FOTÓK: KATONA LÁSZLÓ

Egyre nagyobb az igény a titkosított üzenetküldésre

Üzenetküldők
A legtöbb csevegőszolgáltatás nem tudja garantálni a teljes bizalmasságot

Bordohányi Alexandra

A legtöbb internetező megbízhatatlannak tartja az online üzenetküldő csatornákat a Kaspersky Lab és a B2B International közös kutatása szerint, a megkérdezetteknek mégis csak a 28%-a mondta, hogy nem tárgyal meg személyes témákat online.

Miután a közelmúltban a WhatsApp üzenetküldő alkalmazás titkosította az üzenetküldést a végpontok között, a Viber is biztonságosabb verzióval érkezik: teljes titkosítással, rejtett csevegéssel és távoli törlés funkcióval.

Hiányos biztonság

Az üzenetküldő szolgáltatások, különösen azok, amelyeket más szolgáltatásokkal együtt kínálnak – mint a Facebook Messenger vagy a Google Hangouts – nem képesek a beszélgetések teljes bizalmasságát garantálni, mert a begépelt üzenetek nem titkosított formában jutnak el a szolgáltatóhoz, aki ezt továbbítja, sőt tárolja is. – Ez nem azt jelenti, hogy a szolgáltatón mint harmadik félen kívül a beszélgetések tartalmához nagyon speciális informatikai ismeretek híján más is hozzá tud férni, de csak akkor érdemes őket használni, ha erre vonatkozóan jogi garanciát is vállalnak. Erről az információkat az adatkezelési nyilatkozatában minden szolgáltató közzéteszi a weboldalán – mondta el Pfeiffer Szilárd, a Balasys IT biztonsági szakembere.

Teljes biztonságot azonban ez sem nyújt, a technikai lehetőség megvan az információk hasznosítására. Számos szolgáltatónak pedig törvényi kötelezettsége, hogy tájékoztassa a hatóságokat a beszélgetésekről, ha azok alapján bűncselekmény gyanúja merül fel. – Bízni leginkább azokban az üzenetküldőkben lehet, amelyek kifejezetten a titkosított üzenetküldésre szakosodtak, és részletesen dokumentálják, hogy milyen módszerek és garanciák vannak az üzenetek bizalmasságának megőrzésére. A legfontosabb az – tette hozzá a szakértő –, hogy a virtuális világhoz úgy érdemes viszonyulni, mint a valóshoz: amit nem küldenénk el nyitott borítékban a postán, azt ne küldjük titkosítás nélkül az interneten keresztül se.

A szolgáltató tárol

Csizmazia-Darab István, a Sicontact Kft. vírusvédelmi tanácsadója szerint egyre többször merül fel az az igény, hogy titkosított csatornán keresztül valósítsák meg az online üzenetváltást, ezért elérhetőek olyan megoldások, amelyek biztonságos titkosítást tesznek lehetővé. Egy másik lehetséges megoldás a titkosított e-mail küldésére is használható GPG, mellyel egy privát és egy publikus kulcs segítségével teljesen biztonságos üzenetváltásra nyílik lehetőség. – Meg kell mindenkinek tanulnia, hogy az internet nem felejt, és amit egyszer feltöltöttünk, azt soha többé nem tudjuk letörölni, és nem tudhatjuk, kihez kerülhet még. A küldés után gyakorlatilag nincs efelett többé kontrollunk. Sokan egyébként a licencszerződés szövegét sem olvassák el, pedig a Facebook és a Skype esetében a regisztrációval például azt is jóváhagyjuk, hogy az üzeneteink a szolgáltató tulajdonába kerülnek – hívta fel rá a figyelmet a vírusvédelmi tanácsadó.

Az üzenetküldők nyitott wifi-kapcsolatnál való használata sem javasolt a szakemberek szerint, ekkor ugyanis könnyen lehallgatható a kommunikáció, és az is fontos, hogy minden eszközön fusson vírusvédelmi alkalmazás, mert sok olyan trójai alkalmazás is létezik, amely a háttérben bizalmas adatokat szivárogtat a távoli támadók szervere felé. – A titkosított csatorna igénybevételén felül üzleti és titokmegőrzési megfontolásokból használhatunk virágnyelvet is – tette hozzá –, így az üzenetek illetéktelenek számára semmitmondónak tűnhetnek. Próbáljuk meg tudatosan használni minden internetre kapcsolt eszközünket.

Céges kommunikáció

Hargitai Zsolttól, a NetIQ Novell SUSE Magyarországi Képviseletének üzletfejlesztési igazgatójától megtudtuk: hazánkban a vállalatok alkalmazottai is egyre szélesebb körben használják az azonnali üzenetküldőket a házon belüli kommunikáció során. Ez gyors és hatékony, a telefonálással ellentétben kevésbé zökkenti ki az embereket a munkából, ráadásul szükség esetén visszakeresheto. – A legtöbb ingyenes, azonnali üzenetküldő nem megfelelő az érzékeny, vállalati adatok megosztására, de mivel hatékonyabbá teszik a kommunikációt és így a munkát is, érdemes megvizsgálni, hogyan alkalmazhatóak biztonságosan. A legegyszerűbb, ha nem egy ingyenes megoldást próbálnak biztonságossá tenni, hanem egy, már eleve megbízható, vállalati felhasználásra tervezett megoldást vezetnek be. Ezek ugyanolyan kényelmes kommunikációt tesznek lehetővé – tette hozzá Hargitai Zsolt –, mint amit a felhasználók megszoktak a magánéletben használt programoknál.

Biztonságos üzenetküldők

A szakemberek a legbiztonságosabb üzenetküldőnek az Open Whisper Systemset tartják, mely egyben Edward Snowden kedvenc üzenetküldője is: az alkalmazás mobilról és számítógépről is használható, szöveget, képet és videót is lehet vele küldeni, és telefonálni az appot szintén használó ismerőseinkkel.

Az orosz fejlesztésű Telegram titkosított üzenetküldő használható csevegésre, csoportos beszélgetésre és titkos beszélgetésre is: az üzenetek mellé 1GB korlátig fájlok is csatolhatók, és az elküldött üzenetekhez időkorlátos önmegsemmisítő is beállítható.

A Tox alkalmazás első használatkor generál egy azonosítót a felhasználó számára, melyet annak kell megadnia, akivel kommunikálni akar: ezután csevegésre, telefonálásra és videohívásra is használható a titkosított szolgáltatás.