AZ OROSZ-UKRÁN KIBERHÁBORÚ HATÁSAI A GLOBÁLIS IT-TÁRSADALOMRA

Háború az ötödik dimenzióban: kiberpartizánok akcióban

FORRÁS: 123RF.COM

Több mint ötven napja tart az orosz-ukrán fegyveres konfliktus, ami új megvilágításba helyezte azt, amit eddig a kiberhadviselésről gondolunk: többé nem a fizikai hadviselés, hanem az ötödik hadszíntér, ahol a soha nem látott események zajlanak. Eltévedt „kiberrepeszek”, mozgó kiberfront, hacktivizmus és legégetőbb kérdés: mit hoz az orosz-ukrán kiberkonfliktus a globális és a regionális IT-biztonságra és a jövőre nézve?

A kiberhadviselés több évtizedes múltra tekint vissza, hiszen már a 90-es évek végén, a 2000-es évek elején különböző lehallgatásoktól volt hangos az amerikai sajtó, míg az első súlyosabb kibercsörte az amerikai és kínai állam között 2003 környékére tehető. A világ szeme még 2007-ben szegeződött a kibertérre, ahol Oroszország lerohanta az akkor már az e-közigazgatással kacérkodó Észtországot, a célzott és túlterheléses támadásokkal pedig néhány napra leradírozta az észt kormányzatot és az észt bankrendszert a világhálóról. Ez akkor nem torkollott fegyveres konfliktusba, de a köztudatba emelte, hogy nemcsak a fizikális térben robbanhat ki háború. Kilenc évvel később a NATO deklarálta, hogy az információs hadviselés olyan valódi hadviselés, amelynek hadszíntere a kibertér. Hat évvel később 2022-ben pedig kirobbant egy olyan kiberháború, amelyhez foghatót talán még soha nem tapasztaltunk.

Kik vannak célkeresztben?

A kibertér február 24-e előtt sem volt eseménytelen, a háború kirobbanását megelőző és az azóta tartó időszak, azonban felülírta az elképzeléseket.

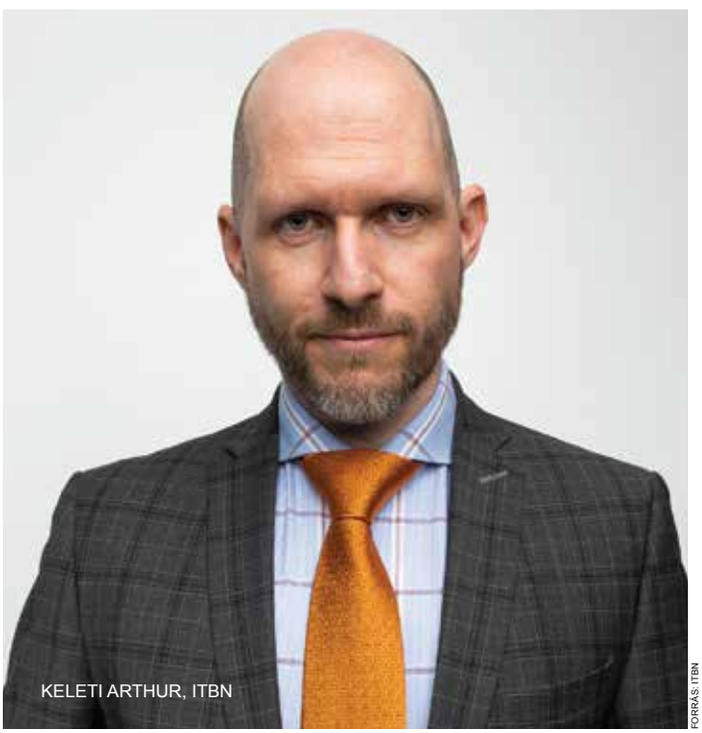
„Trendek szempontjából a kiberháború sebessége és a kiterjedése az, ami szembetűnő. Míg korábban az államokat, kritikus infrastruktúrát, nagyvállalatokat érő támadások kielemzésére és az abból kiolvasható következtetések levonására és integrálására két-három hét vagy adott esetben egy hónap is rendelkezésre állt, most egy-egy ilyen támadás esetén nem, mert már nemcsak havonta egy-kettő fordul elő, hanem napi szinten, óránként érkeznek beszámolók több száz gigabájtnyi adatot vagy több százezer emailt érintő kibertámadásokról”, mondta *Keleti Arthur*, kibertitok-jövőkutató, az Informatikai Biztonság Napja (ITBN) alapítója, az Önkéntes Kibervédelmi Összefogás elnöke.

A támadások célpontjai között szerepelt például az orosz atomenergia-központ, a Kreml honlapja, az orosz posta, egy fehérorosz fegyvergyár, egy orosz gázállomás, a fehérorosz vasúti irányítórendszer vagy az orosz állami tévé. A korábban „tabutémának” számított katonai vagy nukleáris rendszerek sem kivételek, és nem kímélték a titkosszolgálatokat sem. De ugyanez igaz visszafelé is, ukrán vonatkozásban. Ebből a korántsem teljes listából látszik, hogy a célpontok között a kritikus infrastruktúrák – a lakossági ellátásbiztonság stratégiai fontosságú intézményei, úgymint erőművek, kórházak, közműszolgáltatók stb. – előkelő helyet foglalnak el.

„Az is gyakori, hogy kormányzati dolgozók, hivatásos katonák, a különleges egységben szolgálatot teljesítők személyes adatai kerülnek nyilvánosságra. Korábban teljesen elképzelhetetlen volt, hogy ezek az érzékeny adatok nemcsak a hackerek, de a civil lakosság számára is könnyen elérhetővé váljanak. Nemcsak a sebessége gyorsult fel a támadásoknak, hanem a volumene is megnőtt. Csak az elmúlt időszakban több mint 2 terabájt anyag szivárgott ki az orosz-ukrán kormányzati rendszerekből, és a közeljövőben is számíthatunk nyilvánosságra kerülő személyes adatokra, amelyek további sérülékenységekhez vezethetnek. Sajnos, ilyen jellegű, akár teljes szervezetek belső levelezését, érzékeny információit érintő, egyfajta közel 100 százalékos adatszivárgás hatékony kezelésére a legtöbb magyar cég vagy szervezet nem áll készen”, tette hozzá Keleti Arthur.

Targetlista, eltévedt támadások, újrarajzolt védelmi vonalak

Az új keletű támadási formák, és a kevésbé újak is, mintegy „eltévedt golyóként”, a háborúhoz látszólag nem kapcsolódó vállalatokat és a magánfelhasználókat is eltalálhatják. Nem beszélve arról, hogy a szankciókat nem támogató vagy az álláspontjukat nem egyértelműen



KELETI ARTHUR, ITBN

FORRÁS: ITBN


MÁRTON MIKLÓS, VIVETECH

FORRÁS: VIVETECH

kinyilatkoztató országok is felkerülnek a hackerek targetlistájára – ahogy ez Magyarországgal vagy azokkal a vállalatokkal is megtörtént, amelyek nem vonultak ki Oroszországból.

„Előfordulnak »eltévedt« támadások, de ebben a láthatatlan háborúban legfőképpen célzott támadásokról beszélhetünk. Ami jelenleg Oroszország vagy Ukrajna ellen irányul, az főleg hacktivistákhoz, hackercsoportokhoz köthető. A célpontok leginkább kormányzati, hivatali szervek informatikai rendszerei, a hozzájuk kapcsolható belső információk, viszont vannak »civil« célpontok is. Ezek legtöbbször szintén valamilyen formában a háború egyik résztvevőjéhez köthetők; orosz vagy ukrán vállalkozások, esetleg valamelyik félhez politikailag közelebb álló nemzetek kormányzati, hivatali informatikai rendszerei. Orosz oldalról kibertámadás áldozata lett például a Sberbank, míg Ukrajna esetében az UkrTelecom, ezek mellett folyamatos, jellemzően túlterheléses támadások érik a résztvevőkhöz köthető vállalatokat. A civil lakosok nem célpontjai a támadóknak, ezt sok csoport nyilvánosan is lenyilatkozta a közösségi médián keresztül”, mondta *Márton Miklós,* a ViVeTech vezérigazgatója. Hozzátette, hogy „a háború előtt is voltak már támadások, ezek azonban nem feltétlenül jelentek meg koncentrált formában. Amikor egy nagyobb vállalatot súlyos támadás ér, az eseményből felkapott hír lesz, és több emberhez eljut az információ. Fontos azonban leszögezni, hogy nemcsak azok a kibertámadások történnek meg, amelyeket lehoz a sajtó, hanem olyanok is, amelyekről pillanatnyilag az érintett szervezet maga sem tud. Emiatt nagyon nehéz közelítő értéket is mondani arról, hogy valójában mennyi támadás történik a világ számos pontján, akár ebben a pillanatban is.”

Új hullámos hacktivizmus

Bármennyire is azt sulykolják a filmek, valójában nem ül fekete csuklyás, fehér maszkos emberek garmadája, ablaktalan, kék LED-visszfényben derengő gigászi számítógéptermekben, ölükben laptoppal. A valóság ennél sokkal hétköznapibb. „Ebben konfliktusban nemcsak szervezett és profi hackerek vesznek részt ideológiai meggyőződésük függvényében az orosz vagy ukrán oldalon, hanem amatőrök is, akik nem összeszedett hackercsoportokban, hanem egyedül, civilként támadnak, ami a hivatalos jogrend szerint a háborúba való beavatkozást jelenti”, fogalmazta meg Keleti Arthur.

A hackerek ilyen mértékű háborús beavatkozása komoly etikai dilemmákat vet fel a szakemberek körében. „Kritikus infrastruktúrák támadására biztat mindkét fél, amelyeket törvényes módon nem lehet megtámadni. Izgalmas, hogy a legtöbb ukrán szimpatizáns NATO-tagországokban található, így, ha szigorúan nézzük, ezek a szereplők beavatkoznak a háború menetébe. Eddig nagyjából nyolcvan olyan önkéntes hackercsoportot azonosítottak, akik szervezett formában támogatják az erőfeszítéseket, de ezekben a szerveződésekben nemcsak jó fiúk, hanem kiberbűnözők is vannak”, mondta Keleti Arthur.

Nem lehet szemet hunyni a magánzó hacktivisták felett sem. Az ő küldetésük – ukrán szimpatizánsként – bármennyire nemesnek tűnik, valójában veszélyes, hiszen azzal talán nem is számolnak, hogy egy sikeresen bevitt hackertámadásra válaszul megtorló valódi rakéta érkezhet. Kiemelendő még olyan új jelenségek felszínre emelkedése is, mint például a protestware, amelynek írója olyan változtatásokat hajt végre a szoftverben, amely ideológiai megfontolások szerint máshogy működ-

Öt kérdés a megosztott felelősségről

A kiberbiztonság üzleti kockázatot jelent, nemcsak egyszerű IT-probléma a céges igazgatótanácsok 88 százaléka szerint – derül ki a Gartner („Board of Directors Survey 2022”) adataiból. Ez az felismerés azonban nem érhető tetten a felelősségvállalás kultúrájában, a CIO és a CISO továbbra is a kiberbiztonság fő felelőse az esetek 85 százalékában. Az elemzés szerint a CIO-nak a vállalati vezetőkkel közösen kellene megosztani a kiberbiztonsági kockázatokat. Míg a szervezeten belül a CIO-ra és CISO-ra valóban a vállalati biztonság őreként tekintenek, a valóság az, hogy az üzleti vezető naponta hoz olyan döntéseket, amelyek befolyásolják a vállalat kiberbizonságát. Emiatt van szükség a közös felelősségvállalásra, amit a CIO-nak kell szorgalmaznia.

Az alábbi öt kérdés segít felmérni, hogy mennyire felkészült az üzlet az IT-csapattal közösen vállalni ezt a kiberbiztonsági felelősséget, érdemes minél hamarabb végiggondolni ezeket:

– Képes a szervezet kockázati döntéseket hozni a biztonsági szakemberek segítsége nélkül?
– Minden biztonsági kontroll üzleti értékét ki tudja mutatni az IT?
– Mit tükröznek a szervezet biztonsági kontrolljával kapcsolatos mérőszámok: a védelmi szintet (technológiai szempont) vagy a működési funkciókat (üzleti megközelítés)?
– A biztonsági döntések hány százalékát indokolja a szervezet félelmekkel, bizonytalanságokkal az üzleti célokkal összehasonlítva?
– Megvédhető-e a kiberbiztonsági rendszer az ügyfelek, érdekelt felek, szabályozók előtt?

FORRÁS: 123RF.COM

het vagy akár törölhet is, ha bizonyos gépeken, környezetben találja magát. Ugyanígy egyre gyakoribb kiberbiztonsági incidenshez vezető ok a hackerek által ideológiai alapon beszervezett belső munkatárs.
„Fontos figyelembe venni, hogy mivel politikai-társadalmi eredetű a háború, a hacktivisták sokkal intenzívebben járultak hozzá a kibertérben. Számos hackercsoport kiáll amellett, hogy a politikai-társadalmi ellentét szülte háború elszenvedői ártatlan civilek, akiknek védelme érdekében aktívan igyekeznek megállítani egyik-másik fél stratégiai infrastruktúráit az interneten keresztül. Míg a háború fizikai terében részt venni nagyon veszélyes, addig a kibertér személyi biztonság tekintetében kedvező paraméterekkel rendelkezik. Nem szükséges a helyszínre utazni, a világ bármely pontjáról vezethetők kibertámadások internetkapcsolat, internetezésre alkalmas eszköz és a szükséges biztonsági felkészültség és tudás birtokában”, mondta Márton Miklós.

Globális kilátó, és hazai körkép az orosz-ukrán kiberháború IT-biztonsági hatásairól

A háború kitörése után az EU kormányai egyhangúan elkötelezték magukat a védelmi kiadások jelentős növelése mellett. Ez nemcsak történelmi léptékű fordulat – főleg a német hadiipari fejlesztések bejelentése –, hanem azt is jelenti, hogy várhatóan jelentős erőforrásokat csoportosítanak át a kritikus infrastruktúraszolgáltatók kibervédelmére is.
„A háborúhoz köthető kibertámadások várhatóan felnyitják az emberek szemét, és nemcsak magánszemélyek esetén, de a vállalatok vezetésében is megnőhet az érdeklődés a megfelelő védekezés és az online tudatosság iránt. Amikor azt látja egy vállalatvezető a hírekben, hogy hackerek lekapcsolták a belorusz államvasutat, vagy átvették a Kreml belső kameráinak képét, akkor elgondolkodik: ha ezekbe a szuperbiztonságosnak gondolt rendszerekbe így be tudnak hatolni, akkor mit tudnak csinálni az én cégemnél? Szerintem az ukrajnai háború a nagy rádöbbenés élményét hozta el a vállalatok vezetői számára”, mondta Márton Miklós.

> A kiberbiztonság íratlan szabályai teljesen átrendeződtek, feloldódtak, a közeljövőben nem is várható, hogy normális mederbe terelődnek vissza, és ez közvetlenül érinti a magyar cégeket, szervezeteket is

A kibertámadások sokrétűek, ennek elég széles spektrumát mutatják meg a kiberháborúba bekapcsolódó csoportok. A sokrétűség és a médiavisszhang miatt viszonylag mély betekintést nyerhetünk a támadások módszereibe, a kihasznált sérülékenységek, hálózati védelmi hibák és hiányosságok körébe. A megszerzett információk alapján olyan következtetések és tanulságok vonhatók le, amelyekkel a hibák és hiányosságok egy része kiküszöbölhető, és a hasonló támadások megelőzhetők, ezzel direkt és indirekt módon is növelve a biztonsági rendszerek hatékonyságát.
„A Magyarország ellen irányuló, háborús mozgalomhoz köthető támadások száma nem túl magas, így a kiberháborúnak IT-biztonsági szempontból akár pozitív hatásai is lehetnek a fejlődésre. Ami fontos lehet Magyarország, és egész Európa számára, hogy a kritikus infrastruktúrák kiberbiztonságát meg kell erősíteni. Ez a háború megmutatta, milyen sebezhetőek és mekkora károkat tudnak okozni az erőművek, közszolgáltatások, vasutak, kórházak, vagy akár a kiskereskedelmi láncok elleni kibertámadások”, zárta gondolatait Márton Miklós.

Kiss Franciska