EVOLUTION OF CYBERSECURITY AND THE CYBERSECURITY IN THE BANKING SECTOR UNTIL TODAY

A KIBERBIZTONSÁG ÉS A BANKI KIBERVÉDELEM FEJLŐDÉSE NAPJAINKIG

GULYÁS Olivér[1]

Abstract

Cybercrime appeared long before the birth of the Internet. From the early times, computers and networks were used to "produce," store, and transmit data. In the first period, therefore, the only motivation was to steal the data. Before the birth of the Internet, cybercrime was local. With the birth of the email in the '80s the attacks spread particularly hard. In the '90s, the web browsers helped carrying out the attacks. The next significant wave can be attributed to the rise of social media. By sharing all kinds of information about ourselves, it has opened a Pandara's box for personal data and digital data theft. The last major development was the "institutionalization" of cybercrime. The criminals are no longer pimpled teenagers hiding under dark hoods (as people have imagined), but extensive teams operating as international companies, often backed by states. The aim of the article is to present the development of cybersecurity, the cybersecurity in the banking sector, from the early phase to the present day.

Keywords

history of cybercrime, evolution of cybersecurity

Absztrakt

A kiberbűnözés már jóval az internet megszületése előtt megjelent. A korai időktől a számítógépeket és a hálózatokat az adatok „gyártására", tárolására és továbbítására használták. Az első időszakban még csak az adatok eltulajdonítása volt a motiváció. Az internet megjelenése előtt ez még lokális, helyhez kötött bűnelkövetés volt. A 80-as években az email megjelenése különösen nagyot lökött a támadások elterjedésén. A 90-es években a webes böngészők megjelenése segítette a támadások elkövetését. A következő hullám a közösségi média térnyeréséhez köthető. Azzal, hogy az emberek mindenféle információt osztanak meg magukról, megnyitotta a személyes adat és a digitális adatlopás Pandóra-szelencéjét. Az utolsó nagy fejlődési lépés a kiberbűnözés „intézményesedése" volt. A bűnözők már nem sötét szobákban, kapucni alatt rejtőzködő pattanásos tinédzserek (ahogy ezt az emberek elképzelték), hanem nemzetközi cégekként működő kiterjedt csapatok, akiket sokszor államok támogatnak. A cikk célja bemutatni a kiberbiztonság, azon belül is a banki kibervédelem fejlődésének lépéseit a korai fázistól napjainkig.

Kulcsszavak

kiberbűnözés történelme, kiberbiztonság fejlődése

[1] gulyaso@gmail.com | ORCID: 0000-0001-6945-2222 | doctoral candidate, Óbuda University Doctoral School for Safety and Security Sciences | doktorjelölt, Óbudai Egyetem Biztoságtudományi Doktori Iskola

BEVEZETÉS

Az életet alakító nagy törvényszerűségek közül a newtoni hatás és ellenhatás törvény számos területen jön észrevétlenül szembe velünk. Az elmélet egy kicsavart formája, amikor valaki kitalál vagy felfedez valamit, akkor előbb vagy utóbb egy másik ember kitalálja, hogyan lehetne ellopni azt. Amikor az első ember a fizetési kötelezettségét írásba foglalta, abból később megszületett a váltót. Nem kellett sok idő hozzá, hogy egy másik ember rájöjjön, hogyan lehetne a váltót hamisítani. Természetesen az, hogy egy tolvaj megpróbálja ellopni az értékeinket vagy jószágunkat magával hozza azt is, hogy mások megpróbálják megakadályozni azt, hogy az előbbiek ellopják, meghamisítsák azt. Talán ez az elmélet nem fog belekerülni az egyetemes világfejlődés tanok közé, de mégis a direkt kiváltó oka volt a biztonságtechnika kialakulásának.

A bankbiztonság és a kibervédelem története is valahol azzal kezdődött, hogy egyre inkább elterjedt az elektronikus, digitális eszközök alkalmazása. Amikor az eszközét használni kezdte nyilván már az elejétől készült arra, hogy ezt ne lehessen ellopni, de az igazi éles teszt az az volt, amikor tényleg megpróbálták a rendszert feltörni.

A pénzügyi termékek megjelenése majd rohamos fejlődése magával hozta a pénzügyi termékek eltulajdonítási módjának fejlődését, ami viszont magával hozta az eltulajdonítás elleni védelem fejlődését is. Ezen a ponton érkezünk meg a (bank)biztonság megszületéséhez.

A történelem megmutatta, hogy nincsen feltörhetetlen és ellophatatlan rendszer, de az emberek mindig is törekedtek erre – de legalábbis mindig is azt hitték, hogy megtalálták a legjobb módszert.

A cikk célja, hogy az események láncolatát számba vegye és a végén megmutassa, hogyan jutottunk el a biztonságtechnika és azon belül a kibervédelem jelen szintjére. Jelen cikk része egy nagyobb, a pénzintézetek kiberbiztonságát vizsgáló kutatásnak.

BIZTONSÁGRA TÖREKEDÉS, MINT ALAPSZÜKSÉGLET

A biztonságra törekedés az ember alapvető igényeihez tartozik. Az emberek törekednek arra, hogy elkerüljék a veszélyt, megvédjék testi épségüket vagy anyagi javaikat – miután a fiziológiai szükségleteiket már kielégítettek.

1. ábra: Maslow motivációs piramisa, forrás: http://www.azirastukreben.hu/maslow-motivacios-piramisa [1]

A biztonságra való igény már az őskortól meghatározta a működésünket. A szerszámokat és később a fegyvereket az ősember nemcsak az élelem megszerzésére, de saját maga megvédésére is használta. Szintén a biztonságát (is) szolgálta a tűz használata. Mielőtt megtanulta volna a tűzgyújtást, a tűz megőrzésével biztosította a „fűtéshez" szükséges meleget. Szintén a biztonságra való törekvése volt a farkas „domesztikációja révén" háziasított kutya. A kutya nemcsak a vadászatban segített az embernek, hanem védte annak házát is [2]. Már a korai időktől maga a lakhely (barlang, védett üregek stb.) kiválasztásában is a biztonságra való törekvés volt a meghatározó motiváció.

Az ókorban a közösségbe szerveződés már megteremti az alapját a bonyolultabb biztonságtechnikának is. A technika színvonalának, a társadalom szervezettségének emelkedésével vált lehetővé bonyolultabb biztonsági technológiák megjelenése.

A középkor volt az, ahol az állami szervezetek, birodalmak fejlődése magasabb szintre emelte a biztonságtechnika eszköztárát. Utak, úthálózatok, városok, városállamok, vagy akár a templomok és az ott használt harangok, amivel a veszedelmet jelezték mind lépések voltak egy komplexeb biztonságtechnikai rendszer irányába.

Az általános biztonságra törekvésen felül az emberek szerették volna a jószágaikat, értékeiket is biztonságban tudni. A bankbiztonság és azon belül a banki kiberbiztonság kialakulásának történelmét ezért valahol a pénz kialakulásánál kell kezdeni.

PÉNZ ÉS A PÉNZÜGYI RENDSZEREK KIALAKULÁSA

A bankok és a banki szolgáltatások megjelenését, majd azt követően a bankbiztonság megszületését valahol a pénz kialakulásánál kell kezdeni. A pénz kialakulását a legtöbb elmélet a cserekereskedelem kialakuláshoz köti. Amikor a korabeli emberek már nem tudták az egyik árut a másikra cserélni. Nem mindenkinek kellett az adott csereterméke, mert nem lehetett a cserét értékegyeztetéssel végrehajtani, vagy mert a cserélendő termékre az igény nem volt egyidejű (az egyik ember téli fél ruhát készített, de nyáron is ennie kellett valamit stb.), megjelent a pénz.

A nemesfémből készült érmékkel megjelent azok „manipulálása" is. A fém érmék szélét levágták, így próbáltak meg csalni vele. A levágott szélekből újra pénzt lehetett verni. Előfordult, hogy maguk a pénz kibocsátói rontották az értékét azzal, hogy a régieket bevonták és alacsonyabb nemesfém tartalmú érméket bocsátottak ki.

A fémpénz megjelenését követően, első írásos emlék i.e. 3000 körüli Mezopotámiában, a váltó a következő nagy lépés [3].

A nemesfémek kínálata, azok előállítása (bányászata) miatt nem tudta követni a gazdaság növekedését. A pénzhiány eredményeképpen megjelentek a váltók. A váltókibocsátója (adós) kötelezettséget vállalt arra, hogy a váltó birtokosának egy jövőben meghatározott dátumra kifizeti a tartozását.

Ezeket a váltókat az elfogadóik egy idő után tovább forgatták, pénzként adták tovább. A váltókkal az eredendő probléma az volt, hogy a sokadik forgatása után az elfogadó már térben és időben messze került az által ismeretlen adósságot garantáló személytől. Ezért nem mindig fogadták el szívesen. Természetesen a magánszemélyek által kibocsátott váltókkal megjelent azok hamisítása is.

A váltóhamisítás, ahogy a pénz szélének körbevágása, már szofisztikáltabb csalás volt. A magánszemélyek által kiadott váltük esetében az aláírások odahamisítása, díszes papírok lemásolása már komolyabb előkészületeket igényelt.

A középkorban megjelenő bankok őrzésre átvették a pénzeszközöket – a pénz kopása, őrzése és szállítása jelentős költséggel járt. Az átvett pénzeszközökről igazolást adtak ki. A bankok által kibocsátott váltókat már mindenki elfogadta – nagyobb biztonságot jelentett a gazdaság szereplőinek. A bank által kibocsátott fizetési ígérvények már közvetlen ősei voltak a bankjegyeknek.

Egyes bankok csődje, a piac szabályozása és az „önös" érdek is azt eredményezte, hogy az államok magukhoz vették a bankjegykibocsátás monopóliumát. Létrejött az állami bank, a jegybank. „Bár az 1668-ban alapított Sveriges Riksbank a legidősebb központi bank, az állambankári feladatokat ellátó intézmények Európa-szerte az 1694-ben, magánbankként felállított Bank of England példáját követték" [3]. Egy idő után már csak az állam által kibocsátott bankjegyekkel lehetett fizetni. [3] [4] [5]

A bankjegyek hamisítása és a bankok kirablása a mai napig virágzó „üzletág". A hamísítás természetesen magával hozta a bankjegyek hamisítás elleni védelmének fejlődését. A bankok kirablása, pedig a biztonsági rendszerek fejlődését.

TELEKOMMUNIKÁCIÓ ÉS A SZÁMÍTÓGÉP MEGJELENÉSE

Az első időszakban még csak fizikai formában létezett a pénz. A követelések lekönyvelése effektíve könyvekben, papíralapon történt. A papírlapú működés koporsójába az első szöget azonban még nem az informatika, hanem a telekommunikáció fejlődése ütötte.

A London és New York között 1858-ban létrejött távírókapcsolat nem titkolt célja a gazdaság két meghatározó piacának összekötése volt. A korabeli beszámolók alapján a banki tranzakciók időtartama a korábbi négy hétről így egy napra csökkent [6].

A XIX. század közepéig kellett várni, hogy a számítástechnika is hasonló áttörést hozzon a bankok működésében, mint amekkorát a távírógépek hoztak. Az első időszakban a számítógépeket a könyvelésben, a back office területeken használták. Azokon a területeken, ahol a számítások pontossága, gyorsasága és a legtöbb adminisztrációs feladat volt.

A számítógépek használatának elterjedésével és azok összekapcsolásával létrejöttek a komplex rendszerek. 1965-re az Egyesült Királyságban és az Egyesült Államokban a legtöbb nagy bank bevezette az elektronikus adatfeldolgozást, ami lehetővé tette, hogy már a nap végén lássák az aznapi teljes számlaforgalmat [6].

Az 1960-as évek végén az adatbáziskezelő rendszerek megjelenése, a digitalizáció mellett a szabványosítás elterjedése kellett azonban ahhoz, hogy a különböző bankok közötti tranzakciókban is ki tudják szorítani az informatikai megoldások a fizikai instrumentumokat.

Az előzőek teremtette meg annak az alapját, hogy az elektronikus banki szolgáltatások beszivárogtak a lakossági szolgáltatásokba is. Az ügyfelek bankszámlát nyitottak, fizetésüket közvetlenül a bankszámlájukra kapták.

1967-ben Londonban, amikor az első ATM elkezdte működését született meg a 0-24-ben működő szolgáltatás intézménye. A New York-i Chemical Bank már azzal hirdette az automatáját: „Szeptember 2-án bankjaink 9 órakor nyitnak, és soha többé nem zárnak be" [7]. A bankkártya megjelenése, a pénzhasználati kultúra megváltozása magával hozta a bankok működésének átalakulását.

A következő nagy lépés az volt, amikor a bankfiókok beköltöztek az emberek otthonába. Az 1982-ben az Egyesült Királyságban bevezetett „Homelink" rendszer, ahol a televízió teletex dekóderével és a telefonvonal segítségével az emberek otthonából elérhetővé vált a bankszámlájuk. Franciaországban ehhez hasonló és nagyon sokáig közkedvelt megoldás volt az úgynevezett Minitel, aminek 1990-ben 6,5 millió felhasználója volt [8].

Magyarországon 1994-ben az OTP Bank vezette az automatikus telefonos szolgáltatását a Telebankot. Az internet használata a Wells Fargo nevéhez köthető, aki 1995-ben indította online banki szolgáltatását [6]. Mára a Statista kutatása alapján az internetet bankolásra használók száma megközelíti a 2 milliárdot, 2024-re várhatóan a 2,5 milliárdot [8].

Az elektronikus eszközök térnyerésével, az informatika fejlődésével a nyilvántartások elektronikusak lettek. Azt gondolnánk, hogy a mai modern korban már minden elektronikusan tárolt, kereshető, de nagyon sok bank küzd még ma is azzal, hogy archív anyagai nincsenek digitalizálva, bizonyos instrumentumok (például régi garanciák) még papíralapon vannak könyvelve.

Az elektronika térnyerésével a támadók is új módszerekre tértek át. Volt olyan ATM berendezés, a technológia megjelenésének hajnalán, ahol mágneses vagy lyukkártyát kellett a gépbe csúsztatni, esetleg fém zsetont kellet a berendezésbe dobni. Ezeket a zsetonokat a bank később postai úton visszaküldte az ügyfeleknek. Ezzel egy újfajta rablási módszer: a zsetonok ellopása és az azokkal való visszaélés is gyorsan megjelent [9].

KIBERBŰNÖZÉS FEJLŐDÉSE

A kiberbűnözés, ahogy korábban már elemeztük, az elektronikus technológiák fejlődésével párhuzamosan fejlődött. Amikor egy találmány forgalomba került, a bűnözők is megtalálták annak módját, hogy valahogy ők is hasznot húzhassanak belőle.

A következő részben az egyes bűnelkövetési módszereket vesszük górcső alá. Időrendi sorrendben haladva megnézzük a kezdetleges módszerektől hogyan jutottunk el a szofisztikált kibertámadásokig. Olyan eseményeket és technikákat fogunk vizsgálni, amelyek az elődjei voltak a bankokat megcélzó támadásoknak.

Korai telefonok feltörése

Ahogy a számítógépet a telefon, úgy a számítógépes bűnözést is megelőzte a telefonos-bűnözés. A korai években a telefonos központokban tinédzser fiúk dolgoztak. Már 1878-ban, két évvel azután, hogy Alexander Graham Bell „felfedezte" a telefont, megtörténtek az első telefonos visszaélések. A fiatalok hívásokat szakítottak meg vagy irányítottak át, később saját hívásokat indítottak. A visszaélések hatterében inkább a saját maguk szórakoztatása, mint a haszonszerzés volt [10].

Távíró feltörése

Természetesen a korai távírórendszereknek is megvoltak a saját hackereik. 1903-ban a Marconi vezetéknélküli távírójának első nyilvános bemutatását zavarta meg Nevil Maskelyne azzal, hogy sértő, trágár üzeneteket küldött a berendezésre. Célja a biztonságosnak mondott találmány hiteltelenítése volt – saját állítása szerint, hogy felhívja a figyelmet a rendszer sérülékenységére [11].

Fénykép: Nevil Maskelyne, a távíró feltörője, forrás: https://listverse.com [12]

Háborús kódfeltörők

A világháborús kódfeltörőkről több film és regény is született. Leghíresebb talán a német Enigma feltörésének története, ami a talán az etikus hackerkedés előfutára lehetett. 1939-ben az Egyesült Királyságbeli Bletchley Parkban Alan Turing és Gordon Welchman kifejlesztette a BOMBE-berendezést a német Enigma berendezés által titkosított üzenetek dekódolásásra [13].

Az azóta eltelt időben többször szóltak a hírek arról, hogy bizonyos támadások mögött már nemcsak magánszemélyek, hanem szervezett csoportok, esetleg idegen kormányok is állhatnak. Ugyanúgy, ahogy a támadók, a védelem vonala sem néhány elszigetelt emberből áll.

2007-ben az észt számítógépes infrastruktúra elleni támadáskor ismerték fel az emberek az államok által támogatott kiberbűnözői csoportok létezését. Bár ez csak a második jelentős mértékű összehangolt támadás volt, a 2003-as Titan Rain után [14]. Mégis az észtországi támadássorozat volt, ami felnyitotta az államok szemét, és például a NATO kibervédelmi központjának (*Cooperative Cyber Defence Centre of Excellence*) megalapításához vezetett.

Napjainkban, a cikk írásának pillanatában, is a folyamatban lévő „fizikai" háború mellett folyik egy információs háború is. Ebben a háborúban az Oroszország által támogatott hacker-sereg áll szemben az ukrán és az őt támogató országok hacker-seregeivel. A hackerek a másik fél katonai rendszereinek feltörésével, a csapatmozgások nyilvánosságra hozásával próbálnak a fizikai hadszintéren is előnyre szert tenni.

Etikus hacker

Az első etikus hacker René Carmille volt, aki megakadályozta, hogy a Franciaországot elfoglaló nácik kinyerjék az országban élő zsidók adatait – „zsidóságukra" vonatkozó információt – a lyukkártyás alapon működő nemzeti demográfiai nyilvántartó rendszerből. Carmille feltörte a nyilvántartó rendszert. Bárhogyan próbálkoztak is a nácik a zsidóságra vonatkozó adatot bevinni vagy kinyerni a nyilvántartóból a rendszer senkinél se hozott fel erre vonatkozó adatot.

Közel két évig meg tudta akadályozni a nácikat a demográfiai nyilvántartó használatában. Amikor végül 1944-ben rájöttek, hogy Carmille manipulálta a gépeket Dachauba szállították, ahol végül meg is halt [15].

Az etikus hackerség azóta legalább annyira elterjedt lett, mint a „sima” hackerség. Több cég nyújt a kiberbiztonsági tanácsadás kertében etikus hacker szolgáltatásokat. Kontrolált körülmények között megpróbálják megkeresni egy adott cég informatikai rendszerének hiányosságait. Több intézményben, például az Óbudai Egyetemen, képeznek etikus hackereket.

Fénykép: René Carmille, az első etikus hacker, forrás: https://listverse.com [12]

Telefonok feltörése („phone phreaks”)

Az ’50-es évek végétől jelentek meg az úgynevezett „phone phreaks”-ek. Ezek az emberek a telefonokat „hackelték meg”. Rájöttek, hogy a telefonkagylóba a megfelelő zene lejátszásával fel tudják törni a telefonhálózatot és szabadon tudnak hívást indítani bárhova. Az eljátszott vagy elfütyült hangsor, amennyiben megegyezett a megfelelő titkos kóddal, egy belső, a távolsági hívásokat kezelő operátorhoz kapcsolta a hackert. Az operátor ezáltal azt hitte, hogy kolléga van a vonal másik végén, így a kért tetszőleges számra kapcsolta őt – természetesen teljesen ingyen.

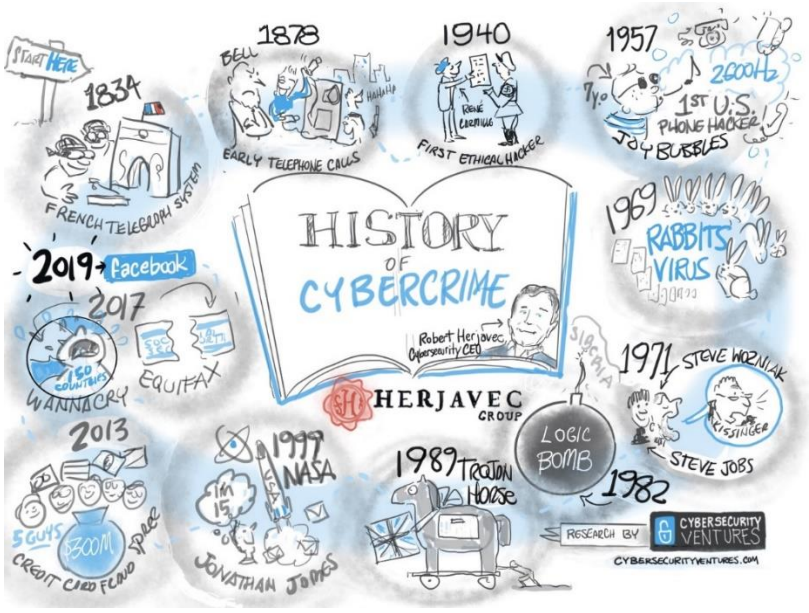
David Condont (1955) tartják az eljárás úttörőjének. Azonban Joe Engressia (Joybubbles), a vak 7 éves tökéletes hallású fiú, lett a leghíresebb „fütyülő hacker” [12].

John Draper, aki egy müzlis dobozban talált síppal törte fel telefonrendszert (innen származik a beceneve Captain Crunch) inspirálta később Steve Jobs-ot és Steve Wozniakot. Az Apple későbbi megalapítói találták ki a telefonvonalak feltörésére alkalmas blue-box berendezést (1971) és kerestek sok pénzt a későbbi „tömeggyártásából” [12].

A telefonok feltörését (phreaking) fejlesztette tovább a Phonemasters csoport. A csoport tagjai először csak lopott, nemzetközi hívásokhoz használható kártyakódokat árultak. Majd kiterjesztették a működésüket és mindenféle személyes adatot árusítottak, amire a „vevőnek” szüksége volt. Legdrágább csomagjuk: 500 dollárért bármelyik híres ember, politikus vagy celebritás, címét vagy telefonszámát meg lehetett vásárolni. Tevékenységükkel közel 1,85 millió dollárt kerestek [16].

Számítógépes jelszó feltörése

Allan Scherr volt az első, aki feltörte egy számítógép belépési jelszavát. Scherr egészen pontosan az első jelszóval védett számítógépet törte fel. Az MIT-n 1962-ben jelszóval védték a számítógépeket. Allan Scherr azonban megelégelte a beállított időkorlátokat, ezért a többi felhasználó feltört jelszavával lépett be, amikor lejárt a saját ideje. Az első számítógépes troll megjelenése is neki köszönhető. Az osztálytársaival az egyik megszerzett jelszóval a tanáruk fiókjába lépett be és tette őt nevetség tárgyává [17].



2. Ábra: Kiberbűnözés története, forrás: https://cybersecurityventures.com [17]

Hackerek megjelenése

Maga a szó, hogy „hacker" is az MIT-ról származik. Carlton Tucker az egy tanár használta az iskola telefonos rendszerét feltörőkre, phone phreak-ekre. A „hack" szót már korábban is használták, de akkor még csak az elektronikával foglalkozókra. Ebben a negatív értelemben először Carlton Tucker használta 1963-ban a „hacker" szót a telefonos rendszert feltörőkre [12].

Számítógépes vírusok és a DDoS

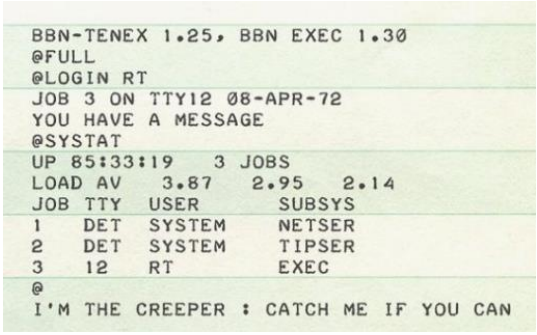
A RABBITS volt 1969-ben az első számítógépes vírus. Programkód eredete nem ismert, de a vírus terheléses támadással térdre kényszerítette a Washingtoni Egyetem számítógép központját. A programot ismeretlenek feltelepítették az egyetem egyik számítógépére és a program elkezdte lemásolni magát. A program két másolatot készített magából, a másolatok tovább szaporodtak – a gyors szaporodási módszerből származik a vírus neve is. Az elszaporodott programocskák egy idő után túlterhelték a számítógépet, ami így leállt [17].

Öt évvel később valaki, aki ismerte a fenti történetet létrehozott egy újabb „nyúlvírust", amit WABBIT-nak hívott. Azért, hogy egy másik számítógépes felhasználót „kiüssön" feltelepítette a programot az APRANET-re, az amerikai tudományos intézetek között kialakított számítógépes hálózatra – az Internet elődjére (Advanced Research Projects Agency Network, „ARPANET"). Ez volt a történelem első számítógép ellen végrehajtott túlterheléses támadása (Distributed Denial-of-Service, „DDoS") [12].

Számítógépes vírus az Interneten

Ray Tomlinson és Bob Thomas volt az első, aki 1971-ben az Interneten keresztül egy levélben juttatott el egy vírust. A Creeper nevezetű féregvírus lemásolta saját magát és

így terjedt az ARPANET-en. Minden egyes másolat egy ablakban felugrott és azt írta ki, hogy „Én vagyok a creeper: kapj el ha tudsz” („I’m the creeper: Catch me if you can”). Később, az Internet felfedezésekor Tomlinson ide is feltöltötte a vírusát [12].



Fénykép: Creeper, az első számítógépes vírus képernyőképe, 1972, forrás: https://listverse.com [12]

Híres hírhedt hackerek

A leghíresebb hacker valószínűleg Kevin Mitnick volt, aki 1970 és 1995 között majdnem a világ összes szigorúan védett számítógépes hálózatát feltörte. Mitnick a „pszichológiai befolyásolás” (social engineering) segítségével törte fel ezeket a rendszereket. A dolgozók megtévesztésével megszerezte azok azonosítóját és jelszavát.

Saját bevallása szerint a különböző rendszerek minél mélyebb szintű megismerése vezérelte a tetteit. Abban az időszakban a leginkább keresett bűnöző volt. Végül kétszer is (1988-ban és 1995-ben) bebörtönözték „áldásos” tevékenységért, először 46 majd 22 hónapra. A büntetéséből 8 hónapot magánzárkában töltött, mert az ügyészek meggyőzték a bírót, hogy telefonba fütyüléssel el tudja indítani a nukleáris rakétákat [18].

„Számítógépes” sikkasztás

Az első sikkasztás, számítógép segítségével, nem sokkal azután történt, hogy a számítógépeket már nem csak a back office-ban alkalmazták elvont számításos műveletek elvégzésére, hanem a normál banki működés része lett. Egy New York-i bank pénztárosa 1973-ban több mint 2 millió dollárt sikkasztott el [17].

Trójai vírusok

Az első trójai vírust John Walker készítette 1975-ben. A vírus két évvel azelőtt született, hogy az első otthoni személyi számítógépek az üzletekbe kerültek volna. A vírus kitalálója, saját bevallása szerint, csupán jóindulatból állította úgy be az általa készített ANIMAL nevű játékot, hogy a háttérben bemásolja magát minden meghajtóra, majd minden a megfertőzött gépbe berakott (akkor még) mágnesszalagra.

Walker állítása szerint így szeretett volna az embereknek segíteni, hogy ne kelljen elkérni a játékot – és nehézkesen átmásolni –, hanem ő már előre „elhelyezte” azt számukra a saját gépükre [12].

Az első kiberbűnöző

Bár Kevin Mitnick sok dologban megelőzte, mégis Ian Murphy volt az első ember, akit 1981-ben el is ítéltek kiberbűnözés miatt. A rajongói által csak Captain Zap-nak hívott

Murphy feltörte az AT&T vállalat hálózatát és átállította a rendszer belső óráját, hogy munkaidőben is csúcsidőn kívüli díjakat számítson fel. Tettéért akkor még csak 1.000 óra közmunka és 2,5 év próbaidő volt a „jutalma". A későbbi a Komputerkémek (Sneakers, 1992) című mozifilm írója a ténykedéséből merítette a film inspirációját [17].

Zsarolóvírus

Az első jelentősebb zsarolóvírus támadást 1989-ra datálják. Ebben az évben egy AIDS adatbázist küldtek több ezer AIDS kutatóknak és egy angol számítógépes magazin előfizetőinek. A program egy trójait tartalmazott, amely 500 dollárt kért a számítógép adatainak „felszabadításáért" [19].

World Wide Web

1994-ben elindul a World Wide Web. A hackerek innentől kezdve határok nélkül „dolgozhattak". A technológia megkönnyítette a számítógépes rendszerek feltörését, de a hackerek egymás közötti kommunikációját is.

A korábbi szűk körű, online fórumokon folyó kommunikáció mindenki számára elérhetővé válik a különböző weboldalakon keresztül. Ezt használja például ebben az évben egy angol diák, aki a web-en talál betárcsázó program segítségével az otthoni Commodore Amiga számítógépéről feltöri Korea nukleáris rendszerét, belép a NASA és több más amerikai hivatal számítógépes rendszerébe [19].

Bankokat ért jelentős kibertámadások

Az egyik első jelentős bankot érintő kibertámadás a 30 éves Vladimir Levin nevéhez köthető. Az orosz kiberbűnöző 1995-ben, az akkor még gyerekcipőben járó világháló segítségével a szentpétervári otthonából törte fel a Citibank New York-i informatikai rendszerét.

A rendszer feltörése után, az ügyfelek belépési azonosítójával és jelszavával csalárd tranzakciókat engedélyezett. A hivatalos becslések szerint közel 12 millió dollárt utalt át különböző számlákra világszerte – Levin ebből „csak" 3,7 millió dollárt ismert el. A tranzakciók egy részét sikerült az FBI-nak lekövetnie. Levint 1998-ban 3 év börtönbüntetésre ítélték, a pénz jelentős részét megtalálták [20]. Az eset, és a jelentős mértékű ellopott, összeg korai figyelmeztető jel volt a banki számítógépes rendszerek sérülékenységére.

Albert Gonzalez, már 14 éves korában felkeltette az FBI figyelmét, amikor feltörte a NASA számítógépes rendszerét. 2003-ban elfogták, amikor a ShadowCrew csapat tagjaként bankkártya adatokat lopott és értékesített online. 2006-tól 2008-as elfogásáig több millió dollárt szerzett hitel- és betétkártya adatok ellopásával – többek között a TJX, Heartland Payment Systems és a Citibank rendszereinek feltörésével. Az ellopott pénzt szállodákban és luxus bulikra költötte el. Tevékenységért a „jutalma" összesen 20 év börtön volt [17].

2005-ben az HSBC több mint 180.000 ügyfélnek küld levelet figyelmeztetve őket, hogy a kártyaadataik az egyik kiskereskedő (Polo by Ralph Lauren) rendszerének feltörésén keresztül kompromittálódhattak [17].

2010-ben egy kelet-európai kiberbűnöző csapat szintet lép. Zeus nevű trójai vírusuk segítségével Egyesült Államokbeli és angol bankok rendszerének feltörésével az ott vezetett bankszámlákról 70 millió dollárt lopnak el. A vírus eredetileg számítógépeket célzott, de upgrade-elve lett mobil telefonokra. A károsultak által megkapott levélben vagy megnyitott oldalon található linkre kattintva feltelepült a program az eszközökre, ami megjegyezte a

károsultak billentyű leütését, amikor azok beírták a belépési azonosítójukat. Az eset arra hívta fel az emberek figyelmét, hogy a XXI. század szervezett bűnözése a kiberbűnözésben is aktívan részt vesz [21].

Zeus rekordja nem tartott sokáig. 2013-tól 2015-ös elfogásukig egy orosz hacker csapat több mint száz pénzintézet számítógépes rendszerét törte fel és lopott el hozzávetőlegesen 800 millió dollárt. Az egész világon átívelő kibertámadás-sorozat keretében egy vírus segítségével beléptek a rendszerekbe, hamis átutalásokat engedélyeztek, sőt sikerült bankjegykiadó automatákat is feltörniük, amikből kártya nélkül készpénzt tudtak felvenni [22].

2013-ban egy másik rekord dőlt meg. Az Egyesült Államok addigi történelmének legnagyobb kiber-bűnesetét és hitelkártya csalását követték el. Az elfogott öt ember több mint 300 millió dollár kárt okozott tettükkel. Elfogásukkor fény derült a Nasdaq, a Visa és egyéb cégek ellen folyamatban lévő támadásokról. Az elkövetők nyomait akkor már évek óta követték. Az öt férfi (négy orosz és egy ukrán) legalább 160 millió hitelkártya adatát lopta el és adta tovább [23].

A hírhedt bangladesi bankrablás nemcsak a rablási érték miatt került a hírekbe: 81 millió dollárt loptak el néhány óra alatt a Bangladesh Banknál vezetett bankszámlákról, de csak egy apró programozási hiba miatt nem tudták a többi közel 1 milliárd dollárnyi összeget ellopni. Ami felkeltette a hatóságok érdeklődését az a technika, ahogy a tolvajok betörtek a bank rendszerébe. A nemzetközi átutalási rendszert, a SWIFT-et használták, hogy feltörjék a bank számítógépeit. A SWIFT egy 1970 óta működő szuper-biztonságos(nak gondolt) zárt pénzügyi rendszer amit világszerte közel 11.000 intézmény használ, közel napi 25 millió tranzakció végrehajtására – a világ pénzügyi átutalásainak jelentős része. Pénzintézetek, kereskedők, pénzügyi szervezetek használják a SWIFT-kódokat az intézmények beazonosítására a tranzakciók ellenőrzésére [24].

ÖSSZEFOGLALÁS

Cikkben bemutattam a pénzügyi rendszer fejlődése mellett hogyan fejlődtek a pénzügyi rendszer elleni támadások is. A pénz megjelenésétől, a pénzintézetek megjelenéséig nagy utat jártunk be. A fejlődés azonban nem állt meg, a papíralapú működéstől a digitalizációig még sok évnek kellett eltelnie. A digitalizáció rohamos fejlődése azonban magával hozta a bankszektort érintő veszély növekedését [25].

A támadásokra adott egyenes válaszként a szakemberek megpróbálták megvédeni az informatikai rendszereket. Először megpróbálták lekövetni, majd később a hackerek előtt járni, csapdába csalni azokat (például a *honey pot* megoldásokkal). Ennek a macska-egér harcnak az közvetlen eredménye a kibervédelem erősödése. A történelmi áttekintés célja az volt, hogy megmutassam milyen utat kellett ahhoz bejárni, hogy a kiberbiztonság mai szintjére érkezzünk meg.

A technika fejlődése azonban természetesen nem állt meg, a Blockchain technológiák vagy a mesterséges intelligencia alkalmazása új lehetőségeket nyithat meg a banki kibervédelemben.

Jelen cikk része egy nagyobb, a banki kiberbiztonságot vizsgáló kutatásnak.

FELHASZNÁLT IRODALOM

[1] Szabó Szilvia, „Maslow motivációs piramisa," [Online]. Available: http://www.azirastukreben.hu/maslow-motivacios-piramisa. [Hozzáférés dátuma: 16 05 2022].
[2] Szűcs Endre, „Az "ősember" biztonságtechnikai eszköze," Hadmérnök, 11. évfolyam 4. szám 2016 december, pp. 216-221. (4 oldal).
[3] Kosztopulosz Andreász, „A pénz és a pénzrendszerek fejlődése," Szegedi Tudományegyetem Gazdaságtudományi Kar, SZTE GTK 2017/2018, 2018.
[4] „kiszamolo.hu," 04 03 2013. [Online]. Available: https://kiszamolo.hu/a-penz-rovid-tortenete/. [Hozzáférés dátuma: 05 05 2022].
[5] Divéki Éva, Keszy-Harmath Zoltánné, Helmeczi István, Innovatív fizetési megoldások, Magyar Nemzeti Bank: MNB Tanulmányok 85., ISSN 1787-5293, Budapest, 2010. május.
[6] OTPédia, 22 04 2022. [Online]. Available: https://www.otpedia.hu/melyviz/ugyvitel/hogyan-forradalmasitotta-szamitogep-bankolast_1/. [Hozzáférés dátuma: 11 05 2022].
[7] Múlt-kor, 17 05 2021. [Online]. Available: https://mult-kor.hu/reggel-kilenctol-az-orokkevalosagig-igy-kezdodott-a-bankautomatak-tortenete-20210519. [Hozzáférés dátuma: 11 05 2022].
[8] Statista, 03 2021. [Online]. Available: https://www.statista.com/statistics/1228757/online-banking-users-worldwide/. [Hozzáférés dátuma: 11 05 2022].
[9] Múlt-kor, OTPédia, 28 05 2021. [Online]. Available: https://www.otpedia.hu/digitalis-korunk/fizetes/atm-sztori_2/. [Hozzáférés dátuma: 11 05 2022].
[10] Cyber Crime In The 21st Century, „UKEssays," 27 04 2017. [Online]. Available: https://www.ukessays.com/essays/media/cyber-crime-in-the-21st-century-media-essay.php#citethis. [Hozzáférés dátuma: 11 05 2022].
[11] Jade Fell, „Hacking through the years: a brief history of cyber crime," 13 03 2017. [Online]. Available: https://eandt.theiet.org/content/articles/2017/03/hacking-through-the-years-a-brief-history-of-cyber-crime/. [Hozzáférés dátuma: 11 05 2022].
[12] Mark Oliver, „10 Early Hackers From Before The Invention Of The Home Computer," 14 05 2018. [Online]. Available: https://listverse.com/2018/05/14/10-early-hackers-from-before-the-invention-of-the-home-computer/. [Hozzáférés dátuma: 11 05 2022].
[13] Crypto Museum, „Bombe, Breaking the Enigma cipher," 23 11 2012. [Online]. Available: https://www.cryptomuseum.com/crypto/bombe/. [Hozzáférés dátuma: 11 05 2022].
[14] „The 7 worst cyberattacks in history," Dvice, 22 09 2010. [Online]. Available: https://web.archive.org/web/20141112155600/http://www.dvice.com/archives/2010/09/7_of_the_most_d.php. [Hozzáférés dátuma: 19 05 2022].
[15] Matthew Wills, WWII and the First Ethical Hacker, Technology and Culture, Vol. 45, No. 1 (Jan., 2004), pp. 80-101: The Johns Hopkins University Press and the Society for the History of Technology, 2017.
[16] John Simons, „Unplugged! The biggest hack in history, ZDNet," 01 10 1999. [Online]. Available: https://www.zdnet.com/article/unplugged-the-biggest-hack-in-history/. [Hozzáférés dátuma: 16 05 2022].

[17] Robert Herjavec, „Cybercrime Magazine," 17 07 2019. [Online]. Available: https://cybersecurityventures.com/cybersecurity-ceo-the-history-of-cybercrime-from-1834-to-present/. [Hozzáférés dátuma: 11 05 2022].
[18] Anthony, Technology means business, „5 Examples of Cyber Crime and the Cyber Criminals Who Got Caught," 09 04 2018. [Online]. Available: https://blog.tmb.co.uk/cyber-criminals. [Hozzáférés dátuma: 16 05 2022].
[19] Vuk Mujovic, „Where does cybercrime come from? The origin & evolution of cybercrime, Le VPN," 18 10 2018. [Online]. Available: https://www.le-vpn.com/history-cyber-crime-origin-evolution/. [Hozzáférés dátuma: 16 05 2022].
[20] The Wall Street Journal, „Russian Hacker Is Sentenced To 3 Years in Citibank Heist," 24 02 1998. [Online]. Available: https://www.wsj.com/articles/SB888360434859498000. [Hozzáférés dátuma: 16 05 2022].
[21] Richard Esposito, Jason Ryan, „ABC News, FBI: Crime Ring Stole $70 Million Using Computer Virus," 16 07 2010. [Online]. Available: https://abcnews.go.com/Blotter/fbi-crime-ring-stole-70-million-computer-virus/story?id=11777873. [Hozzáférés dátuma: 16 05 2022].
[22] Dan Elsom, „The Sun," 11 10 2017. [Online]. Available: https://www.thesun.co.uk/tech/4120942/five-of-the-worst-cases-of-cyber-crime-the-world-has-ever-seen-from-data-theft-of-one-billion-yahoo-users-to-crippling-the-nhs/. [Hozzáférés dátuma: 16 05 2022].
[23] David Jones, Jim Finkle, „U.S. indicts hackers in biggest cyber fraud case in history, Reuters," 26 07 2013. [Online]. Available: https://www.reuters.com/article/us-usa-hackers-creditcards/u-s-indicts-hackers-in-biggest-cyber-fraud-case-in-history-idUSBRE96O0RI20130726. [Hozzáférés dátuma: 16 05 2022].
[24] Kim Zetter, „That Insane, $81M Bangladesh Bank Heist, WIRED," 17 05 2016. [Online]. Available: https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/. [Hozzáférés dátuma: 16 05 2022].
[25] Gulyás Olivér, Kiss Gábor, „Kiberbiztonság 2021-ben a bankszektorban és a pénzügyi szervezeteknél," Biztonságtudományi szemle, pp. 83-90, 2022. IV. évf. 1. szám.