Jön a biztonságos Zoom, de fizetni kell majd érte

A szolgáltató még nem döntötte el, hogy pontosan kiktől szedne majd pénzt, de az biztosnak tűnik, hogy az end-to-end titkosítás fizetős funkció lesz a zoomos videokonferenciákon.

A Zoom videokonferencia-szolgáltató új tervei szerint magasabb szintű biztonságot nyújtana a fizetős ügyfeleinek és bizonyos intézményeknek, így az oktatási szervezeteknek, azonban az ingyenes otthoni felhasználásban nem vezeti be az end-to-end (végponttól végpontig tartó) titkosítást. A Reuters múlt hét végi beszámolója a Zoom biztonsági tanácsadóját, *Alex Stamos*t idézi, aki néhány nappal ezelőtt civil jogvédő szervezetekkel konzultált a tervezett változtatásokról.

A korábban a Facebook biztonsági vezetőjeként dolgozó szakember szerint a társaság tervei még nem véglegesek ezzel kapcsolatban, de az elképzeléseket technológiai, informatikai biztonsági és üzleti megfontolások egyaránt befolyásolják, így minden bizonnyal egy köztes megoldásra számíthatunk. Lehet, hogy a titkosított kommunikációért mindenkinek fizetnie kell, de az is lehet, hogy ingyenesen biztosítják majd bizonyos non-profit szervezeteknek vagy akár politikai menekülteknek is.

A Zoom már április végén azt közölte, hogy világszerte több mint 300 millióan lépnek be napi szinten az általa hosztolt videokonferenciákra, ez a szám pedig azóta minden bizonnyal tovább növekedett. A szolgáltatás népszerűségének villámgyors növekedésével azonban biztonsági aggályok is felmerültek: a Zoomot több vállalat és állami szervezet is tiltólistára tette, és hivatalos vizsgálatok próbálják tisztázni az alkalmazás adatvédelmi gyakorlatainak és transzparens működésének kérdéseit.

Két tűz között kell jó megoldást találniuk

A társaság korábban már bejelentett egy 90 napos ütemtervet, hogy kezelje a videokonferencia-szolgáltatás működésében felmerülő problémákat, és ennek részeként a korábbinál komolyabb titkosítási funkciókat vezetett be. Sor került a vállalat történetének első cégfelvásárlására is, amelynek célpontja a biztonságos üzenetküldő és fájlmegosztó szolgáltatást fejlesztő Keybase volt, hogy a startup technológiáival és tapasztalatával erősítsék a Zoom alkalmazás biztonsági funkcióit.

Stamos és más biztonsági szakemberek megbízása is ezeknek a lépéseknek a sorába illeszkedik. A teljes, minden egyes Zoom konferenciára vonatkozó titkosítás bevezetése azonban egyelőre semmiképpen sem reális: a vállalat nehezen tudna pénzt keresni, ha teljesen ingyenessé tenne egy szofisztikált és nagyon drágán üzemeltethető szolgáltatást. Bár a Facebook hasonlót tervez a Messengerrel, a közösségi hálózat forrásait össze sem lehet hasonlítani a Zoommal, az olyan piaci szereplők pedig, mint például a Signal, non-profit alapon működnek. Mindenki más számára marad az ingyenes alapszolgáltatásokból és magasabb szintű, de fizetős megoldásokból álló modell.

Érdekes egyébként, hogy amíg a New York-i főügyész hivatala éppen a Zoom biztonsági kondícióit vizsgálja, tekintettel a terhelés nagyságrendjének növekedésére, a fiatalok fokozott védelmére vagy az átláthatósági jelentésekre, addig az amerikai igazságügyi minisztérium és sok képviselő is problémásnak tartja az erős titkosítást használó kommunikációs alkalmazásokat, így a Zoomnak a

másik oldalról is fokozódó nyomással kell számolnia, ha komolyabb lépéseket tesz ezen a területen.

Bár a jogvédők nem üdvözölték egyhangúlag a legfrissebb terveket, a Reuters által megkérdezett civil szervezetek képviselői között olyan is volt, aki észszerű kompromisszumnak tartja a Zoom új stratégiáját. A fizetős modell nagyban segítené a spammerek és az ingyenes csatornákat kihasználó rosszindulatú szereplők kiszűrését, bár a végponttól végpontig terjedő titkosítás (ahol még a szolgáltató maga sem figyelheti valós időben a kommunikációt) a másik oldalról eszközöket is ad a bűnözők kezébe.

A hírügynökségnek utóbb a Zoom szóvivője is megerősítette, hogy a cég dolgozik a teljes titkosítás bevezetésén, ami egyrészt a műszaki tervezést jelenti, másrészt annak a modellnek a kidolgozását, amelynek alapján meghatározzák majd az érintett ügyfelek körét.

Forrás: https://bitport.hu/jon-a-biztonsagos-zoom-de-fizetni-kell-majd-erte

Válogatta: Fonyó Istvánné