HADMÉRNÖK
VÉDELEMINFORMATIKA

16. évfolyam (2021) 2. szám 169–185.
DOI: 10.32567/hm.2021.2.12

Jéri Tamás[1]

Az elektronikus levelezés és a kiberbiztonság összefüggései

Relationships between Electronic Mail and Cybersecurity

Az elektronikus levelezés kiemelkedő szerepet játszik napjaink internetes informatikai szolgáltatásai között, hisz a legrégebbi internetes kommunikációs platform, amelynek népszerűsége töretlen. Egy természetesnek vehető alapszolgáltatás, ugyanakkor melegágya az informatikai rendszerek ellen indított sikeres támadásoknak, hisz a kiberbűnözők továbbító eszközként is használják, amellyel számtalan rosszindulatú tevékenységet lehet kezdeményezni. A cikk az elektronikus levelezés és a kiberbiztonság közötti összefüggést vizsgálja.

Kulcsszavak: **e-mail, biztonság, kiberbiztonság**

E-mail plays a prominent role in today's Internet IT Services, as it is the oldest Internet communication platform with unbroken popularity. A basic service that can be taken for granted, but it is also a hotbed of successful attacks against IT systems, as it is also used by cybercriminals as a transmission tool to initiate countless malicious activities. This article examines the relationship between e-mail and cybersecurity.

Keywords: **e-mail, security, cybersecurity**

1. Bevezetés

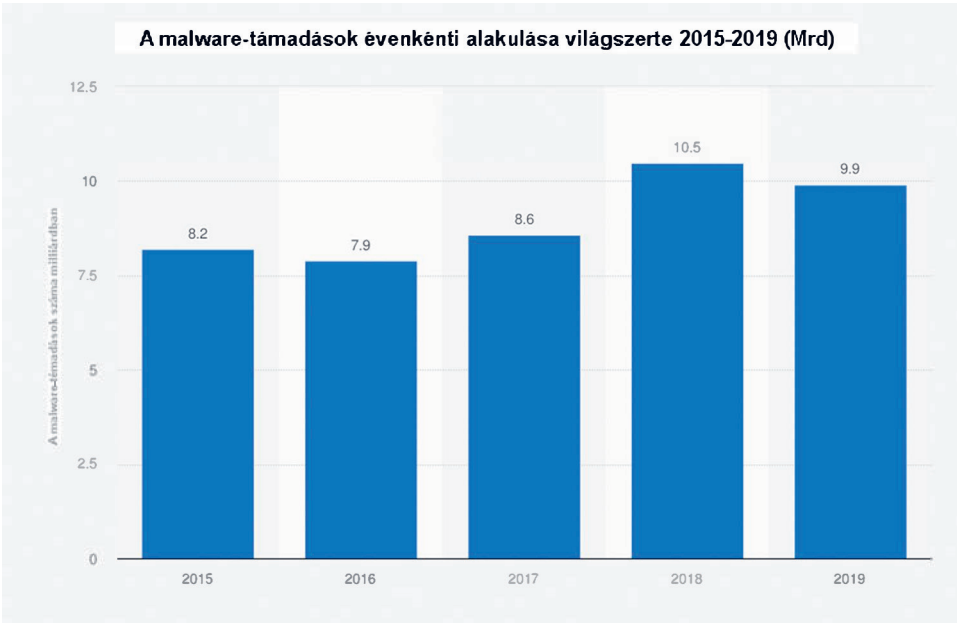
Az informatikai eszközökkel végzett rosszindulatú tevékenység valamely – általában kezdeti – fázisában szerepet kap az elektronikus levelezés, ezért is tartják az e-mailt a szakértők az első számú támadási eszközként nyilván.

„A kibertérben végrehajtott rosszindulatú tevékenységnek kulcsszereplői a »hétköznapi felhasználók«, akik célpontjai, vagy eszközei lehetnek a bűnözőknek. Egyrészt meg lehet őket károsítani, másrészt hasznos információkat lehet tőlük kicsalni a további

[1] Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, doktori hallgató, e-mail: jeri.tamas@gmail.com

célpontok eléréséhez, harmadrészt pedig információs eszközeik erőforrásait fel lehet használni összehangolt kibertámadások végrehajtásához. Ezen műveletekhez – első lépésként – elengedhetetlen a kapcsolatteremtés az emberekkel, amelynek legkézenfekvőbb eszköze az elektronikus levél, hisz lehetővé teszi a küldő részéről az anonimitást, tartalmába bármi beágyazható, ami a megtévesztéshez, az információ kinyeréséhez, vagy az informatikai eszköz hatalomba vételéhez szükséges."[2]

Az 1. ábrán látható adatok szerint, a malware[3]-támadások száma ötéves periódusban emelkedik, amelyben feltételezésem szerint meghatározó szerepe van az elektronikus levelezést biztosító levelezőrendszereknek. Tanulmányom célja, hogy a fertőződés folyamatának és a levelezőrendszer működésének vizsgálatával választ találjak a malware-támadások számszaki emelkedésének okára, továbbá javaslatot tegyek a fertőzések lehetséges csökkentésére.



1. ábra

A malware-támadások évenkénti alakulása 2015-től 2019-ig

Forrás: a szerző szerkesztése a Statista[4] adatai alapján

[2] Jéri Tamás: *A Kritikus Internetes Szolgáltatások biztonsági kérdései a védelmi szférában.* Doktori (PhD-) értekezés tervezet. Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, 2020.

[3] *Malicious software* – rosszindulatú szoftver.

[4] Statista: *Annual number of malware attacks worldwide from 2015 to 2019.* 2021.

2. Kutatási módszerek

Az elektronikus levelezés és a kiberbiztonság összefüggéseinek vizsgálatához át kell tekinteni a megfertőződés folyamatát, az elektronikus levelezés működését és a releváns tényszerű adatokat.

3. Az IT[5]-eszközök megfertőzésének folyamata

Teljesen leegyszerűsítve, egy informatikai eszköz megfertőzéséhez a kártékony kódnak a céleszköz valamely ideiglenes vagy tartós tárhelyére érkeznie, majd aktiválódnia kell. Az utóbbi kulcsa a folyamatnak, hisz a nélkül az érintett eszköz csak a kártékony kód hordozója, de nem fertőződött.

Figyelembe véve, hogy az IT-eszközök a telepítésüket követően zárt, homogén rendszernek tekinthetők, kijelenthető, hogy a kártékony kód tárhelyre érkezéséhez valamilyen emberi beavatkozás szükséges. Ez a beavatkozás jelentheti a zárt rendszer hálózati nyitását (megosztását), amely egy távoli – valószínűleg már fertőzött – eszköznek lehetőséget biztosít a kártékony kód bejuttatására, vagy jelentheti a kártékony kód közvetlen ember általi tárhelyre juttatását.

A kártékony kód aktiválásához szintén emberi beavatkozás szükséges, amely jelentheti az operációs rendszer általi direkt végrehajtást (futtatást), vagy jelentheti az operációs rendszer általi végrehajtás ütemezését. Az ütemezéskor egy későbbi időpontban, például a rendszer újraindítását követően, automatikusan aktiválódik a kártékony kód, amely folyamat többek között magában foglalja a malware-támadást is.

A rosszindulatú tevékenységet folytatók szemszögéből nézve, cél a minél nagyobb számú fertőzés elérése. A fertőzés folyamatából kiindulva, ehhez a potenciális áldozat IT-eszközére el kell juttatni a kártékony kódot, és az áldozatot rá kell bírni annak aktiválására. Nyilvánvaló, hogy a leendő áldozatokat valahogy be kell csapni, rá kell vezetni a fertőzés folyamatára, hisz önszántából azt senki sem fogja végrehajtani. A kártékony kód eljuttatásának egyik módszere a direkt, célzott átadás valamely fizikai adattároló eszközön (például pendrive-on), vagy az interneten mint hálózati összeköttetésen keresztül. A kártékony kód eljuttatásának másik hagyományos módszere, hogy a kódot elhelyezik az internet valamely állandó rendelkezésre álló szerverére, és a potenciális áldozatot rábírják a rosszindulatú tevékenységet folytató kód letöltésére. Mindkét módszer esetén a rosszindulatú kódot valamilyen megtévesztéssel álcázzák, hogy a hiszékeny áldozat azt önszántából juttassa el IT-eszközére, majd aktiválja.

4. Az elektronikus levelezés működésének vizsgálata a fertőzés folyamatának aspektusából

„Az e-levél rendszerek két alrendszerből állnak, a felhasználói ügynökből (user agent), amely lehetővé teszi a felhasználók számára az üzenetek olvasását és küldését, valamint

[5] *Information Technology* – információtechnológia.

az üzenettovábbító ügynökből (message transfer agent), ami a leveleket eljuttatja a feladótól a címzettig."[6] Az üzenettovábbító ügynök ismertebb nevén levelezőszerver.

„A levelezőszervernek az internet valamely hálózati pontjaként kell működnie, egyébként alkalmatlan lenne a világhálón elektronikus levelek fogadására, vagy küldésére.

Az elektronikus levelezés fertőzési tevékenysége a szolgáltatás rosszindulatú felhasználásával vagy kihasználásával valósul meg, amely tevékenységnek azt tekintem, amikor a levelezési szolgáltatás rendeltetésszerű használatával, a rendelkezésre álló, üzemszerű funkciók alkalmazásával rosszindulatú tevékenységet folytat a szolgáltatást igénybe vevő személy.

Az elektronikus levelezési szolgáltatással szemben minimumelvárás:

- az állandó rendelkezésre állás;
- a levelekhez történő korlátlan hozzáférés;
- az érkező levelek fogadása;
- a küldésre szánt levelek célba juttatása.

Ezeknek a minimumelvárásoknak a teljesítése megfelelő táptalajt ad a rosszindulatú felhasználás vagy kihasználás folytatásához, hisz a levelezőrendszer mint eszköz rendelkezésre áll.

A levelezőszerver működésében két fontos terület elkülönül. Az input mint bemeneti egység, amely az érkező levelek fogadását, az output mint kimeneti egység pedig a küldendő levelek kibocsátását végzi. A szerver inputján keresztül fogadja az érkező elektronikus leveleket és az e-mail postafiók rendelkezésre állása esetén elhelyezi azt a tárterületen, egyébként outputján keresztül továbbítja a címzett domainje szerinti levelezőszervernek.

4.1. Nyitott biztonsági rés

A levelezőszerver egyike azon kiszolgáló programoknak, amelyek segítségével rendeltetésszerűen át lehet mozgatni adatokat egyik IT-eszközről a másikra. A nyitott biztonsági rés némileg rendhagyó állítást már a definiált működés is részben alátámasztja:

„Feladatuk, hogy a rendszeren keresztül automatikusan eljuttassák az e-leveleket a feladótól a címzettig az SMTP (*simple mail transfer protocol* — egyszerű levéltovábbító protokoll) segítségével. Ez az üzenettovábbítási lépés."[7]

Az automatizmus azt jelenti, hogy a feladótól a címzettig feltétel nélkül eljuthatnak az elektronikus levelek. A kiszolgálás és szolgáltatás közötti különbség éppen a feltételhez kötöttségben mutatkozik meg, amelyből látszik, hogy a levelezőszerver inkább az első kategóriába tartozik.

Az elektronikus levelezési címmel rendelkező felhasználók, azaz a postafiókok tulajdonosai lehetőséget adnak levelek fogadására és elvárják, hogy a részükre küldött e-maileket megkapják. Ezen – némileg – jogos elvárás teljesítése érdekében,

[6] Andrew S. Tanenbaum – David J. Wetherall: *Számítógép-hálózatok.* Budapest, Panem, 2013.
[7] Tanenbaum–Wetherall (2013): i. m. 3.

a levelezőszervernek feltétel nélküli, levélfogadásra alkalmas kiszolgálóként kell működnie. Az üzenet kézbesítésekor a címzett a levelet postafiókjába megkapja, azaz a levelezőszerver tárhelyére az adattartalom fizikailag elhelyeződik. Leegyszerűsítve, a levél küldője legálisan, egyszerűen – az SMTP-protokolljával – képes adatokat egy adott szerverre eljuttatni, mert a levelezőszerver működtetése alapértelmezésben levelek fogadásának feltétel nélküli biztosítása.

Ezen mechanizmust a rosszindulatú tevékenységet folytatók képesek az ezirányú szándékuk kivitelezésére felhasználni, hisz az elektronikus levélcímek birtokában oda kártékony kódokat, vagy a saját céljaik elérését segítő megtévesztő leveleket tudnak rövid idő alatt is, kis befektetéssel eljuttatni. Az informatikai rendszerekkel szembeni rosszindulatú tevékenységnek egyik sarokpontja az adott célrendszer biztonsági réseinek feltárása, ezért az elektronikus levelezők ezen alapértelmezett biztonsági rése kézenfekvő megoldás a támadások előkészítésére.

Természetesen ezt a „biztonsági rést" nem célszerű – teljesen – nyitva hagyni, kontrolljára számos lehetőség mutatkozik, amelyek alkalmazása a levelezőrendszert működtető hatásköre.

Az e-mail-címmel rendelkező felhasználók másik jogos elvárása, hogy képesek legyenek elektronikus levelek küldésére. Teljesen helyénvaló ez a folyamat mindaddig, amíg a továbbítás nem kéretlen, fertőzött levelek küldésére szolgál. E rosszindulatú tevékenységet folytatók célpontjai lehetnek azok a hétköznapi felhasználók, akiknek jogosultságait felhasználva, a helyükbe lépve fertőzött levelek tucatját küldik ki, gyakran az érintett felhasználó tudta nélkül.

Látható, hogy egy levelezőszerver célpontként és eszközként egyaránt szolgálhat, amellyel szemben védekezni szükséges, ellenkező esetben az elektronikus levelezési szolgáltatás rövid időn belül ellehetetlenül, elbukik.

4.2. Rosszindulatú felhasználás

Az elektronikus levelezés rosszindulatú felhasználása, amikor a levelezőszerver bemenetére malware vagy spam[8] érkezik, amelynek célpontja valamely elektronikus postafiók. Önmagában tehát a rosszindulatú tartalommal rendelkező levél célba juttatását jelenti, amely csatolmányként programtípusú vagy megtévesztő, szöveg alapú malware-t tartalmazhat.

Figyelembe véve, hogy a postafiók-tulajdonosok leveleiket kliensalkalmazással kezelik, a malware-t küldők célja lehet: a kliensgép – rosszindulatú programkód futtatásával történő – teljes vagy részleges hatalomba vétele; megtévesztéssel vagy programkóddal információ kinyerése.

A levelek szöveges részében megtévesztő tartalommal – általában banki – adatok megadására, fertőzött webhely meglátogatására, vagy egyéb cselekmény végrehajtására próbálják rábírni a levél fogadóját.

[8] *Spam* – kéretlen levél.

A teljesség igénye nélkül e-mailben az alábbi malware-ek küldhetők:[9]

- vírusok;
- programférgek;
- ransomware-ek;
- trójai programok;
- backdoor programok;
- dropperek;
- spyware-ek;
- keyloggerek;
- adware-ek;
- scareware-ek.

A rosszindulatú felhasználás elsődlegesen akkor eredményes, ha a levél belépve a levelezőszerverre, eljut a címzett postafiókjába, másodlagosan pedig akkor, ha a postafiók tulajdonosát sikerül megtévesztenie, vagy a rosszindulatú kód futtatására rábírnia. Ezen tevékenység folytatásához bármilyen létező és e-mail küldésére alkalmas postafiók használható, a kijuttatás lehet manuális vagy programozott. Sok esetben önmagában a rosszindulatú felhasználás, további e-mail-címek megszerzésére irányul.

A levelezőrendszer tehát minden, a fertőzés megvalósításához szükséges elemet tartalmazza. Az e-mail-cím birtokában bárki közvetlenül küldhet rosszindulatú kódot, hisz a levélhez csatolmányként az könnyedén társítható, továbbá az aktiváláshoz még a felhasználói beavatkozás szükségessége is megoldott. A levél csatolmányának olvasásához interakció társítható, ezáltal a fertőző kód rögtön aktiválható és a fertőzés könnyedén megvalósítható.

A direkt küldés mellett a kártékony kód letöltésére irányuló rávezetés is lehetséges, hisz a levél tartalmába ágyazott megtévesztő hivatkozással a hiszékeny páciens rábírható az internet valamely szerverének megszólítására, az azon tárolt rosszindulatú kód letöltésére és annak lefuttatására, ezáltal a kód aktiválására és a fertőzés megvalósítására.

4.3. Levelezési szolgáltatás kihasználása

A levelezési szolgáltatás kihasználásának tekintem, amikor adott levelezőszerver kimenetét – leginkább rosszindulatú felhasználás érdekében – veszi igénybe a tevékenységet folytató. A kiszemelt levelezőszerver erőforrásait a fertőzött levelek – elsősorban a világháló irányába történő – kiküldésével használja ki, célja adott időintervallum alatt minél nagyobb számú levél kijuttatása. Általában valamely küldésre jogosult kliens azonosítójának és jelszavának együttes megszerzésével és felhasználásával, az azonosító eredeti tulajdonosának nevében eljárva valósul meg.

„Miután a küldő levéltovábbító ügynök megkapta a levelet a felhasználói ügynöktől, kézbesíti azt a fogadó levéltovábbító ügynöknek az SMTP segítségével.

[9] Kovács László: *A kibertér védelme.* Budapest, Dialóg Campus, 2018.

A megfelelő levelezőszerverrel való kapcsolatfelvétel érdekében meg kell kérdezni a DNS[10]-t.

A válasz egy rendezett lista lesz, amely egy vagy több levelezőszerver nevét és IP[11]-címét tartalmazza.

A küldő levéltovábbító ügynök ezután létrehoz egy TCP[12]-összeköttetést a 25-ös porton lévő levelezőszerver IP-címére, hogy elérje a fogadó levéltovábbító ügynököt, és az SMTP-t használva továbbítja az üzenetet."[13]

A levelezőszerver tehát a küldendő leveleket az általa kezelt fiókok esetében saját hatáskörön belül kézbesíti, egyébként DNS alapján megkeresi az érintett másik levelezőszervert, és az azzal történt kapcsolatfelvételt követően, SMTP-protokoll segítségével, kézbesítés céljából továbbítja azokat. A rosszindulatú kihasználás ezt a továbbító funkciót célozza meg, és kellemetlen következménye, hogy a kéretlen vagy fertőzött levelek küldéséért – a küldő személytől függetlenül – a szerver felelős.

A levelezőszerver SMTP-alapú megszólítása és levél küldése egyaránt lehetséges programozottan automatikusan vagy felhasználói beavatkozáshoz kötötten, ugyanakkor az adott idő alatt kiküldött levelek számának maximalizálása és egyben a szerver kihasználására az automatizált levélküldés az optimális. A küldőprogram készülhet bármilyen program- vagy szkriptnyelven, amely ismeri az SMTP-protokollt és egyaránt lefuthat a levelezőszerveren, vagy az ahhoz kapcsolódó klienseszközön. Magán a levelezőszerveren, annak tesztelése és karbantartása miatt alapból rendelkezésre állnak azok a programok, amelyekkel levelet lehet – akár programozottan is – küldeni, ezért a levelezőszerver sikeres támadásával és operációs rendszerének hatalomba vagy használatbavételével a levelezés kihasználása is megvalósítható.

A klienseszközről érkező levéltovábbító kérések levelezőszerver általi végrehajtását angolul *SMTP Relay*-nek nevezik. A levelezőszerveren meg kell határozni, hogy a Relay-funkciót milyen feltételek teljesülése esetén hajtsa végre. Beállítható, hogy mely hálózati címekről érkező kéréseket, milyen felhasználói azonosítás mellett továbbítsa, amely azonosítási metódust a levelezőprogramokban is le kell követni. A kliensen meghatározandó a továbbító SMTP-szerver címe, és amennyiben van felhasználói azonosítás, úgy azt – ami jellemzően felhasználónév és jelszó – is be kell állítani. Webes levelezőkliens esetén a levelezőszerverhez illesztés a weboldal működtetőjének, klienseszközön futó levelezőprogramban az alkalmazás felhasználójának a feladata.

4.3.1. Open relay

A levelezőszerver azon beállítását és működését jelenti, amikor a vele SMTP-kapcsolatba lépő kliens leveleit felhasználói azonosítás nélkül továbbítja a levél címzettjének. Ez a beállítás általában figyelmetlenség következménye, vagy ritkán szándékos ezirányú konfigurálás. Tekintettel arra, hogy az „open relay" szerverekkel korlátlan lehetőség

[10] *Domain name server* – névszerver.
[11] *Internet protocol* – internetprotokoll.
[12] *Transmission control protocol* – átvitelvezérlő protokoll.
[13] Tanenbaum–Wetherall (2013): i. m. 3.

van – akár fertőzött – levelek anonim küldésére, a rosszindulatú tevékenységet folytatók előszeretettel keresik e levélküldő eszközöket az interneten.

4.3.2. Auth relay

„A levelezőszerver a vele kapcsolatba lépő kliens leveleit feltételhez, felhasználónév és jelszó párosához kötötten továbbítja. A Relayhez használt azonosító és jelszó párosa beállításától függően bármi lehet, de kényelmi okból leggyakrabban magát az e-mail-címet és a hozzá beállított jelszót alkalmazzák az üzemeltetők.

A levelezőszerver *Auth relayen* keresztül történő kihasználása valamely, továbbításhoz alkalmazott azonosító és jelszó ismeretében lehetséges, amennyiben azt a rosszindulatú tevékenységet folytató megszerzi, majd az eredeti tulajdonosnak álcázva magát fertőzött leveleket küld ki. Az Auth relayre feljogosító azonosító és jelszó páros megszerezhető a levelezőszerverről, a levelezőprogramot futtató kliensről, illetve az azonosítási folyamat közben a levelezőszerver és kliens között a hálózatról. A levelezőszerverről és a levelezőprogramot futtató eszközökről azok támadhatósága esetén nyerhetők ki az információk.

A továbbító funkcióval vagy a levelezőszerverről direktben egyaránt megvalósítható a kihasználás. Amennyiben a levelezőszerver és a levelezőprogram közötti kommunikáció titkosítatlan, úgy az azonosítási mechanizmustól függetlenül az elküldött adatok a hálózaton lehallgathatók, továbbá a felhasználónév és jelszó párosa kikövetkeztethető, amely birtokában a kihasználás létrejöhet. A klienseszközön futtatott – akár kártékony – program segítségével, a levelezőalkalmazás felhasználói beavatkozás nélküli, programozott e-mail küldésére bírható rá.

A titkosítatlan csatornán használt webmail-alkalmazást a hálózaton szintén le lehet hallgatni, megszerezve a postafiókhoz hozzáférést jelentő felhasználónevet és jelszót. Figyelembe véve, hogy a webmail-alkalmazás és a levelezőszerver közötti auth relay előre konfiguráltan biztosított, a hozzáférést megszerzőnek megnyílik a lehetősége a levelezőszerver kihasználására.

A levelezőszerver kihasználása lehet közvetlen kapcsolódással megvalósított online kihasználás, vagy a klienseszköz megfertőzésével és azon kártékony program futtatásával megvalósítva offline kihasználás."[14]

4.4. Statisztikai kitekintés

Az 1. táblázatban szereplő adatok alapján látható, hogy az e-mail-felhasználók száma a küldött és fogadott levelek számával együtt dinamikusan növekszik.

A Purplesec[15] kiberbiztonsági cég által közölt 2020-as statisztikai adatok szerint a malware-fertőzések száma 2009-től 2018-ig 12,4 millióról 812,67 millióra emelkedett, amelyeket 92%-ban e-mail útján kézbesítettek.

[14] Jéri (2020): i. m.
[15] *2020 Cyber Security Statistics – The Ultimate List Of Stats, Data and Trends.* 2020.

A Kaspersky – ismert – kiberbiztonsági vállalat enciklopédiája[16] szerint az összes e-mail-forgalom 70-80%-a *spam*, amely elleni védelem nélkül az aktív levelezés lehetetlen, továbbá tapasztalataik szerint a kéretlen levelek 50%-ban az alábbi fő kategóriákba sorolhatók:

- felnőtt tartalom;
- egészség;
- információtechnológia (IT);
- személyes pénzügyek;
- tanulás és tréning.

1. táblázat

Az e-mail felhasználók és a küldött/fogadott levelek alakulása

Forrás: a szerző szerkesztése Email is not dead. But email IS changing adatai alapján

Év	E-mail-felhasználó	Napi küldött/fogadott e-mail
2018	3,83 Mrd	281 Mrd
2020	4,03 Mrd	306 Mrd

A Statista internetes statisztikai oldal 2019-es adatai[17] alapján, a vezető malware-típus több mint 60%-kal a trójai, amelyet a vírus, a féreg és a backdoor típusok követnek.

A DataProt kiberbiztonsági cég 2019. novemberi összefoglaló statisztikája[18] szerint 350 ezer új malware-t detektálnak minden nap; minden percben 4 db vállalat esik áldozatául zsarolóvírusnak.

A security.org internetes oldal az antivírusprogramok használati szokásairól szóló tanulmányában[19] leírja, hogy az amerikai háztartások 18%-a semmilyen kártékony program elleni védelmet nem használ.

4.5. A vizsgálatokból és a statisztikai kitekintésből levont következtetések

- a levelezőrendszerek összességében túlzottan engedékenyek a fertőző kóddal vagy megtévesztő tartalommal érkező levelekkel szemben, azokat nem szűrik elég hatékonyan;
- a felhasználók döntéseiket esetenként úgy hozzák meg, hogy a kártékony kódok IT-eszközeikre kerülnek és aktiválódnak;
- a felhasználók IT-eszközeinek védelmi rendszere nincs eléggé felkészítve a fertőzések automatikus elhárítására;
- határozottabb fellépés nélkül nem érhető el magasabb (kiber)biztonsági szint.

[16] Kaspersky IT Encyclopedia: *Types of spam.* é. n.
[17] Statista: *Distribution of leading Windows malware types in 2019.* 2021.
[18] Bojan Jovanović: *Malware statistics – You'd better get your computer vaccinated.* DataProt, 2019.
[19] Security.org Team: *Personal antivirus consumer usage, adoption and shopping study: 2021.* 2021.

„A rosszindulatú felhasználás és kihasználás áldozatai a felhasználók, amelyhez egyfajta »segédeszköz« a levelezőrendszer. Az üzemeltetők a védelmet a levelezőrendszerre tudják felépíteni, ugyanakkor figyelembe véve, hogy mindig a felhasználó a leggyengébb láncszem, tehetnek és ajánlott is tenni lépéseket a felhasználók védelme érdekében. Érdemes a felhasználókat, vagy ügyfeleket meggyőzni a biztonságról, hogy ők maguk is igényként fogalmazzák meg a lehetséges védelmi szolgáltatások működtetését."[20]

4.6. Javaslatok

Az IT-eszközök fertőzésének csökkentéséhez véleményem szerint az alábbi lépések elengedhetetlenek:

- a levelezőszerverek rosszindulatú felhasználásának és kihasználásának megakadályozása;
  - a felhasználók IT-eszközei magasabb szintű védelmének kialakítása;
  - dinamikusabb levelezőrendszer-üzemeltetés.

5. A rosszindulatú felhasználás és kihasználás megakadályozása

„A rosszindulatú felhasználás és kihasználás egymással lehetnek átfedésben, amelynek leggyakoribb előfordulása, hogy mindkét műveletet egyszerre próbálja végrehajtani a tevékenységet folytató. Lényegi különbség azonban, hogy a felhasználásnál a levelezőszerver postafiókja, a kihasználásnál pedig másik levelezőszerver felé történő továbbítás a fő cél.

5.1. Rosszindulatú felhasználás megakadályozása

A rosszindulatú felhasználás kezdete, amikor a kéretlen levél megjelenik a levelezőszerver bemenetén és, a küldő reménye szerint – a továbbító funkciókon keresztül –, végighalad a címzett postafiókja felé. A rosszindulatú felhasználást szűrők közbeiktatásával lehetséges és kell megakadályozni, amelyekkel vizsgálható az érkező levél

- küldőjének egyedi hálózati azonosítója;
- szöveges tartalma;
- csatolmánya, melléklete;
- feladója, címzettje, tárgya, mérete.

E szűrők használata nélkül az érkező levelek kézbesítését automatikusan, feltétel és vizsgálat nélkül végrehajtaná, használatukkal azonban csak a rostán fennmaradó levelek jutnak el a címzetthez. A szűrők alkalmazásakor eldöntendő, hogy fennakadás esetén mi legyen a beérkező levél további sorsa: eldobja; a címzett figyelmeztetésével egyidejűleg továbbítsa; vagy átmeneti mappába kerüljön.

[20] Jéri (2020): i. m.

5.1.1. Küldő vizsgálata

Az internet hálózati felépítéséből adódóan a küldő SMTP-szerver is egyedi IP-címmel rendelkezik. E cím csupán a küldő levelezőszerver internetes azonosítóját takarja, de nem mutatja, hogy a levelet szerver mögötti kliens küldte-e. A küldő IP-címének, e-mail-címének, valamint a kettő egyezőségének vizsgálatával megállapítható többek között, hogy:

- a küldő e-mail-címében szereplő domainnév megegyezik-e az IP-címből visszafordított domainnévvel;
- a küldő IP címe:
  - valamely szolgáltató által dinamikusan kiosztott cím-e;
  - szerepel-e a kéretlen leveleket küldő szerverek nyilvános adatbázisában.

Ezekből az információkból nagy eséllyel már a levelezőszerver bemenetén megjelenő levélről következtethető, hogy kéretlen, esetleg fertőzött lesz-e. Amennyiben a küldő szerver IP-címéből visszafordított és az e-mail-címben szereplő domainnév nem egyezik, úgy feltételezhető, hogy a küldő megtévesztő szándékkal ál e-mail-címet használt a levél feladásakor. Amennyiben a küldő IP-címe valamely szolgáltató által kiosztott dinamikus cím, akkor gyanús, hogy az elektromos levél nem egy kifejezetten levélküldésre rendszerbe állított számítógépről származik. Feltételezhető, hogy egy otthoni háztartás fertőzött eszközéről, egy rosszindulatú program küldi a levelet, valószínűleg továbbfertőzési céllal, ugyanakkor az is előfordulhat, hogy valaki marketingcélú levelek küldésére – ad-hoc jelleggel – levélküldésre alkalmas programot telepít otthoni gépére, és arról küld leveleket. Ha a küldő IP-címe valamely nyilvános, naprakész, kéretlen leveleket küldő adatbázisban szerepel, úgy feltételezhető, hogy az érkező levél fertőzött vagy kéretlen, ezért fogadása nem ajánlott.

A levelezőszervert úgy kell beállítani, hogy a küldő, világháló szerinti IP-címe alapján döntést tudjon hozni az érkező levél fogadásáról vagy elutasításáról.

5.1.2. Szöveges tartalom vizsgálata

Az elektronikus levelek tartalmi vizsgálata lényegében azt dönti el, hogy az érkező levél kéretlennek, azaz spamnek tekinthető-e. Konkrét definíciója nincs a spam levélnek, a rövidítés a *Monty Python Repülő Cirkusza* című tévésorozat egyik jelenetében feltűnt löncshúsra utal, valójában a ráerőltetést szimbolizálja. Általánosságban a „nagy példányszámban elküldött, azonos tartalmú kéretlen elektronikus üzenet" leírással határolják körül a fogalmat, azonban az egyes leveleket már eltérően sorolják kéretlennek vagy nem kéretlennek az elektronikus levelet vizsgáló programok.

A HTML-alapú megjelenést kihasználva a megtévesztő szövegbe linket helyeznek el, amely látszólag kapocs a tartalommal összefüggő ügyintézéshez, de legtöbb esetben kattintásra aktivizálódó, valamilyen beavatkozást végrehajtó programkód.

A spamek elleni védelemhez elkerülhetetlen és kötelezően alkalmazandó valamilyen levelezőszerverhez illeszthető, szűrésre alkalmas program. A kéretlen levelek szűrésének összetettsége miatt, mindenképpen a levelezőszerverrel együttműködő,

erre specializálódott, folyamatosan frissülő külső program használata ajánlott, hisz a kéretlen levelek tartalma dinamikusan változik, amihez igazodnia kell a szűrési feltételeknek is. Az egyik legnépszerűbb, nyílt forráskódú spamszűrő alkalmazás leírása alapján[21] a program egy nagy szabályrendszert alkalmaz, amely optimalizált keresést tesz lehetővé, minimalizálva a tévesztés lehetőségét. A programban szereplő szabályok manuálisan is bővíthetők, amely lehetővé teszi a személyre szabott, speciális beállítások alkalmazását.

A spamszűrő programok az elektronikus levél tartalma és az aktuális szabályrendszer alapján a levélhez egy pontértéket rendelnek, amelyből következtetni lehet a kéretlen levél valószínűségére, majd a levelezőszerver dönt a levél további sorsáról.

A spamek szűrésének legnagyobb problematikája az emberi leleményesség és a gépiesített, algoritmusszerű vizsgálat közötti ellentmondás. A kreativitás nyilvánvalóan azt a célt szolgálja, hogy az elektronikus levél a szűrőkön átjusson, ugyanakkor a hatalmas mennyiségű levél átnézésére emberi kapacitás nem áll rendelkezésre, azt csak programok, algoritmusok képesek vizsgálni. A jól és hatékonyan működő spamszűrő a felhasználói igényeknek megfelelően a kéretlen leveleket megfogja, a többit viszont hiánytalanul átengedi, ami csak a megfelelő szűrőalkalmazás használatával, a levelezőszerver és a szűrőalkalmazás precíz finomhangolásával, a spamre adandó megfelelő válaszreakció beállításával valósítható meg.

Tekintettel arra, hogy a spamek elleni védelem erősségi szintjét a levelezőszervert üzemeltető saját belátása szerint határozza meg, a megfelelő védelemre egzakt küszöbérték vagy számszaki meghatározás nem adható.

Eldöntendő kérdés a spam kategóriába sorolt levelek további sorsa. Az üzemeltetők hozzáállása különböző, hisz van, aki a felhasználó mappájában egy elkülönített almappába helyezi a kéretlennek minősített leveleket, de van, aki egyszerűen eldobja a spameket, és annak tényét nem is hozza a felhasználó tudomására.

5.1.3. Csatolmány, melléklet vizsgálata

Elsősorban az elektronikus levél mellékletébe rejtett rosszindulatú kódok elleni védelmet jelenti, amelyet leghatékonyabban külső, erre a feladatra specializálódott, frissülő adatbázissal rendelkező program képes ellátni. A megfelelően rugalmas levelezőszerverekhez illeszthetők a rosszindulatú programokat feltárni képes keresőprogramok. A gyakorlatban az elektronikus levelet – kézbesítés előtt – átadja a vizsgáló alkalmazásnak, amely a mellékletek átnézését követően egy jelzéssel visszaadja azt a levelezőszervernek és a levelezőszerver dönt a levél további sorsáról. Erősen ajánlott a malware-t tartalmazó elektronikus leveleket a levelezőszerveren kézbesítés előtt megsemmisíteni és mellőzni a postafiók-tulajdonosokhoz történő eljuttatást.

A rosszindulatú kód vizsgálata előtt szofisztikált megoldást jelent még a csatolmány típusának, kiterjesztésének beazonosítása és kezelése. A legnagyobb – ingyenes – levelezőszerverek is használják ezt a módszert, amelynek lényege, hogy a végrehajtható

[21] Apache Software Foundation: *SpamAssassinRules.*

kódot tartalmazó elektronikus leveleket egyszerűen blokkolják, vagy csak csatolmány nélkül továbbítják a címzettnek, amelyről általában értesítést is küldenek.

A csatolmányok természetesen lehetnek tömörített állományok is, amely esetben a vizsgálatot a kitömörítési eljárással szükséges kombinálni, ugyanakkor figyelembe kell venni, hogy a csatolmányokon végrehajtott műveletek nagyon erőforrás-igényesek.

A csatolmányok vizsgálata a levelezőszerver rosszindulatú felhasználásának elkerülése érdekében kötelező, a vizsgálat mélységét pedig az erőforrások rendelkezésre állásának függvényében célszerű beállítani.

5.1.4. Az elektronikus levél paramétereinek vizsgálata

Az elektronikus levél feladójával, címzettjével, másolati vagy titkos másolati címzettjével, tárgyával és méretének vizsgálatával is szükséges foglalkozni. A mezők kitöltöttsége esetén azok tartalmi vizsgálata mindenképpen indokolt, egyes mezők – például a feladó – ki nem töltöttsége pedig egyenesen felveti a kéretlen levél gyanúját. A levél mérete is fontos információ, hisz egy minimális méret alatt erősen ajánlott spamvizsgálat alá vetni, egy bizonyos méret felett pedig az erőforrások védelme érdekében célszerű korlátokat alkalmazni.

5.2. Rosszindulatú kihasználás megakadályozása

Alapvetően a levelezőszerver általi tömeges levélküldés megakadályozását jelenti, amely magában foglalja a levélküldéshez szükséges jogosultságok illetéktelenhez jutásának megakadályozását is. A kihasználás leggyakrabban valamely rosszindulatú programmal fertőzött – levelezőszerverhez kapcsolódott – klienseszközről, SMTP-protokollon keresztül következik be, amely ellen a levelezőrendszer alábbi területein szükséges védelmet kiépíteni:

- relay funkció;
- hozzáférések;
- levélforgalom;
- kimenő levelek tartalma.

5.2.1. Relay funkció védelme

A levelezőszerver Relay funkciójának működtetése ugyan elengedhetetlen a világháló irányába történő levélküldéshez, azonban lehetséges és mindenképpen ajánlott is meghatározni, hogy azt milyen hálózati tartományból vagy IP-címekről érkező klienseszközöknek biztosítsa a levelezőszerver. Ajánlott alkalmazni az alapértelmezésben „senkinek, kivéve akinek" továbbítási alapelvet, amellyel jelentősen szűkíthető a levelezőszervert potenciálisan kihasználni képes eszközök száma. Ezzel a lehetőséggel biztosítható, hogy csak „megbízható" kliensek tudjanak leveleket küldeni kifelé, egyébként a levelezőszerver csak a levelek fogadását biztosítsa. A küldési jogosultsággal

nem rendelkező klienseknek pedig alternatívát jelenthet a Webmail alkalmazás telepítése, amely eltérő specifikumából adódóan minimálisra csökkenti a kihasználás megvalósítását, ugyanakkor lehetőséget teremt a levelek világháló irányába történő továbbítására. A legnagyobb interneten elérhető ingyenes levelezőrendszerek biztonsági okból alapértelmezésben szintén Webmail-hozzáférést biztosítanak, és kerülik a kliens-eszközökről, hagyományos levelező programmal és protokollal folytatott levelezést.

Amennyiben nélkülözhetetlen a Relay biztosítása, úgy azt mindenképpen autentikációhoz, kötötten szabad csak biztosítani. Érdemes megvizsgálni annak a lehetőségét, hogy a Relayhez alkalmazni kívánt authentikációs adatok lehetnek-e különbözők a levelezési postafiók hozzáférési adataitól, s amennyiben igen, úgy ezt a lehetőséget ajánlott alkalmazni. Szintén elvárt beállítás továbbá a Relayhez alkalmazott hálózati csatorna biztonságossá tétele, amely kódolttá teszi a kommunikációt és nagyban megnehezíti a hálózaton lehallgatott autentikációs adatok visszafejtését.

5.2.2. Hozzáférések védelme

Ha a levelezőszerveren tárolt felhasználói adatok a fentebb említetteknek megfelelően védve vannak, akkor is van lehetőség némelyik megszerzésére, amelyet erősít az általános gyakorlat. Amennyiben az ügyfélkiszolgáló szerveralkalmazás elérhető a világhálón, úgy ahhoz bárkinek lehetősége van csatlakozást kezdeményezni és a megfelelő felhasználónév – jelszó páros ismeretében a postafiók leveleit kiolvasni. A levelezőprogramokban létezik olyan beállítási lehetőség, hogy a levelek küldéséhez ugyanaz az authentikáció tartozzon, mint a levelek olvasásához, amely gyakorlatilag sugallja a felhasználók és az üzemeltetők felé, hogy érdemes ezzel a lehetőséggel élni. A rossz beidegződés miatt a levélküldéshez és a levelek olvasásához gyakran ugyanaz az authentikáció tartozik, ezért aki próbálkozással kitalálja, hogy adott e-mail-postafiók milyen jelszóval olvasható, úgy annak nagy eséllyel arra is lesz lehetősége, hogy leveleket küldjön ki a levelezőrendszerrel, majd azt véletlenül vagy szándékosan kihasználja.

A próbálkozásokkal szemben hatékony védelmi lehetőség a dinamikus tűzfal használata, amely a naplóállományok figyelésével, meghatározott sikertelen belépési kísérletet követően, a klienseszköz csatlakozását – hálózati azonosítója alapján – bizonyos időre megtagadja, ezáltal kizárja a további próbálkozásból. Ez a beállítás egyaránt alkalmazható a levelezésben érintett SMTP-, POP3-[22], IMAP[23]-protokollokat használó programokhoz. A jól beállított helytelen próbálkozási szám és kitiltási idő garantálja, hogy ne sikerüljön kitalálni a postafiókhoz tartozó jelszót, megakadályozva a levelezőszerver kihasználását. Három helytelen próbálkozás után, legalább ötperces kitiltást ajánlott alkalmazni.

[22] *Post Office Protocol version 3* – post office protokoll 3-as verzió.
[23] *Internet message access protocol* – internetüzenet-hozzáférési protokoll.

5.2.3. Levélforgalom kontrollja

Figyelembe véve, hogy a levelezőszerver kihasználása a levelek tömeges kiküldésével valósul meg, mindképpen ajánlott ennek a védelmét is megoldani. A jól kiválasztott levelezőszerver rendelkezik azzal a beállítással, amelyben megadható, hogy adott időintervallum alatt, mekkora számú levelet, hány címzettnek küldhet csak ki. Ennek a paraméternek a helyes megválasztásával garantálható, hogy a felhasználó a leveleit kényelmesen, még sietség esetén is kiküldhesse, ugyanakkor a tömeges levéláradatot megakadályozza. Megítélésem szerint, egy perc alatt maximum 10 levelet, maximum 20 címzettnek elégséges engedélyezni.

5.2.4. Kimenő levelek vizsgálata

A levelezőrendszer rosszindulatú felhasználása témakörben kifejtett tartalmi és mellékletvizsgálat – kimenő levelekre vonatkoztatott – végrehajtásával tovább növelhető a levelezőszerver kihasználásának megakadályozása, azonban figyelembe kell venni, hogy alkalmazása jelentősen terheli a szerver erőforrásait.

6. Felhasználók védelme

A rosszindulatú vagy kéretlen levelek felhasználói fiókba eljutása önmagában csak annyit jelent, hogy a levél a levelezőrendszer szűrőin átjutott, a kód még nem aktiválódott, és a felhasználón múlik a levél további sorsa.

6.1. Felhasználók oktatása

A felhasználók rosszindulatú programokkal és azok terjedésével kapcsolatos hétköznapi, érthető formában történő tájékoztatása nagyban elősegíti a rosszindulatú felhasználás megakadályozását. Amennyiben tisztában vannak a gyanús jelekkel és a felhasználói interaktivitás lehetséges következményeivel, akkor kisebb eséllyel aktiválják a rosszindulatú programkódokat, vagy tesznek eleget ismeretlenek kéréseinek. Amennyiben a levelezőrendszer postafiókjainak felhasználóival az üzemeltetőnek – például munkahely esetén – közvetlen kapcsolata van, úgy mindenképpen személyesen ajánlott visszatérő rendszerességgel oktatást tartani, eltérő esetben elektronikus tájékoztató levelek vagy kisfilmek is sokat segíthetnek a megelőző tevékenységben. Érdemes e-mail-használati protokollt készíteni, amely többek között kitér a többes címzés, a másolat és a titkos másolat közötti különbségre, és azok biztonságos alkalmazását mutatja be, továbbá leírja, hogy miként lehet az e-mailek forrásából meggyőződni a levél eredetéről.

6.2. Felhasználók munkakörnyezetének alakítása

A felhasználók munkakörnyezetét munkahely esetén a vezető befolyásolhatja, egyébként pedig ajánlás tehető annak kialakítására.

Napjainkban számtalan – akár ingyenes – program áll rendelkezésre, amely képes a levelezőprogramba integráltan védelmet nyújtani a kéretlen vagy fertőzött levelekkel szemben, megakadályozva azok aktivizálódását. Ezen programok telepítése erősen ajánlott.

A levelezőprogram és a levelezőszerver közötti kapcsolat felépítésére legtöbbször olyan segítő alkalmazás – „súgó" – áll rendelkezésre, amely laikusként is végigvezeti a felhasználót az elektronikus levelek sikeres kezeléséhez, azonban az alternatív beállítások elvégzésében csak ritkán segít. Ha a felhasználó választhat a biztonságos vagy a nyílt hálózati csatorna, illetve a kódolt vagy a kódolatlan kommunikáció között, akkor előfordulhat, hogy a helytelen döntést hozza meg, mit sem sejtve annak negatív következményeiről. Ebben a témakörben is ajánlott az iránymutatás, vagy a helyes beállítás kikényszerítése.

7. Üzemeltetés

A levelezőrendszer összetettségéből adódóan elkerülhetetlen üzemeltető személy alkalmazása, mert az elektronikus levelezés biztonsága dinamikusan változik, amely kihívásokra időben, megfelelő válaszokat kell adni. A levelezőrendszer a biztonságra tett erőfeszítések nélkül is képes átmenetileg ellátni feladatát, azonban a postafiókok felhasználói ez esetben kitetté válnak, a levélkézbesítés fázisai rendelkezésre állásként, automatikusan végrehajtódnak, és a rendszer valóban „nyitott biztonsági résként" fog üzemelni. A rendszer biztonságának kialakításában létezik radikálisabb vagy humánusabb hozzáállás, a helyes utat azonban a megfogalmazott biztonsági cél elérése adja, a felhasználói elvárásoknak történő megfelelés figyelembevételével. Fontos kiemelni, hogy a felhasználók levelezőrendszerrel szemben támasztott igényei közül, a – hagyományos protokollokkal működő – levelezőprogramok használata növeli a levelezőrendszer kihasználásának lehetőségét, míg a kéretlen és fertőzött levelek elleni védelem növeli a biztonságot, s vele együtt a szerver leterheltségét is.

Az üzemeltető feladatai:

- a felhasználók biztonságkerülő hozzáállása mellett is a rendelkezésre állás megteremtése;
- a levelezőszerver megfelelő védelmi szintjének beállítása, elérése;
- legalább napi mentés, archiválás kialakítása;
- a támadások elhárítása;
- a rendszerben található hiányosságok folyamatos feltárása, kijavítása;
- ügyfelek igényeinek lehetőség szerinti teljesítése."[24]

[24] Jéri (2020): i. m.

8. Összegzett javaslatok

Az elektronikus levelezés biztonságának szükségességét nem lehet eleget hangoztatni. Az internetet és az okoseszközöket használók folyamatos létszámemelkedése egyértelműen kihatással van az elektronikus levelezést igénybe vevők számára is, amely egyenesen arányosan előtérben tartja az e-mail-címeket mint lehetséges támadási célpontokat. A nagy számok törvénye miatt a kiberbűnözők az elektronikus levelezést mint eszközt folyamatosan igénybe veszik, az elektronikus levelezőrendszereket üzemeltetőknek pedig a biztonságot fenn kell tartaniuk. Figyelembe véve, hogy az elektronikus levelezés még mindig az első számú, mindamellett „legális" támadási eszköz az interneten, kiemelt figyelmet kell fordítani a biztonsági kérdésekre: a fertőző kódok továbbítását már a levelezőrendszeren, a lehető leghatékonyabban meg kell akadályozni; a gyanús kódokkal vagy megtévesztő tartalommal rendelkező elektronikus levelek vonatkozásában a felhasználók döntési helyzetét kerülni kell; a felhasználókat képezni kell, és az optimális védelmi munkakörnyezetre javaslatot kell adni.

Felhasznált irodalom

2020 Cyber Security Statistics – The Ultimate List Of Stats, Data and Trends. Purplesec, 2020. Online: https://purplesec.us/resources/cyber-security-statistics

Apache Software Foundation: *SpamAssassinRules.* Online: https://wiki.apache.org/spamassassin/SpamAssassinRules

Email is not dead. But email IS changing. 2021. Online: www.emailisnotdead.com

Jéri Tamás: *A Kritikus Internetes Szolgáltatások biztonsági kérdései a védelmi szférában.* Doktori (PhD-) értekezés tervezet. Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, 2020. Online: https://kmdi.uni-nke.hu/document/kdmi-uni-nke-hu/jeri_tamas_tervezet_20200722.pdf

Jovanović, Bojan: *Malware statistics – You'd better get your computer vaccinated.* DataProt, 2019. Online: www.av-test.org/en/statistics/malware

Kaspersky IT Encyclopedia: *Types of spam.* é. n. Online: https://encyclopedia.kaspersky.com/knowledge/types-of-spam

Kovács László: *A kibertér védelme.* Budapest, Dialóg Campus, 2018.

Security.org Team: *Personal antivirus consumer usage, adoption and shopping study: 2021.* 2021. Online: www.security.org/antivirus/antivirus-consumer-report-annual

Statista: *Annual number of malware attacks worldwide from 2015 to 2020.* 2021. Online: www.statista.com/statistics/873097/malware-attacks-per-year-worldwide

Statista: *Distribution of leading Windows malware types in 2019.* 2021. Online: www.statista.com/statistics/221506/share-of-new-types-of-malware

Tanenbaum, Andrew S. – David J. Wetherall: *Számítógép-hálózatok.* Budapest, Panem, 2013.