ROSKÓ TIBOR

A központosított felhasználó azonosítás jelene és jövője

Kutatási projektünk célkitűzése a globálisan központosított felhasználó azonosítás bevezetés lehetőségének vizsgálata, támogatási modellek kidolgozása. Hipotézisünk, hogy a globálisan központosított felhasználó azonosítás eredményesen növelheti a biztonságot és hozzájárulhat az adatvédelmi előírások hatékony, gyakorlati implementálásához. Az olvasót, jelen publikációnk keretében, egy úton szeretnénk végigvezetni, melynek célállomása hipotézisünk igazolása, miközben átfogóan megismerheti a közelmúlt adatvédelmi incidenseinek hatásait, iránymutatást kaphat mind felhasználóként, mind szolgáltatóként a biztonság növelésére a személyes adatok megosztásával kapcsolatosan és nem elhanyagolandó, kutatásunk célkitűzéseit.

Kulcsszavak: *központosított azonosítás, kormányzati azonosító szolgáltató, szeparált rendszerek közötti együttműködés, adatvédelem támogatás*

Szerzői információ:

Roskó Tibor okleveles programtervező informatikus. Diplomáját a Debreceni Egyetem Informatikai Karán szerezte 2017-ben. Jelenleg a Debreceni Egyetem Informatikai Tudományok doktori iskolájának PhD-hallgatója. Kutatási területe a globális, központosított felhasználó azonosítás absztrakt modelljének kidolgozása, a bevezetés lehetőségeinek vizsgálata. Kutatása részterülete a szeparáltan működő rendszerek közötti együttműködés és az adatvédelmi rendeletek gyakorlati implementációjának támogatási lehetőségei. Részt vett a DETEP Debreceni Egyetem Tehetséggondozó Programban, melynek keretében Köztársasági ösztöndíjat is elnyert. Tagja a Neumann János Számítógép-tudományi Társaság Információbiztonsági szakosztályának; szerkesztője a Különleges Bánásmód (ISSN 2498-5368) interdiszciplináris szakmai folyóiratnak. Weboldal: www.rtibor.hu, MTMT: https://m2.mtmt.hu/gui2/?type=authors&mode=browse&sel=10062535.

Így hivatkozzon erre a cikkre:
Roskó Tibor, „A központosított felhasználó azonosítás jelene és jövője”,
Információs Társadalom XIX, 2. szám (2019): 52–85.
https://dx.doi.org/10.22503/inftars.XIX.2019.2.4

Roskó Tibor

A központosított felhasználó azonosítás jelene és jövője: biztonságos infrastruktúra vagy időzített bomba?

A kutatás célja

Tanulmányunkban bemutatásra kerülő kutatásunk célkitűzése a globálisan központosított felhasználó azonosítás infrastruktúra és az erre épülő digitális identitás profil absztrakt modelljeinek kidolgozása.[1] Célunk, az elméleti modellek kialakítása ajánlásokkal a gyakorlati implementáció kardinális kérdéseiben, például arcképmásra (International Civil Aviation Organization, 9303 part 3 és ISO 19794-5), dátum formátumra (ISO 8601), karakterkészletre (International Civil Aviation Organization, 9303 part 3) irányadó szabványok.

Kutatásunkban megfogalmazott hipotéziseink a globálisan központosított felhasználó azonosítás infrastruktúrájához:

- A ma alkalmazott, egy felhasználóhoz M darab hozzáférési adatot rendelő azonosítási környezettel szemben a globálisan központosított, egy felhasználóhoz egyetlen hozzáférési adatot kapcsoló megoldás szignifikánsan kisebb biztonsági kockázatot eredményez, National Institute of Standards and Technology Authenticator Assurance Level 3 (NIST AAL3) biztonsági szinten, ahol M > 1.
- A központosítás mértékével egyenes arányban csökken mind a felhasználói, mind a szolgáltatói oldal erőforrás ráfordítása
  - o a felhasználó hozzáférési adat menedzselése tekintetben,
  - o a szolgáltató felhasználó bázisának hozzáférési adat és infrastruktúra menedzselése, üzemeltetése tekintetben.
- A felhasználó attribútum megosztásának nyomon követése, monitorozása szignifikánsan eredményesebb, mint elosztott környezetben (a felhasználó lokálisan, manuálisan osztja meg attribútumait, melyek nyomon követésére, például jegyzetfüzetet, szöveges dokumentum fájlt használ).

Jelen publikációnkban szeretnénk ismertetni kutatásunk célkitűzéseit, átfogó, napi aktualitásból vett esettanulmányok mentén rávilágítani a felhasználó azonosítás kritikus pontjaira, például jelszókezelés, felhasználói profil megbízhatósága. Megfogalmazott hipotéziseinket szakirodalmi kutatásokból és részünkről végrehajtott felmérések statisztikai elemzésével és az eredményekből levezethető következtetésekkel szeretnénk igazolni.

Publikációnkban saját felméréseinkre és nemzetközi szabványajánlásokra alapozva egy átfogó elemzéssel szeretnénk ismertetni a ma alkalmazott lokális és lokálisan központosított felhasználó azonosítás hátrányait, nehézségeit és a hordozott veszélyeket, például jelszavak kezelése, N-faktoros autentikáció, Single Sign-On bejelentkezés

[1] A tanulmányban szereplő fogalmak egységes értelmezéséhez a NIST 800-63-3 és Erdősi és Solymos (2018) publikációk és az általunk használt kifejezések az 1. számú mellékletben kerülnek magyarázatra.

eltérítése. Hipotéziseink igazolásával szeretnénk cáfolni a globálisan központosított felhasználó azonosítással szemben megfogalmazott ama feltételezéseket, kritikákat, melyek szerint jelentős biztonsági problémákat idéz elő a központosítás, például egy jelszó kompromittálódása esetén a támadó minden szolgáltatáshoz hozzáférhet; a felhasználóról központosítva profilt alkothatnak.

Ahogyan az előző fejezetben is kiemeltük, az informatika, az online tér a mindennapok részévé váltak. Ennek okán szükséges az átlagfelhasználók közérthető informálása az elérhető megoldások használatáról és annak veszélyeiről. Publikációnkban nekik szeretnénk információt nyújtani az általunk kidolgozandó szolgáltatásról, és rávilágítani, hogy az miben könnyítheti meg a mindennapjaikat, illetve felmérésekkel, eredményekkel alátámasztva cáfolni az új technológiákkal szembeni félelmeket, bizalmatlanságot (például a Mit tehet a felhasználó? vagy Jelszó fejezetekben). Fontos kiemelni, hogy cikkünkben szakirodalmi és saját felmérések eredményeire alapozva, a szakmai közönség számára tudományosan megalapozott és validálható formában ismertetjük eredményeinket. Mindezt úgy, hogy közben az átlagfelhasználó számára közérthető nyelvezettel mutatjuk be az új megoldásokat és a mindennapjainkban fennálló veszélyeket.

Felméréseink

Felméréseink részletes eredményeit cikkünk kapcsolódó fejezeteiben részletezzük, hivatkozva az itt ismertetett felmérésre, az alcímben megadott néven. A megkeresett szolgáltatókat név szerint, adatvédelmi és egyéb szempontokra tekintettel egyik felmérésünkben sem hivatkozzuk.

SSO-100 felmérés

2019 év eleji felmérésünkben véletlenszerűen és saját felhasználásból kiválasztott 100 darab online szolgáltatást vizsgáltunk Single Sign-On (SSO) felhasználás tekintetében az alábbi szempontok szerint:

- kötelező-e lokális regisztráció
- SSO elérhető-e
- N-faktoros azonosítás
  - o elérhető-e
  - o kötelező-e
  - o típusa
- AAL3 biztonsági szintnek megfelelő-e

Objektív szempontok alapján hétköznapi felhasználásból választottunk hazai és nemzetközi kis webshopot (például Daniella.hu, mindigTV, posta.hu) és világszintű szolgáltatást (például Instagram, Viber, Netflix). Elemzésünk célja a lokálisan kötelező hozzáférési adat létrehozás, elérhető központosított autentikáció és kötelező N-faktoros azonosítás alkalmazásának eloszlás vizsgálata volt. A felmérés részletes eredményeit cikkünk kapcsolódó fejezeteiben részletezzük, hivatkozva az itt ismertetett felmérésre, SSO-100 felmérés néven.

GDPR-hiányosságok felmérés

Felmérésünkben 12 általunk használt webes szolgáltatás vizsgálatát hasonlítottuk össze, az alábbi szempontok szerint:

- kezdő és záró dátumok
- hiba típusa
  - o nincs Hypertext Transfer Protocol Secure (HTTPS)
  - o hibás adatvédelmi tájékoztató
  - o egyéb hiba
  - o nincs hiba
- válasz a megkeresésre
  - o van, de nem történt változás
  - o van, a jelzett probléma kijavítva

Napi alkalmazás használat felmérés

Feltáró jellegű vizsgálatunkhoz szubjektív alapon kiválasztottunk 20 átlagfelhasználót, és papír alapon kitöltettünk velük egy kérdőívet az alábbi szempontokat vizsgálva:

- lokális hozzáférési adatot kell-e megadni
- N-faktoros azonosítás
  - o elérhető-e
  - o kötelező-e használni
  - o használja-e
  - o típusa
- SSO
  - o elérhető-e
  - o használja-e
  - o típusa

A mérés szubjektivitása: olyan átlagfelhasználókat választottunk ki, akik kevésbé alkalmazzák az internetet mindennapi tevékenységükben. Ezzel azt szerettük volna felmérni, hogy hány jelszót kell kezelnie egy felhasználónak egy átlagos felhasználás során, legfőképpen hányat kell megtanulnia és megjegyeznie.

A téma aktualitása

A 2017-es, 2018-as év számos rendkívüli esemény bekövetkeztét tudhatja magáénak, gondoljunk csak, például, a Marriott International hotellánchoz köthető, vagy a Cambridge Analytica botrány során kiszivárgott személyes adatokra. A Neumann János Számítógéptudományi Társaság (NJSZT) kiadásában, 2018 második felében megjelent (Erdősi és Solymos 2018) publikáció a 2017-es év, míg a European Union Agency for Network and Information Security (ENISA) által kiadott kötet ENISA report 2018 a 2018-as év fő IT-incidenseit ismerteti, statisztikai adatokkal alátámasztva.

Egy informatikai rendszer ellen elkövetett támadás általánosan két érdek köré csoportosítható: rombolás vagy haszonszerzés. Rombolás során a támadó célja megbénítani, használhatatlanná tenni egy adott infrastruktúrát, például villamos energia- vagy távközlési hálózatokat, kórházakat, kormányzati infrastruktúrákat. Ezzel szemben egy haszonszerzés

reményében kivitelezett támadással a támadó célja az anyagi vagy anyagi javak elérését biztosító erőforrások megszerzése, például bankkártya adatok, hozzáférési adatok vagy szenzitív, egészségügyi adatok. A haszonszerzésből elkövetett támadás minősített esete az eltulajdonított személyazonossággal, más nevében elkövetett bűncselekmény, illetve a napjainkban elterjedt zsarolóvírusok felhasználása.

A fent említett két publikációt felhasználva az alábbiakban szeretnénk összefoglalni a leggyakoribb internetes támadási vektorok, módok taxonómiáját, az elérhető statisztikai mutatók viszonyításával. Az 1. táblázat összefoglalja ezen osztálycsoportosítást, ismerteti a 2017-es, 2018-as év trendjeit, ahol a + növekvő, a - csökkenő és az = stabil trendet szimbolizál.

támadás alanya, forrása	támadás típusa	2017-es trend	2018-as trend
Human Element Attacks (felhasználóra irányuló támadások)			
	Identity Theft (személyazonosság lopás)	+	+
	Phishing (adathalászat)	+	+
	Spam (kéretlen üzenetek)	+	=
Web Based Attacks (web alapú támadások)		+	+
Web Application Attacks (webalkalmazásra irányuló)		+	=
	Denial of Service (szolgáltatás megtagadás)	+	+
drive-by downloads (letöltés általi)	Malware	=	=
	Botnets	+	+
	Ransomware	+	-
drive-by mining (bányászat általi)	Cryptojacking		+
Active Network Attacks (aktív, hálózati támadások)			
	Denial of Service (szolgáltatás megtagadás)	+	+
Supply-chain Attacks (kiszolgáló-lánc támadások)			
software manipulation (alkalmazás manipuláció)	Malware	=	=
Human Errors, Vulnerabilities, Misconfigurations (emberi hibák, sebezhetőségek, rossz beállítások)			
	Information Leakage (információ szivárgás)	+	+
	Botnets	+	+
Data Breaches (adatszivárgás)		+	+

1. táblázat: Internetes támadási módok taxonómiája, 2017-es, 2018-as év trendjei (forrás: ENISA report 2018, Erdősi és Solymos 2018, saját szerkesztés)

A 2017-es, 2018-as év eredményein alapulva összeállítottuk a leggyakoribb, növekvő trendet mutató internetes támadási módok osztályos rendszerét. Érdemes kiemelni – ami az 1. táblázatból is kitűnik –, hogy az egyes támadástípusok sokrétű forrásból származnak, és egyszerre több alanyt is érinthetnek, például, a Ransomware-kártevő egyszerre érinthet webes alkalmazást, infrastruktúrát és egyedi felhasználót is, forrása lehet Spam üzenet, manipulált weboldaltartalom vagy támadó weboldalon elhelyezett kártékony tartalom, melyre eltérítik az eredeti webcímet. Az összetett osztályrendszerben az *Information Leakage* és a *Data Breaches* támadási módok határolhatók el markánsan. Information Leakage esetén emberi mulasztás, hibás konfiguráció vagy szoftversérülékenység eredményezi a gondatlan adatszivárgást, például jelszó nélkül hozzáférhető publikus szerver. Ezzel szemben a Data Breaches gyűjtőfogalom a célzott támadás – mely egyszerre több támadástípusból épülhet fel – eredményeként bekövetkező adatszivárgás eseményét definiálja.

Érdekes megfigyelés, hogy a 2017-es évben a Ransomware-támadás nagy volumenben zajlott, majd e trend 2018-ban lecsökkent, ugyanekkor a Cryptojacking-támadás növekvő tendenciába lépett. Ahogyan említettük, a Ransomware forrása lehet webes alkalmazás is, a Cryptojacking elsődleges forrása olyan weboldal, mely célzott kriptobányász szkriptet alkalmaz, például JavaScript, WebAssembly. Emellett elterjedt a Botnet hálózat kiépítése, melynek során, akár a felhasználó tudta nélkül is, haszonszerzésre vagy célzott támadások kivitelezésére, például, DDOS-támadás, használják fel a megfertőzött és irányítás alá vont eszközöket, például irodai pc, szerver. E hálózat alkalmas kriptobányászat céljára is, kiemelten a nagy kapacitású szerverek. Ez kiváltó oka lehet annak, hogy a támadók az egyszeri bevételt eredményező zsarolóvírus (titkosítja a meghajtón lévő nélkülözhetetlen fájlokat, a feloldókulcsért váltságdíjat kér) helyett, a felhasználó számára sokszor észrevétlen módon (a felhasználó esetenként teljesítménycsökkenést észlelhet számítógépében, viszont a támadó optimalizálhatja úgy a bányászatot, hogy az ne terhelje túlzottan a gép erőforrásait, azaz valóban szinte észrevétlen maradjon), folyamatos hasznot termelő kriptobányász alkalmazásokat használnak.

A 2. táblázat a fent ismertetett támadások elhelyezkedését mutatja be a kibervédelmi Kill Chain csoportosításban.

A Kill Chain 7 fázisra került felosztásra:

1. Reconnaissance: felderítés,
2. Weaponisation: fegyverkezés,
3. Delivery: malware, támadó eszköz célba juttatása,
4. Exploitation: sérülékenység kihasználása, hozzáférés szerzése a célba vett rendszeren,
5. Installation: hátsó ajtók telepítése,
6. Command and Control: irányítás,
7. Actions on Objectives: cél elérése.

Incidensek

Sajnálatos, hogy a közelmúltban számos nagy horderejű incidens is bekövetkez(het)ett, felhasználók százezreinek személyes adatai nyilvánosságra kerülését eredményezve, beleértve kiemelten szenzitív, orvosi információk kiszivárgását is (Freed 2018). Egy-egy adatvédelmi incidens kapcsán a felhasználó bejelentkezési adatainak nyilvánosságra kerülése lehet a legrosszabb forgatókönyv, ennek okozataként nem csak az adott szolgáltató

				Malware		
	Web Based Attacks					
Web Application Attacks			Web Application Attacks			
Phishing						
	Spam					
Denial of Service					Denial of Service	
				Ransomware		
Cryptojacking				Cryptojacking		
Information Leakage						Information Leakage
Identity Theft						Identity Theft
					Botnets	
Recon-naissance	Weaponi-sation	Delivery	Exploitation	Installation	Command and Control	Actions on objectives

2. táblázat: Támadási módok elhelyezkedése a Kill Chain osztálycsoportban (forrás: ENISA report 2018, saját szerkesztés)

rendszere, hanem legrosszabb esetben a felhasználó által használt összes szolgáltatási rendszer is hozzáférhetővé válhat, például e-mail, közösségi média, e-bank. Ezen incidensek közül szeretnénk azokat ismertetni, melyek példaként demonstrálhatják a fent összefoglalt támadási módok aktualitását.

MEGA Collection #1 – példa Data Breaches-támadásra

Az idei, 2019-es év talán legmeghatározóbb eseménye, hogy Troy Hunt biztonsági szakértő egy olyan személyes adat listát tárt a nyilvánosság elé, mely milliós nagyságrendben tartalmaz e-mail-címeket, jelszavakat és hozzáférési adatpárokat (Hunt 2019). Több mint 1.16 milliárd e-mail-cím és -jelszó páros érhető el, mely adathalmaz szennyezett, viszont ennek ellenére is rendkívül nagy mennyiségű hozzáférési adatról beszélhetünk. Az adatok szennyezettsége a támadók hanyagságából adódik, különböző határolókarakterek és fájltípusok alkalmazása okán, például szóköz, vessző, táblázatos forma. Az incidenst magát a 773 millió e-mail-címet megosztó listaként is aposztrofálják, mely arra utal, hogy közel 773 millió elektronikus cím került megosztásra. Önmagában egy e-mail-cím ismerete nem eredményez identitáslopást, viszont a szolgáltatók nevében visszaélésre alkalmas adathalász üzenetek küldhetők (NMHH 2018). Ennek során támadó weboldalra irányító internetes hivatkozást helyeznek el, az üzenet forrása általában Spam üzenet, melyet, például, Botnet hálózaton keresztül küldhetnek ki. A leginkább aggodalomra okot adó eredmény, hogy több mint 22 millió jelszó is bekerült a listába, melyek között nagy

számban találhatunk teljesen új, máshol még nem megjelentetett jelszót is. A publikált jelszavak között vegyesen jelent meg hash érték és visszafejtett, plain text érték is. Az adatok elsődleges forrása nem, vagy nem egzaktan meghatározható, tekintettel arra, hogy a támadók nem hitelesített forrásmegjelöléssel tették közzé a Mega ingyenes tárhelyet biztosító új-zélandi szolgáltató rendszerében. A szakértő cikkében kiemelte, hogy a szolgáltató már eltávolította a tartalmat, viszont az nem ismert, hogy előtte milyen letöltésszámot kapott (feltételezhető, hogy volt rá jelentkező).

26 millió SMS vált publikussá – példa Information Leakage-támadásra

Egy berlini kutató, Sébastien Kaul fedezte fel 2018-ban egy, a Voxox által menedzselt Short Message Service (SMS) üzeneteket tároló adatbázis sérülékenységét, melynek következménye volt, hogy közel valós időben, publikusan kereshetővé váltak a tárolt SMS-üzenetek, például megerősítő 2 faktoros azonosítókódok (Porter 2018). A szolgáltató, a jelzést követően, rövid időn belül leállította az adatbázist kiszolgáló szervert. Az incidens kapcsán ismét reflektorfénybe került az SMS-alapú 2 faktoros megerősítés kiváltására irányuló kampány, mely elsődlegesen az alkalmazásalapú, offline, többfaktoros megerősítés használatát javasolja, például Google Authenticator alkalmazás (Elliott 2017). Az SMS-alapú biztonsági faktor alkalmazását a NIST 800-63-3 specifikáció is kizárja, illetve rendkívül kerülendő megoldásnak jelöli, rövid távú kiváltását szorgalmazva.

Marriott International hotellánc – példa Data Breaches–támadásra

A Marriott szállodaláncot ért kibertámadás egyfajta átvezető is lehet a célzott hozzáférési adatok megszerzésére és a személyes adatok megszerzésére irányuló támadások tekintetében, betekintést nyújtva a *Data Breaches*- és *Information Leakage*-események együttállásába. A szállodalánc által üzemeltetett Starwood foglalási rendszer és nyilvántartás kompromittálása elsődlegesen személyes adatok megszerzését tette lehetővé, viszont a Starwood Preferred Guest (SPG) felhasználói fiók miatt hozzáférési adatok is nyilvánosságra kerülhettek (Leskin 2018). Eme részesemény célzott támadás a rendszer ellen, mely a *Data Breaches* támadási formába sorolandó. A szállodalánc tájékoztatása szerint 383 millió bejegyzés lehetett érintett a rendszer támadása során, melyből több, mint 5 millió titkosítatlan, és több, mint 20 millió titkosított útlevélszám, valamint közel 9 millió titkosított bankkártya száma vált elérhetővé (Del Valle 2019). A rendszerben tárolt adatok egy része titkosítással volt védve, viszont arról nincs információ, hogy a támadók megszerezték-e a titkosításhoz használt kulcsokat is, melynek következménye lehet, hogy a titkosított információk szintén hozzáférhetővé váltak. A titkosítatlan információ vagy hanyagul kezelt titkosítókulcs az *Information Leakage* támadási forma megtestesülése jelen esetben.

Phishing és Identity Theft támadások evolúciója

A Phishing támadás célja megszerezni valamilyen információt a felhasználóról, például hozzáférési adatok, bankkártya adatok, elérhetőségi adatok, lakcím, telefonszám, e-mail-cím. A támadás során álweboldalakra mutató hivatkozást küldenek az áldozat számára, melynek forrása számos csatorna lehet, például e-mail, SMS, közösségi média. A csaló weboldal külső jegyeiben megegyezik az eredeti weboldallal, például e-bank, közműszolgáltató, működésében

viszont begyűjti a felhasználó hozzáférési adatait. Identity Theft végrehajtása internetes környezetben a Phishing támadás során megszerzett hozzáférési adatokkal történhet, például e-bank, elektronikus szja-bevallás, egészségügyi rendszer.

Kolouch (2018) tanulmányából a cseh *Phishing* támadások evolúcióját ismerhetjük meg, melyben internetes banki hozzáférési adatokat és kétfaktoros azonosítókat szereztek meg támadók egy, a számítógépre és okostelefonra telepített *Malware* által. A megszerzett információk birtokában, az elkövetők *Identity Theft* támadást megvalósítva ellopták az áldozatok bankszámláján tartott pénzét. A (Gupta et al. 2017: 250) cikkben bemutatott statisztika alapján a második leggyakoribb támadás pénzügyi irányultságú. A trójai vírust e-mail-csatolmányként küldték ki, rendszerint csomag érkezés értesítőnek vagy például karácsonyi képeslapnak álcázva, zip kiterjesztésű fájlban, mely kitömörítést követően egy futtatható állományt hozott működésbe, telepítve a vírust.

Kolouch (2018) publikációjából megismerhető másik fő támadási forma a *Phishing* területén a céges levelezés hozzáférési adatainak megszerzése (BEC: Business Email Compromise). Ennek során a megszerzett céges e-mail-fiókot felhasználva csalnak ki más cégektől információkat, küldenek el partnereknek és ügyfeleknek egyaránt álbank-számlaszámokat vagy befizetendő számlákat.

A *Phishing* támadás elleni védekezésre cikkünk egy későbbi fejezetében szeretnénk segítséget adni mind a felhasználók, mind a szolgáltatók számára.

A trendek összegzése

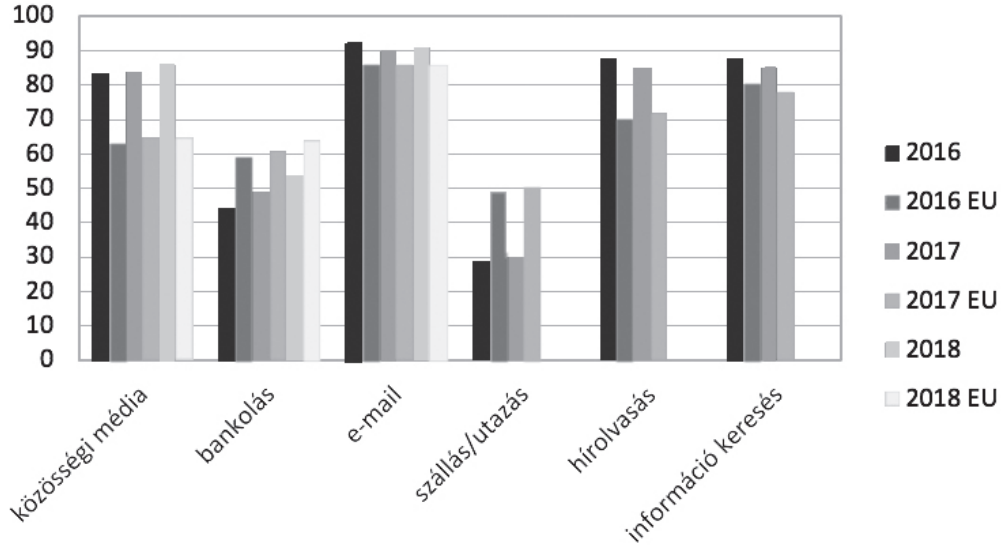
A górcső alá vett incidensek javarészt a felhasználók hozzáférési adatainak megszerzésére irányuló támadások. Az érintett rendszerek jelentős hányada közvetlenül megvalósítja az *Information Leakage*-eseményt azáltal, hogy nem alkalmaznak jelszó- vagy adattitkosítást. Troy Hunt biztonsági szakértő, a nyilvánosságra hozott e-mail-címek és jelszavak ellenőrzésére létrehozott egy weboldalt, https://haveibeenpwned.com, melyen keresztül lehetőség nyílik annak ellenőrzésére, hogy az általunk használt adat érintett-e. Nem tisztünk sem e, sem más ilyen jellegű szolgáltatás auditálása, megkérdőjelezése, de általános javaslatunk, hogy minden esetben gyanakvóan vegyünk igénybe ezeket. Feltételezhető, hogy nem csak jó szándékkal hozhatnak létre ilyen típusú ellenőrzőszolgáltatásokat okulva a különböző szolgáltatók nevében küldött számlabefizetésen alapuló csaló tevékenységekből.

A következőkben szeretnénk átfogóan ismertetni azon biztonsági lépéseket, melyek alkalmazása mind felhasználói, mind szolgáltatói oldalon megtérülő befektetés lehet az adatbiztonság terén.

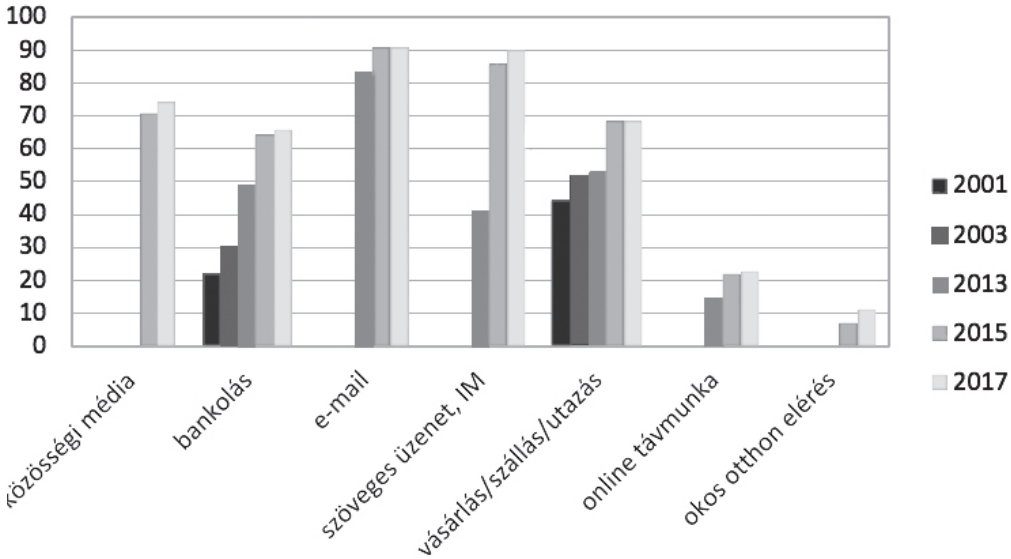
Kutatás

Napjainkban, tevékenységünk számottevő hányadát közvetlenül vagy közvetett módon online (interneten keresztül, otthonról) intézzük, például internetes bankolás, vásárlás, ügyintézés, hírolvasás. E trend évről évre növekvő tendenciáját számos felmérés, elemzés igazolja. Az egyre növekvő online jelenlét, informatikai eszközök használata a napi feladatok elvégzésében, akarva-akaratlanul is hozzájárul egy globális információs társadalom kialakulásához. Ennek köszönhetően az átlagfelhasználónak, aki kevésbé járatos az informatikai megoldásokban, mélyrehatóbb, de ugyanakkor közérthető támogatásban, oktatásban kell részesülnie. Publikációnkban, eredményeink nemzetközi alkalmazhatóságára tekintettel, hazai, európai és amerikai felméréseket együttesen

vizsgáltunk. A hazai és európai trendeket a 2016–2018 közötti időszakra, forrás és együttes összehasonlítás érdekében egységesen az 1. ábrán ábrázoltuk. Az amerikai trendet együttesen a 2. ábrán, a hivatalos statisztikai adatokra építve, a 2001–2017 időszakra vonatkozóan mutatjuk be.



1. ábra: Hazai és európai online tevékenységek trendje 2016–2018 (forrás: Eurostat https://ec.europa.eu/eurostat/data/database, saját szerkesztés)



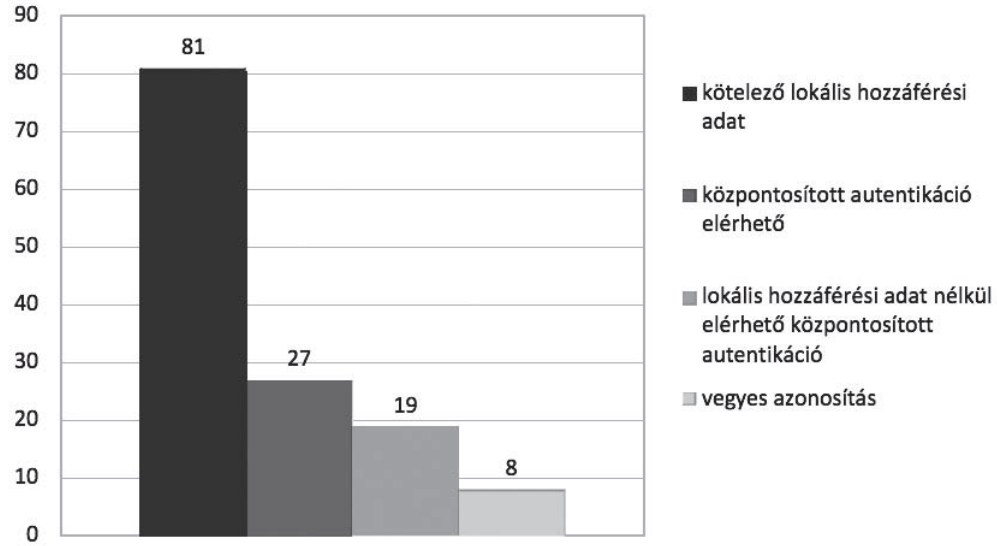
2. ábra: Amerikai online tevékenységek trendje 2001–2017 (forrás: NTIA.doc.gov, saját szerkesztés)

Mind hazai, mind nemzetközi kitekintésben szignifikáns a közösségi média és az online bankolás használatának növekedő tendenciája, melyet kiegészít az amerikai felmérés online távmunka és okos otthon eszközök interneten keresztüli elérés tevékenységek növekedő trendje.

Jól megfigyelhető, hogy a közösségi média és üzenetküldő alkalmazások (instant messaging, text messaging), például Facebook Messenger, WhatsApp, WeChat, térhódításával csökkenő tendenciát mutat az e-mail-küldés és az önálló hírolvasás vagy információkeresés.

A növekvő online tevékenységek köre és az egyre szigorodó adatvédelmi előírások megkerülhetetlenné teszik a felhasználó azonosítás, felhasználói profil menedzsment környezet erőteljes fejlesztését. Kiszolgáltatottak vagyunk a tekintetben, hogy – szinte – kivétel nélkül minden szolgáltatás igénybevételéhez rendelkeznünk kell önálló, lokális felhasználói azonosító adatokkal, például felhasználónév és jelszó. Noha rendelkezésre áll a központosított azonosítás elméleti és gyakorlati megoldása, ennek ellenére számos szolgáltatásban, új belépőként, lokális hozzáférési adatokkal kell regisztrálnunk.

Az SSO-100 felmérés részeredményét, mely alátámasztja, hogy új belépőként nagy hányadban kell lokálisan hozzáférési adatot létrehozni, a 3. ábra ismerteti (az eredmények számszerűsítetten kerültek megadásra).



3. ábra: Központosított autentikáció alkalmazásának megoszlása hétköznapi internetes szolgáltatásokban (forrás: SSO-100 felmérés)

Felmérésünk alátámasztotta, hogy a lokális hozzáférési adat létrehozás kötelezettsége szignifikáns, csupán 19 szolgáltatás esetén érhető el a tényleges központosított azonosítás lehetősége. 8 szolgáltatás kínál központosított autentikációt, de a regisztráció során kötelező lokális hozzáférési adat létrehozása.

A lokális azonosítást használó rendszerek mind felhasználói, mind szolgáltatói oldalon terhelést eredményeznek. A felhasználó egy újabb azonosító létrehozására és megtanulására, míg a szolgáltató az autentikációs folyamat teljes működtetésére kényszerül. Az azonosítók kezelése minden oldalon kockázatos, mely így a rendszer elsődleges gyenge pontja.

A biztonság megteremtésének hétköznapi lehetőségei

Sajnos, napjainkban az online szolgáltatások térhódításának okozataként az adatbiztonsággal kapcsolatosan nem is lehetne helytállóbb szlogent megfogalmazni, mint „Egy rendszer annyira biztonságos, mint annak leggyengébb eleme". A megannyi incidens konklúziója pedig, hogy eme leggyengébb láncszem maga a felhasználó. Természetesen, ahogyan nem minden fekete vagy fehér, úgy ez az állítás sem csupán annyit tesz, hogy mindenért a felhasználó a hibás egy incidens bekövetkeztekor. E fejezetben arról szeretnénk átfogó képet adni, hogy felhasználóként mire kell figyelnünk, szolgáltatóként pedig mit kell betartanunk ahhoz, hogy valódi biztonságról beszélhessünk.

Titkosított adatcsere, a védelem első bástyája

Az európai adatvédelmi rendelet, a General Data Protection Regulation 2016/679 EU rendelet (továbbiakban: GDPR) kapcsán kiemelt figyelem övezi, hogy a személyes adatokat is továbbító weboldalak biztonságos, HTTPS csatornán keresztül kommunikáljanak, GDPR 5. cikk 1/f. pont és 32. cikk. GDPR-hiányosságok felmérésünkben a nem HTTPS-kapcsolatot alkalmazó szolgáltatókkal minden esetben felvettük a kapcsolatot és rendszerint pozitív eredménnyel, szinte minden szolgáltató közreműködött abban, hogy megkeresésünkre válaszoljon, viszont, ahogyan a 4. diagramról is leolvasható, a jelzett hiba megszüntetése kevésbé volt ennyire sikeresnek mondható. A jelentett 7 hibás vagy hiányzó HTTPS-alkalmazásból mindössze 3 esetben történt hibajavítás. A biztonságos kommunikáció létesítését Secure Socket Layer (SSL) tanúsítvány beszerzésével és telepítésével valósíthatja meg a szolgáltató. Az amerikai szabványügyi testület, NIST ajánlása szerint a kiszolgáló rendszernek Transport Layer Security (TLS) 1.2 vagy TLS 1.3 protokollt kell alkalmaznia, Rivest–Shamir–Adleman (RSA) kulcscserélő algoritmus helyett Elliptic-curve Diffie–Hellman-alapú (ECDHE) algoritmussal (McKay és Cooper 2018). *Szolgáltatói oldalról* a biztonságos csatorna alkalmazása megóvhatja a felhasználókat, például, a nyilvános WIFI-hálózaton végrehajtandó adatlopással szemben.

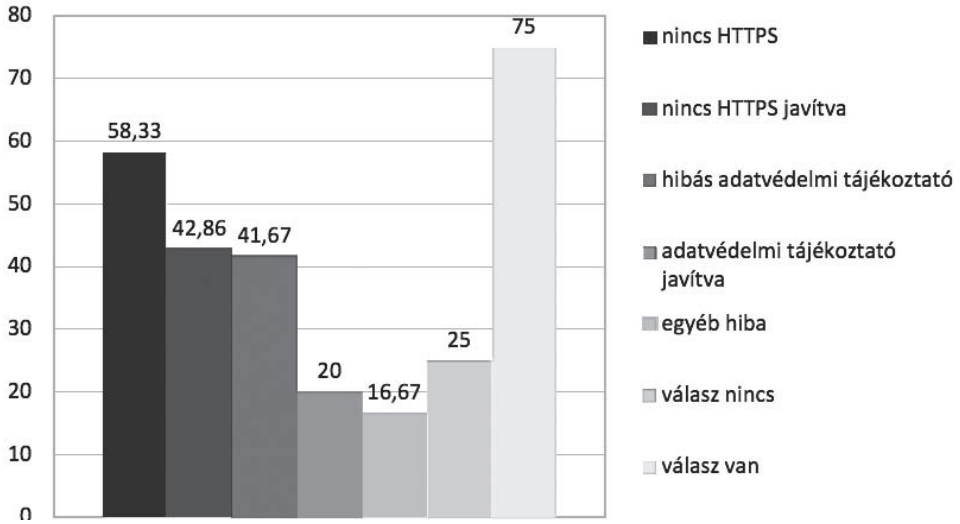
Mit tehet a felhasználó?

Felhasználói oldalról, a biztonságtudatos online interakció lehet meghatározó védekezési lehetőség az adatlopások, csalások kivédésére.

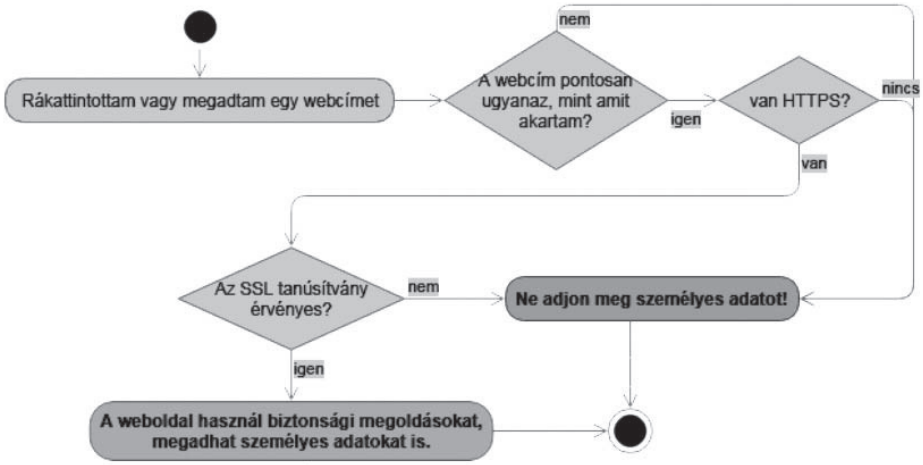
Ahogyan az előző pontban ismertettük, az első védvonal a HTTPS alkalmazása lehet, ebben aktívan részt vehet a felhasználó azáltal, hogy személyes adatait csak olyan weboldalon adja meg, mely használ HTTPS-t. Ritkán, de előfordul olyan eset, amikor a szolgáltató weboldala rendelkezik SSL-tanúsítvánnyal, de beállítási problémák miatt az oldal automatikusan nem HTTPS-alapon töltődik be, ekkor a felhasználó manuálisan adhatja meg a weboldal címében a HTTPS:// előtagot, hogy az oldal biztonságos kapcsolaton keresztül töltődjön be. A *szolgáltató* ilyen esetekben megfelelő konfiguráció alkalmazásával elérheti a HTTPS-oldalbetöltést, például, htaccess fájlban megadott utasítással.[2]

Felhasználóként az 5. ábrán ismertetett egyszerű ellenőrző műveletsort végrehajtva megvizsgálhatjuk, valóban azt a szolgáltatást készülünk-e igénybe venni, amit eredetileg is terveztünk, ezzel elkerülhető, például, az adathalász vagy megkárosító szolgáltatás.

[2] https://www.inmotionhosting.com/support/website/ssl/how-to-force-https-using-the-htaccess-file



4. ábra: Információbiztonsági hiányosságokra irányuló szolgáltatói megkeresések és az ezekre tett szolgáltatói visszajelzések (forrás: GDPR-hiányosságok felmérés)



5. ábra: Weboldal biztonsági ellenőrzése

Egy SSL-tanúsítvány érvényes lehet, ha

- érvényességi ideje nem járt le,
- nem lett visszavonva,
- a címsorban megjelenő webcímhez állították ki,
- megbízható CA (Certificate Authority) szolgáltató állította ki, a CheckTLS 2019 listán[3] elérhetők ezen szolgáltatók adatai.

[3] https://www.checktls.com/showcas.html

A hétköznapi védelem határai

Tanulmányunk a téma aktualitását ismertető fejezetében bemutattuk a leggyakoribb internetes támadási módokat. A fent bemutatott hétköznapi védekezési lehetőségek a *Phishing*-alapú támadásokkal szemben nyújtanak eredményes védelmet. A felhasználó körültekintő magatartása hozzájárulhat az eltérített, például, e-mailben megadott, az eredeti szolgáltatás helyett csaló weboldalra mutató hivatkozás, webcím kiszűréséhez a csaló szolgáltatás adathalászatának kivédéséhez.

Yue (2013) publikációjában részletesen megismerhetjük a Single Sign-On felhasználó azonosítás támadási módszereit, kiemelten a *Phishing* vagy eltérítéses támadások. A Single Sign-On megoldás lehetővé teszi a felhasználó számára, hogy egy adott szolgáltatást lokális hozzáférési adatok regisztrálása nélkül vehessen igénybe, valamely központosított azonosítás szolgáltató révén, például Google Sign-On, Facebook Login, Ügyfélkapu, login.gov.

A publikációban ismertetett támadás során az eredeti Google, Facebook Single Sign-On popup bejelentkezési ablakot másolták le külső jegyeire, majd a saját, támadó weboldalukon építették be, popup megoldás helyett az alapoldal tartalmaként jelenítették meg minden tartalom felett. Ennek célja, hogy a biztonsági elemeket, például webcím, extended validation (EV SSL) tanúsítvány icon, egyszerű képként felhasználva keltsenek hamis biztonságot. A publikáció szerzői, az ismertetett módszerrel, elkészítették saját álweboldalukat, majd önkéntesekkel felmérést végeztek annak megállapítása érdekében, mennyire lehet hatékony a támadás. A felmérés eredményeként a résztvevők 71%-a valódinak azonosította a támadó SSO-megoldást.

Az általunk ismertetett, az átlagfelhasználó által is egyszerűen kivitelezhető ellenőrző lépések mellett számos, szintén közérthetően megfogalmazott módszerrel védekezhetünk az ismert megtévesztő módszerekkel szemben. Tanulmányunk keretein túlmutatna eme módszerek részletes, mindenre kiterjedő bemutatása, de szeretnénk az olvasó figyelmébe ajánlani Erdősi és Solymos (2018) publikációját, melyet jelen cikkünk elkészítéséhez is felhasználtunk. A kiadvány részletesen, közérthető formában ismerteti a leggyakoribb támadási módszereket és védekezési lehetőségeket ellenük.

Felhasználó azonosítás szintjei

Az információbiztonságot megalapozó ismertetést követően a felhasználó azonosítás szintjeit szeretnénk ismertetni. A felhasználó azonosítás történhet lokálisan, lokálisan központosítva, a kettő keverékével vagy globálisan központosítva, függően attól, hogy a hozzáférési adatok hol kerülnek menedzselésre. Az alábbiakban e három szintet szeretnénk részletesen tárgyalni.

LOKÁLIS azonosítás

A felhasználó lokálisan, a szolgáltató rendszerében hoz létre hozzáférési adatokat, például felhasználónév és jelszó regisztrálása. Általában minden szolgáltatás igénybevételéhez új regisztráció szükséges, különböző hozzáférési adatokkal.

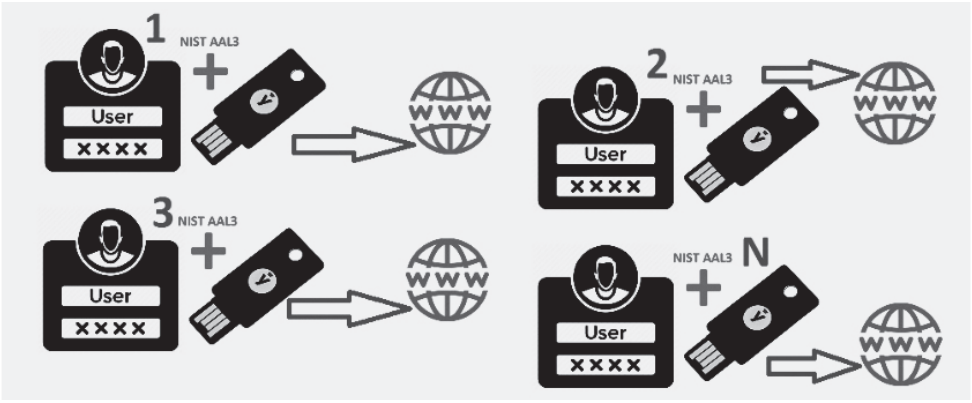
Előnye:

1. egy hozzáférési adat kizárólag egy szolgáltatás hozzáférésére jogosít.

Hátránya:

1. a felhasználónak annyi hozzáférési adatot kell menedzselnie, megtanulnia, amennyi szolgáltatást igénybe vesz; M=N.

Statisztikai elemzések alapján az elérhető internetes szolgáltatások legalább 90%-a igényel lokális hozzáférési adat létrehozást, például felhasználónév-jelszó páros (Ghasemisharif et al. 2018: 1479). Ilyen szolgáltatás lehet webshop, e-bank, közösségi média, oktatási rendszer. A felhasználó hozzáférési adat kezelését a 6. ábra szemlélteti.



6. ábra: Minden szolgáltatáshoz van külön egy hozzáférési adat, M=N

LOKÁLISAN KÖZPONTOSÍTOTT azonosítás

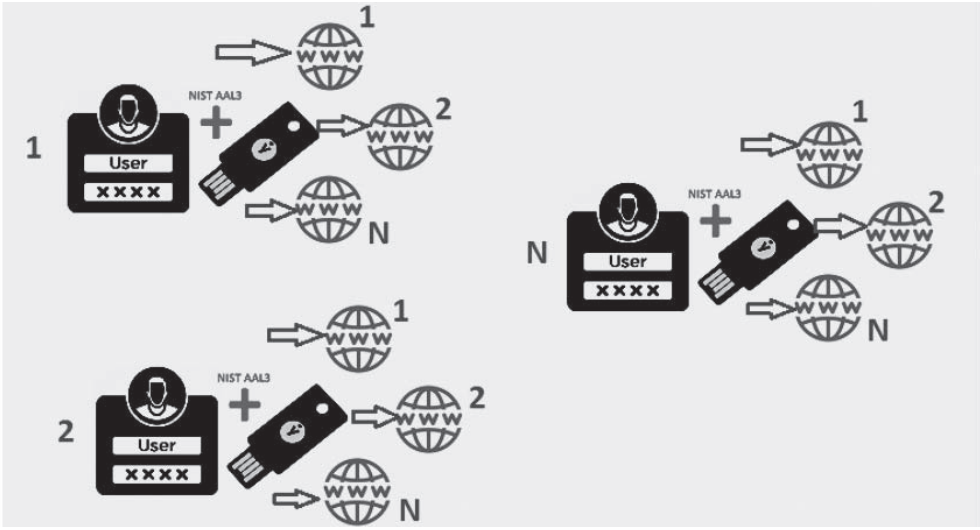
A felhasználó egy meghatározott, limitált térben használható hozzáférési adatot hoz létre (kap központilag kiosztva), például eduID, Ügyfélkapu, magyarorszag.hu, Google Sign-In. A szolgáltatónál nem kerül kezelésre hozzáférési adat.
Előnye:
1. a felhasználó, az egyes hozzáférési adatok által hozzáférhető szolgáltatások függvényében, kevesebb hozzáférési adatot is menedzselhet, mint az igénybe vett szolgáltatások száma; M<=N.

Hátránya:
1. adott hozzáférési adat több szolgáltatás hozzáférésére jogosít;
2. a hozzáférési adat korlátozott szolgáltatási halmazhoz biztosít hozzáférést, ennek okán a felhasználónak M>1 számú hozzáférési adatot kell menedzselnie, megtanulnia.

Statisztikai elemzések alapján az elérhető internetes szolgáltatások csekély mértékben, körülbelül 10%-ban támogatják a központosított hozzáférési adatok használatát (Ghasemisharif et al. 2018: 1479). Ilyen szolgáltatás lehet webshop, e-bank, közösségi média, oktatási rendszer, ha támogatja az SSO-használatát. Azonosítás szolgáltató lehet bármely olyan szolgáltatás, mely vagy csak SSO-megoldásként, vagy SSO-megoldásként is működik, például Google Sign-In, Facebook, login.gov, Ügyfélkapu, magyarorszag.hu, WeChat. A felhasználó hozzáférési adat kezelését a 7. ábra szemlélteti.

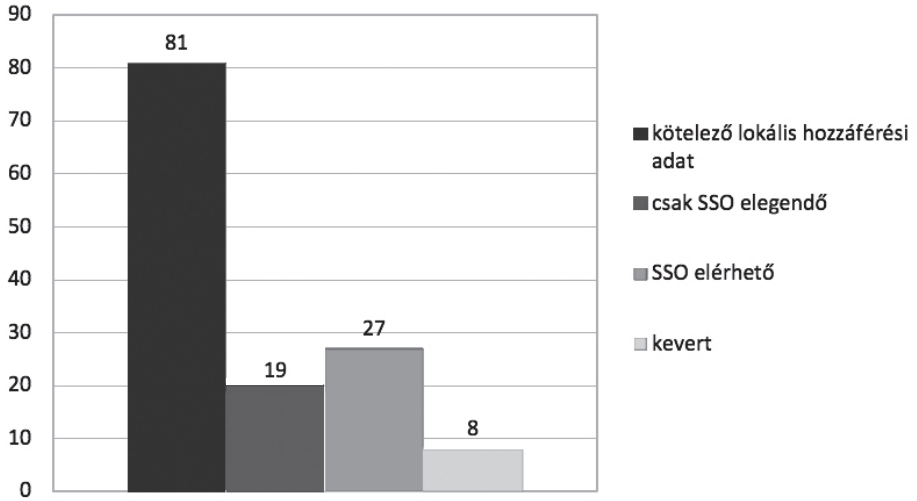
Kevert azonosítás, statisztikai mutatók

A lokálisan központosított felhasználó azonosítást biztosító szolgáltatások kötelezővé tehetik lokális hozzáférési adatok létrehozását is, ezzel megteremtve a kevert azonosítást. Ez esetben a felhasználó lokális és központosított hozzáférési adatokkal egyaránt hozzáférhet a szolgáltatáshoz.



7. ábra: SSO hozzáférési adatokkal egynél több szolgáltatás is elérhető, M<=N

SSO-100 felmérésünkben – objektív szempontok szerint – kiválasztottunk 100 internetes szolgáltatást (webshopok, e-bankok, közösségi média, közműszolgáltatások). Az elemzésben feljegyeztük, mely szolgáltatás igénybevételéhez kötelező a lokális hozzáférési adat létrehozása, mely vehető igénybe kizárólag SSO-val és mely e kettő keverékével. A 8. ábra elemzésünk eredményét ismerteti, százalékos megoszlásban. Az általunk megállapított arányokat alátámasztja a Ghasemisharif et al. (2018: 1479) publikációjában ismertetett eloszlás is. Szignifikáns, hogy a lokális hozzáférési adatok létrehozása dominál, a kötelezően létrejövő kevert azonosítás a teljes halmaz csekély részét teszi ki, mindössze 8%-ot, a csak SSO-hozzáférést tekintve is csupán közel 30% az előfordulás.



8. ábra: Lokális és központosított (SSO) alkalmazásának százalékos megoszlása (forrás: SSO-100 felmérés)

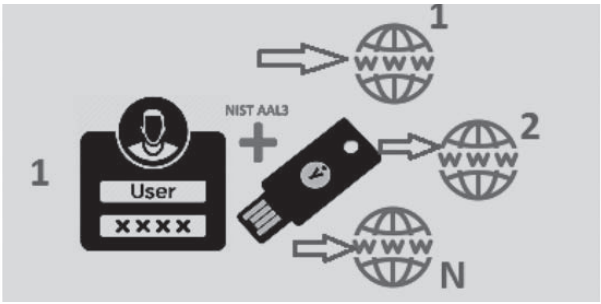
A kevert azonosítás alkalmazásának előnyei és hátrányai élesen nem különíthetők el annak okán, hogy egy adott előny egy másik nézőpontból hátrány is, például, a kötelező lokális hozzáférési adat létrehozása SSO-hozzáférés mellett előnyös, ha az SSO-fiók kompromittálódott, a felhasználó a lokális hozzáférési adatokkal továbbra is hozzáférhet a szolgáltatáshoz, ebből következi, hogy M=N.

GLOBÁLISAN KÖZPONTOSÍTOTT azonosítás

A felhasználó kizárólag egy hozzáférési adattal rendelkezik, melyet önállóan létrehozva vagy központi kiosztás útján kap dedikált azonosítás szolgáltatótól. A dedikált azonosítás szolgáltató lehet egyetlen szolgáltató vagy szolgáltatók halmaza, ha feltételezzük, hogy egynél több szolgáltató esetén a szolgáltatók diszjunktak egy adott felhasználóra. Erre egy lehetséges megoldást saját kutatásunk célkitűzéseinél ismertetünk jelen publikációban. A szolgáltatónál nem kerül kezelésre hozzáférési adat.
Előnye:
1. a felhasználónak kizárólag egyetlen hozzáférési adatot kell menedzselnie, megtanulnia; M=1, függetlenül N-től.

Hátránya:
1. egy hozzáférési adat minden igénybe vett szolgáltatáshoz hozzáférésre jogosít.

Ezen azonosítási módozatra jelenleg nincs gyakorlati megvalósítás. A felhasználó hozzáférési adat kezelését a 9. ábra szemlélteti.



9. ábra: Globálisan központosított azonosítással M=1 hozzáférési adattal minden szolgáltatás hozzáférhető

Nyitott ablak a központosított felhasználó azonosításban

A felhasználók azonosítása terén nem új keletű, hogy szervezeten belül egyfajta központosított azonosítás szolgáltatás keretében történjen az autentikáció. A felhasználó azonosítása rendszerint egy dedikált központi azonosítás szolgáltatón keresztül megy végbe. A szolgáltatás igénybevételéhez nem az adott szolgáltatás rendszerében, hanem a központi azonosítás szolgáltató rendszerében azonosítja magát a felhasználó, ezáltal a szolgáltatás nem ismeri meg a hozzáférési adatokat, például felhasználónév és jelszó.

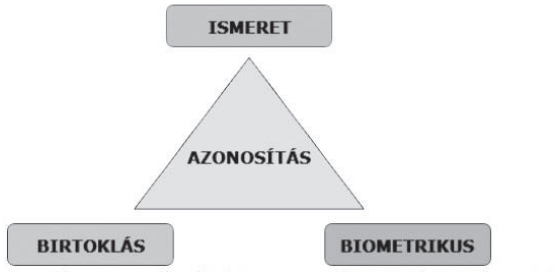
Az infrastruktúra gyenge pontja, ha a szolgáltatás közvetlenül kéri be a felhasználó hozzáférési adatát, ez esetben, a szolgáltatás közvetlenül megismeri, például a felhasználónevet és jelszót. Az ilyen jellegű felhasználás felelőtlenül kockáztatja mind a felhasználó, mind a

szervezeti infrastruktúra biztonságát. Egy nem megfelelően auditált alkalmazás nyitva hagyhat visszaélésre alkalmas ablakokat.

Az előző fejezetben ismertetett hátrány a központosított azonosításhoz kapcsolódva, hogy egy hozzáférési adattal több szolgáltatás is hozzáférhető, ennek okán, ha a hozzáférési adat kompromittálódik, minden ezzel hozzáférhető szolgáltatás is kompromittálódik. E probléma fokozódik, amennyiben a hozzáférési adatot nem az azonosítás szolgáltató kéri be, hanem, például az adott alkalmazás közvetlenül. Tanulmányunk elején ismertetett internetes támadási módszerek közül a *Phishing* az SSO bejelentkezési pontjának manipulációjával, a felhasználó hozzáférési adatainak megszerzésére irányul. A visszaélés sikerességét nagyban támogathatja az azonosítás szolgáltatáson kívül bekért hozzáférési adat cselekmény. A felhasználó megtévesztésének eredményességét Yue (2013) publikációjában 71% által valódinak elfogadott SSO bejelentkezési pont szignifikánsan igazolja.

Autentikációs háromszög

E fejezetben a felhasználó azonosításához alkalmazható faktorok osztályait szeretnénk ismertetni a NIST 800-63-3 publikációjára alapozva. Célunk egyértelműen definiálni az egyes azonosítási megoldások típusait a következő fejezetek értelmezéséhez. A 10. ábra szemlélteti a három osztályt, melybe besorolhatók az egyes azonosítási megoldások.



10. ábra: autentikációs háromszög (forrás: saját szerkesztés)

A 10. ábra és a NIST 800-63-3 kiadvány által definiáltan az azonosítás három osztálya:
1. *ISMERET*alapú:
valami, amit *ismer* a felhasználó.
2. *BIRTOKLÁS*alapú:
valami, amit *birtokol* a felhasználó.
3. *BIOMETRIA*alapú:
valami, *ami maga* a felhasználó.

*Az ismeret*alapú hozzáférési adat olyan karaktersorozat (ISO/IEC 10646), melyet a felhasználó memóriában tárol, azaz megtanul és alkalmaz személyazonossága igazolására, például jelszó.

*A birtoklás*alapú hozzáférési adat olyan eszköz, melyet a felhasználó birtokol és alkalmaz személyazonossága igazolására, például chipkártya, token.

*A biometria*alapú hozzáférési adat olyan egyedi (elméletileg, gyakorlatban statisztikai valószínűséggel közel egyedi) jellemző, melyet a felhasználó fizikailag megtestesít és

alkalmaz személyazonossága igazolására, például ujjlenyomat, írisz, hang, humán DNS. A biometriaalapú megoldások határait másik publikációnkban (Roskó és Adamkó 2018) elemezzük részletesebben.

A fent ismertetett három osztály felhasználásával alakítható ki egy-vagy többfaktoros autentikáció. E kritériumok és fogalmak meghatározásához szintén a NIST 800-63-3 kiadványát használtuk fel.

Single-Factor autentikáció (egyfaktoros): olyan azonosítási rendszer, mely kizárólag egy autentikációs faktor alkalmazását követeli meg a sikeres azonosításhoz. E faktorok a fent ismertetett faktorok közül szabadon kiválaszthatók. Például jelszó, token.

Multi-Factor autentikáció (többfaktoros): olyan azonosítási rendszer, mely megköveteli több mint egy különböző autentikációs faktor alkalmazását. E faktorok a fent ismertetett faktorok közül szabadon kiválaszthatók. Például ismeret- és birtoklásalapú megoldás együttes alkalmazása. Szorosan kapcsolódik a *többfaktoros autentikátor* fogalma, mely egy megoldásban követeli meg több mint egy különböző autentikációs faktor alkalmazását, például, kriptografikus eszköz integrált ujjlenyomat-olvasóval, mely az eszköz aktiválásához, használatához szükséges. Önmagában a többfaktoros autentikáció megvalósítható több egyfaktoros megoldás együttes használatával is.

Egyéb típusú információ, például, tartózkodási hely, IP-cím, készülék identifikációs adat felhasználható további kockázatcsökkentésre a szolgáltató által, de nem tartozik a fent ismertetett kategóriák egyikébe, így autentikációs faktorba sem. Az ismertetett autentikációs faktorok részletekbe menő felsorolása, ismertetése túlmutat tanulmányunk keretein, ennek okán az olvasó figyelmébe szeretnénk ajánlani a NIST 800-63B kiadványának 5. Authenticator and Verifier Requirements fejezetét, mely részletesen tárgyalja az egyes megoldásokat.

Jelszó

A jelszó (Memorized Secret autentikációs faktor) olyan karaktersorozat (ISO/IEC 10646), melyet a felhasználó memóriában tárol, azaz megtanul és alkalmaz személyazonossága igazolására, ismeretalapú hozzáférési adat. A jelszavak létrehozására, tárolására, felhasználási módozataira számos szabvány és de facto ajánlás létezik, ezek áttekintését szeretnénk e fejezetben ismertetni.

Jelszó létrehozása

A felhasználó által megválasztott, létrehozott jelszavak komplexitását a Shannon-féle entrópia alapján szokták megadni. A determinisztikus eloszlású adatokon értelmezett entrópiával szemben a felhasználó által létrehozott karaktersorozat entrópiája nehezen és kevésbé pontosan határozható meg. Ennek okán írnak elő szabályokat a jelszavakra, például hossz, speciális karakter, kis- és nagybetű tartalmazása (NIST 800-63B).

Gyenge jelszót választani olyan, mintha becsuknánk az ajtót, de nem zárnánk kulcsra. Egy jelszó gyengének számít, ha könnyen ki lehet találni, ilyen lehet, például, egy általános (password, p@ssw0rd), vagy személyhez köthető kifejezés (háziállat neve, születésnap) (Huth et al. 2012).

A NIST 800-63B kiadványában több fejezetben is ismerteti a biztonságos jelszó létrehozásának feltételeit, felhasználói interakcióban. Az 5.1.1. Memorized Secrets fejezet

elsősorban az azonosítás szolgáltató rendszerével szemben fogalmaz meg követelményeket, melyek viszont felhasználói oldalon is megfogadhatók, például, legalább 8 karakter hosszú, ismétlődő karakterektől mentes, kontextusspecifikus és triviális elemek elkerülése, elérhető karakterek használata, beleértve a szóközt is. Rossz példa: név, születési dátum, jelszó, 123456. Jó példa: elsősorban egy hozzánk nem kötődő, de könnyen megjegyezhető jelmondat. A jelmondatok alkalmazását ajánlja a (Huth et al. 2012) publikáció is a könnyű megjegyezhetőség és a kitaláció megnehezítése okán. Erre példa lehet *A komplex jelszavak nehezen kitalálhatók* mondat átalakításából keletkező, *AKomplexJelszavakNehezenKitalálhatók 2019#* képzett karaktersorozat. A kiválasztott jelszó hossza egyenes arányban növelheti a jelszó kitalálás idejét, például a Garcia (2017) publikációjában bemutatott kifigurázó ábrán.

Tárolása felhasználóként

Minden jelszó fontos (Huth et al. 2012)! Ennek szem előtt tartásával ne osszuk meg jelszavunkat senkivel, azt ne írjuk le papírcetlire vagy nem biztonságos tárolóba, például titkosítatlan szöveges dokumentumba. Felhasználóként először jegyezzük meg jelszavunkat vagy az ebben előforduló korlátozás miatt – például túl sok, már meg nem jegyezhető jelszavunk van – alkalmazhatunk jelszótároló, biztonságos alkalmazásokat is (Huth et al. 2012). A publikációból megismerhetjük, hogy felhasználóként körültekintően válasszuk ki jelszókezelő alkalmazásunkat:

- használjon titkosítást a jelszavak tárolásához;
- lehetőség szerint a hozzáféréshez két-faktoros azonosítást alkalmazzon;
- biztosítson lehetőséget automatikusan generált jelszavak előállítására, lehetőség szerint a NIST irányelveknek megfelelve (NIST 800-63B Appendix A).

Tárolása szolgáltatóként

A NIST 800-63B kiadvány 5.1.1. Memorized Secrets című fejezetében részletes útmutatást ad az azonosítás szolgáltatók számára, hogyan tárolják, kezeljék a felhasználó hozzáférési adatait, például jelszavait. Prioritás, hogy az elérhető összes RFC 20 ASCII karaktert, beleértve a szóközt is, támogatni kell jelszóösszetevőként. A jelszó hossza legalább 8 karakter legyen, és a bevitelnél támogatott kell legyen a legalább 64 karakter hosszú jelszó megadásának lehetősége is. A szolgáltató alkalmazzon jelszó feketelistákat, melyek tartalmával összeveti a felhasználó által megadott jelszót, és szükség esetén elutasítja annak használatát, ilyenek lehetnek, például, a már kompromittálódott, triviális szavak, ismétlődő karakterek, 123456, abcd, password, jelszó123. A szolgáltató számára a jelszószabály előírásban kizárólag a legalább 8 karakter hosszúság megkövetelését ajánlja a szabvány, további megkötéseket, például, kis- vagy nagybetűk, számok kombinációja, vagy bizonyos karakterek kitiltása nem ajánlott. Ezen felül a kényszerített, periodikus jelszóváltoztatás intézményét sem tehetik meg, mint ahogyan a jelszó hossz korlátozását vagy kényszerített levágását a legalább 64 karakteres hosszra tekintettel.

A részletszabályok mellett a tárolásra is kötelezettségeket ír elő a NIST 800-63B a szolgáltatók számára. A jelszavakat oly módon kell tárolni, hogy azok védettek legyenek offline támadás ellen, *SALT* biztonsági változóval együttesen kell *hash*-t képezni róluk, mely egyirányú, azaz nem visszafejthető lenyomatot eredményez. A biztonsági változó hosszának legalább 32 bitnek kell lennie.

Felhasználó memórialimitje

Az eddig megismert követelményeket, ajánlásokat egy biztonságos jelszó létrehozásához a felhasználó memórialimitje korlátozhatja. Ranghetti et al. (2012) publikációjából megismertük az átlagfelhasználó azon kapacitásait, melyek révén képes jelszavak memorizálására, de egyértelmű, hogy e kapacitás véges. A tanulmány bevezető fejezetében hivatkozik egy korábbi elemzésre (Brown et al. 2004), melyben megállapították – 218 résztvevővel – az átlagfelhasználó 8.2 jelszót használ átlagosan és egy felhasználóra vetítve átlagosan csupán 4.5 jelszó egyedi, azaz legalább egyszer minden jelszó újrafelhasználásra került. A tanulmány ezen elemzés újramérését célozta meg, összesen 263 résztvevő bevonásával, vizsgálandó cél a felhasználók jelszó-elfelejtésének elemzése volt. Az új halmazon 5.38 volt az átlagosan használt jelszó darabszáma, míg az egyedi jelszó csupán 3.98 darab.

A tanulmány résztvevőinek jelszavai elemzésével megállapította, hogy, az összesen 1415 egyedi jelszóból 62.6% kizárólag számokból, 24.3% csak betűkből, 12.4% alfanumerikus és csupán 0.7% az, ami a fentebb ismertetett ISO/IEC 10646 karaktersorozatból épült fel.

A tanulmány szerint a résztvevők 72%-a már tapasztalt olyan memóriaproblémát, melynek során nem tudott pontosan visszaemlékezni egy adott jelszóra. E mérőszám megoszlását két partícióban is elemezték: jelszó darabszámra és memória kiegészítésre vonatkozóan. Memória kiegészítésként, például, a felhasználó papírra írta a jelszót. Azok közül, akik leírták a jelszavukat, 59.8% tapasztalt memóriaproblémát, például, nem tudott visszaemlékezni az adott jelszóra, azok közül, akik nem írták le, 44.6% szintén tapasztalt memóriaproblémát. Darabszámra vetítve az alábbi megfigyelést tették:

- 1-3 darab jelszó: 53.1% tapasztalt memóriaproblémát,
- 4-6 darab jelszó: 80.7% tapasztalt memóriaproblémát,
- 7-9 darab jelszó: 84.0% tapasztalt memóriaproblémát.

Szignifikánsan megállapítható, hogy az átlagos memóriakapacitás a jelszó darabszámának növelésével egyenes arányban csökken. Tekintettel arra, hogy az újonnan elvégzett kutatásban átlagosan 5-6 darab jelszót használtak a résztvevők, a halmaz 4/5-e érintett a jelszómemorizációs problémákban. Ennek negatívumát tovább rontja, hogy a jelszavak karakterisztikája alapján kizárólag 1% alatti darabszámú jelszó felel meg az ajánlásoknak. Ebből következőik, hogy a gyenge jelszavak memorizálása is szignifikáns problémát eredményez. A tanulmányból megismerhetjük, hogy hosszabb jelszavakat a fiatal, iskolázott résztvevők alkalmaznak, míg az idős, kevésbé iskolázottak, rövid jelszavakat.

Authenticator Assurance Levels: autentikátor megbízhatósági szintek, NIST

E fejezetben szeretnénk röviden ismertetni a NIST által meghatározott három autentikátor megbízhatósági szintet, melyek egy adott azonosítási megoldás megbízhatóságát, alkalmazási területét határozzák meg. Az ismertetett fogalmak, leírások a NIST 800-63-3 és NIST 800-63B kiadványokból részletesebben is megismerhetők, behatóbb tárgyalásuk túlmutatna tanulmányunk keretein.

Authenticator Assurance Level 1 (AAL1)

A NIST 800-63B kiadvány 4.1. fejezetében definiáltak alapján, az AAL1 megköveteli *bármely egyfaktoros, többfaktoros autentikátor* használatát, az alább felsoroltakból (5.1. fejezet).

A sikeres azonosításhoz a felhasználónak igazolnia kell biztonságos autentikációs csatornán keresztül, hogy rendelkezik és hozzáférése van az adott autentikátorhoz. *Reautentikáció 30 nap* lejártát követően. Kormányzati azonosítás szolgáltató esetén meg kell felelni a Federal Information Processing Standard (FIPS) 140 Level 1 minősítésnek.

Elfogadott autentikátortípusok:

- Memorized Secret,
- Look-Up Secret,
- Out-of-Band Devices,
- Single-Factor One-Time Password (OTP) Device,
- Multi-Factor OTP Device,
- Single-Factor Cryptographic Software,
- Single-Factor Cryptographic Device,
- Multi-Factor Cryptographic Software,
- Multi-Factor Cryptographic Device.

Authenticator Assurance Level 2 (AAL2)

A NIST 800-63B kiadvány 4.2. fejezetében definiáltak alapján az AAL2 szint magas megbízhatóságot ad arra, hogy a felhasználó rendelkezik az autentikátorok felett, és birtokolja azokat. A sikeres azonosításhoz kötelező *két különböző autentikációs faktor* használata biztonságos autentikációs csatornán keresztül. Jóváhagyott *kriptográfiai megoldás*ok alkalmazása szintén kötelező. *Reautentikáció 12 óra vagy 30 perc inaktivitás* lejártát követően. Kormányzat által biztosított autentikátorok és kormányzati azonosítás szolgáltató esetén meg kell felelni a FIPS 140 Level 1 minősítésnek.

Elfogadott többfaktoros autentikátor típusok:

- Multi-Factor OTP Device,
- Multi-Factor Cryptographic Software,
- Multi-Factor Cryptographic Device.

Elfogadott egyfaktoros autentikátor típusok, Memorized Secret autentikátor együttes használata mellett:

- Look-Up Secret,
- Out-of-Band Device,
- Single-Factor OTP Device,
- Single-Factor Cryptographic Software,
- Single-Factor Cryptographic Device.

Authenticator Assurance Level 3 (AAL3)

A NIST 800-63B kiadvány 4.3. fejezetében definiáltak alapján, az AAL3 szint kiemelten magas megbízhatóságot ad arra, hogy a felhasználó rendelkezik az autentikátorok felett, és birtokolja azokat. A sikeres azonosításhoz kötelező *két különböző autentikációs faktor* használata biztonságos autentikációs csatornán keresztül. Jóváhagyott kriptográfiai megoldások alkalmazása szintén kötelező. Az AAL3 szint a felhasználó által igazoltan birtokolt *kriptográfiai kulcs* meglétén alapul. Kötelező alkalmazni egy *hardveres autentikátor*t és egy autentikátort, mely biztosítja a felhasználó-megszemélyesítéses támadás elleni védelmét. *Reautentikáció 12 óra vagy 15 perc inaktivitás* lejártát követően.

Az alkalmazott megoldások FIPS 140 minősítése AAL3 szinten kiemelten szigorú, ezáltal minden többfaktoros autentikátor hardveres modulként legalább Level 2, egyfaktoros kriptografikus eszköznek legalább Level 1 minősítésű, és ezzel együtt legalább Level 3 fizikai biztonsági minősítésűnek kell lennie. Minden azonosítás szolgáltatónak legalább Level 1 minősítésűnek kell lennie.

Elfogadott autentikátor típusok:

- Multi-Factor Cryptographic Device,
- Single-Factor Cryptographic Device és Memorized Secret,
- Multi-Factor OTP device (software or hardware) és Single-Factor Cryptographic Device,
- Multi-Factor OTP Device (hardware only) és Single-Factor Cryptographic Software,
- Single-Factor OTP Device (hardware only) és Multi-Factor Cryptographic Software Authenticator,
- Single-Factor OTP Device (hardware only) és Single-Factor Cryptographic Software Authenticator és Memorized Secret

Ahogyan kiemeltük, a fent ismertetett AAL szintek leírása, tanulmányunk keretein túlmutatóan, nem terjed ki minden részletre, teljes részletességgel a NIST 800-63B kiadványból ismerhető meg.

Összefoglalva a fent ismertetett három szintet, az alábbi tartalmazás írható fel:

- AAL3
  - o AAL2
    - AAL1.

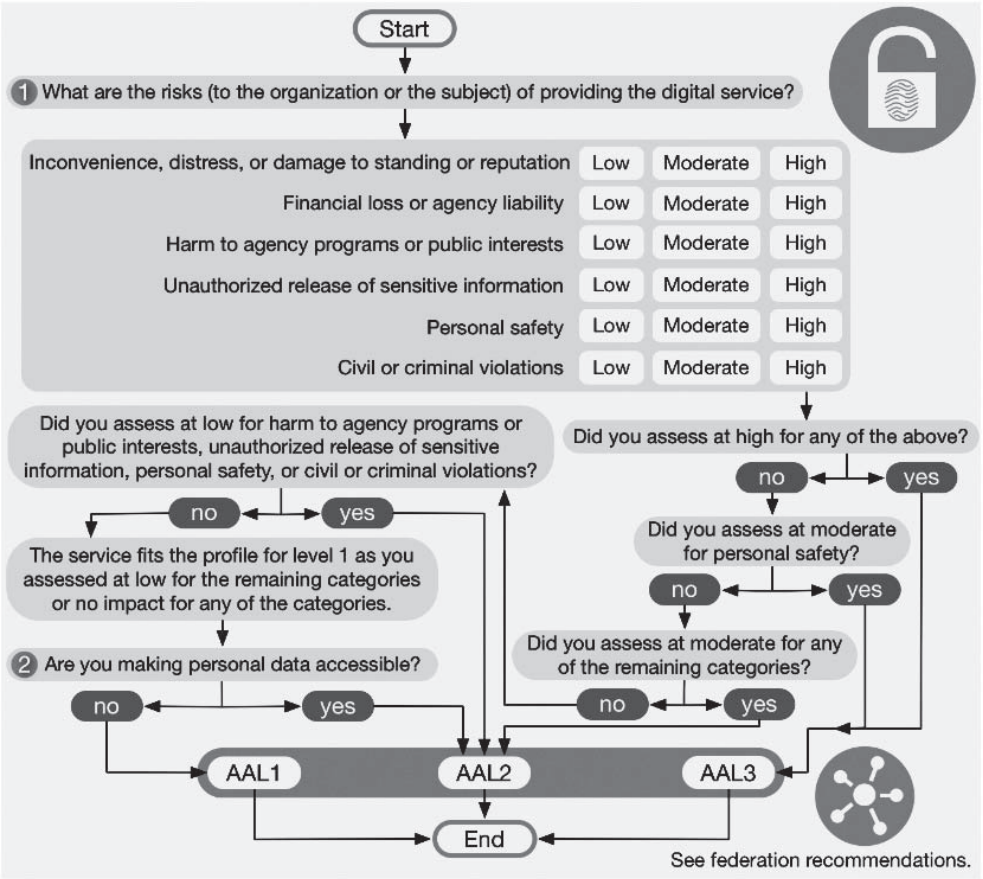
Szignifikánsan látható, hogy az AAL3 szint kiemelt biztonságot eredményez a felhasználó azonosítása során. A biztonsági szint meghatározásában vizsgálandó kockázatok:

A) rendszer leállásból eredő kár
B) pénzügyi veszteség vagy felelősség
C) közérdek sérül
D) jogosulatlan szenzitív adat kiadása
E) személyi biztonság
F) polgári vagy bűnügyi jogsértések

Feltételek a biztonsági szint meghatározásához:

- AAL3 szint, ha
  - o E = Közepes prioritású vagy legalább egy az (A-F)\E = Magas prioritású
- AAL2 szint, ha
  - o legalább egy az (A-F)\E = Közepes prioritású vagy legalább egy a (C, D, E, F) = Alacsony prioritású vagy a személyes adat hozzáférhető
- AAL1 szint, ha
  - o a fent ismertetett feltételek egyike sem teljesül

A kiválasztás metódusát a 11. ábra ismerteti.



11. ábra: Authenticator Assurance Level kiválasztás metódusa
(forrás: NIST 800-63-3 6.2. fejezet)

Hipotézis validálása I.

Szignifikáns biztonsági kockázat redukció

A ma alkalmazott, egy felhasználóhoz M darab hozzáférési adatot rendelő azonosítási környezettel szemben a globálisan központosított, egy felhasználóhoz egyetlen hozzáférési adatot kapcsoló megoldás szignifikánsan kisebb biztonsági kockázatot eredményez, National Institute of Standards and Technology, Authenticator Assurance Level 3 (NIST AAL3) biztonsági szinten, ahol M > 1. Állítás igazolása.

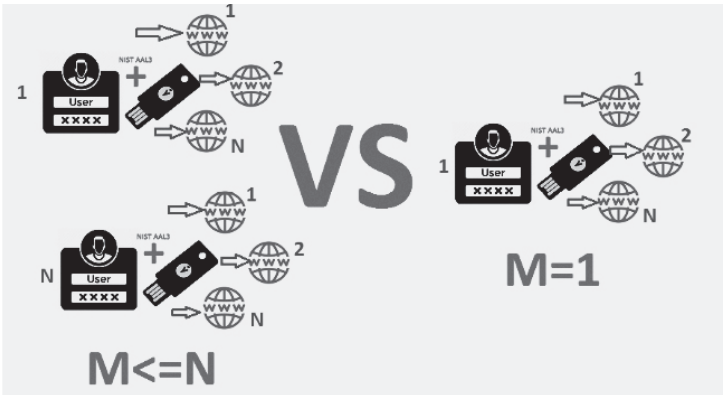
Az SSO által előidézett kockázat: a felhasználó több mint egy szolgáltatáshoz férhet hozzá egy hozzáférési adattal. E kockázatot koncentrálja, de újabbakat nem idéz elő a globálisan központosított felhasználó azonosítás folyamata.

Az *AAL3 szint* azonosítás szolgáltatói oldalon történő *megkövetelésével*, a Felhasználó azonosítás szintjei fejezetben ismertetett mindhárom (lokális, központosított, globálisan központosított) azonosítási mód esetén *igazoltan* (a NIST 800-63B alapján) *elérhető* kiemelt biztonságú, *alacsony kockázatú felhasználó azonosítás*.

Szignifikáns biztonsági kockázat a hozzáférési adat Memorized Secret mennyisége, melynek küszöbértékét a felhasználó memórialimitje határozza meg elsődlegesen. A Felhasználó memórialimitje fejezetben ismertettük, Ranghetti et al. (2012) publikációjának eredményein alapulva, az átlagfelhasználó Memorized Secret átlagos küszöbértékét, mely az 1-3 darabszám. E darabszám esetén 53.1%-a a résztvevőknek tapasztalt memória problémát, például elfelejtett vagy összecserélt jelszó. A publikáció eredményeiből megismerhettük, hogy az átlagos jelszóhasználat során egy átlagos felhasználónak legkevesebb 5-6 jelszót kell kezelnie. A publikációban ismertetett megelőző kutatás (Brown et al. 2004) eredményeként átlagosan 8 jelszót használt egy felhasználó. Napi alkalmazás használat feltáró jellegű vizsgálatunk eredményeként az átlagos jelszó darabszám 9.8, melyben legkevesebb 7 és legtöbb 16 független jelszó alkalmazását kell a felhasználónak átlagosan, napi szinten megtennie. Ranghetti et al. (2012) kutatási eredményei alapján igazolt, hogy a jelszó darabszámának növekedése szignifikáns memóriaproblémákat eredményez. Ebből következik, hogy *a darabszám csökkentése szignifikánsan javítja a jelszavak kezelését*, elsődleges értelemben, elkerülve azok elfelejtését vagy összecserélését.

Az SSO-felhasználó azonosítás szignifikánsan csökkenti a hozzáférési adatok darabszámát, viszont amiatt, hogy adott felhasználónak továbbra is (előfordulhat, és tanulmányunkban ismertetett elemzéseken alapulva igazoltan elő is fordul, hogy) egynél több SSO-hozzáféréssel kell rendelkeznie egynél több szolgáltatás igénybevételéhez, szignifikáns biztonsági kockázatot eredményez, például, *Phishing*-támadás kockázata: egynél több SSO bejelentkezési pont ismertetőjegyeit kell ismernie és validálnia a felhasználónak hozzáférési adatainak megadásakor. A Nyitott ablak a központosított felhasználó azonosítás fejezetben ismertetett probléma a lokálisan központosított felhasználó azonosításban további biztonsági kockázatokat eredményez. SSO esetén a felhasználó és szolgáltató erőforrásigénye csökken, de továbbra is egynél (szignifikánsan) több hozzáférési megoldás menedzselése szükséges: felhasználónak egynél több hozzáférési adata van, szolgáltató egynél több SSO bejelentkezési pontot implementál.

Hipotézisünk első pontjának igazolását összefoglalóan a 12. ábrán szemléltetett erőforrás-igény különbségekre alapozva szeretnénk megfogalmazni.



12. ábra: Lokális, lokálisan központosított VS globálisan központosított felhasználó azonosítás hozzáférési adat szükséges darabszáma

A 12. ábrából látható, hogy az azonosítás központosításának mértéke szignifikánsan redukálja a hozzáférési adat darabszámát. Megfelelve a NIST AAL3 szintnek, jelen példában a hozzáférési adat egy kriptografikus eszközt és egy Memorized Secretet,

felhasználónevet és jelszót definiál. A példaként szerepeltetett Yubico YubiKey eszköz kizárólagosan egy kriptografikus eszköz szemléltetéseként került felhasználásra.

Hipotézisünk első pontjában megfogalmaztuk, hogy az M<=N hozzáférési adatot igénylő felhasználó azonosítás megoldáshoz képest az M=1 hozzáférési adatot igénylő, globálisan központosított azonosítás szignifikánsan kisebb biztonsági kockázatot eredményez. Állításunk igazolásához levezettük, hogy a felhasználó memórialimitje Memorized Secret kezelése kapcsán korlátozott, Ranghetti et al. (2012) publikációjára alapozva legfeljebb 3 Memorized Secret esetén lesz elfogadható mértékű a felhasználó memória problémája, például visszaemlékezés jelszóra, jelszavak nem összecserélése. Ennek eredményeként – hiába csökkenti szignifikánsan az SSO alkalmazása a hozzáférési adat darabszámát – csak legjobb esetben lehet M=1, tanulmányunkban ismertetett szakirodalmi és egyéni elemzések alapján legkevesebb M=2, SSO használatával. Ebből következően, a felhasználó memórialimit problémára szignifikáns kockázatcsökkenést a globálisan központosított felhasználó azonosítás ad, M=1 értékkel. A memórialimittel párhuzamosan kockázati tényező: SSO bejelentkezési ponton *Phishing*-támadás és a NIST AAL3 követelményeként hardveres eszköz darabszáma, azonosítás szolgáltatóhoz tartozás – szintén memórialimitre korlátozott – megtanulása, visszaemlékezés (esetlegesen a hardveres kulcs hozzáférési adatának kezelése). A 12. ábrából látható, hogy NIST AAL3 szint eseténminden hozzáférési adatba beletartozik egy hardveres kulcs, melynek, ha követjük aminden-fiókhoz-egyedi–jelszó- sémát, szintén egyedinek kell lennie, azaz K=M. A kulcsSSO-fiókhoz tartozásának kezelése: megjegyzés, visszaemlékezés, szintén a felhasználómemórialimitjén alapul, mely korlátozza az eszköz darabszámát, illetve előídézi fizikaijegyzet készítését, például noteszben, alkalmazásban, szövegfájlban tárolja a párosítások
(Memorized Secret) információját. Ranghetti et al. (2012) publikációjának eredményére hivatkozva, az elemzés alanyainak 54.75%-a készített fizikai feljegyzést jelszaváról, miközben a jelszavak csupán 0.7%-a fel meg a NIST ajánlásának.

A fentiek alapján igazolható, hogy NIST AAL3 követelmények betartása esetén az M=1 globálisan központosított felhasználó azonosítás szignifikánsan kisebb biztonsági kockázatot eredményez, mint M<=N lokális vagy lokálisan központosított azonosítással. NIST AAL3 szint alkalmazásával, amennyiben Memorized Secret és kriptografikus hardveres kulcs párosával valósítjuk meg a felhasználó hozzáférési adatát, legfeljebb három „jelszó" kezelése lesz szükséges, mely Ranghetti et al. (2012) publikációjának eredményein alapulva elfogadható memórialimit probléma értéket eredményez (53.1%). Az üzemszerű működésben feltételezzük, hogy a használt Memorized Secret megfelel a NIST ajánlásának.

Szignifikáns erőforrás igény redukció

A központosítás mértékével egyenes arányban csökken mind a felhasználói, mind a szolgáltatói oldal erőforrás ráfordítása: a felhasználó hozzáférési adat menedzselése tekintetben; a szolgáltató felhasználó bázisának hozzáférési adat és infrastruktúra menedzselése, üzemeltetése tekintetben. Állítás igazolása.

Hivatkozva a 12. ábrára, triviálisan következik, hogy a hozzáférési adat darabszámánakcsökkentése szignifikáns erőforrásigény csökkenést eredményez mind felhasználói, mindszolgáltatói oldalon. A felhasználó, NIST AAL3 szint esetén, globálisan központosítottfelhasználó azonosítás megoldásban, legfeljebb három Memorized Secret adatot és egykriptografikus hardveres kulcsot kezel. A szolgáltató, ugyanezen környezetben, egyetlenSSO bejelentkezési pontot implementál.

A globálisan központosított felhasználó azonosítás (kutatásunk) célkitűzései

Kutatási projektünkben a globálisan központosított felhasználó azonosítás megvalósításának lehetőségeit vizsgáljuk. Célunk kidolgozni egy olyan felhasználó azonosítást megvalósító infrastruktúra absztrakt modelljét, mely együttműködést teremthet a már meglévő rendszerek között egy egységes protokoll definiálásával. Az így kialakított infrastruktúra lehetővé teszi a már meglévő azonosítás szolgáltatók rendszerbe kapcsolását, biztosítva az újrafelhasználás elvét, csökkentve a redundanciát, növelve az adatok konzisztenciáját. Az infrastruktúra absztrakt modelljén felül gyakorlati implementációt nem kívánunk bemutatni jövőbeni publikációnkban, kizárólag olyan kardinális kérdésekben szeretnénk iránymutatást adni, mint például a közös karakterkészlet vagy a dátumformátum, specifikus szabványokra hivatkozva. Az infrastruktúra keretében létrehozott felhasználói profil kibővíthető digitális identitás profillá, mely az alapadatokon (4T adat: viselt név, születési név, születési hely, születési idő, anyja neve; 1996. évi XX. tv. 4. § 4. a-d.) kívül előre definiált megkötésekkel bármilyen attribútumot tartalmazhat, például telefonszám, lakcím, bankszámlaszám.

A koncepció alapja, hogy az autentikációs modell lehetővé tegye az esetlegesen decentralizált központi azonosítás szolgáltatók használatát is. Erre a különböző országok közötti együttműködés támogatásakor lehet szükség, ha valamilyen oknál fogva nem kivitelezhető az abszolút globális azonosítást végző szolgáltató létrehozása. Például jogi szabályozás nem teszi lehetővé adott személy felvételét a rendszerbe, de egy másik – azonos biztonsági szintű – rendszer biztosítja ezt. *Ilyen esetben egynél több azonosítást végző rendszert együttesen alkalmazva* érhető el a globális, központosított autentikáció.

Az infrastruktúra keretében *nem egy újabb azonosítás szolgáltatás*t szeretnénk megalapozni, *hanem a már meglévők rendszerbe kapcsolás*át, előre definiált követelmények mentén. Az így kialakított infrastruktúra, *függetlenül az azonosítás szolgáltatók típusától*, például kormányzati Ügyfélkapu, login.gov vagy magánszektor Google Sign-In, Facebook, *bármely területen megoldást ad* felhasználó azonosításra. Ahogyan, tanulmányunkban kiemeltük, NIST AAL3 szinten kiemelt megbízhatóságú azonosítás valósítható meg, mely alkalmazható, például internetes bank, hivatalos ügyintézés, adóbevallás szolgáltatásokban is.

Az infrastruktúrabeli együttműködés szabályozásához mind azonosítás szolgáltatói, mind szolgáltatói követelményeket fogalmaztunk meg, melyek betartása elősegíti a gördülékeny együttműködést.

A csatlakozó azonosítás szolgáltatókkal szemben támasztott követelmények:

1. a rendszerbe kapcsolt azonosítás szolgáltatók diszjunktak egy adott felhasználóra (M=1 minden felhasználóra);
2. az azonosítás szolgáltató rendszerében biztosítja a felhasználó számára, hogy adott szolgáltató felé az általa engedélyezett attribútumokat megoszthassa, ezeket később monitorozhassa, visszavonhassa a hozzáférést a szolgáltatótól (GDPR 15. cikk);
3. az azonosítás szolgáltató rendszerében biztosítja a felhasználó számára, hogy adott szolgáltató felé automatizáltan továbbítja a felhasználó adattörlési kérelmét, majd feldolgozza a szolgáltató a kérelemre adott válaszát (GDPR 17. cikk);
4. az azonosítás szolgáltató rendszerében biztosítja a felhasználó számára, hogy adatait egységes, előre definiált formátumban átvihesse más azonosítás szolgáltató rendszerébe, miután az adott azonosítás szolgáltató rendszeréből törölte felhasználói profilját az adott felhasználó (GDPR 20. cikk);
5. az azonosítás szolgáltató rendszerében biztosítja a felhasználó kétséget kizáró, előre definiált protokoll alapján elvégzett videós vagy személyes megjelenés útján

elvégzett azonosítását és a digitális identitás profilba, a felhasználó által, a 4T adatokon felül rögzített adatainak ellenőrzését, szintén előre definiált protokollok alapján (NIST IAL3 megfelelőség).

A csatlakozó szolgáltatókkal szemben támasztott követelmények:

1. a lokális szolgáltató rendszerében biztosítja, hogy implementálja a lokálisan tárolt adatok törlését elvégző funkciót, és együttműködik az azonosítás szolgáltató rendszerével az automatizált törlés végrehajtásában (GDPR 17. cikk);
2. a lokális szolgáltató implementálja a felhasználó egyedi azonosítójának megváltozását kezelő funkciót: a felhasználó kérésére automatizáltan végrehajtja az egyedi azonosító változásának átvezetését.

(Köz)hiteles felhasználói profil

A felhasználói profil hitelessége internetes környezetben kiemelt jelentőségű, annak okán, hogy a felhasználó távoli interakcióban jelenik meg, megfelelő azonosítás nélkül bárkinek kiadhatja magát. A felhasználó regisztrációjakor előírt ellenőrzés metódusát, megbízhatósági szintjét a NIST 800-63A kiadvány 4.5. fejezete tárgyalja részletesen, ebből, tanulmányunk keretében, kiemelt megbízhatóságot elérendő, Identity Assurance Level 3 (NIST IAL3) követelményeinek megfelelést ismertetjük. A felhasználó fizikai, valós világbeli személyazonosságát három csoportosítású, különböző követelményű dokumentumokkal (evidence: bizonyíték) igazolhatja:

1. két darab Superior megfelelőségű,
2. egy darab Superior és egy darab Strong megfelelőségű,
3. két darab Strong és egy darab Fair megfelelőségű.

A megfelelőség besorolásokat az 5.2.1. Identity Evidence Quality Requirements fejezet 5-1. táblázata definiálja, például Superior minősítésben útlevél, mely biometrikus profilt tartalmaz úgy, mint arcképmás, ujjlenyomat.

Az IAL3 legfontosabb követelménye a személyes (In-Person Proofing) vagy felügyelt távoli (Supervised Remote In-Person Proofing) személyazonosítás, önbevallott attribútum nélkül (a felhasználó hiteles dokumentumokkal igazolja az egyes attribútumokat, például, a lakcímet ne csak megadja, hanem igazolja is), kötelező biometrikus (például arcképmás, ujjlenyomat) megerősítéssel. A személyes megjelenés triviális, viszont a távoli azonosítás követelményeit 5.3.3.2. fejezet ismerteti: nagy felbontású videós azonosítás, élőerős ellenőrző személyzettel, biztonságos kapcsolaton keresztül.

Összefoglalva, egy felhasználói profil közhiteles attribútumokat tartalmaz, ha a felhasználó regisztrációkor hiteles dokumentumokkal, például, útlevél, személyazonosító igazolvány, igazolja a rögzített attribútumokat, például születési dátum, lakcím, név. A regisztrátor személyes vagy felügyelt távoli megjelenés útján ellenőrzi a felhasználó személyazonosságát, a benyújtott dokumentumok érvényességét, hitelességét.

Szeretnénk hangsúlyozni, hogy a fenti ismertető egy összefoglalója a NIST 800-63A kiadványában definiált metódusoknak, célunk a közhiteles felhasználói profil követelményeinek közérthető megfogalmazása volt, tanulmányunk keretein túlmutatna egy részletes, minden pontra kiterjedő leírás.

Hipotézis validálása II.

Adatvédelmi megoldások támogatása

A felhasználó attribútummegosztásának nyomon követése, monitorozása szignifikánsan eredményesebb, mint elosztott környezetben (a felhasználó lokálisan, manuálisan osztja meg attribútumait, melyek nyomon követésére, például, jegyzetfüzetet, szöveges dokumentum fájlt használ). Állítás igazolása.

Az infrastruktúra csatlakozás egyik feltétele az azonosítás szolgáltató számára, hogy biztosítson lehetőséget a felhasználó számára az attribútummegosztás nyomon követésére és a megosztással járó attribútumhozzáférés szolgáltatótól történő visszavonására. A ma alkalmazott SSO-attribútummegosztások során teljes részletességgel nem kerül monitorozásra, mely szolgáltatónak, milyen attribútumokat osztott meg a felhasználó, például Google Sign-In esetén. Általánosan szolgáltatás igénybevételéhez tett regisztráció során lokálisan kell attribútumokat rögzíteni, például név, cím, telefonszám. Ezek jövőbeni monitorozására akkor lesz lehetősége adott felhasználónak, ha fizikai naplót vezet, például füzetben, elektronikus dokumentumban.

A monitorozás lehetősége nem csupán a felhasználót támogatja, hanem a szolgáltató GDPR-kötelezettségét is, melynek során a felhasználó tájékoztatást kéri róla kezelt attribútumokról. A tájékoztatás folyamatosan, szolgáltatói interakció nélkül, elérhető az infrastruktúraazonosítás szolgáltató által üzemeltetett felhasználói profilban.

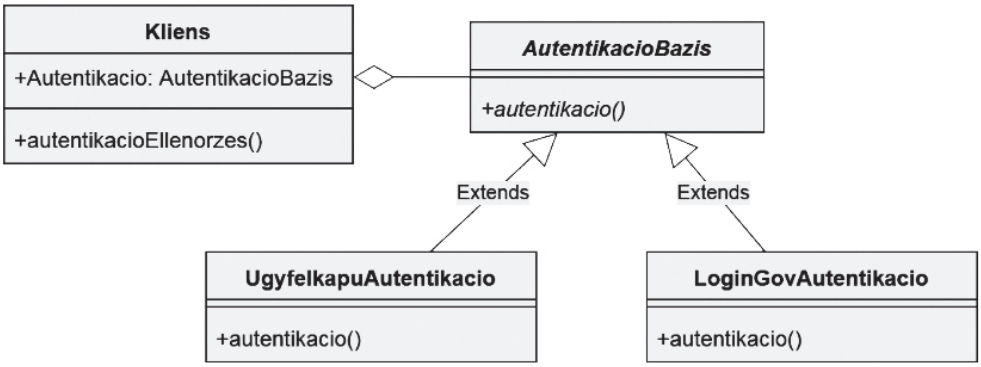
Kutatásunk célkitűzéseinek ismertetése példán keresztül

Az infrastruktúra működését egy webshop interakción keresztül a 13. ábra szemlélteti.

13. ábra: Globális, Központosított felhasználó azonosítás modellje: webshop interakció

A rendszerbe foglalt azonosítás szolgáltatók egy központi útválasztón keresztül kapcsolhatók össze a szolgáltatási rendszerekkel, például e-bank, webshop, oktatási vagy

hivatalos ügyintézési rendszerek. Az útválasztó működése a Stratégia tervezési mintára épül, mely lehetőséget ad az eltérő implementációjú azonosítás szolgáltatók közös interfészen keresztüli használatára (Gamma et al. 1994: 315). Jelen esetben a felhasználó azonosítása, az autentikáció ellenőrzése minden esetben ugyanazon célt valósítja meg. A működés absztrakt modelljét a 14. ábra szemlélteti.



14. ábra: Stratégia tervezési minta lokális autentikáció ellenőrzéshez

Célkitűzésünk, hogy a szolgáltatói oldal tehermentesítése végett, a különböző AutentikacioBazis implementációk alkalmazására közvetlenül az útválasztó szolgáltatásban kerüljön sor. Ez lehetővé teszi, hogy a csatlakozó szolgáltató, például webshop, e-bank, kizárólag az útválasztó autentikációt menedzselő interfészeit implementálja. A központosítás eredménye, hogy egy esetleges implementáció változást kizárólag az útválasztó szolgáltatásban kell átvezetni, elkerülve a kapcsolódó szolgáltatókra kihatást, növelve a konzisztens működést.

A felhasználó azonosítás szolgáltatónál kezelt profiljából attribútumokat oszthat meg a szolgáltatókkal, például név, cím, telefonszám. A megosztás menedzselése tervezetten az OAuth 2.0 RFC 6749 ipari szabvány alkalmazásával történik. Előnye, hogy a felhasználó maga dönthet arról, mely attribútumát kivel osztja meg, illetve nyomon követhetné kinek és mit osztott meg korábban. Ez hozzájárulhat az adatvédelmi jogszabályok támogatásához is:

- a GDPR 15. cikk alapján a felhasználó bármikor megtekintheti kinek, milyen attribútumokat osztott meg;
- a GDPR 16. cikk, az adatok naprakészen tartása rendelkezés támogatható az azonosítást követően az engedélyezett attribútumok átadásával (a szolgáltató ellenőrizheti, változott-e adat és ennek megfelelően frissítheti lokális adatbázisát).

Konklúzió

Jelen publikációnkban áttekintettük a közelmúlt jelentős információbiztonsági és felhasználó azonosítással kapcsolatos incidenseit. Az egyre növekvő kiberfenyegetettség megerősíti, hogy rendkívül aktuális küldetés a felhasználó azonosítás és személyes adatok védelme területén hatékony megoldások kidolgozása. Ennek apropóján áttekintettük, mit tehet a szolgáltatói oldal és mit a felhasználói oldal a biztonság megerősítésére.

Összefoglaltuk a legalapvetőbb ellenőrzés lépéseit, melyek teljesítésével a felhasználó nehézségek nélkül győződhet meg egy, a személyes adatok megadását kérő weboldal megbízhatóságáról. Igyekeztünk tanácsokat adni a szolgáltatói oldal résztvevőinek is, elsősorban a biztonságos adatátviteli kapcsolat megteremtésére, felhívva a figyelmet az SSL-tanúsítvány alkalmazásának jelentőségére. Szakirodalmi és saját felméréseink eredményeit összefoglalva, statisztikai mutatókkal világítottunk rá milyen interakció mentén kezelik az egyes problémákat a szolgáltatók, például hibás SSL-tanúsítvány vagy adatvédelmi tájékoztató javítása.

A felhasználó azonosításnak alapvetően három szintje lehet: lokális, lokálisan központosított, globálisan központosított, illetve a lokális és lokálisan központosított együttesen kevert azonosítást valósíthat meg. Ismertettük e szintek tulajdonságait, a (lokálisan) központosított esetén kiemeltük az esetleges visszaélésre lehetőséget teremtő kockázatokat. Kiemelten, ha a dedikált központi azonosítás szolgáltatást megkerülve, közvetlenül a szolgáltatás kéri el a hozzáférési adatokat.

Az olvasó megismerhette kutatásunk célkitűzéseit a globálisan központosított felhasználó azonosítás kontextusában. Modellünk szemléltetésére egy webshop interakció folyamatát ismertető ábrát készítettünk, mely bemutatja a felhasználó attribútumainak, szolgáltató részére történő átadás lépéseit. A koncepció alapja, hogy az autentikációs modell lehetővé tegye az esetlegesen decentralizált központi azonosítás szolgáltatók használatát is, ha valamilyen oknál fogva nem kivitelezhető az abszolút globális azonosítást végző szolgáltató létrehozása. Például jogi szabályozás nem teszi lehetővé adott személy felvételét a rendszerbe, de egy másik – azonos biztonsági szintű – rendszer biztosítja ezt. Ilyen esetben egynél több azonosítást végző rendszert együttesen alkalmazva érhető el a globális, központosított autentikáció, kulcsfontosságú, hogy ez esetben is teljesül, M=1, azaz minden felhasználó egyetlen hozzáférési adattal rendelkezik a teljes infrastruktúrában.

A rendszerbe foglalt azonosítás szolgáltatók a *Stratégia* tervezési mintára épülő központi útválasztón keresztül kapcsolhatók össze a szolgáltatási rendszerekkel, ezzel tehermentesítve a szolgáltatói oldal implementációra fordítandó erőforrásait.

Kutatásunk keretében kidolgozott modellek, megoldások részletes elméleti ismertetését egy különálló, jövőbeni publikációban tervezzük ismertetni, jelen publikációban, annak célkitűzését szem előtt tartva, kizárólag a kutatás modelljének célkitűzéseit, elérendő céljait ismertettük.

Hipotézisünk igazolására szakirodalmi és saját felméréseink eredményeit elemeztük, igazolva, hogy az átlagfelhasználó 1-3 darab Memorized Secret kezelésével tapasztal elfogadható mértékű memórialimit-problémákat, úgy, mint jelszó elfelejtése, összecserélése. Az ismertetett, AAL3 szintű biztonság megteremtése mellett belátható, annál eredményesebben védhető egy felhasználó hozzáférési adat halmaza, minél kevesebb van belőle, azaz minél magasabb a központosítás szintje. Hasonlóan látható be az adatvédelem támogatása kapcsán az adatok konzisztenciájának fenntartása is, minél kevesebb felhasználói profilban kell naprakészen tartani adatokat, annál eredményesebben biztosítható a tényleges konzisztencia. Ennek egyik eszköze lehet, ha a felhasználó kizárólag egy közhiteles profillal azonosíthatja magát, az infrastruktúrába kapcsolt azonosítás szolgáltatóknak emiatt egy adott felhasználóra diszjunktnak kell lenniük.

Továbbfejlesztési irányok, jövőbeni célkitűzéseink

Publikációnk zárásaként szeretnénk bemutatni jövőbeni célkitűzéseinket, a lehetséges fejlesztési irányokat. Kutatásunk nem titkolt célja kidolgozni a globálisan központosított felhasználó azonosítás modelljét, mely együttműködési platform lehet a meglévő azonosítás szolgáltatók között, közhiteles azonosítást biztosítva a csatlakozó szolgáltatók részére. Az infrastruktúra kiemelt célja, hogy minden felhasználó egyetlen, közhiteles profillal rendelkezzen. Ehhez kapcsolódó célkitűzésünk a globális felhasználó azonosító gyakorlati megvalósítása, mely elválaszthatatlanul kapcsolódik a felhasználóhoz, ugyanakkor arról plusz információt nem oszt meg, kiegészítő információk ismerete nélkül hozzá nem köthető. A globális felhasználó azonosító megvalósításához szorosan kapcsolódik a robusztus személyazonosság megerősítés, mely napjainkban ujjlenyomat vagy arcképmás vizsgálatán alapul. A legelterjedtebb megoldás az arcképmáson alapuló megerősítés, melyben az arc sérülékenysége mellett a megbízható egyezéskeresés is hátrányt jelenthet, a NIST vizsgálatára alapozva az 55 éves kor feletti személyek azonosíthatók megbízhatóan e technológia révén (Grother és Ngan 2014: 36). Alternatív személyazonosság megerősítő megoldás kidolgozását szerveztük egy új kutatási projektünkbe, melynek első eredményeit a 17. PhD konferencián ismertettük a (Roskó és Adamkó 2018) publikációnkban. E megoldás a humán DNS profilalapú személyazonosság ellenőrzésre épül, melynek egyetlen hátránya, hogy egypetéjű ikrek esetén nem, vagy csak korlátozottan alkalmazható. Jövőbeni célunk kidolgozni olyan metódust, mely kiterjeszthető a humán DNS-alapú személyazonosság megerősítést az egypetéjű ikrekre is.

Egy közhiteles felhasználó azonosítást biztosító infrastruktúra számos lehetőség előtt nyithat kaput, például, redukálhatók az ál-profilok a közösségi média platformokon úgy, mint Facebook, linkedIn. Bízunk benne, hogy kutatásunkkal hozzájárulhatunk ahhoz, hogy az online térben legalább annyira biztonságban lehessünk, mint a valós életben.

Irodalom

Az Európai Parlament és a Tanács, (Eu) 2016/679 rendelete http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016R0679&from=hu

Brown, Alan S., Elisabeth Bracken, Sandy Zoccoli and King Douglas, "Generating and remembering passwords", Applied Cognitive Psychology, Vol. 18. (2004) Issue 6., pp. 641–651. https://doi.org/10.1002/acp.1014

Del Valle, Gaby, "The Marriott hack exposed the passport numbers of more than 5 million people", *Vox media*, 2019. https://www.vox.com/the-goods/2018/11/30/18119770/marriott-hotels-starwood-hack

Elliott, Matt, "Why you are at risk if you use SMS for two-step verification", *cnet.com*, 31 July 2017. https://www.cnet.com/how-to/why-you-are-at-risk-if-you-use-sms-for-two-step-verification/

Erdősi Péter Máté és Solymos Ákos, *IT biztonság közérthetően, v3*, Neumann János Számítógéptudományi Társaság, Budapest, 2018.

Freed, Benjamin, "Tennessee health data breach exposes information on thousands of HIV patients", *statescoop*, 13 July 2018. https://statescoop.com/tennessee-health-data-breach-exposes-information-about-thousands-of-hiv-patients/

Gamma, Erich, John Vlissides, Richard Helm, Ralph Johnson, *Design Patterns Elements of Reusable Object-Oriented Software*, Addison-Wesley, 1994.

Garcia, Mike, "Easy Ways to Build a Better P@$5w0rd", *NIST*, 4 October 2017. www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd

Ghasemisharif, Mohammad, Amrutha Ramesh, Stephen Checkoway, Chris Kanich, Jason Polakis, "O Single Sign-Off, Where Art Thou? An Empirical Analysis of Single Sign-On Account Hijacking and Session Management on the Web", *Proceedings of the27th USENIX Security Symposium*, August 15–17, 2018, Baltimore, MD, USA, 2018, pp. 1475-1492. https://www.usenix.org/conference/usenixsecurity18/presentation/ghasemisharif

Grassi, Paul A., Michael E. Garcia, James L. Fenton, *NIST Special Publication 800-63-3 Digital Identity Guidelines*, U.S. Department of Commerce National Institute of Standards and Technology, 2017. https://doi.org/10.6028/NIST.SP.800-63-3

Grassi, Paul A., James L. Fenton and Elaine M. Newton, *NIST Special Publication 800-63B Digital Identity Guidelines Authentication and Lifecycle Management*, U.S. Department of Commerce National Institute of Standards and Technology, 2017. https://doi.org/10.6028/NIST.SP.800-63b

Grassi, Paul A., James L. Fenton, *NIST Special Publication 800-63A Digital Identity Guidelines Enrollment and Identity Proofing*, U.S. Department of Commerce National Institute of Standards and Technology, 2017. https://doi.org/10.6028/NIST.SP.800-63a

Grother, Patrick and Mei Ngan, *Face Recognition Vendor Test (FRVT) NIST Interagency Report 8009*, U.S. Department of Commerce National Institute of Standards and Technology, 2014, pp. 36–38. https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=915761

Gupta, B.B., Nalin A. G. Arachchilage, Kostas E. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions", *Telecommunication Systems*, Vol. 67. (2017) Issue 2., pp. 247-267. https://doi.org/10.1007/s11235-017-0334-z

Hunt, Troy, "The 773 Million Record "Collection #1" Data Breach", 17 January 2019. https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

Huth, Alexa, Michael Orlando and Linda Pesante, *Password Security, Protection, and Management*, Carnegie Mellon University – US CERT, 2012. http://aahuth.com/wp-content/uploads/sites/44/2014/02/PasswordMgmt2012-2.pdf

Kolouch, Jan, "Evolution of Phishing and Business Email Compromise Campaigns in the Czech Republic", *AARMS*, Vol. 17. (2018) No. 3., pp. 83-100.

Leskin, Paige, "Here's how to check if you were one of the 500 million customers affected by the Marriott hack", *Business Insider*, 30 November 2018. https://www.businessinsider.com/marriott-starwood-hotel-hack-data-breach-how-to-check-if-you-were-affected-2018-11

Marinos, Louis, *ENISA Threat Landscape Report 2018 15 Top Cyberthreats and Trends*, European Union Agency For Network and Information Security, 2019. https://doi.org/10.2824/6227572019

McKay, Kerry and David Cooper, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, U.S. Department of Commerce National Institute of Standards and Technology, 2018. URL: https://csrc.nist.gov/CSRC/media/Publications/sp/800-52/rev-2/draft/documents/sp800-52r2-draft2.pdf

NMHH, "Hogyan kerülhetjük el az adathalászok hálóját?", 2018. augusztus 17. http://nmhh.hu/cikk/197741/Hogyan_kerulhetjuk_el_az_adathalaszok_halojat

Porter, Jon, "Major SMS security lapse is a reminder to use authenticator apps instead", *The Verge*, 16 November 2018. https://www.theverge.com/2018/11/16/18098286/vovox-security-breach-two-factor-authentication-2fa-codes-exposed

Ranghetti, Denise, Antonio Jaeger, Carlos F. A. Gomes and Lilian Milnitsky Stein, "Passwords Usage and Human Memory Limitations: A Survey across Age and Educational Background", *PLOS One*, Vol. 7. (2012) Issue 12. https://doi.org/10.1371/journal.pone.0051067

Roskó Tibor és Adamkó Attila, "The human DNA can be the bridge between the Human andits data set in the Future", in *A 15 éves PEME XVII. PhD - Konferenciájának előadásai*, Professzorok az Európai Magyarországért Egyesület, Budapest, 2018, 123-133. old.

Yue, Chuan, "The Devil is Phishing: Rethinking Web Single Sign-On Systems Security", Presented at the 6th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '13), 12 August 2013, Washington https://www.usenix.org/system/files/conference/leet13/leet13-paper_yue.pdf

1. sz. melléklet: Fogalmak, definíciók

Attribútum
Személyt leíró adat, például név, születési dátum, lakcím.

Biztonságos átviteli csatorna (Authenticated Protected Channel)
Elfogadott kriptografikus megoldásokat alkalmazó, titkosított adatátviteli csatorna, melyben a kliens autentikálta a fogadó szervert. Általánosan alkalmazott felhasználó azonosítás során, például Transport Layer Security (TLS).

Hozzáférési adat
Autentikátorok halmaza. Saját fogalom, melyet tanulmányunkban azon autentikátorok, azonosítók egy halmazára vonatkoztatunk, mely magában foglalja egy bejelentkezési pont autentikációjához szükséges összes azonosítót, például felhasználónév, jelszó, token, kriptografikus hardveres eszköz.

Információbiztonság
A biztonság fogalma hétköznapi értelemben veszélyektől mentes, zavartalan állapotot definiál. Az *adatbiztonság*, informatikai fogalomként, három követelmény teljesülése esetén az adatok biztonságát hivatott megteremteni. E három követelmény:

- *bizalmasság: valami, amit csak az arra jogosultak ismerhetnek meg, a megismerésre jogosultak köre korlátozott;*
- *sértetlenség, integritás: valami, ami eredeti állapotának megfelel és teljes;*
- *rendelkezésre állás: a szükséges infrastruktúrák és adatok ott és akkor állnak a felhasználó rendelkezésére, amikor arra szükség van*

Az adatbiztonsághoz kapcsolódva az alábbi fogalmak egyértelműen kijelölik az egyes intézkedések határait:

- *adatbiztonság:* a számítógépes rendszerekben tárolt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának megteremtése (nem foglalkozik az alkalmazások és a kisegítő berendezések – szünetmentes áramforrás – biztonságával);
- *informatikai biztonság:* az információs rendszerekben tárolt adatok és a feldolgozáshoz használt hardveres és szoftveres erőforrások biztonságára vonatkozik. Ha az *adat* fogalmát kiterjesztjük az *információra*, akkor ez a definíció egyenértékű az információbiztonság fogalmával, egyébként szűkebb értelmű nála;
- *információbiztonság:* tények, utasítások, elképzelések emberi vagy gépi úton formalizált továbbítási, feldolgozási vagy tárolási célú reprezentánsai bizalmasságának, sértetlenségének és rendelkezésre állásának megteremtése. Amennyiben az adat fogalmát az emberi formalizálással (beszéd, előadás, beszélgetés) együtt értelmezzük, akkor egyenértékű az informatikai biztonság fogalmával, egyébként bővebb nála;
- *adatvédelem:* személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége.

Memorized Secret
Ismeretalapú autentikációs faktor, mely a felhasználó által memorizálható karaktersorozatot (ISO/IEC 10646) definiálja, például felhasználónév, jelszó, Personal Identification Number (PIN-kód).

Példák
Tanulmányunkban a példaként említett bármely tartalom kizárólag a szemléltetést hivatott megvalósítani, az sem alkalmazási ajánlást, sem kötelezettséget nem eredményez, például Yubico YubiKey, Ügyfélkapu, magyarorszag.hu, login.gov, Google Sign-In, Facebook, OAuth 2.0.

Re-autentikáció
Lejárt felhasználói munkamenetet követő ismételt autentikáció.

Változók
- K: pozitív, egész szám, mely a hardveres kulcs darabszáma
- M: pozitív, egész szám, mely a hozzáférési adatok darabszáma
- N: pozitív, egész szám, mely az igénybe vett szolgáltatások darabszáma