Sajtóközlemény

Jelentős veszteséget okoz a kiberbűnözés a vállalatoknak, a legtöbb kiberbiztonsági kárigény mögött azonban a szervezeten belüli hibák állnak

- Az Global Corporate & Specialty (AGCS) több mint 1700 kiberbiztonsággal kapcsolatos vállalati kárigényt elemezve arra a következtetésre jutott, hogy a legköltségesebb kiberbiztonsági károkat az olyan külső események okozzák, mint a szolgáltatás megtagadással járó (Distributed Denial-of-Service) támadások. Bár kisebb pénzügyi kárt okoznak, azonban az elemzés szerint gyakoribbak az emberi hibához vagy a rendszermeghibásodáshoz hasonló belső incidensek.
- A kiberbiztonsági kárigények szempontjából az üzletmenet-folytonosság megszakadása a legfőbb költségtényező. A vállalatok egyre inkább támaszkodnak az online értékesítésre, ezért az adatok vagy a szolgáltatások elérésének ellehetetlenülése jelentős hatást gyakorolhat a bevételre.
- A zsarolóvírus-támadások növekvő térnyerése, a komolyabb adatvédelmi incidensek költségei, valamint a Covid–19 nyomán kialakult munkakörnyezet jelentős kiberbiztonsági kockázatot hordoz magában a jövőre nézve.

A legköltségesebb, kiberbiztonsággal kapcsolatos biztosítási károkért a vállalatokat érő külső támadások okolhatók, ám számszerűen a munkavállalók hibáiból és a technikai problémákból fakadó kárigények a leggyakoribbak – világít rá az Allianz Global Corporate & Specialty (AGCS) új, kiberbiztonsági trendeket elemző jelentése. (*Managing The Impact Of Increasing Interconnectivity – Trends In Cyber Risk*). Ebben összesen 1736 eset, és mintegy 660 millió EUR értékű, kiberbiztonsághoz kapcsolódó biztosítási kárigény elemzése olvasható, az AGCS és egyéb biztosítók által 2015 és 2020 között kezelt esettanulmányok alapján.

„Napjaink kiberbiztonsági kárigényértékének döntő része elosztott szolgáltatásmegtagadással járó (DDoS) támadásokhoz, vagy adathalászathoz és zsarolóvírus-kampányokhoz hasonló incidensek okozta veszteségeknek tulajdonítható” – nyilatkozta Catharina Richter, az AGCS részét képező Allianz kiberbiztonsági kompetenciaközpontjának (Allianz Cyber Center of Competence) globális vezetője. „Noha a sajtó a kiberbűnözésről ír, a mindennapi rendszermeghibásodásokkal, informatikai szolgáltatáskimaradásokkal és az emberi hibákkal összefüggő incidensek szintén problémát jelenthetnek a vállalatok számára – még akkor is, ha pénzügyi hatásuk általában nem számít súlyosnak. A munkáltatóknak és a munkavállalóknak össze kell fogniuk a tudatosságnövelés és a kiberreziliencia fokozása érdekében.”

Az AGCS tudomására hozott, kiberbiztonsághoz kapcsolódó biztosítási kárigények száma egyenletesen nőtt az elmúlt években. 2016-ban, amikor a kiberbiztonság még viszonylag új kategóriának számított biztosítási berkekben, mindössze 77 kárigényt jegyeztek, ám 2019-re

ez a szám elérte a 809-et. 2020-ban az AGCS már az első három negyedévben 770 kárigénnyel foglalkozott. A kárigények stabil növekedését részben a globális kiberbiztosítási piac bővülése ösztönözte, amelynek értékét a Munich Re jelenleg nagyjából 7 milliárd USD összegre becsüli. Az AGCS 2013-ban kezdett kiberbiztonsági biztosítást kínálni, és 2019-ben több mint 100 millió EUR összegű bruttó díjbevételre tett szert ebben a szegmensben. Ugyanakkor a jelentés azt is kiemeli, hogy a szervezetek kiberbűnözés kapcsán felmerült átlagos költségeiben öt év alatt 70 százalékos növekedés figyelhető meg, amelyek így elérik a 13 millió USD összeget, míg a biztonsági incidensek átlagos száma 60 százalékkal emelkedett[1].

A jelentés szerint az elemzett kárigények értékének nagy részét (85%) külső incidensekből – például DDoS-támadásokból, adathalászatból és rosszindulatúprogram-/zsarolóvírus-kampányokból – származó károk teszik ki, amelyet a rosszindulatú belső tevékenységek (9%) követnek a sorban – noha utóbbiak nem gyakoriak, igen költségesek lehetnek. Számszerűen a véletlenségből fakadó belső incidensek – például a munkavállalók mindennapi feladatok elvégzése közben vétett hibái, az informatikai szolgáltatáskimaradások vagy platform-üzemleállások, a rendszerek és a szoftverek terén felmerült áttelepítési problémák vagy az adatvesztés – okolhatók az elemzett kiberbiztonsági kárigények több, mint feléért (54%), azonban ezek pénzügyi hatása többnyire korlátozott a kiberbiztonsági incidensekével összevetve. A súlyosabb incidensek esetében azonban a veszteségek gyorsan megszaporodhatnak.

Az üzletmenet-folytonosság megszakadása (többek között az enyhítésre fordított költségek és a felelősségbiztosítás) a kiberkárok mögött meghúzódó legfőbb költségtényező, amely a jelentésben elemzett összes kárigény értékének nagyjából 60 százalékát teszi ki. Ezt az adatvédelmi incidensek kezelése során felmerült költségek követik a sorban.

A jelentés szerint a kiberbiztonsági környezet támasztotta kihívások várhatóan a jövőben is fejfájást okoznak majd. A vállalkozások és a biztosítók számos nehézséggel néznek szembe. Ilyenek az üzletmenet-folytonosság költségesebb megszakadásai, a zsarolóvírus-incidensek gyakoriságának növekedése, a súlyosabb adatvédelmi incidensek szigorúbb szabályozásból és peres ügyekből fakadó, költségesebb következményei, valamint a politikai súrlódások kibertérben lezajló, állami támogatású támadások formájában megnyilvánuló hatása. Az AGCS egy új podcast keretében is körüljárja az említett trendek hatását.

A távmunka koronavírus-világjárvány okozta rendkívüli térnyerése is kihívást jelent. A munkavégzés helyét elhagyni kényszerülő munkavállalók új céltáblát jelentenek a kiberbűnözők számára a hálózatokhoz és az érzékeny adatokhoz történő hozzáférés során. A rosszindulatú programokkal és zsarolóvírusokkal kapcsolatos incidensek a beszámolók szerint több, mint egyharmadukkal nőttek 2020 eleje óta, a koronavírus témájával foglalkozó online csalások, és a világjárványról szóló adathalász-kampányok pedig továbbra is jelen vannak a mindennapokban. Emellett az emberi hibákból vagy a technikai meghibásodásból eredő incidensek potenciális hatása is felerősödhet.

Noha a kitettség fokozódik, egyelőre nem jelenthető ki, hogy a Covid–19-járvány közvetlen előidézője lenne a kiberbiztonsági kárigényeknek. Az AGCS már találkozott az első néhány olyan kiberbiztonsági kárigénnyel, amely közvetett formában a Covid–19 nyomán kialakult környezetnek tulajdonítható. Ilyenek többek között azok a zsarolóvírus-támadások, amelyek

[1] Accenture/Ponemon Institute, The Cost of Cyber Crime

a nagyobb arányú távmunkára történő átálláshoz köthetők. Egyelőre azonban túl korai lenne megerősíteni, hogy szélesebb körű trendről van szó.

A zsarolóvírus-támadások veszélyének jelentős fokozódása

A már eddig is igen gyakorinak számító zsarolóvírus-incidensek egyre nagyobb károkat okoznak, és egyre többször veszik célba a nagyvállalatokat kifinomult támadásokkal és komoly összegű követelésekkel. Az elmúlt évben világszerte közel félmillió zsarolóvírus-incidenst jelentettek, amelyek legalább 6,3 milliárd USD összegbe kerültek a szervezeteknek – és ez az összeg még csak a zsarolók követeléseinek teljesítését fedi le[2]. Az incidensek kezelésével összefüggő költségek teljes összege a becslések szerint jócskán meghaladja a 100 milliárd USD összeget.

„Egyre szélesebb körben elérhetők a csúcskategóriás hackereszközök, és ennek a trendnek a »kibertérben elkövetett hackertámadások egyre növekvő kereskedelmi hasznosítása« képezi a mozgatórugóját. A bűnözők körében egyre elterjedtebb az a gyakorlat, hogy a rosszindulatú programokat más támadóknak adják el, akik zsarolás útján próbálnak kifizetéseket kicsikarni a célirányosan kiválasztott vállalkozásokból" – nyilatkozta Marek Stanislawski, az AGCS globális kiberbiztonsági kockázatvállalásért felelős vezetője. „A kizsarolt összegek azonban csak egy része a problémának. A legsúlyosabb károk az üzletmenet-folytonosság megszakadásából fakadnak: a leállások hosszabb ideig tartanak, a rendszer és az adatok helyreállítási költségei pedig gyorsan magasra szökhetnek."

Az üzletmenet-folytonosság megszakadása és a digitális ellátási lánc sebezhetősége egyre nagyobb veszélyt jelent

„Az alapvető fontosságú rendszerek és adatok elvesztése – függetlenül attól, hogy a háttérben zsarolóvírus, emberi mulasztás vagy technikai meghibásodás áll-e – gyorsan térdre kényszerítheti a szervezeteket napjaink digitális gazdaságában" – vélekedik Joerg Ahrens, az AGCS biztosítási kötvények lejárta után rendezett kárigényekért felelős globális vezetője. „Amennyiben hosszabb ideig nem férünk hozzá az adatokhoz, az jelentős hatással lehet a bevételre – például, ha egy vállalat nem tud megrendeléseket fogadni. Ugyanez a helyzet akkor is, amikor egy online platform nem érhető el valamilyen technikai hiba vagy kiberincidens miatt. A platformot használó vállalatok komoly károkat szenvedhetnek, különösen napjainkban, amikor mindenki egyre nagyobb mértékben hagyatkozik az online értékesítésre vagy a digitális ellátási láncokra."

Adatvédelmi incidensek és állami támogatású támadások

Az informatikai rendszerek és a kibereseményekösszetettebbé válásával, valamint a felhő terjeszkedésével és a harmadik felek szolgáltatásainak elterjedésével egyre magasabbra szöknek a kritikus adatvédelmi incidensek kezelésének költségei. Az adatvédelmi szabályozások – amelyek az utóbbi időben számos országban szigorúbbá váltak – szintén fontos költségtényezőt jelentenek, az erőteljesebb felelősségbiztosítással, valamint a csoportos keresetek lehetőségével együtt. Az úgynevezett megaméretű adatvédelmi incidensek (amelyek több mint egymillió rekordot érintenek) egyre gyakoribbak és költségesebbek: jelenleg átlagosan 50 millió USD összegre[3] rúgnak, ami 20 százalékos növekedésnek számít a 2019-es adatokhoz képest.

[2] Emsisoft, Infosecurity Magazine, Ransomware Costs May Have Hit $170bn in 2019
[3] IBM Security, Ponemon Institute, Cost Of A Data Breach Report 2020

A kibertámadásokban megfigyelhető, fokozódó állami részvétel hatása szintén egyre aggasztóbb. Az olyan jelentős események, mint például a választások vagy a Covid–19 ideális lehetőséget jelentenek a támadások végrehajtására. A Google beszámolója szerint 2020-ban negyedévente több mint 11 ezer potenciális kormányok által szponzorált kibertámadást kellett blokkolnia[4]. Az elmúlt években az infrastruktúra kritikus elemei – például a kikötők, terminálok és olaj- vagy gázkitermeléssel foglalkozó létesítmények – kerültek kibertámadások és zsarolóvírus-kampányok kereszttüzébe.

Felkészülés, gyakorlás és megelőzés

A munkavállalók felkészítése és képzése jelentősen csökkentheti a kibereseményekkövetkezményeit, különösen az adathalász és az üzleti e-mail-fiókokkal történő visszaélést célzó kísérletek terén, amelyekben gyakran emberi hibák is szerepet játszanak. Emellett a zsarolóvírus-támadások enyhítésében is segítséget nyújthatnak, bár a megfelelő védelemmel ellátott biztonsági másolatok is mérsékelhetik a károkat. A kereskedelmileg erősen szervezett kiberbűnözés leküzdéséhez elengedhetetlen továbbá az ágazatközi információcsere és a vállalatok közötti együttműködés, amely közös biztonsági normák kidolgozását és a kiberreziliencia javulását eredményezheti. Ennek jó példája a kiberbiztonság fokozását szolgáló Charter of Trust (Bizalmi Charta) kezdeményezés.

A Covid–19 teremtette környezet újabb kihívásokat tartogat. Az otthoni munkavégzés széles körű elterjedése miatt elengedhetetlen a hozzáférési és hitelesítési pontok biztonsága, de a szervezeteknek a megfelelő hálózati kapacitásról is gondoskodniuk kell, ugyanis szolgáltatáskimaradás esetén ez is jelentősen befolyásolhatja a kiesett bevételt.

****

Sajtókapcsolat

Johannesburg: Lesiba Sethoga	+27 112147948	lesiba.sethoga@allianz.com
London: Ailsa Sayers	+44 203 451 3549	ailsa.sayers@allianz.com
München: Heidi Polke	+49 89 3800 14303	heidi.polke@allianz.com
Daniel Aschoff	+49 89 3800 18900	daniel.aschoff@allianz.com
New York: Sabrina Glavan	+1 973 876 3902	sabrina.glavan@agcs.allianz.com
Párizs: Florence Claret	+33 0158 85 88 63	florence.claret@allianz.com
São Paulo Camila Corsini	+55 11 3527 0235	camila.corsini@allianz.com
Szingapúr: Wendy Koh	+65 6395 3796	wendy.koh@allianz.com

Az Allianz Global Corporate & Specialty-ről

Az Allianz globális vállalati és szakirányú üzletága (Allianz Global Corporate & Specialty SE, AGCS) az Allianz Csoport vezető globális vállalati biztosítója és kulcsfontosságú szervezeti egysége. Kereskedelmi, vállalati és speciális kockázatok széles skáláját lefedő kockázati tanácsadást, vagyon- és balesetbiztosítási megoldásokat, valamint alternatív kockázatátruházást kínálunk 10, külön erre a célra létrehozott üzletágban.

Ügyfélkörünk éppoly sokszínű, mint az üzleti világ: a skála a Fortune Global 500-as listáján szereplő nagyvállalatoktól a kisvállalkozásokon át egészen a magánszemélyekig terjed. A legnagyobb fogyasztói márkák, technológiai vállalatok vagy a globális légi közlekedési és hajózási üzletág éppúgy megtalálhatók köztük, mint borászatok, műhold-üzemeltetők vagy hollywoodi filmgyárak. Mind az AGCS-hez fordulnak, ha okos megoldásra van szükségük a

[4] Google Threat Analysis Group, How We're Tackling Evolving Online Threats, 2020. október

mostani dinamikus, multinacionális üzleti környezet által felvetett, legnagyobb és legösszetettebb kockázati kérdésekben, és nyugodtak lehetnek afelől, hogy a biztosítási díjak megállapítása terén kiemelkedő teljesítményt nyújtunk.

Az AGCS a világ 32 országában rendelkezik saját csapattal, és több mint 200 országban és területen van jelen az Allianz Csoport hálózatán és partnerein keresztül. Munkavállalóinak száma meghaladja a 4450 főt. Az Allianz Csoport egyik legnagyobb vagyon- és balesetbiztosítási egységeként erős és stabil pénzügyi minősítésekkel rendelkezünk. 2019-ben az AGCS globálisan bruttó 9,1 milliárd EUR összegű díjbevételt ért el.

www.agcs.allianz.com

LinkedIn:

Twitter: @AGCS_Insurance

A jövőre vonatkozó állításokkal kapcsolatos figyelmeztetés

A jelen dokumentumban szereplő kijelentések jövőbeni kilátásokra és várakozásokra is vonatkozhatnak, amelyek a vezetőség aktuális véleményét és feltételezéseit tükrözik, ugyanakkor ismert és ismeretlen kockázatokat és bizonytalanságokat is tartalmazhatnak, amelyek miatt a tényleges eredmények, teljesítmény vagy események lényegesen eltérhetnek az ilyen állításokban kifejezettektől vagy sugalltaktól. A szövegösszefüggés alapján egyértelmű esetek mellett jövőre vonatkozó állításnak minősül minden olyan kijelentés, amely feltételes módot, vagy jövő idejű, illetve elvárásra, várakozásra, tervre, szándékra, feltételezésre, becslésre, előrejelzésre, lehetőségre vagy folytatásra utaló igét használ.

A tényleges eredmények, teljesítmények vagy események jelentős eltérését a hivatkozott kijelentésektől egyebek mellett az alábbiak okozhatják: (i) az általános gazdasági feltételek, különösen az Allianz Csoport alapvető üzleti tevékenységét vagy főbb piacait érintő gazdasági feltételek, (ii) a pénzpiacok – többek között a feltörekvő piacok – teljesítménye, többek között a piaci ingadozások, valamint a likviditási és hitelkockázati események), (iii) a biztosítási káresetek – beleértve a természeti katasztrófákat is – gyakorisága és súlyossága, és a kárköltségek alakulása, (iv) a halálozási és megbetegedési szintek és trendek, (v) a megtartási szintek, (vi) a hitelek nemteljesítésnek mértéke, (vii) a kamatszintek, (viii) a devizaárfolyamok, többek között az EUR/USD árfolyam, (ix) a verseny változó szintje (x) a jogszabályok és előírások változásai, beleértve a monetáris konvergenciát és az Európai Monetáris Uniót, (xi) a központi bankok és/vagy a külföldi kormányzatok politikáinak változásai, (xii) a felvásárlások, többek között a vállalati integráció hatása, (xiii) az átszervezési intézkedések, és (xiv) az általános versenytényezők, minden esetben lokális, regionális, országos és/vagy globális szinten. A terrorcselekmények és következményeik az itt felsorolt tényezők közül számos valószínűségét vagy intenzitását fokozzák.

Az ebben a jelentésben tárgyaltak az Allianz SE által az Egyesült Államok Értékpapír- és Tőzsdefelügyeletéhez időről időre benyújtott tájékoztatásban leírt kockázatok és bizonytalanságok függvényében is változhatnak. A vállalat nem vállal kötelezettséget a jövőre vonatkozó állítások naprakésszé tételével kapcsolatban.