Maradjon köztünk és a Google között: gondok a Gmail „Bizalmas” módjával

PCLinuxOS Magazine – 2018. augusztus

Írta: Gennie Gebhart és Cory Doctorow az EFF számára, terjesztve a CC-SA-3.0 Creative Commons Licenc szerint

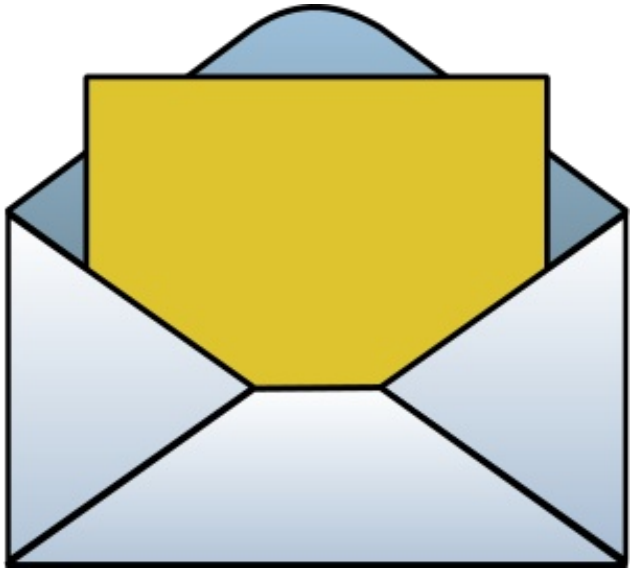
A Gmail új kialakítása egyre több felhasználó számára érhető el és sokan kipróbálhatták az új „Bizalmas” módjot. Miközben a legtöbb jellemzője biztatónak tűnik, a „Bizalmas” mód egyáltalán nem bizalmas. Jobb esetben csak olyanokkal kecsegtet, amit a Gmail nem képes a biztonság és a személyes jelleg területén betartani. Attól tartunk, hogy a Bizalmas mód csökkenti annak a valószínűségét, hogy a felhasználók más, sokkal biztonságosabb eljárásokat keressenek és használjanak. Rosszabb esetben a Bizalmas mód a felhasználókat a Google a falai közé zárja, véleményünk szerint a személyesség és a biztonság hamis érzetét keltve.

A Google az új Bizalmas módról azt állítja, hogy lehetővé teszi az elküldött e-mailek megnyitása és megosztása korlátozását: a Bizalmas módú e-mailt a címzettje nem lesz képes továbbítani, vagy kinyomtatni. Beállítható hozzá „lejárati dátum” is, amikor az e-mail törlődik a címzett fiókjából és egy további biztonsági szintként még egy szöveges üzenetben kód is kellhet az e-mail megtekintéséhez.

Sajnos mindegyik „biztonsági” elem komoly biztonsági problémát vet fel a felhasználó számára.

DRM az e-mail számára

Fontos megjegyezni még az elején, hogy mivel a Bizalmas módú e-mailekben nincs titkosítás, a Google láthatja az üzenetek tartalmát és rendelkezik a szükséges műszaki feltételekkel, hogy a végtelenségig tárolja, függetlenül bármilyen beállított



„lejárati” dátumtól. Más szóval, a bizalmasság a Google irányába nem áll fenn.

Ám a végponttól végpontig tartó titkosítás hiánya ellenére a Google ígéri, a Bizalmas móddal küldhető kinyomtathatatlan, továbbíthatatlan, másolhatatlan e-mail, köszönhetően egy Információs Jogkezelés (IRM) nevű valaminek, amit a Microsoft több mint egy évtizede talált ki (a Microsoft az „Azure Information Protection” kifejezést is használja).

Lássuk, hogyan működik az IRM: a cégek olyan termékeket készítenek, ami ellenőrzi a dokumentumot, hogy van-e „nyomtatás tilos”, vagy „továbbítás tilos” jelzője, és ha ilyet talál, a program kikapcsolja a vonatkozó opciókat. Annak érdekében, hogy a konkurensek ne készíthessenek olyan terméket, ami ezt az ellenőrzést kihagyja, a program kódolja a felhasználói dokumentumot, úgy elrejtve a visszafejtő kódot, hogy azt a felhasználók ne találhassák meg.

Ez elég sekélyes biztonság: ha küldesz valakinek egy e-mailt, vagy dokumentumot, amit megnyithat a számítógépén, a saját helyén, semmi sem akadályozhatja meg abban, hogy képernyőképet, vagy fotót készítsen a képernyőről, amit továbbíthat, kinyomtathat, vagy más módon másolhat.

Ám ez csak egy a Gmail új típusú IRM-jével kapcsolatos problémák közül. Valójában a rendszer biztonságossága nem technikán, hanem a Clinton-korszak copyright szabályozásán alapul. Az 1998-as Digital Millennium Copyright Törvény 1201. szakasza (DMCA 1201) szerint olyan kereskedelmi termék készítése, ami kikerüli az IRM-et, potenciális bűncselekmény, 5 év és 500 000 USD büntetést von maga után első esetben. A DCMA 1201 annyira tágan és felületesen fogalmaz, hogy a Google-IRM bármilyen hibás kezelése miatt a bíróságon köthetsz ki.

Úgy véljük, hogy a „biztonsági” termékek nem alapozhatnak bírósági kikényszerítésre, mint garanciára, hanem inkább olyan technológiára, mint a végponttól végpontig tartó titkosításra, ami tényleges matematikai biztosítékot ad a bizalmasságra. Hitünk szerint, a „Bizalmas mód” kifejezés egy olyan működésre, ami nem biztosít bizalmasságot, az információbiztonság szerinti értelmezést tekintve félrevezető.

„Lejáratos” üzenetek

Hasonlóképpen, úgy véljük, hogy a Bizalmas módban beállítható „lejárati dátum” az érzékeny e-mailekre azt az érzetet keltheti a a felhasználókban, hogy az üzentük teljesen eltűnnek, vagy megsemmisülnek a beállított dátum után. A valóság pedig komplikáltabb. A „rövidlejáratú”, vagy „eltűnő”

üzenetek, olyasmik, mint a Bizalmas mód „lejáratos” üzenete, nem a személyes jelleg csodaszerei. Technikai szempontból számos módja van a lejárat kikerülésének: a címzett képernyőképet készíthet az üzenetről, vagy lefényképezheti a lejárat előtt.

Ám a Google-féle eljárásnak van egy további bökkenője. Ellentétben azzal, amit a lejárat sugall, az üzenet továbbra is valahol ott van a lejárati dátum után is, például a te Elküldött üzenetek fiókodban. Ez a Google-tulajdonság nem teljesíti a rövidlejáratú üzenetváltás egyik legfontosabb biztonsági feltételét: annak biztosítását, hogy a szokásos üzletmenet során, a lejárt üzenetet nem állíthatja helyre egyik fél sem. Minthogy a Bizalmas módban küldött e-mailek továbbra is visszanyerhetők – a küldője és a Google által – a lejáratot követően, úgy véljük, lejáratosnak hívni félrevezető.

Telefonszámok felfedése

Ha kijelölöd az „SMS” jelszóküldés opciót, a fogadó részéről kétlépcsős azonosítási kód kell az e-mail olvasásához. A Google generál és elküld egy kódot a fogadónak, ami azt jelenti, hogy a Google-nak meg kell adnod a címzett telefonszámát – vélhetően a címzett beleegyezése nélkül.

Ha Google-nak még nem lenne meg ez az információ, az SMS „passcode” opció a Google-nak lehetőséget ad potenciális azonosítási információk gyűjtésének új módjára: úgymint egy e-mail cím és egy telefonszám.

Ez a fajta „személyesség” ártalmas lehet azok számára, akik személyes és biztonságos kapcsolattartást akarnak, illetve kellemetlenül érintheti a címzettet, aki talán nem akarja a telefonszáma felfedését.

Nem annyira bizalmas

Végül, az előbbiekben felvázoltak miatt, az EFF szerint a Gmail új „Bizalmas módja”, félrevezető. Semmi bizalmas sincs a titkosítatlan e-mailben úgy általában és a Gmail új „Bizalmas” módjában konkrétan. Noha az új mód korlátozott céges, vagy vállalati környezetben működhet, hiányoznak belőle a személyesség garanciái és olyan tulajdonságok, amik a legtöbb felhasználó számára a biztonságos kommunikáció lehetőségének biztosítékát jelentik.

ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD