GAZDASÁG ÉS PÉNZÜGY • 12. ÉVF. 3. SZ. • 2025. SZEPT. • DOI: 10.33926/GP.2025.3.5

KIBERVÉDELMI FOGALMAK ÉS ÉRTELMEZÉSÜK

Kovács Levente – Terták Elemér[1]

ABSZTRAKT

Az eredményes kibervédelemhez naprakész minőségi ismeretekre van szükség. Ez át kell, hogy hassa a bűnüldözést, a jogszabályi keretrendszert, a szolgáltatói felületeket és védelmi rendszereket, valamint az oktatási és kommunikációs anyagokat. Ahhoz, hogy ez sikeresen megtörténhessen, összeállítottuk az ismereteink szerinti legteljesebb, 2025 nyarán aktuális kibervédelmi fogalmak meghatározását és magyarázatát. Tekintettel arra, hogy a kiberbűnözés egyre inkább határokat áthágó módon tevékenykedik, ezért a kiberbiztonság és a kibervédelem is csak akkor lesz igazán eredményes, ha képes a hatékony nemzetközi együttműködésre, melyhez a releváns fogalmak pontos meghatározása az egyik szükséges feltétel.

JEL kódok: K24, K42, M15

Kulcsszavak: kibervédelem, kiberbiztonság, kibertér fogalmai

A kiberbiztonság és kibervédelem az egyéni, társadalmi, közintézményi, közszolgáltatási és vállalati oldalról napjaink világszerte legégetőbb kihívásainak az egyike. Mivel a kibertér szinte nap mint nap változik, ezért a jogrendszer csak késedelmesen képes követni a végbemenő változásokat. Az egyéni ismeretanyag bővülése sem képes lépést tartani a fejlődés/változás dinamikájával. Emiatt a globális kibertérben való hatékony nemzeti és nemzetközi bűnüldözés komoly lemaradásban van, miközben a kibertéri bűnözés a technológiai fejlődést folyamatosan követve, szakadatlanul új módszereket bevetve próbál mások rovására gazdagodni.

Az egyéni felkészüléshez, a jogszabályok megalkotásához, a hatékony nemzeti és nemzetközi együttműködésekhez a kibervédelemben és kiberbűnözésben használt fogalmak és értelmezésük egységesítésére és pontosítására van szükség. Ezért publikus internetes oldalak alapján ezt a fogalomtárat úgy állítottuk össze, hogy tartalmazza minden releváns fogalom nemzetközileg használatos angol megfele-

1 *Kovács Levente* főtitkár, Magyar Bankszövetség; tanszékvezető egyetemi tanár, Miskolci Egyetem. E-mail: kovacs.levente@bankszovetseg.hu.
Terták Elemér elnökségi tag, Magyar Közgazdasági Társaság. E-mail: elemertertak@gmail.com

lőjét is, ezzel megkönnyítve a nemzetközi bűnmegelőzési és bűnüldözési kapcsolatokban az egyértelmű kommunikációt.

A LEGJELENTŐSEBB KIBERVÉDELMI ÉS KIBERBIZTONSÁGI FOGALMAK

1. **0. napi támadás:** A nulladik napi támadás egy olyan biztonsági kockázat egy szoftverben, amelyről nyilvánosan nem tudunk, és amelyről a szállító sem tud. A nulladik napi támadást azért nevezik így, mert azelőtt történik, hogy a célpont tudomást szerezne sebezhetősége létezéséről. A „nulladik napi" támadás az első vagy „nulladik" napon történik, amikor a fejlesztő már tud a hibáról, de még nem volt lehetősége arra, hogy a biztonsági javítást eljuttassa a szoftver felhasználóihoz. A támadó rosszindulatú programot bocsát ki, még mielőtt a fejlesztőnek vagy a szállítónak lehetősége lett volna javítócsomagot készíteni a sebezhetőség javítására. A nulladik napi támadás azzal kezdődik, hogy egy szoftverfejlesztő sebezhető kódot tesz közzé, amelyet egy rosszindulatú szereplő észrevesz és kihasznál. A támadás ezután vagy sikeres, ami valószínűleg azt eredményezi, hogy a támadó személyazonosság- vagy információlopást követ el, vagy a fejlesztő létrehoz egy javítást a terjedések korlátozására. Amint a javítást megírták és alkalmazzák, a kihasználást már nem nevezik „nulladik napi" kihasználásnak.

   https://www.fortinet.com/resources/cyberglossary/zero-day-attack
   https://hu.wikipedia.org/wiki/Nulladik_napi_t%C3%A1mad%C3%A1s

2. **Adathalászat:** lásd phishing

3. **APT (Advanced Persistent Threat):** Az APT csoportok olyan kiberbűnöző szervezetek, amelyek hosszú távú, célzott támadásokat hajtanak végre az áldozataik ellen, akik jellemzően nagyobb gazdasági szervezetek, elvétve államok. Az APT csoportok célja általában olyan adatok megszerzése, amelyek titkosítottak, érzékenyek, személyes jellegűek vagy szellemi tulajdon részét képzik. Továbbá, bármely olyan adat célponttá válhat, amely zsarolásra, vagy a célszemély megkárosítására használható és komoly anyagi vagy politikai haszonnal járhat. Az egyes szereplők motivációi eltérhetnek egymástól, és jelentős különbségek adódhatnak képességeik, kifinomultságuk, képzési szintjük és a tevékenységükhöz nyújtott támogatások tekintetében. Ezek közül a nemzetállami szereplők számítanak a legkifinomultabb kártékony aktoroknak, akik elkötelezettek, valamint korszerű erőforrásokkal és eszközökkel rendelkeznek. Többnyire a lehető legnagyobb gondossággal vég-

zik műveleteiket azért, hogy elkerüljék a lebukást. Ennek érdekében alapos felderítést végeznek, hogy információkat gyűjtsenek a célpont szervezeti és informatikai infrastruktúrájáról, a vállalati kultúráról, az alkalmazottakról, a biztonsági irányelvekről és eljárásokról. Képesek alkalmazkodni a célpontnál bevezetett biztonsági ellenőrzések változásaihoz. Különleges jellemzőik mellett az APT-k általában időt szánnak a nulladik napi sebezhetőségek felfedezésére és olyan exploitok vagy rosszindulatú programok kifejlesztésére, amelyeket a célpontok nem tudnak időben észlelni. Az ilyen fenyegetéseket elkövető szereplők motivációi jellemzően politikai vagy gazdasági jellegűek.

https://nki.gov.hu/wp-content/uploads/2023/07/APT-csoportok.pdf
https://en.wikipedia.org/wiki/Advanced_persistent_threat

4. **Adware:** Reklámot megjelenítő, speciális futtatható alkalmazás, elsődleges célja olyan reklámanyag kézbesítése, amely a felhasználó számára váratlanul, illetve kéretlenül érkezik. Sok adware alkalmazás hajt végre nyomkövető funkciókat, éppen ezért sorolják ezeket a fürkésző technológiák közé. Számos felhasználó el szeretné távolítani a gépéről ezeket a kéretlen reklámprogramokat, ha azok kémkednek a szokásaik után, nem kívánják látni az adware által megjelenített reklámokat, illetve zavarja őket a reklámprogramnak a rendszer teljesítményét korlátozó hatása. Másrészt vannak olyan felhasználók is, akik részben meg szeretnék tartani ezeket a reklámprogramokat, mert azok jelenléte költségcsökkentő egy adott program vagy szolgáltatás használata esetében, vagyis szándékos, illetve hasznos. Jó példa erre az olyan típusú reklám, amely egyenesen segíti vagy kiegészíti azt, amit a felhasználó alkalmaz, illetve amit éppen keres.

   https://www.eset.com/hu/termektamogatas/veszelyek/
   https://hu.wikipedia.org/wiki/Rekl%C3%A1mprogram

5. **Angler phishing (hamis szolgáltatói ügyintézés a közösségi médiában):** A „horgász adathalászat" az adathalász támadások egy sajátos típusa, amely a közösségi médiában terjedt el. A kiberbűnözők tisztában vannak azzal, hogy a különböző szolgáltatók egyre gyakrabban használják a közösségi médiát az ügyfeleikkel való kapcsolattartásra: nemcsak marketingre és promóciós célra, hanem akár panaszkezelés vagy problémamegoldás céljából is. Az elkövetők figyelik a szolgáltatók közösségi csatornáira érkező ügyfélpanaszokat, majd a szolgáltató képviselőjének kiadva magukat – annak közösségimédia-profilját lemásolva, vagy ahhoz nagyon hasonló, de hamis fiókról – felveszik a kapcsolatot a panasz bejelentőjével. Látszólag a panasz kezelése, a bejelentett probléma érdekében érzékeny információkat (személyes, banki, valamint különböző fiókbejelentkezési adatokat, jelszavakat) kérnek el az ügyféltől, ame-

lyekkel aztán hozzáférhetnek annak bankszámláihoz és különböző online fiókjaihoz.

https://kiberpajzs.hu/csalastipusok/szamitogepes/angler-phishing/
https://www.mnb.hu/fogyasztovedelem/digitalis-biztonsag/az-adathalasz-csalasok-legjellemzobb-tipusai/angler-phishing-hamis-szolgaltatoi-ugyintezes-a-kozossegi-mediaban

6. **Anti-Phishing:** Az anti-phishing olyan védekezési gyakorlat, amelynek célja az adathalász támadások megelőzése vagy mérséklése. Ezek során a támadók megbízhatónak tűnő forrásokat utánozva próbálnak érzékeny adatokat kicsalni. Az anti-phishing technikák kombinálják az emberi éberséget és a fejlett szoftveres megoldásokat, például e-mail szűrőket, linkelemzést és rosszindulatú tartalmak kiszűrésére szolgáló integrált anti-malware rendszereket. A cél egy többrétegű, megelőző és helyreállító biztonsági védelem kialakítása.

   https://perception-point.io/guides/phishing/how-to-prevent-phishing-attacks/

7. **Antivírus:** Az „antivírus" egy szoftver, amely véd a számítógépes vírusok és más károsító programok ellen. A vírusirtó programok célja, hogy azonosítsák, kiszűrjék és megszüntessék a veszélyes szoftvereket a számítógépről, így megvédve a felhasználó adatvédelmét és a rendszer stabilitását. Webshopok esetében a vírusirtók kiemelkedően fontosak, mivel védelmet nyújtanak mind a vásárlók, mind a kereskedők adatainak biztonsága érdekében, lehetővé téve ezzel a biztonságos online tranzakciókat. Az antivírus programok folyamatosan figyelik a rendszeres szoftver-, fájl- és weboldalaktivitásokat, hogy észleljék a potenciális fenyegetéseket. A legújabb vírusminták és támadási formák elleni védelem érdekében az antivírus szoftverek folyamatosan frissítéseket kapnak. Az észlelt kártevőket azonnal eltávolítják vagy karanténba helyezik a további károk elkerülése érdekében.

   https://webshopautomatizalas.hu/e-comm-lexikon/antivirus

8. **Attack Vector:** A kiberbiztonsági támadási vektor egy olyan útvonal, amelyet egy hacker vagy rosszindulatú szereplő használ, hogy jogosulatlan hozzáférést szerezzen egy hálózathoz, szerverhez, alkalmazáshoz, adatbázishoz vagy eszközhöz a rendszer sebezhetőségeinek kihasználásával. Ezeken keresztül különféle támadások indíthatók, például adatlopás, kártékony programok terjesztése vagy zsarolóvírusos támadások. A támadási vektorok gyakori formái közé tartoznak a rosszindulatú e-mail-mellékletek, fertőzött linkek, felugró ablakok és social engineering technikák. Az ilyen támadások mögött gyakran pénzügyi indíték, adatlopás vagy politikai cél húzódik meg.

   https://www.fortinet.com/resources/cyberglossary/attack-vector

9. **Cyber Attribution:** A kiberattribúció célja annak megállapítása, hogy ki követte el a kibertámadást, vagyis a támadó, illetve annak esetleges közvetítője személyazonosságának vagy tartózkodási helyének azonosítása. Az azonosítás eredményeként kiderülhet egy személy neve, felhasználói fiókja, álneve, vagy más olyan információ, amely egy adott személyhez köthető. A helymeghatározás vonatkozhat fizikai (földrajzi) helyre vagy virtuális helyre is, például IP-címre vagy Ethernet-címre (Wheeler–Gregory, 2007).

   https://en.wikipedia.org/wiki/Cyber_attribution

10. **Backdoor:** A backdoor (magyarul: hátsó ajtó) egy rejtett, jellemzően kártékony program vagy kódrészlet, amely lehetővé teszi, hogy a támadók megkerüljék a számítógép, hálózati eszköz (pl. router), vagy más beágyazott rendszer hitelesítési és titkosítási mechanizmusait. Célja, hogy engedély nélküli hozzáférést biztosítson a fertőzött eszközhöz, gyakran teljes irányítást adva a támadónak. A backdoorok általában a háttérben, észrevétlenül működnek, így nehéz őket felismerni. Működésük hasonlít más típusú kártevőkhöz, de az egyik legveszélyesebb fajtának számítanak, mivel lehetővé teszik a felhasználó megfigyelését, fájlok módosítását, új (gyakran szintén kártékony) programok telepítését, vagy akár további eszközök megtámadását. Ezek a programok gyakran további funkciókkal is rendelkeznek: képesek billentyűleütések rögzítésére, képernyőképek készítésére, adatállományok titkosítására, és egyéb, adatvédelmet veszélyeztető tevékenységek végrehajtására. A backdoorok súlyos biztonsági kockázatot jelentenek, különösen azért, mert működésükhöz nincs szükség folyamatos külső irányításra. Fontos megjegyezni, hogy ezek a kártevők jellemzően nem képesek önállóan bejutni a rendszerbe a felhasználó tudta nélkül – gyakran valamilyen más szoftverrel együtt, szándékosan vagy megtévesztéssel kerülnek telepítésre.

    https://avirus.hu/backdoors/
    https://en.wikipedia.org/wiki/Backdoor_(computing)

11. **Baiting:** A baiting, azaz csalizás egy speciális társadalmi manipuláció, amely arra csábítja az áldozatokat, hogy ingyenes termékeket, információkat, kedvezményeket vagy jutalmakat fogadjanak el bizalmas információk közléséért vagy biztonsági kockázatot jelentő lépésekért cserébe. Például egy hirdetés felkérheti a webhely látogatóit, hogy kattintsanak egy ingyenes film letöltésére vonatkozó ajánlatra, de az ajánlatra való válaszadáshoz az áldozatnak meg kell adnia az e-mail címét, ami előkészíti a terepet a további személyazonosság-lopási támadásokhoz. A csalitámadások jellemzően arra törekszenek, hogy az áldozatokat bizalmas információk megadására, rosszindulatú programok telepítésére vagy pénz fizetésére bírják rá. A bűnözők a csali segítségével mind a fogyasztókat, mind a vállalkozásokat megcélozhatják. A rosszindulatú szerep-

lők digitális ajánlatokat és fizikai tárgyakat is használhatnak a csalitámadások indításához. A csalizás bizonyos szempontból hasonlít az adathalászatra, de a két taktika kulcsfontosságú szempontból különbözik; mind a csalizás, mind az adathalászat a társadalmi manipulációra, az áldozatok megtévesztésére támaszkodik. A csalizás azonban látszólagos értéket kínál, hogy az áldozatokat rávegye a válaszadásra. Az adathalászat általában nem kínál semmi értékeset, de legitim forrásnak adja ki magát, és a bizalomra, a sürgősségre vagy a félelemre játszva bírja rá az áldozatokat válaszadásra. Míg az adathalászat a személyes adatokkal való visszaélésre épül, a csalizás csalási taktikákra alapul.

https://www.cobalt.io/blog/cybersecurity-baiting-definition-introuduction

12. **Bálnavadászat:** Bálnavadászat az, amikor a támadók „nagy halnak" számító szereplőre, például egy üzleti vezetőre vagy hírességre vetik ki a hálójukat. Ezek a csalók gyakran mélyreható kutatást végeznek a célpontjaikkal kapcsolatban, hogy megtalálják az alkalmas pillanatot a bejelentkezési hitelesítő adatok vagy más bizalmas adatok eltulajdonítására. Ha valakinek sok a vesztenivalója, akkor nála a bálnavadászok sokat nyerhetnek.

    https://www.microsoft.com/hu-hu/security/business/security-101/what-is-phishing

13. **Beaconing:** A kártevőprogramok világában a beaconing, azaz jeladás azt a gyakorlatot jelenti, amikor egy fertőzött számítógép rövid, rendszeres üzeneteket küld egy támadó által irányított szervernek annak jelzésére, hogy a fertőzött gépen futó kártevő aktív, működőképes, és készen áll az utasítások fogadására. Ezek a jeladások gyakran a vállalati hálózat belső, fertőzött gépeiről (például botokról vagy „zombikról") indulnak, és külső, úgynevezett parancs- és vezérlőszerverekre irányulnak. Ez a „hazatelefonálásként" is ismert kommunikációs stratégia lehetővé teszi a botnetek üzemeltetői számára, hogy automatikusan nyomon kövessék, irányítsák és vezéreljék a több száz, vagy akár több százezer fertőzött gépet (VanBuskirk, 2014).

    https://en.wikipedia.org/wiki/Web_beacon

14. **Beugratások:** lásd hoax

15. **Billentyűzetfigyelő:** lásd keylogger

16. **Binder**: A binder kifejezés gyakran használatos a kiberbiztonságban és a vírusvédelmi programozás területén, olyan szoftvereszközökre utalva, amelyek két különálló fájlt képesek egyetlen futtatható fájlba egyesíteni. Bár hasonló technológiát legitim célokra is használnak szoftverfejlesztésben és rendszer-

gazdai feladatokban, a binderek legfontosabb jellemzője a kiberbiztonsági kontextusban az, hogy jellemzően rosszindulatú szándékkal alkalmazzák őket. Gyakran hackerek használják, hogy egy látszólag ártalmatlan fájlban lévő káros kódrészletet álcázzanak vagy maszkoljanak, ezáltal megtévesztve az átlagfelhasználót, aki akaratlanul is káros rosszindulatú programokat vagy vírusokat futtat az eszközén. A kiberbiztonságban a binder egy legitim fájlt választ (ami lehet kép, dokumentum vagy futtatható program), és egy további rosszindulatú szoftvert vagy kódrészletet ágyaz be bele. Ezáltal egy olyan új fájl jön létre, amely a gyanútlan felhasználó számára úgy jelenik meg és úgy viselkedik, mint az eredeti fájl. Amikor ezt a fájlt megnyitjuk, akkor nemcsak a várt funkcióját látja el, hanem diszkréten futtatja a beágyazott káros kódot is. Ez a technika különösen népszerű a kiberbűnözők körében, mivel elfedi a valódi szándékot, így téve nehezebbé a felderítést. A binderek kulcsszerepet játszanak számos rosszindulatú program, többek között trójaiak, férgek és más vírusok terjesztésében. Veszélyük elsősorban mindennapos jellegükből fakad, hiszen egy jogos fájlt rejtett rosszindulatú programmal kombinálva a legtöbb víruskereső szoftver az eredeti fájl jogossága alapján figyelmen kívül hagyhat. A víruskereső szoftverek számára nehezebb az ilyen fenyegetések észlelése, mert a normál viselkedés, például egy fénykép vagy dokumentum megnyitása általában nem aktivál semmilyen biztonsági protokollt. A kiberbűnözők kifinomult technikákat alkalmaznak, hogy ezeket a kötött fájlokat rendkívül rejtetté tegyék, például fejlett titkosítást használnak a rosszindulatú rész olvashatatlanná tételére, vagy áldozati kódrészleteket, amelyek összezavarják a víruskereső programokat anélkül, hogy befolyásolnák a binder működését.

https://cyberpedia.reasonlabs.com/EN/binder.html

17. **Biometrikus alapú azonosítás:** A biometrikus azonosítás az emberi szervezet bizonyos jellemzőinek felismerésén alapszik. Ezek közül ismert az arc-, hang-, írisz-, retina-, véna-, DNS-, tenyér- és ujjlenyomat-azonosítás, de még az is az egyénre jellemző pontos megkülönböztető jel lehet, ahogyan járunk vagy aláírunk, mi több, a gépelési stílusunk is. A biometrikus azonosítás célja olyan rendszerek kialakítása, amelyek nem kódokkal, jelszavakkal vagy okmányokkal – melyek bárkinek a birtokába kerülhetnek – azonosítják az egyént, hanem annak saját személyes tulajdonságai alapján. Az azonosítási eljárások lehetnek aktívak vagy passzívak. Az aktív eljárások a személy tevékeny közreműködését igénylik, míg a passzív eljárások esetén a személy részvétele csak a mintaadásra korlátozódik (például ujjlenyomat-szkenner használata, vagy DNS-minta szolgáltatása).

https://www.ludovika.hu/blogok/cyberblog/2023/03/07/biometrikus-alapu-szemelyazonositas/

18. **Bizonytalanságon alapuló biztonság:** A „bizonytalanságon alapuló biztonság" (security through obscurity) szemlélet szerint ajánlott minden olyan technikai információt (pl.: szoftvertípusok és verziószámok, belső hálózati IP-k stb.) eltávolítani a potenciális támadók számára elérhető felületekről (pl.: HTTP-fejlécek, kiszolgálói szoftverek bannerei stb.), ami elősegítheti egy támadás sikerességét.

    https://makay.net/kiberbiztonsagi-fogalomtar
    https://en.wikipedia.org/wiki/Security_through_obscurity

19. **Black Hat Hacker:** A black hat, magyarul „feketekalapos" kifejezés olyan hackerekre utal, akik rosszindulatú célból hatolnak be számítógépes rendszerekbe és hálózatokba. Ezek az egyének vagy csoportok szándékosan megsértik a kiberbiztonsági szabályokat és törvényeket, hogy személyes vagy pénzügyi előnyre tegyenek szert, kárt okozzanak, adatokat lopjanak, rendszereket tegyenek működésképtelenné vagy zsarolóprogramokat helyezzenek el. A black hat hackerek általában kihasználják a biztonsági réseket, jelszavakat törnek fel, rosszindulatú szoftvereket használnak, vagy adathalász támadásokat indítanak. Tevékenységük gyakran bűncselekménynek minősül, és jelentős fenyegetést jelentenek a vállalatok, kormányzati szervek, valamint magánszemélyek adatbiztonságára nézve. Ők azok, akik a legtöbb kibertámadás mögött állnak, és szemben állnak a white hat (fehérkalapos) hackerekkel, akik épp a biztonsági gyengeségek azonosításával segítik a védekezést. A black hat kifejezés az 1950-es és 1960-as évek westernfilmjeiből származik, ahol a gonosz szereplők rendszerint fekete kalapot viseltek – innen ered a modern kiberbiztonsági szóhasználatban is a negatív jelentéstartalom.

    https://www.fortinet.com/resources/cyberglossary/black-hat-security
    https://en.wikipedia.org/wiki/Black_hat_(computer_security)

20. **Bloatware:** A bloatware-ek olyan, jellemzően kéretlen alkalmazások, amiket a gyártók telepítenek elő az általuk gyártott/forgalmazott készülékekre (számítógépekre, tabletekre és okostelefonokra). Eredendően nem tekinthetőek kártékony kódoknak, ugyanis csupán kényelmi szolgáltatásokat nyújtanak, viszont nem egy esetben derült ki, hogy egyes előtelepített alkalmazások valamilyen kártevőt rejtettek, vagy lehallgatták a felhasználók tevékenységét – a gyártók tudtával, vagy tudta nélkül.

    https://makay.net/kiberbiztonsagi-fogalomtar

21. **Blocklist/Blacklist:** A tiltólista, más néven feketelista, egy hozzáférés-szabályozó rendszer, amely megakadályozza, hogy a rajta szereplő felhasználók, programok vagy hálózatok hozzáférjenek bizonyos rendszerekhez vagy szol-

gáltatásokhoz. A tiltólista célja a nem kívánt vagy káros forgalom – például spam, illetéktelen hozzáférés vagy rosszindulatú tevékenységek – kiszűrése. A felhasználók vagy entitások automatikusan vagy manuálisan kerülhetnek fel a listára, és a rendszer ennek alapján blokkolja őket.

https://www.infobip.com/glossary/blocklist

22. **BOT:** A robot szó rövidített alakja, a bot egy feladatokat automatikusan végrehajtó program. Kezdetben a botokat a UNIX világban alkalmazták a rendszergazdák a rendszeresen elvégzendő, sablonos feladatoknál. Némely bot automatikusan cseveg is a felhasználóval, vagy válaszol a feltett kérdésekre, mintegy utánozva egy valódi, hús-vér embert. A bot rossz célokra is felhasználható: segítségével egy távoli támadó átveheti az irányítást az áldozat megfertőzött számítógépén. A cél pontosan ez: egyetlen gépről fertőzött számítógépek százezrei válnak távirányíthatóvá. A károkozók (botherder, azaz botnet pásztor) az eltérített számítógépek erőforrásait kéretlen levélszemét (spam) küldésére, illegális szoftverek letöltésére és tárolására használják. Nem ritkán pornográf anyagok tárolására, illetve különféle számítógépes támadásokban (DoS, DDos) való részvételre is használják, sőt meghatározott tarifa fejében akár bérbe is adják ezt a kapacitást. A bot ezenfelül képes végigpásztázni az áldozat merevlemezét, és arról bizalmas adatokat továbbít egy távoli weboldalra, és ezekkel a lopott személyes, banki, lakcím-, társadalombiztosítási stb. információk segítségével további bűncselekményeket követnek el (identity theft, azaz személyiség lopás). Az ilyen fertőzött gépeket gyakran zombi gépeknek is nevezik.

https://www.eset.com/hu/termektamogatas/veszelyek/

23. **Botnet:** A botnet, vagy más néven zombihálózat tagjai olyan felhasználói készülékek, amelyek egy vírusfertőzés következtében távolról irányítható kártevőt futtatnak. A zombihálózat „parancsnokai" képesek tömegesen (esetenként több százezres nagyságrendben) irányítani az áldozatok készülékeit, hogy azok túlterheléses támadást indítsanak egy-egy megadott célpont ellen. Így a támadók nem kerülnek közvetlen kapcsolatba a fő célponttal, helyettük az áldozatok fertőzött eszközei végzik el a munkát.

https://makay.net/kiberbiztonsagi-fogalomtar

24. **Bug bounty:** A bug bounty, magyarul hibajavító program egy olyan program, amelyben szervezetek jutalmat – általában pénzt – ajánlanak fel azoknak az etikus hackereknek vagy biztonsági kutatóknak, akik biztonsági hibákat, sebezhetőségeket tárnak fel a vállalat rendszereiben, szoftvereiben vagy

szolgáltatásaiban. A cél a hibák felelősségteljes bejelentése és kijavítása még azelőtt, hogy azok rosszindulatú kezekbe kerülnének.

https://www.techtarget.com/whatis/definition/bug-bounty-program

25. **Business Email Compromise:** Az üzleti e-mail-feltörés (BEC) során a támadók hozzáférnek egyes cégek levelezéséhez, megfigyelik az esetleges pénzügyi tranzakciókérelmeket (számla, díjbekérő, előlegbekérő stb.) és a szervezet nevében hamis, átírt bankszámlaszámmal ellátott dokumentumokat küldenek az érintett partnereknek, akik így a támadók által kezelt bankszámlákra utalják az összegeket.

https://makay.net/kiberbiztonsagi-fogalomtar

26. **Büntető rutin:** lásd Payload

27. **Célzott adathalászat:** A célzott adathalászat módszerét használják, amikor a támadó kifejezetten egy személyt, vagy a cégét akarja támadni, bizalmas információkhoz igyekszik hozzáférni, mint pl. a cég üzleti titkai, az érzékeny technológiai tervek, vagy bizalmas kormányzati kommunikáció. Az is előfordulhat, hogy a bizonyos személy csak első lépésként szolgál ahhoz, hogy egy másik egyént/céget érjenek el. A támadók igen sokat nyerhetnek, ezért hajlandóak időt és pénzt nem sajnálva feltérképezni a célpontjaikat. Például egy külföldi kormányzat úgy gondolja, hogy a kiválasztott cég olyan terméket vagy technológiát fejleszt, ami kulcsfontosságú a gazdaságukhoz és támadni kezdi a céget. Megvizsgálják a cég weboldalát, és beazonosítanak pár kulcsszereplőt, akikről komplett dossziét készítenek. A kiválasztott egyének elemzését követően, a támadók egy célzott adathalász levelet készítenek, pl. a cég egy beszállítója nevében. A levél egy csatolmányt tartalmaz, amely számlának tűnhet, miközben az a valóságban egy káros kódot tartalmazó fájl. Az emberek kb. 50-60%-át sikerül megtéveszteni, megnyitják a csatolmányt, és ezáltal hozzáférést adnak a támadónak a számítógépükhöz. A célzott adathalászat sokkal veszélyesebb fenyegetés az egyszerű adathalász támadásoknál, mivel a támadók személyre szabott támadást intéznek néhány kiválasztott ember ellen. Ez nem egyszerűen a támadók sikerének esélyét növeli, de ezen támadások felfedezése is sokkal nehezebb.

https://www.biztonsagosinternet.hu/tippek/szemelyes-biztonsag-az-interneten/celzott-adathalaszat

28. **CIRT (A Computer Incident Response Team):** A CIRT, azaz Számítógépes Incidens Válaszadó Csapat egy speciális, jól képzett információbiztonsági szakemberekből álló csapat, amelynek fő feladata a szervezetek kiberbiz-

tonsági eseményeinek és incidenseinek gyors és hatékony kezelése. A CIRT elsődleges szerepe az informatikai rendszerek és hálózatok védelme az esetleges kibertámadásokkal szemben, valamint a támadások következményeinek minimalizálása. A CIRT tevékenységi körébe tartozik az incidensek észlelése, elemzése, a támadások forrásának azonosítása, a helyreállítási folyamatok végrehajtása, valamint a támadások megismétlődésének megakadályozása érdekében kidolgozott védekezési stratégiák és javaslatok készítése. Emellett a CIRT együttműködik más biztonsági egységekkel, például a CERT-ekkel (Computer Emergency Response Team), és aktívan részt vesz az információbiztonsági tudatosság növelésében is. A csoport munkája kulcsfontosságú ahhoz, hogy a szervezetek gyorsan reagáljanak a kibertámadásokra, minimalizálják a károkat, megőrizzék az adatbiztonságot és fenntartsák az üzletmenet folytonosságát.

https://www.group-ib.com/resources/knowledge-hub/cirt/

29. **Cookie**: A cookie, magyarul „süti", egy kis adatcsomag, amelyet a böngésző tárol el egy weboldal kérésére, és minden későbbi oldalletöltés során visszaküld ugyanannak a weboldalnak. A süti tetszőleges információt tartalmazhat, amit a weboldal határoz meg. Fontos, hogy egy weboldal kizárólag a saját sütijeit tudja beállítani, és más oldalak sütijeihez nem férhet hozzá. A weboldalak gyakran használnak sütiket például a felhasználók bejelentkeztetéséhez. Ilyenkor a sikeres azonosítás után a weboldal egy egyedi azonosítót küld a böngészőnek, amelyet az elment. A böngésző ezt az azonosítót minden újabb kéréskor visszaküldi, így a rendszer tudja, melyik felhasználó melyik tartalmat láthatja. Enélkül például egy felhasználó nem tudná elérni saját e-mailjeit. Az európai szabályozások értelmében a weboldalaknak kötelező tájékoztatniuk a felhasználókat a sütik használatáról. Bizonyos típusú sütik – például marketing vagy statisztikai célúak – használatához pedig a felhasználó előzetes, kifejezett hozzájárulása szükséges.

https://lexiq.hu/cookie
https://en.wikipedia.org/wiki/HTTP_cookie

30. **Cross-site scripting:** Ez egy olyan támadás, amelyben egy támadó egy rosszindulatú szkriptet ad hozzá egy legitim weboldal tartalmához. A cross-site scripting (XSS) támadások lehetővé teszik a támadó számára, hogy különféle nyelveken írt szkripteket futtassanak (például JavaScript) gyanútlan weboldal-felhasználóinak böngészőiben. A támadók XSS-t használhatnak munkamenet sütilopásra, amely lehetővé teszi számukra, hogy áldozatul esett felhasználóknak tűnjenek. De eloszthatnak rosszindulatú szoftvert, megcímkézhetik a weboldalakat, felhasználói hitelesítő adatokat keresnek,

és más káros tevékenységeket is végeznek az XSS segítségével. Sok esetben social engineering technikákkal, például a phishinggel kombinálják. Az XSS a közös támadási vektorok között állandóan jelen van, és 2023-ban a CWE legveszélyesebb 25 listáján a második helyen állt.

https://www.zts.hu/blog/hanyfelekeppen-tamadhatjak-meg-a-cegunk-szervereit-2-resz/
https://en.wikipedia.org/wiki/Cross-site_scripting

31. **Cryptojacking:** A cryptojacking egy olyan támadási metódus, amely során a támadók az áldozat készülékére valamilyen formában kriptovaluta-bányászó kódot juttatnak – tehát az áldozat készüléke a támadók számára termeli a digitális pénzt, általában Bitcoin, Ethereum vagy Monero pénznemben.

    https://makay.net/kiberbiztonsagi-fogalomtar
    https://en.wikipedia.org/wiki/Cryptojacking

32. **Cryptotrojan:** A cryptotrojan (kriptotrójai) egy olyan digitális kártevő, amit felhasználói szoftverekbe rejtenek, hogy azok használata közben a kártevő a háttérben digitális pénzt (kriptovalutákat) bányásszon a felhasználók eszközeinek erőforrásaival, a felhasználók tudta nélkül, a kártevő készítői számára.

    https://makay.net/kiberbiztonsagi-fogalomtar

33. **Cyber Threat Intelligence:** A kifejezésnek jelenleg nincs közismert magyar megfelelője, de leginkább olyan hírszerzési műveleteknek feleltethető meg, amelyek során a legkülönfélébb forrásokból (Open Source Intelligence, Social Media Intelligence, Deep Web, stb.) összegyűjtött, hatalmas mennyiségű információban egy erre a feladatra szakosodott csapat azonosítja azokat a potenciális kiberfenyegetéseket, amik veszélyeztethetik az adatok és a rendszerek biztonságát.

    https://makay.net/kiberbiztonsagi-fogalomtar

34. **Cyber warfare:** A cyber warfare-t, azaz kiberháború kifejezést gyakran használják mindenféle online fenyegetés leírására, függetlenül attól, hogy ki a támadó vagy a célpont. Azonban a biztonsági szakemberek körében van egy szűkebb értelmezése is: egy ország által végrehajtott támadás egy másik ország infrastruktúrája ellen. A kiberháború jogi definíciója szerint olyan cselekmények tartoznak ide, amelyek hadüzenettel, háborús cselekményekkel, halálesetekkel vagy pusztítással járnak. Az ilyen események meghatározása és minősítése azonban gyakran vitatott és összetett kérdés.

https://nki.gov.hu/figyelmeztetesek/archivum/tisztazni-kell-a-kiberfegyveres-kiberhaboru-fogalmat/?utm_source https://nki.gov.hu/figyelmeztetesek/archivum/kiberhaboru/?utm_source
https://en.wikipedia.org/wiki/Cyberwarfare

35. **Cyber weapon:** A cyber weapon, azaz kiberfegyver olyan digitális eszköz, rosszindulatú program vagy kód, amelyet kifejezetten érzékeny információk ellopására, rendszerek megbénítására vagy jelentős károkozásra terveztek. Célja lehet a kritikus infrastruktúrák – például energiahálózatok, kommunikációs rendszerek vagy egészségügyi szolgáltatások – megzavarása, illetve katonai vagy politikai célok elérése. Használatuk lehet támadó, védekező vagy kettős rendeltetésű, és működésük során alkalmazhatnak adatmegsemmisítést, kémkedést vagy fizikai szabotázst. A kiberfegyverek gyakran állami szereplők kezében jelennek meg, mivel lehetőséget nyújtanak a valószínűsíthető tagadhatóságra, azaz az érintett ország megtagadhatja a közvetlen felelősséget a támadásért.

    https://www.ebsco.com/research-starters/science/cyberweapon
    https://en.wikipedia.org/wiki/Cyberweapon

36. **Cyber**: A cyber angol nyelvű szó, amelynek a magyar jelentése számítógépes, számítógépekkel kapcsolatos, virtuális. Más szavakkal összekapcsolva szokták használni. Magyar nyelven kiber formában terjedt el. A kifejezés a scifikből került át a hétköznapi szóhasználatba. Akkor használják egy szóhoz kapcsolva, ha azt szeretnék jelezni, hogy az adott dolog számítógépes változatáról beszélnek. Az angol cyberbullying szó például internetes zaklatást, a kiberbűnözés pedig számítógépes bűnözést jelent.

    https://lexiq.hu/cyber
    https://en.wikipedia.org/wiki/Cyber

37. **Cyberbullying:** A cyberbullying, azaz internetes zaklatás, digitális technológiák használatával történő zaklatás. Történhet közösségi médiában, üzenetküldő platformokon, játékplatformokon és mobiltelefonokon. Ismétlődő viselkedés, amelynek célja a célpontok megijesztése, feldühítése vagy megszégyenítése. Példák többek között: hazugságok terjesztése, vagy kínos fotók vagy videók közzététele valakiről a közösségi médiában; bántó, bántalmazó vagy fenyegető üzenetek, képek vagy videók küldése üzenetküldő platformokon keresztül; valakinek a nevében vagy hamis fiókokon keresztül visszaélve, gonosz üzeneteket küldve másoknak; szexuális zaklatás vagy zaklatás elkövetése generatív mesterséges intelligencia eszközök használatával. A személyes és az internetes zaklatás gyakran párhuzamosan történhet. Az

internetes zaklatás azonban digitális lábnyomot hagy – egy olyan feljegyzést, amely hasznosnak bizonyulhat, és bizonyítékként szolgálhat a bántalmazás megállításához.

https://www.unicef.org/stories/how-to-stop-cyberbullying
https://hu.wikipedia.org/wiki/Cyberbullying

38. **Cybercrime:** A kiberbűnözés olyan bűncselekmény, amely számítógépet, számítógépes hálózatot vagy hálózati eszközt céloz meg, illetve használ fel. A legtöbb kiberbűncselekményt pénzszerzésre törekvő kiberbűnözők vagy hackerek követik el. Előfordul azonban, hogy a kiberbűnözés célja a számítógépek vagy hálózatok megkárosítása nem anyagi indíttatásból, hanem politikai vagy személyes okokból. A kiberbűnözést magánszemélyek vagy szervezetek követhetik el. Egyes elkövetők szervezettek, fejlett technikákat alkalmaznak, és magasan képzett technikai szakemberek. A számítógépeket célzó kiberbűnözők kártevőkkel fertőzhetik meg az eszközöket, hogy adatokat töröljenek vagy lopjanak. Előfordulhat, hogy a támadók megakadályozzák a felhasználókat egy webhely vagy hálózat elérésében, vagy gátolják egy vállalkozás szoftverszolgáltatásának működését – ezt szolgáltatásmegtagadási (DoS) támadásnak nevezik. A számítógépek más bűncselekményekhez való felhasználása során kiberbűnözők rosszindulatú programokat, illegális információkat vagy tiltott tartalmakat terjeszthetnek. Gyakori, hogy a támadók többféle módszert is kombinálnak: például először vírussal fertőzik meg a számítógépeket, majd ezeket a gépeket felhasználják további rosszindulatú szoftverek terjesztésére más eszközökre vagy hálózatokon keresztül. Egyes joghatóságok a kiberbűnözés egy harmadik típusát is elismerik, amikor a számítógépet bűnsegédként használják fel – például lopott adatok tárolására.

https://www.kaspersky.com/resource-center/threats/what-is-cybercrime

39. **Cybersecurity:** A cybersecurity, azaz kiberbiztonság olyan folyamatok, ajánlott eljárások és technológiai megoldások összessége, amelyek segítenek a felhasználónak megvédeni a kritikus rendszereit, adatait és hálózatát a digitális támadásoktól. Mivel szinte mindenütt használunk adatokat, és egyre többen dolgoznak és csatlakoznak bárhonnan, az elkövetők széles körű szakértelemre és készségekre tettek szert. A kibertámadások száma évről évre nő, ahogy a támadók folyamatosan fejlesztik taktikájukat, technikáikat és eljárásaikat és skálázzák működésüket. Ez a folyamatosan változó fenyegetési környezet megköveteli, hogy a szervezetek dinamikus, folyamatos kiberbiztonsági programot hozzanak létre, hogy ellenállóak maradjanak, és alkalmazkodjanak a felmerülő kockázatokhoz. Egy hatékony kiberbiztonsági program olyan személyeket, folyamatokat és technológiai megoldásokat ötvöz, ame-

lyek mérséklik a támadásból eredő üzletmenet-kiesések, adatlopások, pénzügyi veszteségek és hírnévcsorbulás kockázatát. A kiberbiztonság elengedhetetlen a jogosulatlan hozzáférés, az adatszivárgás és más kiberveszélyforrások elleni védelemhez.

https://www.microsoft.com/hu-hu/security/business/security-101/what-is-cybersecurity

40. **Cyberspace:** A kibertér az ember által mesterségesen létrehozott, dinamikusan változó tartomány, amelyben az információ gyűjtését, tárolását, feldolgozását, továbbítását és felhasználását végző, egymással hálózatba kapcsolt és az elektromágneses spektrumot is felhasználó infokommunikációs eszközök és rendszerek működnek, lehetővé téve ezzel az emberek és a különféle eszközök közötti folyamatos és globális kapcsolatot.

https://makay.net/kiberbiztonsagi-fogalomtar

41. **Csalizás:** lásd baiting

42. **Dark web:** A dark web (vagy magyarul sötét web) a deep webnek (azaz a hagyományos keresők által nem látott oldalaknak) az a része, ami csak valamilyen speciális szoftver, beállítás vagy elérési jog segítségével tekinthető meg. Egyes dark webes szolgáltatások lehetőséget biztosítanak az állami cenzúra megkerülésére, anonim böngészésre vagy például újságírókkal való biztonságos kommunikációra. Ezen kívül a dark webet gyakran használják illegális tevékenységekre is, például fegyverek, drogok, hamisított termékek adásvételére.

https://lexiq.hu/dark-web

43. **DDoS-támadás:** A DDoS-támadás (Distributed Denial-of-Service, azaz elosztott szolgáltatásmegtagadásos támadás) egy informatikai szolgáltatás szándékos túlterhelését jelenti, melynek célja a szolgáltatás részleges vagy teljes megbénítása, illetve rendeltetésszerű működésének megzavarása. A támadás során több – gyakran több ezer – fertőzött eszköz (ún. zombihálózat tagjai) egyszerre küld túl sok kérést a célrendszer felé, amit az nem tud kezelni, és így elérhetetlenné válik a felhasználók számára. A támadók ezeket az eszközöket központilag irányítják, és a tömeges forgalommal kényszerítik szolgáltatásmegtagadásra a célpontot.

https://makay.net/kiberbiztonsagi-fogalomtar

44. **Deepfake:** A deepfake olyan képek, videók vagy hanganyagok gyűjtőfogalma, amelyeket mesterségesintelligencia-alapú eszközökkel vagy szerkesztőszoft-

verek segítségével módosítottak vagy hoztak létre. Ábrázolhatnak valós vagy kitalált személyeket, és a szintetikus média egyik formájának tekintik őket, azaz olyan médiának, amelyet általában mesterségesintelligencia-rendszerek hoznak létre különböző médiaelemek kombinálásával, egy új médiatermékké. Bár a hamis tartalmak létrehozása nem új keletű dolog, a deepfake-ek egyedülálló módon kihasználják a gépi tanulás és a mesterséges intelligencia technikáit, beleértve az arcfelismerő algoritmusokat és a mesterséges neurális hálózatokat, mint például a variációs autoenkódereket és a generatív adverzális hálózatokat. A képelemzés területe viszont olyan technikákat fejleszt, amelyekkel manipulált képeket lehet észlelni. A deepfake-ek széles körű figyelmet kaptak a gyermekek szexuális zaklatásával kapcsolatos anyagok, hírességpornográf videók, bosszúpornó, álhírek, átverések, zaklatás és pénzügyi csalások létrehozásában való potenciális felhasználásuk miatt.

https://en.wikipedia.org/wiki/Deepfake

45. **Deep web:** A deep web (vagy magyarul mély/láthatatlan web) a webnek az a része, amit nem látnak a hagyományos keresők, mint például a Google. A deep web részei például a webes e-mail vagy banki oldalak jelszóval védett részei, a fizetett tartalmak, a csak regisztráció után megtekinthető oldalak, zárt orvosi adatbázisok, vagy olyan oldalak, amelyek csak valamilyen speciális szoftver (pl. Tor böngésző) letöltése után érhetőek el, a keresők által nem ismert formátumban vannak vagy sehova nincsenek linkelve, ezért nem találnak rájuk a keresők. A kifejezést gyakran tévesen a dark web szinonimájaként használják, az utóbbi azonban valójában csak egy kisebb része a deep webnek.

https://lexiq.hu/deep-web

46. **Demilitarizált zóna (DMZ): A** demilitarizált zóna, más néven demarkációs zóna vagy határhálózat egy olyan fizikai vagy logikai alhálózat, ami egy szervezet belső szolgáltatásait tartalmazza és tárja fel egy nagyobb, nem megbízható hálózatnak, általában az internetnek. A DMZ célja, hogy egy plusz biztonsági réteget biztosítson a szervezet helyi hálózatának (LAN). Így egy külső támadónak csak a DMZ-ben található berendezésekhez lehet hozzáférése, nem az egész hálózathoz.

https://hu.wikipedia.org/wiki/Demilitariz%C3%A1lt_z%C3%B3na_(informatika)

47. **Digitális lábnyom:** Digitális lábnyom minden olyan információ, amit valaki az online jelenlétével hagy maga után az Interneten vagy tágabban értelmezve minden olyan adat, amit valamilyen digitális technológia rögzített, és

összefüggésbe hozható a személyével. Például szándékos digitális lábnyom egy közösségi oldalon közzétett fotó vagy hozzászólás, egy regisztráció valamilyen weboldalon, vagy egy poszt lájkolása. Léteznek akaratlan lábnyomok is, amiket egyes cégek vagy államok gyűjtenek rólunk, például az általunk meglátogatott oldalakról, vagy hogy mennyit görgettünk le egy oldalon és hova kattintottunk. Tágabb értelemben digitális lábnyomnak számítanak például mobiltelefon használata során keletkezett hívásadatok, SMS-ek vagy a térfigyelő kamerák felvételei is. Az így keletkezett adatokat jellemzően arra használják, hogy segítségükkel a felhasználókat érdeklő hirdetéseket tudjanak megjeleníteni számukra; a digitális lábnyomoknak azonban vannak veszélyei is, például felhasználhatják adathalász vagy social engineering támadások során, esetleg manipulatív célokra. Problémát okozhat az is, ha például egy új munkahelyen a korábbi internetes tevékenysége alapján döntenek a jelentkező felvételéről vagy elutasításáról. A széles körű adatgyűjtés miatt a digitális lábnyomok eltüntetése a legtöbb esetben nem megoldható, azonban a csökkentésükre van lehetőség, például törölhetők a korábbi regisztrációk, a GDPR alapján az egyes cégektől kérhető a tárolt adatok törlése, és ellenőrizhető a használt szolgáltatásoknál a beállításokban bizonyos adatok gyűjtésének letiltása is.

https://lexiq.hu/digitalis-labnyom

48. **DKOM (Direct Kernel Object Manipulation):** A DKOM olyan technika, amely közvetlenül módosítja az operációs rendszer kernelében található adatstruktúrákat és objektumokat. Legfőbb célja rendszerint a rosszindulatú tevékenységek elrejtése és a biztonsági intézkedések kijátszása. A kiberbiztonság területén a DKOM-ot gyakran használják arra, hogy folyamatokat, fájlokat vagy rendszerkulcsokat rejtsenek el a hagyományos biztonsági eszközök elől, ezáltal lehetővé téve a kártékony vagy jogosulatlan műveletek észrevétlen végrehajtását. Az ilyen támadások felismerése rendkívül nehéz, mivel a változtatások mélyen, a kernel szintjén történnek, és láthatatlanok maradhatnak a standard védelmi megoldások számára. Éppen ezért az észlelésükhöz speciális elemző eszközök és fejlett technikák alkalmazása szükséges.

https://dotcommagazine.com/2023/09/dkom-a-fascinating-comprehensive-guide/

49. **DNS spoofing:** A DNS, Domain Name Server lehetővé teszi a felhasználók számára, hogy weboldalakhoz férjenek hozzá oly módon, hogy a domain neveket és URL-eket IP-címekhez rendeli, amelyeket a számítógépek használnak a weboldalak megtalálásához. A hackerek kihasználhatják a DNS-eket, hogy átírásokat eszközölve az áldozatokat az eredetileg várt helyett egy

a támadó által ellenőrzött weboldalra irányítsák. Ezek a hamis weboldalak pontosan olyanok, mint a felhasználók által várt weboldalak. Ennek eredményeként a DNS spoofing támadások áldozatai nem gyanakodnak, amikor arra kérik őket, hogy adja meg a fiókjuk bejelentkezési hitelesítő adatait egy olyan weboldalon, amelyet valósnak gondolnak.

https://www.zts.hu/blog/hanyfelekeppen-tamadhatjak-meg-a-cegunk-szervereit-2-resz/

50. **DNS tunneling:** a DNS-protokoll manipulálását jelenti, amelynek célja a rosszindulatú forgalom átirányítása a szervezet védelmi rendszerén. Rosszindulatú domainek és DNS-kiszolgálók használatával a támadó a DNS segítségével megkerülheti a hálózati biztonságot, és adatokat szerezhet meg.

https://www.zts.hu/blog/hanyfelekeppen-tamadhatjak-meg-a-cegunk-szervereit-2-resz/

51. **DoS-támadás:** A DoS-támadás (Denial-of-Service) során egyetlen támadó egyetlen forrásból próbál túlterhelni és szolgáltatásmegtagadásra kényszeríteni egy célpontot. A különböző célpontoldali sebezhetőségek esetenként eredményre is vezethetnek és akár egyetlen okostelefonnal elvégezhető a támadás.

https://makay.net/kiberbiztonsagi-fogalomtar

52. **Doxing:** Egy személy, vagy szervezet magán-, vagy azonosításra alkalmas adatainak (különösen személyazonosításra alkalmas információinak) közzététele. Ezen információk megszerzésére alkalmazott módszerek tartalmazzák a nyilvánosan hozzáférhető adatbázisok és a közösségi média (Social Network) oldalak (mint pl. a Facebook) kereséseit, a hekkelést, és a pszichológiai befolyásolást is. A doxing szorosan kapcsolódik az internetes bosszúálláshoz és hacktivizmushoz. A „doxing"-ot különböző okok miatt alkalmazzák, beleértve a (társadalmilag pozitív értelmű) bűnüldözés támogatását, az üzleti elemzést, de a rosszindulatú (adott esetben törvényellenes) cselekvést is, vagyis például a zsarolást, a kényszerítést, a zaklatást, az online megszégyenítést és a bosszúállást egyaránt.

https://sealog.hu/tudastar/fogalomtar/doxing-v-doxxing

53. **Easter Egg:** A „húsvéti tojás" egy rejtett kód a számítógépes szoftverekben, amely a normál működésén kívül eső funkciót lát el, néha a gyártó által beépített vagy jogellenesen elhelyezett kód, hogy back door-t biztosítson. Ezek a rejtett funkciók vagy üzenetek különféle digitális platformokon, például videojátékokban, weboldalakon és szoftveralkalmazásokban találhatók és

népszerűek a felhasználók körében, a felhasználói élmény javítására és a fejlesztők kreativitásának bemutatására törekednek.

https://www.twingate.com/blog/glossary/easter-egg

54. **Etikus hackelés:** Az etikus hackelés magában foglalja a számítógépes rendszerek vagy hálózatok gyenge pontjainak megkeresését – de ahelyett, hogy illegális tevékenységekre használnák, segítik a biztonsági ellenintézkedések kidolgozását. Az általuk feltört számítógépes rendszer vagy hálózat a tulajdonos engedélyével, a jogszabályok betartásával történik. Minden általuk azonosított biztonsági kockázatról beszámolnak a tulajdonosnak, amennyiben szükséges, tájékoztatják a hardver- és szoftvergyártókat a talált sebezhetőségekről. Az etikus hackelést végző szakértőket „etikus hackereknek" nevezik, akik biztonsági értékeléseket végeznek a szervezet biztonsági intézkedéseinek javítása érdekében.

https://www.unite.ai/hu/what-is-ethical-hacking-how-does-it-work/

55. **Evil twin phishing:** Ennél az elkövetési módnál a támadók egy ismert, legitim vezeték nélküli (wifi) hozzáférési ponttal azonos nevű hamis hozzáférési pontot hoznak létre. A támadók ezután ráveszik az áldozatokat, hogy csatlakozzanak rá az eszközükkel, majd megfigyelik, lehallgatják az óvatlanul a hálózatra csatlakozó felhasználók online forgalmát. Így érzékeny adatokhoz, például felhasználónevekhez és jelszavakhoz férhetnek hozzá. A felhasználók gyakran észre sem veszik, hogy támadás áldozatául estek.

https://kiberpajzs.hu/csalastipusok/szamitogepes/evil-twin-phishing/

56. **Exploit:** A kizsákmányolás olyan program vagy kódrészlet, amelynek célja egy alkalmazás vagy számítógépes rendszer biztonsági hibájának vagy sebezhetőségének észlelése és kihasználása, általában aljas okokból, mint pl. malware telepítés. A kizsákmányolás egy olyan módszer, amelyet a számítógépes bűnözők használnak rosszindulatú programok szállítására, nem pedig magát a rosszindulatú programot. A kihasználások olyan adatokat vagy végrehajtható kódot tartalmaznak, amelyek egy vagy több szoftverhibát képesek kihasználni egy helyi vagy távoli számítógépen. Tegyük fel például, hogy van egy olyan sebezhetőségű böngészőnk, amely lehetővé teszi „tetszőleges kód" futtatását, vagyis egy rosszindulatú alkalmazás telepítését és futtatását a rendszeren, vagy váratlan rendszerviselkedés előidézését a felhasználó tudta nélkül. A támadók kezdeti lépése általában a jogosultság eszkalációja, amely lehetővé teszi számukra, hogy bármit megtegyenek a támadott rendszeren. A böngészők, a Flash, a Java és a Microsoft Office mellett a leginkább célzott szoftverkategóriák közé tartoznak. Elterjedtségük miatt mind a biztonsági

szakemberek, mind a hackerek aktívan vizsgálják őket, a böngészőfejlesztők pedig arra kényszerülnek, hogy rendszeresen készítsenek javításokat a sebezhetőségek kiküszöbölésére. Célszerű ezeket a javításokat a lehető leghamarabb telepíteni, de ez nem mindig lehetséges – elvégre minden lapot el kell vetni. Természetesen a bűnözők által felfedezett és feltáratlan sebezhetőségek, az úgynevezett nulladik napi sebezhetőségek kihasználása egyedülálló kihívást jelent. Sok időbe telhet, amíg a gyártók felismerik és kijavítják a problémát.

https://mpost.io/hu/glossary/exploit/

57. **Féreg:** lásd worm

58. **Firewall:** A tűzfalak olyan szoftverprogramok vagy hardvereszközök, amelyek szűrik és megvizsgálják az interneten keresztül érkező információkat. Az első védelmi vonalat képviselik, mivel megakadályozhatják a rosszindulatú programokat vagy a támadókat abban, hogy hozzáférjenek a hálózathoz és az információkhoz, mielőtt bármilyen potenciális kár keletkezhetne. Hardveres tűzfalakat egyes útválasztók tartalmaznak, és csak alig vagy egyáltalán nem igényelnek konfigurációt, mivel be vannak építve magába a hardverbe. Ezek a tűzfalak az útválasztó hálózatához csatlakozó számítógépek és készülékek forgalmát figyelik, azaz egyetlen berendezéssel szűrhetik az összes készülékhez való hozzáférést. A hardveres tűzfalak alapvető biztonságot nyújtanak az IoT-eszközök, például az intelligens termosztátok és az intelligens izzók számára. Ezeknek az új eszközöknek gyakran gyenge biztonsági jellemzői vannak, amelyek a hálózatot sebezhetővé teszik, ám a hardveres tűzfal segít megakadályozni az ilyen biztonsági problémákat.

https://www.mcafee.com/hu-hu/antivirus/firewall.html

59. **Gray Hat Hacker:** A gray hat hacker, magyarul szürke kalapos hacker olyan személy, aki ugyan engedély nélkül fér hozzá számítógépes rendszerekhez biztonsági rések feltárása céljából, de nem károkozási vagy anyagi haszonszerzési szándékkal cselekszik. Tevékenysége a fehér kalapos (etikus) és a fekete kalapos (rosszindulatú) hackereké között helyezkedik el. Bár előfordulhat, hogy törvénysértő módszereket alkalmaz – például egy rendszer sebezhetőségét a rendszergazda előzetes értesítése nélkül hozza nyilvánosságra –, szándéka gyakran a biztonság növelése. Mivel azonban ezeket az akciókat nem minden esetben végzi az érintett fél tudtával vagy beleegyezésével, a gray hat hackerek tevékenysége jogi és etikai szempontból is megosztó. Egyesek hasznosnak, mások kockázatosnak tartják őket a kiberbiztonság szempontjából.

https://www.twingate.com/blog/glossary/gray-hat-hacker

60. **Hacker:** A hacker olyan informatikában, programozásban jártas személy, akinek célja egy számítógépes rendszer gyenge pontjainak megtalálása. A hacker (vagy olykor cracker) leggyakrabban olyan kiberbűnözőt takar, aki „feltöri" informatikai eszközöket az ott lévő információk, adatok ellopása érdekében. A köznyelvben a kiberbűnözőket is ezzel a névvel illetik, az esetek többségében tévesen. – Nem minden hacker kiberbűnöző és nem minden kiberbűnöző hacker.

    https://makay.net/kiberbiztonsagi-fogalomtar

61. **Hacktivist:** hacktivisták olyan bűnözői csoportok, amelyek politikai ügyek támogatása érdekében összefognak, hogy kibertámadásokat hajtsanak végre. A hacktivisták jellemzően egész iparágakat céloznak meg, de néha olyan szervezeteket is támadnak, amelyekről úgy vélik, hogy nem egyeznek politikai nézeteikkel vagy gyakorlatukkal. Bizonyos esetekben a hacktivisták nem az áldozat szervezetének meggyőződése, hanem az ügyfeleik és üzleti partnereik alapján célozzák meg a szervezeteket (Wheeler–Gregory, 2007).

62. **Hálózatvadászat:** lásd wardriving

63. **Hamis banki SMS:** lásd smishing

64. **Hamis banki telefonhívás:** lásd vishing

65. **Hamis szolgáltatói ügyintézés a közösségi médiában:** lásd Angler phishing

66. **Hamis wifi-hálózat létrehozása:** lásd Evil twin phishing

67. **Hátsó kapu:** lásd backdoor

68. **Hitelesítés:** A hitelesítés az a folyamat, amellyel a vállalatok gondoskodnak arról, hogy csak a megfelelő engedélyekkel rendelkező személyek, szolgáltatások és alkalmazások használhassák a szervezeti erőforrásokat. Ez fontos része a kiberbiztonságnak, mert a rosszindulatú szereplők első számú prioritása, hogy jogosulatlan hozzáférést szerezzenek a rendszerekhez. Teszik ezt úgy, hogy ellopják a hozzáféréssel rendelkező felhasználók felhasználónevét és jelszavát. A hitelesítési folyamat a következő három elsődleges lépésből áll: azonosítás (a felhasználó kilétének megadása, pl. felhasználónévvel), hitelesítés (a megadott kilét igazolása, pl. jelszóval, eszközzel vagy biometrikus adatokkal), valamint engedélyezés (annak ellenőrzése, hogy az adott felhasználó hozzáférhet-e a kért erőforráshoz).

    https://www.microsoft.com/hu-hu/security/business/security-101/what-is-authentication

69. **Hívószám-hamisítás:** lásd spoofing

70. **Hoax:** A hoaxok általában ostoba csínyek, amik lánclevelek vagy úgynevezett városi legendák (Urban Legends) formájában terjednek. A computer vírusokról szóló beugratások megpróbálnak félelmet kelteni, bizonytalanságot és kétséget ébreszteni a címzettekben, hogy egy észrevehetetlen vírussal állnak szemben. Néhány ilyen levélben valóban volt olyan rosszindulatú kód, amely képes volt fájlokat törölni a felhasználók gépeiről. Az ilyesfajta üzeneteket hagyjuk figyelmen kívül, és egyszerűen töröljük ki őket. Jó szerencsénk az életben semmilyen módon nem függ attól, hogy egy figyelmeztető levelet elküldünk-e húsz legjobb barátunknak, és ez a módszer semmiképp nem szolgálja gépünk biztonságát, ráadásul felesleges levélforgalmat is okoz.

    https://www.eset.com/hu/termektamogatas/veszelyek/

71. **Időzített bomba:** lásd Time Bomb

72. **Indicator of Compromise:** Az IOC, azaz jogosulatlan adathozzáférésre vagy biztonsági incidensre utaló jel egy olyan digitális nyom, amely arra enged következtetni, hogy egy végpontot vagy hálózatot esetlegesen feltörtek. Ahogyan a fizikai bizonyítékok is segítenek a nyomozásban, ezek a digitális nyomok lehetővé teszik az információbiztonsági szakemberek számára, hogy azonosítsák a rosszindulatú tevékenységeket vagy biztonsági fenyegetéseket, például az adatlopásokat, belső visszaéléseket vagy kártékony szoftveres támadásokat. A nyomozók manuálisan is összegyűjthetik ezeket a jeleket, ha gyanús tevékenységet észlelnek, de az információk automatikusan is gyűlhetnek a szervezet kiberbiztonsági megfigyelőrendszereinek részeként. Ezeket az adatokat felhasználhatják egy épp zajló támadás mérséklésére vagy egy már megtörtént biztonsági incidens orvoslására, valamint arra is, hogy fejlettebb eszközöket hozzanak létre, amelyek a jövőben képesek azonosítani és karanténba helyezni a gyanús fájlokat. Sajnos az IOC-figyelés reaktív jellegű, ami azt jelenti, hogy ha egy szervezet ilyen jelet talál, szinte biztos, hogy már megtörtént egy jogosulatlan adathozzáférés vagy biztonsági incidens. Ugyanakkor, ha az esemény még folyamatban van, az IOC gyors felismerése segíthet a támadás korai szakaszban való megfékezésében, így csökkentve annak üzleti hatását. Ahogy a kiberbűnözők egyre kifinomultabb módszereket alkalmaznak, úgy válik egyre nehezebbé az IOC-k észlelése is.

    https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/indicators-of-compromise-ioc/

73. **Internetes csalások:** lásd scams

74. **Internetes zaklatás:** lásd cyberbullying

75. **Internet of Things (IoT):** Az IoT, vagyis a dolgok internete, olyan összekapcsolt objektumok és eszközök hálózatát jelenti, amelyek érzékelőkkel, szoftverekkel és más technológiákkal vannak felszerelve, így képesek adatokat küldeni és fogadni más rendszerektől vagy eszközöktől. A legáltalánosabb értelemben minden olyan „dolog" az IoT részét képezheti, amely vezeték nélkül kapcsolódhat az internethez. Napjainkban az IoT különösen azokra az eszközökre utal, amelyek célja, hogy adatokat gyűjtsenek és továbbítsanak a felhasználók tájékoztatása vagy különféle műveletek automatizálása érdekében. Míg korábban a kapcsolódás főként wifi-n keresztül történt, ma már az 5G és más fejlett hálózati technológiák teszik lehetővé a nagy mennyiségű adat gyors és megbízható kezelését, szinte bárhol a világon.

    https://www.sap.com/hungary/products/technology-platform/what-is-iot.html

76. **Intrusion Prevention System (IPS):** Az IPS, azaz behatolásmegelőző rendszer egy hálózatbiztonsági technológia, amely figyeli a hálózati forgalmat, azonosítja a rosszindulatú tevékenységeket, és automatikusan megakadályozza azok végrehajtását. Az IPS rendszerek képesek észlelni és blokkolni a különféle fenyegetéseket, például a rosszindulatú szoftvereket, a sebezhetőségek kihasználását és a parancs- és vezérlési kommunikációkat, még mielőtt azok elérnék a célrendszert. Az IPS rendszerek kulcsfontosságú szerepet játszanak a modern hálózatbiztonságban, mivel képesek valós időben észlelni és megakadályozni a különféle fenyegetéseket, hozzájárulva ezzel a szervezetek informatikai infrastruktúrájának védelméhez.

    https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

77. **Kártevőalapú adathalászat:** Elterjedt adathalászati módszer. Az ilyen típusú támadások közé tartoznak például az e-mailekben megbízható mellékletnek (például önéletrajznak vagy bankszámlakivonatnak) álcázott kártevők. Bizonyos esetekben a kártevőt tartalmazó mellékletek megnyitása akár a teljes informatikai rendszert megbéníthatja.

    https://www.microsoft.com/hu-hu/security/business/security-101/what-is-phishing

78. **Kémprogram:** lásd spyware

79. **Kéretlen reklám program:** lásd adware

80. **Kernel mode:** A kernel mód a számítógépes rendszer központi feldolgozóegységének (CPU) privilegizált működési módja. Az operációs rendszer architektúrájának kritikus elemeként lehetővé teszi az összes gépi utasítás végrehajtását, valamint korlátlan hozzáférést biztosít a hardver- és rendszererőforrásokhoz. Ebben a módban a CPU a legmagasabb szintű vezérléssel rendelkezik, így képes a memória, a hardvereszközök és a folyamatok kezelésére.

    https://www.ituonline.com/tech-definitions/what-is-kernel-mode/

81. **Keylogger:** A keylogger, vagyis billentyűzetfigyelő egy olyan program vagy hardvereszköz, amely nyomon követi és rögzíti a felhasználó billentyűleütéseit gépelés közben. Az így begyűjtött információkat elküldi egy hackernek egy úgynevezett parancs- és vezérlőszerveren (C&C – Command and Control) keresztül. A hacker ezután elemzi a billentyűleütéseket, hogy megtalálja a felhasználóneveket és jelszavakat, amelyeket felhasználva bejuthat egyébként védett rendszerekbe. A keyloggereknek két típusa van: a szoftveres keylogger kártékony programként települ a számítógépre, és akár más eszközökre is képes átterjedni, míg a hardveres keylogger egy fizikai eszköz, amely ugyan nem terjed tovább, de szintén képes érzékeny információk kiszivárogtatására. Mindkét típus komoly veszélyt jelent a digitális biztonságra, mivel képesek hozzáférést biztosítani a támadók számára különféle fiókokhoz és rendszerekhez.

    https://www.fortinet.com/resources/cyberglossary/what-is-keyloggers

82. **Kiberbiztonság:** lásd cybersecurity

83. **Kiberbűnözés:** lásd cybercrime

84. **Kiberfegyver:** lásd cyber weapon

85. **Kiberháború:** lásd cyber warfare

86. **Kibertér:** lásd cyberspace

87. **Kiberterrorizmus:** lásd cyberterrorism

88. **Killware:** A killware olyan digitális kártevők (malware-ek) gyűjtőneve, amelynek célja, hogy fizikai sérülést vagy veszélyt okozzon a kritikus infrastruktúrákban, mint például az olajvezetékek, vízellátó rendszerek vagy kór-

házak. Ide sorolhatók például az olyan zsarolóvírusok, amelyek kifejezetten kórházakat és létfenntartó rendszereket támadnak meg.

https://makay.net/kiberbiztonsagi-fogalomtar

89. **Lándzsás adathalászat:** lásd spear phishing

90. **Levélszemét:** lásd spam

91. **Live Response:** A Live Response (vagy Live Triage) a kiberbiztonságban egy olyan valós idejű incidenskezelési módszer, amellyel a biztonsági szakemberek aktív, működő rendszerekről gyűjtenek adatokat egy kibertámadás vagy gyanús tevékenység idején. A cél az, hogy gyorsan azonosítsák a fenyegetéseket és megtegyék a szükséges lépéseket a károk minimalizálása érdekében. A folyamat során például futó folyamatokat, hálózati kapcsolatokat, naplóállományokat és memóriaadatokat vizsgálnak, gyakran távoli parancssori hozzáféréssel.

https://www.upguard.com/blog/cybersecurity-triage

92. **Logic Bomb:** A logikai bomba egy szoftverbe ágyazott rosszindulatú kód, amely addig marad alvó állapotban, amíg bizonyos feltételek nem teljesülnek. Bekapcsoláskor a logikai bomba vírus romboló műveletet hajt végre, például fájlok törlését vagy kritikus rendszerek megzavarását. A hagyományos rosszindulatú programokkal ellentétben a logikai bomba nem terjed aktívan, hanem az előre meghatározott aktiválási eseményre vár.

https://www.beyondtrust.com/resources/glossary/logic-bomb

93. **Logikai bomba:** lásd Logic Bomb

94. **Malvertising:** A malvertising az online hirdetési hálózatokat használja arra, hogy kártevőkkel fertőzze meg az áldozatok számítógépét vagy mobil eszközét. A támadók hamis hirdetéseket vagy rosszindulatú kódot helyeznek el a legitim hirdetési hálózatokon, amelyeket a megjelenő weboldalak egy része megjeleníthet, és amelyek megfertőzhetik az áldozatok számítógépét, ha rákattintanak a hirdetésre. Előfordult, hogy a támadók rosszindulatú hirdetéseket helyeztek el az eBay online aukciós weboldalán is.

https://www.zts.hu/blog/hanyfelekeppen-tamadhatjak-meg-a-cegunk-szervereit-2-resz/

95. **Malware:** A malware kifejezés magában foglal mindenféle rosszindulatú szoftvert vagy kódot, beleértve ezek legismertebb fajtáit, mint a trójaiak, zsarolóvírusok, vírusok, férgek és banki kártevők. A közös tulajdonságuk a

szerzőik és alkotóik rosszindulatú szándéka. Egy általános felhasználó nehezen tudja megállapítani, melyik fájl malware, és melyik nem. Ezért vannak a biztonsági megoldások, amelyek hatalmas adatbázisokat tartanak fent a korábban felismert rosszindulatú mintákból, és többféle védelmi technológiát alkalmaznak az újak ellen, ezzel segítve a hatékony felismerést. A malwareírók az utóbbi időben sajnos nagyon kreatívak. „Termékeik" elavult rendszerek sebezhetőségein keresztül terjednek, korábbi biztonsági szabályokat játszanak ki, a memóriában rejtőznek vagy ismert alkalmazásokat utánozva maradnak észrevétlenek. Azonban még ma is a leggyengébb láncszem a leghatékonyabb fertőzésekhez maga a felhasználó. A jól kialakított, rosszindulatú melléklettel ellátott e-mailek bizonyítottan hatékony, mégis olcsó módjai annak, hogy kellemetlen helyzetbe hozzanak egy rendszert.

https://www.eset.com/hu/malware/

96. **Man in the middle támadás:** Az MitM támadás során a két fél közötti kommunikációt egy támadó jogosulatlan hozzáféréssel és manipulációval befolyásolja úgy, hogy a kommunikációs csatornát (tipikusan valamilyen számítógépes hálózatot) eltérítve mindkét fél számára a másik félnek adja ki magát. Így a két fél azt hiszi, hogy egymással beszélget, miközben valójában mindketten a támadóval vannak csak kapcsolatban, aki így kijátszhatja az ilyen támadásra fel nem készített kihívás/válasz protokollokat, egyszerűen továbbítva a kihívást a másik félnek, majd visszaküldve annak válaszát. Egy sikeres MitM támadás lehetővé teszi a támadóknak, hogy elfogják vagy manipulálják az érzékeny személyes információkat, például a bejelentkezési hitelesítő adatokat, tranzakciós részleteket, számlaadatokat és hitelkártya számokat. Ezek a támadások gyakran az online banki alkalmazások és az e-kereskedelmi weboldalak felhasználóit célozzák meg, és sok esetben a phishing e-maileket használják fel a felhasználók megfertőzésére, hogy olyan kártevőket telepítsenek, amelyek lehetővé teszik a támadást.

https://www.zts.hu/blog/hanyfelekeppen-tamadhatjak-meg-a-cegunk-szervereit-2-resz/

97. **Man in the Disk:** Az MitD sérülékenység a sebezhető szoftveren és annak felhasználóján kívül egy harmadik fél (személy vagy kártékony kód) számára is hozzáférést és/vagy módosítási lehetőséget biztosít a szoftver lokálisan tárolt adataihoz, komponenseihez.

https://makay.net/kiberbiztonsagi-fogalomtar

98. **Multifactor Authentication (MFA):** A multifactor authentication, magyarul többtényezős hitelesítés egy olyan biztonsági eljárás, amely során a felhaszná-

lónak a bejelentkezéshez nemcsak egy, hanem legalább két különböző hitelesítési tényezőt kell megadnia. Ezek a tényezők három kategóriába sorolhatók: valami, amit a felhasználó tud (például jelszó vagy PIN-kód), valami, ami a birtokában van (például mobiltelefon vagy biztonsági kulcs), és valami, ami ő maga (például ujjlenyomat vagy arcfelismerés). A többtényezős hitelesítés célja, hogy jelentősen csökkentse az illetéktelen hozzáférések esélyét, és növelje az online fiókok és adatok biztonságát.

https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661

99. **Nigériai típusú csalások:** A „nigériai típusú" csalás a megtévesztés egyik legrégebbi, 19. század végén elterjedt formája, amit nigériai levelekként vagy 419-es átveréseként is említenek. Kezdetben hagyományos, postai úton vagy faxon terjedt, de a telekommunikációs eszközök fejlődésével, valamint az internet és az e-mail terjedésével ennek a csalástípusnak is az online tér vált a fő platformjává. A nigériai csalások során az elkövetők valamilyen megtévesztő kommunikációval – jellemzően e-mailben – pénz utalására veszik rá az áldozatukat, vagyis ezekben az esetekben az ügyfelek maguk utalnak! A hamis levelekben, megkeresésekben általában segítséget kérnek az elkövetők: menekültek vagyonának vagy jogtalanul elvett örökségnek a visszaszerzéséhez, valamilyen okból átmenetileg hozzá nem férhető összeg megszerzéséhez, stb. Közösségimédia-oldalakon, online társkereső portálokon terjed a nigériai csalás azon változata, amelynél az elkövető romantikus kapcsolatot épít fel leendő áldozatával, mielőtt valamilyen megható történettel pénzt kér tőle. A megtévesztő történetet valódinak látszó, de hamis közösségimédia-profillal és eredetinek tűnő, de szintén fiktív iratokkal igyekeznek alátámasztani. Hogy a történet hihetőbb legyen, előfordulhat, hogy a csalók nemzetközi átutalást kezdeményeznek, amit aztán visszavonnak, így mutatva, hogy az összeg valójában rendelkezésre áll, csak a levélben jelzett adminisztratív nehézség áll a kifizetés útjában. A levélben kért segítség kizárólag egy bizonyos pénzösszeg átutalását jelenti. Mindezért későbbi busás jutalmat ígérnek, amit azonban a károsultak végül nem kapnak meg, de a befizetett összeget elvesztik. Az is egy bevett forma, hogy a vagyon kimenekítéséhez a címzettnek meg kell adnia a bankszámlaadatait, aminek az eredménye természetesen nem az, hogy pénzösszeg érkezik rá, ellenkezőleg: az elkövetők immár hozzáférnek a bankszámlához, így akár le is nullázhatják azt.

https://www.mnb.hu/fogyasztovedelem/digitalis-biztonsag/az-adathalasz-csalasok-legjellemzobb-tipusai/nigeriai-csalas

100. **Online Fraud (Online csalás):** Az online csalás – más néven kibercsalás vagy internetes csalás – olyan jogellenes tevékenységeket foglal magában, amelyek célja magánszemélyek vagy szervezetek megtévesztése annak érdekében, hogy pénzbeli vagy más jellegű előnyhöz jussanak. Ezek a csalások különböző módszereken alapulnak, és az internet anonimitását, valamint széles körű hozzáférhetőségét használják ki. Következményei lehetnek az adatvesztés, anyagi kár vagy a jó hírnév sérülése is.

https://www.fraudsmart.ie/personal/fraud-scams/online-fraud/

101. **OSINT:** Az OSINT (Open Source Intelligence vagyis nyílt forrású hírszerzés) olyan hírszerzési módszer, amely nyilvánosan elérhető információkat gyűjt és analizál, hogy információkat szerezzen, például az interneten. Az OSINT célja a hírszerzési szempontokból fontos információk gyűjtése, szelektálása, elemzése, értékelése és felhasználása, például biztonsági célokból, de más szervezetek és egyének számára is használható.

https://makay.net/kiberbiztonsagi-fogalomtar

102. **Payload:** Káros rutin, vagy gyakran payload néven emlegetett funkció az, amit egy rosszindulatú program (például vírus, féreg vagy trójai) valóban végrehajt, miután bejutott egy rendszerbe. Ez a kiegészítő funkció a támadó eredeti célját szolgálja. A káros rutin sokféle lehet: adatlopás (érzékeny információk, például jelszavak, bankkártya adatok vagy személyes fájlok ellopása), fájlok módosítása vagy törlése (fontos dokumentumok, rendszerelemek megsemmisítése vagy átírása), rendszerösszeomlás (a számítógép működésképtelenné tétele), lemezterület felülírása (a merevlemez adatainak helyreállíthatatlan tönkretétele), BIOS felülírása (a számítógép alapvető indítási programjának megrongálása, ami megakadályozza a gép elindulását). Fontos szem előtt tartani, hogy nem minden kártékony program okoz azonnal észrevehető károkat. Vannak például olyan régebbi vírusok, amelyek csak kisebb, zavaró hatásokat idéztek elő – például hangot adtak ki billentyűlenyomásra –, és bár nem rongálták meg a rendszert, kellemetlenséget okoztak a felhasználónak. A trójai programok esetében a kártékony működés egy rejtett funkció, amelyet a készítő szándékosan elrejtett. Ez a funkció jelenti a program valódi célját – például egy hasznosnak tűnő alkalmazás mögé elrejtett adatlopó modul formájában jelenhet meg.

https://www.eset.com/hu/termektamogatas/veszelyek/

103. **PDoS-támadás:** A PDoS-támadás (Permanent Denial-of-Service) során a támadó arra törekszik, hogy egy adott szolgáltatást vagy rendszeralkalmazást tartósan elérhetetlenné tegyen fizikai, vagy hardveres károsítással.

Ez ellentétben áll a hagyományos DoS (Denial of Service) támadásokkal, amelyek a szolgáltatást túlterhelésen keresztül elérhetetlenné teszik. A PDoS támadások veszélyesek lehetnek, mivel a szolgáltatást hosszabb ideig elérhetetlenné teszik, sőt, akár fizikai károkat is okozhatnak.

https://makay.net/kiberbiztonsagi-fogalomtar

104. **Penetrációs teszt:** A penetrációs teszt egy informatikai rendszer (kiszolgáló, weboldal stb.) értékelése biztonsági (szoftveres, konfigurációs) sebezhetőségek szempontjából. A sérülékenységvizsgálattal ellentétben a penetrációs (behatolás) tesztelés a vizsgálat tárgya által küldött válaszokból és viselkedési mintákból nemcsak feltételezi egy-egy sérülékenység meglétét, de azok kihasználhatóságát is teszteli offenzív módszerekkel.

https://makay.net/kiberbiztonsagi-fogalomtar

105. **Phishing:** adathalász csalási forma ügyfeleket célzó, csaló szándékú e-mail, amely személyes, pénzügyi vagy biztonsági információi megosztására próbálja rávenni a címzettet. Ezek a levelek azonosnak tűnhetnek azokkal az üzenetekkel, amelyeket a létező bankok küldenek: a csalók lemásolják a valódi e-mailek logóit, kinézetét és stílusát, esetenként korábbi (hamis vagy valós) levélváltások részleteit is tartalmazzák. Általában sürgető hangvételűek, például büntetéssel fenyegetnek arra az esetre, ha valaki nem válaszol, de arra is kérhetik, hogy töltsön le egy mellékletet, vagy kattintson egy hivatkozásra. A kiberbűnözők arra építenek, hogy az emberek elfoglaltak: felületes áttekintésre, futó pillantásra a hamis e-mailek igazinak tűnnek. Ennek következtében a címzett nagyobb valószínűséggel veszi komolyan őket, és cselekszik a leírtak szerint.

https://kiberpajzs.hu/csalastipusok/emailes/phishing/

106. **Phreaking:** A phreaking olyan tevékenységet jelent, amely telekommunikációs rendszereket, például nyilvános telefonhálózatokhoz csatlakoztatott berendezéseket és rendszereket tanulmányoz, kísérletezik vagy felfedez. A phreaking során az illetéktelen személyek technikai eszközökkel manipulálják vagy megkerülik a telefonrendszerek működését, hogy ingyenes hívásokat kezdeményezzenek vagy hozzáférnek a hálózat bizalmas részeihez. Eredetileg az analóg telefonhálózatokkal kapcsolatos csalásokra vonatkozott, de a digitális technológia fejlődésével a tevékenység kiterjedt a modern kommunikációs rendszerek feltörésére is.

https://www.ninjaone.com/it-hub/endpoint-security/what-is-phreaking/

107. **Polimorf vírus:** A polimorf vírusok olyan összetett kódok, amelyek képesek minden fertőzés során módosított verziókat létrehozni magukból, miközben megőrzik az alapvető működési rutinokat. A forráskód-felismerés elkerülése érdekében a vírus kódját titkosítják, és minden alkalommal más titkosítási kulcsokat alkalmaznak. Működésük alapja a mutációs motor, amely minden új fertőzésnél megváltoztatja a visszafejtési rutint. Ezáltal a polimorf vírus nem statikus kódot használ, így a hagyományos víruskereső szoftverek számára nehezebben észlelhető. A fejlettebb mutációs motorok akár több milliárd különböző dekódoló rutint is képesek előállítani, még tovább növelve a vírus rejtőzködő képességét.

    https://www.trendmicro.com/vinfo/us/security/definition/polymorphic-virus

108. **Pretty Good Privacy (PGP):** A PGP egy titkosító szoftver, amelyet az online kommunikációs rendszerek adatvédelmének, biztonságának és hitelesítésének biztosítására terveztek. Bár kezdetben csak e-mail üzenetek és mellékletek védelmére használták, a PGP-t ma már széles körben alkalmazzák, beleértve a digitális aláírásokat, a teljes lemeztitkosítást és a hálózati védelmet. A PGP egyik leggyakoribb felhasználási módja az e-mailek védelme. A PGP-vel védett e-mail olvashatatlan karakterlánccá (titkosított szöveggé) alakul, amelyet csak a megfelelő visszafejtési kulccsal lehet megfejteni. A működési mechanizmusok gyakorlatilag megegyeznek a szöveges üzenetek védelme esetében alkalmazottakkal, és vannak olyan szoftveralkalmazások is, amelyek lehetővé teszik a PGP más alkalmazásokra való telepítését, így gyakorlatilag titkosítási rendszert adnak hozzá a nem biztonságos üzenetküldő szolgáltatásokhoz. Bár a PGP-t elsősorban az internetes kommunikáció biztonságossá tételére használják, egyes eszközök titkosítására is alkalmazható. Ebben az összefüggésben a PGP alkalmazható számítógép vagy mobileszköz lemezpartícióira. A merevlemez titkosításával a felhasználónak minden rendszerindításkor meg kell adnia a jelszavát.

    https://academy.binance.com/en/articles/what-is-pgp

109. **Pszichológiai manipuláció:** A pszichológiai manipuláció olyan stratégia, amelyet egyének vagy csoportok alkalmaznak, hogy manipuláció és megtévesztés révén rávegyék az embereket arra, hogy érzékeny információkat fedjenek fel, vagy a biztonságukat veszélybe sodró dolgokat tegyenek. E módszer inkább a pszichológián és az emberi viselkedésen, mintsem a technikai szaktudáson alapul. A pszichológiai manipulációs támadások során gyakran előfordul, hogy a támadó megbízható személynek vagy forrásnak adja ki magát, hogy az áldozat bizalmába férkőzzön. A támadók által hasz-

nált taktikák közé tartozik többek között a hamis személyiség felvétele, a meggyőzés, illetve a megtévesztés az olyan értékes információk megszerzése céljából, mint például jelszavak, pénzügyi adatok, rendszerek és hálózatok hozzáférési adatai. A pszichológiai manipulációs támadások többféle formát ölthetnek. E stratégia lényege az emberi sebezhetőségek kihasználása: a támadók így akarják elérni céljaikat, legyen az akár jogosulatlan hozzáférés, akár adat- vagy pénzlopás.

https://www.consilium.europa.eu/hu/policies/cybersecurity-social-engineering/

110. **QR-kódos csalás**: Az ilyen típusú csalások esetében az elkövetők azt használják ki, hogy a QR-kód beolvasása előtt a felhasználók nem tudhatják biztosan, mi fog történni, így kénytelenek megbízni annak készítőjében. A csalás célja adathalászat: az elkövetők személyes adatokhoz, illetve bankszámla-adatokhoz próbálnak hozzáférni. Hamis weboldalakon vagy matricákon helyeznek el QR-kódokat, és különféle trükkökkel ösztönzik az embereket azok beolvasására. A QR-kódok adatokat tartalmaznak, és linkként, hivatkozásként működnek, amelyek mögött lehet egy hamis weboldal, káros alkalmazás letöltési linkje, vagy akár egy automatikus fizetési művelet is. Gyakran előfordul, hogy a támadók legitim szervezetek arculatát kihasználva, hivatalos plakátokon, posztereken vagy szórólapokon cserélik ki az eredeti QR-kódokat a sajátjaikra.

https://www.mnb.hu/fogyasztovedelem/digitalis-biztonsag/az-adathalasz-csalasok-legjellemzobb-tipusai/qr-kodos-csalas

111. **Ransomware:** A zsarolóprogramok olyan típusú rosszindulatú szoftverek vagy kártevők, amelyeket a kiberbűnözők arra használnak, hogy megakadályozzák az áldozat kritikus adataihoz való hozzáférést, megsemmisítsék vagy közzétegyék azokat, hacsak nem fizetnek jelentős összegű váltságdíjat. A hagyományos zsarolóprogramok mind magánszemélyeket, mind szervezeteket veszélyeztetnek, de két közelmúltbeli fejlesztés, az ember által irányított zsarolóprogramok és a szolgáltatásként nyújtott zsarolóprogramok egyre nagyobb fenyegetést jelentenek a vállalatokra és más nagy szervezetekre nézve. Az ember által irányított zsarolóprogramok esetében a támadók egy csoportja a kollektív intelligenciát használja arra, hogy hozzáférjen a vállalati hálózatokhoz. A zsarolóprogram telepítése előtt kutatást végeznek a vállalattal kapcsolatban, hogy megismerjék a biztonsági réseket, és egyes esetekben pénzügyi dokumentumokat tárnak fel, amelyek segítségével meghatározhatják a váltságdíj összegét. A szolgáltatásként nyújtott zsarolóvírus-modell lényege, hogy egy csapat bűnszervezeti fejlesztő létre-

hozza a zsarolóprogramot, majd felbérel más kiberbűnöző társvállalatokat, hogy feltörjék a szervezet hálózatát és telepítsék a zsarolóprogramot. A két csoport megállapodás szerinti arányban osztozik a nyereségen. Minden zsarolóprogram jelentős veszteséget okoz a megtámadott egyéneknek és szervezeteknek. Napokba, hetekbe vagy akár hónapokba is telhet, amíg az érintett rendszerek ismét online állapotba kerülnek, ami a termelékenység és az értékesítés csökkenését eredményezi. A szervezetek jó hírneve is sérülhet az ügyfelek és a közösség körében.

https://www.microsoft.com/hu-hu/security/business/security-101/what-is-ransomware

112. **Reklámprogram:** lásd adware

113. **Romance Scam:** A romance scam, magyarul romantikus csalás a csalások olyan formája, amelyben romantikus szándékot színlelnek a csalók, hogy elnyerjék az áldozatok szimpátiáját, majd a jóindulatukat kihasználva rávegyék őket, hogy különböző hamis ürügyekkel pénzt küldjenek nekik. A célcsoport kiválasztásának pszichológiai okai vannak, ugyanis megfigyelhető, hogy egy idősebb, egyedülálló hölgy esetén van a legnagyobb esély a magány érzésére, amely magában hordozza annak a veszélyét, hogy egy párkapcsolat reményében az átlagosnál óvatlanabb legyen. A csalók ilyenkor kihasználják azt az emberi tulajdonságot is, hogy a racionalitás és a józan döntések meghozatala háttérbe szorul, vagyis azt az állapotot, amikor a szív dominál. A csalás létjogosultságát és a növekvő tendenciáját sajnálatos módon az adja, hogy az emberek nem kellően tudatosak. Amennyiben képesek lennének felismerni a csalókat és azok trükkjeit, rövid időn belül eltűnnének a közéletből, mert nem érné meg számukra a befektetett energia. A használt technikákban, történetekben és kisebb részletekben előfordulnak eltérések az egyes esetek között, de általánosan elmondható, hogy az említett főbb pontok az ilyen jellegű csalások mindegyikében megtalálhatók.

https://nki.gov.hu/wp-content/uploads/2024/02/A-romantikus-csalas.pdf

114. **Rootkit:** A rootkit egy olyan rosszindulatú program, amely lehetővé teszi a kiberbűnözők számára, hogy észrevétlenül hozzáférjenek a számítástechnikai eszközökhöz és átvegyék egy számítógép vezérlését. Kezdetben a rootkitek a UNIX operációs rendszerre jelentek meg (beleértve a Linux platformokat is), és ezek olyan eszközök gyűjteményét jelentették, amely alkalmas arra, hogy egy támadó rendszergazdai jogokat szerezhessen az adott rendszeren belül (ezt hívják a UNIX alatt „root" jognak). A rootkit kifejezést Windows alapú rendszereken általában az olyan programok meghatá-

rozására szokták használni, amelyek futó folyamatokat, állományokat vagy rendszerleíró adatbáziskulcsokat (Registry) rejtenek el az operációs rendszer, illetve a felhasználó elől. Az ilyen, Windowsra telepített rootkit olyan funkciókat használ, amelyekkel nem csak saját magát képes elrejteni, hanem további kártékony kódokat – például billentyűleütés-naplózót (keylogger) - is észrevehetetlenné tud tenni. A rootkitek nem szükségképpen csak rosszindulatú kódok elkészítéséhez használhatók, de az utóbbi időben jelentősen növekvő mértékben használták fel ezt a rejtőzködő technikát a rosszindulatú kódok készítői.

https://www.eset.com/hu/termektamogatas/veszelyek/

115. **Rosszindulatú program:** lásd malware

116. **Sandbox:** A sandboxing egy olyan kiberbiztonsági gyakorlat, amely egy elszigetelt detonációs környezetet, vagy „homokozót" használ, ahol a biztonsági csapatok a biztonsági műveleti központban (SOC) az incidensreakciós ciklus részeként detonálják, megfigyelik, elemzik, észlelik és blokkolják a gyanús leleteket. Ez a módszer további védelmi réteget biztosít az ismeretlen támadási vektorokkal szemben. A sandbox használatával a biztonsági csapatok fejlett rosszindulatú programok elemzését végezhetik el a gyanús fájlok elkülönített környezetben történő futtatásával, amely a végfelhasználó operációs rendszerét emulálja. A sandboxing legfontosabb előnye, hogy megfigyelheti a futtatható fájlok, szkriptek vagy rosszindulatú dokumentumok viselkedését, és ezáltal lehetővé teszi teljesen új és ismeretlen rosszindulatú programok, vagy akár olyan rosszindulatú programok felderítését, amelyeket egy adott környezetben történő futtatásra terveztek. Ez a következő evolúciós lépés a vírusirtó (AV) motorok által megvalósított aláírásalapú felismerés után.

https://hungarian.opswat.com/blog/what-is-sandboxing

117. **Scams:** A csalások nagyon hasonlatosak az adathalászathoz, de ilyenkor nem a személyes adatok kifürkészése a támadók célja, hanem az emberi érzések manipulálására (social engineering) építenek: szánalmat ébresztenek, vagy az emberi kapzsiságra alapoznak. Például, majdnem minden természeti katasztrófa (földrengés, vihar, áradás, háború, éhínség) után megjelenik a csalási szándék állítólagos jótékony gyűjtések formájában. Van aztán a csalásoknak egy illetékekkel kapcsolatos csoportja (ezeket gyakran nigériai típusnak vagy 419-esnek is nevezik), amikor a csalók azzal kecsegtetik a célszemélyt, hogy nagy összegű pénzhez juthat, ha segít egy vagyont kimenekíteni valamelyik afrikai országból. Ezek a trükkök mindig arra épülnek, hogy

megkérik az áldozatot, küldjön előlegbe az adminisztrációhoz egy kisebb összeget (ez lehet akár több ezer dollár is). Előfordulhat az is, hogy az adott országba utazó megtévesztett áldozatot egyszerűen elrabolják vagy megölik. A kevésbé szélsőséges csalási esetekben igen sok ember vesztett már el így sok ezer dollárt. Íme néhány jó tanács, hogyan kerülhetők el az ilyen csalárd trükkök: A jótékonysági intézmények csak olyan érdeklődőkkel veszik fel a kapcsolatot e-mailjeikben, akik ezt kifejezetten kérik (előzetesen külön kérték, illetve hozzájárultak ahhoz, hogy ilyen levelet kaphassanak a szervezettől, ezt szakkifejezéssel Opted In-nek nevezik). A kéretlen, spam jellegű levelek szinte minden esetben csalások – és különösen katasztrófák, rendkívüli események után egészen hamar megjelennek. Éljen bennünk egy egészséges gyanakvás! Az e-mail üzenetek lemásolják egy adott szervezet levélformátumát, grafikai elemeit, ezáltal szinte teljesen hitelesnek látszanak. Sok levél tartalmazza a katasztrófák áldozatainak tragikus történetét.

https://www.eset.com/hu/termektamogatas/veszelyek/

118. **Script Kiddie:** A „script kiddie" egy lekicsinylő kifejezés, amelyet a számítógépes hackerek alkottak meg az internetes biztonsági réseket kihasználó éretlen, de gyakran ugyanolyan veszélyes személyekre. A script kiddie-k már meglévő, jól ismert technikákat, programokat és szkripteket használnak az internetre csatlakoztatott számítógépek gyengeségeinek felkutatására és kihasználására. Támadásaik véletlenszerűek, és kevés ismerettel rendelkeznek az általuk használt eszközökről, azok működéséről és az általuk okozott károkról. A forgatókönyvíró gyerekeket jellemzően egyszerű, személyes okok motiválják – szórakozás, káoszkeltés, figyelemfelkeltés vagy bosszú.

https://www.techtarget.com/searchsecurity/definition/script-kiddy-or-script-kiddie

119. **Sérülékenységvizsgálat:** A sérülékenységvizsgálat egy informatikai rendszer (kiszolgáló, weboldal stb.) értékelése biztonsági (szoftveres, konfigurációs) sebezhetőségek szempontjából. A penetrációs (behatolás) teszteléssel ellentétben a sérülékenységvizsgálat a vizsgálat tárgya által küldött válaszokból és viselkedési mintákból feltételezi egy-egy sérülékenység meglétét, annak kihasználhatóságát viszont nem teszteli offenzív módszerekkel.

https://makay.net/kiberbiztonsagi-fogalomtar

120. **Smishing:** A smishing (az angol „SMS" és „phishing", vagyis SMS és adathalászat szavak kombinációja) olyan csalás, amelynél a támadók SMS segítségével próbálnak megszerezni személyes, pénzügyi vagy biztonsági adatokat, információkat. Megbízható forrásnak álcázzák magukat, úgy tesznek,

mintha egy bank, kártyakibocsátó, futárszolgálat, közműszolgáltató vagy valamilyen egyéb szolgáltató képviseletében jelentkeznének. Az üzenet arra kéri a címzettet – általában sürgető módon –, hogy nyisson meg egy weboldalra vezető hivatkozást, telepítsen egy alkalmazást, vagy hívjon fel egy telefonszámot például a fiókja ellenőrzése, frissítése vagy újraaktiválása érdekében. A hivatkozás hamis weboldalra mutat, a telefonszámon pedig egy csaló jelentkezik, aki az adott cég munkatársának adja ki magát. A csalás célja olyan információk megszerzése, amelyek segítségével aztán ellophatják az óvatlan ügyfél pénzét.

https://kiberpajzs.hu/csalastipusok/sms/smishing/

121. **Social engineering:** A social engineering, magyarul társadalmi manipuláció egy olyan biztonsági támadási technika, amely során a támadó pszichológiai manipulációt alkalmaz, hogy megtévessze vagy rávegye az embereket bizalmas információk kiadására, hozzáférések megadására, vagy olyan cselekedetek végrehajtására, amelyek általában nem lennének megengedettek vagy biztonságosak. Ez a módszer nem technikai eszközökre, például szoftveres vagy hardveres feltörésekre épít, hanem az emberi bizalomra, figyelmetlenségre vagy jóhiszeműségre alapoz. A társadalmi manipuláció különféle formákban jelenhet meg, például telefonos átverésként, e-mailes adathalászatként, vagy személyes meggyőzésként, és célja, hogy az áldozat akaratlanul segítsen a támadónak megszerezni érzékeny adatokat vagy hozzáférést rendszerekhez.

https://en.wikipedia.org/wiki/Social_engineering_(security)

122. **Spam:** A spam bármilyen kéretlen digitális kommunikáció, amelyet tömegesen küldenek szét. A spam gyakran e-mailben érkezik, de terjedhet szöveges üzenetekben, telefonhívásokban vagy közösségi médiában is. A spammerek számos kommunikációs formát használnak a kéretlen üzenetek tömeges elküldésére. Ezek némelyike kéretlen árukat kínáló marketingüzenet. Más típusú spamüzenetek rosszindulatú programokat terjeszthetnek, rávehetik a címzettet személyes adatok megadására, vagy elriaszthatják azzal a gondolattal, hogy fizetnie kell a baj elkerülése érdekében. Az e-mail spamszűrők sok ilyen típusú üzenetet kiszűrnek, és a telefonszolgáltatók gyakran figyelmeztetnek az ismeretlen hívóktól származó „spamveszélyre". Akár e-mailben, SMS-ben, telefonon vagy közösségi médiában érkezik, egyes spamüzenetek átjutnak; érdemes felismerni őket, és elkerülni ezeket a fenyegetéseket.

https://www.malwarebytes.com/spam

123. **Spear phishing**: A spear phishing, magyarul szigonyozás olyan csalási technika, amely során a támadók személyre szabott üzenetekkel próbálják tőrbe csalni a potenciális áldozatot. A támadók folyamatosan finomítják módszereiket, és egyre több személyes információhoz férnek hozzá a közösségi média és egyéb online platformok révén. A hitelesség látszatát a kiberbűnözők az úgynevezett social profiling módszert alkalmazva építik fel: a leendő áldozatról nyilvánosan elérhető adatokból, részletes elemzést követően összeállítják annak profilját és elkészítik a személyre szabott félrevezető üzenetet. Ezek az üzenetek általában olyan információkat tartalmaznak, mint a személy neve vagy munkahelyének neve stb. A támadás jellemző elemei közé tartoznak a gyanús hivatkozások és mellékletek, amelyek gyakran rosszindulatú weboldalakra vezetnek, vagy kártékony szoftvereket tartalmaznak.

https://kiberpajzs.hu/csalastipusok/szamitogepes/landzsas-adathalaszat/

124. **Spoofing:** Spoofingnak általában azt a folyamatot nevezzük, amikor az információt küldő azonosságát módosítják vagy megváltoztatják, ezáltal elrejtve azt. A hívószám-spoofing, azaz hívószám-hamisítás a vishing (hamis banki hívások) adathalász tevékenységek egyik speciális elkövetési technikája. Lényege, hogy az elkövetők módosítják a hívószámot, amely a hívott fél telefonjának kijelzőjén megjelenik, ezzel elrejtve a valódi hívó fél azonosságát. Vagyis híváskor nem a hívást kezdeményező igazi telefonszáma jelenik meg a készüléken, hanem egy másik, jellemzően olyan szám, ami ismerős: például egy banké, ezáltal még inkább hitelesnek tűnik a hívás. Az ilyen hívások célja elsősorban a bizalom kiépítése, illetve az adathalász támadások első számú védvonalának, az óvatosságnak a kiiktatása. Az ismerős telefonszám megnöveli annak esélyét, hogy az áldozat együttműködik, és érzékeny információkat ad át, alkalmazást telepít, vagy pénzügyi műveletet hajt végre a támadó utasítására.

https://kiberpajzs.hu/csalastipusok/telefonos/spoofing/

125. **Spyware:** A spyware, magyarul kémprogram egy olyan nyomkövető szoftver, amelyet a felhasználó tudta és beleegyezése nélkül telepítenek egy számítógépre. Célja a felhasználói szokások, érzékeny adatok – például böngészési előzmények, jelszavak, banki azonosítók – megfigyelése és azok illetéktelen harmadik félhez való továbbítása. Egyes spyware-ek más programok beépített részeként, trójai alkalmazásokhoz hasonlóan, vagy számítógépes férgek részeként kerülnek a rendszerbe. Előfordul, hogy sebezhető weboldalakon keresztül, rejtett módon települnek az eszközre. Léteznek továbbá olyan hamis kémirtó programok is, amelyek valójában maguk is spyware-ek. Tágabb értelemben – az Anti-Spyware Coalition szerint – a kémprogramok közé so-

rolhatók a kéretlen megfigyelő és adatgyűjtő szoftverek, például egyes sütik (cookie-k), kereskedelmi keylogger-ek és más nyomkövető technológiák is.

https://www.eset.com/hu/termektamogatas/veszelyek/

126. **SQL Injection:** Az SQL Injection során a támadó vagy a feljogosított etikus hacker olyan kódot, karakterláncot ad meg az online beviteli felületen (keresés, regisztrációs/bejelentkezési űrlap, stb.), ami a szerveroldali feldolgozás során lehetőséget biztosít (akár módosítását) az adatbázis manipulálására, amelyhez nem lenne hozzáférése.

https://makay.net/kiberbiztonsagi-fogalomtar

127. **Szintetikus identitáslopás:** Ez a módszer nem csupán a személyes adatok ellopását foglalja magában, hanem egy fiktív digitális személyiség felépítését is. Az adatokat különböző forrásokból gyűjtik össze, mint például nemzeti azonosítók, születési dátumok, email címek, telefonszámok és lakcímek. Az így létrehozott szintetikus identitás első ránézésre valódinak tűnhet, mivel valós adatokból épül fel. A csalók ezt követően életre keltik a személyiséget a digitális térben, ahol valós emberekkel megegyező viselkedést mutatnak, aktívak a közösségi médiában, e-kereskedelmi felületeken, fórumokon és online közösségekben. Ezáltal hiteles, valósnak tűnő személy látszatát keltik.

https://www.fintechradar.hu/fintech/0603/novekvo-fenyegetest-jelent-a-szintetikus-szemelyiseglopas/

128. **Time Bomb:** Az időzített bomba egy olyan rosszindulatú kódrészlet, amelyet szoftverbe ágyaznak, és kizárólag egy előre meghatározott időpontban aktiválódik. Ezzel szemben más típusú kártevők működésbe lépéséhez valamilyen felhasználói tevékenység vagy feltétel teljesülése szükséges. Az időzített bomba azonban az idő múlására épít: addig észrevétlenül rejtve marad, míg el nem érkezik az aktiválás ideje. Ez a tulajdonsága különösen alattomossá teszi. Gyakran szándékosan időzítik fontos eseményekhez vagy dátumokhoz, hogy a lehető legnagyobb zavart vagy kárt okozzák – például adatvesztést, rendszerek leállását vagy más jogosulatlan tevékenységeket idézve elő.

https://www.twingate.com/blog/glossary/time-bomb

129. **Titkosítás:** A titkosítás olyan technikai módszerekre utal, amelyek biztosítják az adatokat és a rendszereket, megnehezítve az információkhoz való hozzáférést, illetve a hálózatok és tranzakciók megzavarását. A modern kriptográfiában a titkosításhoz egy titkosítási algoritmus vagy rejtjelező használata szükséges, hogy az olvasható egyszerű szöveget rejtjelezett szö-

veggé (olvashatatlan titkosított adat) lehessen átalakítani. A rejtjelezett szöveget csak azok tudják visszafejteni egyszerű szöveggé, akiknek hozzáférést biztosítottak az adatokhoz.

https://bitmarkets.academy/hu/crypto-for-advanced/what-are-encryption-and-decryption

130. **Trojan Horse:** A „trójai" – melynek történetét a görög regékből ismerhetjük – egy olyan program, amely valami mást csinál, mint amit magáról eredetileg állít. Ez a más nem minden esetben okvetlenül romboló vagy káros, de sok esetben igen: fájlokat törölnek, felülírják a merevlemezt, vagy távoli hozzáférést biztosítanak a rendszerhez a támadónak. A klasszikus trójai általában tartalmaz egy billentyűleütés naplózót (keylogger) is, amelyet készítői játéknak vagy valamilyen hasznos segédprogramnak álcáznak. Az ilyen trójaiakat sokféle céllal alkalmazhatják: rejtett távoli elérést (backdoor) szeretnének biztosítani egy adott számítógéphez, ellenőrizni kívánják a billentyűleütéseket, valamint jelszavak lopására specializálódnak (a legtöbb kémprogram ez utóbbi kategóriába tartozik).

https://www.eset.com/hu/termektamogatas/veszelyek/

131. **Tűzfal:** lásd firewall

132. **Vírus:** A vírus egy olyan rosszindulatú program, amely képes reprodukálni saját magát – akár megegyező, akár módosított formában – egy másik végrehajtható kódba. A vírusok többféle gazdaprogramot (host) használhatnak, a legismertebbek: végrehajtható állományok (számítógépes programok), betöltő (boot) szektorok (amelyek megadják a számítógépnek, hol találja a rendszerindítási folyamathoz szükséges adatokat), szkript kódok (olyan szkript nyelvek, mint például a Windows Scripting, vagy a Visual Basic), dokumentumokba ágyazott makró utasítások (ezek veszítettek a jelentőségükből, amióta a Microsoft Windows nem hajtja végre őket alapértelmezésben). Amikor egy vírus beágyazza saját másolatát egy másik végrehajtható kódba, ezzel biztosítja azt, hogy a vírus kódja is lefuthasson amikor az eredeti program fut, és úgy terjed, hogy futás közben mindig újabb, tiszta és megfertőzhető programok után kutat. Néhány vírus felülírja az eredeti programkódot – tönkre téve ezzel az eredeti programot –, de a legtöbb esetben úgy fűzik hozzá magukat, hogy mind a gazdaprogram, mind a víruskód életképes maradjon. A kódolástól függően a vírusok sokféle fájltípuson keresztül képesek terjedni a rendszerben, hálózati megosztásokon keresztül is, dokumentum állományokban, de akár lemezek rendszerbetöltő (boot) szektoraiban is. Bár néhány vírus e-mail üzenet útján is terjed, az elektronikus levelezésben sze-

replő kártevők legnagyobb része féreg. A vírusnak elegendő, ha a sokszorosításáról megfelelően gondoskodik, nem szükséges, hogy büntető rutint is tartalmazzon vagy, hogy széles körben elterjedjen.

https://www.eset.com/hu/termektamogatas/veszelyek/

133. **Vishing:** A vishing (az angol „voice" és „phishing", vagyis hang és adathalászat szavak kombinációja) olyan telefonos csalás, amelynél a támadó megpróbálja személyes, pénzügyi vagy biztonsági információi megosztására vagy pénz átutalására rávenni az áldozatokat, akik általában banki ügyfelek. A vishing tipikus formája, amikor a csaló az adathalász hívás során megpróbálja elhitetni a felhasználóval, hogy ténylegesen egy banki alkalmazottal beszél, és egy pénzügyi tranzakció során fellépett hiba vagy csalásgyanú miatt telefonál.

https://kiberpajzs.hu/csalastipusok/telefonos/vishing/

134. **Visszahívásos telefonos csalás:** lásd wangiri

135. **Wallet recovery:** A wallet recovery phrase (helyreállító kulcsmondat) egy biztonsági mechanizmus, amelyet a kriptovalutás pénztárcák (wallet) használatakor hoznak létre. Ez egy előre meghatározott, többnyire 12-24 szóból álló sorozat, amely lehetővé teszi a felhasználó számára a pénztárca helyreállítását abban az esetben, ha elveszíti a hozzáférést vagy elfelejti a jelszót. A helyreállító kulcsmondat birtokában bárki képes újra hozzáférni a pénztárcához, tehát kiemelten fontos a kód biztonságos tárolása. A kulcsmondat elvesztése vagy nyilvánosságra kerülése a kriptovalutákhoz való hozzáférés teljes elvesztését eredményezheti.

https://nki.gov.hu/it-biztonsag/tudastar/mi-az-a-wallet-recovery-phrase/

136. **Wangiri:** A Japánból származó wangiri a mobiltelefonoknak köszönhetően vált az egyik legelterjedtebb csalástípussá. Lényege, hogy a csalók tömegesen generált számítógépes hívások részeként ismeretlen, általában külföldi – jellemzően 2-essel kezdődő országhívószámmal rendelkező afrikai, vagy 5-össel kezdődő országhívószámmal rendelkező közép-amerikai – számról hívják fel áldozataikat, ám a hívást egy-két csöngés után bontják a visszahívás reményében. A visszahívás azonban a belföldinél jóval magasabb tarifán zajlik, és a csalás akkor is eredményes, ha a hívás látszólag sikertelen: például folyamatosan kicsöng, vagy épp nem csöng ki, hanem vonalszakadást vagy folyamatosan foglaltat jelez.

https://kiberpajzs.hu/csalastipusok/telefonos/wangiri/

137. **Wardriving:** A wardriving olyan tevékenység, amikor valaki mozgó járműből – például autóból, bicikliről vagy akár gyalogosan – WiFi hálózatokat keres okoseszközök és ingyenesen elérhető szoftverek segítségével. Célja jellemzően a sebezhető vagy nyitott hálózatok azonosítása, amelyeket később illetéktelenül felhasználhatnak, de etikus hackerek is alkalmazhatják biztonsági hibák feltárására. A kifejezés a WarGames (1983) című filmből ered, a jelenlegi értelmében Pete Shipley biztonsági kutató vezette be 2000-ben. A wardriving során gyűjtött adatokat gyakran térképeken is megjelenítik (ún. access point mapping). Az elmúlt években a modern titkosítási technológiák elterjedése miatt csökkent a jelentősége.

    https://www.kaspersky.com/resource-center/definitions/what-is-wardriving

138. **Watering hole támadás:** A water hole támadás során a támadó egy biztonsági sebezhetőséget használ fel ahhoz, hogy rosszindulatú kódot adjon hozzá egy legitim weboldalhoz, hogy amikor a felhasználók ellátogatnak a weboldalra, a kód automatikusan megfertőzze a számítógépet vagy mobil eszközt. A watering hole támadás egyik formája, amelyben a támadók azonosítják és kihasználják azokat a biztonsági réseket, amelyeket rendszeresen látogatott weboldalak nyitva hagynak. A támadók a watering hole támadásokat rendszerint olyan oldalakon hajtják végre, amelyek sok látogatót vonzanak, és akiknek hozzáférésük van olyan információkhoz, amelyeket a támadók meg akarnak szerezni. Például egy biztonsági szakember felfedezte, hogy a támadók egy portugál nyelvű stratégiai tanácsadó weboldalt használtak arra, hogy az európai és dél-amerikai látogatókat fertőzzék meg kémkedő kártevőkkel. A watering hole támadások általában csendesek és láthatatlanok, és gyakran csak akkor észlelhetők, amikor már kárt okoztak.

    https://www.zts.hu/blog/hanyfelekeppen-tamadhatjak-meg-a-cegunk-szervereit-2-resz/

139. **White Hat Hacker:** A white hat hacker, más néven etikus hacker, olyan informatikai szakember, aki engedéllyel és jogszerűen vizsgálja a rendszerek, szoftverek vagy hálózatok biztonsági hibáit annak érdekében, hogy megelőzze a rosszindulatú támadásokat. Csak olyan rendszereken végez teszteket, amelyek vizsgálatára felhatalmazást kapott, gyakran hibavadász programok keretében, amelyek jutalmazzák a sebezhetőségek felelősségteljes felfedését.

    https://www.techtarget.com/searchsecurity/definition/white-hat

140. **Wildcard tanúsítvány**: A wildcard tanúsítvány tipikusan olyan szerveroldali biztonsági tanúsítvány, amelynek „Subject Alternative Name" mező-

jében nemcsak az elsődleges domain www aldomaines változata szerepel, hanem a * karakterhelyettesítő segítségével számos egyéb domainvariáció is (pl.: *.makay.net). Ez a tanúsítványkibocsátási és -igénylési politika biztonsági kockázat miatt kerülendő, ugyanis egyetlen (szintén az adott tanúsítványt használó) kiszolgáló biztonsági incidense maga után vonhatja a többi kiszolgáló kommunikációjának jogosulatlan hozzáférését és sérülését is.

https://makay.net/kiberbiztonsagi-fogalomtar

141. **Worm:** A számítógépes terminológia szerint a férgek a vírusok egy részhalmaza, és bár megvan a képességük önmaguk sokszorosítására, a fertőzéshez hordozó gazdaprogramot (host file) nem igényelnek. Ahogy a vírusok programokat fertőznek meg, úgy a férgek rendszereket árasztanak el. Az ilyen férgek rendkívül gyorsan képesek sebezhetőséget tartalmazó hálózatokon terjedni, és ehhez még a felhasználó beavatkozása sem szükséges. A féreg általában fertőzött e-mail üzenetekkel terjed, amelyekben valamilyen számítógépes sebezhetőséget kihasználó kód található, és maga a levél valamilyen csábító, érdekes üzenetet közvetít. A férgeket általában sokkal könnyebb eltávolítani, mint a vírusokat, mert nem fertőznek fájlokat, egyszerűen törölhetőek. A féreg rendszerint gondoskodik arról, hogy minden rendszerindításkor lefuthasson, ezt az Indító Pult (Startup Folder) vagy a rendszerleíró adatbázis (Registry) bejegyzések manipulálásával éri el.

https://www.eset.com/hu/termektamogatas/veszelyek/

142. **Zero Trust:** A „Zéró bizalom elv" azt a biztonsági szemléletmódot jelenti, mely szerint feltételezzük, hogy rendszereink jogosulatlan hozzáférése vagy biztonsági incidense elkerülhetetlen – mi több, valószínűleg már meg is történt –, ennélfogva egyetlen rendszerelem vagy hozzáférési kísérlet sem tekinthető megbízhatónak. A modell középpontjában az adatok, rendszerelemek, alkalmazások és szolgáltatások (DAAS) hozzáférés védelme áll, amelyet szigorú ellenőrzéssel, rendszeres újraértékeléssel, valamint a hálózati fenyegetések folyamatos monitorozásával kell biztosítani. Fontos tisztában lennünk azzal, hogy ennek bevezetése egy rendkívül idő- és erőforrásigényes folyamat, különösen, ha egy már meglévő IT struktúrát szeretnénk átalakítani.

https://nki.gov.hu/it-biztonsag/hirek/nsa-utmutato-a-zero-bizalmi-biztonsagi-modell-megvalositasahoz/

143. **Zombihálózat:** lásd botnet

144. **Zsarolóprogram:** lásd ransomware

ÖSSZEFOGLALÁS

A kibervédelmi fogalomtár az elkészítésekor, azaz jelen tanulmány közreadásakor 111 olyan kibertéri alapfogalmat és 33 magyar fogalomnak az angol változatra való átirányítását tartalmazza, amely szükséges ahhoz, hogy a kibervédelem, a kiberbiztonság iránt érdeklődők és az ezen a területen dolgozók ebben az új térben el tudjanak igazodni.

Ez a fogalomtár akkor lesz időtálló, ha ezen első, nyomtatott változat melletti „e" változat – várhatóan a www.kiberpajzs.hu oldalon – folyamatosan bővülni és aktualizálódni fog. Ebben számítunk a kiberkérdésekkel foglalkozó szakemberek támogatására.

HIVATKOZÁSOK

Binance Academy https://academy.binance.com/en/.
Avirus https://avirus.hu/.
BitMarkets Academy https://bitmarkets.academy/.
Cyberpedia – ReasonLabs https://cyberpedia.reasonlabs.com/.
DotCom Magazine https://dotcommagazine.com/.
Wikipédia https://www.wikipedia.org/.
OPSWAT Magyarország https://hungarian.opswat.com/.
KiberPajzs https://kiberpajzs.hu/.
Lexiq https://lexiq.hu/.
Makay.net https://makay.net/.
Mpost.io https://mpost.io/.
Nemzeti Kibervédelmi Intézet https://nki.gov.hu/.
Perception Point https://perception-point.io/.
Sealog https://sealog.hu/.
Webshop Automatizálás https://webshopautomatizalas.hu/.
BeyondTrust https://www.beyondtrust.com/.
Biztonságosinternet.hu https://www.biztonsagosinternet.hu/.
Cobalt.io https://www.cobalt.io/.
Európai Unió Tanácsa https://www.consilium.europa.eu/.
CrowdStrike https://www.crowdstrike.com/en-us/.
EBSCO https://www.ebsco.com/.
FintechRadar https://www.fintechradar.hu/.
Fortinet https://www.fortinet.com/.
FraudSmart https://www.fraudsmart.ie/.
Group-IB https://www.group-ib.com/.
Infobip https://www.infobip.com/.

ITU Online https://www.ituonline.com/.
Kaspersky Magyarország https://hu.kaspersky.com/.
Ludovika Egyetem https://www.ludovika.hu/.
Malwarebytes https://www.malwarebytes.com/.
Mcafee https://www.mcafee.com/.
Microsoft Magyarország https://www.microsoft.com/hu-hu/.
Magyar Nemzeti Bank https://www.mnb.hu/web/fooldal.
NinjaOne https://www.ninjaone.com/.
Palo Alto Networks https://www.paloaltonetworks.com/.
SAP Magyarország https://www.sap.com/hungary/index.html.
TechTarget https://www.techtarget.com/.
TrendMicro https://www.trendmicro.com/en_gb/business.html.
Twingate https://www.twingate.com/.
UNICEF https://www.unicef.org/.
Unite.AI https://www.unite.ai/.
UpGuard https://www.upguard.com/.
ZTS Hungary https://www.zts.hu/.