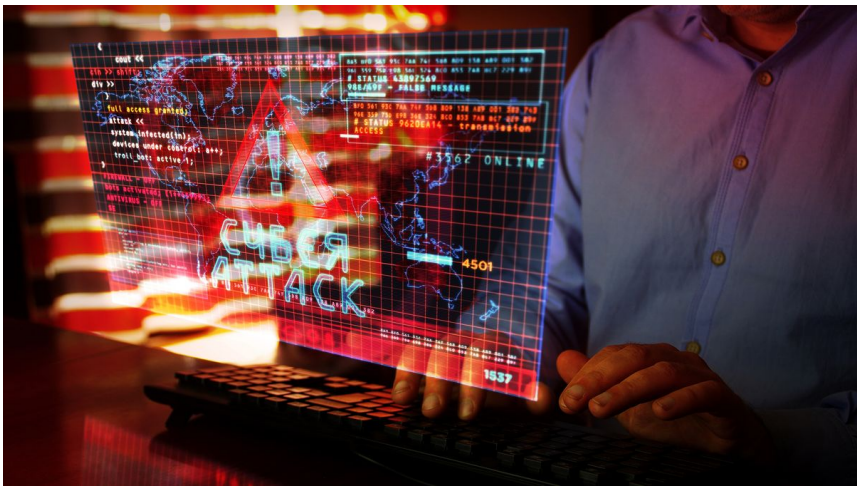
# Hány nap alatt lehet tönkretenni kibertámadásokkal egy országot?

Informatikus, IT-s szakmai körökben alapvetés: a kiberbűnözés napjainkra már olyan szintre jutott, hogy rövid idő alatt hatalmas károkat és káoszt lehet okozni egy relatíve átlagos országban a világ bármely pontján. Nyilván ezzel párhuzamosan a támadásokat elhárító rendszereket is veszett tempóban fejlesztik a szakértők. Ám sorsdöntő lehet, ki lép először, s ki az, aki már csak „válaszol” a játszmában?

2023.11.03 | Szerző: Horváth Éva

A kérdés, hogy mennyi idő alatt lehet egy országot kiberbűnözéssel tönkretenni, bonyolult és nagyon sok összetevőből áll, számos tényező befolyásolhatja. „Célszerűbb átfogalmazni a felvetést úgy: hány óra, nap alatt lehet egy ország ellátó és fenntartó rendszerében súlyos károkat okozni?” – válaszolt kérdésünkre egy célzott, szakmai kérdéssel a Sicontact Kft. IT vezetője.




A kiberbűnözők különböző technikákat alkalmazhatnak, akár ötvözve a fizikai, logikai támadásokat is.
Fotó: Shutterstock

Béres Péter több összetevőt is felsorolt, amelyektől függhet egy ilyen támadássorozat sikeressége:

- A támadások céljától és a célzott területektől. A kiberbűnözők különböző célokat tűzhetnek ki maguk elé: például az infrastruktúra megbénítását, a gazdasági rendszerek destabilizálását vagy akár a kormányzati rendszerek gyengítését, megsemmisítését.
- A támadások összetettségétől. A kiberbűnözők különböző technikákat alkalmazhatnak, akár ötvözve a fizikai, logikai támadásokat is, vagy egyszerűen csak a kibertérben felkészülten, akár több hónapon keresztül csak figyelni a támadni kívánt rendszerek működését, majd jól előkészítve egycsapásra támadni.
- Az ország kiberbiztonsági intézkedéseitől. Az ország kiberbiztonsági képességei és védekezési mechanizmusai szintén fontos szerepet játszanak. Ha egy ország erős kiberbiztonsági intézkedéseket alkalmaz, akkor nehezebb lehet „tönkretenni”. Itt lehet említeni Ukrajna példáját, ahol készülve a legrosszabbra, szinte a teljes állami infrastruktúrát elköltöztették az országból, és az évek során megerősítették az ellenálló képességüket.
- A támadók motivációjától és erőforrásaitól. A támadó felek ezek is meghatározó tényezők. Például egy jól finanszírozott és szakértő csoport képes lehet gyorsabban végrehajtani hatékony támadásokat, ami nem jelenti azt, hogy teljesen térdre kényszerítenek egy országot, de nagy károkat okozhatnak.

## Ez már nem fikció, hanem a valóság

Volt is már korábban rá precedens, hogy igyekeztek megbénítani egy másik ország kulcsfontosságú szolgáltatásait. Az elsők között említhető az a 2007-es Észtország elleni orosz támadás, amelyet egy eltávolított katonai emlékmű miatt hajtottak végre. „Az április 27-i incidensben célzottan támadták észt szervezetek weboldalait, mint például a parlamentét, a bankokét, minisztériumokét, újságokét és műsorszolgáltatókét.

Ha egy ország erős kiberbiztonsági intézkedéseket alkalmaz, akkor nehezebb lehet „tönkretenni”. Jó példa erre Ukrajna. Fotó: Shutterstock

„Mivel a pénzügyi szolgáltatások is teljesen ellehetetlenültek, az egész ország megszenvedte a célzott kibertámadást” – emlékeztetett érdeklődésünkre Csizmazia-Darab István, a Sicontact Kft. IT biztonsági szakértője.

Emiatt került fel aztán a korábbi négy klasszikus hadszíntér – föld, víz, levegő, világűr – mellé ötödiknek a kibertér, valamint a NATO is létrehozta a NATO Cooperative Cyber Defence Centre of Excellence nevű szervezetét, amely a kibervédelem létrehozását és megerősítését tűzte ki célul.

Alig telt el egy év, és ismét bekövetkezett egy emlékezetes „kiberháború”: 2008-ban az Orosz–Grúz konfliktusban a két ország kölcsönösen blokkolta a másik egyes weboldalait, illetve igyekezett dezinformációkkal félrevezetni az ellenfelet.

## Az örök harcban állók esete

A Sicontact Kft. IT-biztonsági szakértőjének tarsolyában azonban további esetek is vannak: 2010 júniusában történt, hogy az USA és Izrael egy közös fejlesztésű Stuxnet nevű vírussal sikeresen megtámadta az iráni busheri atomerőmű urániumdúsító Siemens centrifugáit, és a szabotázsakció keretében ezeket az eszközöket fizikailag is tönkre tudta tenni a kártevő kódjának segítségével. A zárt ipari rendszerbe úgy tudták bejuttatni a vírusokat, hogy USB-kulcsokat szórtak szét az erőmű közelében, és amikor valaki ezeket megtalálva bedugta őket a helyi számítógépekbe, akkor a Stuxnet leégette a Siemens centrifugákat. A cél annak a megakadályozása volt, hogy Irán atomfegyvert hozhasson létre.

Az eset érdekessége, hogy azóta már számtalan ilyen állami kártevő látott napvilágot (Flame, Duqu, Gauss, Careto), amelyeket egyes országok egy másik ország ellen fejlesztettek ki kémkedésre vagy rombolási szándékkal.

Ukrajna is többször szenvedett már el célzott orosz kibertámadásokat – említette Csizmazia-Darab István.

A Krím-félsziget 2014-es annektálása óta rendszeresekké váltak az ipari létesítmények, és a kritikus infrastruktúrák elleni támadások. Ezekben sok esetben áramszüneteket tudtak létrehozni, speciális kártevők célbejuttatásával adattörlést, szabotázsakciókat hajtottak végre ellenük.

Külön kiemelhető az ESET kutatói által felfedezett úgynevezett Industroyer kártevő, amely ipari vezérlő protokollokkal támadta az ukrán áramellátókat, kommunikációs és egyéb stratégiai létesítményeket. Az ilyen típusú támadások egészen napjainkig több-kevesebb rendszerességgel azóta is ismétlődnek.

## Kontinenseken átívelő akciók

Átugorhatunk a nagy víz túlsó partjára is: 2021-ben a DarkSide nevű zsarolóvírus banda mért csapást az USA Colonial Pipeline olajvezetékét üzemeltető cégre, emiatt leállás, hetekig tartó káosz és üzemanyaghiány lépett fel.

A központi katonai szervereket fokozottan őrzik, mivel egy-egy kibertámadás esetén hatalmas károkat szenvedhet a megtámadott fél. Fotó: Shutterstock

A támadás egy azóta már tömegesen alkalmazott kombinált módszert használt: nemcsak eltitkosította az adatokat, amiért váltságdíjat követeltek, hanem el is loptak bizalmas adatokat, így a követelés arról is szólt, hogy nem fizetés esetén a kényes adatokat feltöltik az internetre. Ezt hívjuk doxingnak. Sajnos az ilyen támadások szinte mindennaposak lettek különféle kórházak, oktatási intézmények, pénzügyi és állami szervezetek, ipari és gyártó cégek ellen.

Végül – a biztonsági szakértő szerint – érdemes megemlíteni azt az esetet is, amely gyaníthatóan politikai céllal kifejezetten, egy adott ország ellen irányult 2022 nyarán. Ez alkalommal a hírhedt Oroszországhoz köthető Conti és Hive bűnbanda indított zsarolóvírus támadást Costa Rica ellen. Számos állami intézményt, többek közt a pénzügyminisztérium hálózatát, adó- és vámhivatalokat, kereskedelmi központokat, közműveket, egészségügyi intézményt ért kiterjedt ransomware (zsarolóvírus) incidens. A megtámadott célpontok hosszú időre kényszerültek leállni.

A hivatalos tájékoztatás szerint 1500 kormányzati szerverből legalább 30 megfertőződött, a helyreállítás időpontjára az incidens idején még becslések sem voltak, és hetekig tartott a leállás.

„Mindezek után nem véletlen, hogy egyre több fórumon és egyre gyakrabban igyekeznek a szakértők felhívni a figyelmet a kiberbiztonság fokozásának fontosságára és a támadások elleni védekezés minél fejlettebb módszereire. Az országok kiberbiztonsági helyzetének javítása érdekében fontos, hogy a kormányok és a vállalatok egyaránt befektessenek a kiberbiztonságba, és folyamatosan fejlesszék a védelmi mechanizmusokat” – fogalmazott Béres Péter. Majd hozzátette: ahogyan legalább ilyen fontos tudatosító kampányokat szervezni a magasabb szintű biztonság megteremtése érdekében.

## Itthon sem ülünk ölbe tett kézzel

Kovács László és Krasznay Csaba 2010-ben mutatták be a magyarországi Hacktivity hacker konferencián a Digitális Mohács elnevezésű tanulmányukat, amely azt mutatta meg, hogy kellő tudás és rossz szándék birtokában mennyire sebezhetők a kritikus infrastruktúrák. Az előadás résztvevőit megdöbbentette, hogy jól irányzott támadásokkal, az áram, a víz, a műsorszórás, a banki szolgáltatások lerombolásával, blokkolásával mekkora káosz idézhető elő kevés erőfeszítéssel viszonylag gyorsan.