CORPORATE SECURITY AND THE DARK WEB

VÁLLALATBIZTONSÁG ÉS A DARK WEB

GULYÁS Attila[1]

Abstract

The changes that have taken place in recent decades have posed significant challenges to companies. Responses to new challenges have not only yielded positive results, but there have also been new risks to which companies need to provide new types of responses. New tools and technologies that appeared in the field of information technology revolutionized production technologies, and the role of information as a corporate asset increased. This wealth is threatened by new, unprecedented risks, such as the growing use of Dark Web technology, which, with the anonymity it provides, challenges corporate security professionals who can only meet the challenges with special training and preparedness. The aim of the study is to highlight the possible meeting points between information security and the Dark Web.

Keywords

security,dark web,information asset, crypto currency, hacker

Absztrakt

Az elmúlt évtizedekben a környezetünkben lezajlott változások jelentős kihívások elé állították a vállalatokat. Az új kihívásokra adott válaszok nem csak pozitív eredménnyel jártak, hanem új kockázatok is jelentkeztek, amelyekre a vállalatoknak új típusú korábban nem alkalmazott válaszokat kell adniuk. Az informatikai területén megjelent új eszközök, technológiák forradalmasították a termelési technológiákat, az információ mint vállalati vagyon szerepe felértékelődött. Ezt a vagyont olyan új, eddig nem látott kockázatok fenyegetik, mint az egyre elterjedtebb Dark Webes technológia, amely az általa biztosított anonimitással kihívás elé állítja a vállalati biztonsági szakembereket, akik csak speciális képzettséggel és felkészültséggel tudnak megfelelni a kihívásoknak. A tanulmány célja, hogy rávilágítson az információbiztonság és a Dark Web lehetséges találkozási pontjaira.

Kulcsszavak

biztonság, dark web, adatvagyon, kriptovaluta, hacker, darknet piac

[1] agulyas66@gmail.com | ORCID: 0000-0001-5645-144X | Retired military officer, PhD student, Óbuda University Doctoral School on Safety and Security Sciences | nyugállományú hivatásos katona, doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

Az elmúlt évtizedekben a környezetünkben lezajlott változások jelentős kihívások elé állították a vállalatokat. Az új kihívásokra adott válaszok nem csak pozitív eredménnyel jártak, hanem új kockázatok is jelentkeztek, amelyekre a vállalatoknak új típusú korábban nem alkalmazott válaszokat kell adniuk. Az informatikai területén megjelent új eszközök, technológiák forradalmasították a termelési technológiákat, az információ mint vállalati vagyon szerepe felértékelődött. Ezt a vagyont olyan új, eddig nem látott kockázatok fenyegetik mint az egyre elterjedtebb Dark Webes technológia, amely az általa biztosított anonimitással kihívás elé állítja a vállalati biztonsági szakembereket, akik csak speciális képzettséggel és felkészültséggel tudnak megfelelni a kihívásoknak. A tanulmány célja, hogy rávilágítson az információbiztonság és a Dark Web lehetséges találkozási pontjaira.

VÁLLALAT ÉS INFORMÁCIÓS VAGYON

Az elmúlt évtizedekben a környezetünkben lezajlott változások következtében jelentős változásokon mentek át hazánkban a vállalatok [1].

Említés szintjén néhány a kihívások közül:

- A határokon átívelő globalizáció új felfogást és szemléletet követel meg
- A tudásalapú társadalomban megnőtt a szerepe a szellemi tőkének
- A vállalati informatikai rendszereknek szervesen kell kapcsolódniuk nemzetközi hálózatokba, a világhálóba és annak felismerése, hogy a hagyományos papír alapú irodai munka egyre inkább elektronikussá válik annak előnyeivel és hátrányaival

Ezekre a kihívásokra adott válaszok azonban nem csak pozitív eredményeket hoztak, nem csak a hatékonyságot és az eredményességet növelték, hanem új kockázatokkal is járnak. A vállalatirányításnak ezekre az új fenyegetésekre is meg kell találniuk a választ.

A vállalatokat valamilyen feladatra hozzák létre. Ez a vállat tevékenységének alapja, létrehozásának értelme. Ebben a vonatkozásban nem fontos, hogy az adott vállalat kereskedelmi vagy más egyéb céllal került-e létrehozásra.

A vállalat küldetése tulajdonképpen annak a megjelenítése, hogy a vállalat ezt a célt milyen módon kívánja teljesíteni. A küldetésében tükröződnie kell a működési területének, belső működési elveknek, a külső gazdasági környezettel kiépítendő kapcsolatoknak.

A fentiekből következik, hogy az üzleti követelményeknek kell alárendelni minden vállalaton belül végbemenő tevékenységet, amelyek az üzleti cél elérése érdekében szükségesek.

A COBIT kocka alapján az alábbi üzleti követelményekről beszélhetünk:

- Minőség: magas színvonal, gazdaságosság, időbeni teljesítés
- Megbízhatóság: hatékonyság, kiszámíthatóság, jogszabályi megfelelőség
- Biztonság: bizalmasság, sértetlenség, rendelkezésre állás (MSZ ISO/IEC 27001)

A tanulmány szempontjából kiemelendő, hogy a biztonság üzleti követelmény, ebből adódóan az üzleti célok biztonság nélkül nem teljesíthetőek.

Az információbiztonság nem azonos az informatikai biztonsággal. Az előbbi egy tágabb szélesebb fogalom. Amíg az informatikai biztonság az informatikai rendszerek biztonságát jelenti az egyértelmű hozzáférés hitelesítéssel, tűzfalrendszerekkel, illetve vírusirtó szoftverek telepítésével, illetve futtatásával, addig az információs biztonság magába foglalja a vállalati adatvagyon védelmét beleértve a stratégiai partnerek, beszállítók, pénzügyi

partnerek részéről jelentkező esetleges nem szándékos fenyegetések elleni intézkedéseket is. A saját belső információk, a partnerek, ügyfelek adatai bizalmasságának, sértetlenségének és vagy rendelkezésre állásának sérülése anyagi, erkölcsi, reputációs és egyéb járulékos károkkal járhat, nem beszélve a törvényi kötelezettség megszegéséért járó büntetés, illetve szankció következményeiről. A vállalati információ vagyon védelme érdekében általánosságban az információ és információhordozók kezelése kerül szabályozásra. Ebből a szempontból érdektelen, hogy milyen az információ megjelenési formája. A helyes védelem érdekében meg kell határozni a védendő információkat, a lehetséges külső-belső fenyegetéseket, ezek bekövetkezésének valószínűségét és az ezek kivédéséhez szükséges szabályozást és eszközrendszert. (ISO/IEC 27002) [2].

Az információvédelem nem korlátozódhat az informatikai és ügyviteli rendszerek védelmére a védelmi intézkedéseknek ki kell terjedniük az adatok feldolgozására, kezelésére, átadására és tárolására, amely így már magában foglalja a fizikai biztonságot, a humán erőforrás biztonságát, a hozzáférés-jogosultságkezelést és az üzletmenet folytonos működésének biztosítását. Gyakori hiba, hogy a védelmi intézkedések szegmensenként kerülnek kidolgozásra és végrehajtásra ugyanakkor ez a megoldás nem hatékony, átfedések, hiányosságok alakulhatnak ki, amelyek ellen a rendszerszemléletű holisztikus megközelítésű komplex védelmi rendszer kialakítása jelenti a kiutat.

1. ábra: Információbiztonsági irányítási rendszer. Forrás: Oroszi (2014), Információbiztonsági stratégia és vezetés, Budapest: Nemzeti Közszolgálati Egyetem p.9.

Az 1. számú ábrán látható Információbiztonsági irányítási rendszer vázlatán jól látható, hogy a technológiai és az adminisztratív információbiztonsági intézkedések összehangolásával egymással összefüggő komplex rendszer alakítható ki. Egy ilyen rendszer kialakításával egy szervezet képes a védelmi intézkedések és kontrolok kialakítására és hatékony alkalmazására.

A rendszer alappillére az információbiztonsági politika, illetve egy megfelelő információbiztonsági stratégia kidolgozása és annak megvalósításáért felelős szervezet felállítása, továbbá a megfelelő irányítás, vezetés, valamint a hatékony működés figyelemmel kísérése és visszaellenőrzése.

A vállalti adatvagyon több területen is értéket teremthet, ezek a teljesség igénye nélkül az alábbiak lehetnek: [3]

- Hatékony üzleti döntéstámogatás: ügyfelek, termékeink, szolgáltatásaink és a versenytársak és piacaik jobb megismerésére, a saját pénzügyi folyamatok nyomon követésére, az emberi és egyéb erőforrások jobb és hatékonyabb kihasználására.

- Folyamat, termék és szolgáltatásoptimalizálás: a rendelkezésre álló adatvagyon birtokában lehetőség van a vállalati folyamatok, termékek és szolgáltatások optimalizálására. Ezáltal versenyképesebb termék vagy szolgáltatás előállítására, biztosítására

Néhány példa a konkrét felhasználásra:

- A gyártás: hibás termékek arányának csökkentése, minőségjavítás, intelligens leállás tervezés a gépek kopásának folyamatos figyelemmel kísérésével, anyag, eszköz, idő megtakarítás
- Üzleti folyamatok javítása, optimalizálása: adatalapú kockázatbecslés, csalás, visszaélés felfedése
- Raktározás, szállítás: szállítási útvonal optimalizáció, automatizált raktárkészlet, költség optimalizáció
- Értékesítés: ügyfélmegtartás, elvándorlás előrejelzés, személyre szabott termékajánlás, ügyfél elégedettség mérés stb..

A fenti felsorolás kellőképpen érzékelteti a vállalati adatvagyon jelentőségét, ebből adódóan ennek sérülése, elérhetetlenné tétele, vagy megváltoztatása a vállalati cél teljesítésének időleges, vagy akár szélsőséges esetben teljes meghiúsulását okozhatja, nem beszélve az esetleges erkölcsi kárról, amelynek mértéke esetenként felbecsülhetetlen és helyreállítása jóval több időt vesz igénybe, mint valamely fizikai káresemény.

A vállalati információvagyont a teljesség igénye nélkül az alábbi veszélyek fenyegethetik:

- hibás szoftveralkalmazások (sebezhetőségek, javító csomagok hiánya)
- szakszerűtlen információs technológiai tervezés, vagy üzemeltetés
- jogosulatlan hozzáférés, illetve használat
- meg nem engedett, ellenőrizetlen, vagy nem kompatibilis szoftverhasználat
- vírusok, kémprogramok, zsaroló programok
- a hálózat szándékos túlterhelése
- nem megfelelő archiválási politika
- felkészületlen személyi állomány
- szándékos belülről eredő, bennfentes személy támadása, károkozása
- szerződéses partner, együttműködő szándékos, vagy felelőtlen információkezelése

A tanulmány továbbiakban arra próbál választ adni, hogy a vállalati adatvagyont veszélyeztető fentebb felsorolt tevékenységek eredménye hogyan és milyen formában jelenhet meg a Dark Weben. Leginkább arra keresi a választ, hogy egy vállalatnak szükséges-e monitoroznia a Dark Webet, ha igen akkor azt saját erőből, vagy esetleg outsourcing útján más erre szakosodott vállalkozások szolgáltatásainak felhasználásával. Az erre vonatkozó döntésnek mik az előnyei és hátrányai, milyen tényezőket figyelembe venni a döntés meghozatalkor.

Mielőtt ez a kérdés részletes tárgyalásra kerülne elengedhetetlen, hogy az olvasó megismerkedjen a Dark Web lényegével és azon zajló – a tanulmány szempontjából releváns – folyamatokkal.

A DARK WEB

Mielőtt a Dark Web mibenlétének tisztázására sor kerülne néhány alapfogalom értelmezése elengedhetetlen. Még a szakirodalomban is előfordul, hogy az Internet és a World Wide Web fogalmát felcserélik, vagy egyiket a másikkal helyettesítik, holott az Internet tulajdonképpen hálózatok hálózatának bonyolult rendszere, míg a World Wide Web (a továbbiakban: WWW, vagy web) csak egyike a számos protokollnak, amelyeken keresztül a zajlik a kommunikáció az Interneten. Ez a nyelv a HTML nyelv, amelyet 1989-ben alkotott meg Tim Berners-Lee, majd 1990-ben megírta az első böngésző programot. Az internet böngésző 1991-ben indult el világhódító útjára [4, pp.32,33].

A Word Wide Web alapvetően három fő részre osztható fel. A könnyebb érthetőség érdekében a felosztást gyakran a jéghegy hasonlattal szoktak szemléltetni (2. ábra).

Az első rész a Nyílt Web, amelyre a „Clear Net", vagy „Surface Web", esetleg „Open Net" néven szokás hivatkozni. Ez a web arra a részére vonatkozik, amely bárki számára elérhető és hozzáférhető mindössze Internet hozzáférés, és valamilyen böngésző szükséges hozzá. Az ismert kereső motorok, mint „Google", vagy a „Bing" ezeket az oldalakat a robotjaik által bejárják, feldolgozzák, indexelik és a keresését indító felhasználó számára találatként visszaadják az oldal elérhetőségét. Ilyen típusú oldalból több milliárd érhető el és számuk napról napra növekszik.

A következő rész, amelyre valódi magyar kifejezést nem igazán alkalmaznak a „Deep Web", amely gyakorlatilag hasonló a Nyílt Web-hez, de az ebbe a kategóriába sorolható oldalak csak valamiféle belépési jogosultság ellenőrzést követően érhetők el. Ilyenek lehetnek vállalati adatbázisok, vagy hálózatok, egészségügyi adatok, vagy akár az olvasó email fiókja. Ezek az oldalak már alap esetben nincsenek nyilvántartva a kereső motorok adatbázisaiban, az oldalak tartalmára nem lehet rákeresni. Az ilyen típusú oldalból is ugyancsak több milliárd található szerte az világhálón.

Az előbbi két kategóriában közös vonás, hogy a felhasználók, a weboldalakat meglátogatók nyomon követhetők, viszonylag egyszerűen beazonosíthatók, tartózkodási helyük megállapítható.

Végül a harmadik rész a „Dark Web", Dark Net, vagy „Sötét Web". Ez az Internet olyan része, amely hagyományos eszközökkel már nem érhető el. Az itt tárolt tartalmak csak speciális böngészőkkel, kifejezetten erre a célra fejlesztett szoftverekkel érhetők el. Azonban ez a szegmens korántsem egységes, ugyanis több szoftver megoldás is létezik, amelyeknek a célja ugyan az nevezetesen: az anonimitás, a követhetetlenség és lenyomozhatatlanság biztosítása. Ezek alapján meg kell említenünk, a TOR [5] hálózatot, az I2p [6], a Freenet [7], vagy az egyébként magyar vonatkozással is rendelkező ZeroNet [8] rendszereket. Ezek a rendszerek egyenként mind egy részét fedik a Dark Webnek, és közöttük alapesetben nincs átjárhatóság.

Jelentős eltérés a nyílt Internettel szemben, hogy a Dark Weben nem működnek érdemi kereső motorok. Tekintettel arra, hogy ezek az oldalak a támadások kivédése érdekében általában valamilyen módszerrel blokkolják a közvetlen hozzáférést, amely lehet CAPTCHA, vagy regisztrációhoz kötött belépés a kereső robotok mint a már említett Google vagy Bing [9] nem tudják indexelni az oldal témáját illetve tartalmát.

A meglévő keresők leginkább a weboldalak készítőinek önkéntes regisztrációján, illetve a linkgyűjtemények alapján épített adatbázisokból építkeznek. Ez a körülmény jelentősen megnehezíti a Dark Web feltérképezését és a tájékozódást ebben a viszonylag új közegben.

Az alábbi ábra a World Wide Web felosztását szemlélteti, a már említett jéghegy hasonlat bemutatásával.

2. ábra: A World Wide Web felosztása. Forrás: https://www.webhostingsecretrevealed.net/wp-content/uploads/our-web.jpg

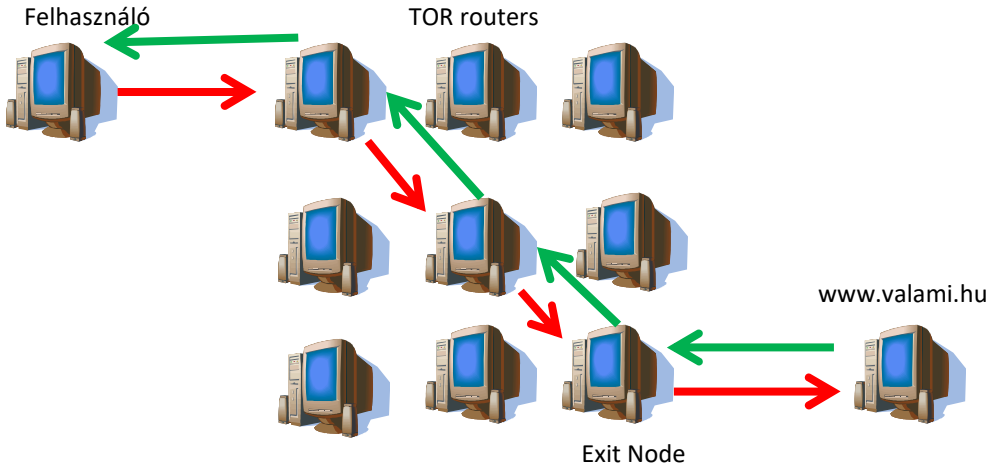
Eredetileg a Dark Web (a TOR rendszer elődje) egy rejtett réteg volt az 1970-es években az amerikai ARPANET hálózaton, és azzal a céllal hozták létre, hogy titkosított összeköttetést biztosítson az egyes munkaállomások között. A Dark Web tudott adatokat fogadni az ARPANET-től, de ugyanakkor láthatatlan maradt annak munkaállomásai számára. Időközben az ARPANET Internetté nőtte ki magát és a Dark Web bárki számára elérhetővé vált, mi több népszerűsége napról napra növekszik.

A Dark Web eléréshez a felhasználónak le kell töltenie és telepítenie valamelyik szoftvert a fentebb felsoroltak közül. Tekintettel arra, hogy az elérhető szoftverek közül a TOR rendszer rendelkezik a legnagyobb felhasználó táborral és a legtöbb úgynevezett rejtett szolgáltatással (a TOR rendszerben „hidden service”-nek nevezik a rendszer segítségével létrehozott weboldalakat), ezért ennek telepítése és használata javasolt. A továbbiakban a Dark Web megjelölés alatt ezt a rendszert takarja.

A TOR a The Onion Router kifejezés első betűiből összeállított mozaikszó. Az „onion router” kifejezés arra utal, hogy a TOR rendszeren belül az adatok a hálózat egyes elemi között titkosítva rétegesen egymásra építve kerülnek továbbításra és a köztes állomások egy titkosított réteget lefejtve jutnak hozzá a következő munkaállomás címéhez és oda továbbítják a megmaradt tikosított adatcsomagot. A következő állomás szintén lefejt egy réteget és ismét továbbítja a csomagot a következő routerhez, amíg csak el nem jut a célállomáshoz, ahol az utolsó réteget lefejtve megmarad az eredeti adat.[10] Ezzel a módszerrel megoldható, hogy a csomag eredete ismeretlen marad, és az egyes állomások nincsenek tudatában annak milyen adatot továbbítanak. A TOR rendszer kommunikációja természetesen jóval összetettebb, de jelen cikknek nem célja a működés részletekbe menő ismertetése. A rendszer egyik sajátságos vonása, hogy úgynevezett rejtett szolgáltatást (weboldalt)

bárki létrehozhat a rendszeren, anélkül, hogy bármilyen azonosító adatot hátrahagyna így a létrehozó kiléte, illetve földrajzi elhelyezkedése titokban marad [11]. A másik különlegesség, hogy a létrehozott weboldal alapesetben csak addig lesz elérhető a rendszeren, amíg a létrehozója a csatlakozik a rendszerhez, hiszen a weboldalt a számítógépén futó web szerverén hozta létre. Ennek köszönhető, hogy a Dark Webes oldalak fluktuációja óriási, ugyanis, ha a felhasználó kilép a rendszerből a weboldala elérhetetlenné válik. Természetesen léteznek a nyílt webhez hasonló tárhely szolgáltatók is a TOR rendszeren is, de az alapértelmezés az első eset.

A TOR rendszer másik sajátossága, hogy kialakításánál fogva lehetővé teszi a TOR rendszeren keresztül az Nyílt Internetes tartalmakhoz történő hozzáférést. A felhasználó a TOR rendszert elindítva a TOR böngészőn keresztül meglátogathat hagyományos weboldalakat, úgy hogy a kiléte a rendszer által biztosított anonimitás miatt gyakorlatilag azonosíthatatlan marad. A rendszer önkéntesek által működtetett úgynevezett „Exit Node" –okon keresztül csatlakozik a Nyílt Webhez. Egy ilyen „Exit Node" adott esetben több ezer TOR felhasználó kérését továbbítja az nyílt webes szolgáltatókhoz anélkül, hogy tudatában lenne annak a kérés honnan érdekezett és a válasz hová tart. A 2. ábra ezt a folyamatot ábrázolja. A képen látható nyilak a titkosított kommunikációt mutatják a felhasználó és a webszolgáltatás között.



3. ábra: A nyílt webes tartalom felkeresése a TOR rendszeren keresztül. Saját szerkesztés.

A Dark Web biztosította anonimitás kedvez a különböző bűnelkövetőknek, [12] akik a hatóságoktól való elrejtőzés és a biztonságos bűnelkövetés érdekében a bűncselekmények széles körét követik el a Dark Weben [12], [x3]. Ezek közül a legjellemzőbbek, a különböző fizetőeszközzel, vagy azt helyettesítő szolgáltatásokkal történő visszaélés, hamis dokumentumok, és személyazonosító okmányok forgalmazása, kábítószer és gyógyszer kereskedelem, beleértve a hamisított gyógyszerek forgalmazását is nem beszélve a fegyverkereskedelemről. Ezen felül különféle szolgáltatások is igénybe vehetők a hackerbérléstől kezdve a bérgyilkosságig, de akár migráns útvonalat is lehet vásárolni az érdeklődőknek.

A felsorolt bűncselekmények színtere általában valamelyik „Black Market", vagy más néven „Crypto Market" (a továbbiakban itt darknet piac), ahol a fizetőeszköz jellemzően valamely virtuális valuta, mint a Bitcoin, vagy a Monero [4, pp. 107-111]. A tanulmány szempontjából azonban két területet célszerű külön szemügyre venni. Egyik a már említett darknet piacok, a másik terület azok az oldalak és fórumok, chatszobák, Pastebin stílusú oldalak, ahol a kiberbűnözők árusítják termékeiket és szolgáltatásaikat, illetve kölcsönös információcserével fejlesztik eszközeiket, technikájukat, valamint módszereiket. A megvásárolható sérülékenységeknek, exploitoknak a már említett piacokon kívül dedikált oldalaik is vannak, ahol akár nulladik napi sérülékenységeket (0Day vulnerability), vagy különböző rendszerekhez exploitokat, lehet vásárolni részletes utasítással egyetemben.[4,pp.85-112] A fentieken túl beszélhetünk még az úgynevezett „Doxing" oldalakról. Ezek olyan tartalmakat takarnak, amelyek ismert személyek, „celebek", üzletemberek, politikusok magánéletével kapcsolatos bizalmas adatokat illegális úton megszerezve azokat nyilvánosságra hozva erkölcsi károkat okoznak, etikai szempontból rossz színben tűntetik fel az áldozatot. Az ilyen oldalak célja általában nem a közvetlen anyagi haszonszerzés, inkább valamiféle bosszú, vagy politikai indok állhat a háttérben.

A következőkben a könnyebb áttekinthetőség érdekében a hacker fórumok vagy dedikált hacker oldalak és a darknet piacok működésének néhány jellemző vonása kerül összehasonlításra.

Hacker fórumok	**Darknet piac**
Téma specifikus	Kialakítása hasonló az online áruházakhoz
Az árukínálat jellemzően csak informatikával, illetve informatikai bűncselekményekkel kapcsolatos	A kínálat változatos, a drogoktól kezdve a lopott telefonig gyakorlatilag bármi kapható. A vásárlók értékelhetik az eladókat és termékeiket
Fórumoktól függően ingyenes vagy fizetős tudás, eljárás, és technika megosztás	Biztosítékkezelő rendszer (csak a szolgáltatás teljesítését követően kapja meg az eladó az ellenértéket)
Ingyenes vagy fizetős illegálisan szerzett adatbázis letölthetőség	Változatos árukészlet általában drog, pénzügyi szolgáltatások, adatbázisok, sebezhetőségek, exploitok stb..
Az illegális módon szerzett adatokat az elkövető trófeaként kezeli és megosztja a közösséggel.	Egyszerű belépés, illetve regisztráció
A bejutás esetenként többszintű ellenőrzést követően lehetséges. Nem ritka, hogy a jelöltnek bizonyítania kell rátermettségét valamely bűncselekmény kategóriába tartozó feladat végrehajtásával.	Belső fórum a termékekkel és az eladókkal kapcsolatban

Hacker fórumok	Darknet piac
A sebezhetőségek, technikák módszerek a legfrissebbek lehetnek	A piacon árusított technikák és sebezhetőségek leginkább már a speciális fórumokon feldolgozott, esetleg már a IT biztonsági szervek által is ismertek
Zárt közösség	Nyitott közönség

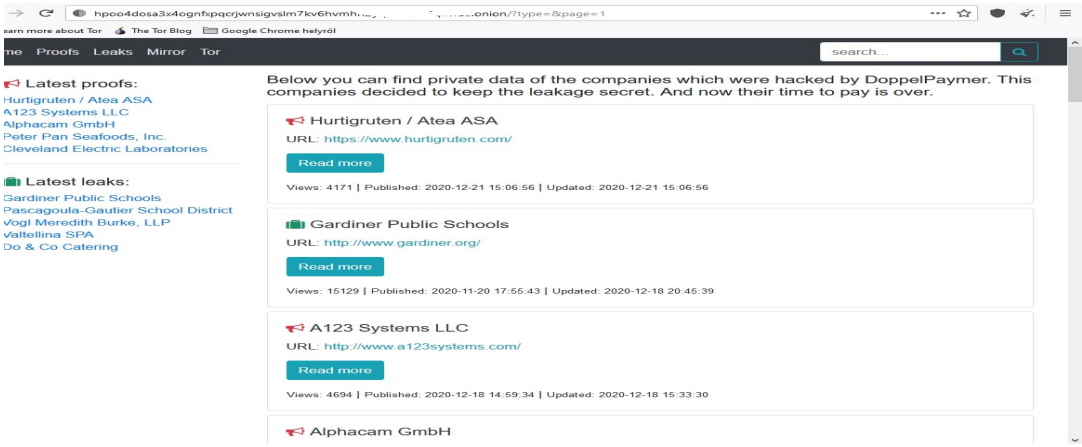
1. táblázat: A hacker fórumok és a darknet piacok összehasonlítása. Saját szerkesztés.

AZ ADATOK SORSA A DARK WEBEN

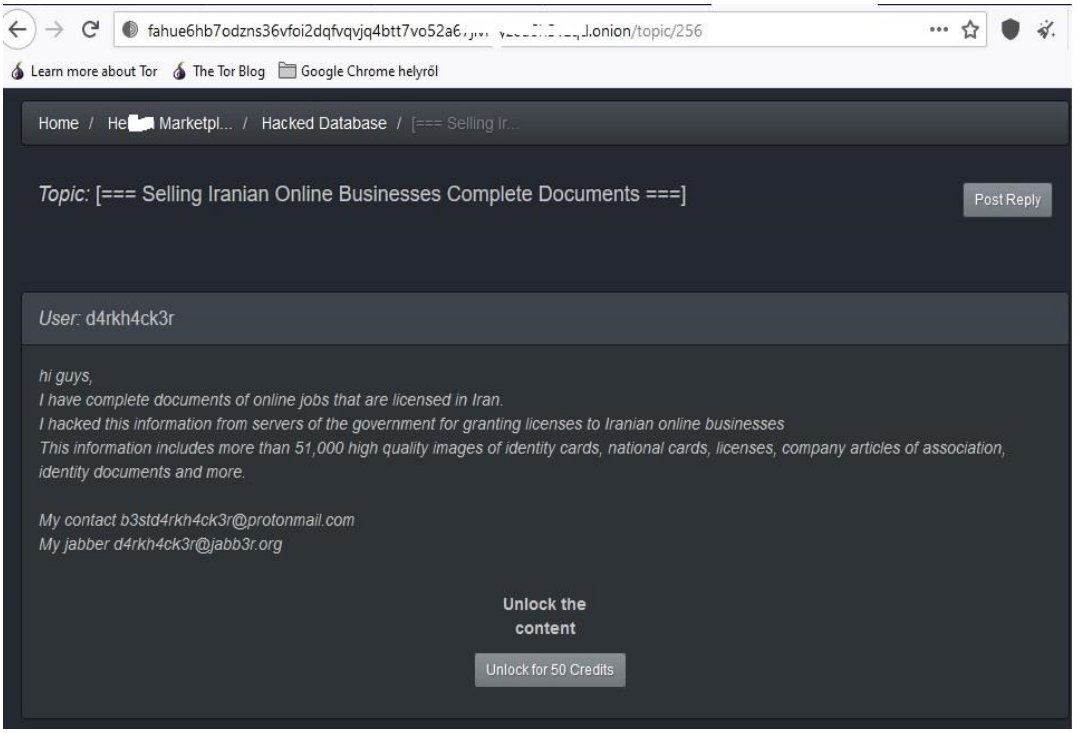
A feketepiacra kerülő adatot jellemzően célirányos hackertámadás útján szerzik meg, azonban ennek részletezése túlnyúlik a tanulmány határain. A kettős célú zsarolóprogramok (ellopja a felhasználó fájljait, majd titkosítással megakadályozza az azokhoz való hozzáférést.) használatát követően az áldozat fizetési hajlandóságától függetlenül, az ellopott adatot először felkínálják visszavásárlásra, és /vagy nyilvánosan áruba bocsájtják. Erre a darknet piacokon számtalan példa előfordul. A fentiek alapján nem célszerű a váltságdíj kifizetése, ugyanis így a keletkezett kár valamelyest csökkenthető.

A másik jellemző forrás a bennfentes elkövető útján szándékosan anyagi haszonszerzés, vagy bosszú céljából kijuttatott adat.

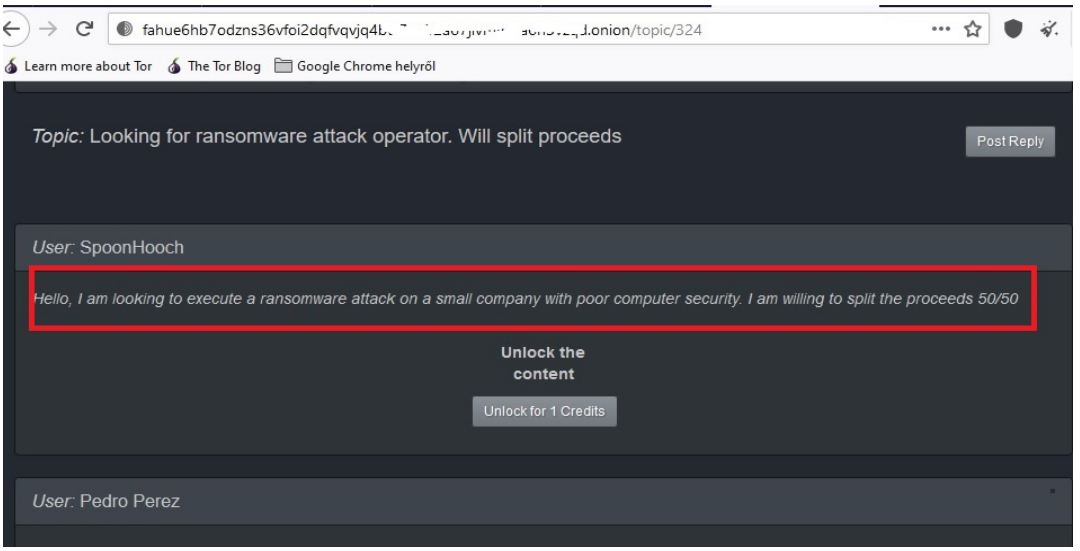
A vállalattól ellopott, vagy kiszivárgott adat több lépcsőn is keresztülmegy mire valamely hacker oldalon, vagy a darknet piacon megjelenik. A bennfentesek az adatot ellenőrzik, egymás között eladják, újracsomagolják, újra eladják, újracsomagolják, esetleg több részre osztják el, majd ez után kerül ki a nyilvános darknet piacokra [13] , [14]. A 4-es és 5-ös számú képeken az olvasó példákat láthat az ellopott adatok árusítására, míg a 6-os számú képernyőfotón egy kisvállalkozás elleni zsarolóvírus támadás irányítására keresnek jelentkezőt.



4. ábra: Ellopott információk a Dark Web egyik darknet piacán. A szerző felvétele.



5. ábra: Dark Web hacker fórumon iráni üzleti adatbázist kínálnak eladásra. A szerző felvétele



6. ábra: Ransomware operatort keres a megrendelő egy vállalkozás elleni támadáshoz. A szerző felvétele

A DARK WEB MONITOROZÁSÁNAK LEHETŐSÉGEI

Napjainkban a Dark Web térhódításával a vállalatok információ biztonsági helyzetének szilárdan tartása érdekében az ellenük tervezett támadások szándékának, illetve az onnan már megszerzett, vagy kiszivárgott adatok felderítésének érdekében elengedhetetlen a Dark Web monitorozása [15]. Ehhez azonban komoly helyismerettel, és pozícióval kell rendelkezni a vizsgálatot végzőnek. Mint az már korábban említésre került a Dark Webnek nincs érdemi kereső rendszere, annak ellenére, hogy van néhány próbálkozás ezek csak részleges és megbízhatatlan eredményeket tudnak produkálni. A Dark Webet kutató szakembernek a különböző linkgyűjteményekből, nyílt webes utalásokból, fórumbejegyzésekből kell elindulnia és építkeznie [15]. Azonban ez még nem elég, hiszen az informatikai bűncselekményeket elkövető hackerek minőségi fórumaikra, vagy chatszobáiba csak alapos ellenőrzési procedúrát követően engednek be új belépőket. Ezekbe a belső körökbe történő bejutás még egy felkészült biztonsági szakembernek is hosszú időt igényel, nem beszélve az esetleges próbafeladatok végrehajtásáról, hiszen a bűnös körnek érdeke, hogy kiszűrje a rendfenntartó erők tagjait és a biztonsági IT szakembereket. A rendfenntartó erők akcióira a fórumok, erősebb titkosítással még szigorúbb és agresszívabb ellenőrzéssel válaszolnak ezzel tovább nehezítve a bűnüldöző szervek munkáját [16].

A másik nehézség, hogy egyszerre több ilyen oldalt kell figyelemmel kísérni, ezek száma a több tucatot is elérheti, nem beszélve a számtalan darknet piacról. Egy bizonyos méret alatt vállalatok nem engedhetik meg maguknak, hogy külön Dark Web ellenőrző részleget tartsanak fenn és most nem említve a tanulmány határain kívül eső Nyílt Web ellenőrzését, amely legalább ennyire fontos.

Az ellenőrzéssel kapcsolatban van még egy olyan tényező, amelyet semmiképpen sem szabad figyelmen kívül hagyni. A Dark Web oldalak keresése és elemzése rendkívüli körültekintést kíván az ellenőrzők részéről, ugyanis nagyon könnyen törvényszegést követhet el, az ellenőrző, aki nem kellő odafigyeléssel meggondolatlanul navigál bizonyos oldalakra. A Dark Webnek külön nyelvezete és zsargonja van, aki ezt nem ismeri, könnyen gyermek pornó, vagy más tiltott oldalra navigálhat, ahol a tartalmak akár véletlen letöltésével is bűncselekményt követhet el, vonatkozik ez a helytelenül beállított automata keresőkre is. [17] Tehát a tapasztalat és jártasság olyan tényezők, amelyek a profi elemző vállalkozás megbízása felé lendítik a mérleg nyelvét. [18]

A felsorolt kihívásokra válaszokat az úgynevezett „Threat Intelligence" vállalkozások nyújthatják, amelyek magukra vállalják a Nyílt Web és a Dark Web megrendelő igényeinek megfelelő szempontok alapján történő monitorozását.[6]. Ezek a vállalatok profiljukból adódóan feltérképezték a Nyílt és Dark Web releváns részét, folyamatosan aktualizálják adatbázisaikat, figyelemmel kísérik a változásokat, munkatársaik útján, illetve a mesterséges intelligenciát felhasználva szoftveres úton ellenőrzik és elemzik az internetes tartalmakat és jelzést adnak a megrendelőnek, ha érdeklődésére számot tartó információ vagy adatot derítenek fel. A nemzetközi színtéren már számos külföldi vállalat nyújt ilyen szolgáltatást, de már hazánkban is akad példa ilyen szolgáltatókra. [19].

ÖSSZEGZÉS

A vállalati információvagyon esetleges kiszivárgásának felderítése, illetve az vállalatot érintő esetleges támadási szándékok időbeni felfedési jelentős előnyt jelent a vállalati vezetés számára az időbeni megelőző, vagy kárenyhítő intézkedések bevezetésére, a vétkesek felderítésére, illetve felelősségre vonására. A Dark Web vonatkozásában mindehhez speciális szakértelem, jártasság és eszközrendszer szükséges, amelynek megteremtése saját erőforrásokból nem tűnik járható útnak. Ezzel szemben egy erre a célra szakosodott vállalat megbízása reális választásnak tűnik [19]. A tanulmánynak nem célja, hogy gazdaságossági hatástanulmányt végezzen, mindössze a Dark Webnek és az vállalati adatvagyon megőrzésének összefüggéseire kívánt rávilágítani.

FELHASZNÁLT FORRÁSOK

[1] Vasvári, G., Lengyel, C. and Valádi, Z., 2006. *Vállati Biztonság Keretrendszere*. Budapest: Budapesti Műszaki és Gazdaságtudományi Egyetem, Biztonságmenedzsment kutató csoport, pp.5, 12,21-26.

[2] Dr. Michelberger, P., 2020. *Információ-, Folyamat- és Vállalatbiztonság*. 2nd ed. Budapest: Óbudai Egyetem, pp.9,10,25,26,29-45.

[3] https://www.pwc.com/hu/hu/szolgaltatasok/technologiai_tanacsadas/data_analytics/adatstrategia.html

[4] Akhgar, B., Gercke, M., Vrochidis, S. and Gibson, H., 2020. *Dark Web investigation*. 1st ed. Cham,Switzerland: Springer Nature Switzerland AG,

[5] https://www.torproject.org/download/

[6] https://geti2p.net/en/

[7] https://freenetproject.org/

[8] https://zeronet.io/

[9] https://www.imf.org/external/pubs/ft/fandd/2019/09/the-truth-about-the-dark-web-kumar.htm

[10] https://tb-manual.torproject.org/about/

[11] https://tb-manual.torproject.org/onion-services/

[12] Márton Tibor, D., 2020. *Dr. Serbakov Márton Tibor: Kriminalitás a dark weben: illegális piacok, pedofil oldalak, terroristák és az ellenük való küzdelem | Büntető Törvénykönyv (új Btk.) a gyakorlatban*. [online] Ujbtk.hu. <https://ujbtk.hu/dr-serbakov-marton-tibor-kriminalitas-a-dark-weben-illegalis-piacok-pedofil-oldalak-terroristak-es-az-ellenuk-valo-kuzdelem/> [Letöltve: 2021.04.16.].

[13] https://www.vaadata.com/blog/are-your-corporate-data-and-sensitive-documents-on-the-dark-web/

[14] Hhs.gov. 2020. *HHS Cyber Security Program*. [online]. <https://www.hhs.gov/sites/default/files/dark-web-and-cybercrime.pdf> [Letöltve: 2021.05.02.].

[15] Pascucci, M., 2016. *Threat monitoring: Why watching the dark web is crucial*. [online] SearchSecurity.<https://searchsecurity.techtarget.com/tip/Threat-monitoring-Why-watching-the-dark-web-is-crucial> [Letöltve: 2021.04.22.].

[16] Ablon, L., Libicki, M. and Golay, A., 2014. *Markets for Cybercrime Tools and Stolen Data*. [online] Rand.org. https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf> [Letöltve: 2021.04.28.].

[17] https://iaca-darkweb-tools.com/dictionary/
[18] https://www.comparitech.com/net-admin/best-dark-web-monitoring-tools/
[19] Lewis, N., 2019. *Should large enterprises add dark web monitoring to their security policies?*. [online] SearchSecurity. https://searchsecurity.techtarget.com/answer/Should-large-enterprises-add-dark-web-monitoring-to-their-security-policies> [Letöltve: 2021.04.14.].