

Intézményi bizalom növelése a Kormányzati Hitelesítés-Szolgáltató, mint SZEÜSZ felé

Erdősi Péter Máté

2019. január 11.

Bevezetés

Az intézményi bizalom megteremtése nem nélkülözheti a három népszerű fogalom, a bizalom, a biztonság és a sérülékenység közötti kapcsolatrendszer boncolgatását és elemzését meglátásom szerint, amit az alábbiakban megkísérlek bebizonyítani.

A bizalom szót gyakran használjuk a mindennapokban, de amikor meg akarjuk ragadni a lényegét, sokszor korlátokba ütközünk. Feltehető emiatt az a kérdés, hogy lehetséges-e ezeket a korlátokat keretekbe szintetizálni?

A bizalom és a biztonság között is gyakran feltételezhető valamilyen kapcsolat, ezt fogjuk a következő szakaszban néhány esettanulmányt feldolgozva megvizsgálni. Külön figyelmet érdemel a hitelesség, mint biztonsági elem, ezért az esettanulmányok egy részét a hitelességi témakörből fogjuk venni. Megemlíjtük továbbá a biztonság olyan definícióját is, mely visszanyúlik az első biztonsággal kapcsolatos matematikai modellek létrejöttéig és említés szintjén vizsgálat alá kerülnek a modellek egymásra gyakorolt hatásai is.

A biztonság elleni külső fenyegetések megvalósítását lehetővé tevő belső tényezők a sérülékenységek, ebből adódóan valamilyen kapcsolatuk biztosan létezik a biztonsággal és a bizalommal is. Ha növekszik a bizalom, ennek hatással kell lennie a biztonságra is, amennyiben a bizalom tárgya erősíti a biztonság szintjét.

Mi az a bizalom?

A „bizalom” szó definíciója: (Magyar Értelmező Kéziszótár [1])

1. A körülmények kedvező alakulásába vetett hit, bizakodás.
2. Az olyan személyre irányuló érzésünk, akiben (meg)bízunk.

Pol: Bizalmat szavaz vkinek, vminek: Szavazatával kinyilvánítja, hogy bízik a vezetésben.

A fentiekből is kiderül, hogy a bizalom egyszer egy tevékenység (bizakodás, szavazás), másszor egy érzés – vagyis többértelmű fogalom.

Lőrincz András „A társadalmi bizalom” című előadásában [2] A Haza Szolgálatában 2014 konferencián ismertette a bizalom kategóriáit, amelyeket az alábbiakban jelölt meg:

1. feltétlen bizalom: bizalom minden és mindenki iránt (ősbizalom),
2. intézményi bizalom: az egyes intézmények irányában megjelenő kapcsolati minőség,
3. interperszonális bizalom: az egyes emberek egymás közötti kapcsolatára utaló fogalom.

Kapcsolat a bizalom és a biztonság között

Vasvári György szellemes megfogalmazásában [3] a biztonság olyan kedvező állapot, mely megváltozása nem valószínű, de nem is lehet kizárni. Ebben az értelmezésben a „biztonság” a „bizalom” tárgyának materializált formája, hiszen míg a „bizalom” egy (emberen belüli) hit, bizakodás, érzés, addig a „biztonság” mérhető (emberen kívüli) valóság, mely tevékenységek révén áll elő és maradhat fenn. Visszahatás is létezhet közöttük, hiszen a „gondolat-érzés-cselekedet” láncolatban a tevékenység későbbi, míg az érzés korábbi eleme az időszámításnak, és a biztonság megteremtésére és fenntartására irányuló tevékenységek (védelem) megteremtése nélkül a biztonság mérhető értéke nem változik.

A biztonság formális modelljei már viszonylag régen ismertek, példának felhozható Landwehr 1981-es cikke [4], melyben összefoglalja az addig létrejött biztonsági modelleket.

Anélkül, hogy belemennénk a formális modellek ismertetésébe, összefoglaló jelleggel annyit

mondhatunk, hogy formális szempontból a biztonság egy véges állapotú (Turing) gép azon állapotainak halmaza, melyek úgy jöhetnek létre, hogy engedélyezett állapotból engedélyezett műveletekkel az adott objektumok tulajdonságait engedélyezett módon megváltoztatják. Amíg ezen belül maradunk, addig biztonságban vagyunk, amint kilépünk, elveszítettük a formális biztonságot. Érdekes itt még az is, hogy az egyes formális modellek között ütközés áll fenn, például a bizalmasság modellje teljesen ellentétes a sértetlenség modelljével, ami azt jelenti, hogy másként kell a kettőt biztosítani.

Meg kell itt említeni Muha Lajos informatikai biztonsági rendszertanában [5] alkalmazott definícióját a biztonságnak, mely szerint a biztonság a rendszer olyan — az érintett számára kielégítő mértékű — állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg. Láthatóan tehát a biztonság nem hit, bizakodás eredményeként jön létre, hanem védelem megvalósításával, vagyis tevékenységek révén.

A kockázatok és a biztonság közötti összefüggés ebből tehát világos. Az arányosság annyit jelent, hogy egy bizonyos kockázattűrő képességi szint alatt biztonságban vagyunk, felette pedig nem. Vagyis a kockázatok értékének kiszámításával és számosságukkal is jellemezhető a biztonság, az incidensek számossága mellett. Az incidensek számossága pedig egyenesen arányos a – statisztikailag kezelhető – kockázatokkal, és fordítottn arányos a biztonsággal. A fordított arányosság természetesen súlyozottan kerülhet csak megállapításra, hiszen egy nagy kockázat kárkövetkezménye felérhet 1000 alacsony kockázat kárkövetkezményével is. Megemlítjük, de részletezésétől eltekintünk annak, hogy ugrásszerű változások általában akkor következnek be a biztonság érzékelésében, amikor statisztikailag nem kezelhető kockázatok következnek be (pl. 9/11, Csernobil). Természetesen ezeket is lehetséges kezelni, de más módon – ezekhez eszközül a logikai és a percepciók kockázatelemzés módszertana szolgál, melynek tárgyalásától itt eltekintünk.

A bizalom és a kockázat a döntéshozatal két oldala, melynek nemcsak pozitív, hanem negatív oldala is létezik (2004, Audun Jøsang and Stephane Lo Presti, [6]), akik egyébként a bizalmat a negatív következmények lehetőségei ellenére valakitől illetve valamitől való függésre vonatkozó hajlandósággal definiálták. A bizalom és a kockázat táblázatát Manchala [17] az alábbiakban adta meg, a múltbéli tranzakciók minősítése és az ellenőrzés szükségességének megítélése közötti összefüggés bemutatásával:

		V Verify every transaction				
Transaction history	Excellent					V
	Good				V	V
	Normal			V	V	V
	Bad	V	V	V	V	V
	Worst	V	V	V	V	V
		Micro	Small	Medium	High	Expensive
		Cost of one transaction				

(Forrás: D.W. Manchala: [17: 39])

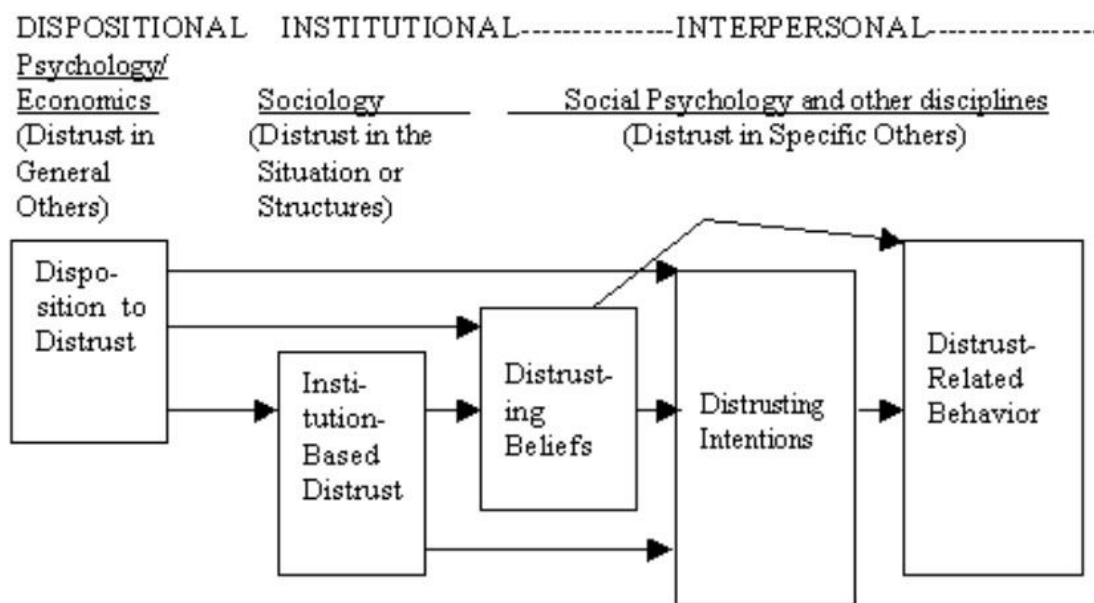
Az ábráról az olvasható le, hogy míg a magas költségű tranzakciókat szinte kivétel nélkül ellenőrizni kell akkor is, ha minden rendben volt a múltban, addig ez az ellenőrzési kényszer a tranzakciók költségének csökkenésével valamelyest elmúlik, és a múltbéli tranzakciók megbízhatóságától függ. Manchala megállapította, hogy a hitelkártya-tranzakciók historikus elemzése semmilyen támpontot

nem ad a bizalom elméleti megalapozásához, továbbá az online tranzakciókkal szembeni bizalom támogatására sem alkalmas. Ez a megállapítás azért figyelemre méltó, mert a hitelkártya-történet alapvetően a kártya jelenlétét fizikailag megkövetelő tranzakciókon (card-present, CP) alapul (webkártya szolgál az online tranzakciókra), míg az elektronikus hitelesítés alkalmazásánál jellemzően az ügyfelek nincsenek fizikailag jelen a hivatalban. Ebből következik, hogy a bizalom üzleti modellje a közigazgatásban csak módosításokkal alkalmazható. Egyik módosító tényező az aláírások ellenőrzése, mely ügýtípustól és ügyértéktől függetlenül minden esetben végre kell hajtani az ügyintézés megelőzően, a másik a bizalom mértéke, mely nem függhet az ügyfél múltbéli ügyintézési teljesítményétől.

Szabó Katalin és Hámori Balázs [7] játékelméleti megközelítésben vizsgálja meg az eladó és a vevő kontextusában a csalás-korrekttség és ellenőrzés-nem ellenőrzés párok alakulását, a kifizetések és egyensúlyok kiszámításával. Mindkét fél kifizetése akkor a maximális, ha az ellenőrzés költsége és a csalárd tranzakciók értéke minimális. Ők mondják azt, hogy az üzleti szereplők esetében a kockázatok csökkentése a biztonság növelését jelenti. A kockázatcsökkentésre négy alapvető mechanizmust definiálnak:

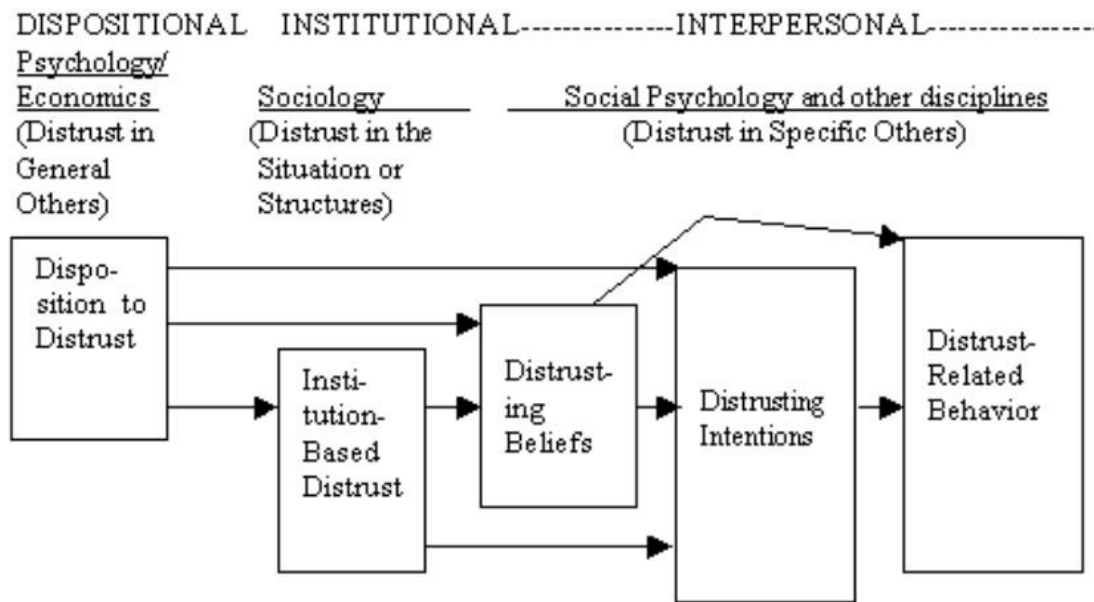
1. tranzakciók technikai biztonságának növelése
2. tranzakciók korrekttségét garantáló, a tisztességtelenségből (vagy másból) adódó károkat ellensúlyozó és szankcionáló jogintézmények kiépítése
3. társadalmi mechanizmusok kifejlesztése, melyek elviselhető mértékűre csökkentik a kockázatot, a személyes bizalmat támogatva
4. személyes bizalom (interpersonal trust)

A bizalom és bizalmatlanság vonatkozásában azok struktúráját a következőképpen rögzítették:



A bizalom interdiszciplináris modellje

Forrás: R. Falcone, M. Singh, and Y.-H. Tan (Eds.): Trust in Cyber-societies [8].



A bizalmatlanság interdiszciplináris modellje

Forrás: R. Falcone, M. Singh, and Y.-H. Tan (Eds.): *Trust in Cyber-societies* [8].

Ebből adódik, hogy az állampolgárok hiába bíznak meg egy-egy ügyintézőben interperszonálisan (mert például ismerős, szomszéd, rokon, ismerős ismerőse), ez nem jelent automatikus bizalmi transzfert az ügyintézők által képviselt intézmény és szolgáltatásai felé, ahogyan ezt a Mozilla fogalmazta meg a hitelesítés-szolgáltatók számára: „CAs *SHOULD NOT* assume that trust is transferable.”¹ Az ábrából látható továbbá, hogy a bizalom alapú viselkedésnek sok esetben előfeltétele az intézményi bizalom megteremtése a kibervilágban, mely különbözik az interperszonális bizalomtól.

Hitelesség és bizalom

Egyik példaként tekintsük meg azt az esetet, amikor két kód-aláíró tanúsítványt adtak ki a Microsoft Corporation számára, mint később kiderült, jogosulatlanul. A hitelesítésszolgáltató (Verisign) telefonos visszahívást is alkalmazott, mégis sikerült a csalóknak a tanúsítványokat megszerezniük. Milyen kockázatot jelenthet ez? Az automatikus frissítés révén számítógépek százmillióihoz juthat el azonnal (rövid időn belül) egy rosszindulatú kód (malware), mely lehet akár egy botnet-szoftver is, főként akkor, ha érvényes digitális aláírással van ellátva. Az eset 2001-ben történt, a bizalom a kód-aláíró tanúsítványokkal szemben azóta sem változott jelentősen. Kérdés persze, hogy létezik-e egyáltalán ez a bizalom, a frissítések vagy programok telepítésénél mennyire gátló tényező ma az esetenként a csomagokon elhelyezett digitális aláírás érvénytelensége. A microsoftos esetről kibocsátott CERT Advisory így aposztrofálta azt [9]:

„On January 29 and 30, 2001, VeriSign, Inc. issued two certificates to an individual fraudulently claiming to be an employee of Microsoft Corporation. Any code signed by these certificates will appear to be legitimately signed by Microsoft when, in fact, it is not. Although users who try to run code signed with these certificates will generally be presented with a warning dialog, there will not be any obvious reason to believe that the certificate is not authentic.”

Ennek ellenére a Microsoft és a VeriSign szolgáltatásaival szembeni bizalom lényeges csorbát akkor nem szenvedett.

Másik jól ismert eset a Diginotar esete. Amikor 2011-ben távolról sikerült teljes mértékben

¹ <https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/>

meghackelni a holland igazságügy-minisztérium szolgáltatóját, ez totálisan visszavetette a holland minisztérium bizalmát (és sok más szereplőét is) a PKI technológiában, a Diginotar pedig csődbe ment és meg is szűnt. A támadás pikantériája, hogy vélhetően több hónapon keresztül fennállt, mielőtt külső szereplők (Google) azt észrevették és jelezték a szolgáltatónak.

A vizsgálati jelentést nyilvánosságra hozták [10]. A nyomozati kérdések igen érdekesek és kényelmetlenek egy bizalmi szolgáltatást emelt szinten nyújtó szervezet részére:

1.2 Nyomozati kérdések

A nyomozás az előzetes információk alapján a következő kérdésekre fókuszált:

1. Hogyan fértek hozzá a behatolók a hálózathoz?

2. Mi a behatolás terjedeleme és állapota?

- Történt-e másik DigiNotar CA környezetbe is betörés?
- Láthatóak-e még mindig hacker-aktivitások a DigiNotar belső hálózatán?
- Elkezdtek-e aktívan használni a hackerek a hamisított tanúsítványokat?

3. Felfedezhető-e bármilyen következménye az incidensnek?

- Mely tanúsítványok lettek kibocsátva a DigiNotar tudta nélkül?
- Milyen más hamis tanúsítványokat generálhattak a támadók?
- Mennyi hamisított kapcsolatot létesítettek a hamis tanúsítványokkal?
- Milyen természetűek voltak ezek a kapcsolatok?

Következmény:

- 2011. szeptember 3: A holland kormány nyilvánosan megvonta a bizalmat a DigiNotar-tól és az általa kibocsátott tanúsítványoktól. Ennek a bejelentésnek a következményeként a legtöbb böngésző gyártója is megvonta a bizalmat a DigiNotar-tól – ha még nem tették volna meg ezt korábban.
- 2011. szeptember 5: A betörésről készült belső vizsgálati jelentést nyilvánosságra hozták, a DigiNotar hivatalosan is megtette a rendőrségi feljelentést.
- 2011. szeptember 14: az OPTA megszüntette a DigiNotar B.V. minősített hitelesítés-szolgáltatási tevékenységek nyújtására jogosító regisztrációját a holland távközlési törvény alapján (Dutch Telecommunicatiewet)
- 2011. szeptember 19: a DigiNotar csődvédelmet kért a holland csődvédelmi törvény 4. cikke alapján
- 2011. szeptember 20: a Haarlem Bíróság megállapította a DigiNotar B.V. csődjét.
- 2011. szeptember 28: a DigiNotar által kibocsátott összes minősített és PKI-alapú tanúsítványt visszavonták, azaz végleg érvénytelenítették.

Ebben az esetben a bizalom megszűnt, mely a szervezet és a szolgáltatás megszűnését is maga után vonta.

Nem hitelességi témakörből vehetjük például az autó-visszahívási eseteket, melyek jól kimutatható módon rövid időtávon belül csökkentik az eladási adatokat, vagyis a bizalmatlanság itt is pénzbe kerül – a gyártónak mindenesetre.

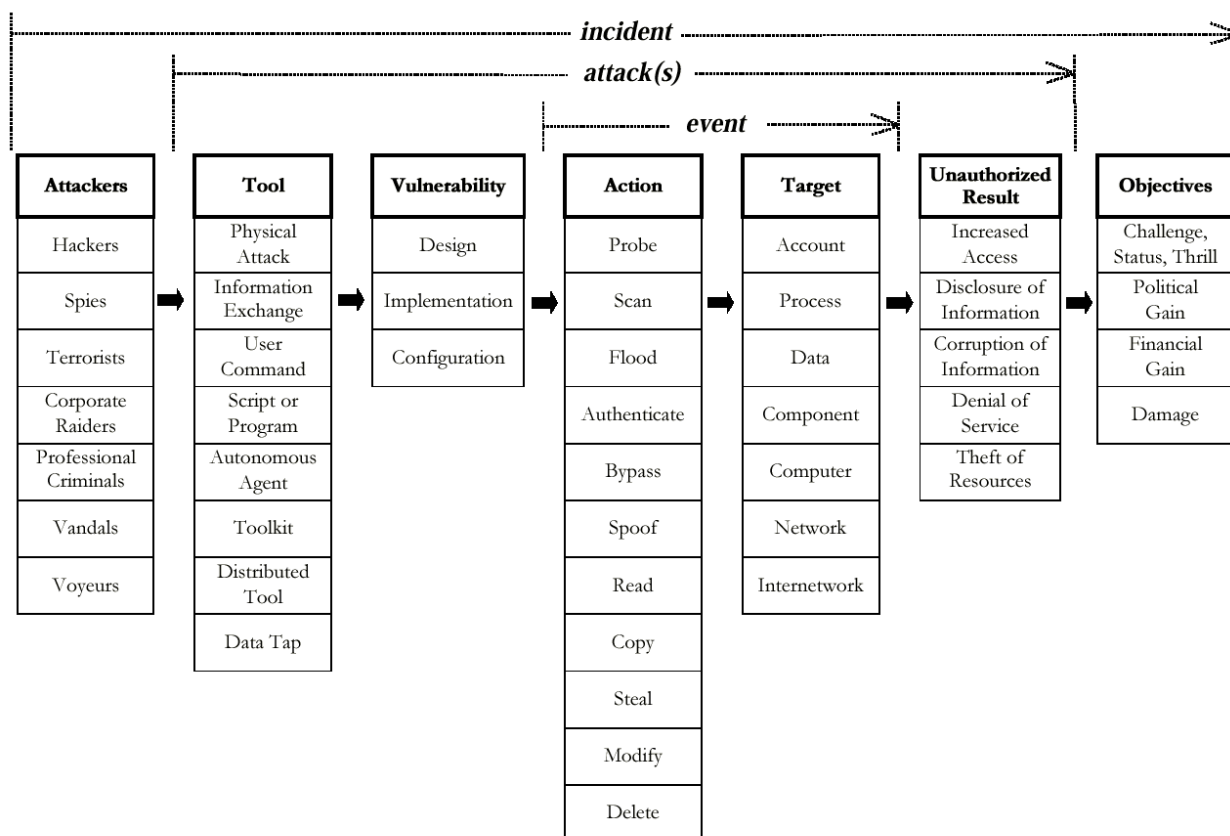
1969-ben a General Motors 4,9 millió autót hívott vissza biztonsági okokból, ez akkor kb. 50 M USD-be került a cégnek [11]. Azóta is számos ilyen hír érkezett az autógyártókról, például a GM 2010-ben több mint 3 millió, 2009-ben 2,2 millió autóját volt kénytelen visszahívni az Egyesült Államokban. A Chrysler több százezer autót rendelt vissza 2010-ben, a Ford pedig 2009 őszén történetének legnagyobb, 4,5 milliós visszahívásáról döntött. A Toyota 2009-2010-ben világszerte több mint 8

millió autóját rendelte vissza különféle meghibásodások, köztük a gázpedál beragadásának kockázata miatt [12].

A gyártók érintettségének uniformizálódása vélhetően csökkenti ezt a fajta hatását a felbukkanó sérülékenységeknek, illetve a gyakori használati igény lerövidíti a negatív periódus hosszát – mivel nincs reális sérülékenység-mentes alternatíva, ezért a felhasználók *kénytelenek* használni a sérülékeny eszközöket. Hozzá kell tenni, hogy léteznek megbízhatósági listák is a tárgyban, melyeken a visszahívást bejelentő gyártók termékei is ott találhatók. (Pl. ADAC lista [13])

Sérülékenységek és biztonság

A CERT-ek folyamatosan közzéteszik a sérülékenységek listáját és tulajdonságait. Ehhez a gyakorlatban az ún. Howard-sémát alkalmazzák mind a mai napig Common Language Security Incident Taxonomy néven, John D. Howard 1997-ben elkészített, az internetes biztonsági incidensek analizálásáról szóló publikációjában [14] lefektetett taxonómia alkalmazásával, mely azóta Howard-séma néven is ismert. Ezt a CERT-ek azóta is használják – módosítás nélkül – osztályozási rendszerként. A séma technikai riportként is megjelent a SANDIA kutatólaboratórium publikációi között 1998-ban [15].



A séma [16] lényege, hogy a támadó valamilyen eszköz segítségével kihasználja a rendszer sebezhetőségét, ami egy nem kívánt eseményt eredményez a megcélzott eszközökben, jogosulatlan tevékenység jön így létre, amivel a támadó eléri a célját.

A támadások lehetséges típusai a CERT taxonómiája szerint az alábbiak lehetnek:

- Hitelesítés:** a hitelesítési mechanizmusok (pl. Kerberos) hibáit kihasználó támadások
- Titkosítás:** a kriptográfiai mechanizmusok (pl. cryptfs) hiányosságait kihasználó támadások
- Visszaélés:** nem rendeltetésszerű módon, támadásra felhasznált információk megszerzésére irányuló támadások

- d) **Szivárgás:** a rendszerben tárolt adatok jogosulatlan hozzáférhetőségére irányuló támadások
- e) **Infrastruktúra:** a kiszolgáló IT infrastruktúra (pl. hálózatok, technológiai rendszerelemek) ellen irányuló támadások
- f) **Bemenet módosítás:** az inputként felhasznált adatok módosítására irányuló támadások
- g) **Verseny:** az erőforrások tartós lekötését eredményező versenyhelyzet kialakítására irányuló támadások
- h) **Átkonfigurálás:** a hiteles konfigurációt módosító támadások
- i) **DOS:** denial of service, szolgáltatás-megtagadás előidézésére irányuló támadások
- j) **Biztonsági szabályok megkerülése:** az adatokhoz való hozzáférésre irányuló támadások a jogosultsági rendszer vagy védelmi szabályok megkerülésével
- k) **Rendszer-hozzáférés:** a rendszerekhez hozzáférhetőséget biztosító támadások
- l) **Egyéb, ismeretlen, vagy nem részletezett:** a fentiekől eltérő típusú, vagy nem besorolható támadások, illetve a részletezni nem kívánt támadások.

A sikeres támadások hatásai az ismert biztonsági osztályokba sorolhatók (több is választható egy-egy sérülékenységhöz, ezek a bizalmasság elvesztése - a támadás hatása információ nem kívánt kikerülése, a sértetlenség elvesztése - a támadás módosítja a rendszerben tárolt adatokat vagy tulajdonosaikat és a rendelkezésre állás elvesztése - a támadás során a tárolt adatok törlése, végleges elérhetetlensége megvalósul.

Tekintettel arra, hogy a hitelesség elleni támadások szerepelnek a támadások lehetséges típusai között, továbbá a sértetlenség elvesztése egyik lehetséges kárkövetkezménye ezeknek a támadásoknak, az ezek ellen ható tényezők ebből adódóan növelhetik a biztonságot, csak el kell érni, hogy használják a védelmet jelentő és megvalósító szolgáltatásokat.

Javaslat

Az NJSZT információbiztonsági szakosztály 2019. évi munkatervének legyen egyik pontja az intézményi bizalom növelésében való közreműködés a SZEÜSZ-ök, különösen a Kormányzati Hitelesítés-Szolgáltató szolgáltatásaival kapcsolatosan.

Ennek érdekében munkatervet is meg lehet fogalmazni, mely részleteit egy későbbi szakosztály-megbeszélés részletezhetné. Az alábbi tevékenységek merültek fel idáig a teljesség igénye nélkül:

- tudományos cikkek felkutatása és feldolgozása a tárgyban
- ismeretterjesztő, demonstráló előadások szervezése, ideértve az online prezentációk összegyűjtését, kidolgozását, hozzáférhetővé tételét is
- partnerek megszólítása (pl. NISZ GovCA, MELASZ, Hétpecsét, NJSZT ECDL Iroda, ISZE, NKE) és konkrét együttműködés kialakítása
- online kommunikáció megvalósítása (IT hírportálok, MTI)
- a kapcsolódó jogintézmény létezésnek és működésének kommunikálása létező példákon keresztül, és meg lehet vizsgálni, hogy van-e hiány ezen a téren jelenleg:
 - Guccifer-sztori (<https://en.wikipedia.org/wiki/Guccifer>)
 - Netlock bírság (http://nmhh.hu/dokumentum/164196/netlock_hatarozatok.zip)

Fogalmilag ez a tevékenység illeszthető a jelenlegi kormányzati szakmai kommunikációhoz², de az intézményi bizalom megteremtéséhez nyilván nem elegendő annyi, ha az állampolgárokat nem nézi

² <https://kormanyablak.hu/hu/hirek/bizalmon-alapulo-rendszert-szeretnenk-kiepiteni>

az állam *de facto* bűnözőknek, azonban természetesen segíthet. Oktatási vetülete is van ennek a kérdésnek, ahogyan azt dr. Ignác István megfogalmazta³:

„Fontos azonban megjegyezni, hogy Észtország teljes lakossága kisebb, mint Budapesté, és a hazai fejlesztések előrehaladását tovább nehezíti, hogy az internet adta lehetőségek kihasználásához szükséges készségek sem olyan elterjedtek, mint a balti államban. Ezért ahhoz, hogy Magyarország is meg tudja alapozni jövőjét az e-kormányzati fejlesztésekkel, az újabb és újabb szolgáltatások megjelenése mellett arra is szükség van, hogy már az alapfokú oktatásban is különös figyelmet fordítsunk a digitalizáció adta lehetőségek kihasználásához szükséges készségek elsajátítására.”

Tekintettel arra, hogy az éves tervünknek több pontja is lehet, érdemes munkacsoportokban gondolkodni az operatív megvalósítás során, a szakosztály felügyeleti szerepét megtartva.

Hivatkozások

- [1] Magyar Értelmező kéziszótár, harmadik, változatlan kiadás. Budapest, Akadémiai Kiadó, 1978. ISBN 963 05 1588 1. p138.
- [2] Rezümékötet 2014 - A haza szolgálatában konferencia. Lőrincz András: *A bizalom bizonytalanságáról és magyarországi állapotáról*. Budapest, Nemzeti Közszerződési Egyetem, 2014. ISBN 978-615-5491-88-7. p94
- [3] Vasvári György: A társadalmi és szervezeti (vállalati) biztonsági kultúra. Budapest, Ad Librum Kft., 2009. ISBN 978-963-9934-66-5. p11
- [4] Carl E. Landwehr: Formal Models For Computer Security. Association for Computing Machinery (ACM), USA. 1981. ISSN:0360-0300. Computing Surveys; Vol 13. No. 3. pp247-278
- [5] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana. Nemzeti Közszerződési Egyetem, Budapest. 2008. ISSN 1416-1443. Bolyai Szemle; 17. évf.(4). pp137-156
- [6] Risk Tunneling Matrix (Forrás: Jøsang, Audun, and Stéphane Lo Presti. "Analysing the relationship between risk and trust." Trust Management. Springer Berlin Heidelberg, 2004. 135-15.)
- [7] Szabó Katalin – Hámori Balázs: Információgazdagság. Digitális kapitalizmus vagy új gazdasági rendszer. 7. fejezet: *Bizalom, reputáció és identitás az elektronikus piacokon*. Budapest, Akadémiai Kiadó. 2006. ISBN 978 963 05 8402 9, ISBN 963 05 8402 6. pp188-205
- [8] R. Falcone, M. Singh, and Y.-H. Tan (Eds.): Trust in Cyber-societies, LNAI 2246. D. Harrison McKnight and Norman L. Chervany: Trust and Distrust Definitions: One Bite at a Time. 2001. Springer Berlin Heidelberg, ISBN: 978-3-540-43069-8 (Print) 978-3-540-45547-9 (Online). Lecture Notes in Computer Science, ISSN: 0302-9743 2001, VIII, pp. 27–54, fig. 1.
- [9] CERT Advisory CA-2001-04 Unauthentic "Microsoft Corporation" Certificates. http://www.lafn.org/faq/virus/fraud_certificate.html. (letöltés: 2014.12.30.)
- [10] FOX-IT BV: Black Tulip. Report of the investigation into the DigiNotar Certificate Authority breach. 2012. The Netherlands, Fox-IT BV. <http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/08/13/black-tulip-update/black-tulip-update.pdf> (letöltés: 2014.12.30.)
- [11] George Fisk: Guideline for Warranty Service after Sale. 1970. USA, American Marketing Association, ISSN 0022-2429, Journal of Marketing, January 1970, Vol.34. No.1.pp63-67
- [12] Autóblog: Több mint 240 ezer autót hív vissza a GM. 2010. augusztus 18. 21:39. http://www.autoblog.hu/hirek/tobb_mint_240_ezer_autot_hiv_vissza_a_gm/ (letöltés:2014.12.30.)
- [13] TW!CE: ADAC autós megbízhatósági statisztika 2013. 2013-08-07 <http://twice.hu/hobby/adac-autos-megbizhatosagi-statisztika-2013>. (letöltés: 2014.12.30.)

³ <https://hirlevel.egov.hu/2016/07/19/digitalis-kormanyzat-az-eszt-csoda-titka/>

[14] John D. Howard: An Analysis of Security Incidents on The Internet 1989 – 1995; A dissertation submitted to the graduate school in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Engineering and Public Policy. Pittsburgh, Pennsylvania, USA. Carnegie Mellon University, April 7, 1997.

http://resources.sei.cmu.edu/asset_files/WhitePaper/1997_019_001_52455.pdf

(letöltés: 2014.12.30.)

[15] John D. Howard and Thomas A. Longstaff: A Common Language for Computer Security Incidents. Sandia National Laboratories [Technical Sandia Report: SAND98-8667]. October 1998.

<http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=0D5C3F25DF29655195ABE38B20B8F7E3?doi=10.1.1.31.4289&rep=rep1&type=pdf>. (letöltés: 2014.12.30.)

[16] Taxonomy of the Computer Security Incident related terminology; TERENA Incident Taxonomy and Description Working Group; Work in progress. https://www.terena.org/activities/tf-csirt/iodef/docs/i-taxonomy_terms.html (letöltés: 2014.12.30.)

[17] Daniel W. Manchala: e-commerce Trust Metrics and Models. March, 2000. IEEE Internet Computing, ISSN: 1089-7801. pp.36-44.