Mobil eszközök biztonsága

A munkahelyi és magánhasználatú mobil készülékek biztonsági kérdései

2016. május 15. | 1.0 verzió

A mobil informatikai eszközök jelentősen hozzájárulnak a munkavégzés megkönnyítéséhez, hatékonyságának javításához. A kétségtelen előnyök mellett azonban megjelentek széles körben még nem ismert veszélyek, amelyek mind a felhasználóra, mind a kezelt adatokra kockázatot jelentenek.

Kiadványunk célja bemutatni az alapvető kockázatokat és a védekezés lehetőségeit.

A kiadványt ajánljuk

a közigazgatási szervezetek munkatársainak

Veszélyek

A kiberbiztonsági veszélyekkel kapcsolatos részek jelölése.

Tudatos munkavégzés

A hivatali munkavégzéssel kapcsolatos, a felhasználói magatartásból fakadó kockázatok jelölése.

Védelem

A tudatos munkavégzést elősegítő, valamint a privát szférában is alkalmazható védelmi és biztonsági eljárások és megoldások jelölése.

Kapcsolat

06 1 336 4840

info@GovCERT.hu

www.GovCERT.hu

Kommunikáció, internet

A mobilinformatikai eszközök kockázati tényezői

A jelenleg használt mobilinformatikai eszközök az üzleti élet számos területén könnyítik meg a felhasználók munkavégzését, amelyhez az információkhoz történő valós idejű hozzáférés, feldolgozás és továbbítás elengedhetetlen fontosságú.

A mobilkészülékek olyan kompakt informatikai eszközök (akár teljes értékű számítógépnek is tekinthetőek), amelyeken keresztül különböző adatok kezelése is megvalósul (pl. hang, kép).

Ezen szolgáltatások megvalósítását segítette elő olyan mobil operációs rendszerek megjelenése, mint a 2007-ben kereskedelmi forgalomba kerülő Apple iPhone, a 2010-ben debütáló iPad, valamint a többi nagy IT céghez köthető rendszerek (Google, Microsoft, Blackberry) is. Míg korábban a mobilinformatikai piacon számos gyártó vett részt (gyakran kizárólag saját maguk által fejlesztett rendszerekkel), addig mára a következő három nagy mobilplatform uralja a mobilpiac közel 90 %-át: Android, iOS és Windows.

Az okos eszközök megjelenése, a kapcsolt szolgáltatások (egészség, életvitel, stb.) új területeket nyitottak a gyártók, fejlesztők és forgalmazók számára. Az így rögzített személyes adatok feletti rendelkezési jog IT biztonsági kérdéseket vet fel, hiszen ezekkel való visszaélés kárt okozhat az érintettnek (pl.: személyiséglopás, pénzügyi visszaélés).

A mobileszközök veszélyei

A fenti áttekintés szemlélteti, hogy az okos készülékek használatából adódó kockázatokat komplex biztonsági problémáknak kell tekinteni, a feltárt kockázatokat ezért egyben kell kezelni. A kockázatok több rétegben is jelen vannak (adatok, hardver, szolgáltató, operációs rendszer, alkalmazás, felhasználó). Ezen rétegekben különböztetünk meg sérülékenységeket, illetve támadási felületet, amelyek összefüggenek egymással, a támadási eljárások gyakran egymásra épülnek (bizonyos sérülékenységek kihasználásához elengedhetetlen egy másik rétegben bekövetkező kompromittáció előfeltétele).

A kialakult helyzetet megnehezíti, hogy a korábban megjelent felhő alapú eljárások mára teljes körűen beépültek a szolgáltatásokba, ezáltal további – igen komoly – kockázati tényezőt jelentenek a felhasználó adataira.

Fontos különbséget tenni a felhasználó által tudatosan kezelt adatok köre (dokumentumok, e-mailek, telefonszámok, stb), valamint azon adatok tekintetében, amelyek jelenlétére, valamint folyamatos keletkezésére és további feldolgozására nincs ráhatása a felhasználónak (ún. metaadatok: pozíció, böngészési és bejelentkezési adatok, biometrikus jelek stb.). Ez utóbbi adatok keletkezését elősegítik az eszközökbe integrált különféle szenzorok (orientáció, vérnyomásmérő), amelyek működésére sokszor a felhasználó akaratától függetlenül is megtörténik.

A mobil eszközök hivatali kockázatai

Ki kell hansúlyozni, hogy míg korábban a felhasználói és a hivatali adatok szétválasztása kellőképpen megvalósulhatott (iratkezelés, stb.), addig mostanra ezek az információk a mobileszközön egyesülnek (pl. e-mailen hazaküldött dokumentum további szerkesztése), és ezek az adatok sok esetben a felhő alapú rendszereken kerülnek továbbításra.

A levélküldés, adattárolás, hozzáférés különféle eszközökről stb. jellegű tevékenységek egyes elemeinek komprommittálódása hatással van a lánc többi elemére (a telefon elvesztése, ellopása hozzásegítheti a támadót a vállalati rendszerekbe történő bejutáshoz: pl. tárolt jelszavak, vállalati rendszerekhez történő automatikus csatlakozási lehetőségek).

Fontos megemlíteni, hogy a gyártók hivatalos piactérein (Google Play, AppStore stb.) is felbukkantak már olyan alkalmazások, amelyek speciális rosszindulatú kódokat tartalmaztak.

A rendszer egészét érintő sérülékenység abban az esetben előzhető meg, ha a felhasználó csak és kizárólag megbízható forrásból (vagy egyáltalán nem) tud applikációkat telepíteni, vagy a munkahely által biztosított mobil eszközét teljes egészében munkáltatója üzemelteti.
A munkahelyi eszközökre nem javasolt előzetesen be nem vizsgált alkalmazások telepítése, illetve használata, tekintettel arra, hogy azokban kártékony kódok lehetnek elrejtve, amelyek nemcsak a tárolt adatokat, hanem a felhasználó aktuális tevékenységét is a felhasználó tudta nélkül, illetéktelenek számára továbbíthatják.

Ahhoz, hogy a mobil eszközök használatából fakadó kockázatokat csökkenteni lehessen a következő egyszerű szabályok betartására és tudatos viselkedésre van szükség.

Javasolt biztonsági intézkedések

Személyes használatú mobil eszközök

- Gondoskodni kell a készülék eredeti működési állapotának fenntartásában, azaz a jailbreak (rootolás) alkalmazását el kell kerülni.
- A privát használatban álló eszközön ne valósuljon meg a hivatali levelezés.
- Meg kell gátolni az idegeneknek a készülékhez / felhasználói fiókhoz / tárolt adatokhoz történő hozzáférését (képernyőzár, PIN kód, készülék felügyelete, szervizbe adás előtt adatmentés, a készüléken tárolt adatok törlése és a készülék gyári állapotra történő visszaállítása).
- Kerülni kell az ismeretlen forrásból származó alkalmazások telepítését.
- A telepítésre kerülő alkalmazások által igényelt jogosultságok megfontolt engedélyezése (a szükségtelennek tűnő jogosultságokat igénylő alaklmazások használatának mellőzése).
- Az alkalmazások fejlesztői által kiadott frissítések mielőbbi telepítése (a már nem támogatott készülékek használata kerülendő).
- Vírusvédelmi alkalmazás telepítése.

További óvintézkedések munkahelyi készülékre

- Általános, a felhasználó személyéhez nem köthető felhasználói fiók használata.
- Lehetőség szerint a beépített tárhely és a kivehető memóriakártya titkosítása.
- A felhő alapú szolgáltatások használatának korlátozása, amennyiben ez nem lehetséges, akkor több felhasználói fiók együttes használatának mellőzése.
- Nem biztonságos vezeték nélküli hálózathoz (pl.: szállodai WiFi) csatlakozás kerülése.
- Egy készülék, egy felhasználó alapelv betartása: meg kell akadályozni a kollégák, családtagok készülékhez / felhasználói fiókhoz történő hozzáférését.
- A munkáltató által meghatározott biztonsági szabályok betartása.