IIIA - DIGITÁLIS KÉSZSÉGEK, ESZKÖZÖK ÉS JÁRTASSÁG

KIBERBIZTONSÁGI ALAPOK KÖZTISZTVISELŐKNEK

A COMPETENCE projektet Izland, Liechtenstein és Norvégia finanszírozza az EGT és Norvég Alap a Regionális Együttműködésért keretében.

Dokumentum-összefoglaló

Ez a képzési segédanyag a színvonalasabb közszolgáltatások nyújtása érdekében az önkormányzati alkalmazottak kapacitásépítését célzó COMPETENCE (Capacity building of eMployees of municiPalities for betTEr provisioN of public sErvices) projekt keretében készült.

A képzési segédanyag célja	**Referenciaanyag az informatikai biztonsági kockázatok különböző fajtáinak megismeréséhez és gyakorlatias megelőzési tippek elsajátításához** Ennek a szöveges képzési anyagnak a célja bemutatni a kiberkockázatok minimalizálására irányuló gyakorlatias módszereket. A dokumentum két fejezetre oszlik: 1. Alapvető információk a biztonsági kockázatokról és azok megelőzéséről minden számítógép-felhasználónak. 2. Részletesebb technikai információk további biztonsági kockázatokról és azok megelőzéséről rendszergazdáknak és magas szintű technikai készségekkel rendelkező számítógép-felhasználóknak.
Célközönség	**Minden önkormányzati alkalmazott**, aki számítógépet használ a munkája során, és már rendelkezik alapvető ismeretekkel az informatikai biztonság terén.
Tervezett felhasználás	**Elsődleges felhasználás: önálló tanulás** Az önkormányzati alkalmazottak mindennapi munkájuk során önállóan elolvashatják és alkalmazhatják a tartalmát. A helyi nyelvre és önkormányzati sajátságokra szabva az összes számítógép-felhasználó számára „Kiberbiztonsági kézikönyvként” szolgálhat. **Másodlagos felhasználás: szemléltető segédanyag irodáknak** A főbb üzenetek és biztonsági figyelmeztetések vizuális formában is sokszorosíthatók, és kifüggeszthetők az önkormányzati hivatalokban.

BEVEZETÉS

A digitális adatok, a személyazonosság, a bankszámlaadatok és a közösségimédia-profilok eltulajdonításának lehetősége mindenkit aggaszt, aki a munkája vagy a saját mindennapos tevékenységei során használja az internetet, akár személyi számítógépen vagy laptopon, akár okostelefonon, okostelevízión vagy egyéb olyan eszközön, amelyek lehetővé teszi az internet elérését.

Manapság szinte minden tevékenység előfeltétele az internet, de az internetnek nincs maradéktalanul hatékony ellenőrzési rendszere. Ezért valójában minden internethasználó szervezet folyamatosan ki van téve különböző kockázatoknak a visszaélésszerű felhasználástól kezdve a súlyos személyazonosság- vagy adatlopásokon át a társadalmi és gazdasági következményekig.

Ugyanakkor a kiberbiztonsággal, a felelős viselkedéssel és a hálózat használatával kapcsolatos tudás elmélyítésével hozzájárulhatunk a kockázat csökkentéséhez.

Ennek a képzési anyagnak a célja bemutatni a kiberkockázatok minimalizálására irányuló gyakorlatias módszereket.

I. RÉSZ MINDEN SZÁMÍTÓGÉP-FELHASZNÁLÓNAK

A SZEMÉLYI SZÁMÍTÓGÉP/LAPTOP BIZTONSÁGOSSÁ TÉTELE

DIÓHÉJBAN:

- ➔ ***A JELSZÓ BIZTONSÁGOT AD: Használjon erős jelszavakat, és rendszeresen módosítsa őket. Soha senkivel ne ossza meg a jelszavát. Amikor csak lehet, használjon kétfaktoros hitelesítést.***
- ➔ ***ÓVJA AZ ADATAIT: Rendszeresen készítsen biztonsági másolatot az adatairól. Használja a titkosítási funkciót az érzékeny adatok védelmére. Használjon biztonságos kapcsolatot az adatok továbbításához.***
- ➔ ***VÉDJE ESZKÖZÉT A TÁMADÁSOKTÓL: Rendszeresen frissítse az operációs rendszert és az alkalmazásokat.***
- ➔ ***FORDULJON SZAKEMBERHEZ: Lépjen kapcsolatba a helyi informatikai részleggel a maximális biztonságról való gondoskodás érdekében.***

TÖBBET SZERETNE TUDNI? Olvasson tovább!

JELSZÓKEZELÉS

A használt jelszavaknak erősnek kell lenniük (tartalmazniuk kell alfanumerikus karaktereket és speciális szimbólumokat), nem szabad ugyanazokat több fiókhoz használni, és rendszeresen meg kell őket változtatni. Egyes esetekben ajánlott lehet jelszókezelőt használni a bonyolult, egyedi, számítógép által generált jelszavak tárolására.

KÉTFAKTOROS HITELESÍTÉS

Ez egy nagyon hatékony és modern módszer, amely egy további eszközt (pl. biztonsági token vagy okostelefon) használ a további lépésen keresztül bejelentkező felhasználó személyazonosságának megerősítéséhez. További hitelesítésre kerülhet sor biometrikus adatok használatával.

KORLÁTOZOTT JOGOSULTSÁGOKKAL RENDELKEZŐ FIÓKOK HASZNÁLATA

A korlátozott jogosultságokkal rendelkező fiókok használata rendszergazdafiók helyett blokkolja az operációs rendszer érzékeny területeihez való hozzáférést, és alapértelmezés szerint blokkolja a szervezet szolgáltatásait, fájljait vagy könyvtárait célzó támadásokat.

ADATOK BIZTONSÁGI MÁSOLATA

Az adatokat rendszeres időközönként el kell menteni (*biztonsági másolat*), és megbízható magnetooptikai hordozón, biztonságos helyeken kell tárolni őket, lehetőleg titkosítva a jogosulatlan hozzáférés elkerülése érdekében. Ezeket a biztonsági másolatokat több fizikai helyszínen (létesítményben) kell tárolni az elemi csapások és a vállalaton belüli belső fenyegetések kivédése miatt.

ÉRZÉKENY ADATOK TITKOSÍTÁSA

Ajánlott harmadik féltől származó alkalmazásokat vagy olyan operációs rendszereket használni, amelyek az egyes fájlok, mappák vagy a teljes logikai meghajtó szintjén eszközöket foganatosítottak az érzékeny adatok titkosítására.

BIZTONSÁGI ALKALMAZÁSOK ÉS CSOMAGOK

Ajánlott kártevőirtó alkalmazásokat vagy összetett, nagy teljesítményű biztonsági csomagokat telepíteni, amelyek védelmet nyújtanak a legújabb fajta kiberfenyegetésekkel szemben. A legújabb fenyegetések észlelésének szükséges feltétele a kártevők aláírását tartalmazó adatbázis naprakészen tartása. Kérjen segítséget a helyi informatikai részlegtől.

ALKALMAZÁSOK FRISSÍTÉSE

Ez egy teljességgel szükséges lépés, mert megelőzi a kibertámadásokat és a költséges adatszivárgásokat, és így segít biztonságban tartani az érzékeny adatokat. A felhasználóknak minden lényeges alkalmazás esetében engedélyezniük kell az automatikus frissítést.

MOBILESZKÖZÖK BIZTONSÁGOSSÁ TÉTELE

LOPÁSVÉDELMI FUNKCIÓK AKTIVÁLÁSA

Az aktiválható funkciók között szerepelnek az alábbiak:

- ujjlenyomat- vagy arcfelismerés;
- az eszköz feloldása mintázatokkal vagy PIN-kódokkal;
- az eszköz helye;
- hozzáférés blokkolása vagy távoli adattörlés.

ADATSZINKRONIZÁLÁS

Az adatok szinkronizálása egyéb eszközökkel vagy a felhőszolgáltatások használata lehetővé teszi, hogy a fontos információk (névjegyek, dokumentumok, SMS-ek, képek) elérhetők legyenek, ha az eszköz elvész vagy ellopják.

ALKALMAZÁSOK FRISSÍTÉSE

Folyamatosan frissíteni kell az operációs rendszert és az alkalmazásokat a biztonsági incidensek orvoslása és a legújabb funkciók használata miatt.

HASZNÁLATOK KÍVÜLI KAPCSOLATOK KIKAPCSOLÁSA

Ajánlott kikapcsolni az infravörös érzékelőket, a Bluetootht és a Wi-Fi-kapcsolatot, ha azok nincsenek használatban, mert így blokkolni lehet a jogosulatlan hozzáférést.

BIZTONSÁGOS ALKALMAZÁSOK HASZNÁLATA

Ajánlott csak hivatalos forrásokból letölteni alkalmazásokat és kikapcsolni a nem biztonságos alkalmazások letöltésének lehetőségét.

ELLENŐRZÖTT ADATHORDOZÓK HASZNÁLATA

Mielőtt cserélhető adathordozót csatlakoztatnak a mobileszközéhez, vizsgálja meg kártevőirtó eszközökkel.

SZEMÉLYES ADATOK MEGOSZTÁSA

A személyes adatok megosztása (mint például a valós idejű földrajzi hely GPS-t vagy vezeték nélküli hálózatokat használva) lehetővé teheti harmadik feleknek a gyakori útvonalak és mindennapos tevékenységek nyomon követését.

QR-KÓDOK ÓVATOS HASZNÁLATA (GYORS VÁLASZ)

A QR-kódok rosszindulatú weblapokra mutató hivatkozásokat tartalmazhatnak, ami különféle káros hatással lehet az adatbiztonságra: fényképező/mikrofon aktiválása, földrajzi hely kinyerése, fájlokhoz, névjegyekhez vagy SMS-ekhez való hozzáférés, kéretlen üzenetek küldése e-mailben, SMS-ben vagy csevegőalkalmazásokban, szolgáltatásmegtagadási csomag elindítása, személyazonosság-lopás.

ALKALMAZÁS HOZZÁFÉRÉSI JOGAINAK ELLENŐRZÉSE

Ajánlott engedélykezelőt használni egy alkalmazás különféle erőforrásokhoz (fényképezőgép, mikrofon, tartózkodási hely, tárolás) való hozzáférésének beállításához.

KIEGÉSZÍTŐ BIZTONSÁG ÜZLETI ESZKÖZÖKNEK

Az utazás során használt eszközöknek rendkívül biztonságosnak kell lenniük az adattitkosítást, a vezeték nélküli kapcsolatokat (Bluetooth, Wi-Fi) és a cserélhető adathordozókat (USB-meghajtók, CD-DVD-meghajtók) tekintve.

BIZTONSÁGOS ADATKAPCSOLATOK

Ajánlott kerülni a nyilvános Wi-Fi-elérési pontokat, és amikor csak lehet, mobiladatot használni.

A SZÁMÍTÓGÉP BIZTONSÁGÁRÓL VALÓ GONDOSKODÁS

FIZIKAI BIZTONSÁG

Ügyeljen arra, hogy videókamerás megfigyelőrendszer és biztonsági személyzet által védett vagy a hozzáférést (sorompókkal, zárakkal, ajtókkal) megakadályozó helyeken tárolja a számítógépét.

TŰZFALRENDSZEREK

Ezek az informatikai infrastruktúra stratégiai összetevői, amelyeknek célja a hálózat figyelemmel tartása és a rosszindulatú tevékenységek nyomon követése (behatolás észlelése, kártevők blokkolása vagy veszélyes tartalmak szűrése). Kérjen segítséget a helyi informatikai részlegtől.

VIRTUÁLIS MAGÁNHÁLÓZAT (VPN)

A VPN (virtuális magánhálózat) technológiák olyan megoldások, amelyek biztonságossá teszik a távoli hozzáférést és az információk titkosítását. Ajánlott VPN-kapcsolatot használni, ha érzékeny adatokat továbbít az interneten.

KÁRTEVŐK

A kártevő egy olyan szoftver, amelyet kimondottan a számítógépes rendszerek megzavarására, megrongálására vagy a hozzájuk való jogosulatlan hozzáférésre terveztek.

A kártevők fő típusai:

- **Vírusok:** A saját kódjukat megadva módosítanak más számítógépes programokat, és így sokszorosítják magukat.
- **Trójai programok**: Azt a benyomást keltik, hogy jogszerű műveleteket hajtanak végre, miközben valójában megpróbálják feltárni a rendszer sebezhetőségeit, és lehetővé teszik a kiberbűnözőknek a rendszerhez való jogosulatlan hozzáférést.
- **Féregprogramok**: Káros hatást kifejtő alkalmazások, amelyek megfertőzik a számítógépes rendszereket, és az interneten keresztül terjednek.

- **Zsarolóvírusok**: Titkosítják vagy blokkolják a fájlokhoz való hozzáférést, és váltságdíjat követelnek a korlátozások feloldásáért.
- **Kriptovaluta-bányászok**: Alkalmazások, amelyek a számítógép erőforrásait használják arra, hogy kriptovalutát bányásszanak a kiberbűnözőknek.
- **Reklámprogramok**: Programok, amelyek agresszívan közvetítenek hirdetéseket a felhasználóknak.
- **Kémprogramok**: Rögzítik a felhasználók internetes aktivitásával kapcsolatos különböző információkat.
- **Hamis vírusirtó szoftver**: Olyan program, amely félrevezeti a felhasználót, aki fizet az operációs rendszerben észlelt hamis fertőzések eltávolításáért.

ESZKÖZ VÉDELME A KÁRTEVŐKTŐL:

VÍRUSIRTÓ MEGOLDÁS LETÖLTÉSE a kártevők valós idejű észleléséhez és eltávolításához.

TŰZFAL TELEPÍTÉSE a weblapokon, e-mailekben és alkalmazásokban zajló forgalom vizsgálatára.

ALKALMAZÁSOK ÉS MŰKÖDŐ RENDSZEREK FRISSÍTÉSE a létező sebezhetőségek kivédése érdekében.

PARANCSFÁJLOK AUTOMATIKUS VÉGREHAJTÁSÁNAK LETILTÁSA a weboldalakon a kártevők telepítésének megakadályozása céljából.

E-MAIL-SZŰRŐ ALKALMAZÁSOK HASZNÁLATA a fertőzött üzenetek és mellékletek felismeréséhez és észleléséhez.

RENDSZERGAZDAFIÓKOK HASZNÁLATÁNAK KERÜLÉSE annak kivédésére, hogy a kártevők rendszergazda-jogosultságokat kapjanak.

BIZTONSÁGI MÁSOLAT KÉSZÍTÉSE AZ ADATOKRÓL, hogy egy sikeres kártevőfertőzés esetén helyre lehessen őket állítani.

KORSZERŰ ESZKÖZÖK HASZNÁLATA (mint például behatolásérzékelő és -megelőző rendszerek – IDPS) a kártevők észleléséhez.

NAPLÓK SZEMMEL TARTÁSA biztonsági incidensek és események kezelésére (SIEM) szolgáló megoldásokkal.

BIZTONSÁGI IRÁNYELVEK HASZNÁLATA a fertőzés esetén követendő lépések meghatározására.

FUNKCIÓKHOZ VALÓ HOZZÁFÉRÉS KORLÁTOZÁSA annak érdekében, hogy vissza lehessen szorítani a káros kódok konzolon történő végrehajtásának lehetőségét.

BIZTONSÁGI INCIDENSEK JELENTÉSE a helyi kiberbiztonsági csoportnak.

E-MAIL-FIÓKOKAT CÉLZÓ TÁMADÁSOK

Támadások fajtái:

- **Elektronikus levélbomba alkalmazása:** Nagy csatolmánnyal rendelkező e-mail ismételt elküldése egy adott e-mail-címre. Ez ahhoz vezet, hogy megtelik a kiszolgálón lévő elérhető tárhely, és elérhetetlen lesz az e-mail-fiók.
- **E-mail-hamisítás**: E-mailek küldése a hamisított feladóhoz tartozó címmel. Ez a fajta támadás elrejti a feladó valós személyazonosságát, és arra használják, hogy kiderítsenek olyan bizalmas információkat vagy hitelesítő adatokat, amelyek egy adott e-mail-fiókhoz történő hozzáféréshez kellenek.
- **E-mailes levélszemét:** Kéretlen e-mailek küldése kereskedelmi tartalommal. Ennek a támadásnak az a célja, hogy rávegye a címzettet arra, hogy látogasson el egy weboldalra, és vásároljon többé-kevésbé legitim termékeket vagy szolgáltatásokat.
- **Adathalász e-mail:** Üzenetek küldése, amiben arra kérik a címzettet, hogy adjon információt a bankszámlájáról, bankkártyájáról, jelszavairól vagy egyéb személyes adatáról.

E-MAIL-FIÓK VÉDELME:

AUTOMATIKUS VÉGREHAJTÁS TILTÁSA KÓDOK, valamint makrók, renderelő gráfok és előzetes lehívást végző hivatkozások esetében az e-mail-kliensben.

BIZTONSÁGI MEGOLDÁSOK HASZNÁLATA E-MAILEZÉSHEZ, például levélszemét-szűrők, kártevőkeresők, URL-elemzők az adathalász oldalak valós idejű azonosításához.

E-MAIL-KLIENS, OPERÁCIÓS RENDSZER ÉS WEBBÖNGÉSZŐ NAPRAKÉSZEN TARTÁSA ÉS ÉRVÉNYES LICENCRŐL VALÓ GONDOSKODÁS. Ha megjelennek a frissítésre vonatkozó értesítések, telepítse a frissítést, amint elérhetővé válik.

BIZTONSÁGOS KOMMUNIKÁCIÓ HASZNÁLATA E-MAILEKHEZ digitális aláírásokkal vagy titkosítással érzékeny adatok és információk továbbítása esetén.

NE KATTINTSON A HIVATKOZÁSOKRA, ÉS NE TÖLTSE LE A CSATOLMÁNYOKAT, ha nem bízik meg teljes mértékben az e-mail feladójában.

KÉTLÉPÉSES HITELESÍTÉS HASZNÁLATA a fiókok védelmére. Ha rendelkezésre áll, ajánlott használni, mert így megelőzhető, hogy mások átvegyék az irányítást a saját fiókja fölött.

ÖSSZETETT, ERŐS ÉS EGYEDI JELSZÓ HASZNÁLATA minden egyes online szolgáltatáshoz. Komoly biztonsági kockázatot jelent ugyanazt a jelszót használni több szolgáltatáshoz, és ezt mindig kerülni kell.

LEGALÁBB 2 FORRÁSBÓL, KÜLÖNBÖZŐ CSATORNÁKON ELLENŐRIZZE A BANK SZOLGÁLTATÓJÁRA VONATKOZÓ INFORMÁCIÓKAT pénzküldés esetén.

CSALÁS A KÖZÖSSÉGI OLDALAKON

A közösségi médiában előforduló csalásokat a közösségi hálózatok oldalain követik el. A csalók gyakran hamis profilt hoznak létre, ártatlan emberekkel barátkoznak össze, és levélszemétnek minősülő üzeneteket vagy rosszindulatú weboldalakra mutató hivatkozásokat küldenek.

CSALÁS ELKERÜLÉSE A KÖZÖSSÉGI OLDALAKON:

SAJÁT ADATOK VÉDELME

Kerülje a közösségi médiával kapcsolatos azon adatai megosztását, amelyek által mások lemásolhatják a személyazonosságát, és fontolja meg azt, hogy privátra állítja a profilja láthatóságát.

ALKALMAZÁSOK ELLENŐRZÉSE

Ellenőrizze a barátoktól vagy ismerősöktől érkező kéréseket, mielőtt elfogadja őket. Lépjen közvetlen kapcsolatba ezekkel az emberekkel, hogy meggyőződjön arról, nem lett csalás áldozata.

FIÓKOK BIZTONSÁGÁRÓL VALÓ GONDOSKODÁS

Hozzon létre egy erős és egyedi jelszót az összes online fiókjához. Semmilyen személyes adatát ne használja fel a jelszavaihoz.

NYILVÁNOS WI-FI-KAPCSOLATOKTÓL VALÓ ÓVAKODÁS

Nyilvános Wi-Fi-kapcsolat használatakor kerülje az érzékeny információkat tartalmazó alkalmazások használatát.

HIVATKOZÁSOK GYANÚVAL TÖRTÉNŐ KEZELÉSE

Gondosan ellenőrizze az URL-t, mielőtt bejelentkezik egy közösségimédia-oldalra. Figyeljen oda a rövidített hivatkozásokra.

KÉRDŐÍVEK KITÖLTÉSÉNEK MELLŐZÉSE

Gondosan kerülje a közösségi média figyelemfelkeltő kérdőíveit. Még ha egyes kérdőívek jogszerűnek tűnnek is, fel lehet használni őket személyes adatok gyűjtésére.

INGYENES ALKALMAZÁSOK LETÖLTÉSÉNEK KERÜLÉSE

Ellenőrizze a közösségi hálózatokon személyes adatokat kérő alkalmazások forrását. Kerülje harmadik felek alkalmazás-áruházait.

CSALIK ÉSZLELÉSE

Legyen résen a figyelemfelkeltő bejegyzések esetén, amelyek ajándékutalványokat, lottónyereményeket, a legfrissebb híreket vagy híresség fotóit ígérik.

TÚL SOK INFORMÁCIÓ MEGOSZTÁSÁNAK KERÜLÉSE

A legtöbb ember túl sok információt oszt meg. Ez hasznos információval szolgálhat a bűnözőknek ahhoz, hogy jobban kidolgozott csalásokkal tévesszék meg a gyanútlanokat.

SOHA NE TÖLTSÖN LE OLYAN CSATOLMÁNYT, AMINEK AZ ÉRKEZÉSÉRE NEM SZÁMÍTOTT

Ne töltsön le üzenethez csatolt váratlan, de legitimnek tűnő dokumentumokat, mert ez ahhoz vezethet, hogy kártevőt telepít le az eszközére és ellopják a személyes adatait.

MOZIFILMEK ÉS ÉLŐ ADATFOLYAMOK MEGTEKINTÉSÉRE IRÁNYULÓ AJÁNLATOK KERÜLÉSE

Kerülje a hamis élő adatfolyamokra vagy mozifilmekre történő kattintást, mert ez gyakran olyan weboldalakra visz, amelyek kártevőket terjesztenek, vagy bankkártyaadatokat kérnek az ingyenes megtekintéshez.

ONLINE TRANZAKCIÓK BIZTONSÁGA

Támadások fajtái:

- A **kártyaadatok elektronikus lefölözése** olyan támadásokat takar, amelyek azokat a kereskedőket célozzák meg, akiknél online lehet fizetni. A támadás során módosítják az online áruházhoz tartozó weblapok forráskódját, hogy valós idejű hozzáférést szerezzenek az ügyfelek hozzáférési adataihoz.
- A **kártya felmutatása nélküli (CNP)** csalás egy adathalász minta, amely során a támadók megpróbálnak csalárd tranzakciókat végrehajtani anélkül, hogy náluk lenne a kártya.

ONLINE TRANZAKCIÓK BIZTONSÁGÁRÓL TÖRTÉNŐ GONDOSKODÁS:

***ELLENŐRIZZE ONLINE AZ ÜZLETEKET ÉS ELADÓKAT**, és győződjön meg a legitimitásukról. Ha nemrégiben hoztak létre egy e-kereskedelmi weboldalt, az csalás jele lehet.*

***ELLENŐRIZZE A WEBOLDAL BIZTONSÁGÁT:** Olyan weboldalakat nyisson meg, amelyek digitális tanúsítvánnyal és HTTPS-kapcsolattal rendelkeznek (ez esetben az URL bal oldalán egy lakat ikon látható).*

***LEHETŐLEG NE ADJA MEG A BANKKÁRTYAADATAIT A WEBOLDALAKON.** Számos olyan weboldal van, ahol bankkártyaadatokat kell megadni a hitelesítéshez, és amint ezek az oldalak megszerzik ezeket az adatokat, később jogosulatlan tranzakciók végrehajtására*

használhatják őket.

***ISMERJE A JOGAIT**, amikor online vásárol termékeket és szolgáltatásokat, és ellenőrizze a visszatérítési szabályzatot.*

***ONLINE FIZETÉS SORÁN HASZNÁLJON VIRTUÁLIS KÁRTYÁT**, amelyre feltöltheti a tranzakciókhoz szükséges minimális összeget, és amelyet könnyen pótolhat feltörés esetén, vagy próbáljon alternatív elektronikus fizetési rendszereket igénybe venni, mint amilyen a PayPal.*

***EGYES WEBÁRUHÁZAK FELKÍNÁLJÁK A VÁSÁRLÓKNAK A LEHETŐSÉGET A BANKKÁRTYAADATOK TÁROLÁSÁRA** a tranzakciók megkönnyítése érdekében. Alaposan mérje fel ezeket a helyzeteket, valamint az ezen weboldalakhoz társuló kockázatokat és a lehetőséget, hogy ezek a weboldalak kiberbűnözők ellenőrzése alatt állhatnak (akik hozzáférést nyernek az Ön adataihoz).*

***A LEHETŐ LEGHAMARABB ÉRTESÍTSE AZ ILLETÉKES HATÓSÁGOKAT**, ha úgy gondolja, hogy csalás áldozata lett.*

LEGYEN ÉBER! Ha egy ajánlat túl jónak tűnik ahhoz, hogy igaz legyen, gondoljon arra, hogy talán hamis.

SZEMÉLYAZONOSSÁG-LOPÁS

Személyazonosság-lopásra akkor kerül sor, amikor valaki engedély nélkül használja az Ön személyes vagy pénzügyi adatait. Ez rossz hatással lehet a hitelképességére, emellett időbe és pénzbe kerülhet.

Különböző fajta technikák:

- **SIM-csere**: Ez a technika a kriptovalutával rendelkező és nagy kaliberű embereket vagy fiókokat célozza meg azzal a szándékkal, hogy ellopja az áldozat személyazonosságát.
- **Digitális hasonmások**: A „digitális maszk” nevű csalásellenes technika akkor került feltárásra, amikor lopott digitális személyazonosságok jelentek meg kereskedelmi termékként a darknet piacain.
- **Üzleti e-maileket érintő visszaélés (BEC)**: A támadók egy (általában vállalaton belüli) megbízható ember személyazonosságát használják, és ráveszik az áldozatot arra, hogy pénzügyi tranzakciót hajtson végre vagy érzékeny, személyes vagy vállalati információkat tárjon fel.

A SZEMÉLYAZONOSSÁG-LOPÁS MEGELŐZÉSE:

KERÜLJE A BÖNGÉSZŐ ÁLTAL RENDELKEZÉSRE BOCSÁTOTT JELSZÓKEZELŐ HASZNÁLATÁT. Ha szüksége van jelszókezelőre, használjon offline védelemmel ellátott változatot.

A TÖBB-TÉNYEZŐS BEJELENTKEZÉS OLYAN BIZTONSÁGI INTÉZKEDÉS, amely megakadályozza a jelszavak ellopását vagy elvesztését, és gondoskodik a többtényezős hitelesítési folyamat sikeréről.

ELLENŐRIZZE A PÉNZÁTUTALÁSI KÉRÉSSEL ELŐÁLLÓ ÖSSZES SZEMÉLY SZEMÉLYAZONOSSÁGÁT *személyesen vagy telefonon.*

MEGFELELŐEN VÉDJE AZ A SZEMÉLYAZONOSSÁGÁT IGAZOLÓ DOKUMENTUMOKAT ÉS AZOK MÁSOLATÁT (legyen szó fizikai vagy digitális példányokról) a jogosulatlan hozzáféréssel szemben.

NE OSSZA MEG A SZEMÉLYAZONOSSÁGÁRA VONATKOZÓ ADATOKAT kéretlen telefonhívásokban vagy e-mailekben megfogalmazott kéréseknek eleget téve, amelyekre nem kell válaszolni.

HASZNÁLJON JELSZÓVAL VÉDETT ESZKÖZÖKET, gondoskodva a megfelelő minőségű hitelesítő adatokról és a tárolásukra szolgáló biztonságos módszerekről.

NYILVÁNOS WI-FI-HÁLÓZAT HASZNÁLATAKOR LEGYEN KÜLÖNÖSEN KÖRÜLTEKINTŐ.

Ha ilyet használ, kerülje az érzékeny alkalmazásokhoz vagy adatokhoz való hozzáférést. Használjon megbízható VPN-szolgáltatást a nyilvános Wi-Fi-hálózatokhoz való csatlakozásra.

GONDOSKODJON MEGFELELŐ MINŐSÉGŰ HITELESÍTŐ ADATOKRÓL ÉS AZ EZEK TÁROLÁSÁRA SZOLGÁLÓ BIZTONSÁGI MEGOLDÁSOKRÓL az összes igénybe vett adathordozón.

ELLENŐRIZZE A DOKUMENTÁLT TRANZAKCIÓKAT a banki kivonatokon. vagy rendszeresen tekintse át a nyugtákat szabálytalanságokat keresve.

TELEPÍTSEN TARTALOMSZŰRŐT a kéretlen csatolmányok, a rosszindulatú levélszemetet tartalmazó e-mailek és a kéretlen hálózati forgalom kiszűrésére.

SZEMÉLYES ADATOKRA IRÁNYULÓ KÉRÉSEK

KÉRÉSEK ALKALMAZÁSOK ÁLTALI BEKÜLDÉSE

Használja a szervezete által beállított csatornákat. Határozza meg pontosan a helyzetet/adatokat/kérés fajtáját. Bocsásson rendelkezésre elegendő információt és dokumentumot.

ADATOKHOZ VALÓ HOZZÁFÉRÉS JOGA

Kérjen további részleteket, ha a kérés túl általános és jelentős mennyiségű adatról szól. Ellenőrizze a kérés elutasításának jogi követelményeit – pl. törvényes titoktartási kötelezettség.

II. RÉSZ TAPASZTALT FELHASZNÁLÓKNAK ÉS RENDSZERGAZDÁKNAK

Ez a fejezet hasznos kiberbiztonsági információkat tartalmaz az informatikai rendszergazdák és azon felhasználók számára, akik magas szintű tudással rendelkeznek az informatikai szoftver- és hardver-infrastruktúráról.

ÁLTALÁNOS KIBERBIZTONSÁGI INTÉZKEDÉSEK

FIZIKAI BIZTONSÁG

A fizikai biztonság a videókamerás megfigyelőrendszer és biztonsági személyzet által védett vagy a hozzáférést (sorompókkal, zárakkal, ajtókkal) megakadályozó, a kiszolgálókat és kábelcsatornákat biztonságban tartó helyekhez való hozzáférés felügyeletére utal.

AZ OPERÁCIÓS RENDSZER BIZTONSÁGÁRÓL VALÓ GONDOSKODÁS

Ezt úgy lehet elérni, ha orvosolják a biztonsági incidenseket és szoftverhibákat az operációs rendszer minden összetevőjének szintjén (rendszeres, automatikus vagy manuális frissítések alkalmazásával), valamint felügyelik az erőforrások felhasználóinak hozzáférését (fájlokhoz, szolgáltatásokhoz és alkalmazásokhoz való hozzáférési jogosultságok).

A LEGKISEBB JOGOSULTSÁG ELVÉNEK ALKALMAZÁSA

Minden egyes új fiókhoz a legkorlátoltabb hozzáférési jogokat kell hozzárendelni, és szükség szerint további jogosultságokat lehet adni a fióknak. Ha már nincs szükség az érzékeny adatokhoz való hozzáférésre, az összes vonatkozó jogosultságot vissza kell vonni.

FELHASZNÁLÓK NYOMON KÖVETÉSE

A *bennfentes* támadás kockázatának minimalizálása érdekében szükség van a jogosultsággal rendelkező fiókok számának korlátozására és csak minimális engedélyek megadására. Ha már semmi sem indokolja a jogosultságok megtartását, minden egyes jogosultsággal rendelkező fiókot inaktiválni kell.

BIZTONSÁGI INTÉZKEDÉSEK VEZETÉK NÉLKÜLI HÁLÓZATOK ESETÉN

- Biztonságos hálózati protokollok (pl. WPA2) és kompatibilis eszközök használata;
- Használaton kívüli szolgáltatások és funkciók letiltása;
- A hálózaton engedélyezett eszközök szűrése MAC-cím alapján;
- A hálózatazonosító (SSID) elrejtése;
- Statikus IP-címej hozzárendelése vagy a dinamikusan kiosztott IP-címek tartományának szűkítése.

ALAPÉRTELMEZETT JELSZAVAK MÓDOSÍTÁSA HÁLÓZATI ESZKÖZÖK ÉS IOT-ESZKÖZÖK ESETÉBEN

Mivel számos eszköz alapértelmezett beállítása nyilvánosan elérhető az interneten, a beállítások rosszindulatú módosításának elkerülése érdekében azonnal módosítani kell az alapértelmezett beállításokat.

HARMADIK FELEK ADATOKHOZ VALÓ HOZZÁFÉRÉSÉNEK NYOMON KÖVETÉSE

A harmadik felek (pl. együttműködők vagy üzleti partnerek) belső hálózathoz való hozzáférésének nyomon követése lehetővé teszi a káros tevékenységek észlelését és azt, hogy szükség szerint kezdeményezni lehessen a vizsgálatokat.

TÁJÉKOZOTTSÁG NÖVELÉSE

Úgy lehet elérni, ha tájékoztatják a szervezet munkavállalóit a biztonsági intézkedések okairól és hatásairól. A munkavállalók megfelelő képzése ahhoz vezet, hogy a szervezeten belül magas szintet képvisel a kiberbiztonság.

WEBOLDALAKAT CÉLZÓ TÁMADÁSOK

Ez a rész azokat a támadásokat ismerteti, amelyek feltartóztathatják vagy károsíthatják az Ön tulajdonában álló vagy Ön által üzemeltetett weboldalakat. Ha nem rendelkezik weboldallal vagy nem üzemeltet weboldalt, átugorhatja a következő részt.

Webes támadások fajtái:

- **Álcázott letöltés**: Rosszindulatú tartalmat tölt le az áldozat eszközére. A felhasználó felkeres egy legitim oldalt, amelyen kiberbűnözők rosszindulatú parancsfájlokat helyeztek el böngészőalapú exploitok futtatására vagy a felhasználó fertőzött webhelyre történő átirányítására.
- **Ivóhely**: Célzott támadás, amely álcázott funkciókkal rendelkező exploitkészleteket használ. Egy rosszindulatú szereplő azáltal akarja felhasználók bizonyos csoportját veszélybe sodorni, hogy exploitokat vagy a weboldalra juttatott rosszindulatú tartalmakat használ.
- **Űrlapeltérítés**: A támadók káros kódot juttatnak egy weboldal legitim fizetési űrlapjára. Ez a támadás főként banki és egyéb személyazonosításra alkalmas adatokat rögzít, és a rosszindulatú parancsfájl ezzel egy időben továbbítja az adatokat a portálnak és a kiberbűnözőknek.
- **Rosszindulatú URL**: Hivatkozás, amelyet kártevők terjesztése vagy csalás megkönnyítése érdekében hoztak létre. A folyamat pszichológiai manipulációra építő tevékenységekkel szerez meg információkat az áldozattól és győzi meg őt a rosszindulatú URL-re történő kattintásról. Ez az URL egy kártevőt telepítve veszélyezteti az áldozat számítógépét.

WEBOLDALAK VÉDELME:

SZOFTVERFRISSÍTÉS

Az ismert sebezhetőségek kivédése érdekében tartsa naprakészen az operációs rendszereit, internetböngészőit, a beépülő modulokat, a bővítményeket és az alkalmazások hibajavító csomagjait.

ENGEDÉLYEZZE A HALADÓ FUNKCIÓKAT A VÉGPONTVÉDELEMHEZ

Használja a behatolásmegelőző és heurisztikus fájlmegóvó rendszert a rendszerben lévő fájlok viselkedésének teljes körű nyomon követéséhez.

ALKALMAZÁSOK ENGEDÉLYEZÉSI LISTÁJA

Különítsen el alkalmazásokat, és hozzon létre tesztkörnyezetet az álcázott letöltéses támadások kockázatának csökkentésére.

ALKALMAZZON PROAKTÍV MEGKÖZELÍTÉST (KISZOLGÁLÓK ÉS SZOLGÁLTATÁSOK)

Rendszeresen ellenőrizze a tartalomszkriptek verzióját, valamint vizsgálja át a fájlokat és helyben tárolt parancsfájlokat.

TARTALMAK KORLÁTOZÁSA A WEBEN

Használjon reklámblokkolóhoz hasonló eszközöket, amelyekkel korlátozni tudja annak lehetőségét, hogy az egyes weboldalak felkeresésekor káros kódok kerüljenek végrehajtásra.

MEGFIGYELÉS ÉS SZŰRÉS

Használjon olyan eszközöket, amelyek nyomon követik és szűrik a webes tartalmakat és az e-maileket. Ezek észlelik és kivédik a rosszindulatú URL-eket és fájlokat.

VISSZAFELÉ TÖRTÉNŐ ÉS DDOS TÁMADÁSOK

A DDoS jelentése elosztott szolgáltatásmegtagadásos támadás. Ezzel a módszerrel a kiberbűnözők olyan sok rosszindulatú forgalommal árasztanak el egy hálózatot, hogy az már nem tud úgy üzemelni vagy kommunikálni, ahogy általában tenné.

Ez a rész azokat a támadásokat ismerteti, amelyek feltartóztathatják vagy károsíthatják az Ön tulajdonában álló vagy Ön által üzemeltetett informatikai hálózatot. Ha nem rendelkezik hálózati infrastruktúrával vagy nem üzemeltet ilyet, átugorhatja a következő részt.

A visszafelé történő vagy DDoS támadások fajtái:

- **Mennyiségen alapuló támadások**: A támadás célja telíteni a megcélzott oldal sávszélességét.
- **Protokolltámadások**: Ez a fajta támadás a kiszolgáló vagy a közbülső kommunikációs eszköz (mint például tűzfal és terheléselosztó) valós erőforrásait emészti fel.
- **Alkalmazás szintjén történő támadások**: Látszólag legitim kérésekből állnak, céljuk blokkolni a webkiszolgálót.

A HÁLÓZAT VÉDELME:

A SZOLGÁLTATÁS ISMERETE

Legyen tisztában azzal, hol merülhetnek ki az erőforrások, és hogy ki felel ezekért az erőforrásokért.

REAGÁLÁSI TERV

Dolgozzon ki egy *szolgáltatásmegtagadási* támadásra vonatkozó reagálási tervet, amely magába foglalja a szolgáltatás fokozatos teljesítménycsökkenését.

TÁMADHATÓ FELÜLET CSÖKKENTÉSE

Minimalizálja a támadható felületet és ezzel a támadók lehetőségeit. Ne fedjen fel olyan portokat, protokollokat és alkalmazásokat, ahonnan semmilyen kommunikációt nem vár.

SZOLGÁLTATÓ FELKÉSZÍTÉSE

Gondoskodjon arról, hogy a beszállítói naprakészek legyenek és hogy a szolgáltatásaik készen álljanak az erőforrások túlterhelésével való megküzdésre, valamint a szolgáltatás védelmére.

MEGFIGYELÉS ÉS TESZTELÉS

Kövesse nyomon a szolgáltatásmegtagadási támadásokat, és tesztelje a reakciókészségét.

AGGODALOMRA OKOT ADÓ JELEK ÉSZREVÉTELE

A DDoS támadás jelei közé tartoznak a csatlakozási rendellenességek, a hálózat lelassulása és a weboldal időszakos leállása. Ha a teljesítményhiány elhúzódik vagy súlyosabb a szokásosnál, akkor a hálózat feltehetően DDoS támadás alatt áll.

WEBALKALMAZÁSOKAT CÉLZÓ TÁMADÁSOK

Ez a rész azokat a támadásokat ismerteti, amelyek megbéníthatják vagy károsíthatják az Ön tulajdonában álló vagy Ön által üzemeltetett alkalmazásokat. Ha nem rendelkezik webalkalmazásokkal vagy nem üzemeltet ilyeneket, átugorhatja a következő részt.

Webalkalmazások ellen indított támadások fajtái:

- **Webhelyek közötti szkriptelés (XXS):** Egy rosszindulatú parancsfájl feltöltése a weboldalra adatok eltulajdonítása vagy más károkozás céljából.
- **SQL-injekció (SQLi):** Káros kód küldése egy beviteli űrlapon keresztül. Ha a rendszernek nem sikerül megtisztítania magát ettől az információtól, az az adatbázisba bejutva a támadó kívánságának megfelelően módosíthatja, törölheti vagy kinyerheti az adatokat.

- **Útvonalátjárás**: A megadott adatok nem megfelelő védelme. Ezek a webkiszolgáló ellen indított támadások olyan modelleket juttatnak a webkiszolgáló hierarchiájába, amelyek engedéllyel rendelkeznek a felhasználói jogosultságok, adatbázisok, konfigurációs fájlok és

a kiszolgálókon tárolt egyéb információk megszerzésére.

- **Helyi fájlbelefoglalás**: Olyan támadási technika, amely az adott rendszer nem nyilvános részében található fájl végrehajtására kényszeríti a webalkalmazást.

WEBALKALMAZÁSOK VÉDELME:

HASZNÁLJON HITELESÍTÉSI TECHNIKÁKAT, ÉS KÜLÖNÍTSE EL A BEMENETEKET *injekciós támadások esetén.*

HASZNÁLJON JOGOSULTSÁGI SZINTEKET ÉS SZIGORÚ HITELESÍTÉSI MECHANIZMUSOKAT *a biztonsági incidensek megelőzéséhez.*

KÖVESSE NYOMON A FORGALMAT ÉS A SZÉLESSÉGKEZELŐ FUNKCIÓKAT*, és a bejövő forgalmat korlátozza a szükséges szolgáltatásokra.*

GONDOSKODJON A FEJLESZTÉS BIZTONSÁGÁRÓL (TERVEZETT BIZTONSÁG) *úgy, hogy biztonsági eljárásokat alkalmaz az alkalmazásfejlesztés és -karbantartás életciklusa során.*

VIZSGÁLJA ÁT AZ ALKALMAZÁST*, hogy rábukkanjon a sebezhetőségekre, és amint lehet, orvosolja ezeket.*

FOGANATOSÍTSON KEZELÉSI ELJÁRÁSOKAT, ÉS TESZTELJE *a webalkalmazásokhoz használt javítócsomagokat.*

VÉGEZZEN KOCKÁZATÉRTÉKELÉST, ÉS MÉRJE FEL A SEBEZHETŐSÉGEKNEK VALÓ KITETTSÉGET *a webalkalmazás fejlesztési folyamata előtt és alatt.*

KÉSZÍTSEN LELTÁRT A HASZNÁLT API-KRÓL (ALKALMAZÁSPROGRAMOZÁSI FELÜLET)*, és hitelesítse az API-kat a biztonsági környezet határát célzó vizsgálatok felfedezéseinek tükrében, titkosítsa a kapcsolatot és az API-k kommunikációját.*

TELEPÍTSEN WEBALKALMAZÁSHOZ VALÓ TŰZFALAT *a webalkalmazáshoz való hozzáférés irányítására előre meghatározott szabályokat használva a gyanús tevékenység felismerésére és korlátozására.*

SZEMÉLYES ADATOKRA IRÁNYULÓ KÉRÉSEK

SZEMÉLYES ADATOK HELYESBÍTÉSE

Hajtson végre módosításokat az összes informatikai rendszeren és helyen, ahol személyes adatok találhatók.

HORDOZHATÓSÁG

Strukturált módon készítse elő az adatokat, ahogy azokat általában a számítógép használja és olvassa (pl. .csv). A megjelölt személyeknek vagy szervezeteknek küldje el az adatokat.

AUTOMATIZÁLT DÖNTÉSEK

Nyújtson elegendő információt az egyéneknek az algoritmus és a döntéshozatali folyamat megértéséhez. Ellenőrizze az automatikus döntések mechanizmusát és ezek egyénekre gyakorolt hatását.

TILTAKOZÁSOK, TÖRLÉSEK ÉS A KEZELÉS KORLÁTAI

Ellenőrizze, hogy az elutasítás okai vonatkoznak-e az adott helyzetre. Alkalmazza az intézkedést a szervezetnél és az adatkezelőknél lévő személyes adatok összes másolata esetében.

ADATVÉDELEM

Ez a rész áttekintést nyújt a személyes adatok megóvásával kapcsolatos biztonsági intézkedésekről.

Négy területet kell figyelembe venni:

(1) A személyes adatok áramlása (a szervezeten belül és a szervezet felé/szervezettől);

(2) Az adatáramlásban érintett informatikai rendszerek;

(3) Az adatok közzététele más szervezeteknek/más szervezetektől származó adatok közzététele;

(4) Megfelelő belső eljárások.

ADATÁRAMLÁS ÉS SZÁNDÉK

Azonosítsa

(a) az adatok gyűjtését, tárolását, kezelését és közzétételét;

(b) a kezelés alapját;

(c) az adatok helyét;

(d) a kezdeti és az azt követő kezelés célját.

BIZTONSÁGI KOCKÁZATOK CSÖKKENTÉSE BIZTONSÁGOS ADATÁRAMLÁSSAL:

ADATOK* MINIMALIZÁLÁSA*: Csak a szükséges fajta és mennyiségű adatot gyűjtse, tárolja és kezelje.

KEZELÉS ÁTLÁTHATÓSÁGA: A gyűjtés vagy kezelés előtt nyújtson megfelelő információt a személyes adatok általános kezeléséről.

SAJÁTOS BIZTONSÁGI INTÉZKEDÉSEK

(a) korlátozza a hozzáférést az ügyfél-átvilágítás korlátozásának elve szerint;

(b) óvja a tárolt és továbbítás alatt álló adatokat;

(c) végezzen titoktartási, sértetlenségi és elérhetőségi ellenőrzéseket a tárolt adatok és az informatikai rendszer adatáramlásban betöltött szerepe alapján.

HARMADIK FÉL ÁLTALI KEZELÉS

(a) azonosítsa a személyes adatok közzétételét;

(b) kössön megfelelő szerződéseket;

(c) kövesse nyomon/gondoskodjon a megfelelő és folyamatos megfelelőségről.

ADATVÉDELEM

Specifikus elemzésekkel gondoskodjon az egyének jogainak megfelelő védelméről, hivatkozva a szervezet érdekére/szándékára.

BELSŐ ELJÁRÁSOK ÉS FOLYAMATOK

(a) Ütemezze be az összes fenti ajánlást, beleértve az incidenskezelést és az emberek kéréseire adott választ;

(b) Alkalmazzon a megvalósításhoz megfelelő mechanizmusokat;

(c) Ellenőrzés: folyamatosan kövesse nyomon a megvalósítást;

(d) Cselekedjen az ellenőrzésnek, nyomon követésnek, kivizsgálásnak vagy a személyes adatokat érintő incidensek megfigyelt szempontjainak megfelelően.

ISMÉTELJE MEG A LÉPÉSEKET.

Szerkesztők:

Anamaria Varga, Aradi Szociális Jóléti Főigazgatóság
Sorin Mircea Mocuta, Aradi Szociális Jóléti Főigazgatóság
Ancuta Daniela Deac, Aradi Szociális Jóléti Főigazgatóság

Szakmai támogatást nyújtott:
Thibault Rabussier, Åpenhet AS

Lektorálta:
Uj Anikó, Business Coach Kft.
Forgách Géza Business Coach Kft.

A szerkesztés lezárva:
2023. július

Szakfordítást készítette:
Országos Fordító és Fordításhitelesítő Iroda Zrt.

A képzési anyag tartalmáért a szerzők, valamint a szakmai támogatást nyújtó és a lektorálást végző szakemberek a felelősek.

A képzési anyag a COMPETENCE című projekt keretében, nemzetközi partnerségi együttműködés keretében készült.

A COMPETENCE projekt Izland, Liechtenstein és Norvégia támogatásával valósult meg az Európai Gazdasági Térség és a Norvégia Regionális Együttműködési Alapon (EEA and Norway Grants Fund for Regional Cooperation) keresztül.