EXAMINATION OF THE HISTORY OF INFORMATION SECURITY MILESTONES, EVENTS AND ANSWERS

INFORMÁCIÓBIZTONSÁG FEJLŐDÉSTÖRTÉNETI VIZSGÁLATA MÉRFÖLDKÖVEK, ESEMÉNYEK ÉS VÁLASZOK

SZŰCS Endre[1], ZÁHONYI Lajos[2]

Abstract

No discipline can exist without antecedents. All science is on the move, every science is looking for answers and thus evolving. These answers are built on each other and this raises new questions. Development is unstoppable. To better understand the problems of the present age, we must look back and learn from these answers. The focus of the present study is also on the milestones, tools, and toolkits that have significantly influenced the development of information security. In this study, we examined the history of the development of information security, in the framework of which we reviewed a significant event of the 20th and 21st centuries that can be highlighted from the point of view of information security, and the answers given to it.

Keywords

information security, history of information security, principles of information security, milestones of information security

Absztrakt

Egy tudományterület sem létezhet előzmények nélkül. Minden tudomány mozgásban van, minden tudomány keresi a válaszokat és ezáltal fejlődik. Ezek a válaszok egymásra épülnek és ebből újabb kérdések keletkeznek. A fejlődés megállíthatatlan. Ahhoz hogy jobban megértsük a jelen kor problémáit bátran vissza kell tekinteni a múltban és tanulni ezen válaszokból. Jelen tanulmány fókuszában azon mérföldkőnek is tekinthető események, eszközök és eszközrendszerek állnak, amelyek jelentősen befolyásolták az információbiztonság fejlődését. A tanulmányban információbiztonság fejlődésének történetiségét vizsgáltuk, melynek keretében a 20. és a 21. század egy-egy jelentős információbiztonság szempontból kiemelhető eseményét és az arra adott válaszokat tekintettük át.

Kulcsszavak

információbiztonság, információbiztonság fejlődéstörténete, információbiztonsági elvek, információbiztonsági mérföldkövek

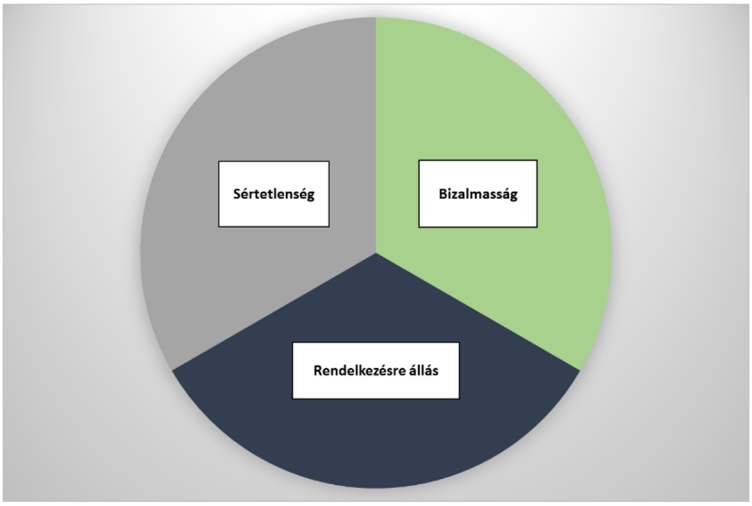
[1] szucs.endre@bgk.uni-obuda.hu | ORCID: 0000-0003-2818-262X | assistant professor, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering Institute of Mechanical Engineering and Security Sciences | adjunktus, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Gépészeti és Biztonságtudományi Intézet
[2] zahonyi.lajos@phd.uni-obuda.hu | ORCID: 0000-0001-9999-9624 | PhD Student, Óbuda University Doctoral School on Safety and Security Sciences | PhD hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

Jelen tanulmány fókuszában azon mérföldkőnek is tekinthető események, eszközök és eszközrendszerek állnak, amelyek jelentősen befolyásolták az információbiztonság fejlődését.

„Az információbiztonság helyzete sajátos, egyszerre van jelen egy szervezet minden területén, sőt, a feltételeinek megfelelő kialakítása és működtetése jóval túlmutat az információ biztonságos kezelésén. A szervezet minden erőforrásának, az embereknek, az eszközöknek, az információs rendszereknek, és más vagyontárgyaknak a szabályozását, viselkedését, használatát, ellenőrzését jelenti." [1]

Az információbiztonság három alappillérre épül. Az első, hogy az adott információ sértetlen legyen, pontos maradjon és ne torzuljon a második, hogy az arra felhatalmazott felhasználó mindig hozzáférjen az adott információhoz és kapcsolódó értékekhez végül pedig a harmadik a jogosultság, avagy bizalmasság kérdése azaz csak az arra jogosult vagy felhatalmazott személy számára legyen elérhető az adott információ.



1. Ábra: Információbiztonság alapelvei. Lehet tanulni a múltból. [2]

Ezen alappillérek mentén vizsgáljuk meg milyen eszközökkel és eszközrendszerekkel találkoztunk az elmúlt 100 évben milyen válaszok születtek a kor kihívásainak és technikai lehetőségeinek figyelembevételével egy-egy információbiztonsági „incidens" kezelésére, illetve kivédésére. Jelen írás keretei arra adnak lehetőséget, hogy a kor egy-egy jellegzetes incidensének és eszközrendszerének helyzetét vizsgáljuk meg. Ezen incidensek vizsgálata lehetőséget ad, hogy a jelen kor kihívásaira nagyobb hatásfokú választ legyünk képesek adni. A tanulmányban információbiztonsági incidensnek tekintjük „azokat a nem kívánt, illetve nem várt egyedi vagy sorozatos információbiztonsági eseményeket, amelyek nagy valószínűséggel veszélyeztetik a működési tevékenységet és fenyegetik az információk biztonságát" [3].

A számítógépek megjelenésével és gyors fejlődésével a kezelt információs adatok száma, mennyisége és tárolási nagyságrendje sokszorosára növekedett az azt megelőző időszakokhoz képest. A nagy koncentrációban történő adattárolás pedig új dimenziókat nyitott

az adatok mennyiségi feldolgozása területén. Aki ezekhez az adatokhoz hozzáfér, óriási információs erőforrásokhoz tud hozzájutni.

„Az információtechnológiai rendszerek és összetevők új sebezhetőségeket hordoznak, új - elsősorban információs jellegű - veszélyeztető hatások számára teremtenek lehetőségeket." [4] Az információk kezelőinek és használóinak óriásira nőtt a felelőssége abban, hogy ezen információk ne sérüljenek és ne torzuljanak, hogy a felhatalmazott felhasználók számára ezek az információk és kapcsolódó értékek mindig elérhetőek legyenek illetve hogy csak az arra jogosult vagy felhatalmazott személy számára legyenek elérhetőek. Ez egy védelmi rendszer kiépítését igényli, amely rendszer védelmi módszereket kíván.

INCIDENSEK, AMELYEK HATÁSSAL VOLTAK A FEJLŐDÉSRE

Jelen tanulmányunkat néhány jellegzetes példával indítjuk, amelyek a múltban az információbiztonság fejlődéstörténetében meghatározóak voltak. [5]

- A 1971-ben jelent meg az első vírus a „Creeper" [6]. Ez egy önreplikáló program volt, amelyet az internet elődjeként tekintett ARPANET-et használta a DEC PDP-10 számítógépek megfertőzéséhez és az alábbi üzenet megjelenítéséhez: „I'm the creeper, catch me if you can!" azaz „Én vagyok a Creeper, kapj el ha tudsz!".
- 1976 és 2006 között, azaz mintegy 30 éven át, Greg Chung Boeing alkalmazott 2 milliárd dollár értékű űrrepülési dokumentumokat adott át Kínának. A vizsgálat során 225.000 oldalnyi érzékeny információkat tartalmazó dokumentumokat fedeztek fel az otthonában. Ez volt a történelem legnagyobb léptékű rendszeren belülről jövő rosszindulatú támadása, amelynek az volt a célja, hogy egy idegen országnak juttassanak el katonai és űrkutatási szabadalmakat, dokumentumokat. Ez az incidens nem „csak" a Boeing vállaltot érintette, hanem az Amerikai Egyesült Államok nemzetbiztonságát is.
- 2013-ban „robbant" a Snowden ügy. Edward Snowden a CIA alkalmazottja volt és az Egyesül Államok kormányával volt munkaszerződése. A minősített információkat a National Security Agency-től másolta és szivárogtatta ki. Noha nem ez volt a legnagyobb belülről jövő támadás mégis ez az incidens volt az, amelyik a legnagyobb társadalmi vitát váltotta ki az Egyesült Államokban. A cselekedete megosztotta a társadalmat, sokan elvesztették a bizalmukat az állami szervekben ugyanakkor sokan a mai napig is hősnek tekintik Snowdent.
- Szintén még ez évben történt, hogy a hackerek egy csoportja feltörte mintegy 3 milliárd (!) Yahoo felhasználó fiókját. Nevek, jelszavak, valamint biztonsági kérdésekre adott válaszok kerültek veszélybe. A Yahoo próbálta eltusolni az ügyet és egészen 2016-ig nem jelentette be a jogsértést. Végül is az Egyesült Államok bírósága 35 millió dolláros kártérítést szabott ki a vállalatra amiért elmulasztotta az időben történő jelentést. Az ügy a Yahoo eladási árát 350 millió dollárral csökkentette.
- 2015-ben Az Egyesült Államok Személyzeti Ügyekért Felelős Hivatala (The U.S. Office of Personnel Management) támadás áldozatává vált. Az incidens során 4,2 millió volt és jelenlegi kormányzati személy, állományi adatait lopták el. Ez 21,5 millió átvilágítási vizsgálati fájlt és 5,6 millió ujjlenyomatot tartalmazott. Ez az esemény cselekvése ösztönözte a civil szervezeteket az adatbiztonság ügyének felkarolására.

- Az első „váltságdíjas" kriptoféreg a „Wannacry" 2017-ben jelent meg a Microsoft Windows operációs rendszer hiátusait kihasználva. A rendszer kódolta a gépen lévő adatokat és a helyreállító kulcsért cserébe Bitcoin kriptovalutát kért. A globális világunkban ez volt az első „féreg vírus", amely sokkolta a felhasználókat. Csak az első napon már megközelítőleg 230.000 számítógépet fertőzött meg 150 országban.
- Szintén 2017-ben jelent meg a NotPetya féregvírus, ami a Microsoft Operációs rendszer sebezhetőségét kihasználva több mint 12.500 – köztük energiaipari cégek, bankok, repülőterek és magasrangú állami tisztviselők - informatikai rendszeréből törölt adatokat és kért „váltságdíjat" a visszaállító kulcs megküldéséért cserébe.
- Az eddigi legnagyobb Hitelkártya adatlopási ügy is 2017-ben történt, amikor is a becslések szerint 143 millió adat került veszélybe amikor az Equifax Hitelintézet (Credit bureau, Equifax) 209.000 partnerének hitelkártyájához fértek hozzá a hackerek. Ez az incidens a vezérigazgató lemondásához vezetett.
- 2020 februárban az Amazon Web Services (AWS) a nyilvántartott eseteket tekintve az eddig legsúlyosabb túlterheléses (DDoS) támadást szenvedte el. A támadás során a legnagyobb adatforgalom 2,3 Tbps volt.
- 2021 május: a Colonial Pipeline amely az Egyesült Államok keleti partvidékét látja el üzemanyaggal, zsarolóvírusos kibertámadás áldozata lett. Ez a fajta vírus az, amely zárolja és titkosítja az áldozat számítógépes rendszerét és a feloldásért pedig váltságdíjat kér. Tekintve a támadás volumenét és célját, ez már az amerikai nemzetbiztonság helyzetét is befolyásolja.

Tudománytörténeti alapok

Egy tudományterület sem létezhet előzmények nélkül. Minden tudomány mozgásban van, minden tudomány keresi a válaszokat és ezáltal fejlődik. Ezek a válaszok egymásra épülnek és ebből újabb kérdések keletkeznek. A fejlődés megállíthatatlan. Ahhoz hogy jobban megértsük a jelen kor problémáit bátran vissza kell tekinteni a múltban és tanulni ezen válaszokból. Nincs ez másképpen a biztonságtudomány területén sem.

„A biztonságtudomány célja, hogy: a rendszerek biztonsági funkciói a kezdeti állapotuktól fogva elemzésre kerüljenek, a rendszerek biztonságának tervezése a lehetséges legnagyobb részletességgel kerüljön végrehajtásra." [7]

Az időben előre haladva a technika fejlődésével, újabb és újabb információvédelmi kihívások jelenek meg. Kicsit több mint, egy évtizede jelent meg az ISO27001-es információbiztonsági rendszer szabványcsalád, amely akkor egy megfelelő szabályozási válasz volt a kor kihívásaira. Magyarországon a jogalkotási rendszer szintén próbálja felvenni a tempót, amelyet ez a fejlődés okoz. A világ minden területén köztük az Európai Unióban és Magyarországon is folyamatosan születnek vonatkozó szabályozási formák, előírások és jogszabályok. [8] Ha az ok-okozati összefüggéseket vizsgáljuk, látjuk, hogy a biztonsági eszközrendszerek is folyamatosan változnak, alkalmazkodnak. Az adott kor kihívásaira az adott kor eszközrendszereinek és technikai színvonalának megfelelő válaszok érkeznek.

A biztonság megismerésének folyamatát történetileg négy szakaszra tudjuk felosztani. Ezek:

Az első szakasz az „ártatlanság kora" [9] amely az ipari forradalom előtti – a XVII.-XVIII. századig tartó – időt jelöli. E korszak jellemzője, hogy az ember még nem foglakozott tudatosan a biztonság mai értelemben vett problémáival, nem mérte és nem is elemezte

azokat. A természeti csapások, katasztrófák, járványok, de maga a háború jelenléte is egy elfogadott helyzetnek az élet velejáró részének tekintették. Bár az adott kor konfliktusai szintén válaszokat kényszerítettek ki, mégis a válaszok az eszközök és eszközrendszerek még inkább ösztönösnek tekinthetőek voltak, mint tudatosnak.

Második szakasz a „felfedezés kora" [10] amely az ipari forradalom bekövetkezését követő és a XIX.- XX. század fordulójáig tartó időszakot jelöli. Ebben az időszakban már felismerték a biztonság fontosságát és már kidolgoztak elméleti alapokat. A műszaki tudományok vagy az orvostudomány már rendelkezett bizonyos eszközökkel, amely alapján feljegyezték és használták az elméleti alapokat. Ebben az időszakban a társadalmi fejlődés magával hozta az igényt a biztonság szükségességére. „Az új eszközök és technológiák alkalmazása során az ember felfedezte a biztonsági problémákat maga körül és így tehetett néhány kezdeti lépést a veszélyes szituációk feloldása felé." [11]

Harmadik szakasz a „rendszerbiztonság" [12] kora, amely XX. század elejétől induló fejlődési robbanásra adott válaszok mentén jegyezhető. Magas fokú ipari fejlődés, a hadipar fejlődése, az új technikai vívmányok, mint a repülő, az automobil kifejlődése és elterjedése vagy később az űripar kialakulása jellemzi.

A negyedik a „biztonságtudomány" [13] szakasza, amely már a tudomány és technológia fejlődésére egzakt és érdemleges válaszokat nyújt. Az ember már felismeri a biztonsággal kapcsolatos alapelveket és összefüggéseket, kialakítja a maga eszközrendszereit és ezen eszközrendszereinek segítségével kidolgozza az erre vonatkozó válaszokat. Legyenek azok akár különböző technikák vagy rendszerek.

Tudománytörténetiséget tekintve a jelen tanulmány az Első Világháború információbiztonsági kihívásaiból indulva tekinti végig a XX. és XXI század jellegzetes információbiztonsági incidenseit.

„Cher Ami" – egy élő „eszköz" az Első Világháborúból

Az információ eljuttatásának módja és az információ védelme nagyban az adott kor jellemző eszközeinek hatékonyságán alapul. Ha manapság megírunk egy e-mailt és annak egyértelmű és valós címzettet adunk, akkor az az üzenet továbbításra kerül. 100 évvel ezelőtt a kézbesítés szerepét sok esetben a kor eszközrendszer részének is tekinthető postagalambok látták el. [14]

Az Amerikai Egyesült Államok 1917-ben belépett az Első Világháborúba az Antant oldalán. 1918. októberében az argonne-i erdőben az amerikai hadsereg tüzérsége a saját alakulatainak állásait lövi, ugyanis nem áll rendelkezésre az a pontos információ, amelyben a pontos koordinátákat vagy helyet jelölnék. Ekkor indítják útnak az utolsó hírvivő galambjukat az alábbi üzenettel: "We are along the road parallel to 276.4. Our own artillery is dropping a barrage directly on us. For heaven's sake, stop it." Major Charles W. Whittlesey 4 October1918. Magyar fordításban: „A 276,4-el párhuzamos úton haladunk. Saját tüzérségünk közvetlenül ránk lő. Az ég szerelmére állítsátok le. – Charles W. Whittlesey őrnagy" [15]

2. Ábra: Az információk rendelkezésre állása nem tekinthető evidenciának – A korabeli eszközrendszerek része a galamb, amely lehetővé tette, hogy az információk elérhetővé váljanak. [16]

Ez a hírvivő galamb akit úgy hívtak „Cher Ami" (Kedves Barát), 25 mérföldet repül, 25 perc alatt és eljuttatja az üzenetet az amerikai főhadiszállásra, miután azonnal beszüntetik az ágyúzást, ezzel megmentve mintegy 200 amerikai katona életét. „Cher Ami"-t útja során többször eltalálták, elvesztette az egyik szemét és az egyik lábát. Az üzenet azonban elérhetővé vált. Az Első Világháborúban a postagalambokat mind az Antant mind a Központi Hatalmak széles körben alkalmazták. Az egyik legbiztosabb információs eszközök voltak az adott korban. Korabeli megfigyelések szerint, a postagalambokkal indított üzenetek 95%-a célba ért. Ez mai szemmel nézve is egy komoly eredmény.

Enigma - kódolás

Mint ahogy a kiberbűnözés világában úgy 80 évvel ezelőtt a II. Világháborúban sem volt más a cél: adatok megszerzése és a megszerzett adatok valamely előnyös felhasználása.

Az információbiztonság történet vizsgálatának az egyik mérföldköve, a kódoló gépek megjelenése amelyek már bizonyosfajta számítógépnek is tekinthetőek. A kódoló gépek szerepe az, hogy az információkat csak és kizárólag az arra jogosult felhasználó tudja értelmezni. A háborúban minden információ szerepe felértékelődik és a gépekkel küldött üzenetek védettsége nagyban a kódolás összetettségén múlik. Ezért a kódoló gépek feltörése és ezáltal a szó szerint életbevágó információk megszerzése elemi érdeke mindegyik harcoló félnek. A kódoló gépek biztonságának szükségessége – beleértve maga szerkezetet és a benne lévő adatokat is – a második világháború idején merült fel először, amikor is az első nagygépeket, - amelyeket a kommunikációs kódok törésének számításainak elősegítésére fejlesztettek ki - használatba vették. Védeni kellett a gép fizikai helyét, a benne lévő szerkezetet (hardver) és kódolási elveket (szoftver) a fenyegetések ellen. Több szintű biztonság eszköze volt melyek között a védett katonai helyszínek a jelvények, a kulcsok és arckezelés használata volt a legjellemzőbb és amelyeket dedikált biztonsági személyzet segítségével ellenőriztek.

3. Ábra: Az Enigma – német gyártmányú, forgótárcsás, elektromechanikus berendezés, amelyet a II. Világháború alatt használtak a németek. [17]

Az Enigma név termékcsaládot takar, amely számos modellből állt 1923-1945 között. A gépeket többször is feltörték és ezzel a háború idején a Szövetségesek jelentős információs lépéselőnyben voltak [18].

Hidegháború korszaka és a 60-as évek

A hidegháború idején jelentősen megnőtt az igény bonyolultabb és kifinomultabb feladatok elvégzésére és az adatok tárolására. Szükségessé vált a gyakran teremnyi méretű nagygépek közötti kommunikáció javítása és az akkor használatos mágnesszalagos adattovábbítás, illetve adatkommunikáció hatékonyabbá tétele. Az Egyesült Államok Honvédelmi Minisztériumának Fejlett Kutatási Projekt Ügynöksége (Department of Defense's Advanced Research Project Agency, a továbbiakban ARPA) megkezdte egy redundáns és közös hálózatba kapcsolt kommunikációs rendszer megvalósíthatóságának vizsgálatát annak érdekében, hogy támogassák a katonai információcserét. A programot 1969-ben az internet alapítójaként is emlegetett Larry Roberts koordinálta. Ezt a rendszert nevezték ARPANET-nek amely gyakorlatilag a ma ismert internet történeti előzménye volt.

A 70-es 80-as évek

A következő évtizedek során az ARPANET népszerűvé és széles körben elterjedté vált. Az ARPANET-ben lévő potenciál egyre erősebb kihasználása miatt a visszaélések száma is gyakoribbá vált. 1973 decemberében Robert M. "Bob" Metcalfe, - akinek nevéhez később az egyik legnépszerűbb hálózati protokoll az Ethernet fejlesztése fűződik - felismerte az ARPANET biztonságával kapcsolatos alapvető problémákat. Az rendszerben lévő egyes távoli helyszínek nem rendelkeztek elegendő kontrollal és védelemmel az adatok illetéktelen felhasználóktól történő távoli megvédésére. Egyéb problémákkal is bővelkedett a rendszer, úgymint: a jelszó szerkezetének és formátumainak sebezhetősége, a telefonos kapcsolatokhoz igazodó biztonsági eljárások és felhasználói azonosítás hiánya.

A gazdagépek és felhasználók számának robbanásszerű ugrása következményeként a rendszerben lévő telefonszámokat széles körben terjesztették és nyíltan nyilvánosságra hozták a például a telefonfülkék falain. Ezek után nem csoda, hogy a korabeli „hackereknek" könnyű hozzáférésük lehetet az ARPANET-hez. Ezt a súlyos információbiztonsági rést egy 1978-ban megjelent tanulmány a „Protection Analysis: Final Report" leplezte le

egyértelműen. Ebben a tanulmányban írták le és fejtették ki az ARPANET operációs rendszerek biztonságának sebezhetőségét. Ezt követően az amerikai védelmi minisztérium reagált és kiadott egy mérföldkőnek tekinthető dokumentumot: Rand Report R-609. Ez az első dokumentum, amely definiálta a többszintű számítógépes rendszer tartalmát és ez az a papír amelytől számíthatjuk a számítógépes biztonság kezdetét.

A Rand Report R-609 volt az első széles körben elismert publikált dokumentum, amely azonosította a menedzsment szerepét és a szervezeti / vállalati policy jelentőségét a számítógépes biztonságban.

A riport megállapította, hogy a széles körű használat a katonai információs rendszerek hálózati komponenseinek bevezetése jelentős biztonsági kockázatokat hozott magával, amit nem tudtak enyhíteni az akkori elhárítási rutin gyakorlatok, amelyeket e rendszerek biztonsága érdekében használtak. A riport három lényeges területet azonosított:

- Az adatok biztonsága.
- Az adatok véletlenszerű és illetéktelen hozzáférésének korlátozása.
- A személyzet bevonása a szervezet több szintjéről az információbiztonság megteremtése érdekében.

A kor jellegzetes információbiztonsági eseményei:

Év	Információbiztonsági esemény
1967	Jelszóbiztonság megjelenése a számítógépes rendszerekben
1973	A katonai rendszerek többszörös biztonsági mechanizmusának megjelenése
1975	Digital Encryption Standard (DES) megjelenése
1978	Operációs rendszer biztonság és automatizált sebezhetőség észlelésének megjelenése
1979	Biztonságos felhasználó azonosítás
1984	Számítógépes biztonsági kontrolok azonosítása: fizikai ellenőrzés, menedzsment elkötelezettsége, alkalmazottak oktatása és adminisztratív eljárások kidolgozása
1984	Crypt parancs megjelenése az UNIX-ban és általános fájlbiztonság megjelenése
1990	A hitelesség, a rendelkezésre állás és a hasznosság kérdése kapcsán megjelenik az első információbiztonsági triád: titoktartás, elérhetőség és integritás.

1. Táblázat: Főbb információbiztonsági események a 70-es-80-as évekből. [19]

Az internet megjelenése a 90-es években

A 20. század végén a személyi számítógépek használata egyre inkább elterjedt és vele együtt az az igény is, hogy ezek a számítógépek hálózatban csatlakozzanak egymáshoz. Ez az igény hozta létre hálózatok globális hálózatát az internetet. Az internet gyakorlatilag minden számítógéphez csatlakozási lehetőséget adott, amelynek volt telefonvonali vagy csatlakoztatott helyi hálózat (LAN) elérése. Az internet kereskedelmi forgalomba hozatala után a technológia elterjedté vált, a világ szinte minden sarkába eljutott. Az internetes kapcsolatok eleinte, de facto szabályokon alapultak, amelyek alig tették lehetővé az információk biztonságát. Később, mivel ezeket az előd technológiákat széles körben elfogadták és ipari szabványokká váltak, és ez bizonyos fokú biztonságot eredményezett. A korai internetes telepítések azonban alacsony prioritásként kezelték a biztonságot, hiszen abban az időben, amikor szinte az összes internet és e-mail felhasználó informatikus volt, a mail szerver hitelesítés és az e-mail titkosítás nem tűnt szükségesnek. Valójában sok olyan probléma merül fel, amely manapság is levelező rendszerinket sújtja az interneten. Ahogy a számítógépek hálózatos összeköttetésbe kerültek, elveszett a hálózatba kötött számítógép fizikai biztonságának képessége, és a tárolt információk jobban ki voltak téve fenyegetéseknek.

2000-es évek válaszai

Az Internet a számítógépes hálózatok millióit hozza folyamatos kommunikációba egymással. Az egyes számítógépek tárolt adatainak biztonsága függ minden további számítógép biztonsági szintjétől, amellyel kapcsolódik. A 2000-es évek elejétől kezdve egyre nagyobb tudatosságot tapasztalunk az információbiztonság javításának szükségessége kapcsán. Megjelennek az ajánlások és a szabványok.

A szabványosítási törekvések az információtechnológia fejlődéssel parallel módon erősödtek. Az 1980-as évektől kezdve számítógépek üzleti célú felhasználása egyre elterjedtebbé vált. Az üzleti folyamatok és benne az adatok használata kezdett az egységes gyakorlat irányába haladni. Egyre nagyobb igény merült fel valamilyen egységesített keretrendszer létrehozására, amely mintegy „sorvezetőként" segíti a rendszerben lévő információk védelmét.

Erre az igényre először a COBIT (Control Objectives for Information and Related Technology) adott választ, amely nem szabvány és nincs szabványként bejegyezve, a gyakorlatban azonban sokszor szabványszerűen alkalmazzák. Ez egy informatikai ajánlási gyűjtemény egy keretrendszer, amely elsősorban az információtechnológiai auditálás céljait szolgálja.

A másik irány a szabványosítás. Erre példa az ISO27001 nemzetközi szabvány, amely abból a célból készült, hogy követelményeket adjon egy információbiztonság-irányítási rendszer kialakítására, bevezetésére, fenntartására és folyamatos fejlesztésére. [20] A szabvány folyamatközpontú, alkalmazza a Plan-Do-Check-Act (PDCA) modellt és a megvalósított IBIR integrálható a meglévő minőségirányítási (ISO 9001) és a környezetirányítási (ISO 14001) rendszerekkel. Egy adott szervezet számára stratégiai döntés, hogy bevezeti-e az információbiztonság-irányítási rendszert vagy sem. A rendszer kialakítását befolyásolja a szervezet céljai, folyamatai, a szervezet mérete és felépítése, illetve a biztonsági elvárásai.

Az információbiztonság-irányítási rendszer egy kockázatkezelési-folyamat segítségével őrzi meg az információk bizalmasságát, sértetlenségét és rendelkezésre állását, és az

érdekelt felekben bizalmat kelt a tekintetben, hogy a kockázatokkal kielégítő módon foglalkoznak. [21]

Záró gondolatok

Mint minden tudomány a biztonságtudomány területe is folyamatos fejlődésben van. Kiváltképp igaz ez biztonságtudományon belül az információbiztonság területére.

A cikk néhány sajátos példát megjelenítve rámutat arra, hogy az információbiztonság történelmének eseményei komoly hatással voltak és vannak az információbiztonság fejlődésére. Ezeket a hatásokat – az információbiztonság helyzete és viszonyulási eszközrendszereinek tekintetében - egyfajta mérföldköveknek is tekinthetjük.

„Az informatikai rendszerre vonatkozó információk tartalmazzák az adott rendszer felépítésére, működésére vonatkozó adatokat és a rendszerhez csatlakozó eszközök jellemzőit. Nem létezett és nem létezik tökéletes biztonság. A fejlődéssel párhuzamosan folyamatosan jelennek meg újabb és újabb támadási módszerek, biztonsági rések, ennek következtében minden kockázatra kiterjedő védelemről sem beszélhetünk.” [22]

FELHASZNÁLT FORRÁSOK

[1] Horváth G. K., Közérthetően az IT biztonságról. Budapest: KIFÜ, 2013 p.13
[2] Előadáson ismertetett saját ábra
[3] https://sealog.hu/tudastar/fogalomtar/informaciobiztonsagi-incidens [letöltés ideje: 2021.05.22.]
[4] Munk S., Információbiztonság vs. Informatikai biztonság. Hadmérnök Különszám Robothadviselés 7. Tudományos Szakmai Konferencia ROBOTHADVISELÉS 7. TUDOMÁNYOS SZAKMAI KONFERENCIA [2007. november 27.] p1
[5] S. Hospelhorn, Events That Changed Cybersecurity Forever 3/29/2020 [letöltés: 2020.05.25.] pp 1-5
[6] A „Creeper” angol kifejezést a https://gyerekaneten.hu/szocikk/creeper forrás alapján használjuk. Jelentése: olyan személy, akitől az embernek borsódzik a háta, vagy akiből simán kinézi, hogy zaklat másokat.
[7] Kiss S., Biztonságtechnika alapjai, Budapest: Óbudai Egyetem, 2019 p13
[8] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
[9] [10] [11] [12] [13] KISS S., A biztonságtechnika kialakulásának történetéről. Hadmérnök X. Évfolyam 4. szám 2015. december, pp. 26-28.
[14] Magyar Nemzeti Levéltár Katonagalambok az I. világháborúban http://mnl.gov.hu/mnl/nml/csak_a_legritkabb_esetben_tagadja_meg_a_szolgalatot [Letöltés ideje: 2021.05.20]
[15] Fordítás: Záhonyi Lajos
[16] https://www.worldwar1centennial.org/index.php/communicate/press-media/wwi-centennial-news/1210-cher-ami-the-pigeon-that-saved-the-lost-battalion.html [Letöltés ideje: 2021.05.20]
[17] https://www.smithsonianmag.com/smart-news/wwii-enigma-machine-found-flea-market-sells-51000-180964053/ [letöltés ideje: 2021.05.21.]

[18] Whitman, M. E., Introduction to Information Security cengage learning Principles of Information Security, 4th Edition, Institute for Cybersecurity Workforce Development, Kennesaw State University Herbert J. Mattord Michael J. Coles College of Business, Kennesaw State University pp4
[19] Moinak, A. M., Information Security – Evolution, Impact and Design Factors. International Journal of Computer Applications (0975 – 8887) Volume 100– No.2, August 2014 pp.3.
[20] [21] MSZ ISO/IEC 27001:2014 P6
[22] Az információbiztonság lélektana (Psychology of Information Security) https://nki.gov.hu/wp-content/uploads/2019/07/01-Az-inform%C3%A1ci%C3%B3biztons%C3%A1g-l%C3%A9lektana.pdf [letöltés ideje: 2021.05.21.] p10