NEMZETI KIBERBIZTONSÁGI INTÉZET

ÍGY TEHETŐ BIZTONSÁGOSABBÁ A SIGNAL

Hardening javaslatok a Signal üzenetküldő alkalmazáshoz

Az elmúlt időszakban kifejezetten nőtt a Signal felhasználók ellen irányuló kibertámadások száma, amely során a támadók egyre gyakrabban konkrét felhasználókat és eszközöket próbálnak kompromittálni. Több fenyegető aktor tudatosan célozza a Signal (és más titkosított üzenetküldők) felhasználóit **célzott adathalász-kampányokkal**. Többféle technikát alkalmaznak, például **hamis QR-kódokkal** történő eszköz-hozzáférést, **legitim alkalmazások hamis másolatainak terjesztését**, **zero-click** (felhasználói interakciót nem igénylő) **sebezhetőségeket**, illetve **social engineering**-et a felhasználók megtévesztésére.

Az alábbiakban szeretnénk néhány technikát és beállítást bemutatni, amelyekkel megakadályozható vagy legalább megnehezíthető, hogy illetéktelenek hozzáférjenek a Signal fiókunkhoz és üzeneteinkhez.

BIZTONSÁGI ELEMZŐ SZAKTERÜLET

BIZTONSÁGI JAVASLATOK

Regisztrációs zár (PIN) – Extra PIN-kódot kér a fiók újraaktiválásához, hogy más ne tudja csak a telefonszám birtokában átvenni a fiókot. Mivel a Signal alapvetően a telefonszámunkkal működik, annak birtokában könnyen megszemélyesíthetnek minket mások is. Ennek elkerüléséhez, lépjünk be a profilunkba, majd a *Beállítás - Fiók* menüponton belül kapcsoljuk be a *„Regisztrációs zár”* lehetőséget, így egy plusz PIN kóddal lehet csak aktiválni a telefonszámunkat másik eszközön.

Képernyőzár az alkalmazáson belül – A Signal ikon megnyitása után az alkalmazás újra kéri a felhasználó azonosítását a jelszó/ujjlenyomat/FaceID újboli megadásával, így csökkentve annak a kockázatát, hogy idegenek hozzáférhessenek az üzeneteinkhez a készülék felnyitásával. Ez a funkció elérhető *Beállítások - Adatvédelem - Kijelző zárolás* pontban.

Képernyővédelem – Kikapcsolja az üzenet előnézeteket a multitasking (alkalmazás választó) nézetben és akadályozza a képernyőkép készítését saját eszközön. Ez a funkció elérhető *Beállítások - Adatvédelem - Képernyővédelem* pontban.

Önmegsemmisítő üzenetek – Beállíthatjuk, hogy adott idő után automatikusan törlődjenek az üzenetek (pl. néhány óra/nap), így minimalizálhatjuk az érzékeny adatok megmaradását. Lépjünk be egy csevegésbe, ahol ezt a funkciót aktiválni szeretnénk, majd a *bal felső sarokban kattintsunk a profilra*, majd aktiváljuk az *„Eltűnő üzeneteket”*, és válasszuk ki a számunkra megfelelő időtartamot az üzenetek láthatóságára.

Telefonszám láthatóságának korlátozása – Ez a funkció a *Beállítások - Adatvédelem - Telefonszám* pontban érhető el, ahol megadhatjuk ki láthatja a telefonszámunkat és ki találhat meg minket telefonszám alapján Signalon. Ezzel megakadályozhatjuk, hogy ismeretlenek felvegyék velünk a kapcsolatot telefonszámunk alapján.

Társított eszközök ellenőrzése – Egyik legfontosabb pont, hiszen itt láthatjuk milyen eszközökön van bejelentkezve a Signal profilunk. Rendszeresen ellenőrizzük a hozzáadott eszközök listáját, ha ismeretlen eszközt látunk, azonnal töröljük! A profilunkon belül ellenőrizhetjük a társított eszközeinket a *Beállítás - Társított eszközök* menüben.

Üzenetek megjelenítése zárolt képernyőn – Ezzel a beállítással megakadályozhatjuk, hogy például az asztalon felejtett telefonunkról illetéktelenek leolvassák a beérkező üzeneteinkről szóló értesítéseket. A *Beállítás - Értesítések* menüben az *Értesítés tartalma - Mutasd* pontban több lehetőségek közül választhatjuk ki, hogy mik azok, amiket látni szeretnénk egy értesítésből a zárolt képernyőn.

Üzenetek olvasottságának és gépelés láthatóságának kikapcsolása - Az olvasottsági visszajelzés kikapcsolásával csevegőpartnerünk nem látja, hogy olvastuk-e már az üzenetét, így kevesebb információ derül ki a kommunikációs szokásainkról (pl.: időzítés, reakciók). A beállítás hátránya, hogy így mi sem látjuk, hogy elolvasták-e már az üzeneteinket vagy sem. A gépelési visszajelzés kikapcsolásával nem látják, ha gépelünk, így csökkenthető a valós idejű viselkedési minták (pl. reakcióidő, jelenlét) megfigyelhetősége. Ezekkel a beállításokkal nem az üzenetek tartalmát, hanem a kommunikációs metaadatokat védhetjük.

A biztonsági beállítások önmagukban nem elegendők, a támadások túlnyomó többsége továbbra is felhasználói figyelmetlenségre és megtévesztésre épít. Hiába erős a Signal titkosítása, ha a felhasználó gyanús üzeneteket nyit meg, rosszindulatú linkekre kattint, vagy hitelesítési kéréseknek gondolkodás nélkül eleget tesz. Ezért a kockázatcsökkentés kulcsa a **tudatos felhasználói magatartás**, az ismeretlen források megfelelő kezelése, a szokatlan kérések megkérdőjelezése és az alapvető biztonság betartása. Mindig fogadjuk gyanakvással az ismeretlenektől vagy akár ismerőseinktől kapott, de gyanús, szokványostól eltérő hangvételű üzeneteket, illetve rendszeresen ellenőrizzük nem áll-e rendelkezésre frissítés az alkalmazásainkhoz, operációs rendszereinkhez.

1996
NEMZETBIZTONSÁGI SZAKSZOLGÁLAT
NEMZETI KIBERBIZTONSÁGI INTÉZET