Lehetséges egyetemi adatbázisokat fenyegető veszélyek

Bálint Krisztián

Egyetemi tanársegéd, Óbudai Egyetem, Keleti Károly Gazdasági Kar,
Vállalkozásfejlesztés és Infokommunikációs Intézet,
balint.krisztian1@uni-obuda.hu

Abstract: Az egyetemi adatbázisok érzékeny adatokat tartalmaznak, ezért azok védelméről gondoskodni kell, mivel az utóbbi években a statisztikai adatok azt mutatják, hogy egyre inkább növekednek az adatbázisokat ért támadások száma. Amennyiben az egyetem érzékeny adatokat tárol a hallgatóiról, úgy az adatabázisbiztonság témakörét szükségszerű behatóbban megvizsgálni, a lehetséges veszélyeket felismerni és időben csökkenteni egy sikeres támadás lehetőségét. Napjainkban a leggyakrabban alkalmazott támadási módszerek közé sorolható a zsarolóvírusok okozta fenyegetések, valamint a DDoS Distributed Denial of Service - Elosztott szolgáltatásmegtagadással járó támadások száma. A központosított adattárolás következtében a centralizált rendszerek nem minden eseben nyújtanak megfelelő védelmet, ezért a decentralizált megoldásokban rejlő lehetőségeket is kutatni kell, úgy mint az On-Chain és Off-Chain alapú blokklánc megoldásokat, annak függvényében, hogy egy optimális adatbázis biztonságot lehesen kialakítani.

Keywords: Blokklánc technológia, adatbázis-biztonság, On-Chain, Off-Chain

1 Egyetemi adatbázis-biztonság fontossága

Az adatbázis-biztonság definicióját nehéz megfogalmazni, mivel meglepő módon széleskörűen elfogadott értelmezése nincsen, holott az informatika aktívan foglalkozik ezzel a témakörrel. Fontos szerepet játszik a bizalmasság, mivel az adatokhoz való hozzáférést a jogosultság függvényében szabályozza. Továbbá a sértetlenség is lényeges, amely azt jelenti, hogy csak az arra jogosultak változtathatják meg az adatokat. A rendelkezésre állás alatt az adatokhoz való hozzáférést értjük, azon belül is csak azokat a személyeket, akiknek ehhez joguk van.

Saját értelmezés és megfogalmazás alapján a következő képpen definiálom az adatbázis-biztonságot:

Adatbázis-biztonság definíciója alatt a fenyegetettségeknek és a támadásokkal való ellenálást értjük, azokkal szemben alkalmazott védelmi erőforrások

összeségét, amelyek megakadályozzák, hogy az arra jogosulatlan fizikai és jogi személyek, valamint kártékony számítógépes programok kihassanak azon működésére, bárminemű kárt okozzanak azok jogos tulajdonosainak, illetve felhasználóinak. Ide sorolandó még a bizalmasság, sértetlenség és rendelkezésre állás, valamint a letagadhatatlanság és a hitelesség biztonsági kritériumait is.

Az elmúlt években számos esetben kerültek nyilvánosságra bizalmas információk, amelyek személyes adatokat tartalmaztak. Az ilyen típusú támadások negatívan hatnak ki a vállalatok megítélésére és az emberek bizalmatlanokká vállhatnak. Ezekben az esetekben nem csak a hírnév megítélésében esik csorba, hanem többletmunkát jelent az adatok visszaállítása, már amennyiben arra adott a lehetőség. Ezen felül az is előfordulhat, hogy jogi pereskedések, valamint különböző bírósági eljárások is kezdetét veszik. (Fleiner, 2010). A GDPR bevezetése óta a nem megfelelő adatkezelés következtében büntetetések kiszabására is sor kerülhet.

A fenyegetések ellen számos módon lehet védekezni, azonban teljes biztonság, feltörhetetlen adatbázis nem létezik. Kockázatelemzéssel, azonosítással és értékeléssel azonban ki lehet építeni egy olyan védelmi szintet, amely csökkenteni tudja a sebezhetőséget. (Fleiner & Munk, 2011)

A webes technológiának köszönhetően az adatok az internetet használatával is hozzáférhetőek. A kényelmi szolgáltatások mellett ez a lehetőség komoly kockázatot hordoz magában, mivel szélesebb kör számára válnak elérhetővé az adatok. Az adatbázisok általában struktúrált adatokat tartalmaznak, így azok áttekinthetőek. Amennyiben egy hacker hozzáfér az adatokhoz, úgy azokat átlátja, könnyedén tudja értelmezni. A leggyakoribb támadások az adatbáziskezelőkben található sérülékenységek és a hibás tűzfalbeállításokból keletkező kockázatok, amelyek hamis biztonságérzetet adnak. [73]

A Data Brench Investigation Report szerint 819 támadás, illetve esemény történt az oktatási intézmények ellen 2020 júliusáig, ebből 228 esetben erősítették meg az intézmények, hogy nem kívánatos adatok kerültek nyilvánosságra. Továbbá a támadások 67%-a kívülről jött, míg 33%-uk belülről irányult az oktatási intézmények ellen. (Bálint, 2021) A támadások célja 92%-ban a haszonszerzés volt, míg a maradék százalékban a kémkedés, illetve szórakozás céljából történt. A támadások 75%-ában személyes adatok kompromitálódtak. A támadások 80%-ában leggyakrabban a Ransomware vírust használták, amelyről tudvalevő, hogy nagy hatékonysággal titkosít és töröl adatokat.[74]

Messzebről szemlélve az adatbázis-biztonságot érintő statisztikai kimutatásokat észre lehet venni, hogy komoly fenyegetetségnek vannak kitéve az adatok, amelyet

[73] Computerwolrd: Adatbázisok biztonsági kérdései. https://bit.ly/32MjkZA Letöltés ideje: 2023.04.26.

[74] Verizon: 2020 Data Breach Investigations Report. https://vz.to/2ONnvfu Letöltés ideje: 2023.04.26.

a támadók valószínűleg ki is használnak. A következő statisztikai adatokat a Varionis szofvercég tette közzé a 2020-as évben:

- Az adatsértések 4.1 milliárd rekordot érintettek 2019 első felében,
- A vállalatok mappáinak mindössze 5%-a van kellőképpen védve,
- Az adatkezelési szabályok megsértése 2014 óta 67%-kal, 2018 óta pedig 11%-kal növekedett,
- A vállalati adatok 83%-a 2020-ban valószínűleg a felhőbe kerül,
- A hackerek és a rossz indulatú támadók 39 másodpercenként próbálnak adatbázist feltörni, naponta átlagosan 2244 alkalommal.
- A jogsértések időtartama, amely felöleli a jogsértéstől az elhatárolásig tartó időtartamot átlagosan 314 nap volt 2019-ben. [75]

A 2019-es Global Data Risk Report from the Varionis Data Lab vizsgálatában 785 szervezet került kielemzésre. A kutatás a következő hiányosságokat tárta fel:

- A vállalatok 53%-a ezernél is több olyan érzékeny fájlal rendelkezik, amely minden ott dolgozója számára elérhető. Ugyanez a kutatás a 2018-as évben „még csak" a vállalatok 41 százalékánál tárta fel ezt a hiányosságot,
- Átlagban a vállalati teljes adatkészlet és az összes mappa 22%-a volt elérhető minden alkalmazott számára, amelyben az adatok 17%-a érzékeny adatnak minősült.
- A vállalatok 58%-a talált több mint 1000 elavult fiókot találtak.[76]

A decentralizált adatbázisokra a következő lehetséges veszélyes leselkednek:

- Sybil támadás esetében a hálózatot egy hozzá hasonlóan működő, de szimulált P2P bot hálózat alkalmazása által kísérletet tesz a konszenzus befolyásolására. Amennyiben a konzorcium a hálózatára próbálna kihatni, úgy az egy új csomópont hozzáadását tenné szükségszerűvé, amelyhez regisztrációra és jogosultság megadásra is szükség lenne. Nyilvános blokklánc esetében Sybil támadással kizárólag lassítani, illetve túlterhelté lehet tenni a hálózatot, módosításra ebben az esetben nincsen lehetőség.
- Sikeres 51 százalékos támadás alatt a blokklánc felett át lehet venni az irányítást. Ha egy csomópont 50%-nál nagyobb számítási kapacitással rendelkezik, akkor hackelés útján át lehet venni az irányítást. A hálózat addig működik megbízhatóan, ameddig a hálózat kétharmada hibamentes. Ezt a bizánci tábornokok matematikai modelljével lehet magyarázni.

---

75 Varionis: 110 Must-Know Cybersecurity Statistics for 2020. https://bit.ly/3eY3LQQ Letöltés ideje: 2023.04.26.

76 Varionis: 2019 Data Risk Report from the Varionis Data Lab. https://bit.ly/2OYUjSJ Letöltés ideje: 2023.04.26.

- A Goldfinger támadásnak a célja, hogy teljesen tönkre tegye a rendszert. A haszonszerzés ebben az esetben mellékes. A legnagyobb blokklánc hálózat sikeres megtámadásához egy atomerőmű teljes kapacitására lenne szükség, amely esetben a szükséges energiát a Proof-of-Work kriptográfiai probléma megoldására kellene fordítani. (Trinh & Szegő, 2023)

2 Jelentősebb adattámadási módszerek

A DDoS (Distributed Denial of Service - Elosztott szolgáltatásmegtagadással járó támadás) komoly fenyegetést jelenthet az egyetemek számára, mivel a biztonsági felvételeket adatbázisokban tárolják. Egy ilyen támadás esetében az adatbázis elérhetetlenné válhat, illetve akár bizalmas adatok is kiszivároghatnak. A hallgatók adatbázisa, amely az azonosításhoz, illetve az arfelismeréshez szükséges mindenképpen ide sorolandó.

A DDoS támadások alkalmával számos számítógépet vesznek igénybe jogosulatlanul a támadók ezzel kialakítva egy zombihálózatot. (Douligeris & Mitrokotsa, 2004) Egy ilyen támadásban több ezer, vagy akár millió megfertőzött számítógép is részt vehet, úgy, hogy közben a valódi számítógéptulajdosonok erről mit sem tudnak. Ezek az OSI modell különböző rétegeiben végeznek támadásokat. A következők támadási modelleket szokták alkalmazni:

- Alkalmazási réteget érintő támadások alkalmával a botnet számítógépek egyszerre próbálnak hozzáférni az adott szerverhez, ezzel túlterhelté téve azt. Gyakran előfordul, hogy ennek következtében a szerver összeomlik.
- A protokoll támadásokra jellemző, hogy félkésznek tűnő csomagokat küldenek a szervernek, amely megpróbálja azokat összerakni, ezért megerősítésre van szüksége. A támadás lényege, hogy a forrás IP cím irányából a megerősítés nem fog megérkezni, sőt egyre több csomag összeillesztésre érkezik.
- Hálózati túlterheléses támadás hasonlóan működik, mint az alkalmazási réteget érintő támadás. A cél a teljes szerver sávszélességének a lefoglalása. Ilyen esetben egy komplex támadásról van szó, mivel a szerver már saját magának is küld adatmennyiségeket feldolgozásra. (Porter, 2020)

A Kasperski jelentés szerint a DDoS támadások 2020 első három hónapjában jelentősen megnövekedtek. 2019 negyedik negyedévéhez képest a támadások száma megkétszereződött, míg ugyanez év első feléhez képest 80%-al növekedett. Továbbá a támadások időtartama is növekedett. Az elmúlt évhez képest 25%-kal tovább tartott, mint előtte. Egyik lehetséges magyarázat oka, hogy a járvány idején az emberek még jobban függnek az adatbázisoktól, mivel elszigeteltebben

dolgoznak, távol a munkahelyeiktől, ezért a támadók még inkább kihasználják ezeket a lehetőséget.[77]

Decentralizált adattárolás esetében a sikeres DDoS támadásnak az esélye viszonylag alacsony, mivel a hálózatban az adatok nem egy központi szerverre összpontosulnak, hanem számos csomópontra. Ahhoz, hogy a DDoS támadás sikeres legyen, az egész hálózatot, annak teljes kapacitását, minden számítógépével együtt egy adott időpontban kellene megtámadni. A támadás kivitelezhető, azonban igencsak drága és körülményes megoldás, mivel ez azt jelenti, hogy egyszerre számos számítógépet kell túlterhelni adatcsomagokkal.

A zsarolóvírus (Ransomware) egy olyan rossz indulatú kártékony szoftver, amely titkosítja a fájlokat és kizárólag váltságdíj kifizetése esetén oldja fel azokat. Éves szinten több milliós károkat okozva ezzel. (Scaife et al., 2016)

Az oktatási intézémények fokozott veszélynek vannak kitéve. Előfordulhat, hogy a hallgatók személyes adatait, illetve a biztonsági felvételeket egy ilyen vírus titkosítja, illetve hozza nyilvánosságra. A ransomware jellemzői:

- Számítógépes állományok titkosítása,
- Támadás után zsarolóüzenet küldése (ransomnote),
- Határidó kiszabása a váltságdíj kifizetésére,
- Fizetés megtagadása esetén az állományok titkosítottak maradnak, illetve azok törlődnek. Fizetés esetén nagy valószínűséggel ugyanez a forgatókönyv játszódik le.

Leginkább kéretlen email-en keresztül történik a fertőzés, amelynek a csatolmányában rejtőzik a vírus. Leggyakrabban valamilyen sérülékenységet, illetve hibás konfigurációt kihasználva fér a vírus a számítógepes adatokhoz. [78]

A Nemzeti Kibervédelmi Intézet a következő ajánlásokat fogalmazta meg a vírussal kapcsolatban:

- Fontos az adatok biztonságok másolatáról gondoskodni. Lehetőleg több különböző helyre célszerű elmenteni azokat,
- Biztonságtudatos és átgondolt Világháló használat, legfőképpen az ismeretlen levelekkel kell elővigyázatosnak lenni,
- Mappák hozzáférésének korlátozása,
- Vírusvédelemi megoldások alkalmazása. [79]

---

77 Security Brief: DDoS attacks doubled in Q1 2020 as attackers target remote workers. https://bit.ly/2YHcVMV Letöltés ideje: 2023.04.26.

78 Nemzeti Kibervédelmi Intézet: Riasztás zsarolóvírus (Ransomware) támadásokkal kapcsolatban. https://bit.ly/39ASEwu Letöltés ideje: 2023.04.26.

79 Nemzeti Kibervédelmi Intézet: Zsarolóvírus (Ransomware). https://bit.ly/3f5wnaU Letöltés ideje: 2023.04.26.

Kaspersky Labs jelentése szerint az iskolák 2019-ben 530 bejelentett esetben szenvedtek el különböző ransomware támadást, amelyben az adataik is sérültek. [80]

A Purplesec 2020-as statisztikai adatai alapján kijelenthető, hogy a zsarolóvírussal kapcsolatos átlagos váltságdíj értéke folyamatosan növekszik:

- 2018-ban 4.300 USD,
- 2019-ben 5.900 USD,
- 2020-ban már elérte a 8.100 dollárt.

A támadással kapcsolatos átlagos költségek eseményenként a következőképpen alkultak az utóbbi években:

- 2018-ban 46.800 USD,
- 2019-ben 141.000 USD,
- 2020-ban 283.000 USD.[81]

3 Koronavírushoz kapcsolodó támadások

A 2020-as évben a koronavírus elterjedése számos országot érintett, ezzel megváltoztatva az emberek munkavégzéssel kapcsolatos szokásait. A vállalatok többsége áttért az otthoni munkára, az egyetemek pedig a távoktatásra. Feltételezhetően az emberek többsége otthoni környezetben máshogyan végzi el a munkát, mint az irodában.

A folyamatos rendelkezésre állás senkinek sem könnyű feladat. Az egyetemi szerverek és online tanulást biztosító felületek elérhetőek kell, hogy legyenek, úgy a tanárok, mint a hallgatók számára. A biztonságos kapcsolat kiépítése komoly feladatot tesz az informatikusok vállára. A hallgatóknak hozzáférésük van a feltöltött tananyagokhoz és érdemjegyeikhez, amely előnyös az oktatásban részt vevők számára. Adatbázis-biztonság szempontjából azonban komoly kockázatot rejt magában. Az Interpool 2020-ban a következő ajánlásokat és tanácsokat fogalmazta meg covid idején az adatbázisokat érintő fenyegetettségek következtében:

- Otthoni hálózat megerősítése, biztonságosabbá tétele,
- Biztonsági és adatvédelmi beállítások rendszeres ellenőrzése,
- Mindig a legújabb szoftver frissítések alkalmazása,

---

80 Security Boulevard: Ransomware attacks are on the rise and they're estimated to cost global organizations $20 billion by 2021, according to Cybersecurity Ventures. https://bit.ly/300KSbQ Letöltés ideje: 2023.04.26.

81 Purplesec: 2020 Ransomware Statistics, Data, & Trends. https://bit.ly/303xBPR Letöltés ideje: 2023.04.26.

- Biztonsági másolatok készítése az adatokról, több különböző helyen egyszerre,
- Kellő elővigyázatosság a közösségi média használata során,
- Jelszavak felülvizsgálata, azok biztonságos tárolása. [82]

Az otthoni számítógépen végzett munka komoly veszélyt rejthet magában, mivel előfordulhat, hogy a saját számítógép gyengébb vírusvédelemmel, valamint tűzfallal rendelkezik, mint a vállatlati eszközök többsége. Az otthon használt hordozható vállalati számítógépek esetében pedig előfordulhat, hogy személyes, vagy magánjellegű feladatokat is ezeken az eszközökön végeznek el. A biztonsági szakemberek távolról nehezebben tudják megvédeni a számítógépeket ezzel pedig megnő az esélye egy sikeres rosszindulatú támadásnak.

A járvány előtt a munkavállalók mindössze 4 százaléka dolgozott tartósan otthonról, 43%-uk pedig valamilyen rendszerességgel. A Gartner kutatása szerint a közeljövőben a vállalatok háromnegyede tervezi az otthoni munkavégzést jóváhagyni, ezzel is csökkentve a saját költségeit, egyúttal növelve a dolgozóinak biztonságát, amelyet a Covid vírus jelent.[83]

Az ESET nevű kibervédelmi vállalat felhívta a figyelmet arra, miszerint a kártékony programok 38%-a álcázza magát valamilyen Microsoft Office dokumentumnak, úgy, mint a Word, a Power Point és az Excel, mivel számos iskola és munkahely használja azokat. Az eLearnig, valamint a Mobile Learning széleskörű elterjedésével az okostelefonokra és azok operációs rendszereire megemelkedett a kártékony programok száma. Az áruházak megközelítőleg napi szinten 24.000 rosszindulatú alkalmazást blokkolnak, továbbá a 2019-es évben naponta 350.000 rosszindulató programot észleltek. Ez a Covid idején 667%-kal növekdedett, továbbá vele párhuzamossan a zsarolóvírus támadások száma is jelentősen megemelkedett. 2016-ban 40 másodpercenként, míg 2020 elején 13 másodpercenként történt támadás.[84]

4 On-Chain és Off-Chain alapú adattárolás

A decentralizált blokklánc alapú adattárolásnak két jelentősebb megvalósítása létezik. Ez az On-Chain és Off-Chain blokkláncok.

---

82 Interpol: COVID-19 cyberthreats. https://bit.ly/338TcIB Letöltés ideje: 2023.04.26.

83 Computerworld: A Micro Focus gépi tanulási megoldásával az ismeretlen fenyegetések ellen. https://bit.ly/39DOR1s Letöltés ideje: 2023.04.26.

84 Portfolio: Felpörögtek a hackerek: 667%-kal nőtt a koronavírushoz kapcsolódó támadások száma. https://bit.ly/2P5r017 Letöltés ideje: 2023.04.26.

Az On-Chain a legbiztonságosabb blokklánc alapú adattárolási megoldás, mivel minden adat minden blokkban mentésre kerül. Ennek következtében a hálózat működése lelassulhat, extrém esetben elérhetetlenné is vállhat a túlterhelés miatt. Ezen felül a csomópontok megőrzik az összes adatot, folyamatosan szinkronizálódnak egymással. Amennyiben támadás történik az adatok nem vesznek el. Ez egy drága, de biztonságos megoldás. (Bálint, 2021)

Az adatokat blokkonként elmenteni nem érdemes, mivel az On-Chain a kisebb adatok, illtve szöveges fájlok tárolására lett kitalálva. Az egyetemeknek ezt a megoldást jelen esetben nem érdemes választaniuk. Helyett ajánlatos az Off-Chain tároláson elgondolkodniuk. Általában a blokkláncok különböző tranzakciókkal kapcsolatos információkat tárolnak, ezért kis blokkmérettel rendelkeznek. Ezt részletesen az első táblázat szemlélteti:

Coin megnevezése	Blokkok mérete	Blokklánc mérete	Napi új blokkok száma
Ethereum Classic	1,3 KB	3.8 GB	6695
Ethereum	30KB	132 GB	2232
Dash	2MB	23GB	244
DigiByte	0.5KB	1,9MB	1152

1. Táblázat: Különböző alt coin-ok csoportosítása blokklánc méretük alapján [85]

Az Off-Chain nem tárol el minden egyes adatot csomópontoként, helyette azok hash értékét rögzíti. Az adatok tényleges tárolása a bányászok merevlemezén történik. Ezeket az adatokat mentés előtt több példányban feldarabolják. A bányászok coin-okat (digitális érméket) kapnak a szolgáltatásaikért. [90] A hash nagyban hasonlít az adat ujjnyomatára és algoritmusára, amely a különböző adatokból ujjnyomatot csinál az SHA-256 függvény segítségével. A blokkmódosítást, illetve hashmódosítást minden bányásznak el kell fogadnia és hitelesítenie kell, hogy az érvényes maradjon.[86]

Megállapítható, hogy a decentralizált Off-Chain technológia nyújta a leghatékonyabb és egyben a legbiztonságosabb adattárolási megoldást az egyetemek számára.

[85] Cryptocurrency statistics: Különböző coin típusoknak a blokklánc méretei https://bit.ly/3ueCzX1 Letöltés ideje: 2023.04.26.

[86] Ethereum blog: How to build serverless applications. https://bit.ly/3fBjLJO Letöltés ideje: 2023.04.26.

Összegzés

Az internet technológiának köszönhetően a személyes adatokhoz könnyen hozzá lehet férni, valamint a felhő megjelenésével a folyamatos szinkronizáció által az adatbázisok naprekészen tarthatóak. A számos előny mellett azonban nem szabad megfeledkezni az adatbázis-biztonságról sem, mivel nem egy esetben az adatbázisokban az adatok rendezetten kerülnek tárolásra a könnyebb áttekinthetőség és értelmezhetőség céljából. Amennyiben egy hacker sikeresen eltulajdonítja az adatokat, úgy az adatok könnyen értelmezhetővé válnak a számára. Ebből kifolyólag célszerű a megfelelő adatbázis-biztonság érdekében mindent megtenni. A centralizált adatbázisok hiányosságaiból kiindulva az egyetemeknek érdemes lenne elgondolkodniuk a blokklánc alapú adattárolás lehetőségén, mivel ez esetben egy sikeres rosszindulatú támadás könnyebben kivédhető.

References

[1] Bálint, K. (2021). Possibilities for the Utilization of an Automatized, Electronic Blockchain-based, Students' Attendance Register, using a Universities' Modern Security Cameras; Acta Polytechnica Hungarica, DOI: 10.12700/APH.18.2.2021.2.718(2), pp.127-142.

[2] Bálint, K. (2021). The connection of a Blockchain with Students' Attendance Register based on Security Cameras, IEEE 19th International Symposium on Intelligent Systems and Informatics (SISY 2021), Subotica, Serbia, pp.67-70.

[3] Computerwolrd: Adatbázisok biztonsági kérdései. https://bit.ly/32MjkZA Letöltés ideje: 2023.04.26.

[4] Computerworld: A Micro Focus gépi tanulási megoldásával az ismeretlen fenyegetések ellen. https://bit.ly/39DOR1s Letöltés ideje: 2023.04.26.

[5] Cryptocurrency statistics: Különböző coin típusoknak a blokklánc méretei https://bit.ly/3ueCzX1 Letöltés ideje: 2023.04.26.

[6] Douligeris, C. & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art, Elseiver, Computer networks, pp. 643-666.

[7] Ethereum blog: How to build serverless applications. https://bit.ly/3fBjLJO Letöltés ideje: 2023.04.26.

[8] Fleiner, R. (2010). Az adatbázis-biztonság alapja Hadmérnök; V. Évfolyam, 2. szám, június, pp.1-16.

[9] Fleiner, R., Munk, S. (2011). Informatikai biztonsági útmutatók, kontrollok és szerepük az adatbázis-biztonság megvalósításában, Hadmérnök, VI. Évfolyam, 3. Szám, Szeptember, pp.1-17.

[10] Interpol: COVID-19 cyberthreats. https://bit.ly/338TcIB Letöltés ideje: 2023.04.26.

[11] Nemzeti Kibervédelmi Intézet: Riasztás zsarolóvírus (Ransomware) támadásokkal kapcsolatban. https://bit.ly/39ASEwu Letöltés ideje: 2023.04.26.

[12] Nemzeti Kibervédelmi Intézet: Zsarolóvírus (Ransomware). https://bit.ly/3f5wnaU Letöltés ideje: 2023.04.26.

[13] Porter, E.: Mi az a DDoS-támadás, és hogyan védekezhetünk ellene 2020-ben? https://bit.ly/3iajAXO Letöltés ideje: 2023.04.26..

[14] Portfolio: Felpörögtek a hackerek: 667%-kal nőtt a koronavírushoz kapcsolódó támadások száma. https://bit.ly/2P5r017 Letöltés ideje: 2023.04.26.

[15] Purplesec: 2020 Ransomware Statistics, Data, & Trends. https://bit.ly/303xBPR Letöltés ideje: 2023.04.26.

[16] Scaife, N., Carter Patrick, H., Traynor, K., Butler, R.B. (2016). CryptoLock (and Drop It), Stopping Ransomware Attacks on User Data, IEEE 36th International Conference on Distributed Computing Systems,, pp 303-312.

[17] Security Boulevard: Ransomware attacks are on the rise and they're estimated to cost global organizations $20 billion by 2021, according to Cybersecurity Ventures. https://bit.ly/300KSbQ Letöltés ideje: 2023.04.26.

[18] Security Brief: DDoS attacks doubled in Q1 2020 as attackers target remote workers. https://bit.ly/2YHcVMV Letöltés ideje: 2023.04.26.

[19] Tuan Anh Trinh, Szegő Dániel: Ezek a legvadabb módszerek, amelyekkel kifosztják a bitcoinosokat. https://bit.ly/2P5B3mZ Letöltés ideje: 2023.04.26.

[20] Varionis: 110 Must-Know Cybersecurity Statistics for 2020. https://bit.ly/3eY3LQQ Letöltés ideje: 2023.04.26.

[21] Varionis: 2019 Data Risk Report from the Varionis Data Lab. https://bit.ly/2OYUjSJ Letöltés ideje: 2023.04.26.

[22] Verizon: 2020 Data Breach Investigations Report. https://vz.to/2ONnvfu Letöltés ideje: 2023.04.26.