhetőség).

- **Munkaviszony megszűnése:** A munkaviszony megszűnésével kapcsolatos kötelező érvényű eljárásrendeket és ajánlásokat célszerű a BYOD szabályzóban is lefektetni, különös tekintettel a tárolt adatok, telepített alkalmazások, és az esetleges munkáltató hozzájárulás rendezésének tekintetében.

Fizikai biztonság

Hiába hozott létre a szervezet mindenre kiterjedő és átfogó eljárásrendet és belső szabályzókat, hiába épültek be a különböző szintű technikai kontrollok az informatikai eszközrendszerbe, ha a fizikai biztonság gyenge, vagy nem létezik, nem beszélhetünk átfogó biztonságról. A nyílászárók zárása és védelme épp olyan fontos, mint a ki-beléptetések ellenőrzése, a vendégek folyamatos kísérése, vagy a beléptető rendszer és a zárt láncú kamerahálózat. Fontos, hogy a vendégek ne csak belépéskor, hanem kilépéskor is essenek át ellenőrzésen, minden személy épületen belüli mozgása nyomon követhető legyen, illetve, hogy a zárt körletbe csak az kapjon bebocsájtást, akinek erre tényleges felhatalmazása van.

Felhasználói javaslatok

- **A protokoll szabályai csak a következő ellenőrző pontig érvényesek:** Azaz csak akkor engedjünk át magunk előtt valakit az áteresztőponton, ha megbizonyosodtunk arról, hogy joga van áthaladni (érvényes a kártyája).

- **Ismeretlen személyt ne engedjünk át az ajtón:** Nem számít udvariatlanságnak, ha megkérjük az utánunk belépni szándékozó személyt, hogy igazolja a jogosultságát, mielőtt áthalad.

- **Ne támasszuk, ékeljük ki az ellenőrző pontokon lévő ajtókat még ideiglenesen sem:** Áruszállítás, vagy fokozott, gyakori áthaladási igény esetén, esetleg nagyobb vendégcsoport kísérésekor kérjük meg a biztonsági szolgálatot, hogy biztosítsák az átjárót.

- **Ha nem tartózkodunk az irodában, annak ajtaját zárjuk be:** Ha nem tartózkodik senki az irodában, mielőtt kilépünk, zároljuk a számítógépet, majd zárjuk az iroda ajtaját is, megelőzendő, hogy jogosulatlan személyek oda belépjenek.

- **A biztonsági személyzet legyen éber, és még az ismerős kollégáktól is követelje meg a belépési igazolvány felmutatását.** Előfordulhat, hogy valakinek már rég megvonták a belépési jogosultságát, de ez csak akkor derülhet ki, ha az áthaladási pontokon ez ellenőrzésre is került.

Technikai Kontrollok

- **Belátás elleni védelem:** A felhasználók számítógépükön szenzitív információkat is megtekinthetnek, így azok védelme is elengedhetetlen. Fólia felhelyezésével korlátozható a monitorok belátási szöge, valamint – erre a célra kialakított – fólia használatával az ablakok átláthatósága is csökkenthető.

- **Beléptető rendszer használata:** A szervezet számára kiemelt fontosságú, hogy az épületükbe és irodáikba belépő személyekről megfelelő nyilvántartást vezessenek, amelyben egy beléptető rendszer segítséget jelent. Helyszíni jelenléttel kivitelezett incidens esetén a kivizsgálásnál a belépési naplók segítséget jelenthetnek. Kiemelt védelmi eljárásokat szükséges alkalmazni a jobban védendő helyiségek esetében, így az oda belépni kívánó személyek körét korlátozni szükséges. A csoportos átlépést tiltására intézkedni szükséges, korlátozásához „anti-passback” funkció használata javasolt.

- **Behatolásjelző rendszer használata:** A helyiségek megfelelő védelméhez egy behatolásjelző rendszer kiépítése is javasolt. A területet funkciók szerint zónákra szükséges bontani, így korlátozható, hogy a munkatársak mely zónákat riaszthatják.

- **Védendő területek / munkaállomások vizuális megfigyelése:** Átlépési pontokhoz, valamint kiemelt munkaállomásokhoz (pl.: a beléptető-rendszer adminisztrátori számítógépe, pénztár, stb.) kamera kiépítése javasolt, így az illetéktelen belépési- és behatolási kísérletek felderíthetőek.

- **TEMPEST védelem:** A számítógépes hardver minden egyes alkatrésze kibocsát nem kívánt jeleket. Sugárzási szempontból a leginkább védtelenek a monitorok és a soros kábelek (RS232, Ethernet). A PC monitor szinkronjeleinek megfelelő berendezéssel történő rekonstruálásával a megjelenő kép a "távolban" visszaállítható. A kiemelten védendő munkaállomások tekintetében TEMPEST védett konfiguráció használata javasolt.

Eljárásrendek

- **Rendszeres biztonsági szint értékelés:** Az elektronikus információs rendszereket bizalmassági, sértetlenségi és rendelkezésre állási elvárásaik alapján biztonsági szintbe kell sorolni. Az elvárt és valós biztonsági szint közötti különbségek feltárásának érdekében biztonsági szint értékelés keretében fel kell mérni az adott időpillanatban a tényleges biztonsági szintet, és intézkedési tervet kell létrehozni a nemmegfelelőségek kezelésére.