SZABÁLYOZÁSI KEZDEMÉNYEZÉSEK A RANSOMWARE KIBERTÁMADÁSOK KEZELÉSÉRE

SZERZŐ: DR. DOMOKOS MÁRTON SZENIOR TANÁCSADÓ|REGIONÁLIS ADATVÉDELMI CSOPORT KOORDINÁTORA, KERESKEDELMI JOG, TMT, ADATVÉDELEM

2023-ban az egyik legtöbbet emlegetett kiberbiztonsági kockázat a „ransomware", vagyis a zsarolóprogramok segítségével elkövetett kibertámadás, amikor a bűnözők titkosítják a megtámadott szervezet által kezelt adatokat, és a titkosítást csak egy meghatározott pénzösszeg (váltságdíj) megfizetése ellenében oldják fel, illetve a váltságdíj elmaradása esetén nyilvánosságra hozzák, vagy továbbértékesítik az adatokat.

A legújabb jelenség a „Ransomware-as-a-Service" megjelenése - a rosszindulatú felhasználók akár előre kifejlesztett „zsarolóprogram-csomagot" is vásárolhatnak az interneten.

A ransomware által felvetett specifikus problémák mind a jogalkotók, mind a kiberbiztosítási piac szereplőinek a figyelmét felkeltették. Ebben a cikkben megvizsgáljuk a legfontosabb szabályozási kezdeményezéseket és a joggyakorlat fejleményeit.

Magas szintű szabályozási kezdeményezések az Amerikai Egyesült Államokban

Az Amerikai Egyesült Államok (USA) kormányzatának frissen kidolgozott Nemzeti Kiberbiztonsági Stratégiája (National Cybersecurity Strategy)[1] átfogó szövetségi és nemzetközi megközelítést javasol a zsarolóvírusok növekvő problémájának kezelésére - várhatóan 2023 folyamán dől el, ez milyen formában valósul meg, és milyen tanulságokkal szolgál más országok számára.

AAz USA kormányzatának másik figyelemreméltó kezdeményezése a nemzetközi zsarolóvírus-ellenes kezdeményezés (International Counter Ransomware Initiative - CRI)[2], melynek célja, hogy az EU, valamint 36 másik ország konkrét együttműködési intézkedéseket dolgozzanak ki a ransomware támadások elterjedése ellen. A CRI öt munkacsoporttal dolgozik: reziliencia (Litvánia és India vezetésével), zavarok elhárítása (Ausztrália vezetésével), jogszabálysértő finanszírozás elleni küzdelem

[1] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[2] https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/fact-sheet-the-second-international-counter-ransomware-initiative-summit/

(Egyesült Királyság és Szingapúr vezetésével), közszféra-magánszektor partnerség (Spanyolország vezetésével) és diplomácia (Németország vezetésével). A CRI keretében kidolgozásra kerülne egy „nyomozói eszköztár" - tanulságok és stratégiák kidolgozása a ransomware támadásokra való reagáláshoz, trendfigyelés, valamint erőforrások biztosítása kapacitásépítéshez. További figyelemreméltó eleme a tervezetnek, hogy közös lépéseket irányoz elő annak megakadályozására, hogy a támadók a kriptovaluta ökoszisztémáját használhassák a kapcsolódó fizetések lebonyolítására. Ide tartozik a bitcoin pénztárcákkal kapcsolatos információk megosztása, valamint pénzmosás elleni/terrorizmus finanszírozása elleni nemzetközi (AML/CFT) szabványok és ügyfélazonosítási (KYC) szabványok kidolgozása és végrehajtása a kriptovaluták használatával kapcsolatban.

Franciaország - kötelezettségek a biztosítási szerződésekkel kapcsolatban

A ransomware által jelentett fenyegetést a kiberbiztosítások feltételei is folyamatosan tükrözik, adott esetben a biztosítási díjak növelésével, valamint a biztosítási események körének finomításával. Úgy tűnik, hogy az ilyen jellegű biztosításokkal kapcsolatban specifikus jogszabályok is meghatározzák majd, milyen kötelezettségei vannak a biztosítóval szerződő feleknek kibertámadások esetén.

A francia biztosítási törvény új, 2023. április 24-én hatályba lépő L12-10-1 cikke új kötelezettségeket vezet be a kibertámadások által érintett felek számára. Azok a szervezetek, akiknek az automatizált nyilvántartási rendszerét kibertámadás érte, csak akkor igényelhetik a biztosításuk alapján járó - a „jogsértésből eredő veszteségek és károk" fedezetére szolgáló - összeg megtérítését, ha a tudomásszerzését követő 72 órán belül jelezték a támadást az illetékes hatóság számára. Az értesítési kötelezettség fő célja egyrészről, hogy felgyorsítsa a nyomozást, megkönnyítse az elkövetők azonosítását, és elkerülje az anyagi veszteséget, másrészről pedig az, hogy az illetékes hatóságok által gyűjtött adatok lehetővé tegyék a kibertámadások jobb megértését. A kötelezettség bármely típusú biztosításra vonatkozik, nem csak a kiberbiztosításokra, és kiegészíti az egyéb, a GDPR és a NIS 2 Irányelv alapján fennálló incidens-bejelentési előírásokat.

A francia jogszabály módosítás alapján bekövetkező változások tanulságosak lehetnek más országok jogalkotói, valamint a biztosítási szektor szereplői számára, a törvényszöveg azonban számos gyakorlati kérdést nyitva hagy.

Az „illetékes hatóság” fogalmát a jogszabály például nem határozza meg részletesen, de a bejelentést feltehetőleg a rendőrség számára kell megtenni. A jogszabályból nem derül ki az sem, hogy milyen formában kell a bejelentést teljesíteni, és hogy a megtámadott szervezeten belül melyik döntéshozó szint tudomásszerzésétől számítandó a 72 órás időablak. Bizonytalan az is, hogy a rendelkezés kifejezetten megtiltja-e a biztosítóknak az alapulfekvő összeg kifizetését, vagy ezt esetről-esetre mérlegelhetik.

A biztosításokkal kapcsolatos bírósági gyakorlat az Amerikai Egyesült Államokban

Érdekes tanulságul szolgál az Emoi Services LLC kontra Owners Insurance Company ügy[3], amelyben az Ohio-i Legfelsőbb Bíróság megállapította, hogy a szoftver olyan immateriális tárgy, amelyet nem érhet közvetlen kár vagy veszteség, ha a felperes nem volt képes hozzáférni vagy használni a szoftvert egy zsarolóvírus-támadás során.

Az Emoi Services számítógépes szoftvercég orvosi alkalmazásokkal kapcsolatos online szolgáltatásokat nyújt egészségügyi szolgáltatóknak. 2019 szeptemberében ransomware támadás indult a társaság ellen,titkosítva annak szoftvereit, és használhatatlanná téve online szolgáltatásait.

Az Emoi körülbelül 35.000 USD váltságdíjat fizetett a visszafejtési kulcsokért cserébe. A visszafejtési folyamatot követően az Emoi rendszereinek és fájljainak többsége visszaállt normál működési állapotába.

A kibertámadás idején az Emoi az Auto-Owners Insurance Group nevű biztosítónál tartott fenn biztosítást. A biztosító szerint a kötvény „elektronikus berendezésekre” vonatkozó rendelkezései nem fedezik a károkat, vagyis az Emoi nem jogosult az általa birtokolt, bérelt vagy ellenőrzött „médiában” bekövetkezett közvetlen kár vagy veszteség megtérítésére, valamint az elvesztett adatok azonosításához és helyreállításához szükséges költségek megtérítésére. Az Ohio-i Legfelsőbb Bíróság egyetértett ezzel az érveléssel - véleménye szerint „a szoftver olyan immateriális tárgy, amely nem szenvedhet közvetlen fizikai veszteséget vagy közvetlen fizikai kárt”.

Figyelemmel az ítélet megállapítására, fontos minden esetben részletesen megvizsgálni a biztosítási feltételeket, hogy megfelelően kiterjednek-e egy ransomware támadás által okozott károkra.

Jogszabályi tiltás a váltságdíj kifizetésére

Az Amerikai Egyesült Államokban a Pénzügyminisztérium Pénzügyi Bűnüldözési Hálózata

[3] https://law.justia.com/cases/ohio/supreme-court-of-ohio/2022/2021-1529.html

(Department of the Treasury's Financial Crimes Enforcement Network - FinCEN) és a Külföldi Vagyonellenőrzési Hivatal (Office of Foreign Assets Control - OFAC) 2020. október 1-jén iránymutatás bocsátottak ki a ransomware támadásokkal kapcsolatos váltságdíjak kifizetésével teljesítésével kapcsolatos lehetséges jogi kockázatokról. Az OFAC szerint az egyik fő kockázat, hogy a kifizetés valamely szankciós listán szereplő személy vagy szervezet javára történik, ezzel pedig a kifizetést teljesítő fél megszegi a szankciót előíró jogszabályt.

Egyes esetekben a váltságdíj kifizetése a „terrorizmus finanszírozása" bűncselekményét is megvalósíthatja. Az Egyesült Királyságban a Nemzeti Kiberbiztonsági Központ (National Cyber Security Centre - NCSC) és az adatvédelmi hatóság (Information Commissioner's Office - ICO) ezért közös nyilatkozatukban[4] rögzítették, hogy nem támogatják a ransomware támadások során a váltságdíj kifizetését. Az Egyesült Királyság gyakorlata szerint ugyanis nem szükséges, hogy az elkövető ténylegesen tudatában legyen annak, hogy a váltságdíj kifizetésével terrorcselekmény elkövetését támogatja - elegendő, ha az elkövető által objektíven ismert információk alapján észszerűen gyanítható, hogy a váltságdíjat terrorcselekmény támogatására használják.

Az USA-ban eddig Észak-Karolina tiltotta meg jogszabályban az állami szerveknek és a helyi önkormányzatoknak, hogy ransomware támadást követően váltságdíjat fizessenek. A jogszabály azt is megtiltja az érintett szerveknek, hogy kommunikáljanak a támadóval, a ransomware támadást pedig jelenteni kell az illetékes hatóságnak (North Carolina Department of Information Technology). A jogszabály elfogadásának indoka az állami szerveket ért ransomware támadások megnövekedett száma: 2022. április 8-án a North Carolina A&T Egyetemet például zsarolóvírus-támadás érte, amely megszakította az iskola vezeték nélküli kapcsolatait, és számos online oktatási eszközt leállított. Észak-Karolina példáját követve a pennsylvaniai szenátus a közelmúltban jóváhagyott egy törvényjavaslatot[5], amely tiltja közpénzek felhasználását váltságdíj kifizetésére, kivéve, ha a kormányzó engedélyezi. New York állam jogszabálytervezete általánosságban tiltaná a váltságdíj kifizetését mind az állami, mind a magánszektorban.[6]

A szervezeteknek érdemes tehát felülvizsgálniuk a hatályos kockázatkezelési és incidenskezelési eljárásaikat, hogy tartalmaznak-e rendelkezéseket a ransomware támadók ellenőrzésére, különös tekintettel a pénzmosás-ellenes és a szankciós szabályoknak való megfelelés, valamint a bűnüldöző szervek és más kormányzati szervek bevonása szempontjából.

[4] https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/07/ico-and-ncsc-stand-together-against-ransomware-payments-being-made/
[5] https://www.legis.state.pa.us/CFDOCS/Legis/PN/Public/btCheck.cfm?txtType=PDF&sessYr=2021&sessInd=0&billBody=S&billTyp=B&billNbr=0726&pn=1326
[6] https://www.nysenate.gov/legislation/bills/2021/s6806