Az

„IT és hálózati sérülékenységek tovagyűrűző társadalmi-gazdasági hatásai”

NKFIH PD-109740

kutatási projekt záró beszámolója

1 A kutatás előzményei

A Puskás Tivadar Közalapítvány – Nemzeti Hálózatbiztonsági Központ (PTA CERT-Hungary) 2010 elején kérte fel az Információs Társadalomért Alapítvány – INFOTA Kutatóintézetet (INFOTA), hogy legyen segítségére a számukra hazai és nemzetközi hálózatokból beérkező nagy mennyiségű informatikai biztonsággal kapcsolatos, szoftver-sérülékenységi adat feldolgozásában és értelmezésében. A feladat a CERT negyedéves és éves jelentéseihez szükséges háttéranyagok elkészítése volt. Az INFOTA kutatóintézetben személyes kutatási előéletem alapján engem bíztak meg ennek a projektnek a kutatási és koordinációs feladataival.

Ez volt az a pont, hogy elkezdtem elmélyedni az informatikai biztonság és szoftver sérülékenységek területében és elkezdtem vizsgálni, hogy a jellemzően az IT-biztonsági, mérnök végzettségű szakemberek nyelvén íródott szoftver sérülékenységi adatbázisok és adatok hogyan válhatnának értelmezhetővé az állami/vállalati döntéshozók számára és milyen módon lehetne ebből a lakosság számára információkat szolgáltatni. Akár nem is magukról a sérülékenységek pontos mibenlétéről és működéséről, hanem ezek hatásairól a szervezetekre, azokra a rendszerekre, struktúrákra, amelyek körül vesznek minket, kiszolgálják a mindennapi igényeinket. Milyen hatással lehetnek ezek az áttételes hatások a makro- és mikrogazdaságra, illetve a társadalmi folyamatokra, a biztonságérzetre egy olyan korban, ahol minden egyre okosabb körülöttünk, ahol a technológia folyamatosan körülvesz és az életünknek egyre több szegmensét éljük összekapcsolt rendszerek között?

Ezek a kérdések vezettek el ehhez az OTKA-pályázathoz, ahol is a támogatás elnyerése után célzottan kezdtük el vizsgálni a területet. Ám sajnálatosan nem sokkal a pályázat kezdete után a PTA-val meg kellett szakítanunk az együttműködést (az okokat ld. az eredeti kutatási tervtől való eltéréseket bemutató 6.1. alfejezetben), így a legjelentősebb adatforrástól megfosztva kellett újragondolni a projektet. A célkitűzéseken nem akartunk változtatni, viszont az adatgyűjtésre fordítandó energia az eredetileg tervezettnek többszöröse lett hirtelen, ráadásul még azt is újra ki kellett találni, honnan tudjuk megszerezni a szükséges elemi adatokat, hiszen ez a szakértelem alapvetően a CERT Hungary birtokában volt. a kutatás kezdetén.

2 Szakértők, segítők, kutatási hely és köszönetnyilvánítás

Az már a pályázat benyújtásakor világos volt, hogy szükség lesz segítségre a projekt megvalósításához. Szakértői segítségként informatikai, illetve IT-biztonsági szakemberekre volt szükség, akik segítettek az szoftver sérülékenységek működésének informatikai oldalát, a sérülékenységek és kihasználási mechanizmusaik működését megérteni. **Erdősi Péter Máté (CISA, IT-biztonsági szakember), valamint Agócs Péter és Zéman Gábor programozók, informatikai szakemberek** segítettek ezt megvalósítani a projekt során.

Szükség volt továbbá segítőkre, különösen, hogy az elemi adatgyűjtési, rendszerezési és feldolgozási feladatok megsokszorozódtak. **Szanyi István** az INFOTA Kutatóintézet munkatársa, ő ezen kívül a záró publikációkat tartalmazó kötet tördelésében, nyomdai előkészítésében is értékes segítséget nyújtott, valamint **Török Marianna PhD-hallgató és Benkő Zsanett MA**-hallgató munkája felbecsülhetetlen értékű volt, hiszen nagyon sok időt és energiát takarítottunk meg segítségükkel.

Négy nappali tagozatos BA hallgató is nagy segítségemre volt a Budapesti Metropolitan Egyetemről: **Szabadkai Balázs, Tallósi Zoltán, Ács Máté és Veszprémi Tamás** szakmai gyakorlatukat az INFOTA-nál töltötték, így kapcsolódtak be a projektbe egy rövid időre: az adatgyűjtés és tisztítás folyamatába segítettek be, mindeközben értékes tapasztalatokkal gazdagodtak a tudományos kutatómunka alapjait illetően, amelyet néhányuk azóta TDK- és szakdolgozatok formájában is hasznosított.

Köszönet Illeti **Angyal Zoltánt és Vasvári Györgyöt** is, akik a mélyinterjúk alanyaiként hasznos tudásukkal segítették a kutatás elkészültét.

Külön öröm, hogy Vasvári Györggyel, aki informatikai biztonsági szakértő, nyugdíjas CISM, címzetes egyetemi docens, arany diplomás villamosmérnök, a magyar számítástechnika kiemelkedő alakja volt, amellett, hogy a Műegyetemen tanáromként ő oktatott először informatikai biztonsági ismeretekre, e kutatás kapcsán is sikerült még kapcsolatba kerülni, hogy tudásával gyarapíthassa az eredményeket, mielőtt a kutatás 2. évében, 2015 júniusában elhunyt.

Épp ezért **a kutatás eredményeit bemutató kötetet az iránta való tiszteletből az ő emlékének dedikáltuk**, és a kutatási eredmények mellett, életrajza, illetve néhány tematikailag kapcsolódó, ám nem a kutatási projekt keretében készült, a régi pályatársaktól származó írás is belekerült.

Emellett köszönet illeti meg az Információs Társadalomért Alapítvány – INFOTA Kutatóintézet vezetőit, **Korcsmárosné dr. Bassa Liát és Dr. Kiss Ferencet, valamint minden munkatársát**, hogy a kutatás lefolytatásához támogató és professzionális környezetet biztosítottak, segítségük nélkül ezek az eredmények nem jöhettek volna létre.

3 A kutatás folyamata

3.1 Az 1. év

Az első év során a kutatóhely először megszűnése előtt a PTA-val, majd az IBM Magyarországgal együttműködve is végzett kutatást, amely a felhő alapú technológiákkal, az elektronikus üzletvitellel és a távmunka kérdéseivel foglalkozott. Ezen kutatásokban a kockázatok elemzése, az egyes témakörök biztonsági aspektusai, az egyes technológiák gazdasági hatásai és az azok alapjául szolgáló rendszerek sérülékenységi vizsgálatai is erőteljesen fókuszba kerültek. Ez remek lehetőséget jelentett a fenti projektek és az OTKA-pályázat összekapcsolására. Így a kutatásnak lett egy ilyen tematikusan átstrukturált része, ahol kifejezetten a fenti technológiai megoldások, kiemelten pedig a felhő esetében, a lakossági, az üzleti és a közigazgatási-kormányzati területek aspektusai is alapos feltérképezésre kerültek.

Mivel az üzleti és a kormányzati terület feltérképezése az eredeti kutatási terv szerint a 2. illetve 3. kutatási év feladata volt, itt előre dolgoztunk. A folyamatos fejlődés miatt természetesen ezeket az eredményeket frissítettük, bővítettük a következő években, de ezekben a témakörökben képződött egy olyan szilárd alap, amely már publikálásra is került a kutatási év során.

Ez maradéktalanul megtörtént, sőt mint a fent bemutatott változások indokolták, az alap adatforrások körét is ki kellett terjeszteni.

A PTA-CERT Hungary adatbázisa helyett a kutatásban a továbbiakban 4 forrásra építettük fel az új adatgyűjtési módszertant:

- Az US-Cert (USA Homeland Security) által üzemeltetett National Vulnerability Database – mivel a szoftver sérülékenységek nemzetközi problémát jelentenek, így ez a forrás teljesen lefedi a kutatás igényeit, ám az itt található szűretlen, nyers adatok primer feldolgozása nagyobb energiát emészt fel.
- A Secunia Advisories – a világ egyik vezető információbiztonsági szolgáltatójának sérülékenységi adatai
- Mitre.org – Common Weakness Enumeration (CWE)
- Gyártói adatok, reakciók a sérülékenységekre a gyártók saját oldalain

A megbízható szekunder adatforrások körét áttekintve, az alábbiak rendszeres, strukturált és összehasonlítható eredményeket adó gördülő kutatásokat publikálnak az egyes témákban:

- Nagy kutatóintézetek: Gartner, az IDC vagy a Forrester Research;
- Nagy tanácsadócégek: KPMG, Ernst&Young, PriceWaterhouseCoopers, Deloitte;
- A jelentős információbiztonsági szállítók: Symantec, Kaspersky Lab, F-secure, McAfee, stb;
- Nagy szoftver- és megoldásszállítók: Oracle, Microsoft, SAP, IBM, Google, Amazon, stb;
- A hálózati eszközökkel foglalkozó vállalatok pl. Cisco.
- Specializált kutatóintézetek: pl. Ponemon Institute, Sophos Labs.

A hazai információs háttér jóval szűkebb, az elszórt felsőoktatási kutatóközpontok mellett a Bellresearch, az NMHH által megrendelt kutatások biztosítanak kiemelkedő szekunder adatokat, valamint a hazai vállalatok közül a Kürt Zrt. szponzorál és publikál rendszeresen gyakorlati adatokat és eredményeket. A hazai szaksajtó médiumai közül kiemelhető az IT-business és Bitport.hu online portálok, amelyek részletes adatokat sokszor nem tartalmaznak, viszont remek kiindulópontot jelentenek, hiszen rengeteg hazai és nemzetközi vonatkozású kutatási eredmény publikálásáról adnak hírt.

2. A szekunder források anyagainak összegyűjtése

A fenti forrásokból számos kutatás, tanulmány, cikk, adatbázis és módszertan került összegyűjtésre. A projekt asszisztens és a hallgatói segítő segítségével több száz releváns forrás képezte a későbbi fázisok alapját.

A Bellresearch 2012-es Infokommunikációs Jelentése egy másik kutatási projekt kapcsán megvásárlásra került a Kutatóintézet által, még mielőtt az OTKA-kutatás megkezdődött volna 2013 szeptemberében, így a jelentés megvásárlása a tervezet ellenére nem ebből a költségvetésből történt meg.

3. Szekunder források előzetes szűrése, elemzése

A vizsgált források számos fontos információt tartalmaztak a vizsgált terület technológiai, jogi, gazdasági, politikai hátteréről, valamint a későbbiekben alkalmazható módszertanokról.

A szükséges adatok kinyerése mellett a modell építéséhez használható módszertanok feltérképezése jelentette a legfontosabb célt.

Az alábbi módszertanok kerültek megvizsgálásra, illetve beépítésre a vizsgálati módszertanokba:

- Az ISACA által kidolgozott ValIT 2.0 módszertan: Az informatikai beruházások valódi értékteremtő folyamatainak beazonosítása, azon szervezeti kulcsterületek felderítése, ahol a biztonsági befektetések nyomán valódi érték keletkezik
- Return on Security Investment (ROSI): A befektetett IT-biztonsági munka és erőforrások megtérülésének kalkulálása
- A Harvardon, Robert S. Kaplan Professzor által kidolgozott, és IT-biztonsági mérésekhez a Ponemon Institute által átalakított Tevékenységalapú Költségszámítás módszertan: Azon szervezeti és társadalmi folyamatok beazonosítása, amelyek függenek az egyes informatikai sérülékenységektől, biztonsági beruházásoktól. Ezek a folyamatok generálják azokat a költségeket, amelyekre a megfelelően kivitelezett IT-biztonsági beruházások hatással vannak. Ahol a legnagyobb költségek keletkeznek, illetve lehetőség van a legkomolyabb megtakarításokra.
- Sztochasztikus kockázatelemzések: A várható kárértékek és bekövetkezési valószínűségek kapcsolatának vizsgálatával, idősoros tapasztalati elemzésekkel segítenek beazonosítani a kulcsfontosságú kockázati forrásokat és osztályozni azokat súlyossági fokuk szerint.

4. Az adatok összevetése, az elemzés elkészítése

Az US-CERT adatbázisából leszűrt adatok és a szekunder források lehetőséget biztosítottak a lakossági szektor kritikus eszközeinek megvizsgálására, mivel az alap adatforrások újra felfedezése és a kutatás felhő technológiák irányába történő kitérője kissé átrendezte a tervezett időbeosztást, ezek az eredmények csak a második kutatási év elején kerülnek publikálásra. Már elfogadott előadás absztrakttal rendelkezem a 2014-es XI. Országos Gazdaságinformatikai Konferenciára, ahol bemutatásra kerülnek az eredmények.

5. Szakemberek, szakértők, szervezetek feltérképezése

A primer adatgyűjtés előkészítéséhez kapcsolódóan a kutatóhely kapcsolatain és a párhuzamosan futó kutatásokon keresztül számos multinacionális vállalat hazai kirendeltségéhez (IBM, HP, Microsoft, Google, SAP, Oracle, kereskedelmi bankok, iparvállalatok, kereskedelmi vállalatok) sikerült kapcsolatokat építeni, valamint számos hazai kutatóintézettel (eNET, Bellresearch), illetve elektronikus kereskedelmi vállalattal szintén megkezdődött az együttműködés.

6. Az eredmények publikálása

Az első kutatási év alapvetően az előkészítésről, az adatok, kapcsolatok, modellek összegyűjtését tűzte ki célul, néhány konkrét kutatási részcél megvalósításával együtt. A fent bemutatott változások miatt az alapadatok begyűjtése több energiát igényelt az előre tervezettnél, ám így is születtek publikálásra érdemes eredmények, a publikálás részben megtörtént, részben folyamatban van, a közlemények a jelentéshez tartozó publikációs adatbázisba rögzítésre kerültek.

3.2 A 2. év

1. Primer kutatás

Folytatódott a primer kutatás, hiszen az US-CERT folyamatosan publikálja az újabb és újabb megjelenő sérülékenységi adatokat, amelyek mintázata a technológiai fejlődéssel, a fókuszpontok eltolódásával – pl. a mobil technológiák irányába – szintén változik, így ezek folyamatos nyomon követését sem lehet elhanyagolni.

Az adatbázis összeállításában a kutatásban részt vevő hallgatók jelentős segítséget nyújtottak, hiszen a nyers adatok összegyűjtését jórészt ők végezték, míg a sérülékenységek kiértékelését én és a segítő szakértők végeztük.

2. A vállalati szekunder adatforrások feldolgozása

Ez maradéktalanul megtörtént, a vállalti szekunder adatok összegyűjtésénél jórészt az első éves jelentésben bemutatott adatszolgáltatóktól származó kutatások, tanulmányok jelentették az alapot. Természetesen más tematikájú, a vállalatok működésével, problémáival foglalkozó kutatások és eredmények vizsgálata került előtérbe.

3. Mélyinterjúk

A fókuszcsoportos beszélgetések helyett a kutatás ezen fázisában a mélyinterjúkat választottam, több szakértővel, többek között Erdősi Péterrel, Angyal Zoltánnal, Vasvári Györggyel készült beszélgetés. A legfontosabb cél itt a hazai online biztonsági szektor valós napi problémáinak megismerése és a kérdőív csiszolása volt, de természetesen az interjúk ebben a formában is értékes anyagokkal gyarapították a kutatást.

4. Kérdőíves kutatás

A kérdőíves kutatást végül a 6.1. fejezetben ismertetett okok miatt elvetettük. Úgy ítéltük meg, hogy a befektetett energia messze nem lenne arányos a nyerhető eredményekkel, illetve az elemi adatok felkutatása más irányba, sokkal mélyebbre vitte a kutatási eredményeket.

5. Az eredmények publikálása

A második kutatáséi év során folytattuk a primer kutatást, valamint a vállalati és kormányzati területet vizsgáltuk komolyabban az interjúkon és kapcsolatépítéseken keresztül. Ez egy átmeneti év volt, amelynek igazi eredményei valójában a 3. évben bontakoztak ki, ennek ellenére születtek publikációk ebben az évben is.

3.3 A 3. év

1. Primer kutatás

A primer kutatáshoz tartozó elemi sérülékenységi adatgyűjtést 2015-ben lezártuk, a harmadik év az adatok értékeléséről, illetve a belőlük levonható információk, következtetések előállításáról szólt. A kutatási adatbázist, amely majdnem 2000 rekordot tartalmaz, szintén publikáljuk, a kutatás eredményeként, a belőle levont következtetések pedig tudományos publikációk formájában kerültek közlésre.

2. A közszféra vizsgálata

A közszférára vonatkozó eredmények már az első évtől kezdve gyűltek a forráskutatásnak és az interjúknak köszönhetően. Ennek végleges formáját azonban a 3. év során állítottuk össze. A záró tanulmányokban kiemelt szerepet kapott a közszféra és az IT-biztonság kapcsolata, stratégiai és operatív szintű együttműködése, a biztonság megjelenítési lehetőségei a nemzetgazdasági mutatókban.

3. Az eredmények publikálása: a 2016-os év nagy részét a kutatás eredményeire vonatkozó záró publikációk elkészítése, valamint az azokat tartalmazó kötet szerkesztése, tervezése, tördelése, nyomdai előkészítése tette ki. Megtörtént a nyomdai kivitelezéshez szükséges vállalkozó kiválasztása és a kötet nyomdai munkáinak elvégeztetése.

A kötet összesen hét, a kutatáshoz tartozó publikációt tartalmaz, valamint Vasvári György életrajzát és három írást a pályatársaktól, megtisztelve ezt a kiemelkedő, mára sajnos eltávozott szakembert, egykori tanáromat és munkatársamat.

4 A kutatás legfontosabb eredményei

A kutatás legfontosabb eredményeit és megállapításait az évek során érintett és lefedett témakörökbe csoportosítva mutatom be a következőkben.

4.1 A kutatási adatbázis

A kutatás során az elemi adatgyűjtésből összeállt egy, mintegy 2000 rekordot tartalmazó kutatási adatbázis, amibe az elmúlt 5 év sérülékenységeit gyűjtöttük össze, jellemzően azokat, amelyek a Common Vulnerability Scoring System (CVSS) pontértékei alapján súlyos vagy kritikus státuszt kaptak. Az adatbázisba összegyűjtöttük:

- a sérülékenységek azonosítóját,
- publikálási dátumát,
- megnevezését magyarul/angolul,
- rövid definícióját, összefoglaló leírását,
- részletes leírását,
- az érintett rendszer(ek) megnevezését,
- az érintett rendszerverziók listáját,
- a támadás típusát (Bemenet módosítás/Konfiguráció/Visszaélés/Információ vagy adat szivárgás/Titkosítási probléma/Hitelesítés/Rendszer hozzáférés/Egyéb/Stb.)
- az értintett szoftver gyártóját,
- a sérülékenységre adott megoldást, ha publikáltak ilyet,
- az internetes referencia linkeket,
- a hatást (vagyis hogy Bizalmasság és/vagy Sértetlenség és/vagy Rendelkezésre állás ellen irányul-e),
- a szükséges hozzáférés típusát (Helyi/Távoli/Konzol), valamint
- a sérülékenység CVSS pontszámait (Base/Temporal/Environmental/Összesített), illetve
- a sérülékenység összesített súlyosság indexét.

Ezen adatok feldolgozása által értünk el sok eredményt az alábbiak közül.

4.2 Sérülékenységek vizsgálata a Sértetlenség/ Bizalmasság/ Rendelkezésre állás tükrében

Az eseménykezelő központok által nyilvántartott sérülékenységi vektorok számos aspektusból megmutatják a sérülékenység karakterisztikáját l. Az egyes információrendszerek teljes érintettségének meghatározásához szükséges ismernünk az egyes rendszerelemek kitettségét is. A biztonság megteremtésekor a bizalmasság, sértetlenség és rendelkezésre állás biztonsági követelményeknek kell teljesülniük az adott információs rendszerre és elemeire is. A sérülékenységek a biztonsági követelményeket különböző módon támadjak. Statisztikai vizsgálattal igazoltuk az egyes biztonsági követelmények támadása közötti dependenciák létezését. A bizalmasság és a sértetlenség támadása között nagyon erősen fennálló gyenge korreláció adódhat egyrészről az értékelő gondolkodásmódjából (ha egy rendszerhez olvasásra hozzá lehet férni, akkor sok esetben a módosítás is lehetséges), másrészről a nem teljes mértékben differenciált jogosultsági rendszerek implementációiból is, hiszen elméletben az egyes informatikai műveletek jogosultságai nagyon differenciáltan is kioszthatók, a gyakorlatban azonban a rendszeradminisztrátori és felhasználói jogosultságok mellett további differenciálás csak jelentős adminisztrációs erőforrások bevonásával oldható meg. Ennek elmaradása azt okozza, hogy ha egy entitás hozzáfér olvasásra egy adathoz, akkor annak módosítására is sok esetben képes. A sértetlenség és a rendelkezésre állás közötti gyenge lineáris függés magyarázata lehet az, hogy ha a sértetlenség megszűnik, akkor az eredeti információ rendelkezésre állása nyilvánvaló módon sérül, de ez nem áll fenn, ha az eredetiség megváltozása a forrásra korlátozódik és a tartalmat nem érinti.

További érdekes vizsgálati irány lehet nem lineáris függések keresése és kimutathatóságának megállapítása, a feltárt dependeciák magyarázatának finomítása és verifikálása mellett. A jelen cikkben feltárt függés természetének mélyebb megismerése az informatikai biztonság mérésben is szerepet játszhat, mivel a mérési módszereknek szükséges garantálniuk a megvalósítás hatékonyságának a mérhetőségét, és le is kell tudni írnia a biztonság méréshez felhasznált adatok gyűjtésének és elemzésének a módszereit is

4.3 A CVSS rendszer kritikai vizsgálata

Többek között a tapasztalatok alapján megvizsgáltuk magát az egységes Sérülékenységi Pontozási Rendszert (Common Vulnerability Scoring System - CVSS), az egyik legáltalánosabb eszközt az egyes szoftver sérülékenységek potenciális negatív hatásainak mérésére az informatikai rendszerekben. Kiterjedten használtuk a rendszert kutatásaink során, de hamarosan meg kellett tapasztalnunk a gyenge pontjait is, ahogyan elkezdtük használni a rendszer 2. verzióját a kutatás elején. Az egész kutatás során ragaszkodtunk a kettes verzió alkalmazásához, hiszen, bár időközben megjelent a 3. verzió, a korábbi sérülékenységek esetében a források nem frissültek az új rendszernek megfelelően, ellenben az új sérülékenységek esetében a folytonosság fenntartása érdekében a források egyelőre mindkét számítási metódust publikálják. Ennek ellenére részleteiben tanulmányoztuk a 3. verziót, hogy kijavította-e azokat a hibákat, amelyek megnehezítették a kutatómunkát. Néhány a legfontosabb gyengeségek közül, amelyeket beazonosítottunk a 2. verzióban:

- lehetséges 0.0 pontszám elérése, pedig minden sérülékenység, még a legspeciálisabb, legkevésbé elterjedt rendszereket érintő is hordoz kockázatot, legalább azok számára, akik mégis használják az érintett verziókat, tehát a pontszám soha nem lehetne 0.0.

- a nyílt forráskódú modulokból, könyvtárakból felépülő termékek öröklik a beépített modulok sérülékenységeit, amelyet a rendszer nem kezel pontszámok tekintetében. A sérülékenységeket automikusan vizsgálja, áttételes hatások nélkül.
- Mi történik, ha bizonyos paraméterek nem ismertek? A zárt rendszerben így nem lehet pontozni a sérülékenységeket, pedig nem minden esetben ismert minden paraméter.
- sok esetben a kategória lépcsők túl nagyok: Igen – Részben – Nem. A „Részben" kategóriánál viszont nagyon nem mindegy, hogy az „Éppenhogy", vagy a „Majdnem teljesen" esetet takarja.

A hármas verzió az alappontokat is eltérő kategóriákkal, eltérő pontozási rendszerben hasonlítja össze, példák segítségével összehasonlítottuk a két rendszer verziót, és azt is bemutattuk, miért nem lehet transzformációs függvény segítségével egyszerűen migrálni a v2 adatokat a v3 rendszerébe.

4.4 Az informatikai fertőződések vizsgálata

Az infokommunikációs technológia fejlődése eddig nem küszöbölte ki a sérülékenységek megjelenésének lehetőségét. Az új technológiák is rendelkeznek befogadóképességgel a szoftverek sérülékenységeit kihasználó rosszindulatú programkódokat tekintve (pl. trójai, backdoor, vírus). A globálisan működtetett vírusvédelmi rendszereknek természetes módon van egy reakcióideje, mely nem csökkenthető minden határon túl, mert a reakciók előállításához időre van szüksége a gyártóknak, vagyis a reakcióidő alulról korlátosnak tételezhető fel. Emiatt a védelem létrejötte nem lehet exponenciális. A védelem megjelenésének vizsgálatához adódik a lehetséges időpontok következő négy mérföldköve: nulladik napi támadás megjelenése, fenyegetettségi intervallum, védelem létrejötte, védelem elterjedése. A fertőződések elterjedésének vizsgálata alapvető fontosságú a védelmi prioritások meghatározásánál és a rendelkezésre állási paraméterek folyamatosságának biztosíthatóságában.

A sérülékenységek közzététele a javítások megjelenését követően tűnik praktikusnak, hiszen addig az információ terjedése korlátozottan mehet csupán végbe, ami csökkentheti a fenyegetettségi intervallumban bekövetkező incidensek számát. A védelem létrejötte és elterjedése szakaszok szétválasztását az indokolja, hogy számos esetben hiába dolgoznak ki a gyártók védelmi megoldásokat az egyes sérülékenységekre, az üzemeltetésért felelősök nem telepítik azt, így egy ismert sérülékenységből adódó fenyegetettség akár évekig is fennmaradhat. Ehhez hozzátartozik az is, hogy a gyártók hiába javítják a sérülékenységeket egyes szoftverekben vagy fejlesztői környezetekben, ha a programfejlesztők nem frissítik azokat tervezett módon, akkor az elavult program használhatóságának fenntartása érdekében kell működésben tartani a régebbi sérülékeny környezetet, a rendelkezésre állás biztosításának kényszeréből adódóan. A biztonság fenntartása tehát nem egy szereplőn – nem csak a felhasználón – múlik ilyen esetekben.

A felhasználók elégedettségének egyik mérőszáma a hozzáférési index, amit értelemszerűen befolyásol egy rosszindulatú programkód sikeres támadása, ahogyan ez a múltban is előfordult (DDoS támadások, zsaroló programok). Fontos kérdés a polgárok védelme egy kiberkonfliktusban, noha kevés az ilyen események számossága napjainkban, azonban a védelem megteremtésekor gondolni szükséges erre is. A helyzetet árnyalja, hogy az új technológiák elterjedésével együtt fog élni sok esetben a régi és az új, amelyek használatához bátorság szükséges.

A megfelelő információbiztonsági védelem kialakításához a támadások elterjedési paramétereit és mechanizmusait alapvető fontosságú megismerni, ideértve a támadások realizálhatóságát eredményező veszélyforrások vizsgálatát is, az optimális, azaz zárt, folytonos, teljes és kockázatarányos védelem minden időpontban való fenntarthatóságáért, amíg az ICT eszközöktől való függősége a társadalmainknak fennáll.

4.5 IT-biztonsági trendelemzés

A kutatás során végig figyelemmel kísértük az IT-biztonsággal kapcsolatos legfontosabb problémákat, megoldandó feladatokat és trendeket. A 3. év végére ezekből az adatokból összeállt az a kép, amely a jelen legfontosabb trendjeit és a jövő kulcsterületeit azonosítja be ezen a területen. Az eredményekből egy több mint 50 oldalas tanulmány született, amely sorra veszi az IT-biztonság jelenlegi kulcsterületeit. Ebben a kutatási részben először a dolgok internetével, majd a jelenleg legtöbb problémát okozó zsaroló vírusokkal foglalkozunk. Ezután megvizsgáljuk a célzott támadások természetét, a hagyományos kártékony kódok jelenlegi helyzetét, majd pedig a rendszerek feltörésének tudatos emberi tevékenységét a hekkelést, és annak hatásait vizsgáljuk. Ezek után foglalkozom a mobil eszközök biztonságával, a kritikus infrastruktúrák védelmével, a jogi és iparági szabályozási környezettel, majd pedig a legkiszolgáltatottabb korosztály, a gyerekek és tinik helyzetével, az interneten rájuk leselkedő veszélyekkel. Mindezt megfelelő adatforrásokkal, példákkal és előrejelzésekkel alátámasztva, illetve kiegészítve.

A támadások egyre kifinomultabbá válnak. Az adat- és információbiztonság egyre drágább és komplexebb intézkedéseket kíván, még a jól képzett személyzet is egyre nehezebb helyzetben van. A biztonság megteremtése, a szükséges költségek fedezése sziszifuszi küzdelemnek tűnik, ám a felhasználó, az állam és az üzleti szféra összefogása, az irányítás, az oktatás és a technológia együtt sikeres védelmet teremthet.

Mivel a technológia egyre inkább átszövi életünket, különösen az okoseszközök, a dolgok internete korában, el kell fogadni, hogy a biztonsági rések, a támadási felület akárhol lehet, olyan helyeken is, amire korábban nem is gondoltunk volna. Ez nagyon nagy kihívást jelent a biztonság-menedzsmentnek, a kockázatok teljeskörű felmérésének.

A jövő kihívása egyértelmű, 5 év múlva 21 millió eszköz fog kapcsolódni a világhálóra a Gartner szerint, de ez nem azt jelenti, hogy a felhasználóknak paranoiássá kell válniuk, mindenhol ellenséget kutatva. A biztonságba való tudatos befektetés viszont továbbra sem maradhat el. A vállalatoknak hozzá kell jutniuk a legfrissebb technológiákhoz, amelyekkel megvédelmezhetik üzleti érdekeiket. A védelmi rétegek, az előjelző- és felderítő rendszerek tudatos és szisztematikus elhelyezése és karbantartása kiemelt feladat az adatszivárgások és kibertámadások megelőzéséhez.

Ha az alkalmazottak képesek felismerni a veszélyt, a támadást, ami többnyire e-mailben érkezik, az jelentősen csökkenti a reakcióidőt és sokszorosára növeli a sikeres védekezés esélyét. Ezt a képességet természetesen csak állandó biztonság-tudatosítás és megfelelő képzések segítségével lehet elérni. Ez a képesség sosem fog kifejlődni, ha a felhasználót, a felhasználók bevonódását a szervezet nem kezeli a biztonsági rendszer integráns részeként, fontos üzleti területként. Megfelelően képzett alkalmazottak hiányában egy szervezet sokkal sebezhetőbb a kibertámadásokkal szemben.

A kiemelkedően sikeres, nagy kárt okozó támadások legtöbbször nem a támadási módszerek, az innováció miatt lesznek kiemelkedően sikeresek, hanem a felhasználói nemtörődömség, tudatlanság, óvatlanság vezet el oda. Az államnak, a vállalatoknak, de az otthoni felhasználóknak is aktívan kell cselekedniük, ha infrastruktúrájukat és adataikat meg akarják védeni.

A felhasználók egyre magasabb szintű biztonságot és adatvédelmet kívánnak, biztonságban akarják tudni gyermekeiket, és elvárják, hogy az állam és a biztonsági cégek tegyenek meg mindent, hogy az a sok millió új eszköz, ami összeköttetést teremt az életünkben, biztonságosan működhessen és kommunikálhasson.

Bár a biztonsági cégek, a vállalatok és az állam szerepe jelentős, az IT-biztonságban az egyén szerepe egyre inkább felértékelődik. A rengeteg adat és szolgáltatás, amit felhasználunk, már mind digitálisan tárolódik valahol, nem lehetünk benne biztosak, hogy hol, pontosan milyen rendszeren és egyáltalán melyik országban, minden esetre a saját, közvetlen befolyásunk alatt álló rendszereken kívül, ahol persze dönthetünk a sorsáról, amennyire a felhasználói megállapodások, ÁSZF-ek megengedik, de fizikailag sosem lesz már nálunk.

A vállalati stratégiák három pillére a menedzsment, a technológia és a képzés. Az állam és a biztonsági cégek szerepét is hangsúlyozni kell, hiszen megfelelő jogi keretek között lehet csak hatékony védelmet kialakítani, meg kell határozni azokat a szabványokat, amelyekhez a biztonságnak, a technológiának, a fejlesztésnek alkalmazkodnia kell. Fenn kell tartani az emberek biztonságérzetét, az adataik védelmét, valamint a közszolgáltatások és a kritikus infrastruktúra folyamatos működését. Az új technológiai irányokat kutató R&D projektek esetében a biztonság, mint szempont meg kell hogy jelenjen már az ötletnél, a tervezés legelső lépéseinél, csak így tud majd integráns részévé válni a végleges terméknek, szolgáltatásnak.

Egyre több sérülékenység válik ismertté, és ilyen körülmények között kell a jövőben fenntartani a hálózatokat, a hozzáférést az internethez és azokat a megoldásokat, amelyekkel az egyes eszközök képesek összekapcsolódni. A routerektől, amelyek az otthoni internet-hozzáférés kapui, az okos városokig minden szinten ki kell emelni a biztonság szerepét, amely csak a megfelelő együttműködés során érhető el.

Az itt bemutatott szempontokat tükröző proaktív, együttműködő, stratégiai-, taktikai- és egyedi akciók szintjén megtervezett, jogilag támogatott informatikai biztonság az egyetlen, amely képes az állandóan megjelenő új sérülékenységek és a napi szinten érkező új technológiai eszközök tengerében megvédelmezni a mindennapi életnek, működésnek, létezésnek egyre inkább elválaszthatatlan részét képező informatikai szolgáltatásokat és rendszereket.

4.6 Az IT-biztonság helye a makrogazdasági számításokban

Megvizsgáltuk továbbá az informatikai biztonság nemzetgazdasági, makrogazdasági stratégiai kérdéseit és gazdasági számszerűsítési lehetőségeit. Foglalkoztunk az infokommunikációs technológiák, és ezen belül az IT-biztonság nemzetgazdaságban, gazdasági növekedésben elfoglalt helyével és szerepével, hogyan hat az egyes országok, régiók fejlődésére, generál 1-2%-os GDP-növekedést a lakosság minden 10%-ának bekapcsolása a digitális kommunikációba. A terület közvetve akár a teljes GDP 8%-áért is felelhet, a feldolgozóiparban pedig hamarosan 50% fölé nő az automatizált, okos technológiákat és hálózati működést kihasználó területek súlya. Megvizsgáltunk egy hételemű modellt, amely jól reprezentálja egy nemzetgazdaság felkészültségét a digitális korszak

előretöréséből eredő kihívásokra és arra jutottunk, hogy jelenleg nincs olyan ország, amely teljes felkészültséggel rendelkezne. A modell elemei a következők:

1. Létezik-e az adott országban nemzeti kiberbiztonsági stratégia?
2. Megoldott-e e szervezett incides-kezelés?
3. Megfelelően kezeli-e a törvényhozás és a bűnüldözés a kiber-bűncselekményeket?
4. Része-e az adott ország azoknak az információ-megosztó hálózatoknak, amelyek segítenek megfelelően és gyorsan reagálni a fenyegetésekre?
5. Megfelelő-e az informatikai biztonsági kutatás-fejlesztésbe való befektetések aránya?
6. Része-e az IT-biztonsági problémák kezelése a diplomáciai, külpolitikai, illetve kereskedelempolitikai tevékenységnek?
7. Megfelelő szintű-e a kibervédelem és az incidenskezelés a honvédelmi, külső elhárítási területen?

Ezután megvizsgálok több alap és később kifejlesztett, alternatív makro mutatót (GDP, GNI, munkanélküliség, infláció, FDI, HPI, GPI), keresve bennük a fenti hatásokat, a kiberbiztonsági szempontok közvetett vagy közvetlen megjelenését. Végül pedig bemutatásra kerül egy mikro szintű modell, kutatási és statisztikai adatok felhasználásával a ROSI módszertan alapján, amelynek segítségével vállalati környezetben számszerűsíthetők a biztonsági erőfeszítések gazdasági hatásai.

4.7 A nyílt forráskódú és a hagyományos szoftvertermékek összevetése sérülékenységi szempontból

A hacktivizmus kialakulása óta számos sérülékenység jelenik meg nap mint nap az egyes szoftverek vonatkozásában és felmerül a kérdés, hogy létezik-e olyan módszer, olyan gyártó, akinek a termékei magasabb szintű biztonságot eredményeznek az azt használó szervezetek számára. Kutatásunkban több mint három év sérülékenységeit vizsgáltuk meg gyártói szempontból, arra a kérdésre keresve a választ, hogy létezik-e olyan gyártó vagy olyan fejlesztési módszer, mely jobban vagy kevésbé érintett a folyamatosan megjelenő sérülékenységek számára és hogyan érinti ez a biztonsági követelményeket.

Eredményünk azt támasztja alá, hogy a szoftverek között a biztonság tekintetében nincsen kimutatható különbség, az egyes sérülékenységek sikeres kihasználásával mind a bizalmasság, mind a sértetlenség, mind a rendelkezésre állás sikeresen támadható. Az egyes termékek közötti különbségek a vonatkozó sérülékenységek számosságában jelennek meg, mely arányos a szoftverek penetrációjával – szélesebb körben elterjedt termékhez több sérülékenység jelent meg a vizsgált időintervallumban.

4.8 Az információbiztonsági törvény definiálta besorolások és a szoftver sérülékenységek összefüggései

A 2013. évi L. törvény hatályba lépését követően az állami és önkormányzati szervezetek számára kötelező a információbiztonsággal foglalkozni, rendszeres védelmi tevékenységeket végezni a vonatkozó jogszabályokban foglalt előírások végrehajtásával. Kutatásunkban arra a kérdésre kerestük a választ, hogy az előírt biztonsági besorolásoknak a szervezetek és a rendszerek vonatkozásában és a hozzájuk tartozó védelmi intézkedéseknek milyen hatása lehetséges a szoftveres sérülékenységek által jelentett információbiztonsági kockázatok csökkentése aspektusából. Kimutattuk, hogy nem létezik olyan szoftverkombináció, melyhez a vizsgált sérülékenységi adatbázisból nem tartozik

sérülékenység, másrészről azt is megállapítottuk, hogy az egyes sérülékenység kihasználásából adódó következmények az információbiztonságot hasonló módon érintik. Más szóval ezt azt jelenti, hogy a szoftvereket használó szervezetek az információbiztonsági kockázataikat nem tudják jelentősen befolyásolni a termékek megválasztásával, és a sérülékenységek kihasználhatósága lényegében független a szervezet biztonsági besorolásától. Következésképpen a biztonsági besorolások hatása a feltáró és a javító védelmi intézkedések létezésében jelentkezik, preventív hatás – a kiváltó okok függetlensége miatt – korlátozottan érhető csupán el.

4.9 A mobilitás és a mobil munkavégzés biztonsági követelményei

Az okostelefonok folyamatosan egyre nagyobb teret nyernek a felhasználók eszköztárában. A trendekből egyértelműen következik, hogy világszerte és ennek megfelelően hazánkban is egyre erőteljesebben átalakul a társadalom, az internetezés, mint tevékenység egyre inkább átadja a helyét a folyamatos online jelenlétnek, és a munkavállalók jelen vannak, jelen lesznek a virtuális térben okos és viselhető eszközeiknek köszönhetően. A vállalatok tehát stabilan építhetnek erre a jelenségre. A trend várhatóan nem fog megtörni, bár a piac telítődésével a konkrét eszközeladási számok visszaeshetnek, az általuk generált igény a folyamatos online jelenlétre, elérhetőségre és kapcsolattartásra viszont csak fokozódni fog a következő években.

A távmunka, mint jelenség, szintén egyre elfogadottabbá válik. Bár igazi teret érdekes módon a fejlődő országokban tudott csak nyerni, Európában és az USA-ban is egyre inkább egyetértenek a munkaadók azzal, hogy a technológiai fejlődés mára megteremtette nagy tömegek távoli foglalkoztatásának lehetőségeit. A tapasztalatok pedig bebizonyították, hogy sem menedzseri, sem beosztotti szinten nem kell szignifikáns teljesítménycsökkenéstől tartani a távmunka bevezetésével, sőt jelentős költségmegtakarítás érhető el a vállalkozások számára, miközben legtöbbször a munka minősége is javul.

A dolgozók a munka és magánélet egyensúlyát jobban megszervezve, azt utazási stressztől és időveszteségtől mentesülve sokszor produktívabbak tudnak így lenni, mint a hagyományos foglalkoztatási keretek között. Természetesen nem minden munkakör, nem minden ágazat alkalmas erre, jellemzően a szellemi, individuális munkakörök ilyenek, ám a kommunikációs technológiák egyre inkább megvalósíthatóvá teszik az intenzív csapatmunkát is ezen a területen.

Az új foglalkoztatási formák új munkaszervezési elveket is magukkal hoznak, hiszen a nagy feladatokat automatizáltan apró részletekre lebontva hatalmas párhuzamos kapacitások mozgósíthatók jelentős infrastrukturális beruházások nélkül a humán erőforrás területen. Ez a crowdsourcing világa, amelyre már itthon is van sikeres példa, és amelyet ugyancsak a fenti technológiai fejlődés hozott létre.

Egyre jobban terjednek vállalati, intézményi környezetben az „okos” mobileszközök, amelyek állandó adatkapcsolatban vannak a nyilvános hálózatokkal. Segítségükkel nagyon sok feladat egyszerűbben megoldható, hatékony mobil munkakörnyezet alakítható ki, ám megjelenésük új kihívások elé állítja az informatikai biztonsági szakembereket.

A mobil IT-biztonság egy nagy fejezete tehát az egyre szaporodó okos mobileszközök (smartphone, tablet) tömeges beáramlása az intézményi hálózatokba, többnyire megfelelő protokollok és ellenőrzés nélkül.

Amíg mindenki asztali PC-ken dolgozott, nem sok értelme lett volna az angol kifejezés (bring your own device – „hozd a saját eszközöd”) alapján csak **BYOD-nak** nevezett lehetőségnek, de a mobilitás – valamint az egyre inkább megfizethető és egyre nagyobb teljesítményű számítógépek és főleg a terjedő okostelefónia – ezen a téren is változást hoztak.

Különösen a mobileszközöknél lényeges, hogy tisztázásra kerüljön: milyen adatok kerülhetnek fel a készülékre, illetve azokról milyen vállalati erőforrások érhetők el. Meg kell határozni az érzékeny adatok körét, és hogy ezek hogyan és honnan érhetők el (csak cégen belül, vagy otthoni netkapcsolatról igen, de nyilvános hotspotról nem). Szintén dönteni kell az esetleges adatvesztés esetén követendő eljárásról is, legyen az adatlopás vagy magának a készüléknek az elvesztése. Igen lényeges, hogy minden felhasználó tudja, ilyen esetekben mit kell tennie (például azonnal bejelenteni az elveszett mobilt).

Nem elég, ha tud a munkaadó az elveszett készülékről, cselekvőképesnek is kell lennie. Erre szolgálnak a mind nagyobb választékban rendelkezésre álló mobileszköz-menedzsment (mobile device management, mdm) szoftverek, sőt szolgáltatások. Segítségükkel nem csak központilag kezelhetők és ellenőrizhetők az eszközök, de például olyan fontos funkciók is megvalósíthatók, mint a távoli adattörlés, akár kikapcsolt állapotban.

Egyre szaporodnak az okostelefonokat érintő hagyományos fenyegetések is: A mobil fenyegetettségek egyik legfontosabb szeletét a rosszindulatú programok (malware) adják. A támadások nagyobb részének motivációját ma már itt is a profitszerzés jelenti.

Ezek sokféle módon veszélyeztetik a felhasználót, a készülékén tárolt személyes vagy vállalati adatokat. Feliratkozhatnak a felhasználó nevében különféle prémium szolgáltatásokra, jelentős összegekkel megterhelve a mit sem sejtő előfizető számláját, üzeneteket küldhetnek a levelezési listákra, ellophatják a telefonon tárolt adatokat, átvehetik az irányítást a készülék felett, stb.

A jelentős mértékű piaci térhódításnak egyenes következménye, hogy az okostelefonok, különösen a szabadon hozzáférhető, Android operációs rendszert futtató, egyben legnépszerűbb csoport, a kártékony programok íróinak körében is népszerűvé vált.

A beépített védelmek magas szinten történő használata, a letöltések tudatos kezelése, a források ellenőrzése, a mobil készülékekre elérhető vírusvédő szoftverek alkalmazása, speciális biztonsági szoftverek használata például jelszótárolásra, mobilkövetésre (ellopás, elvesztés esetén történő távoli törlésre), a közösségi hálózatokban való ésszerű és átgondolt részvétel, a geolokációs adatok tudatos kezelése, a vezetéknélküli kapcsolatok biztonságos használata, a rendszeres biztonsági másolat-készítés mind szükséges a kockázatok csökkentéséhez.

4.10 A felhő szolgáltatások sérülékenységeinek hatásai

A számítási felhőkkel kapcsolatban az alábbi kockázati tényezőket szokták a leggyakrabban emlegetni:

- hálózati kapcsolat: ha az adatok bármilyen okból nem elérhetők, az üzletmenet leáll;
- végpontok biztonsága: a felhő könnyen elérhető mobileszközökről is, amelyek biztonságára viszont korántsem fordítunk kellő figyelmet;
- adatbiztonság: az adatoknak nemcsak folyamatosan elérhetőknek kell lenniük, hanem garantálni kell, hogy a szükséges ideig változatlan formában fenn is maradnak
- adatvédelem: garantálni kell, hogy csak az férhet hozzá az adatokhoz, akinek erre jogosultsága van
- ellenőrzés: a felhasználói jogosultságkezelés, az eszközök beállításai, a szabályrendszerek kialakítása több odafigyelést igényel

A helyzet valóban ellentmondásos. Egyfelől igaz, hogy a felhőszolgáltatásokat kínáló vállalatok többsége komolyan veszi a biztonság minden aspektusát. Mivel pedig ebből élnek és hatalmas adatközpontokat üzemeltetnek, elemi érdekük, hogy a létező legjobb fizikai és informatikai védelmi rendszereket alkalmazzák.

Ennek megfelelően védelmi intézkedéseik és biztonsági szakembereik felkészültsége messze meghaladja azt, amit ügyfeleik többsége valaha is megengedhetne magának. Másfelől viszont azt sem lehet tagadni, hogy nem minden szolgáltató egyforma, mint ahogy azt sem, hogy előfordultak már adatvesztések, szolgáltatáskimaradások.

Ahogy a hagyományos informatikában, a felhőszolgáltatások esetében is a technológia, a folyamatok és az emberek hármasán múlik a biztonság. A kérdés csak az, hogy a felhasználó miként tud meggyőződni választott szolgáltatója biztonsági felkészültségéről. Ebben segíthetnek a már alakulóban lévő iparági ajánlások, mint például a CSA Guidance, de van néhány kérdés, amelyeket érdemes lehet feltenni a potenciális felhőszolgáltatónak. A válaszokból már elég jól fel lehet mérni, mennyire is veszi komolyan az információbiztonságot a szolgáltató.

A közszféra leginkább saját felhő alapú szolgáltató-központok létrehozásában gondolkodik. Ebben az esetben mindenképpen szem előtt kell tartani az alábbi biztonsági követelményeket.

1. Titkosítás

Nem elég az illetéktelen hozzáférés elől jelszóval védeni az állományokat, vagy csak a mozgásban lévő adatokat titkosítani, tárolás közben pedig szabadon hagyni. A mindenre kiterjedő védelem egyik talpköve, hogy az adatot mindenkor és mindenhol (a tárolás helyén, átvitel közben és lehetőleg a felhasználó eszközén is) titkosítani kell. A titkosítatlan adatok elvesztése komoly jogi szankciókkal is járhat. Ha pedig már titkosítás, nincs értelme alább adni a 256 bites AES technológiánál, de igény szerint ennél erősebb kulcsok is elérhetők.

2. Titkosító kulcsok

A titkosítás nehézsége nem is annyira az adatok kódolásában rejlik, mint inkább a titkosító kulcsok kezelésében. A kulcsokat nemcsak logikailag, hanem fizikailag is el kell választani a velük titkosított adatoktól – az a legjobb, ha egy másik adatközpontban tárolják őket, így nincs egyetlen gyenge pont.

Arra sem árt figyelni, hogy ugyanannak az alkalmazottnak ne legyen hozzáférése mind a kulcsokhoz, mind a titkosított adatokhoz.

3. Redundancia

A felhasználók elvárása, hogy minden adatuk azonnal és hiba nélkül a rendelkezésükre álljon. A szokásos szolgáltatói vállalás (99,999 százalékos rendelkezésre állás) az elérhetőségre jó lehet, de az adatmegőrzésnél ennél többre lehet szükség. A szokásos adattükrözés (két merevlemezen tárolják az adatot) nagyjából 99,99 százalékos biztonságot nyújt: várhatóan minden 10 ezer állományból elvész egy. Ha tényleg nélkülözhetetlen adatokról van szó, ragaszkodjunk ahhoz, hogy adatainkat több, egymástól távol eső adatközpontban tárolják, mindenütt legalább három példányban, és ezek között azonnali és automatikus legyen a szinkronizáció.

4. Ellenőrzés az adatok felett

Az ügyfélnek teljes kontrollt kell kapnia az adatai felett, legyen szó azok létrehozásáról, feltöltéséről, tárolásáról, megosztásáról és a végén a törléséről.

A szolgáltatónak garantálnia kell, hogy az ügyfél munkatársai képesek a távolból véglegesen törölni állományokat és mappákat a felhasználók eszközeiről, vagy megszüntetni egy-egy felhasználó hozzáférését az adatokhoz. A szolgáltatóval együtt fel kell készülni azokra az eshetőségekre is, amikor az adat illetéktelen kezekbe kerül.

5. Jelszókezelés

A gyenge, átlagos, könnyen kitalálható jelszavak minden informatikai rendszer leggyengébb pontját jelentik. Ha a felhasználóknak újabb név–jelszó párost kell megtanulniuk a felhőszolgáltatások igénybevételéhez, valószínűleg a legkisebb ellenállást választják. Akkor már jobb, ha a szolgáltatást a meglévő – és például az Active Directoryban tárolt – jelszavakkal lehet igénybe venni. Ha a felhő integrálható a már kialakított jelszó- és felhasználó-azonosítási eljárásrenddel, a kockázat csökkenthető.

6. Adat szeparáció

Úgy tudják hatékonyan kihasználni erőforrásaikat a felhőszolgáltatók, hogy egy fizikai szerveren több virtuális gépet alakítanak ki, és azzal több ügyfelet is kiszolgálnak. A virtuális szerverek, valamint a rajtuk futó alkalmazások és adatok csak logikailag vannak szétválasztva, ezért aztán rendkívül fontos, hogy a szolgáltató hogyan menedzseli a virtuális erőforrásokat. Senki nem szeretné, ha adatai egy másik szervezet dolgozói számára lennének elérhetők.

7. Naplózás

A szolgáltatónak teljes naplózást kell folytatnia minden, az ügyfelet érintő változásról, hogy a változások nyomon követhetők legyenek.

8. Skálázhatóság

A felhő egyik nagy előnye, hogy a szolgáltatási kapacitást az igényeknek megfelelően lehet alakítani. Ha az ügyfél a terhelés gyors növekedésére számít (akár új felhasználók, akár még több adat miatt), győződjön meg arról, hogy a szolgáltató később is képes lesz kielégíteni igényeit.

5 Publikációk

A kutatás eredményei folyamatosan és több fórumon publikálásra kerültek. A legkiterjedtebb publikációs tevékenység a 3. kutatási év végén történt, összefoglalva az eredményeket, és több aspektusból is bemutatva az elvégzett munka eredményeit.

A 1. kutatási évben:

- egy folyóirat cikk (angol nyelven)
- két konferencia közlemény (angol nyelven)
- két könyvfejezet (magyar nyelven)

A 2. kutatási évben:

- egy konferencia közlemény (angol nyelven)
- egy folyóirat cikk (angol nyelven)

A 3. kutatási évben:

- egy kutatási adatbázis (mintegy 2000 rekord)
- két konferencia közlemény (1-1 angol és magyar nyelven)
- Egy szerkesztett, ISBN számmal rendelkező kötet
    - abban 7 különálló könyvfejezetnek minősülő publikáció született, a kutatás záró tanulmányai (ebből egy angol nyelvű)

Mindösszesen:

- 1 adatbázis
- 2 folyóirat cikk
- 5 konferencia közlemény
- 9 könyvfejezet

született a kutatás során, amiből 6 angol nyelvű publikáció. Összesen mintegy 400 oldalnyi szakmai publikáció született a 3 év során.

6 Eltérések, nehézségek, módosítások az eredeti tervekhez képest

A kutatás első két évében az eredeti költségvetési soroktól jelentős mértékben nem tértünk el, költségvetési oldalról a terveknek megfelelően tudtunk haladni, a harmadik év során viszont a megnövekedett személy jellegű feladatok miatt kellett módosításokat végezni.

A szakmai menetében rögtön a kutatás kezdete után olyan nehézségek merültek fel, amelyek a teljes tervezett folyamatot megváltoztatták, hiszen az alapvető adatgyűjtési folyamatot kellett átalakítani, ennek sikeres áthidalása után viszont sikeres és eredményes kutatómunkát sikerült végezni, ám a rendelkezésre álló idő és erőforráskeret lecsökkent, hiszen az alapvető adatgyűjtésre sokkal több energiát kellett fordítani az eredetileg tervezettnél.

6.1 Szakmai eltérések az eredetik kutatási tervtől, ezek indoklása

A kutatási munkatervtől való kisebb eltérésnek alapvetően két oka volt:

1. A projekt előzményéül szolgált az INFOTA és a Puskás Tivadar Közalapítvány (PTA) – Nemzeti Hálózatbiztonsági Központ (Cert Hungary) közös kutatássorozata, amely a tervek szerint e projekt során végig folytatódott volna, fenntartva a két szervezet közötti folyamatos adatcserét, illetve a szakmai közösségek közötti kommunikációt. Sajnálatos, hogy a kormány 2013-ban bevezetett új Nemzeti Kiberbiztonsági Stratégiája végrehajtásával együtt járó szervezeti változások eredményeképpen 2013 végén a PTA megszűnt, a CERT-Hungary feladatai, szűkített formában (az új stratégia szerint a továbbiakban csak a kormányzati kiberbiztonsággal foglalkozik) a Belügyminisztériumhoz, azon belül a Nemzetbiztonsági Szakszolgálathoz kerültek. Ez megszakította a közvetlen kapcsolatot a két szervezet között. És bár a szakmai kapcsolat megmaradt a CERT-Hungary eredeti kollektívájával, a sérülékenységi adatok beszerzése sokkal nehézkesebbé vált, fel kellett deríteni az eredeti adatforrásokat, egy lépéssel távolabb lépni és az eredeti külföldi források alapján nekünk feldolgozni a sérülékenységi adatokat. Ez egyrészt előnyökkel is járt, hiszen így a teljes előfeldolgozás nélküli adattömegből nyerhetjük ki a minket érdeklő információkat. Ez azonban egyben hatalmas hátrány is, hiszen jóval több primer kutatási feladatot jelent, és így több időt és erőforrást emészt fel az elemi adatok beszerzése, mint azt előzetesen terveztük, így kevesebb energia marad az egyéb feladatokra.

Az adatok feldolgozása során az alapvető értékelő módszertanokat is újra ki kellett dolgozni, de a kutatás szempontjából úgy tekinthetjük, megérte: mintegy 2000 sérülékenység gyűlt össze az adatbázisban, ami a 2010-2015. időszakot fedi le.

2. Az eredetileg tervezett kérdőíves kutatás végül kimaradt a kutatási programból. Ennek az volt az oka, hogy az alapkutatás során összegyűjtött komoly sérülékenységi adatbázis feldolgozása maga is komoly munkát jelentett, de ennek megfelelően komoly eredményeket is szolgáltatott, másik részről pedig a szakértői mélyinterjúk során kiderült, hogy az eredetileg lekérdezni tervezett kérdéssor megválaszolásához valószínűleg nem elég széles körben van meg a szükséges szaktudás. Így aránytalanul nagy energia lenne a kérdőív lekérdezése és feldolgozása, kétségesen hasznosítható eredmények reményében, ezért végül elvetettük ezt a kutatási formát.

6.2 A kutatásban részt vevő szakértőkre és segítőkre vonatkozó eltérések

A kutatásban részvevők személyében változás nem történt, mind a technikai segítő, mind a hallgatók csak 2014 januárjában tudtak csatlakozni a projekthez, így néhány feladat 2014 őszére húzódott át.

Az pályázatban megjelölt két hallgató alkalmazása helyett először egy hallgatót vontunk be a projektbe [Török Marianna, a BME-VIK Informatikai Tudományok Doktori Iskola hallgatója], magasabb óraszámban, mint az előzetesen tervezett, így egyedül el tudta látni a szükséges feladatokat. 2014 szeptembere folyamán azonban sor került egy második hallgató bevonására.

A harmadik kutatási év során a pályázat költségvetésében az alábbi költségátcsoportosításokra volt szükség a személy jellegű feladatmódosítások finanszírozásához:

Jelenlegi költségvetési sor	**Új költségvetési sor**	**Összeg**
4. Befektetett eszközök és immateriális javak költsége	1.2.2 Teljes, vagy részmunkaidejű alkalmazás nem kutatói minőségben	800 000 Ft
3.1. Külföldi utazás, külföldi konferencián való részvétel dologi kiadásai	1.5. Hallgatói alkalmazás	360 000 Ft
3.2. Készletbeszerzés és egyéb dologi költségek (egyéb működési kiadások)	2. Munkaadókat terhelő járulékok	300 000 FT

A pályázat megvalósítása során a megnövekedett feladatok miatt a kutatás utolsó évében szükséges volt Szanyi István részmunkaidős alkalmazása esetében a korábbi hónapok heti 10 óra terhelésének növelése heti 20 órára.

Ezt a megnövekedett terhelést a korábban megkötött szerződése lehetővé tette, azonban a költségvetés tervezésénél a (pályázat beadásakor) csak a heti 10 órával összefüggő költségek kerültek tervezésre. Így szükségessé vált a táblázatban szereplő összeg átvezetése az 1.2.2-es költségvetési sorra. A korábban megkötött szerződést jelen levelemhez mellékletben csatolom.

A hallgatói alkalmazást (2 fő) korábban évi 8 hónapra terveztem csak, azonban a megnövekedett feladatok miatt itt is szükséges volt további hónapokban is bevonni a kutatásba a hallgatókat. A korábban tervezett 8 hónap helyett az egész év során segítették/segítik munkámat.

Ezen átcsoportosított bruttó bérköltségek a munkaadót terhelő járulékokra is hatással vannak, emiatt szükséges 300 000 Ft átcsoportosítása a 2-es fősorra.

Szanyi Istvánhoz, továbbá a hallgatókhoz kapcsolódó többletfeladatok a kutatás utolsó évében:

- A kutatási adatbázis összeállítása az eredetileg tervezetthez képest sokkal nagyobb munkának bizonyult, rengeteg primer adatforrást kellett párhuzamosan feldolgozni és a különböző formátumú adathalmazokat összefésülni a kutatás számára feldolgozhatóvá tenni. (A Nemzeti Hálózatbiztonsági Központ hazai szervezeti átalakítása után, amikor is megszűnt a közvetlen segítő kapcsolat a kutatással kapcsolatban, vissza kellett nyúlnunk az elemi nemzetközi adatforrásokhoz és abból építeni fel a kutatási adatbázist.) A primer források többek között: US-CERT, Mitre.org, NVD.nist.gov, stb.
- A fenti okok miatt sokkal több adatforrást és szaksajtó megjelenést kellett párhuzamosan megfigyelni és a releváns adatokat a kutatás számára kiválogatni.
- A kutatás dokumentációjaként a kutatási adatbázis is publikálásra kerül, ennek formázásában, publikálható, szabványos kialakításában jelentős segítséget nyújtott.

- A kutatást záró kötet összeállítása, a cikkek formázása, borítóterv és grafikai munkák elkészítése is jelentős feladatmennyiséget biztosítottak.

Továbbá a pályázatban tervezett szakértői feladatra a 3. kutatási évben a korábban engedélyezett és igénybe vett Agox Bt. helyett Zéman Gábor egyéni vállalkozót vettem igénybe. Zéman Gábor szerződés tervezetét, illetve a fenti két segítőre vonatkozó összeférhetetlenségi nyilatkozatot a korábban beküldött módosítási kérelemhez csatoltan megküldtem az NKFIH részére.

Indoklás: Jómagam közgazdász végzettségű vagyok, és a kutatás fő irányvonala is az informatikai biztonsági problémák gazdasági-társadalmi hatásait állítja középpontjába. Mindazonáltal nem lehet IT-biztonságról, szoftver sérülékenységekről és azok hatásairól megfelelő szakmaisággal beszélni, hogy a kutatást végzők ne értsék meg, hogy pontosan hogyan jelennek meg a sérülékenységek programkód szinten az egyes szoftvertermékekben, mi maga a sérülékenységek kihasználási mechanizmusa, akár helyi, akár távoli hozzáféréssel, különböző támadási vektorokkal. Milyen autentikációs megoldások állnak rendelkezésre, amelyek a sérülékenységeket kihasználó felek működését igyekeznek akadályozni Milyen áttételes hatások jelentkezhetnek egy rendszerben, ha egy támadó sikeresen bejut vagy bejuttat egy általa meghatározott kódrészletet egy rendszerbe? Hogyan történik az egyes, pl. infrastruktúra vezérlési rendszerek távoli menedzsmentje, hogyan lehet ezeken a funkciókon keresztül hozzáférni a kritikus folyamatokhoz? Ez csupa olyan kérdés, amely műszaki-informatikai szakértelmet igényel, de megértése elengedhetetlen a megfelelő összkép kialakításához és a helyes következtetések levonásához. Ennek megfelelően szükség volt ilyen háttérrel, végzettséggel és gyakorlati szakértelemmel rendelkező szakértővel való konzultációra és Zéman Gábor kiválóan bővítette az ez irányú ismereteimet, nagyban hozzájárulva a kutatás sikeréhez.

Budapest, 2016. szeptember 30.

Dr. Horváth Attila

Vezető kutató