GYIK/FAQ az adatvédelemről

- *Tárhelyek/felhő*
  Az EU-n belűl szigorúan vannak szabályozva a felhőszolgáltatások. Több közül lehet választani pl Google, Microsoft, Amazon, Apple –
  Felhőszolgáltatás esetén végig kell gondolni, hogy mire akarom használni a felhőt. Egyénileg vagy cégben? Tárhelyre van csak szükségem, vagy több szolgáltatást is használni akarok felhőben? Nincs két ugyanolyan megoldás. Ha tárhelyet akarok és Androidot használok a Google Drive lehet megoldás. Ha Office csomagom van, akkor Onedrive előfizetés lehet az ideális megoldás. Ez cégenként és egyénenként eltérő lehet.
- *Apple (iOS) vs Android –*
  Alap biztonság kérdésében nincs különbség a két eszköztípus között.
- *Verziókövetés – kell-e cserélnem telefont újra, ha lejár a biztonsági frissítés?*
  A Apple hivatalos közleménye szerint 5 évig ad ki frissítéseket egy adott verziójú iPhone-hoz. A legnagyobb Android gyártó a Samsung és maga a Google is 7 évet vállal. Ezt követően biztonsági szempontból kockázatos a telefonokat használni.
- *Hol tudom ellenőrizni, milyen biztonsági verziós a telefonom (Apple / Android) ÉS hol teszik közzé hivatalosan a verziókövetés határidejét (Apple / Android)?*
  A beállításokban található meg az aktuális verzió.
- *Bankolás telefonon applikációval*
  Mivel legalább 2 faktoros ellenőrzés van hozzá szükség, ezért alapvetően biztonságos
- *E-mailezés telefonon*
  A legtöbb ember csak olvassa az emailjeit. Javasolt megbízható email kliens használata és a jelszavak megváltoztatása időnként.
- *Applikációk a telefonon, mire figyeljünk telepítés esetén (Google Play / App Store) – (PRO licence, vélemények, letöltésszám stb.)*
  Több alkalmazásbolt is van, ahonnan le lehet tölteni egy programot. A telefonokon az alapbeállítás az operációs rendszertől függően A Google Play vagy az App Sore. De ilyen alkalmazásboltja van pl az Amazonnak is. Néhány szempont amire figyelünk letöltésnél
    - A legfontosabb, hogy direktbe ismeretlen weboldalról ne töltsön le senki semmilyen alkalmazást.
    - mielőtt letölt bármilyen programot nézze meg, hogy hányan töltötték le
    - milyen vélemények vannak a programhoz kapcsolódóan
    - honnan vannak a vélemények pl mindenki Bangladesből szól hozzá, az elég gyanús
    - mikor frissítették az alkalmazást legutoljára
    - ha az van odaírva, hogy vásárlási lehetőség az appban, akkor ott nagy valószínűséggel reklámmal fogunk találkozni
- *DÁP? (Megkerülhetetlen is lehet majd persze, ha úgy alakítják ki.)*
  Jelenleg a kivárás a legjobb irány. Nincs pontosan leírva, hogyan garantálják az adatok biztonságát
- *Mac vs PC; szoftverfrissítések (operációs rendszer, programok)*
  Mindig a legfrissebb operációs rendszer használata javasolt.
  Az iMacek frissítése ritkán jár jelentős hardverberuházással és a gépek hardware-e kevésbé avul el. Egy akár 10 éves iMac gép is normál használatra tökéletes lehet.
  A Windowsos gépek elavulása sokkal gyorsabb, mert sokszor gyenge hardware-rel rendelkeznek és az újabb és újabb verziók egyre nagyobb teljesítmény írnak elő.
- *Webáruház üzemeltetés.*
  Nem lehet mindenhez érteni. A webáruházakkal kapcsolatban rengeteg szabály van, amit be kell tartani. Javasolt vagy külsős üzemeltetésű webáruházat használni, vagy saját embert felvenni hozzá, vagy megbízni egy céget vele

- *Adataink biztonsági mentése eszközökről és tárhelyekről (telefon, számítógép, webáruház, ERP-rendszer, saját szerver, felhő szerver) – honnan, mit, hova, hogyan?*
  Az egyik legalapvetőbb dolog, hogy védeni kell az adatokat. Azt kell végig gondolni, hogy mely eszközöket és az ezeken található adatokat hogyan akarja a vállalkozás lementeni. Mentési megoldások alapvetően a következők lehetnek
    - Helyi adathordozóra pl NAS
    - Felhőbe

  A felhő mindenkinek kézenfekvő megoldás, de ott olyan szolgáltatás érdemes választani, amit be lehet állítani telefonra és PC/laptopra is pl OneDrive.
- *Meghajtó titkosítása - Bitlocker*
  A felhasználók számára, különböző segédprogramok segítséget nyújtanak, hogy az összes adatot titkosítsák a merevlemezen. A BitLocker Drive Encryption egy Microsoft Windows biztonsági és titkosítási funkciója. Ilyen lehetőségek az okostelefonon is rendelkezésre állnak.
- *Régi eszközök, háttértárak eladása, megszüntetése (data recovery!)*
  Rendkívül kritikus probléma a háttértárak eladása. A bankok pl. kifejezetten tiltják. Az egyre fejlettebb visszaállító programok miatt könnyen kerülhetnek az adataink illetéktelen kezekbe
- *Vírusirtók*
  Minden évben kiadnak különböző listákat, amiben tesztelik a virusírtókat. 2024-ben El kell dönteni, hogy mire akarjuk használni. Tud-e komplett védelmet adni, pl. több operációs rendszerre vagy csak egyre. Ez egyénenként és cégenként is változhat. Az biztos, hogy legyen vírusírtó minden eszközünkön a **telefonon is**!
- *VPS-szolgáltatók,*
  A VPS (Virtual Private Server) szolgáltatás egy olyan erőforrás szolgáltatás, amely lehetővé teszi, hogy saját, elkülönített szerveren futtassuk weboldalainkat és alkalmazásainkat.
- *VPN csatlakozás*
  A VPN az online adatvédelem alapvető biztonsági eszköze. VPN nélkül mások könnyen lehallgathatják és megtekinthetik az internetes tevékenységeidet. Ebbe beletartoznak a böngészési előzmények, a letöltött fájlok, az online banki adatok és a jelszavak.
  A VPN segítségével az adatok védve lesznek, de pl lassíthatja az internetes sávszélességet
- *Szerverkérdés: saját szerver vs. hazai VPS vs. külföldi VPS (ott is melyik)*
  Ez a cégmérettől függ. Ha van dedikált munkatárs, aki ért hozzá és karban tudja tartani, csak akkor érdemes saját szervert üzemeltetni. Ha nincs, akkor érdemes virtuális szervert használni. Ebben az esetben olyat érdemes használni, ami garantálja, hogy adataink az EU-n belül maradnak. Vagy Svájcban pl TresorIT
- Saját szerver / VPS esetén: elérési, biztonsági kérdések
  Itt már haladó ismeretek szükségesek. Ha weboldalról lépünk be, akkor mindenképp csak https protokollt használó oldalról. Ha nem weboldalról, akkor akor FTPS-en keresztül lépjünk be
- *Jelszavak: erős jelszóhasználat; jelszókezelési program használata*
  Alapvető kérdés, hogy erős, egyedi jelszavakat használjon a cég és ezeket meghatározott időközönként cserélje le. Mivel nem lehet minden jelszót fejben tartani érdemes jelszókezelőt használni pl KeePassXC.
- *Nyílt forráskódú vs. fizetős szoftverek. Megbízható szoftverek.*
  A kérdés, hogy mit használunk és erre hajlandóak vagyunk-e áldozni. Pl LibbreOffice egy megbízható és jól működő program. Az MS Word azonban jóval elterjedtebb. Ez egy üzleti döntés. Ha szükségem van IT támogatásra, akkor érdemes fizetős software-t használni. Ha azonban ritkán használok egy programot akkor pl egy GIMP tökéletes választás lehet a Photoshop helyett.

- *Humán tényező (gyerek; én; kollégák; kollégák gyerekei; takarítónő; stb.)*
  A legnagyobb veszélyfaktor a humán tényező. Egy módon lehet elkerülni. A folyamatos tudatosítással, oktatással.
- *IT-szolgáltató cégek megbízhatóságának ellenőrzése (ISO 27001; más?)*
  Minden ISO szabvány annyit ér, amennyit betartanak belőle. Egy ISO 27001-es szabvány egy jól jel, de nem garancia semmire.