OKOSTELEFONOK KIBERBIZTONSÁGI ÉS ADATVÉDELMI KÉRDÉSEI

SZERZŐ: DR. KRASZNAY CSABA A NEMZETI KÖZSZOLGÁLATI EGYETEM DOCENSE, AZ EÖTVÖS JÓZSEF KUTATÓKÖZPONT KIBERBIZTONSÁGI KUTATÓINTÉZETÉNEK VEZETŐJE,A TALLINNI MŰSZAKI EGYETEM TUDOMÁNYOS MUNKATÁRSA

Az okostelefon a legszemélyesebb tárgyunkká vált az elmúlt évtizedben. Minden titok, minden személyes információ ezen az eszközön tárolódik, vagy legalábbis hozzáférhető az azon beállított hozzáféréseken keresztül.

Valószínűleg mindenkinek megvan az a pillanat, amikor a leginkább kedvelt közösségi hálózat hirdetései között feltűnik egy olyan téma, amiről épp nem rég beszéltünk, vagy akár csak gondoltunk rá. Ezek a kimondott szavak vagy ki nem mondott gondolatok sem lennének hirdetéssé konvertálható információk, ha nem lenne folyamatosan mellettünk egy olyan eszköz, ami minden adatot rögzít és továbbít a nagy adatkapitalista cégeknek rólunk és a környezetünkről. A 2020-as évek adatvédelmi kihívásai sokkal kevésbé lennének jelen az okostelefonok nélkül. A 2020-as évek digitális gazdasága azonban működésképtelen lenne a mobilitás, a mindenkinél jelen levő okoseszközök nélkül. Ennek az évtizednek tehát az egyik legfontosabb feladata megtalálni az egyensúlyt a mindenki számára hasznos digitalizáció és privát szféránk fenntartása, a személyes kiberbiztonság megteremtése között.

De mit jelent a személyes kiberhigiénia? Milyen veszélyek leselkednek ránk az okostelefon használata közben?

Ezek azok a kérdések, amit az indokoltnál sokkal kevesebbszer tesz fel a modern kor embere. Pedig a kiberbiztonsági szakember szemszögéből a teljes mobil ökoszisztéma olyan időzített bomba, ami csoda, hogy még nem robbant ránk teljesen. Ehhez persze hozzá kell tenni, hogy probléma van bőségesen. Vegyük is sorra azokat a szempontokat, melyeket mindenképpen érdemes megfontolni!

Kezdjük az eszköznél! A kibertámadások az elmúlt években egyre többször veszik célba a hardveres réteget, hiszen egy olyan komplex eszköznél, mint például az okostelefon, könnyen előfordulhat, hogy olyan részegységek kerülnek beépítésre, melyek ismert sebezhetőséggel rendelkeznek és viszonylag könnyen támadhatóvá teszik a platformot.

Olcsóbb vagy régebbi eszközöknél például könnyen jöhet olyan hír a sajtóban, mely után eszközök százmillióinak biztonsága válik kérdésessé, ahogy történt az az Apple eszközök esetében is a biztonságot megvalósító egyik chip sebezhetősége után (https://ipon.hu/magazin/cikk/javithatatlan-sebezhetoseget-talaltak-az-apple-biztonsagi-chipjen). Az ilyen sérülékenységek kihasználásához persze fizikailag hozzá kell tudni férni az eszközhöz, de ez még ilyen eszközöknél is előfordul időnként. Jelen sorok szerzője például mindig hevesen dobogó szívvel adja le okostelefonját a Nemzetibiztonsági Szakszolgálat zárható szekrényeibe. Első lecke: az újabb és a drágább biztonsági szempontból jellemzően jobb, a fizikai hozzáférés pedig sokszor sikeres támadást tesz lehetővé.

Ugorjunk tovább az operációs rendszerre!

A világ szinte kizárólag két operációs rendszert használ: az Apple iOS és a Google Android rendszerét. Mindkét cég gyorsan és hatékonyan javítja rendszereinek biztonsági hibáit, a kérdés csak az, hogy vajon a végfelhasználók ezeket a javításokat mennyi idő után telepítik? Illetve, egy régebbi eszköz mennyi ideig kapja meg egyáltalán a biztonsági frissítéseket?

Egy-egy biztonsági frissítés azt jelenti, hogy az éppen használt operációs rendszer változat valamilyen biztonsági hibát tartalmaz, amelyet kibertámadók ismerhetnek és potenciálisan ki is használhatnak. Ergo, ha nem telepítjük a frissítést, lehetséges támadásnak vagyunk kitéve. Ennek ellenére a felhasználók nem elhanyagolható része akkor sem telepíti a legújabb változatokat, ha a telefon ezt egyébként határozottan szeretné. A referenciaként használt iOS frissítések esetében például a felhasználók nagyjából 40%-a olyan verziót használt, melynél volt már frissebb és biztonságosabb (https://gs.statcounter.com/ios-version-market-share/). Ez az arány az Android felhasználóknál sokkal rosszabb, mivel ahány gyártó, annyiféle operációs rendszer változat, nincsen olyan egységes frissítési séma, mint az Apple-nél. Második lecke: frissítsünk, ahogy tudunk, különösen akkor, ha ezt már a telefon is nagyon szeretné. Az elavult telefonok pedig jellemzően elavult operációs rendszereket jelentenek, melyek az idő múlásával egyre könnyebben támadhatók.

Folytassuk az alkalmazásoknál! Hány alkalmazás van a Nyájas Olvasó telefonjára telepítve? Néhány? Több tucat? Százas nagyságrendű? És mikor frissítette ezeket utoljára? Biztonsági szempontból talán az applikációk okozzák a legtöbb gondot.

A „csak kipróbálom”, az „úgyis ingyen van” mentalitás hozza magával azt, hogy telefonunk tele van biztonsági és adatvédelmi szempontból erősen kérdéses minőségű alkalmazásokkal. Az szinte már természetes, hogy az adatvédelmi szabályozást el sem olvassuk, így azok a felhasználói adatok, melyek egy alkalmazás használata közben keletkeznek, rövid úton a Metánál (azaz Facebook) vagy a Google-nél kötnek ki, hiszen „ha valami ingyen van, mi magunk vagyunk az áru”, azaz a remek „ingyenes” játékszoftverek jellemzően abból élnek, hogy a náluk keletkezett adatokat ezeknek az adatkapitalista cégeknek adják el. Ennél sokkal rosszabb a helyzet akkor, amikor az applikációk eleve csalárd szándékkal kerülnek megírásra. Szerencsére a nagy alkalmazás boltok (Google Play, Apple App Store) kínálatába ezek egyre nehezebben kerülnek be, de az „alternatív” boltok kínálatában, ahol például normál esetben fizetős szoftvereket ingyen ajánlanak vagy olyan alkalmazásokat kínálnak, melyek a nagy boltoknál illegálisak lennének, nyugodtan számíthatunk egy kis „meglepetésre”. Ezek olyan, az alkalmazásokba írt kártékony kódok, melyeket szándékosan adatlopásra, esetleg kriptovaluta bányászatra írtak. Harmadik lecke: mindig olyan alkalmazást használjunk, ami megbízható forrásból jön, olvassuk el az adatvédelmi tájékoztatót és persze mindig frissítsük az applikációt, hogy az ezekben levő biztonsági sebezhetőségek se okozzanak gondot.

A helyhiány miatt biztonsági gyorstalpalónkat fejezzük be a felhasználóknál!

A kiberbiztonsági szakma egyik legtöbbet emlegetett aranyköpése szerint a kiberbiztonsági problémák túlnyomó többségét a szék és a billentyűzet között kell keresni, azaz az emberi hibák nélkül a kibertámadások túlnyomó többsége meg sem történne. Statisztikailag ez minden kétséget kizáróan igaz, de annyival finomítani kell ezt az állítást, hogy a felhasználókat, jellemzően senki sem figyelmezteti arra, hogy a nem körültekintő használatból baj lehet. Erre kiváló példa a FluBot trójai terjedése (https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-csomagkuldo-szolgaltatok-nevevel-visszaelo-malware-terjesztessel-osszefuggo-sms-uzenetekkel-kapcsolatban/). Talán sokakban megmaradt az a 2021. márciusi eset, amikor magyar (és egyébként más országbeli) telefonszámok milliói kaptak SMS értesítést arról, hogy a csomagküldő szolgálat hamarosan kézbesíteni fogja a rendelt csomagot, aminek követése érdekében telepítsünk egy alkalmazást, amit az SMS-ben levő linkről lehet letölteni. Az alkalmazás telepítése után a netbanki hozzáférést próbálta megszerezni, a belépéshez szükséges egyszeri, SMS-ben érkező jelszóval együtt.

Ha a felhasználó először végiggondolja, hogy vár-e egyáltalán csomagot, ha nem kattint a linkre, ha nem telepíti az alkalmazást, a telepítés közben nem kattint többször is a továbbengedésre, az operációs rendszer figyelmeztetése ellenére, a FluBot nem tudott volna ilyen sikeresen terjedni. Negyedik és egyben utolsó lecke: gondolkodjunk! Ami kicsit is gyanús, az valószínűleg megér egy utánaolvasást vagy legalábbis egy kérdést egy információbiztonsághoz értő ismerőstől. A kiberhigiénia ugyanis nem csak személyes ügy. A teljes kibertér biztonsága nagyban függ attól, hogy az egyes felhasználók hogyan viszonyulnak a biztonsághoz.