INFORMÁCIÓBIZTONSÁG

MUNKAVÁLLALÓI ALAPISMERETEK

MIRŐL LESZ SZÓ?

- "Tiszta asztal, tiszta képernyő" szabály
- Okoseszközök biztonságos használata
- Otthoni Wifi hálózat biztonságosabbá tétele
- Levelezés biztonsága/Biztonságos levelezés
- Jelszó választás és jelszószéfek használata

OKOSESZKÖZÖK BIZTONSÁGOS HASZNÁLATA

- Az okoseszközeink (telefon, tablet) esetén is ugyanolyan fontos a szoftverfrissítések rendszeres telepítése, kártékony kód elleni védelmi programok telepítése (~ vírusírtó telepítése).
- Miért? Mert a mobil operációs rendszereket, alkalmazásokat is emberek írják, így hibákat, sérülékenységeket tartalmaznak. A támadók célzottan keresik ezeket a sérülékenységeket, hogy megszerezzék adatainkat, vagy az eszközeink feletti irányítást.

OKOSESZKÖZÖK BIZTONSÁGOS HASZNÁLATA

- De mi a helyzet a többi okoseszközzel? Életünk egyre több területén bukkannak fel a „smart” eszközök. Ma már szinte minden háztartásban található okostv, egyre elterjedtebbek az okoshűtő, okosizzó, okosmosógép, home-security, stb. megoldások. Viszont amire nem gondolunk, az ezek védelme. Ezeken az eszközökön a legtöbbször ugyanolyan mobil operációs rendszer fut, mint a telefononunkon. Ez egyrészt jó dolog, ugyanazokat az alkalmazásokat megkapjuk velük, amik a telefonunkon a mindennapi életünk részévé váltak.
- **Viszont ugyanazokat a sérülékenységeket is kapjuk hozzájuk! Sőt, a helyzet ennél rosszabb, mivel a legtöbb ilyen eszköz esetén még ha akarnánk sem tudnánk telepíteni a frissítéseket, mert nincs rá felületünk ahol ezt megtegyük ☹**

OKOSESZKÖZÖK BIZTONSÁGOS HASZNÁLATA

- Mit tehetünk?
  - Telepítsük rendszeresen a frissítéseket. („*Patch early, patch often!*”)
  - Legyünk körültekintők az alkalmazások telepítésénél, jogosultságainak engedélyezésénél – („*Biztos, hogy kell a zseblámpa alkalmazásnak hozzáférés a címjegyzékhez?*”)
  - Azokat az eszközöket, amik felett nincs (akkora) kontrollunk ne engedjük a belső hálózatra, használjunk elszeparált hálózatot (pl. vendég wifi) számukra.

"TISZTA ASZTAL, TISZTA KÉPERNYŐ" SZABÁLY

- A munkakörnyezetünk rendben, „tisztán” tartása több előnnyel is jár:
  - Könnyebben átlátjuk, megtaláljuk a keresett dokumentumot
  - Jobb benyomást alakul ki rólunk diák- vagy munkatársainkban, felettesünkben, oktatóinkban – olyankor is, amikor erre nem is gondolnánk
    - Dolgozat bemutatása
    - Prezentáció tartása
    - Szülői/munkáltatói ellenőrzés

De hogy jön ide a biztonság?

TISZTA ASZTAL, TISZTA KÉPERNYŐ" SZABÁLY

- A fizikai munkakörnyezetünkben elől hagyott iratokhoz a tudtunkon kívül (azaz az engedélyünk, felügyeletünk nélkül!) bárki hozzáférhet!
- A tényleges, rajtuk tárolt adatokon (nevek, címek, telefonszámok, banki, egészségügyi adatok, stb…) kívül szokásainkról is rengeteg információt elárulhatnak a naptárbejegyzések, jegyzetek, cetlik, stb.
- *Feladat: Gondoljuk át, mi mindent lehet megtudni rólunk ezekből az adatokból*
- Ha nincs rá szükségünk, vagy hosszabb időre elhagyjuk a munkakörnyzetünket, akkor zárjuk el (de legalább tegyük el szem elől) az iratokat, jegyzeteket.

TISZTA ASZTAL, TISZTA KÉPERNYŐ" SZABÁLY

- A számítógépes munkavégzés esetén ugyanúgy oda kell figyelnünk az Asztal tisztántartására – a képernyőre aggatott cetlik (fizikai, de az alkalmazás is), a már nem szükséges, de megnyitott dokumentumok, a képernyőn olvasható állománynevek és típusok nem csak a prezentációk során, de a számítógépünk képernyőjére rálátó (mellettünk, mögöttünk ülő, álló) személyek számára is rengeteg, rájuk nem tartozó, nem nekik szánt információt hordozhatnak.

OTTHONI WIFI BIZTONSÁGOSABBÁ TÉTELE

Az otthoni hálózat biztonságossá tételéhez a Wi-Fi hozzáférési pont (általában Wi-Fi router) megfelelő beállítása szükséges. Ehhez csatlakoznunk kell az otthoni hálózathoz, majd egy böngésző segítségével navigáljunk el az eszközön, vagy kézikönyvében található IP címre (például: https://192.168.1.1), vagy használjuk a gyártó által biztosított segédprogramot, illetve alkalmazást. Ezt követően az alábbi lépéseket hajtsuk végre:

1. **Változtassuk meg az admin jelszót:** használjunk minél hosszabb (legalább 10-12 karakter hosszú) jelszót, amely tartalmaz kisbetűt, nagybetű és számot, valamint speciális karaktert is.

2. **Hozzunk létre egy hálózati jelszót:** állítsuk be a Wi-Fi hálózatot, amit szintén védjünk egyedi erős jelszóval. Figyeljünk, hogy eltérő legyen az előbbiekben megváltoztatott admin jelszótól.

3. **Firmware frissítése:** Engedélyezzük a Wi-Fi hozzáférési pont operációs rendszerén az automatikus frissítést. Ha ez a funkció nem engedélyezhető, rendszeres időközönként végezzük el manuálisan

OTTHONI WIFI BIZTONSÁGOSABBÁ TÉTELE

4. **Vendéghálózat használata:** a vendéghálózat egy virtuálisan elkülönített hálózat, amit szintén a Wi-Fi hozzáférési ponton hozhatunk létre. Ez azt jelenti, hogy két külön hálózat létezik az eszközön, ahol az elsődleges hálózatra csatlakoztathatjuk a megbízható eszközinket (pl. banki notebook), a vendéghálózatra pedig a hozzánk látogatók csatlakozhatnak.

5. **Használjunk DNS szűrést:** Lépjünk be eszközünk menüjébe és változtassuk meg a DNS szerver beállítást egy biztonságosabb alternatívára.
A DNS egy internetes szolgáltatás, amely a weboldalak neveit fordítja le numerikus címekké. Ez az, ami biztosítja, hogy számítógépünk csatlakozni tud egy weboldalhoz, amelynek nevére rákeresünk. A Wi-Fi hozzáférési pontok általában az internetszolgáltató által biztosított, alapértelmezett DNS szervert használják, de több biztonságosabb ingyenes alternatíva is létezik, mint például az OpenDNS, a CloudFlare for Families vagy a Quad9, amelyek extra biztonságot nyújthatnak a nem biztonságos weboldalak blokkolásával.

OTTHONI WIFI BIZTONSÁGOSABBÁ TÉTELE

6. **Felhasználói név megváltoztatása:** Ha az eszközünk ad rá lehetőséget, akkor az adminisztrátori fiók felhasználói nevét is változtassuk meg. A brute force típusú támadásoknak ezzel is elejét vehetjük.

7. **Megfelelőt titkosítás használata:** lehetőség szerint ne használjunk nyílt (open) wifit. Az ezeken bonyolított forgalom nem titkosított, bárki számára lehallgatható! Kerüljük az elavult, bizonyítottan sérülékeny, könnyen feltörhető titkosító kulcsokat a WiFi beállításoknál (pl. WEP).
Használjunk WPA2 vagy WPA3 megoldást.

OTTHONI WIFI BIZTONSÁGOSABBÁ TÉTELE

Vendéghálózat használata

A vendéghálózatot ugyan azon a Wi-Fi hálózaton tudjuk létrehozni, amit külön felhasználónévvel és jelszóval védhetünk. A router gondoskodik róla, hogy a vendéghálózatra felcsatlakozó eszközök „kilássanak” az Internetre, ezzel a felhasználói elvárásoknak megfelelően működjenek, ugyanakkor az elsődleges hálózathoz nem enged hozzáférést. A hozzánk látogató személyek eszközei mellett biztonsági szempontokat figyelembe véve szükséges az otthonunkban lévő egyéb okoseszközöket (pl. okosizzó, okoshűtő, okosmosógép) is a vendéghálózatra csatlakoztatni, ezzel elkülönítve az érzékeny adatokat kezelő/tároló eszközeinktől: számítógépektől, tabletektől, hálózati fájltárolóktól és az okostelefonoktól.

LEVELEZÉS BIZTONSÁGA/BIZTONSÁGOS LEVELEZÉS

Az e-mail szolgáltatásokkal kapcsolatos általános tévhit, hogy biztonságos csatorna.

A helyzet az, hogy nem csak, hogy nem biztonságos, de még csak nem is számít garantált kézbesítési szolgáltatásnak. A levelek az internet hálózaton titkosítatlan formában közlekednek, gyakorlatilag bárki lehallgathatja a tartalmukat. Az internet „hőskorában”, amikor az e-mail szolgáltatás elindult, nem volt szempont a biztonság. Szűk körű, jóindulatú felhasználó használta a rendszert, nem merült fel senkiben az igény a biztonságos működést támogató elemek beépítésére. Ezért van az, hogy nincsen mailS szolgáltatás (a http-> https analógiára), meghamisíthatjuk a feladót (gyakorlatilag bárki nevében írhatunk levelet), stb.

LEVELEZÉS BIZTONSÁGA/BIZTONSÁGOS LEVELEZÉS

Természetesen az idők folyamán felszínre bukkantak ezek a hiányosságok, ezért kiegészítő megoldások születtek, azonban ezek használata nem része az eredeti szabványnak, megmaradtak ajánlás szinten.

Természetesen a rosszindulatú felhasználók is felfedezték ezeket a lehetőségeket, számos támadási módszerben ki is használják ezeket, elég ha csaló, megtévesztő, adathalász vagy épp a káros kódokat tartalmazó vagy terjesztő emailekre gondolunk.

Éppen ezért szükséges körültekintően eljárnunk az emailek kezelése kapcsán, az ismeretlen címről érkező, vagy látszólag valid, ám nem

Ma már szerencsére lehetőség van annak ellenőrzésére, hogy a levél valóban attól a levelező szervertől jött, aminek mondja magát, vagy hogy a küldő IP címe engedélyezve van feladóként az adott szolgáltatónál.

LEVELEZÉS BIZTONSÁGA/BIZTONSÁGOS LEVELEZÉS

Mit tehetünk felhasználóként, hogy az elektronikus levelezést biztonságosan használhassuk?

Érzékeny adatokat ne, vagy csak titkosított csatolmányként küldjünk emailben. Így ha a levelet valaki megszerzi vagy „lehallgatja” is, a tartalmához, azaz az érzékeny adatainkhoz nem fog hozzáférni (de legalábbis meg kell dolgoznia érte a jelszó feltörésével).

A jelszót küldjük külön csatornán – smsben, IM-kliensben (teams, skype, messenger, stb.). Így ha elírnánk az email címzettjét, vagy valaki más módon megszerzi a tartalmát, még mindig nem fogja tudni hozzá a jelszót is.

Küldés előtt ellenőrizzük a címzettet. Ezzel a kis időráfordítással számos problémát megelőzhetünk.

JELSZAVAK HASZNÁLATA

Az informatikai rendszerekben a leggyakoribb azonosítási mód a tudás alapú azonosítás. Ennek leginkább kézzelfogható, mindenki által ismert módja a jelszavak használata. Célja, hogy a felhasználói név mellé ennek megadásával igazoljuk, hogy tényleg azok vagyunk, akiknek mondjuk magunkat.

A rosszindulatú felhasználók, alkalmazások igyekeznek megszerezni ezeket a jelszavakat, hogy segítségükkel különböző visszaéléseket követhessenek el – megszerezzék adatainkat, minket megszemélyesítve hajtsanak végre különböző tevékenységeket.

Ezért különösen fontos, hogy vigyázzunk jelszavainkra, biztonságos módon tároljuk, használjuk azokat.

JELSZAVAK HASZNÁLATA

Milyen a jó jelszó?

- Nem tartalmaz szótári szót (azaz értelmes, valamely névben létező szót egybefüggő alakban.)
- Tartalmaz kis- és nagybetűt, számot, speciális karaktert.
- Könnyen megjegyezhető
- Kellően hosszú (ma már legalább 10 karakter hosszú jelszavak megadását tekintjük biztonságosnak, de a számítási (jelszófeltörési) kapacitások rohamos növekedésével hamarosan ez is kevés lesz
- Nem utal ránk, a szokásainkra (nem tartalmazza rokon nevét, kedvenc autómárkánkat, rendszámunkat, stb.)
- Csak egy rendszerben használjuk (ha ellopják, akkor ezzel ne férjenek hozzá a más rendszerben ugyanezen felhasználói névvel regisztrált fiókjainhoz.

JELSZAVAK HASZNÁLATA

Jó gyakorlatok

- A megjegyezhetetlen, bonyolult jelszavak helyett válasszunk hosszabb, de könnyebben megjegyezhető jelszót. Pl a kedvenc versünk első pár sorát.
- Használjunk jelszószéf alkalmazásokat. Segítségükkel nem kell fejben tartanunk a különböző rendszerekben tárolt jelszavakat, csak a jelszószéf jelszavát. Így akár mindenhol használhatunk 64 karakter hosszúságú, random generált jelszót.
- Ne adjuk oda másnak a jelszavunkat!

„A jelszó olyan mint a fehérnemű: tartsd tisztán, cseréld rendszeresen és ne add oda másnak!”

INFORMÁCIÓBIZTONSÁG

- Köszönjük a figyelmet!

REDMENTA TESZT
(A REDMENTA SZÓRA KATTINTVA ÁTUGRIK A REDMENTA OLDALÁRA)

A FELADATLAP DIREKTCÍME: INFOBIZT_MUNKAVALISM_TESZT

(AKI MÉG NEM CSINÁLT ILYET, AZ A FELSŐ MENÜSORON A DIREKTCÍMRE RÁKATTINT, ÉS ODA BEMÁSOLJA A FENTI CÍMET, MAJD A KITÖLTÉS ELKEZDÉSÉRE KATTINTVA ELKEZDI A TESZTET)

A TESZTET 1X LEHET KITÖLTENI, 40 PERC VAN A KITÖLTÉSÉRE ÉS MÁJUS 14 –E 22:00 –IG LEHET ELKEZDENI!