III. Országos Települési Csapadékvíz-gazdálkodási Konferencia 2021

Tanulmányok

Szerkesztette
Bíró Tibor

LUDOVIKA
EGYETEMI KIADÓ

Tartalom

A tanulmánykötet szerzői

Balatonyi László: osztályvezető, Települési Vízgazdálkodási Osztály, Országos Vízügyi Főigazgatóság; adjunktus, NKE Víztudományi Kar Víz- és Környezetbiztonsági Tanszék

Balogh Balázs: okleveles építőmérnök, FCSM

Bana Zsolt: okleveles térképész

Bene Viktória: PhD-hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, Katonai Műszaki Doktori Iskola; Honvédelmi Minisztérium Hatósági Főosztály

Cimer Zsolt: egyetemi docens, oktatási dékánhelyettes, tanszékvezető, NKE Víztudományi Kar Víz- és Környezetbiztonsági Tanszék

Hábermayer Tamás: tűzoltó ezredes, megyei igazgatóhelyettes, Tolna Megyei Katasztrófavédelmi Igazgatóság

Hegyi Zoltán: környezetvédelmi albizottság-vezető, MAÚT; ügyvezető igazgató, VIKÖTI Kft; vezető tervező

Hetesi Zsolt: egyetemi docens, NKE Víztudományi Kar, Víz- és Környezetbiztonsági Tanszék

Kozák Péter: okleveles építőmérnök, igazgató, Alsó-Tisza-vidéki Vízügyi Igazgatóság

Márton Attila: okleveles építőmérnök, csoportvezető, Közép-Duna-völgyi Vízügyi Igazgatóság Vízgyűjtő-gazdálkodási Csoport

Máthé Katalin: tudományos munkatárs, NKE Víztudományi Kar Víz- és Környezetbiztonsági Tanszék

Mrekva László: mesteroktató, NKE Víztudományi Kar, Víz- és Környezetbiztonsági Tanszék

Nagy Zoltán András: egyetemi docens, NKE Rendészettudományi Kar Bűnügyi, Gazdaságvédelmi és Kiberbűnözés Elleni Tanszék

Rácz Tibor: okleveles építőmérnök, PhD-hallgató

Nagy Zoltán András

Kibertámadások víziközművek ellen

Bevezetés

A víz napjaink, életünk alapfeltétele, stratégiai elem. A lakosság vízfogyasztása mellett sok szektor tevékenységéhez nélkülözhetetlen. Természetessé és ezzel láthatatlanná vált, ahogy az lenni szokott. Értékét, jelentőségét akkor fedeztük fel, amikor hiánya, a vízellátás problémái realitássá váltak.

Az 1992-ben született dublini elvek leszögezték, hogy „a víznek valamennyi versengő felhasználásában gazdasági értéke van, és gazdasági jószágként kell elismerni" [1].

Az elmúlt évek trendje, hogy a természetet, annak elemeit gazdasági értékkel (természeti tőkével) ismerik el annak érdekében, hogy megvédjék és megőrizzék nemcsak a mai, hanem a jövő nemzedékek számára is. A természeti tőke a fizikai természeti javak állománya – egyszerűen minden, amit a természet ingyen ad nekünk, például a víz, a talaj, az erdők és a biológiai sokféleség [2].

Ahogy a 2021. évi víz világnapját méltató weboldal összegzi: „a víz értéke sokkal több, mint az ára – a víznek óriási és összetett értéke van háztartásaink, kultúránk, egészségünk, oktatásunk, gazdaságunk és természetes környezetünk épsége szempontjából. Ha figyelmen kívül hagyjuk ezen értékek bármelyikét, azt kockáztatjuk, hogy rosszul kezeljük ezt a véges, pótolhatatlan erőforrást." [3]

Az iparágak folyamatos fejlődéséhez növekedésre orientált, fogyasztásra kényszerített, túlnépesedett világunkban egyre több vízre van szükség. Ezzel szemben a nagyipari és mezőgazdasági környezetszennyezés, valamint az ipari-nagyüzemi felhasználókra és az egyéni felhasználókra egyaránt jellemző pazarló vízgazdálkodás miatt az édesvíz egyre korlátozottabb mennyiségben és minőségben áll rendelkezésre, ami rendkívüli nyomást jelent az ágazatnak. A víziközművekre és vízügyi igazgatóságokra komoly kötelezettséget ró a működés biztonságának megteremtése a vízkivételtől a szennyvíz kezeléséig.

A víz a mai technikai-technológiai fejlettségnek köszönhetően megbízhatóan tisztítható, újrahasznosítható, a fogyasztók felé eljuttatható, a keletkezett szennyvíz elvezethető. A jogszabályban meghatározott fizikai, kémiai, bakteriológiai,

biológiai, toxikológiai és radiológiai határértékeknek megfelelő minőségű víz szolgáltatása a víziközművek felelőssége.

A kor technikai követelményeivel lépést tartva a növekvő igények kielégítéséhez, a működési költségek – legalább – szinten tartásához, az ügyfelek kiszolgálása, az adminisztratív tevékenységek modernizálása céljából és nyilván más okok folytán is, a víziközmű-vállalatok jelentős digitális fejlesztéseket hajtottak végre az elmúlt évtizedekben.

A digitális adatátvitel egyben megteremtette annak lehetőségét, hogy a vállalaton belül a telephelyek, ügyfélirodák, laboratóriumok és más egységek összekapcsolódjanak, a sokszor bizonytalan, netán akadozó analóg telefonkapcsolat helyett stabil, folyamatosan megbízható minőségű kommunikációra nyílt lehetőség.

Ugyanakkor – kifelé – kiterjedt kapcsolatrendszer épült ki egyfelől az államigazgatás különböző szerveivel, a pénzügyi szférával, a meteorológiai intézetekkel, felhőszolgáltatókkal és másokkal, másfelől az ügyfelek is elérhetik a vállalat szervereit. Tehát a hozzáférési pontok a veszélyeztetettek.

A víziközmű-vállalatok, vízügyi igazgatóságok valós térbeli üzemi tevékenységének integráns részei a virtuális térben zajló folyamatok, ezáltal veszélyeztetettségük is növekedett, több irányból, különböző védelmi szinten levő tevékenységek, részlegek védelmét kell megoldani.

A víziközműveket érintő kiberfenyegetettség és -biztonság

Korábban a víziközműveket a valós térből potenciálisan fenyegető – jellemzően rongálásban megmutatkozó – támadásoktól kellett óvni, azok fizikai védelmére kellett komoly figyelmet fordítani. Ez természetesen ma is elengedhetetlen követelmény. A védművek veszélyeztetői a magányos elkövetőktől (ittas, garázda személyek, elbocsátott dolgozók, a védművek építkezései ellen tiltakozók stb.) az emberi életet sem kímélő és különösen nagy kárt okozó terroristákig terjedhetnek.

A valós térbeli cselekmények köre és elkövetőik viszonylag jól behatárolhatók a védművek rongálásától, amely rendkívül veszélyes árvizek idején, az ivóvíz mérgezésén át (a 13. században a tatárok ellen alkalmazták önvédelemként; a régi magyar jogban a „kútmérgezés” sokáig büntetendő cselekmény volt) a vízellátás megzavarásáig.

Az állam biztonsága, az állampolgárok jóléte, a gazdasági-társadalmi folyamatok zavartalansága, az egyéni felhasználók tevékenysége védelmének alapkövetelménye a kiberbiztonság [4 p69–72]. Ennek hiánya nem csupán elbizonytalaníthat a modern technikai eszközök, applikációk és megoldások alkalmazásában, hanem hatásai felmérhetetlenek, jelesül a demokráciát és annak értékeit kockáztatják.

A cselekmények kriminológiai ismérve az is, hogy a kiberfenyegetések gyakran profitérdekből elkövetett bűncselekmények, azok egyre gyakrabban politikai, stratégiai motivációjúak. Egyre gyakrabban terrorszervezetek és államilag támogatott terroristák hajtják végre nemtelen cselekményeiket.

Kriminalisztikai tapasztalat az, hogy a kiberbűnözés és a „hagyományos" bűnözés közötti határ elmosódik, mivel a bűnözők az internetet, a digitális eszközöket használják tevékenységeikhez, valamint a digitális környezet az új módszereket és eszközöket tálcán kínálja a bűncselekmények elkövetéséhez. Lehetséges, hogy bármely bűncselekménnyel összefüggésbe hozott bizonyítékok elektronikus formában állnak rendelkezésre számítógépes rendszerekben, adathordozókon, mobileszközökön, és azok tartalmát, integritását a büntetőeljárás során a nyomozó hatóság és a védelem érdekei miatt biztonságosan meg kell őrizni.

Napjainkban a víziközművek és vízügyi igazgatóságok a virtuális térből is támadhatók. A támadás veszélyességét fokozza, hogy az bármikor, bárki által, bárhonnan elkövethető. Az IP-címek leplezésének technikái miatt akár egy „szomszéd épületből" is indítható a támadás. Lássunk néhány tipikus támadástípust.

„Elektronikus betörés" (hacking)

A számítógépes rendszer közvetlen, az adatállomány közvetett veszélyeztetésének legkorábbi stádiuma. Az ilyen cselekmény a Büntető törvénykönyv 423. §-ába ütköző információs rendszer vagy adat megsértése bűncselekménye (1) bekezdése szerint minősülhet.

A védett adatállományokhoz való jogosulatlan hozzáférés következtében az ott kezelt adatok megismerhetők, megszerezhetők (lemásolhatók), azok részben vagy egészben megváltoztathatók (kiegészíthetők, felülírhatók, részben törölhetők), teljességükben törölhetők, az elért adatállomány átrendezhető, amelynek eredményeképpen az nem vagy másképp értelmezhető. Az ilyen

cselekmények a Büntető törvénykönyv 423. §-ába ütköző információs rendszer vagy adat megsértése bűncselekménye (2) bekezdésének b) pontja szerint minősülhetnek.

Profi hacker a dark weben bérelhető (Cr2Cr, Criminals to Criminals, bűnözők a bűnözőkkel ügylet keretében). A megszerzett személyes adatok, különösen a nevek, e-mail-címek, bankszámlaszámok is „piacképes áruk". 2020 januárjában az Egyesült Államokban a Greenville Water bejelentette, hogy célzott kibertámadást szenvedett, amely 500 000 ember munkabérének utalására, online kifizetésére volt hatással [5]. Ebben a hónapban a michigani Detroit Víz- és Csatornázási Osztály 300 fiókjának ügyfélérzékeny információi kerültek nyilvánosságra [6].

Az „elektronikus betörés" további valós veszélye az, hogy lehetőség nyílik a számítógépes rendszer működését befolyásoló, szabotáló malware-ek feltöltésére, megosztására.

Jogosulatlan felülírás (defacing)

Az „elektronikus betöréssel" megnyílik a lehetőség a vízügy weboldalának jogosulatlan felülírására *(defacing)* is. Hamis hírek, sőt rémhírek tölthetők fel a víziközművek tevékenységéről, valóságos vagy nem létező árvizekről, azok következményeiről, a víz minőségéről, mérgezéséről, és más lejáró tartalmak jeleníthetők meg.

Az adathalászat (phishing)

Az adathalászat felöleli a dolgozók, alkalmazottak személyes és a rendszer eléréséhez szükséges adatainak, továbbá a vállalat pénzügyi-gazdasági, technológiai információinak, valamint valamennyi munkavállalónak a munkáltatónál kezelt személyes adatainak tiltott megszerzését.

Az adathalászat céljára – mára – különféle csalárd e-mailek ismertek. Nézzük a legismertebbeket:

- BEC (Business E-mail Compromise) – a vállalat vezetője, a társintézmény, a társszerv nevében érkezik az e-mail, amelyre az alkalmazott, dolgozó jellemzően ellenőrzés nélkül, kvázi „szolgaian" válaszol. A kért információkat szinte „automatikusan" közli a megkereső féllel.

- A Spear Phishing (szigonyozás) meghatározott felhasználói kört (vezetőt, döntési pozícióban, információk birtokában lévő stb. személyt) vesz célba.
- Whaling – kifejezetten felső vezetőket megkereső e-mail.

A víziközművek, igazgatóságok dolgozóinak, alkalmazottainak e-mailes megkeresését megkönnyítik a vállalati ismertetők, továbbá az interneten közölt elérhetőségek, ahol a dolgozók, alkalmazottak, vezetők e-mail-címei, telefonmellékei elérhetők.

Az adathalászat másik ismert módszere a *social engineering.* Jellemzően a felhasználóval már meglévő vagy később kialakított bizalmi viszony kihasználásával történik. A személyes kapcsolat kialakítása a dolgozóval, az alkalmazottal, az ajándékokkal elhalmozás, érzelmi, szexuális viszony kezdeményezése, netán házasság ígérete vagy más típusú kapcsolat kihasználásának egyetlen célja van, ez pedig a számítástechnikai rendszerbe belépést biztosító adatok megszerzése. Lehetséges az is, hogy az elkövető számítógép-szerelőnek kiadva magát javítás színlelésével elkéri a dolgozó, alkalmazott belépési adatait.

Az adathalászat kapcsán említeni kell azon e-mailes visszaéléseket, amelyek ugyan kívül esnek a vízügyi igazgatóság hatáskörén, ám az ügyfeleket érinthetik. Az ügyfelek az e-mail-címükre kaphatnak olyan hamis leveleket, amelyek ki nem fizetett tartozásról, annak befizetéséről tájékoztatnak, a befizetés elmaradása esetében pedig szolgáltatáskorlátozással fenyegethetnek. Majd a tartozás kifizetésére egy hamis számlaszámot közölnek, amely nem a vízügyi igazgatósághoz, hanem a bűnözőkhöz köthető. Általában ezek nem túl jelentős összegek, pár ezer forintos (pár tíz eurós) követelésekről van szó, és a kis összegekre tekintettel a gondatlan felhasználó befizeti azt. Az ilyen cselekmények a Büntető törvénykönyv 373. §-ába ütköző csalás bűncselekményének minősülhetnek.

Az ügyfelek megtévesztésére alkalmas e-mailek kapcsán a víziközművek, vízügyi vállalatok adatvédelmi kötelezettségére kell a figyelmet felhívni, azaz semmilyen személyes vagy vállalati (pénzügyi-gazdasági-technológiai) adat ne szivárogjon ki a számítástechnikai rendszerből.

Az adatszivárgások (adatvesztések) tipikus okai lehetnek:

- a vállalati számítástechnikai rendszer fizikai vagy logikai biztonságának hiányosságai, gyenge védelmi rendszer;
- a fentebb említett hackertámadás, amelynek kifejezett célja az adatszerzés;
- valamely adathalász technika (például a *social engineering*) csapdájába került dolgozótól, alkalmazottól a belépési adatok megszerzése, amelynek

a következménye a vállalat védett adatállományához való hozzáférés lehetőségének a megteremtése;

- „cselédbosszú" *(maid's revenge),* az elbocsátott, elégedetlen dolgozók, alkalmazottak „bosszúból" többféle kárt okozhatnak (volt) munkáltatójuknak, így például belépési kódokat, majd az ott dolgozók személyes adatait, egyéb vállalati információkat jogtalanul megszerezhetnek, azokat törölhetik, illetéktelen személyek számára – anyagi előnyért vagy anélkül is – hozzáférhetővé tehetik;
- gondatlanságból vagy véletlenekből is származhatnak nagyon súlyos jogsértések, károk (adatvesztések), így valamely, a dolgozó, alkalmazott által munkavégzésre használt laptop, más adathordozó elvesztése; e-mail-cím elírásából illetéktelen személyhez kerülhetnek adatok; fokozottabb az önhiba lehetősége, ha a dolgozó, alkalmazott a vállalat számítógépéhez saját adathordozóját csatlakoztatja, amely viszont malware-rel fertőzött is lehet.

A rosszindulatú programok (malware-ek)

A rosszindulatú programokkal intézett támadások többféle hátrányt okozhatnak a számítástechnikai rendszerekben, a felhasználók számítógépeiben, mobiltelefonjaiban. Jellemzően az alábbi módokon kerülhetnek a dolgozók, alkalmazottak eszközeire:

a) külső adattárolóról töltik fel, például saját otthoni pendrive-ukat használják a munkahelyen, és ezen a pendrive-on fertőzött fájl található;

b) letöltik a rosszindulatú fájlokat az internetről, akár a munkahelyen, akár otthoni munkavégzés vagy privát tevékenységük során (böngészés, különböző játékok, applikációk, zenék, filmek és más fájlok letöltögetésével, fertőzött bannerre klikkeléssel, e-mailhez csatolt vagy alkalmazásfájlok [.exe, .bat, .com] kibontásával, telepítésével vagy szövegfájlok [.doc, .docx] megnyitásával) telepíthetik a gépeikre. Ez utóbbiak, az úgynevezett emotet-malware-ek a legújabb támadásfajta.

Biztonsági okokból a vállalati laptopokra letöltögetést ki kell zárni.

A malware-ek fajtái között vannak olyan vírusok, amelyek az adatállományok tartalmát megváltoztathatják (felülírhatják), részben vagy egészben törölhetik,

a memóriáját telíthetik, a számítógép működését (indítását stb.), programját befolyásolhatják, és más károkat okozhatnak.

Az ilyen cselekmények a Büntető törvénykönyv 423. §-ába ütköző információs rendszer vagy adat megsértése bűncselekménye (2) bekezdésének b) pontja szerint minősülhetnek.

A zsarolóvírus (ransomware)

Napjaink egyik legveszélyesebb kibertámadás-fajtája a zsarolóvírus [7], amely a számítógépen, mobiltelefonon levő adatállományt (fájlokat, könyvtárakat) titkosítja, azokat mintegy „túszul ejti", aminek a következménye az, hogy a dolgozó, alkalmazott sem fér hozzá a munkavégzéséhez szükséges fájlokhoz. A bűnelkövetők a titkosítás feloldását pénzösszeg megfizetésétől teszik függővé. Az elkövető kilétének megismerése sokszor lehetetlen. A „váltságdíjat" virtuális valutában követelik. A pénz kifizetése sem garancia arra, hogy a zsaroló a titkosítást feloldja. Előfordulhat, hogy a váltságdíj fejében a titkosított adatállomány egy részét ismét elérhetővé teszi, majd további követelésekkel áll elő – ha egyáltalán jelentkezik az elkövető a pénz megszerzése után.

A vállalati (és az otthoni) számítástechnikai, mobileszközök használatakor a zsaroló- és más rosszindulatú programok veszélyére is fel kell hívni a figyelmet. Egy malware-támadás miatt 2017 januárjában az angliai Lincolnshire-ben négy napra leállították a víziközművet, a leállás 1 millió font kárt okozott [8]. Az orosz bűnözők által írt Kelihos malware napi 3,8 milliárd spam-e-mail küldésére volt képes, amelyek között zsarolóvírusok, illetve botnetvírusok is voltak [9].

A zsarolóvírus veszélyességére példa az az eset, amely 2016-ban az Egyesült Államokban a Lansing Board of Water and Light vízügyi vállalattal történt. Egy spear-phishinggel támadták egyik munkatársát, akinek a figyelmetlensége zsarolóvírust szabadított a rendszerbe. A fertőzött számítógépek és szoftverek cseréje 10 millió dollárba került, és további 2,4 millió dollár volt a helyreállítás költsége [10].

Ismertek olyan rosszindulatú programok is, amelyek meghatározott szerver ellen, meghatározott tevékenység szabotálására születtek, ilyen a Stuxnet és DuQu. A Stuxnet a natanzi (Irán) atomerő urándúsításának szabotálására íródott, és sikeresen alkalmazták [11].

Robot-network-vírusok

A robot-network-vírusok egy másik veszélyes támadásfajtához, a túlterheléses támadás végrehajtásához szükségesek. A túlterheléses DoS- és DDoS-támadások célja számítógépes szolgáltatások, hálózatok, rendszerek olyan mérvű terhelése, amely ellehetetleníti azok működését. A botnetvírus hálózatba fogja a zombi-számítógépek (tíz)ezreit, amelyek egy parancsra egyszerre fognak kapcsolatot teremteni a megcélzott szerverrel. A túlterheléses támadást anyagi haszonszerzés céljából indítják. Az ilyen cselekmények a Büntető törvénykönyv 423. §-ába ütköző információs rendszer vagy adat megsértése bűncselekményének minősülhetnek.

Megjelent a virtuális térben a valós térben már ismert „védelmi pénz" követelése is. Ebben az esetben egy kilátásba helyezett túlterheléses támadás végre nem hajtása fejében pénzt, általában virtuális valutát (bitcoint, ethereumot vagy egyéb altcointot) követelnek a célzott szerver tulajdonosától, üzemeltetőjétől. E támadástípus kiemelésének az az indoka, hogy ezen támadások, illetőleg az ezzel való fenyegetések „hathatós célpontjai" azok a szerverek, amelyeknek folyamatos (0–24 órás) működéséhez nemzetgazdasági, honvédelmi, energetikai, pénzügyi vagy más komoly érdek fűződik. A víziközművek ebbe a kategóriába tartoznak. Az ilyen cselekmények a Büntető törvénykönyv 367. §-ába ütköző zsarolás bűncselekményének minősülhetnek.

Man-in-the-Middle-támadás

A hálózati támadás egyik fajtája az úgynevezett Man-in-the-Middle-támadás, amelynek lényege az, hogy az ügyfél és a szolgáltató közötti kommunikációba egy harmadik fél jogellenesen kapcsolódik be, és a szolgáltatónak adja ki magát, az ő nevében kéri el a személyes adatokat, befizetéseket, és más tiltott tevékenységeket végezhet.

A számítástechnikai rendszer manipulálása

Potenciális veszélyt jelent az ügyfelek részéről a befizetések manipulálása, csalás esetében az elektronikus adatfeldolgozás és -átvitel folyamatába történő jogosulatlan beavatkozás.

A számítástechnikai rendszerben történő manipulációk változatos formát ölthetnek:

- az ügyfél mint elkövető maga vagy egy másik ügyfél számlájára fiktív befizetéseket végez;
- az ügyfél mint elkövető önmaga vagy egy másik ügyfél tartozásának összegét csökkenti;
- az ügyfél mint elkövető egy másik valódi vagy fiktív ügyfélként azonosítja magát;
- az ügyfél önmaga vagy egy másik ügyfél ügyfélprofil mivoltát megszünteti, törli a rendszerből.

Az ilyen cselekmények a Büntető törvénykönyv 375. §-ába ütköző információs rendszer felhasználásával elkövetett csalásnak minősülhetnek.

A víziközművek lehetséges támadói

A víziközművek támadásának az alábbi elkövetői lehetnek:

a) Az egyik csoport az elégedetlen vagy elbocsátott munkavállalók, alkalmazottak, akik ismerik, használják/használták a számítástechnikai rendszert, az azokhoz tartozó belépési azonosítókat, a rendszer működésében a loophole-okat, amelyeket felfedeztek, vagy amelyeket csak bennfentes információ birtokában levő tudja. Ezen ismeretekkel munkaadóiknak, volt munkaadóiknak kárt tudnak okozni. Cselédbosszú *(maid's revenge)* az elnevezése a szakirodalomban ennek az elkövetési formának.

b) A „magányos farkasok" gyakori elkövetői különböző valós és virtuális térbeli bűncselekményeknek. Ők azok, aki előlépnek az ismeretlenségből, felderítésüket megnehezíti az a tény, hogy előéletük ismeretlen, szervezethez nem kapcsolódnak, cselekményük kiszámíthatatlan. Példaként említhetjük a floridai víztisztítótelep megmérgezését tervező magányos hackert 2021-ből [12].

c) A terroristák, akik hadüzenet nélkül, a legváratlanabb helyeken, szituációkban, aljas céljaiktól vezéreltetve hajtják végre gonosztetteiket. A víziközművek, amelyek az egyik legfontosabb népgazdasági tevékenységet látják el, különösen veszélyeztetett célpontok. A terroristatámadások mind a valós térben, mind a virtuális térben jelentkezhetnek. Valós térben a fegyveres, robbantásos vagy vegyi, biológiai, radiológiai és nukleáris

(CBRN-) támadások történhetnek. A virtuális térbeli támadásra példa a Kemuri Water Co. elleni támadás, amikor egy szíriai csoport manipulálni próbálta az ivóvíz vegyszeradagolását 2016-ban [13].

A kibertámadások elleni védekezés lehetőségei

Az ISO-27001 szabvány [14] hasznos kiindulópont a víziközművek számára. Ez szabályozza az információbiztonsági felügyeleti rendszer (ISMS) specifikációját. Az ISO-27001 bevált módszerei segíthetik a szervezeteket információbiztonságuk kezelésében az emberek és folyamatok, valamint a technológia terén is.

A védekezés legfőbb alapja a dolgozók, alkalmazottak fizikai biztonsága, a számítástechnikai rendszerek magas szintű fizikai és logikai védelme. A dolgozókat, alkalmazottakat fel kell készíteni a digitális környezet veszélyeire, a kiberfenyegetésekre. Tudatosítani kell felelősségüket a számítástechnikai eszközök alkalmazása során, az ő felkészületlenségük, gondatlanságuk sodorhatja veszélybe a vállalatot, annak tevékenységét, termékeit, szolgáltatásait.

Felhasznált irodalom

1. The Global Development Research Center [Internet]. The Dublin Statement on Water and Sustainable Development [cited 2021 Sep 22]. Available from: www.gdrc.org/uem/water/dublin-statement.html
2. Capitals Coalition [Internet]. How do we value water?; 2017 Jan 13 [cited 2021 Sep 22]. Available from: https://capitalscoalition.org/how-do-we-value-water/
3. World Water Day [Internet]. Celebration World Water Day 2021 [cited 2021 Sep 22]. Available from: https://archive.worldwaterday.org/2021/
4. Haig Zs, Várhegyi I. Hadviselés az információs hadszíntéren. Budapest: Zrínyi Kiadó; 2005. 286 p.
5. Dornfeld L. A kiberbűnözés elleni küzdelem kihívásai. Diskurzus. 2015;5 (különszám):27–35. Elérhető: https://epa.oszk.hu/02200/02234/00012/pdf/EPA02234_Diskurzus_2015_ksz_27-35.pdf

6. Cyware Social [Internet]. Water utilities face incresing risk of cyberattacks; 2020 May 19 [cited 2021 Sep 22]. Available from: https://cyware.com/news/water-utilities-face-increasing-risk-of-cyberattacks-37a1d084
7. Mezei K, Nagy ZA. A zsarolóvírus és a botnet, mint napjaink két legveszélyesebb számítógépes vírusa. In: Gaál Gy, Hautzinger Z, szerkesztők. Szent Lászlótól a modernkori rendészettudományig. Pécs: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja; 2017. p. 155–163.
8. Open Access Government [Internet]. Malware ransom of £1m for Lincolnshire County Council; 2016 Febr 1 [cited 2021 Sep 22]. Available from: www.openaccessgovernment.org/malware-ransom-1m-lincolnshire-county-council/24093/
9. The United States Department of Justice [Internet]. Russian national convicted of charges relating to Kelihos botnet; 2021 June 16 [cited 2021 Sep 22]. Available from: www.justice.gov/opa/pr/russian-national-convicted-charges-relating-kelihos-botnet
10. Palmer K. BWL paid $25,000 ransom after cyberattack. Lansing State Journal [Internet]. 2016 Nov 8 [cited 2021 Sep 22]. Available from: https://eu.lansingstatejournal.com/story/news/local/2016/11/08/bwl-paid-25000-ransom-after-cyberattack/93488502/
11. Cserháti A. A Stuxnet vírus és az iráni atomprogram. Nukleon [Internet]. 2011 [letöltve 2021. szeptember 22.];4(85):1–7. Elérhető: https://nuklearis.hu/nukleon/stuxnet-virus-es-az-irani-atomprogram
12. In Florida city, a hacker tried to poison the drinking water. The Detroit News [Internet]. 2021 Feb 8 [cited 2021 Sep 22]. Available from: https://eu.detroitnews.com/story/news/nation/2021/02/08/florida-water-treatment-hack-lye/115453008/
13. Leyden, John: Water treatment plant hacked, chemical mix changed for tap supplies. 2016 Mar 24 [cited 2021 Sep 22]. Available from: www.theregister.com/2016/03/24/water_utility_hacked/
14. SGS [Internet]. Egészség és biztonság. ISO/IEC 27001:2013 – Információbiztonsági irányítási rendszer [letöltve 2021. szeptember 22.]. Elérhető: www.sgs.hu/hu-hu/health-safety/quality-health-safety-and-environment/risk-assessment-and-management/security-management/iso-27001-2013-information-security-management-systems?gclid=Cj0KCQjwqp-LBhDQARIsAO0a6aLQNdUZ1aKBtKQsu01FMPoJrgTSJZBE1ooFRrN1ZJZcsfapu2Kc9EEaAodzEALw_wcB#