

36. Országos Tudományos Diákköri Konferencia
Had- és Rendészettudományi Szekció
Budapest, 2023. április 18-20.
Nemzeti Közszolgálati Egyetem
Rendészettudományi Kar

**Adatvédelmi paradoxon vizsgálata egy kiberbiztonsági képzés
végzős hallgatói körében**

Jelige: *ap21*

Pályamunka lezárásának időpontja: 2021. 11.

2023.

Tartalomjegyzék

BEVEZETŐ RÉSZ	3
Témaválasztás indokolása	3
Téma helye, szerepe, kapcsolódásai, jelentősége, aktualitása	3
Célkitűzések megfogalmazása	5
Hipotézisek	6
Kutatómódszertan	6
Dolgozat gyakorlati alkalmazásának lehetséges esetei	6
1. – BEVEZETÉS AZ ADATVÉDELEM ALAPVETŐ FOGALMAIBA	7
2. – SOCIAL ENGINEERING	12
2.1 – A social engineering sajátossága	13
2.2 – Social engineering támadási metodikája	14
2.3 – Módszerek csoportosítása	16
2.3.1 – Emberközpontú megközelítés	16
2.3.2 – Szocio-technikai megközelítés	19
3. – ADATVÉDELMI PARADOXON	20
3.1 – Korai kutatások	21
3.2 – Összefüggések keresése – demográfiai és nem-demográfiai csoportosítások	22
3.3 – Lehetséges elméleti magyarázatok	24
3.3.1.- Privacy calculus	24
3.3.2 – Korlátozott racionalitás	25
3.3.3 – Tapasztalat, tudás hiánya	26
3.3.4 – Társadalmi befolyásolás	26
3.4 – Adatvédelmi paradoxon - összegzés	27
4 – KÍSÉRLET	28
4.1 – Kísérlet célja	28
4.2 – Kísérlet módszerei	28
4.3 – Kísérlet célcsoportja	28
4.4 – Kísérlet menete	28
4.5 – Kérdőív	29
4.5.1 – Önbevallott biztonságtudatosság	29
4.5.2 – Elméleti ismeretek	30
4.5.3 – Gyakorlati alkalmazás	30
4.5.4 – Következtetések	35
4.6 – Adathalász kísérletek	35

4.6.1 – <i>Befolyásoló tényezők</i>	36
4.6.2 – <i>Első e-mail – állásajánlat</i>	36
4.6.3 – <i>Második e-mail – Gyanús tevékenység</i>	38
4.6.4 – <i>Következtetések</i>	39
AJÁNLÁS	40
ÖSSZEGZÉS	41
FORRÁSJEGYZÉK	42
MELLÉKLETEK:	46
1. sz. melléklet: Kérdőív és eredményei	47
2. sz. melléklet: kérdőív szöveges válaszai	56
ÖSSZEGZÉS (ANNOTÁCIÓ)	61

BEVEZETŐ RÉSZ

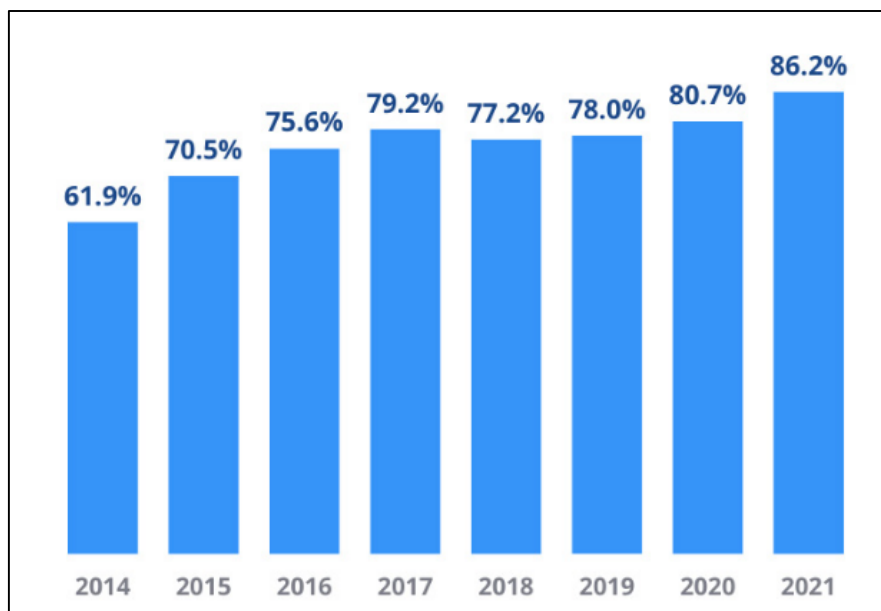
Témaválasztás indokolása

Személyes érintettségem a témaválasztás kapcsán, hogy régóta foglalkoztat, nem csak az, hogy vajon egy magánszemélynek, felhasználónak milyen adatvédelmi lehetőségei vannak, hanem az is, hogy ezek mennyire széleskörben ismertek és milyen szinten követik a tudatosítási törekvéseket, legjobb gyakorlatokat. Ugyanis a kibertámadások száma folyamatosan növekszik, technikai, technológiai módszerekkel nem lehet minden támadást elhárítani, főleg, ha az eszköz kezelője nem mindig cselekszik tudatosan a kibertérben. Minél többet foglalkoztam a gondolattal, annál több tudatosító anyaggal találkoztam, majd annál több eszmecserét futtattam a tudatosítás fontosságáról. A biztonságtudatossági szint és az elsajátított információbiztonsággal, adatvédelemmel kapcsolatos tudás ismerőseim körében egészen sokáig különböző volt, de közben egy dolog állandó maradt: az említett tudás gyakorlati hasznosítása, pontosabban annak hiánya. Meggyőződésem szerint attól még, hogy valaki azt gondolja, mindent tud személyes adatainak védelméről, ugyanúgy előfordulhat, hogy nem fogja elégséges szinten megvédeni azokat valamilyen oknál fogva. A helyzet érdekességéből és a támadások online térbe áthelyeződéséből következik, hogy egyre aktuálisabbá és sürgősebbé vált a téma mélyebb vizsgálata, így ezen ellentmondás elemzése, lehetséges okok feltárása.

Téma helye, szerepe, kapcsolódásai, jelentősége, aktualitása

Ahogy említettem, napjainkban egyre növekszik a kibertámadások száma, egyre sokrétűbb, szofisztikáltabb módszereket alkalmaznak a kiberbűnözők ¹. Számos kutatás vizsgálja ezt a növekvő tendenciát, a Cyberedge Group 2021-es Kibervédelmi jelentés rögzíti, hogy az elmúlt években a szervezetek hány százalékát érte legalább egyszer kibertámadás. Ezt az 1. számú ábra szemlélteti, melyről leolvasható a támadások számának folytonos emelkedése.

¹ Europol - Internet Organised Crime Threat Assessment (IOCTA) 2021, Europol, Publications Office of the European Union, Luxembourg, 2021, 8. o.



1. ábra: Azon szervezetek százalékos aránya, amelyek az elmúlt években legalább egyszer kibertámadások áldozatává váltak

Azt már nagyon helyesen felmérték mind a jogalkotók, mind a vállalatok, hogy a lakosságot tudatosítani szükséges, ennek megfelelően számtalan képzési program elindult. Hatásukat, hatásosságukat viszont nehéz mérni, a támadások száma folyamatosan nő, ennek következtében nem egyértelmű, hogy mennyire tekinthetők hatékonyak a rendelkezésünkre álló programok. Úgy gondolom, jelen dolgozatom célja kettős: nem csak szimplán biztonságtudatosság növelése jelenik meg célként a kutatás végrehajtása és elemzése során megállapított következtetések segítségével, hanem úgy gondolom, érdemes felmérni, hogy egy kifejezetten erre szakosodott felsőoktatásban résztvevő csoport hogyan vélekedik az adat- és információbiztonság kérdéseiről, milyen ismeretekkel rendelkezik elméletben, mit használ a gyakorlatban, s a kettő között milyen összefüggések vannak – tekintettel az adatvédelmi paradoxonra. Amennyiben a vizsgált csoport alulteljesít, úgy értékelhető visszajelzést kaphatunk arról, hogy a tudatosítás útjában milyen akadályok állhatnak, miért nem lehet annyira sikeres, mint azt elvárnánk. Választ kaphatunk arra is, vajon létezik az adatvédelmi paradoxon? Az elméleti tudásból nem következik annak gyakorlati kamatoztatása? Feleslegesnek ítéltető a tudatosításra tett megannyi próbálkozás? Számos további kérdés vár megválaszolásra, azonban amennyiben a csoport jól teljesít, úgy arról tehet a felmérés tanúbizonyságot, hogy a biztonságtudatosság jegyében történő oktatás működőképes lehet, érdemes rá pénzt, embert, időt és energiát szánni, mert lesz előttünk egy példa, hogy milyen az, amikor sikerült, milyen egy biztonságtudatos felhasználó, látni fogjuk, hogyan védi az adatait, s

mindebből további következtetéseket tudunk levonni arra vonatkozóan, milyen jövő vár ezekkel a programokra, mi működik, mi nem, mely módszerek sikeresek, esetleg mely témaköröket lehetne hangsúlyosabban megpróbálni átadni. Elengedhetetlen továbbá, hogy kiszűrjük, melyek azok a főbb pontok, rések, ahol hiányosság körvonalazódik. Ezeket a tapasztalatokat jogszabályokkal (például az SCA²) kombinálva, valamint technológiai megoldásokkal (példánál maradva: banki applikációk) jó eséllyel csökkenthető lenne a kibertámadások, ezen belül is a kiemelt jelentőségű adatlopások sikerességének aránya.

Célkitűzések megfogalmazása

Az adatbiztonság az egyik legnagyobb „sláger” témája a 21. századnak. A felhasználók okítására számtalan program született, temérdek tudatosító témával foglalkozó céget alapítottak. A jogalkotók is egyre nagyobb hangsúlyt fektetnek a vonatkozó jogszabályok kidolgozására, a joghézagok csökkentésére, továbbá a munkáltatók is egyre komolyabb figyelmet szentelnek a kérdésnek. Sajnos azonban a biztonságtudatosság kialakítására irányuló törekvések még mindig nem érik el a töredékét sem annak, amit ideálisnak nevezhetnénk. Sem színvonalban, sem lefedettségben. A dolgozat célja kettős: az egyik a további tudatosítás, különös hangsúllyal a social engineering támadásokra, azok felismerésére és elhárítási lehetőségeire. Ugyancsak célja emellett, hogy felmérje, ezeknek a programoknak van-e a gyakorlatban haszna. Jelen dolgozatomban megvizsgálom egy konkrét felhasználói csoport körében, képesek voltak-e túlnyomó részt elsajátítani az adatbiztonság elméletét, majd összevetem a kapott eredményeket azzal, gyakorlatban használják-e a megszerzett tudást a mindennapokban, képesek-e a tudásukat kamatoztatni. Összehasonlítom továbbá azzal a felvetéssel, hogy létezik-e az adatvédelmi paradoxon, s ha igen, akkor milyen okok lehetnek a háttérben, s ezen okok hogyan lehetnének kezelhetőek, hogy kiküszöbölésük esetén felhasználók biztonságtudatosságát minél magasabb szinten kialakíthassuk.

² Strong Customer Authentication – erős ügyfél-hitelesítés, az EU PSD2 (Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC) irányelv alapján 2021-től a bankok egy második hitelesítést is kérnek a fizetések során, ezzel védve ügyfeleiket a visszaélésektől.

Hipotézisek

Mint említettem, a hipotéziseim az adatvédelmi paradoxon köré fognak csoportosulni, céljuk annak megcáfolása egy konkrét felhasználói csoportban.

H1. Az hogy az adatvédelmi paradoxon nem releváns egy kiberbiztonsági képzés hallgatói körében.

H2. A hallgatók mind a digitális, mind a valós világban alkalmazzák az adatbiztonsági, információbiztonsági intézkedéseket.

Kutatásmódszertan

Kutatásom első része a rendelkezésre álló szakirodalom átvizsgálása és összegzése. Ezután saját kísérletet végzek az adatvédelmi paradoxon cáfolására a célcsoport tekintetében. Ezt először mind elméletet, mind ellenőrző kérdésekkel gyakorlatot tartalmazó kérdőívvel teszem meg, majd ezután kettő adathalász szimulációval fogom ugyanazt a csoportot felmérni. Amint minden információ rendelkezésemre áll, összegzem az eredményt.

Dolgozat gyakorlati alkalmazásának lehetséges esetei

Dolgozatom elméleti felvezetése, különösen a social engineering támadási technikák felismerése és elhárítása alkalmas lehet a jelenlegi tudatosítási anyag bővítésére, vagy új létrehozására. A dolgozat kísérlet része pedig egy közvetlen visszajelzést ad egy Magyarországon működő kiberbiztonsági felsőoktatási képzés sikerességéről, a képzés során elsajátított ismeretanyag minőségéről. Továbbá ideális esetben rávilágít arra, hogy az adatvédelmi paradoxon nem egy univerzális igazság, létezik biztonság tudatos felhasználó, ha megfelelő képzést kap. Így jelen dolgozat megerősítése is lehetne a tudatossági programok hasznosságának és szükségességének.

1. – BEVEZETÉS AZ ADATVÉDELEM ALAPVETŐ FOGALMAIBA

Az adatvédelmi paradoxon teljeskörű megértéséhez elengedhetetlen a téma fogalomtárával megismerkedni. Úgy gondolom, mint minden biztonsági kérdést, ezt a problémakört is a *biztonság* fogalmával érdemes kezdeni. Már ezen a ponton nehézségbe is ütközünk, ugyanis nincsen egy, általánosan elfogadott definíció. Heinz Gärtner Nemzetközi Biztonság A-tól Z-ig c. lexikonjában például tizennyolc féle értelmezés található³, s magabiztosan kijelenthető, hogy azóta ez a szám a hazai és nemzetközi szakirodalomban, a téma komplexitásának köszönhetően exponenciálisan nőtt. Abban a gondolkodók egyetértenek, hogy a latin „securus” szóból (sine = nélkül, cura = aggodalom, félelem) származik⁴. Számtalan aspektusa számtalan különböző nézőpontból közelíti meg a fogalommeghatározást. Ami szerintem a legközelebb áll az általam ismertetni kívánt témához, így hangzik: a fenyegetettség hiányaként értelmezhető, hiszen a biztonság nem értelmezhető a fenyegetés, fenyegetettség fogalma nélkül. Azért gondolom ezt az egyik legpontosabbnak, mert úgy gondolom, nem akkor vagyunk biztonságban, ha nem történik semmi, hanem akkor, ha fel vagyunk készülve a veszélyhelyzetekre. Egy másik tökéletesen ide illő definíció inkább kockázatelemzési szempontból közelíti meg a kérdést, mely szerint „*a biztonság a rendszer olyan – az érintett számára kielégítő – állapota, amelyben zárt, teljes körű, folytonos és kockázatokkal arányos védelem valósul meg*”⁵. A biztonság tehát olyan állapot, amelyben a biztonság alanya a lehetséges fenyegető hatások ellen a megkívánt mértékben védett. Ilyen szituációkkal pedig bármikor találkozhatunk, tekintettel arra, hogy a 21. században az „*adat az új olaj*”.⁶ Magánszemély számára a biztonság leginkább azt jelentheti, hogy sem a fizikai, sem a kibertérben nem éri támadás, pontosabban az alkalmazott védelmi megoldásokon nem tud átjutni a támadó. Így adatait biztonságban tudhatja, nem kerülnek jogosulatlan személyek kezébe.

Az előző definíció leírásában különbséget tettünk biztonság és védelem között. A *védelem* az a tevékenység, vagy tevékenységek sorozata, amely arra irányul, hogy megteremtse, fejlessze, vagy szinten tartsa azt az állapotot, amit biztonságnak nevezünk. A különbség közöttük tehát, hogy a

³ Gazdag Ferenc – Tóth Péter: A biztonságot veszélyeztető tényezőkről I. Nemzet és Biztonság, 1, 2008, 3. o.

⁴ Gazdag Ferenc – Tóth Péter: A biztonság fogalmának határaitól. Nemzet és Biztonság, 1, 2008, 3. o.

⁵ Muha Lajos – Krasznay Csaba: Az elektronikus információsrendszerek biztonságáról vezetőknél, NKE, Budapest, 2018, 13. o.

⁶ A 20. században az olaj volt az az olyan tempóban növekedésnek induló bevételi forrás, mint ami ma az adat. A legnagyobb óriásvállalatok majdnem mindegyikének bevételi forrásait nagyobbik részben az adat garantálja.

<https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>
(Megtekintés: 2021. 10.10.)

biztonság egy állapot, a védelem pedig az erre irányuló tevékenység, tevékenységek összessége. Azaz a biztonság megmutatja, hogy hogyan is védekezünk, milyen aktív és passzív megoldásokat választunk, hogy megvédjük magunkat és adatainkat.

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) konkrét definíciókkal segíti a téma megértését, mélyebb vizsgálatát. A biztonság definíciója után érdemes azt a fogalomkört átgondolni, amely miatt a fenyegetettségünk lényegében folytonosnak tekinthető: az *adat*. Az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas.⁷

Ezen belül a szükséges megemlíteni a *személyes adatot*, ami a GDPR⁸ értelmében: *„azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható”*⁹.

Különleges adat az előzőekhez képest annnyival több, hogy egy alcsoportja a személyes adatnak, érzékenyebb részeit tartalmazza. A könnyű összehasonlítás érdekében ismét a GDPR-ból idéznék: *„a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok”*¹⁰. A példákból tökéletesen látszódik, hogy ezeket az adatokat különös figyelemmel védenünk kell, vagy kellene, ugyanis ha egy esetleges támadó megszerzi ezeket, kis túlzással a kár mértéke csak a kreativitására van bízva.

⁷ Ibtv. 1. §

⁸ GDPR: General Data Protection Regulation, az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet).

⁹ GDPR 4. cikk

¹⁰ Uo. 9. cikk

Mindenképpen szükséges kiemelni az információ fogalmát, ugyanis az adat és az információ nem ugyanazt a fogalmat jelöli. Egy véleményem szerint rövid, de nagyon pontos definíció szerint az *információ* egy új ismeretté értelmezett adat.¹¹ E meghatározás feltételez közöttük egy halmaz-részhalmaz összefüggést, ahol az adat a tömérdek impulzust jelöli, melyek közül a jelentéssel felruházottakat információnak hívjuk. A kettő közötti különbség tisztázása azért is hasznos már az elején, mert későbbi értelmezés során is adódhatnak eltérések; a szakzsargonban a legkivételesebb esetekben felcserélhetőek.

Az előzőekből logikus, hogy a következő, amit értelmezni szükséges, nem más, mint az információbiztonság, az adatbiztonság, az információ-, és az adatvédelem fogalmak, valamint a közöttük levő különbségek és összefüggések. Az *információbiztonság* azt a folyamatot jelöli, melynek során az információkat megvédjük a nem engedélyezett hozzáféréstől, használattól, kiszivárgástól, megsemmisítéstől, módosítástól, és megzavarástól.¹² Az *adatbiztonság* az adatok jogosulatlan megszerzése, módosítása és megsemmisítése elleni műszaki és szervezési megoldások rendszere.¹³ Az *adatvédelem* a személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége.¹⁴ Az *információvédelem* pedig az információk bizalmasságának, sértetlenségének és rendelkezésre állásának védelme.¹⁵

A fent tárgyalt fogalommeghatározásokból néhány részletet érdemes külön kiemelni, mert magyarázatra szorulnak. Ilyen a bizalmasság, sértetlenség, rendelkezésre állás, ahogy az angol terminológia nevezi: CIA-hármas¹⁶, az információvédelem alapkövei. Nézzük tehát őket sorban, segítségül hívva az ISO 27000-es sorozat¹⁷ ISO/IEC 27001-es szabványát.¹⁸ A *bizalmasság* jelentése, hogy az információ csak annak a felhasználónak érhető el, akinek van hozzá jogosultsága, s csak a megfelelő jogosultsági szinten. Jellemzően ez a hozzáférés az adat gazdájától eredeztethető,

¹¹ Claude E. Shannon - Warren Weaver: A kommunikáció matematikai elmélete. Az információelmélet születése és távlatai. 1949. Budapest, 1986.

¹² László Gábor: Kockázateértékelés, kockázatmenedzsment, 2014. 4. o.

¹³ <https://www.naih.hu/adatvedelmi-szotar> (Megtekintés: 2021. 10. 22.)

¹⁴ Uo.

¹⁵ Muha Lajos - Krasznay Csaba: Az elektronikus információs rendszerek biztonságának menedzselése, NKE, Budapest, 2014. 117. o.

¹⁶ Confidentiality, Integrity, Availability – bizalmasság, sértetlenség és rendelkezésre állás

¹⁷ International Organization for Standardization (Nemzetközi Szabványügyi Szervezet) információbiztonság és annak menedzselése témakörének fenntartott szabványcsalád

¹⁸ ISO/IEC: ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements Geneva, Switzerland: ISO/IEC, 2013.

vagy olyan egyéb személytől, aki már kapott olyan szintű engedélyt, hogy hozzáférést oszthasson tovább. A sértetlenség attribútum arról szól, hogy a tárolt információ pontos és teljes, forrása, tartalma és tulajdonságai az elvárttal megegyeznek. Illetéktelen módosítás nem történik, sem tudtunk, sem hozzájárulásunk nélkül. A *rendelkezésre állás* annak biztosítása, hogy a hozzáférésre jogosult személyek elérjék az információt akkor, amikor szükségük van rá, a szükséges időtartamra.

A biztonság elemzése közben is számos olyan kifejezést használtam, ami további kifejtésre szorul, őket az Ibtv. tömören és lényegre törően kifejti. A *zárt* jelző a kontextusban, a védelemre vonatkozik, mivel a számításba vehető összes fenyegetést figyelembe veszi, a *teljes körű* minden elemre kiterjed, a *folytonos* időben megszakítás nélkül történik, a *kockázatokkal arányos* védelem pedig hozzámérhetővé teszi a védelem költségeit a potenciálisan okozható károk mértékével.¹⁹ Tökéletes biztonság nincsen, tudatos döntések lehet meghatározni, hogy mit szeretnénk védeni és milyen szinten. Ugyanis a világ összes pénzét rá lehet szánni biztonsági megoldásokra, de nem biztos, hogy érdemes. Fontos, hogy a védelem kialakítása során az „arany középutat” célszerű szem előtt tartani.

A fogalomtár következő eleme a *kibertér*. Definíció tekintetében nehéz egyértelműen állást foglalni, ugyanis számtalan különböző megfogalmazás létezik a különböző álláspontok alapján. Ami legtöbbször közös bennük, az 4 aspektus említése. Az első a hálózat, vagy hálózatok hálózata, ami a kibertér alapja. A második, az adat, vagy információ tárolása, feldolgozása, hozzáférése, továbbítása, vagy cseréje, megosztása. A harmadik, az ember-számítógép interakció, mesterségesség. Végül pedig az idő.²⁰ Lényegében minden „kütyü”, ami kapcsolódik a hálózathoz, így például egy telefon, okosóra, laptop, nyomtató, akármilyen IoT²¹ eszköz, mind része a kibertérnek. Mivel a csatlakozott eszközök száma rohamosan nő, főleg az említett IoT-nek és az 5G-nek köszönhetően, egyre több személy egyre jobban érintett a kibertér mindennapos használatában, valamint a kibertérből érkező fenyegetésekben egyaránt, így tudatosításuk elengedhetetlenül fontos, ugyanis a támadások módszere is folyton változik, tolódik át a kibertérbe.

¹⁹ Ibtv. 1. §

²⁰ H. Ning, X. Ye, M. A. Bouras, D. Wei and M. Daneshmand,: General Cyberspace: Cyberspace and Cyber-Enabled Spaces, IEEE Internet of Things Journal, 5. kötet, 3. szám, 2018, 1844-1845. o.

²¹ Internet of Things – Dolgok internete: minden olyan eszköz, amiben vannak érzékelők, van feldolgozási képessége, szoftvere, vagy egyéb technológiát tartalmaz, ami csatlakozik és adatot vált, kommunikál a többi eszközzel hálózaton, vagy az interneten keresztül. Nem számítógépek, telefonok, hanem számtalan egyéb, például autók, okosothon eszközök, stb.

A kibertérből következik természetesen a kiberbiztonság és a kibervédelem fogalmának ismertetése. A kiberbiztonság fogalmát úgy gondolom, legjobban egy olyan definícióval lehetne összefoglalni, amely a legtöbb közismert álláspontot magában foglalja, mindegyikből kiemelve a közös, vagy egyedi, ugyanakkor fontos elemeket. Ennek megfelelően tehát a *kiberbiztonság* olyan erőforrások, folyamatok és struktúrák szerveződése, gyűjteménye, amelyek a kibertér és a kibertér-kompatibilis rendszerek védelmére szolgálnak az olyan eseményektől, amelyek tényleges tulajdonjoga – akár szándékosan, akár véletlenül – eltér a vélt tulajdonjogtól.²² A *kibervédelem* pedig egy tevékenység, amely megelőzésre épül, s védelmi intézkedéseket foglal magában. Célja a kibertér fenyegetéseinek, kockázatainak kezelése, valamint az ehhez szükséges eszköztár fejlesztése.²³

A tudatossághoz szorosan kapcsolódik az is, hogy magunkról milyen információkat osztunk meg az interneten, mi elérhető a nyilvánosság számára. Ugyanis a támadó sikerrátáját nagyban növelni tudja, ha a támadás előtt nyomoz, információt szerez annak érdekében, hogy a lehető legnagyobb hatásfokkal személyre szabhassa a tervét. Ez a nyomozás többféle módszerrel történhet, viszont amire a legnagyobb hatásunk van, vagy lehetne, az pontosan a mindenki számára elérhető információk kontrollálása, minimalizálása. Ezek megszerzésére irányuló technikát a szaknyelv *OSINT*-nak – open-source intelligence – nyílt forrású hírszerzésnek nevezi.²⁴ A nyílt forrású információszerzés során nyílt adatforrásból elérhető információk megszerzése a cél. Ilyen adatforrás lehet például az internet, rádió- és televízióadás, újság, könyv, stb. Minden, amit alapvetően bárki megtalálhat. Az Információs Hivatal a következőképpen fogalmaz: „*A nyílt forrású információk a bárki számára hozzáférhető, nyilvános és legális eszközökkel megszerezhető információk, melyeknek forrásai az elektronikus média, az írott sajtó, az internetes oldalak, az ingyenes és kereskedelmi adatbázisok lehetnek. Ezek szisztematikus gyűjtése és feldolgozása révén hírszerzési szempontból releváns információk keletkeznek.*”²⁵ Amiért kiemelt fontosságú beszélni róla az az, hogy miközben a felderítési módszerek közül statisztikailag az információk 80%-át nyílt forrású hírszerzés adja, addig a felderítési költségek kevesebb, mint 5%-át teszi ki az erre fordított

²² Craigen, D., Diakun-Thibault, N., & Purse, R.: Defining cybersecurity, Technology Innovation Management Review, 4. szám, 2014, 13-17. o.

²³ 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

²⁴ <http://www.mkih.hu/a-hirszerzes-forrasai.html> (Megtekintés: 2021.11.12.)

²⁵ Uo.

keret.²⁶ Így ez nem csak a hivatalos szerveknek optimális választás, hanem bárkinek, aki információt szeretne szerezni, így a támadónak is. Kiemelt fontosságát az előbb említett Információs Hivatal is megerősíti, rögtön a hivatalos weboldaluk „Hírszerzés forrásai” aloldaluk bevezető bekezdésében: „A hírszerzés alapvető feladata a más állami szervek eszközszerével nem hozzáférhető titkos és bizalmas információk megszerzése; ennek érdekében humán és technikai forrásokat létesít. Azonban egyetlen modern nemzetbiztonsági szolgálat sem mondhat le a nyílt forrású információk szisztematikus feldolgozásában és a nemzetközi együttműködésben rejlő lehetőségekről.”²⁷

Végül, de nem utolsó sorban adatbiztonság tekintetében ismertetném az *információs önrendelkezés jogát*. Az Info tv.²⁸ kifejti, hogy az egyénnek lehetősége van arra, hogy befolyásolja, vele kapcsolatban ki, milyen adatot kezelhet, s ezek a szabályozások egyértelműen definiáltak a hazai jogszabályban.²⁹

2. – SOCIAL ENGINEERING

Elérkeztünk a dolgozat szempontjából az egyik legizgalmasabb kérdéskörhöz, a „social engineering”-hez. Egyes becslések addig a szélsőségig is elmennek, hogy minden kibertámadás 99%-a social engineering módszereken alapszik.³⁰ A mérési módszertől függetlenül az egyértelműen kijelenthető, hogy 2021-ben bekövetkezett kibertámadások esetén megállapítható, hogy a leggyakrabban az ember a leggyengébb láncszem, így ilyen tekintetben logikus, hogy a legtöbb támadás ezt a tényezőt célozza. De mindemellett ugyancsak az ember az az eleme egy szervezetnek, ami az IT eszközökhöz, valamint adatokhoz keletkezésükől, megsemmisítésükig a teljes cikluson keresztül hozzáfér, ahogy a 2. számú ábra is mutatja: az összes ponton lehetséges emberi beavatkozás, amiből következik, hogy léteznek hozzáférések. Így az adat teljes életciklusában ki vagyunk téve social engineering támadásoknak.. Mindez számunkra azért kifejezetten fontos, mert kivétel nélkül minden felhasználói típusra vonatkozóan kell a tudatosítási

²⁶ Dr. Izsa Jenő: Nemzetbiztonsági alapismeretek (A titkosszolgálatok működése), Egyetemi jegyzet, Budapest, 2009. 66. o.

²⁷ <http://www.mkih.hu/a-hirszerzes-forrasai.html> (Megtekintés: 2021.11.12.)

²⁸ 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, majd GDPR-ral való összehangolás érdekében módosítva: 2018. évi XXXVIII. törvény az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek az Európai Unió adatvédelmi reformjával összefüggő módosításáról, valamint más kapcsolódó törvények módosításáról

²⁹ Info tv.

³⁰ <https://www.itgovernance.co.uk/social-engineering-attacks> (Megtekintés ideje: 2021.11.14.)

programokat megtervezni, kialakítani, s végrehajtani, ugyanis aki adatot kezel, könnyedén áldozat lehet.



2. ábra: Adat-életciklus modell (Saját szerkesztés)

2.1 – A social engineering sajátossága

Magyar megfelelőjét a mai napig nem sikerült meghatározni – minden próbálkozás, ami egy konkrét, az eredeti angol szókapcsolatnak megfelelő szakkifejezés létrehozására irányul, kudarcba fullad, ugyanis semmi sem tudja azt a számtalan szempontot és sajátosságot visszaadni, amit maga a támadási technika magában hordoz, így jelen dolgozatban én is az angol terminológiát fogom használni.. A biztonság legfontosabb összetevője az ember. Lehet jogszabályokat alkotni, lehet eszköz, vagy technológiai alapon próbálni megakadályozni a támadást, de amíg az emberi tényező által okozott fenyegetés nincs kizárva – márpedig például saját adataim kontextusában ez lehetetlen – addig foglalkozni kell azzal, hogy milyen támadások érhetik a felhasználót és hogyan lehet őket megelőzni, elhárítani. A social engineering pontosan az emberi tényezőt igyekszik kihasználni, gyengeségeinket – leggyakrabban a hiszékenységet – felhasználni a sikeresség érdekében. A téma kifejtésekor megkerülhetetlen idézni Kevin D. Mitnicket: „*A social engineering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer –technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni.*”³¹ A

³¹ Mitnick, K. D. - Simon, W. L.: A legendás hacker – A megtévesztés művészete, Budapest, 2003.

támadási forma elsődleges célja a támadó számára szükséges információk amely lehet többek között – a teljesség igénye nélkül – munkahelyi, vagy magánéletben használt jelszó, bankkártya adat, születési hely, idő, szervezet életére vonatkozó bizalmas információ. Gondolhatunk akár egy megszemélyesítésre, például a banki jóváhagyó SMS-hez tartozó telefonszámot vagy egy 5 jegyű számsor segítségével, vagy néhány születéshez köthető adattal tudjuk megváltoztatni, mindezt telefonon. Felelőtlen felhasználótól sem az 5 jegyű számsor, sem pedig a születési hely és idő nem egy nehezen megszerezhető adat, s mindezt úgy, hogy mi adjuk lényegében oda neki. Az Alkotmányvédelmi Hivatal 'Awareness' nevű programjában a következő top 10 hibát említik, amit a felhasználók jellemzően elkövetnek – a ritkábbtól a leggyakoribbig: nyilvános Wi-Fi használata, privát videóhívás nyilvános helyen, helyadat megadása appon keresztül, tartózkodási hely felelőtlen megosztása, kompromittáló szituáció, hivatalos információk megosztása, könnyen kitalálható jelszó, őrizetlenül hagyott adathordozó eszközök, könnyen feltörhető számkombináció, személyes tartalmak nyilvános megosztása.³² A felsorolás véleményem szerint jól alátámasztja azt, hogy mennyire figyelmetlen, naív a felhasználó, s gyakorlatilag tálcán kínálja az adatait bárkinek, célkeresztet festve önmagára, amin az áll: itt támadjatok. A különböző social engineering módszerekben közös, hogy a tradicionális, nem kibertérben elkövetettek adatkinyerésekhez képest egyre szofisztikáltabbak, könnyebben megvalósíthatóak, gyorsabban több információt szolgáltatnak.³³ A dolgozatnak nem célja, hogy az összes különböző technikát részleteiben kifejtse, különös tekintettel arra, hogy számuk, a támadók kreativitásának függvényében napról-napra nő, jelen dolgozat kizárólag a népszerűbbeket, valamint a kérdőívben, kísérletben szereplőket hivatott ismertetni.

2.2 – Social engineering támadási metodikája

Mint minden támadási technika, egy social engineering támadás is akkor igazán sikeres, ha egy előre alaposan felépített stratégia mentén alkalmazzák, ezzel is minimalizálva a szükséges rögtönzést, a támadás idejét, a lebukás veszélyét, ezek által maximalizálva a siker valószínűségét.

³² <https://ah.gov.hu/awareness-program/> (Megtekintés: 2021. 11. 14.)

³³ Aldawood, H., Alashoor, T., & Skinner, G.: Does awareness of social engineering make employees more secure?. International Journal of Computer Applications, 177(38), 2020, 45-49. o.

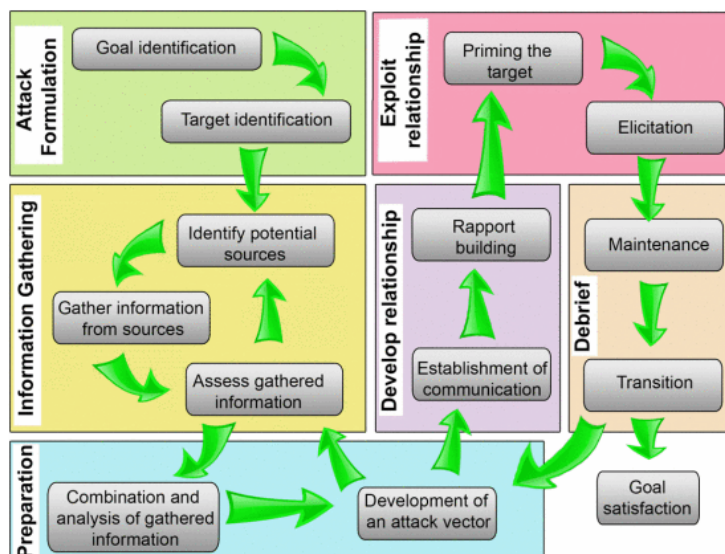
Ezt a keretrendszert Mitnick munkássága alapján, azt kibővítve szeretném bemutatni, amelyet a következő, 3. számú ábra is szemléltet.³⁴

- Ennek a metodikának az első nagyobb eleme a támadás megfogalmazása. Pontosan mit szeretne elérni a támadó? Ezen belül a legelső lépés a cél, célok definiálása. Ezután következik a célpont, célpontok beazonosítása.
- Majd miután mindkét kiinduló pontot átgondolta a támadó, jöhet az információgyűjtés. Ez jellemzően OSINT módszerekkel történik, melybe akár a terepszemle is beletartozhat. Ennek a pontnak az első eleme a lehetséges források azonosítása. Az azonosított forrásokból ezután információt nyerünk ki. Az információszerzés alanyai közé sorolható minden, ami kapcsolódik a céljainkhoz, célpontjainkhoz. Mikor a megszerzett információ a rendelkezésünkre áll, akkor jön el az idő azokat kiértékelni: mi az, ami hasznos, mi az, ami felesleges. Amennyiben szükséges, ez a ciklus újraindul, további források felkutatásával.
- Ha az eddig összegyűjtött információhalmaz tartalmilag is megfelelő, jöhet a következő lépés, az előkészület. Az összegyűjtött információkat egyeztetik és elemzik, belőlük kiindulva kialakítanak egy, vagy több támadási vektort, amelynek tartalmaznia kell a célt, a célpontot, a közeget, a támadási technikát, s természetesen a social engineert.
- Ezután következik a kapcsolat kialakítása, mely először a kommunikációs csatorna létrehozásával kezdődik, majd folytatódik a célponttal történő megfelelő, jellemzően barátságos viszony, a bizalom felépítése.
- Ha ezt sikerült végrehajtani, a következő feladatunk a célpont felkészítése arra, hogy átadja az információt. Ez különféle manipulációs technikákkal történhet, attól függően, milyen támadási módszer kerül alkalmazásra. A manipuláció alapjául szolgálhat például egy érzelmi állapot, mint a boldogság, vagy szomorúság, de a befolyás során lehet sürgetéssel, vagy segítség kérésével dolgozni. Amint ez az állapot bekövetkezett, elkezdődhet az információ kinyerése, például a kívánt jelszó megszerzése.
- A potenciálisan utolsó teendő az összegzés, zárás. Ennek egyik része, hogy a célpontot olyan állapotban hagyjuk ott, hogy ne sejtse, hogy megtámadták, például visszabillentve abba az állapotba, amilyenben a manipulációs tevékenység előtt volt. Ezután már csak el kell dönteni, hogy sikerrel zárult-e a social engineering tevékenység, a szükséges információ rendelkezésre áll-

³⁴ F. Mouton, M. M. Malan, L. Leenen and H. S. Venter, "Social engineering attack framework," 2014 Information Security for South Africa, 2014, 1-9. o.

e. Amennyiben a válasz nem, úgy új támadási vektor létrehozása lehet szükséges, esetleg az információszerző ciklus újratekintése.

- Amennyiben viszont a válasz igen, a szükséges információt sikerült megszerezni, úgy a támadást siker zárja.



3. ábra: Social engineering támadási keretrendszer³⁵

2.3 – Módszerek csoportosítása

A témát feldolgozó számtalan szakirodalom tanulmányozása közben azt a közös nevezőt véltem felfedezni, hogy legtöbbször egyetértenek azzal, hogy két fő csoportra érdemes osztani a social engineering tevékenységeket. Ez a szempont pedig a támadási vektorokat veszi alapul: az utat, amin keresztül a social engineer hozzáférést szerez az adatokhoz, kihasználja a sérülékenységeket – beleértve az emberi tényezőt is.³⁶

2.3.1 – Emberközpontú megközelítés

A csoportosítás első eleme az emberközpontú megközelítés. Az bennük a közös, hogy az interakció ember és ember között, támadó és áldozat között történik, hogy technikai tudás nélkül is kivitelezhetőek, kifejezetten az embert tekintik leggyengébb láncszemnek, s használják ki sérülékenységeinket. Visszatérő elem közöttük még az, hogy a támadónak gyakran fizikailag jelen

³⁵ Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. (2014, August). Social engineering attack framework. In 2014 Information Security for South Africa (pp. 1-9). IEEE.

³⁶ Breda, F., Barbosa, H., & Morais, T.: Social engineering and cyber security, International Technology, Education and Development Conference, 3/3 szám, 2017, 106-108. o.

kell lennie, hogy véghez vigye tervét, s adatot, információt nyerjen.³⁷ A következőkben néhány, az ezen csoportba sorolható támadási technika kerül bemutatásra.

A *szoros követés* (tailgating) az a fajta támadási módszer, ahol egy konkrét épületbe való bejutás a cél. Gyakorlatilag besurranás, egy jogosultsággal rendelkező személy, vagy személyek csoportja mögött, között. Arra épít, hogy az alkalmazottak úgy sem ismerik teljeskörűen egymást, vagy ha igen, akkor sem jellemző, hogy ahelyett, hogy nyitva tartanák az ajtót egy „kollégának”, inkább rácsukják, hogy majd úgymint kinyitja a saját belépőkártyájával. Ezt kihasználva a támadó be tud jutni az épületbe, hogy végrehajtsa az eltervezett tevékenységét.³⁸ A széleskörben elterjedt dohányzási szabályozások kiváló táptalajt nyújtanak ennek a megoldásnak, ugyanis a zárt terekben való dohányzás tiltásának következtében az erre kiszemelt helyszín gyakran az épület előtt található, ahova még belépőkártya nélküli személyeknek is van hozzáférése.

Az *identitáslopás* (impersonation) alapvető gondolata, hogy a támadók egy valós, vagy kitalált személy bőrébe bújva tévesztik meg a többi alkalmazottat, vagy célpontjukat. A csel alapja, hogy a legtöbb alkalmazott általában nem ismeri ezeket a személyeket. Kellék lehet hozzá egy álruha, mely segítségével hitelesen eljátszható a rendszergazda, takarító, futár, karbantartó, vagy akár egy hivatásos egyenruhás szerepe. De előfordulhat, hogy a támadó az adott (nagy) vállalatnál egy alkalmazott bőrébe bújik, mivel ott nem ismer mindenki mindenkit, de ha ugyanott dolgozik, könnyebben adhat át a gyanútlan ott dolgozó olyan információkat, amiket adott esetben egy külsősnek nem, ugyanis a közös szervezet bizalmat teremt. Ugyanígy sikeres lehet, ha a választott szerep egy új alkalmazott, ugyanis a segítségkérés/nyújtás egy komoly motivációs faktor lehet. Ezen kívül a támadó célja lehet egy fontos ember bőrébe bújás, például másik részleg vezetőjének, hatósági személynek, vagy akár egy auditornak megszemélyesítése, amely esetben az autoritás az extra szempont.³⁹ A korábban említett OSINT tevékenységekkel a hatásfok nagyban növelhető, ha például a támadó kifigyeli, milyen munkaruhája van a takarítónak, vagy futárt álcázva szerez egy pizzásdobozt, illetve kihallgatja, milyen rendszerekkel dolgoznak az alkalmazottak. Fontos, hogy a támadó a szakzsargont megfelelően használja, vagy tudjon válaszolni keresztkérdésekre. Hasznos

³⁷ Ivaturi, K., & Janczewski, L.: A taxonomy for social engineering attacks, International Conference on Information Resources Management, Centre for Information Technology, Organizations, and People, 2011, 1-12. o.

³⁸ Conteh, N. Y., & Schmick, P. J.: Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6(23), 2016, 32. o.

³⁹ Algarni, A., Xu, Y., & Chan, T.: Social engineering in social networking sites: the art of impersonation, 2014 IEEE International Conference on Services Computing, IEEE, 2014, 797-804. o.

lehet a támadó számára, ha utánajár a megszemélyesítés alanyának közösségi médián, vagy nyomozást végez LinkedIn-en, a potenciálisan talált információk tárháza bőséges, s mind-mind hitelesebbnek tűnteti fel az álcát. És abban egyetérthetünk, hogy a felsorolt példák közül egyik sem igazán komoly erőfeszítés.

A *váll szörfölés* (shoulder surfing) egy különleges esete az ember-központú megközelítésnek, ugyanis a célpontja az ember, de interakció a támadó és az áldozat között nem jön létre. Lehet a cél egy PIN kód megszerzése egy ATM-nél, hogy később, mikor a kártyát megszerzi a támadó, akkor egyből hozzáférhessen a pénzhez, vagy akár a korábban említett besurranás során egy alkalmazott mögé állva a social engineer egyszerűen csak leolvassa a jelszót, mikor a „kolléga” beírja, s ő csak pont arra járt. Kicsit szofisztikáltabb módszer lehet, ha rendszergazdának adja ki magát, s megkéri, hogy jelentkezzen ki-be a rendszerből (így viszont interakció jön létre a felek között). A közös bennük, hogy akár tudtával, akár nem, az áldozat mögött áll és észrevétlenül feljegyzi a jelszót, PIN kódot, egyéb szükséges információt, mikor épp beírja azt, s egyetlen visszatérő, lényeges eleme, hogy fizikailag közel kell kerülni a célponthoz.⁴⁰

Nagyon hasonlít az előző módszerhez a *hallgatózás* (eavesdropping). Ennél a támadási technikánál interakció ugyanúgy nem jön létre, a támadó ismételten csak „arra jár”, mikor a gyanútlan célpontok a folyosón, vagy munkaállomásuknál párbeszéd során olyan információkat ejtenek el, amik értékesek lehetnek.⁴¹

Szintén speciális eset a *kukabúvárkodás* (dumpster diving). Előzőekhez hasonlóan ember-ember közötti interakcióról nem lehet itt sem beszélni. Lényege a szemetes átvizsgálásában rejlik, s a támadás arra épít, hogy az adott cégnek nem teljeskörűen kielégítő az adatmegsemmisítési procedúrája. Így szimplán az alkalmazottak a hulladékok (jobb esetben 2021-ben már a papír-szelektívbe) közé dobhatnak olyan iratokat, amelyeken személyes, vagy akár különleges adatok szerepelnek. Rendkívül hatékony módszer, ugyanis az emberek jellemzően bele sem gondolnak

⁴⁰ Long, J. No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing, Syngress, 2011, 27-60. o.

⁴¹ Parthy, P. P., & Rajendran, G.: Identification and prevention of social engineering attacks on an enterprise, 2019 International Carnahan Conference on Security Technology (ICCST), IEEE, 2019, 1-5. o.

abba, hogy egy bankszámlarészletező, vagy orvosi lelet milyen információkat rejthet, s milyen könnyű velük visszaélni, nem is beszélve a jelszavas cetlikről.⁴²

2.3.2 – Szocio-technikai megközelítés

A második alcsoport pedig a szocio-technikai megközelítés. Különbség az előző csoporthoz képest, hogy technikai tudást is igényelnek ezek a támadások, végrehajtásukhoz valamilyen technológiai segítség is szükséges. Kedvező módszer olyan tekintetben, hogy személyes kontaktus nincs, ebből következően a lebukás veszélye is kisebb.

Az első és leghangsúlyosabb az *adathalászat*. Három különböző típusát emelném ki, a phishing-et, a smishing-et és a vishing-et. A *phishing* támadási technikához a hamis e-mailek és weboldalak tartoznak.⁴³ Egy példán keresztül remekül szemléltethető: elektronikus levélben elkérlik az adatainkat, vagy egy kifejezetten erre a célra létrehozott weboldalra irányítanak át, ahol ugyanez a lehetőség adott, meg kell adnunk azt, amit éppen kérnek, így például felhasználó nevünket, jelszavunkat, születési helyet, időt, bankkártya adatokat, de a lehetőségek tárháza szinte végtelen. A *smishing* ugyanezt a tevékenységet foglalja magában, csak az alapja nem e-mail, hanem SMS, ebből ered a neve is.⁴⁴ Az elmúlt időszakban a médiában több ilyenről lehetett hallani, ilyen volt például a 2021. márciusában keringő, csomagküldő szolgálatok nevében érkező SMS incidens.⁴⁵ Az sms-ben a támadó arról értesítette az áldozatokat, hogy csomagjuk érkezett, s a kattintható linken tudják letölteni a hozzá szükséges csomagkövető applikációt. Ezzel egy adathalász program települt a telefonra, ami hozzáfért a személyes adatokhoz, akár netbank-applikációkban tárolt információhoz is. Végül pedig a *vishing* (voice phishing) ezeknek egy kockázatosabb megoldása, ugyanis telefonon, hívásban érkezik.⁴⁶ Használhatósága azonban nem csekélyebb, ugyanis egy-két kulcsszót, nevet, titulust, szakszót megemlítve a dolog hitelesnek tűnhet, s az emberek hajlamosak megadni az adataikat.

⁴² Long, J. No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing, Syngress, 2011, 1-12. o.

⁴³ Yeboah-Boateng, E. O., & Amanor, P. M.: Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. Journal of Emerging Trends in Computing and Information Sciences, 5/4 szám, 2014, 299. o.

⁴⁴ Uo.

⁴⁵ <http://www.police.hu/hu/hirek-es-informaciok/bunmegelozes/aktualis/vigyazat-sms-ben-erkezhethet-a-kartekony-kod> (Megtekintés: 2021.11.11.)

⁴⁶ Yeboah-Boateng, E. O., & Amanor, P. M.: Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. Journal of Emerging Trends in Computing and Information Sciences, 5/4 szám, 2014, 300. o.

A következő módszer az úgynevezett *szétszórás* (baiting). Központi eleme egy adathordozó, amit „elhagy” a támadó a célhelyszínen, arra építve, hogy aki megtalálja, majd úgyis behelyezi egy informatikai eszközbe.⁴⁷ Ez az eszköz természetesen kártékony kódot tartalmaz, melyet ha szeretnének, leplezhetnek normál tartalmakkal, például (nem saját) fényképekkel, zenékkel, stb. A behelyezés pillanatában a kártékony kód lefut, s elvégzi, ami a feladata. Ismét csak a támadó kreativitására van bízva a kártékony program funkciója, így például ellophat személyes adatokat, végigfertőzheti a rendszert, vagy akár elkezdheti egy APT támadás előkészítését.

3. – ADATVÉDELMI PARADOXON

Azt természetesnek vesszük, nyílt titokként tartjuk számon, hogy a legtöbb vállalat, kezdve a cégóriásoktól, egészen a kisebb vállalkozásokig, mindenki adatot gyűjt. Bármit vásárlunk, a vásárlási szokásainkat elemzik, mind a kereskedésekben, üzletekben, mind a banki oldalon, bankkártya használat esetén.⁴⁸ De a közösségi média platformok elterjedése következtében ez az adathalmaz már azt is tartalmazza, amit leírunk, megosztunk magunkról, amelyekből összeállítják, mit gondolunk, következtetéseket vonnak le, profilokat hoznak létre, eltárolva egy szerveren. Ilyen elgondolások mentén jönnek létre például az egyén saját visszhangkamrái⁴⁹ is, amelyek annak érdekében, hogy maximalizálják az oldalon eltöltött időt, olyan tartalmat tesznek elénk, amit szívesen olvasunk (vagy legalábbis ami felett jellemzően időt töltünk), amit korábbi tevékenységeink alapján állítanak össze.⁵⁰

Fontos leszögezmem az első gondolatként, hogy az *adatvédelmi paradoxon* (privacy paradox) egy mai napig kutatott téma, ennek ellenére nincsen még egyértelmű konklúziója. Alapvetően arról szól, hogy létezik egy érdekes ellentét a felhasználói szokásokban. Vannak, akik jellemzően támogatják a biztonság tudatos döntéseket, üdvözlik az ezzel kapcsolatos pozitív híreket, szabályozásokat, önbevallásos alapon gyakran kifejezetten magas szintre helyezik a saját tudásukat, s ezzel kapcsolatban számukra a téma fontosságát. Ellenben a gyakorlat pedig azt mutatja, hogy

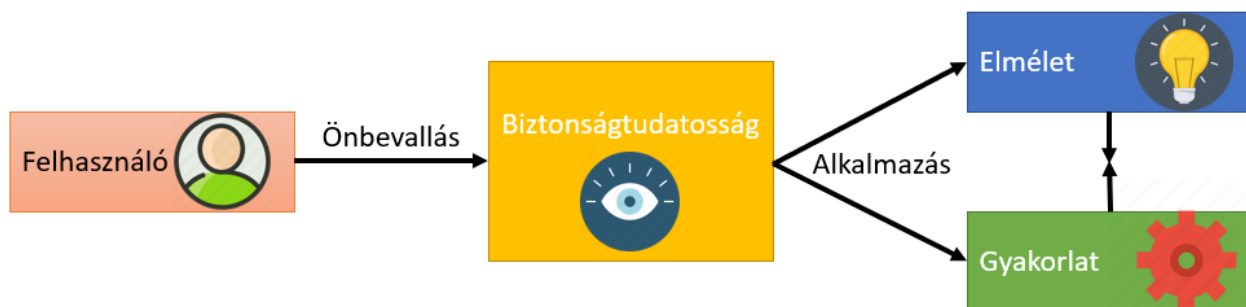
⁴⁷ Krombholz, K., Hobel, H., Huber, M., & Weippl, E.: Advanced social engineering attacks. Journal of Information Security and applications, 22, 2015, 115. o.

⁴⁸ Barnes, S. B.: A privacy paradox: Social networking in the United States. First Monday, 2006.

⁴⁹ Echo chambers: egy olyan saját „világa” egy felhasználónak, ahova hír és információ nem jut be kívülről, csak a „falak visszhangozzák” a saját látásmódját. Nem találkozik ellenvéleményekkel, nem alakul ki vita, nem bővül az ismeret.

⁵⁰ Cinelli, M., Morales, G. D. F., Galeazzi, A., Quattrociocchi, W., & Starnini, M.: The echo chamber effect on social media. Proceedings of the National Academy of Sciences, 118(9), 2021, 1-7. o.

ténylegesen viszont nem tesznek semmit ennek érdekében, vagy kifejezetten ezzel ellentétesen viselkednek.⁵¹



4. ábra: Adatvédelmi paradoxon (Forrás: saját szerkesztés)

2012-ben egy terepkísérlet során 2 teljesen ugyanolyan DVD árusító boltból kellett vásárolniuk az alanyoknak, egyetlen DVD-t. Az elsőben a vásárlásnál a fizetésükről és a születési adataikról kellett nyilatkozniuk, a másik bolt kizárólag a kedvenc színre és a születési évre kérdezett rá vásárlás előtt. Egyértelműen az első sokkal érzékenyebb információkat kért, hogy létrejöhessen a tranzakció. Amennyiben a két bolt ugyanolyan áron adta a szóban forgó DVD-t, ugyanolyan arányban vásároltak tőlük a tesztalanyok. Amikor az első bolt egyetlen euróval olcsóbban adta az árut, majdnem mindegyik résztvevő tőlük vásárolt, az adatvédelmi aggodalmaik ellenére. A kísérlet utáni kérdőívből a következő derült ki: 75%-uk azt jelezte, hogy erősen érdekeltek az adatvédelemben, 95%-uk pedig azt nyilatkozta, hogy érdekelte őket a saját személyes adataik védelme.⁵²

3.1 – Korai kutatások

2001-ben Barry Brown mélyinterjúkon keresztül azt az észrevételt fedezte fel, hogy az emberek, akik online vásárolnak, alapvetően óvatosnak vallják magukat, s csak akkor adják ki az adataikat, ha feltétlenül szükséges – amibe beletartoznak az akciók, kedvezmények, kuponok is. Ameddig a megkérdezettek kaptak valamit az adataikért cserébe, addig félre tudták tenni aggodalmaikat.

⁵¹ Kokolakis, S.: Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & security, 64, 2017, 122-134. o.

⁵² Beresford, A. R., Kübler, D., & Preibusch, S.: Unwillingness to pay for privacy: A field experiment. Economics letters, 117(1), 2012, 25-27. o.

Brown a kutatásai során már felfedezni vélt valamiféle adatvédelmi paradoxont a felhasználói szokásokban.⁵³

2006-ban, mikor a Facebook még „gyerekcipőben járt”, a Myspace volt a legnagyobb közösségi média platform, Susan B. Barnes az adatvédelmi paradoxon kapcsán azt írta: Alapvetően a felelőtlen tinédzsereket érinti, s az volt az aggodalom fő tárgya, hogy az információkat, amiket megosztanak magukról, – mivel nyilvánosak – egyéb célokra is felhasználhatják akik látják azokat és így például oktatási intézmények szűrhetik a nem kívánatos iskolán kívüli tevékenységeket.⁵⁴

2008-as kutatásában Stefanie Pötzsch tovább erősíti azt az álláspontot, hogy aggodalomra ad okot az eredeti célhoz képest az online megosztott tartalmak másodlagos, alternatív felhasználása. Viszont a tizenévesek, mint leginkább veszélyeztetett csoport már ebben a kutatásban nem szerepel, szerinte egy általános problémával állunk szemben. Feltételezhetnénk, hogy a biztonság tudatosság az emberek számára azt jelenti, hogy képesek informált döntést hozni az adataik kapcsán, ezáltal kevesebb adatvédelmi jellegű problémával rendelkeznek. Tovább folytatván ezt a feltételezést, logikusnak tűnik, hogy aki tudatos az adatbiztonság tekintetében és hangoztatja ennek fontosságát, az a személy ennek megfelelően is fog eljárni. A tapasztalatok alapján azonban ez általánosságban nem így történik.⁵⁵

3.2 – Összefüggések keresése – demográfiai és nem-demográfiai csoportosítások

2010-ben Mark Zuckerberg⁵⁶ úgy nyilatkozott, hogy az internethasználók már kényelmesebbé váltak azzal kapcsolatban, hogy magukról több információt, több emberrel osszanak meg; a magánélet többé nem társadalmi norma.⁵⁷ Természetesen ez egy elég szélsőséges kijelentés, s nem szabad megelégednünk arról, hogy a Facebook (ebben az időben) adatokkal kereskedett, célzott hirdetési célokkal, így érdeke volt, hogy a magánélet, biztonság fontosságát ilyen színben, „lejárta lemezként”, opcionálisként említse.⁵⁸ Ugyanis minél több adatot osztanak meg magukról a felhasználóik, annál pontosabban lehet őket marketing tekintetében behatárolni. S azt ne feledjük,

⁵³ Brown, B.: Studying the Internet Experience, Publishing Systems and Solutions Laboratory, HP, Bristol, 2001, 1-22. o.

⁵⁴ Barnes, S. B.: A privacy paradox: Social networking in the United States. First Monday, 2006.

⁵⁵ Pötzsch, S.: Privacy awareness: A means to solve the privacy paradox?. IFIP Summer School on the Future of Identity in the Information Society, Springer, Berlin, Heidelberg, 2008, 229. o.

⁵⁶ A Facebook egyik alapítója, ma a Meta vezérigazgatója.

⁵⁷ Johnson, B., & Vegas, L.: Privacy no longer a social norm, says Facebook founder, The Guardian, 2010.

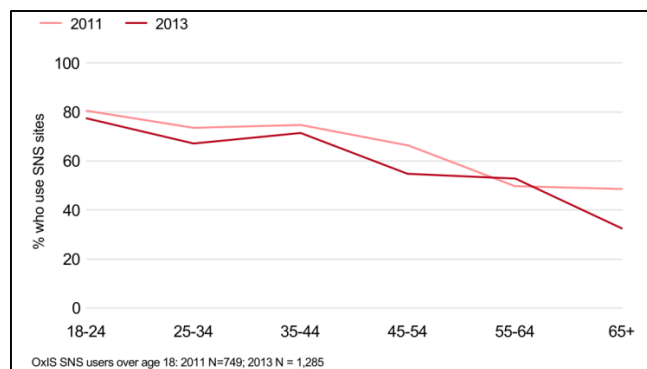
⁵⁸ Blank, G., Bolsover, G., & Dubois, E.: A new privacy paradox: Young people and privacy on social network sites., Prepared for the Annual Meeting of the American Sociological Association (Vol. 17), 2014, 1. o.

hogy a Facebook 2008-ban megelőzte a Myspace-t, ezzel minden idők legnagyobb közösségi média platformja lett.⁵⁹

Egy 2014-es kutatás ismét azt az összefüggést vizsgálja, hogy vajon az adatvédelmi paradoxon korfüggő-e? A fiatalok kevésbé tudatosak? A kutatás számos demográfiai szempont alapján összeszedett korábbi megfigyeléseket. Eltérő eredményeket tudott felmutatni annak tekintetében, hogy milyen szinten vannak a férfiak és milyenek a nők. Végrehajtásra került olyan kutatás, ahol volt számottevő eltérés és volt olyan is, ahol rendkívül csekély. A kutatás említést tesz arról, hogy az elméleti tudatossági szint az oktatással szoros kapcsolatban áll: alacsonyabban iskolázott személyek kevésbé jártasok a témában, magasan iskolázottak pedig jobban elsajátították azt. Anyagi szempont szerint a következtetés ismét nem egyértelmű, de volt olyan felmérés, ahol a tehetősebbek kevésbé voltak biztonságtudatosak, viszont ez a kutatás sem tért ki a tudatosság gyakorlati oldalára. Korosztályok tekintetében eltérőek az eredmények. Számos következtetés született annak tekintetében, hogy a kornak semmilyen szerepe nincsen az adatvédelmi szokások kialakulásában. Született azonban számos olyan mérés is, ahol a korábbi kutatásokat megcáfolták: az idősebb korosztály volt felelőtlenebb a megosztott tartalmaik terén, s a fiatal korosztály volt bizalmatlanabb, vagy tudatosabb. A kutatás azt az egyértelmű következtetést hozta, több alátámasztott szemszögből, hogy ellentétben a korábbi kutatások eredményeivel, a fiatalok sokkal biztonságtudatosabbak, a kornak egyértelmű szerepe van. Az alábbi 5. számú ábra szemlélteti a kutatás során felmért közösségi média felhasználók szokásait, hangsúlyozva hány százalékuk használja a biztonsági beállításokat, korosztályos megoszlásban.⁶⁰

⁵⁹ Hall, Mark. "Facebook". Encyclopedia Britannica, 2021, <https://www.britannica.com/topic/Facebook> (Megtekintés: 2021. 11. 12.)

⁶⁰ Blank, G., Bolsover, G., & Dubois, E.: A new privacy paradox: Young people and privacy on social network sites., Prepared for the Annual Meeting of the American Sociological Association (Vol. 17), 2014, 7-9. o.



5. ábra: Közösségi média felhasználók, akik változtatták az adatvédelmi beállításait, korosztály szerint⁶¹

Ugyanez a kutatás részletezi a nem-demográfiai jellegű szempontokat is. Személyiségjegyekkel kapcsolatos összefüggéseket véltek felfedezni: akinek népszerűsége van szüksége, vagy nárcisztikus, kevésbé foglalkoztatja az adatbiztonsága, többet oszt meg önmagáról, akinek pedig bizalmi, vagy önbizalmi problémái vannak, esetleg szorong, limitálja ezeket a megosztásokat. Informatikai tudás tekintetében arra a következtetésre jutottak, hogy összefüggés lehet az IT tudás és a biztonsági beállításokkal való „játszadozás” között, de ezek a kutatások nem teljesen alkalmasak egyértelmű eredménynek, ugyanis az önbevalláson alapuló számítógépes tudás szintjét gyakran az utókövető interjún nem tudták prezentálni. Korábbi rossz tapasztalatok és a bizsontágtudatosság közötti összefüggés nem jutott megcáfolhatatlan konklúzióra, bár a mintavételezés mérete ugyan kicsi volt, de így is arra enged következtetni, hogy akinek már korábban volt incidense, körültekintőbb lett utána.⁶²

3.3 – Lehetséges elméleti magyarázatok

A hazai és nemzetközi szakirodalom elemzését követően összegyűjtöttem a leggyakrabban előforduló lehetséges magyarázatokat.

3.3.1.- *Privacy calculus*

A privacy calculus-nak a social engineeringhez hasonlóan nincsen olyan magyar megfelelője, ami az eredeti jelentést teljes egészében visszaadja. A 'homo oeconomicus' elméleti koncepcióján alapszik. A gazdaságtudományban ez az elmélet arról szól, hogy létezik egy gazdasági ember prototípus, a fogyasztó, akinek a döntései, tettei és céljai aköré épülnek, hogy maximalizálni tudja

⁶¹ Uo.

⁶² Blank, G., Bolsover, G., & Dubois, E.: A new privacy paradox: Young people and privacy on social network sites., Prepared for the Annual Meeting of the American Sociological Association (Vol. 17), 2014, 9-12. o.

a hasznát. Az adatbiztonság tekintetében az adatok átadásával egy tranzakció jön létre, amely egyik oldalán az adatokért kapott potenciális haszon található, a másikon pedig az adatok átadásából eredő lehetséges hátrányok. Az előnyök, a haszon jellemzően kézzelfogható, mint például a különféle kedvezmények, vagy bizonyos kényelmi funkciók. A hátrány, mindennek az ára pedig már sokkal absztraktabb. Következmény lehet például személyiséglopás, az adatok harmadik fél számára továbbítása, s egyéb kockázatok az előbb felsorolt előnyökkel állnak szemben. Az elmélet szerint, ameddig a fogyasztó számára az előnyök meghaladják a hátrányokat, addig elvárható, hogy a felhasználó kiadja az adatait. Mindemellett ettől függetlenül lehetősége van arra, hogy kifejezze aggodalmát személyes adatainak védelmével kapcsolatban – a magyarázat szerint innen ered a különbség a gyakorlat és az elmélet között.⁶³

3.3.2 – Korlátozott racionalitás

Az előző elmélettel ellentétben, ahol arról volt szó, hogy létezik egy racionális fogyasztó, ez az elmélet inkább azt a megközelítést helyezi előtérbe, hogy ugyanazon döntés meghozatalakor az embernek nincsen minden információ a birtokában, így választását ezekre a hiányos információkra építi. Így könnyen torzul az eredmény, a felhasználó alá-, vagy fölébecsüli az előnyöket, vagy a hátrányokat. Ez kívülről irracionálisnak hathat, de belülről a rendelkezésre álló adatok alapján teljesen racionális. Emellett, ha az ember minden szükséges információ birtokában van, valószínűsíthetően akkor sem tudja egyszerre mindegyiket helyesen feldolgozni és tudatos döntést hozni – ezt nevezzük korlátozott racionalitásnak.⁶⁴ Ezt az információhiányt úgynevezett kognitív torzításokkal (cognitive bias) kompenzálják. Ezek alternatív, szubjektív valóságképek, melyet az agy annak érdekében végez, hogy leegyszerűsítse az információfeldolgozást. Nina és Paul Gerber, valamint Melanie Volkamer a következő néhány példán keresztül szemlélteti őket⁶⁵:

- Hozzáférhetőségi torzítás (availability bias): azon események bekövetkezése valószínűbb, amelyekre könnyebben visszaemlékszünk.

⁶³ Gerber, N., Gerber, P., & Volkamer, M.: Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. Computers & security, 77, 2018, 229. o.

⁶⁴ Flender C., Müller G.: Type Indeterminacy in Privacy Decisions: The Privacy Paradox Revisited. In: Busemeyer J.R., Dubois F., Lambert-Mogiliansky A., Melucci M. (eds) Quantum Interaction. QI 2012. Lecture Notes in Computer Science, vol 7620. Springer, Berlin, Heidelberg, 2012, 151-152. o.

⁶⁵ Gerber, N., Gerber, P., & Volkamer, M.: Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. Computers & security, 77, 2018, 229-230. o.

- Optimista torzítás (optimism bias): úgy érzékeljük, a negatív események (például adatvédelmi incidens) könnyebben történik meg másokkal, mint velünk, kisebb kockázatnak vagyunk kitéve.
- Megerősítő torzítás (confirmation bias): az emberek olyan információ után kutatnak, vagy úgy értelmezik a hallottakat, amely megerősíti a saját véleményüket, a korábbi tapasztalataikat.
- Affektív torzítás (affect bias): az emberek hajlamosak gyorsan ítélni érzelmeik alapján. Például alábecsülik a kockázatait azoknak a dolgoknak, amiket szeretnek, túlbecsülik azokat, amelyeket pedig nem.
- Azonnali öröm torzítás (immediate gratification bias): az emberek könnyebben értelmezik az azonnali örömeket, vagy kockázatokat, mint a jövőbenieket.
- Valencia hatás (valence effect): a számunkra szimpatikus eseményeket valószínűbbnek hisszük.
- Keretező hatás (framing effect): az emberek másképp reagálnak ugyanarra a kérdésre, ha másképpen van feltéve, más a kerete, az előadásmód, stb.
- Racionális tudatlanság (rational ignorance): lehetséges, hogy azért nem törődik az ember például az adatbiztonságával, mert nagyobb az ára megtanulni, foglalkozni vele, mint annak, ha egyszerűen csak elvész az adat, vagy illetéktelen kezekbe kerül.

3.3.3 – Tapasztalat, tudás hiánya

Ahhoz, hogy egy felhasználóban kialakuljon a megfelelő hozzáállás, a rutin adatai védelmének tekintetében, ideális lenne, ha saját kézből szerezne tapasztalatot, hisz ez lenne a legerősebb motivátor. Ehhez azonban az kellene, hogy mindenkit érjen valamilyen adatvédelmi incidens. Ez pedig nyilván távol áll az ideális állapottól. Ebből következik, hogy jellemzően másodkézből tudnak csak tanulni az emberek, ami pedig kevésbé effektív.⁶⁶ Vonatkozhat ez a hiány továbbá a technikai, műszaki ismeretek hiányára is.

3.3.4 – Társadalmi befolyásolás

A társadalmi jellegű szempontok több különböző irányból közelíthetők meg. Amennyiben közösségi média tekintetében vizsgáljuk a kérdést, mindenképpen érdemes szem előtt tartani, hogy jellemzően közösségeket találunk ezeken a platformokon, amelyeknek saját szokásaik, szabályaik

⁶⁶ Dienlin, T., & Trepte, S.: Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. European journal of social psychology, 45(3), 2015, 287. o.

vannak. Ha a csoportba való tartozás a szempont, szükségesnek tarthatunk kiadni magunkról információkat, ha a csoport igényli, cserébe megkapjuk az érzést, hogy közéjük tartozunk.⁶⁷ Érkezhet továbbá nyomás barátoktól, családtól, párkapcsolatból, hogy osszunk meg magunkról információkat, például „ha már ők is, akkor mi is, egyéb esetben tiszteletlenség”. A közösség ereje hatalmas ilyen esetekben, az emberek egymástól tanulják a normát, így mindenki hatással van a körülötte lévőkre. Emellett az is egy létező jelenség, hogy aki nem oszt meg magáról semmilyen információt, biztosan rejteget valamit.⁶⁸

3.4 – Adatvédelmi paradoxon - összegzés

A téma sokszínűségéből látszik tehát, hogy egy komplex problémakörrel van szó. Egyértelmű konklúzióra nem sikerült még jutni. Demográfiai szempontból a kutatások jelentős része a fiatalokat jelöli meg, mint különösen érintett csoport, egy másik jelentős része pedig őket jelöli meg, mint leginkább biztonság tudatos csoport. További kutatások elindultak, s megpróbálták személyiségjegyekhez kötni az adatbiztonság kérdését. Ezek sem jutottak megcáfolhatatlan eredményre, ilyen tulajdonságok alapján idáig még nem sikerült megjósolni, előrejelezni valakinek a tudatosságát.

Sikerült számos teóriát felállítani a kutatóknak a témával kapcsolatban, melyből a 4 legnépszerűbbet ismertettem. Ezeknek a gyakorlati alátámasztása még a mai napig folyamatban lévő feladat. Ráadásul látszólag a különböző elméletek között nincsen semmilyen összefüggés, ennek ellenére úgy tűnik, mindegyik hatással van az embernek azon döntésére, hogy milyen odafigyeléssel adja ki a személyes adatait. Mindezeknek köszönhetően az adatvédelmi paradoxon véleményem szerint egy érdekes, kutatandó terület. Jelen kutatással céloim az adatvédelmi paradoxon jelenségének elemzése egy konkrét felhasználói csoport keretében, következtetések levonása, melyek segítségével meggyőződésem szerint jelentősen fejleszthető a felhasználók tudatossága.

⁶⁷ Kokolakis, S.: Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & security, 64, 2017, 128-129. o.

⁶⁸ Gerber, N., Gerber, P., & Volkamer, M.: Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. Computers & security, 77, 2018, 230. o.

4 – KÍSÉRLET

A következőkben az adatvédelmi paradoxon létjogosultságának vizsgálatát mutatom be, különböző szempontok alapján.

4.1 – Kísérlet célja

A kísérlet célja, a tárgyi hipotézisek igazolása, ennek keretében annak bebizonyítása, hogy a célcsoport tekintetében nem releváns az adatvédelmi paradoxon. Mindemellett célja felmérni a felhasználók aktuális adatvédelmi, adatbiztonsági ismereteit, s a már elsajátított tudás gyakorlati alkalmazását is, hogy mind a digitális, mind a valós világban használják az adatbiztonsági, információbiztonsági tudásukat és az erre vonatkozó adatvédelmi intézkedéseket.

4.2 – Kísérlet módszerei

Kísérletem alapvetően két részből áll. Az első része egy kérdőív kitöltése, második pedig két, eltérő tartalmú adathalász kísérlet. A kutatás mindkét része ugyanarra a célközönségre irányult.

4.3 – Kísérlet célcsoportja

Mindkét kísérlet ugyanarra a célcsoportra irányul. A csoport tagjai mind elvégeztek már valamilyen felsőoktatási képzést, mind egy azonos kiberbiztonsági képzésre járnak, ahol végzősök, ez a közös pont bennük. Nem és kor szerint a csoport heterogén, ezek az információk nem képezik a mérés részét, nincs befolyással annak eredményeire. Azért választottam őket, mint a vizsgálat tárgyát, mert már legalább egy éve hallgatják egyetemi kereteken belül az adatbiztonság rejtelseit, a tudatosság fontosságát, valamint különféle védelmi intézkedések szerepét. Ebből következik, hogy a célcsoport a társadalom egy olyan részének tekinthet, akik kiemelt mennyiségben és minőségben kapnak tudatosító anyagokat feldolgozásra, ezért különösen érdekes megvizsgálni, az adatvédelmi paradoxon teljesülésére irányuló vizsgálatban hogyan szerepelnek. A választott csoport a speciális kiválasztási szempontoknak és a létszámnak köszönhetően nem reprezentatív.

4.4 – Kísérlet menete

Első lépésként meghatároztam a kísérlet célját, mely szerint jelen kutatás során célom, hogy az adatbiztonsági tudatosságot mérjem egy kifejezetten erre specializálódott célcsoportban. Ezután kiválasztottam a csoportot és az alkalmazott módszereket. Először a kérdőívet készítettem el és küldtem ki a hallgatók számára, ez volt az adatgyűjtési időszak. Ebben az időszakban

megterveztem mindkét adathalász kísérletet. Amikor az adatgyűjtés lezárult, akkor kezdődtek a kísérletek. Ez a két adathalászatnak tűnő próbálkozásból az első futott 24, a második 12 órát, majd kiértékelésre került. Ezeknek az időtartamoknak a leteltekor utókövetem a célpontokat és rövid interjú keretein belül megkérdeztem, mi volt a benyomásuk, kattintottak-e a megküldött linkekre. Végül a gyűjtött adatokat összevettem a gyakorlatban alkalmazottakkal.

4.5 – Kérdőív

A kísérlet első része egy 27 kérdésből álló kérdőív. Azért ezt a módszert választottam, mert alkalmas az alanyok véleményeinek megismerésére, trendek kimutatására, valamint a paradoxon mindkét oldalának feltérképezésére: a kérdések egy része foglalkozik azzal, milyen szintre becsülik a biztonságosságukat, egy másik része pedig ellenőrző kérdésekkel visszakérdez a korábban elhangzottak igazságtartalmára, kifejteti azokat részleteiben, így növelve a pontosságot. Gyengesége a kérdőívnek, hogy önmagában nem alkalmas a gyakorlatban használtak mérésére, mert teljesen önbevallás-alapú, a kitöltőknek igazat mondaniuk nem kell, ferdíthetnek, vagy túlozhatnak. 60%-os kitöltési hajlandóság mellett 12 fő válaszából fogom a következtetéseket levonni. A kérdőív kérdéseit és válaszait a következők szerint csoportosítom: önbevallott biztonság tudatosság, elméleti ismeretek, gyakorlati ismeretek.

4.5.1 – Önbevallott biztonság tudatosság

Alapvetően az alanyok egyértelműen inkább biztonság tudatosnak vallották magukat. Ezt mutatja, hogy a 12 fő átlagosan 5-ös skálán 3,75-re értékelte magát (ahol az 1 az egyáltalán nem, 5 pedig a teljes mértékben), kettő eltéréssel egyhangúan 4-esre. Ezt a gondolatot követi még, hogy egyhangúan, 100%-ban úgy nyilatkoztak, hogy ismerik a social engineering fogalmát, valamint azt állítják ismerik a különbséget a http és a https kapcsolatok között. Zárásképpen rákérdeztem, milyen alapossággal állítanak be egy új Wi-Fi kapcsolatot, például otthoni hálózatot. 75% teljeskörű biztonsági beállításokról nyilatkozott, 25% néhány biztonsági beállításról, a harmadik opció, miszerint alapbeállításokat alkalmaznak, nem kapott jelölést.

Összefoglalva elmondható, hogy jellemzően úgy gondolják, tisztában vannak képességeikkel, amelyek az átlagtól valamelyest jobbnak mondhatóak, eszerint biztonság tudatosabbaknak tekinthetők. Így ez az eleme megvalósul az adatvédelmi paradoxonnak – úgy gondolják, tudják. De vajon alkalmazzák-e?

4.5.2 – Elméleti ismeretek

Az elméleti ismereteknek az első része, hogy rákérdeztem a kérdőívben korábban elhangzott kérdésekre ellenőrzésképpen, hogy mi is a social engineering és mi a http és https közötti különbség – szabadkezes válaszként. Az elsőre egy kivétellel (12/11) egybehangzó válasz érkezett, mely tartalmazza röviden összefoglalva a helyes definíciót. Egy kivétel pedig részben téves, inkább a nyílt forrású információszerzés fogalma irányába vitte el a választ, arra helyezte a hangsúlyt. A secure/biztonságos kapcsolatot pedig 100%-ban helyesen válaszolták meg.

A második része ennek az osztályozásnak egy feleletválasztós kérdéssor volt, ahol ki kellett választaniuk 4 opcióból, melyik a kérdésben feltett kifejezés definíciója. Ezt 4 különböző kérdésben tettem meg, szétszórva a kérdőívben, hogy minimalizáljam a kikövetkeztetés valószínűségét. 100% helyesen választották ki az adathalászat, a szoros követés, a szétszórás és a váll szörfölés technikák definícióját.

A harmadik elméleti tudást felmérő kérdéskör az ideális jelszó erősségéről szól. A következő szabályokat szavazták meg, feleletválasztással, ahol több opció volt engedélyezett: minél hosszabb, legalább 8 karakter; kisbetűket tartalmaz; nagybetűket tartalmaz; számokat tartalmaz; különleges karaktereket tartalmaz; nem tartalmaz értelmes szót; egyedi, korábban nem használt jelszó. 4 helytelennek tűnő választ is elrejtettem az opciók között, összesen egy lett egyszer megjelölve: személyünkkel összefüggő adatot tartalmaz. Ezek alapján megállapítható, hogy ez az egy „hibás” válasz még hibahatáron belül van. A többi válaszban átlagosan 12-ből 11-en helyesen állapították meg, 91,66%-os hatékonysággal, 8-an pedig hibátlanul kitöltötték, ami 2/3-a a kitöltőknek.

Az elméleti ismeretek terén megállapítható, hogy kimagaslóan szerepelt a csoport, minden megmérettetést legalább 90%-os sikerrel vesznek átlagban, több helyen a 100%-ot is sikerül stabilan elérni. Ez részben továbbra is alátámasztja a paradoxont, ugyanis nem csak azt mondják, hogy tudják és nekik ez fontos, hanem tényleg vannak információk a birtokukban. A kérdés továbbra is ugyanaz: vajon alkalmazzák-e a gyakorlatban?

4.5.3 – Gyakorlati alkalmazás

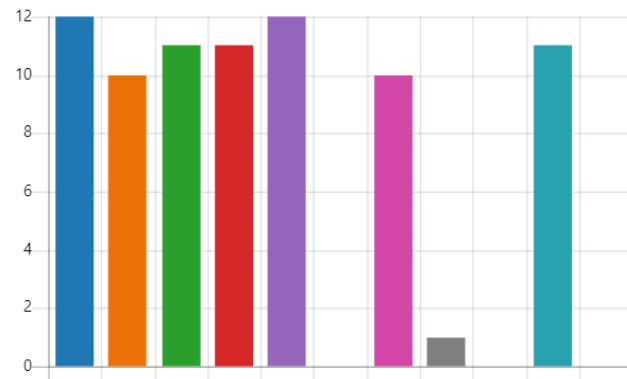
A gyakorlati alkalmazás esetén több kérdést is feltettem, melyeket különböző csoportokba osztok.

4.5.3.1 – Elmélet ellenőrző kérdései

Az első alcsoportja a gyakorlatnak az elmélet ellenőrző kérdései. Ide tartozik az említett jelszókezelési szokásokra irányuló kérdések. A 6. és 7. ábra összehasonlításán jól látszik, hogy alapjaiban betartják az általuk elméletben felvázoltakat. Egyetlen szembeötlő különbség van, mégpedig az egyedi, korábban nem használt jelszó kritérium, amelyet csak 3 ember alkalmaz a 12-ből. Ez a 3 személy átlagosan kb. 36 jelszót kell megjegyezzen, körülbelül ugyanennyi eszköze/applikációba. Aki megjelölte az értelmes szót, véletlen megjelölte azt is, hogy tartalmazzon is, s azt is, hogy ne, így hibának könyvelem el. Az előző 91,66%-os sikerrátához képest a gyakorlati kérdés 80,95% értéket mutat abban a tekintetben, hogy betartják-e amit elméletben tudnak. Ketten tökéletesen megfelelnek nem csak annak, amit elméletben tudnak, hanem ami az optimális jelszókezelést jelenti a valóságban. Négy kitöltő 7-ből 6 szempontot betart. Fontos megemlítenem, hogy volt lehetőség nem válaszolni, amivel hárman éltek, az ő álláspontjuk: nem szeretnék válaszolni. Ezt a statisztikákból kivontam. Összegezve a kitöltők nem teljesen alkalmazzák az elméletben elsajátítottakat, de nem mutatnak komoly eltéréseket, így azt a következtetést vonnám le, hogy nagyrészt követik a saját tanaikat.

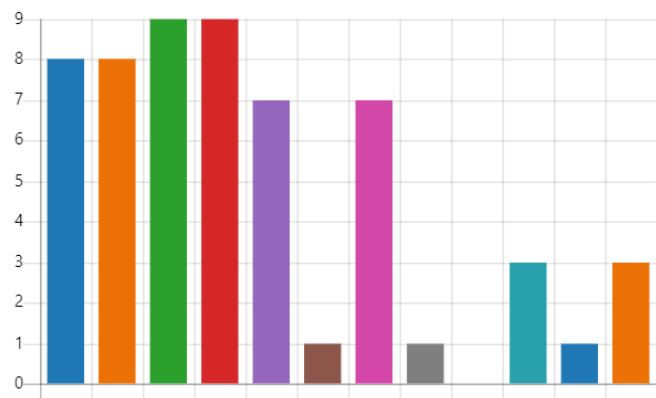
Rákérdeztem a jelszóismétlődésre is. A különböző élethelyzetek nagy szórást eredményeztek. Jellemzően 6-10 különböző jelszóról számolnak be, de a minimum a 4-5, a maximum pedig 50 felett jelentkezett, melyet ketten is jelöltek. Hárman másként értelmezték a kérdést, ők 3-5 eszközről számolnak be, hozzájuk pedig átlagosan kb. 38 jelszóról, sajnos az ő adatukat nehéz kontextusba helyezni. A többi 8 ember hasonlóképpen értelmezte a kérdést, az ő átlaguk a következő: egy jelszó kb. 3,63-szor ismétlődik. Ezt az átlagot nagyon felhúzza egy kitöltő, aki kb. 12,5-ször annyi helyen aktív, mint ahány jelszava van, nagyon javítja pedig egy másik, akinél kb. minden jelszó egyedi. Nélkülük egy jelszó átlagosan 2,74-szer ismétlődik, nem tekinthető rossz átlagnak. További mérés szükséges, hogy összehasonlítható legyen más csoportok átlagaival.

Minél hosszabb, de legalább 8...	12
Kisbetűket tartalmaz.	10
Nagybetűket tartalmaz.	11
Számokat tartalmaz.	11
Különleges karaktereket tartal...	12
Értelmes szót tartalmaz.	0
Nem tartalmaz értelmes szót.	10
Személyünkkel összefüggő ad...	1
Minden rendszerben ugyanazt...	0
Egyedi, korábban nem használ...	11
Adott eszközön elmentve táro...	0



6. ábra: Jelszókezelés elméletben (Forrás: kérdőív)

Minél hosszabb, de legalább 8...	8
Kisbetűket tartalmaznak.	8
Nagybetűket tartalmaznak.	9
Számokat tartalmaznak.	9
Különleges karaktereket tartal...	7
Értelmes szót tartalmaznak.	1
Nem tartalmaznak értelmes sz...	7
Személyeddel összefüggő ada...	1
Minden rendszerben ugyanazt...	0
Egyedi, korábban nem használ...	3
Adott eszközön elmentve táro...	1
Nem szeretnék válaszolni.	3



7. ábra: Jelszókezelés gyakorlatban (Forrás: Kérdőív)

Emellett jelszavaik egyéb tulajdonságaira is rákérdeztem. Erre a kérdésre ketten nem válaszoltak, így a maradék 10 főből 9 fejben tárolja a jelszavait, ketten használnak jelszókezelőt (is), ketten pedig az eszközön elmentve (is) tárolják ezeket – ez a két-két ember különböző, nem a jelszókezelőt jelölték kétféleképpen. 10-ből 6 személy egy-egy jelszó különböző változatait használja, öten pedig generált jelszavakkal dolgoznak. Ebből a kérdés-válasz párosból egyértelmű következtetéseket nem lehet levonni, a felhasználási szokásaik ebben a tekintetben átlagosnak tűnnek.

Ellenőrzésre került a Wi-Fi beállítási kérdés. A három személyből kettő, aki néhány beállítást alkalmazna, a következők mellett tették le a voksukat: erős jelszó, esetleg tűzfal. A harmadik kitöltő pedig olyan beállításokat sorol fel, amivel inkább a teljeskörűbe tartozik. Kettő személy nem válaszolt, a többiekből 3-an is említették a vendég Wi-Fi hálózat létrehozását, egyéb válogatott beállítások mellett. Ez alátámasztja azt, hogy nem csak megjelölték, hanem használják is az opciókat.

Ez a kérdéscsoport az első, ahol valóban rátérhetünk arra, vajon betartják-e azokat a szabályokat, amiket elméletben bebizonyítottak, hogy tudnak. Kettő válasz tekintetében sikerről számolhatok be, nem csak beszélnek róla, hanem ténylegesen alkalmazzák a tudást – legalábbis önbevallásos alapon. Másik két kérdés esetében a végeredmény nem egyértelmű abban a tekintetben, további mérések szükségesek, hogy biztosan állítani lehessen, hogy átlagosan, vagy átlag felett szerepeltek.

4.5.3.2 – Adatok, információk rendszerezése, védelme

Következtetéseket lehet levonni az adatok, információk rendszerezéseiből, védelméből is, melyet öt szempont szerint is vizsgáltam a kérdések során. Az egyik, a papír alapú dokumentumok rendszerezése. Kifejezetten az adatok érzékenységét említette egy személy, aki kitért a megsemmisítési eljárás fontosságára is. Heten valamilyen tematika, tartalom alapján csoportosítják, négyen sehogy, csak ömlesztik – ebből a 2 csoportból egy kitöltő mindkét technikát alkalmazza. Egy ember nem válaszolt, egy pedig kifejtette részleteiben, hogy nem rendszerez ugyan, de nem is elégedett ezzel a szokásával. Így a válaszadók 68,18%-a valamilyen, jellemzően tematikus rendszer szerint kezeli a dokumentumait, 31,81%-a – a többi – pedig nem végez semmi rendszerezést. Összegezve megállapítható, hogy a megkérdezettek többsége rendszerezi dokumentumait, különös figyelmet fordít az iratok biztonságos tárolására, azonban az is kitűnik a válaszokból, hogy van még hová fejlődni a biztonságos papír alapú tárolás terén.

Digitális dokumentumok logikai védelme tekintetében 2 ember nem válaszolt, 1 nem használ semmit saját bevallása szerint, 1 pedig rosszul értelmezte a kérdést. A konkrét választ adók 90%-a helyesen értelmezte a logikai védelmet, s legtöbbjük számos megoldás felsorol.

Papír alapú dokumentumok fizikai védelme tekintetében ugyanez a két ember nem válaszolt. Itt már kicsit rosszabb a helyzet, ugyanis a konkrét válaszadók közül 4-en (40%) arról számoltak be, hogy semmilyen védelmet nem használnak. Ebből vagy az következik, hogy tényleg nem, vagy az,

hogy nem ismerik a fizikai védelem lehetőségeit – véleményem szerint az utóbbi áll fenn. Az összes többi kitöltő (60%) felsorolta különböző változatokban egy lakás esetében az elvárható védelmi intézkedéseket, vagy többet.

Adatbiztonsági technikai megoldásainak tekintetében biztonságtudatosságról számolnak be az adatok. A kitöltők 100%-a erős jelszavakat használ, egy-egy kivételtől eltekintve mindenhol megjelenik a tűzfal, a vírusirtó és a rendszer, programok frissen tartása – külön személyeknél, így ezt még hibahatáron belülnek gondolom. Erősen jelen van még a kétlépcsős azonosítás és a folyamatos ismeretbővítés. A kitöltők 60%-a használ publikus felhőszolgáltatást, a felsőoktatási intézményét senki, a biztonságosan tárolt pendrive pedig 50% számára az ideális választás. Egy személy nem szeretett volna válaszolni. Akik a biztonságos, akár rejtett pendrive megoldást választották, ki is fejtették, a biztonsági mentés és a fizikai biztonság fontosságát. Megjelent kettő kifejezetten csak preferencia alapú, valamint mind felhő, mind pendrive tekintetében visszatérő válasz az ár/érték arány, a költséghatékonyság/ráfordított energia arány, valamint a kockázatokkal arányos jelző a válaszban.

Legfontosabb dokumentumok CIA védelme egy átfogó kifejtős kérdés volt. Hárman nem válaszoltak, abból kettő visszatérő. A kérdést utolsónak tettem fel, így a szabadkezes válaszok mennyiségéből adódóan a részletezés már nem teljeskörű, de továbbra is őszintének látszik. A kitöltők jellemzően kibontották a CIA rövidítést és jól értelmezték annak elemeit. Válaszok tekintetében a bizalmasság és a sértetlenség jellemzően valamilyen módon megjelenik, a rendelkezésre állás tekintetében nem egyértelmű teljesen. Három személynél valamilyen megoldás jelen van, kettőnél pedig egyértelműen nincsen, melyből aki korábban a rendszerezési szokásaival elégedetlenkedett, itt is kifejtette, hogy amennyiben egy eszköze elveszne, megsérülne, pótlását hatalmas nehézségekbe ütközne, így fejlesztésre szorul ez a szempont.

Végül szempont, hogy mennyire bíznak a kitöltők a nyilvános Wi-Fi-kben. 12-ből 6 kitöltő csak az általuk ismert hálózatokra csatlakozik, 5 csak a biztonságosnak tűnő megoldásokat választja, 1 pedig sosem használ Wi-Fi-t. Olyan válaszadó nem volt, aki körültekintést nélkülözve kapcsolódik fel bármire, ami elérhető, ez alátámasztja a biztonságtudatosságukat.

Alapvetően a kitöltők biztonságtudatosságról számolnak be a szokásaik terén is. Jellemzően helyesen értelmezik a kérdésben elrejtett szakkifejezéseket, s annak megfelelően válaszolnak, s általánosságban kimondható, hogy a válaszok nagyrésze több különböző védelmi megoldást is

tartalmaz. Kettő gyengepontja volt csak ennek a nagyobb lélegzetvételű résznek: a papír alapú dokumentumok védelme, valamint a rendelkezésre állás biztosítása.

4.5.3.3 – *Közösségi média szokások*

Az egyértelműen látszik a válaszokból, hogy 1 személyt leszámítva mindenki aktívan használ valamilyen beállítást a közzési média platformokon. Ennek az egynek a profilja nyilvános és nem is érdeklik a beállítások. Egy kitöltő önmarketingre használja a nyilvános profilját, s egy kitöltő pedig több profilról számol be, melyből van magán, teljesen zártan, s nyilvános, az előzőhöz hasonlóan tudatos megosztásokkal. Ketten nem használnak közösségi médiát, nincsenek szokásaik ezzel kapcsolatban. Az összes többi kitöltő csak ismerősök, vagy azok számára sem elérhető beállításokat használnak, s jellemző közöttük, hogy a biztonsági beállítások oka, hogy fontos számukra a biztonságtudatosság.

4.5.4 – Következtetések

Úgy gondolom, a kérdőív sikeresen igazolta dolgozatom hipotéziseit. Fenntartásokkal kell kezelni ugyan, mivel a gyakorlatot bevallásos alapon mérte, de a számtalan ellenőrző kérdés, a válaszok megfogalmazása és összetettsége arra enged következtetni, hogy a kitöltők őszinték voltak. Az elméletet a várakozásaimnak megfelelően komoly pontossággal tudták, a gyakorlat tekintetében pedig összehasonlíthatóan jó eredményeket értek el, egy-két pontot leszámítva. A jövőben szükség lenne egy reprezentatív kérdőívre is, ugyanezekkel a kérdésekkel, hogy összehasonlíthatóak legyenek az eredmények, amelyben feltételezésem szerint még a gyengébb pontok is átlagon felülieknek számítanak.

4.6 – Adathalász kísérletek

A következő része a kísérletnek gyakorlatiasabb irányt vett. Adathalász kísérleteket hajtottam végre a célcsoporton. Ezeknek célja az volt, hogy felmérjem, a való világban hogyan alkalmazzák a korábban elsajátított ismereteket. Két e-mailt küldtem el a 20 embernek, akik között a kérdőívet is megosztottam. Az e-mail címeket egy zárt csoportban, önként osztották meg korábban, amelynek én is tagja vagyok.

4.6.1 – Befolyásoló tényezők

Korábbi megfigyeléseim azt mutatták, hogy a hasonló próbálkozásokat a csoport tagjai kibeszélik, ha van lehetőségük, akkor személyesen, ha nincs, akkor online. Lehetőségeimhez mérten igyekeztem ezt az eshetőséget minimalizálni és olyan időpontot választani a leveleknek, amikor a tanórai kereten kívül vannak a célcsoport tagjai. További befolyásoló tényező volt, hogy kikerüljem a spam szűrőket. Erre azt a megoldást választottam az egyik esetben, hogy volt rugalmasságom egy népszerű e-mail szolgáltatót, Gmail-t választani, így ez a rész le volt fedve. A másikinál sajnos ilyen lehetőségem nem volt, az e-mailcímnek valósnak kellett tünnie, így nem választhattam ugyanazt a szolgáltatót. A spam szűrő képességeit teszt e-mailekkel tettem próbára, melyek óriási százalékban elakadtak, így több újrafogalmazás, újraformázás vált szükségessé. Végül sikerült mindkét esetben létrehozni egy olyan levelet, ami a tesztek alapján képes lehet átjutni a spam szűrőkhöz. Ehhez mind a kettő levelet magyarul kellett megfogalmaznom, s mind a kettőt elég közvetlen módon, kevésbé hivatalosan, inkább barátságosan. Ezek egyik levél esetében sem voltak problémás pontok, ugyanis olyan szempontok szerint választottam ki a tartalmukat, hogy hitelesnek tűnjön ezekben az esetekben is.

4.6.2 – Első e-mail – állásajánlat

Egy állásajánlatot választottam az első kísérlet alapjaként. Az ihletet az adta, hogy én is kaptam egy hasonló valódi álláshirdetést tartalmazó levelet, s tudtak benne olyat írni, amely miatt kattintottam, továbbá a végzős hallgatók jellemzően úgy gondolom, nyitottak lehetnek egy szakmába vágó, jól fizető állásajánlatra. Emellett nehéz leellenőrizni, ugyanis az e-mail cím lehet általános, például annak a neve, aki küldi a levelet. Így is döntöttem, létrehoztam egy keresztnév és vezetéknévből álló e-mail címet egy népszerű szolgáltatónál, elkészült tehát Réka Gmail fiókja, reka.benedek.01@gmail.com. Az említett valódi levél tartalmát lemásoltam, megtartottam belőle a formátumot, az összegeket, amelyekkel engem is kattintásra bírtak, de átírtam benne néhány elemet, például nem informatikai, hanem kiberbiztonsági szakértőt keresnek, s ideális jelöltnek tünnek, a megszólítást személyre szabtam, valamint elláttam aláírással, ami fiktív név, fiktív cégnév, emellett egy jogdíj nélküli stock fotón szereplő fiatal hölgyet állítottam be mind az aláírásba, mind a profilképhez, a Pixabay-ról⁶⁹. Az eredeti és az én verzióm is tartalmazott egy rövidített bit.ly linket, azzal a különbséggel, hogy az eredeti az állásportálra vezetett, az enyém

⁶⁹ <https://pixabay.com>

pedig egy blogra. Ezen a blogon nem volt semmilyen tartalom, csak annyit kértem az odatévedtektől, hogy ne osszák meg a csalást a társaikkal, hogy az eredmény a lehető legtisztább maradjon. Mindkét esetben, az ihletet adó és az én levelem esetében is, a hozzá tartozó ötlet az volt, hogy a link mögött elérjük a részleteket.

Ez az adathalász e-mail 24 órára volt tervezve. Ennél több úgy gondolom, nem szükséges, lényegében mindenki az első adandó alkalommal olvassa a leveleit. Megközelítőleg az első 5 percben ketten is kattintottak. Azután néma csönd. Kettő óra után értesültem róla, hogy megjelent a téma a csoportban. Ez egyrészt valamelyest lehetséges, hogy módosítja az eredményeimet, másrészt mivel ez vissza-visszatérő elem a csoportban, s eleve számítottam rá, hogy ez előfordulat, nekem megfelelő bizonyíték arról, hogy a csoport tagjai alapvetően biztonság tudatosak, s érdeklődési körükbe tartozik, hogy foglalkozzanak a témával, valamint jellemzően nem kattintanak még a legjobban megszerkesztett megoldásokra sem, inkább megosztják és megbeszélik egymás között.

Az e-mail tartalma és külleme a következő képen található.



8. ábra: 1. adathalász kísérlet

Az utólagos interjú során senki sem vallotta be a kattintást – bár 20-ból 3-an nem válaszoltak a kérdéseimre. 6-an pedig nem kattintottak saját bevallásuk szerint, 5-en jelezték, hogy spam mappába került a levél, 4-en pedig nem vették észre. Érkezett még olyan visszajelzés, hogy előnézetrel meg tudta vizsgálni a csoport egyik tagja, hová vezet a link, így nem folytatta, volt, aki

jelezte, hogy a vírusírtó még malware-t is kimutatott rá. Egy személytől pedig „majdnem kattintottam” visszajelzést kaptam. Itt jegyezném meg, hogy az első 5 percben még megbízhatóan működött a létrehozott blog belső számlálója, ezért biztosan tudom, hogy volt azonnal kettő kattintó, emellett a 24 órából 22 úgy telt el, hogy már volt téma a zárt csoportban, beillesztett fényképpel az adathalász próbálkozásom, így az eredmény nem egyértelmű.

4.6.3 – *Második e-mail – Gyanús tevékenység*

A második e-mail 12 órára volt tervezve, egy másik időpontban. A fontos változás az előzőhöz képest, hogy itt a kattintásnál bejelentkezési felületre számíthatnak, akiket sikerül átverni, így ha nem az általam készített másik blogon található megnyugtató üzenet fogadja őket, könnyen lehetséges, hogy ha megfelelő színvonalon készíti el valaki azt a weboldalt, ki tud csalni belőlük bejelentkezési adatokat. A küldő, akinek az álcáját felvettem, egy népszerű streaming szolgáltató, a Netflix, ugyanis előzetes felméréseim arra engedtek következtetni, hogy széleskörben elterjedt a csoport tagjai között, így maximalizálni tudom az érdekeltségüket. Az e-mailcím amit használtam igyekezett egy támadót imitálni, így ingyeneset használtam, de a lehető legkörültekintőbben állítottam össze, hogy első ránézésre akár hivatalosnak is tűnhessen. Így hoztam létre assist.netflix@europe.com-ot. Az e-mail tartalma arról szólt, hogy gyanús tevékenységet észlelt a szolgáltató Madridból, ami egy általam szabadon választott, távoli város. Amennyiben nem a jogos előfizető jelentkezett be onnan, akkor a linkre kattintva intézkedhet – szintén egy (másik) rövidített bit.ly link vezetett egy másik blogoldalamra. Használtam még emellett a cég logóját, valamint a formátumukat lemásolva, követtem a betűméret, tagolás és stilisztikai jellemzőket. Emellett használtam a 'lépj velünk kapcsolatba' és 'írj nekünk' linkeket is, mint ténylegesen létező opciók, ezzel tovább erősítve a levél hitelességét. Természetesen ez nehezebben jutott át a spam szűrőn, de a tesztelések végül sikerrel jártak.

Az e-mail tartalma és külleme a következő képen látható.



9. ábra: 2. adathalász kísérlet

Az utólagos interjú során egy személy bevallotta, hogy kattintott. Hárman ugyanúgy nem válaszoltak kérdéseimre. 5-en azt állították, nem kattintottak. 6-an spam mappát említettek, 4-en pedig nem vették észre. Egy pedig személy azt jelezte vissza, hogy „annyira lehetetlen e-mail cím volt, hogy azonnal törölte egy mosoly kíséretében”.

4.6.4 – Következtetések

Azt már az előkészületek során biztosan kijelenthettem, hogy borzasztó nehéz átütni a spam szűrőt. Órákig fogalmaztam az e-maileket, mire lett egy olyan verzió, ami átjut. Ebből és a tesztelés közbeni alanyok beszámolóiból arra tudok következtetni, hogy a komolyabb e-mail szolgáltatóknak már nagyon jó rendszereik vannak arra, hogy megszűrjék a leveleket. Keresnek szavakra, figyelnek meg trendeket, tanulnak a felhasználói visszajelzésből. Ha valami spamnek tűnik, a megfelelő mappába kerül. Ha valami nagyon nincs rendben, külön felhívják a figyelmet rá, hogy a linkek, képek és csatolmányok el vannak rejtve addig, amíg biztosan meg nem erősíti a felhasználó azt, hogy az e-mail tartalma valós. Arra a következtetésre lehet jutni tehát, hogy a biztonságtudatosság a cégek által egy jól megtámogatott állapot 2021-ben.

A támadóknak rendkívül nehéz dolguk van. Viszont mivel nem ez a dolgozat célja, így egyik részben ez a kísérlet nem vezetett egyértelmű konklúzióra. Sajnos olyan sok levél akadt fent a szűrőn, hogy a maradék adatból nehéz következtetni. Ellenben ami biztos, hogy a csoport általános biztonságtudatosságát jelzi, hogy azonnal téma lett a levél és azonnal megtárgyalták a közös közösségi platformon található csoportban. Továbbá a tiszta adat azt mutatja, hogy 34 próbálkozásból – kivonva a nem válaszolókat – 3 járt sikerrel. Ehhez nyugodtan hozzászámolhatjuk, hogy mivel az ellenőrzési módszerem interjú volt, ezért nem feltétlen kellett őszintének lenniük. Továbbá 11 került a spam mappába, emellett 11-szer biztosan nem kattintottak, saját bevallásuk szerint. A 4-4 válaszadó általi nem vette észre visszajelzés arra enged következtetni, hogy a legközelebbi kísérletnél hosszabb időintervallumot érdemes hagyni a kifutásra. Az a konklúzió is levonható, hogy a tudatosságot értelmezhetjük úgy is, hogy a csoport tagjai tisztában vannak az elméleti és gyakorlati megoldásokkal, valamint azzal hogyan akadályozzanak meg egy támadást, így például a vírusírtó jelzése, az előnézet használata és a feladó e-mail címének ellenőrzése mind sikernek számítanak. Összegzésként úgy gondolom, hogy 40-ből 6-ot nem értékelünk, mert nem válaszoltak. 8-at, mert feltehetőleg nem ment elég ideig a kampány. A maradék 24-ből 3 érte el a célját (12,5%), 11 (45,833%) technológiailag akadt el, 11 (45,833%). Tudatos döntés következtében nem jutott el a célig. Természetesen, mint korábban említettem, mivel ez több, mint 100%, egy, vagy két fő vagy nem vallotta be, vagy nem válaszolták meg a kérdéseimet. Egyértelmű, hogy a következő ilyen időszakra nem csak hosszabb futási idő szükséges, hanem még pontosabb mérőeszköz, valamint annak még kiterjedtebb, hosszabb ideig tartó tesztelése az éles kísérlet előtt, hogy minden kivételre és hibára fény derüljön. Emellett feltételezem, hogy a 12,5% is egy jó arány, ennek bizonyítására a következő kísérletre hasznos lehetne egy reprezentatív csoport, hogy összevethessük az eredményeket.

AJÁNLÁS

Ahogy említettem, a dolgozatom egyik célja a biztonságtudatosság további növelése Magyarországon. A hazai szakirodalomban elvétve találkozni az adatvédelmi paradoxon fejtegetésével, a felsőoktatási tantervekben pedig nemrégiben jelent csak meg a social engineering fogalma. Úgy gondolom, hogy az adatvédelmi tudatosítás keretein belül a social engineering támadási formák és felismeréseik oktatása szélesebb körben hasznos lenne, valamint az adatvédelmi paradoxon témakörével is érdemes lenne bővíteni ezt, hogy a hallgatók felismerjék

magukban és környezetükben azokat a jeleket, amik arra engednek következtetni, hogy felelőtlenül bánnak az adataikkal. Ugyanis nem csak a social engineer verhet át bárkit, ami ellen fel kell készülni, hanem saját magunkat is könnyen kellemetlen helyzetbe hozhatjuk külső manipuláció nélkül is, s legalább ugyanannyira fontos, hogy széleskörben elkerülhetővé váljanak ezek az alapvető hibák.

Azzal a javaslattal is élnék még, hogy ezeknek az anyagoknak az oktatásával nem érdemes várni felsőoktatásig, ugyanis a fiatalabb gyermekek is használják az internetet, nekik is kellene legyen privát szférájuk, s mivel bizonyos kutatások szerint ők a legkitettebbek, valamint jellemzően pozitív példa híján egymástól tanulnak, fontos lenne számukra a tudatosítást a lehető legkorábban elkezdni.

ÖSSZEGZÉS

Az már régóta egyértelmű számomra, hogy az információs társadalomban az adatok védelme fő prioritás, ezt a szellemiséget próbálom az ismerősi körömben is terjeszteni. Viszont amikor az érdeklődési köröm középpontjába került az adatbiztonság, majd találkoztam az adatvédelmi paradoxonnal, még nem számítottam arra, hogy mikor végzek a vizsgálódással, fordulat fog bekövetkezni. Olyan csoporttal találkoztam, aminek a tagjai látszólag nem csak értik a tudatosságot, hanem alkalmazzák is, ezzel megborítva a korábban stabilnak tűnő paradoxon-elméletet, s azt engedi sejtetni, hogy az emberek jellemzően csak nem elég képzettek ahhoz, hogy érdemben megvédjék magukat, hanem tesznek is a biztonságuk érdekében. A különböző támadási módszerek ismerete elengedhetetlen ahhoz, hogy valaki biztonságtudatosnak nevezhesse magát, s a kérdőív segítségével bebizonyítottam, hogy létezik olyan csoport, aki elérték az ideálisnak nevezhető állapotot ilyen téren. Kísérletem második felében pedig bebizonyítottam azt, hogy ennek a biztonságtudatossági szándéknak a technikai feltételei is adottak, így a kettő együttesen használva elegendő ahhoz, hogy egy támadást nagy hatásokkal elhárítsanak. Ebben a célcsoportom kiemelkedően jól teljesített, ami alapján kijelenthetem, hogy rájuk tekintve az adatvédelmi paradoxon nem releváns, mind a kibertérben, mind a való világban tudatosan viselkednek, így például szolgálhatnak abban a tekintetben, hogy működhet-e a tudatosítás. Ugyanis működhet. Úgy gondolom, hogy mindenki felelőssége ennek a szellemiségnek a terjesztése, melyhez elengedhetetlenek a további, bővített képzési anyagok, melyeket egyre szélesebb körben érdemes terjeszteni.

FORRÁSJEGYZÉK

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

2018. évi XXXVIII. törvény az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek az Európai Unió adatvédelmi reformjával összefüggő módosításáról, valamint más kapcsolódó törvények módosításáról

<https://ah.gov.hu/awareness-program/> (Megtekintés: 2021. 11. 14.)

Aldawood, H., Alashoor, T., & Skinner, G.: Does awareness of social engineering make employees more secure?. International Journal of Computer Applications, 177(38), 2020, 45-49. o.

Algarni, A., Xu, Y., & Chan, T.: Social engineering in social networking sites: the art of impersonation, 2014 IEEE International Conference on Services Computing, IEEE, 2014, 797-804. o.

AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679 RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet - GDPR)

Barnes, S. B.: A privacy paradox: Social networking in the United States. First Monday, 2006.

Beresford, A. R., Kübler, D., & Preibusch, S.: Unwillingness to pay for privacy: A field experiment. Economics letters, 117(1), 2012, 25-27. o.

Blank, G., Bolsover, G., & Dubois, E.: A new privacy paradox: Young people and privacy on social network sites., Prepared for the Annual Meeting of the American Sociological Association (Vol. 17), 2014. 1-33. o.

Breda, F., Barbosa, H., & Morais, T.: Social engineering and cyber security. In International Technology, Education and Development Conference, 3/3 szám, 2017, 106-108. o.

Brown, B.: Studying the Internet Experience, Publishing Systems and Solutions Laboratory, HP, Bristol, 2001, 1-23. o.

Cinelli, M., Morales, G. D. F., Galeazzi, A., Quattrociocchi, W., & Starnini, M.: The echo chamber effect on social media. *Proceedings of the National Academy of Sciences*, 118(9), 2021, 1-8. o.

Claude E. Shannon - Warren Weaver: A kommunikáció matematikai elmélete. Az információelmélet születése és távlatai. 1949. Budapest, 1986.

Conteh, N. Y., & Schmick, P. J.: Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, 6(23), 2016, 31-38. o.

Craig, D., Diakun-Thibault, N., & Purse, R.: Defining cybersecurity, *Technology Innovation Management Review*, 4. szám, 2014, 13-21. o.

Dienlin, T., & Trepte, S.: Is the privacy paradox a relic of the past? An in - depth analysis of privacy attitudes and privacy behaviors. *European journal of social psychology*, 45(3), 2015, 285-297. o.

Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

<https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> (Megtekintés: 2021. 10.10.)

ENISA: Threats and trends, 2021, <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends> (Megtekintés: 2021. 11. 13.)

Europol: Internet Organised Crime Threat Assessment (IOCTA) 2021, Publications Office of the European Union, Luxembourg, 2021.

Ferreira, A., Coventry, L., & Lenzini, G.: Principles of persuasion in social engineering and their use in phishing, *International Conference on Human Aspects of Information Security, Privacy, and Trust*, Springer, Cham, 2015, 36-47. o.

F. Mouton, M. M. Malan, L. Leenen and H. S. Venter, "Social engineering attack framework," 2014 Information Security for South Africa, 2014, 1-9. o.

Flender C., Müller G.: Type Indeterminacy in Privacy Decisions: The Privacy Paradox Revisited. In: Busemeyer J.R., Dubois F., Lambert-Mogiliansky A., Melucci M. (eds) Quantum Interaction. QI 2012. Lecture Notes in Computer Science, vol 7620. Springer, Berlin, Heidelberg, 2012.

Gazdag Ferenc – Tálas Péter: A biztonságot veszélyeztető tényezőkről I. Nemzet és Biztonság, 1, 2008, 3-12. o.

Gazdag Ferenc – Tálas Péter: A biztonság fogalmának határaitól. Nemzet és Biztonság, 1, 2008, 3-10. o.

Gerber, N., Gerber, P., & Volkamer, M.: Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. Computers & security, 77, 2018, 226-261. o.

Hall, Mark. "Facebook". Encyclopedia Britannica, 2021, <https://www.britannica.com/topic/Facebook>. (Megtekintés: 2021. 11. 12.)

H. Ning, X. Ye, M. A. Bouras, D. Wei and M. Daneshmand,: General Cyberspace: Cyberspace and Cyber-Enabled Spaces, IEEE Internet of Things Journal, 5/3. szám, 2018, 1843-1856. o.

<https://www.is-c2.org/-/media/ISC2/Research/Cyberthreat-Defense-Report/2021/CyberEdge-2021-CDR-Report-v10--ISC2-Edition.ashx> (Megtekintés: 2021. 11. 12.)

ISO/IEC: ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements Geneva, Switzerland: ISO/IEC, 2013.

<https://www.itgovernance.co.uk/social-engineering-attacks> (Megtekintés ideje: 2021.11.14.)

Ivaturi, K., & Janczewski, L.: A taxonomy for social engineering attacks. In International Conference on Information Resources Management, Centre for Information Technology, Organizations, and People, 2011, 1-12. o.

Dr. Izsa Jenő: Nemzetbiztonsági alapismeretek (A titkosszolgálatok működése), Egyetemi jegyzet, Budapest, 2009.

Johnson, B., & Vegas, L.: Privacy no longer a social norm, says Facebook founder, The Guardian, 2010.

László Gábor: Kockázatértékelés, kockázatmenedzsment, 2014.

Kokolakis, S.: Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & security, 64, 2017, 122-134. o.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. : Advanced social engineering attacks. Journal of Information Security and applications, 22, 2015, 113-122. o.

Long, J. No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing, Syngress, 2011.

Michael Aminzade: Confidentiality, integrity and availability – finding a balanced IT framework, Network Security, Volume 2018, 5. kiadvány, 2018, 9-11. o,

Mitnick, K. D. - Simon, W. L.: A legendás hacker – A megtévesztés művészete, Budapest, 2003.

<http://www.mkih.hu/a-hirszerzes-forrasai.html> (Megtekintés: 2021.11.12.)

Muha Lajos – Krasznay Csaba: Az elektronikus információs rendszerek biztonságának menedzselése, NKE, Budapest, 2014.

Muha Lajos – Krasznay Csaba: Az elektronikus információsrendszerek biztonságáról vezetőknak, NKE, Budapest, 2018.

<https://www.naih.hu/adatvedelmi-szotar> (Megtekintés ideje: 2021. 10. 22)

ORFK Kommunikációs Szolgálat: Vigyázat! SMS-ben érkezhetsz a káros kód, 2021, <http://www.police.hu/hu/hirek-es-informaciok/bunmegelozes/aktualis/vigyazat-sms-ben-erkezhetsz-a-kartekony-kod> (Megtekintés: 2021.11.11.)

Parthy, P. P., & Rajendran, G.: Identification and prevention of social engineering attacks on an enterprise, 2019 International Carnahan Conference on Security Technology (ICCST), IEEE, 2019, 1-5. o.

Pöttsch, S.: Privacy awareness: A means to solve the privacy paradox?. IFIP Summer School on the Future of Identity in the Information Society, Springer, Berlin, Heidelberg, 2008, 226-236. o.

Yeboah-Boateng, E. O., & Amanor, P. M.: Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. Journal of Emerging Trends in Computing and Information Sciences, 5/4 szám, 2014, 297-307. o.

MELLÉKLETEK:

1. sz. melléklet: Kérdőív és eredményei
2. sz. melléklet: kérdőív szöveges válaszai

1. sz. melléklet: Kérdőív és eredményei

Biztonságtudatosság felmérés

12

Válaszok

18:02

A kitöltés átlagos időtartama

Lezárt

Állapot

1. Mennyire érezd magad biztonság tudatosnak? (1 - Egyáltalán nem, 5 - Teljes mértékben)

12

Válaszok

3,75

Átlagos szám

2. Ismered a Social Engineering kifejezést?

Igen

12

Nem

0



3. Tisztában vagy a http és https kapcsolatok közötti különbséggel?

Igen

12

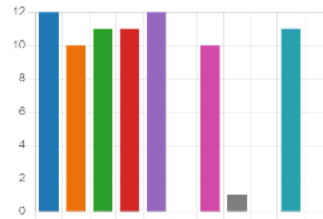
Nem

0



4. Ha a rendszer engedi, egy erős jelszónak milyen követelményeknek kell megfelelnie? (Több válasz lehetséges)

- ☒ Minél hosszabb, de legfeljebb 8 k... 12
- ☒ Kisebbséget tartalmaz. 10
- ☒ Nagybetűket tartalmaz. 11
- ☒ Számokat tartalmaz. 11
- ☒ Különböző karaktereket tartalm... 12
- ☐ Értelmes szó tartalmaz. 0
- ☐ Nem tartalmaz értelmes szót. 10
- ☐ Személyi adatai összefüggő adat... 1
- ☐ Minden rendszerben ugyanaz a... 0
- ☒ Egyedi, korábban nem használt... 11
- ☐ Adott események elmentve tárolj... 0



5. Milyen osztályozód, csoportosítód számítógépes adataid, dokumentumaid? (Kérlek foglald össze pár mondatban, vagy gondolatban!)

Legújabb válaszok

..

12
Válaszok

"tárhelyek és felhőket szerte"
"Funkcionális alapján (pl. egyetemenhez kapcsolódik, egy projekthez kapcsolódik). Ritka vagyok a tulajdonosok és típusok (pl. csatlakozó + fotók)."

6. Kérlek 1-2 mondatban foglald össze a Social Engineering lényegét:

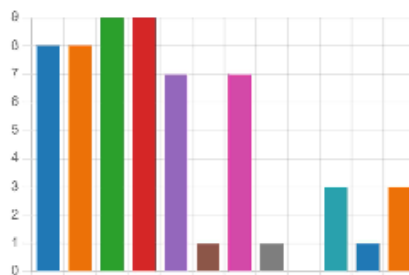
Legújabb válaszok

12
Válaszok

"humán manipulációs sérülékenységének kihasználása"
"a társasági viszonyok pszichológiai befolyásolása"
"különböző online területek kihasználása"
"Sérülékenység emberi tulajdonságok kihasználása manipuláció útján."

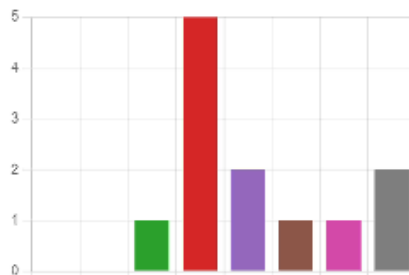
7. A legtöbb általad használt jelszó melyik követelményeknek felel meg? (Több válasz lehetséges)

- ☒ Minél hosszabb, de legálább 8 k... 6
- ☒ Kisebőit tartalmaznak. 8
- ☒ Negybetűket tartalmaznak. 9
- ☒ Számokat tartalmaznak. 9
- ☒ Különlleges karaktereket tartalm... 7
- ☐ Értelmes szót tartalmaznak. 1
- ☒ Nem tartalmazznak értelmes szót. 7
- ☐ Személyesddel összefüggő szavak... 1
- ☐ Minden rendszerben ugyanazt a... 0
- ☒ Egyedl, korábban nem használt]... 3
- ☒ Adott eszközön elmentve tárolód. 1
- ☒ Nem azonnali választás. 3



8. Körülbelül hány különböző jelszót használisz? (Kérlek szíj rá egy percet és próbáld megközelítőleg összeszámolni - munkahely, magánélet, minden szóba jöhet)

- ☒ 1 0
- ☒ 2-3 0
- ☒ 4-5 1
- ☒ 6-10 5
- ☒ 11-20 2
- ☒ 20-30 1
- ☒ 30-50 1
- ☒ 50 felett 2



9. Körülbelül hány eszköze? (Kérlek írj akár egy megközelítőleges számot, például 5-ös, vagy 10-es kerekítéssel, számold bele az applikációk, rendszerek jelszavait, stb.)



10. Mi alapján rendszerezed otthon papír alapú információid, dokumentumaid? (Kérlek foglald össze pár mondatban, vagy gondolatban!)

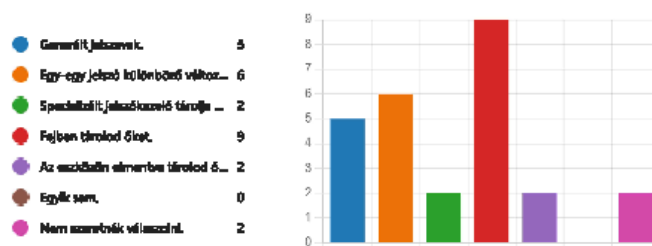


11. Az alábbiak közül melyiket nevezzed adathalászatnak (phishing)?

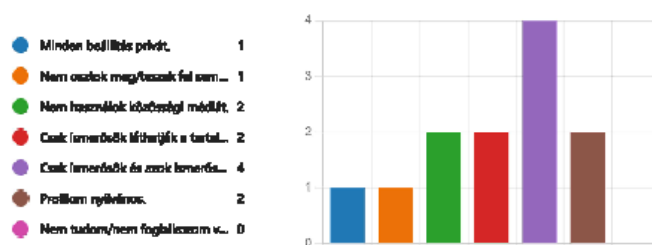
- Látványlag megbízható partnerrel... 12
- Felhasználó mágiá ábrán... 0
- Jogosultsággal rendelkező szems... 0
- Egy IT szakos (például pendrive)... 0



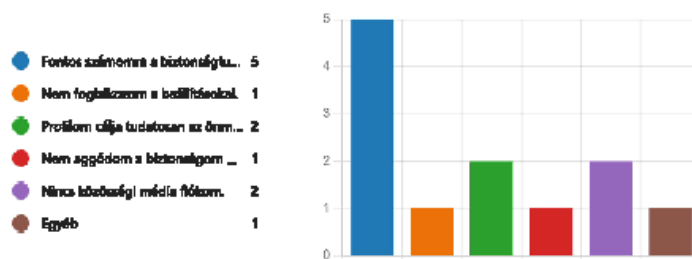
12. Az alábbiak közül melyik igaz a jelszavaidra? (Több válasz lehetséges)



13. Közösségi média oldalaidon mennyire foglalkozol a biztonsági beállításokkal? (Ha több van, kérlek válaszd azt, amelyet a legtöbbet használod)



14. Mi az oka, hogy ezeket a közösségi média beállításokat használod?

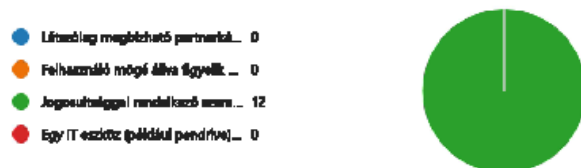


15. Mit takar a https-ben az 'S'?

12
Válaszok

Legújabb válaszok
"secure"
"secured kapcsolat"
"security"

16. Az alábbiak közül melyiket nevezzük szoros követésnek (tailgating)?



17. Milyen körültekintéssel állítanál be egy új Wi-Fi kapcsolatot, például otthoni hálózatot?



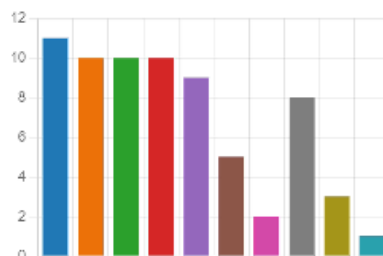
18. Milyen körülményekkel csatlakozol WI-FI-re?

- Csak az általam ismert lehetősé... 6
- Sosem csatlakozom WI-FI-re. 1
- Nem számít, milyen WI-FI, nem f... 0
- Csak a biztonságosnak tűnő leh... 5



19. Milyen biztonsági megoldásokat használ az adataid védelmére?

- Erős jelszavak. 11
- Tűzfal. 10
- Vírus/ret. 10
- Rendszert/programokat frissen tart... 10
- Kétfaktoros azonosítás. 9
- VPN. 5
- Specializált jelszókezelő program. 2
- Folyamatos ismeretbővítés. 0
- Eszközön eltávolítás. 3
- Egyéb. 1



20. Milyen logikai védelmet használ az digitális dokumentumaid megvédésére? (Kérek foglald össze pár mondatban, vagy gondolatban!)

12
Válaszok

Legújabb válaszok
 "nem szeretném megmondani :)"
 "Számítógép esetlegesen malware-vel jelszavak védelmére"
 "Hordozható eszközöknél háttértár titkosítása, biztonsági mentések."

21. Az alábbiak közül melyiket nevezzük váll szörfölésnek (shoulder surfing)?

- Látványlag megfigyelés perimetere... 0
- Felhasználó mögé állva figyelték... 12
- Jogosultsággal rendelkező személy... 0
- Egy IT eszköz (például pendrive)... 0



22. Milyen fizikai védelmet használ az papír alapú dokumentumaid megvédésére? (Kérlek foglald össze pár mondatban, vagy gondolatban!)

12
Válaszok

Legújabb válaszok
 "nem szeretném megmondani"
 "semmilyen"
 "-"

23. Hogyan biztosítod legfontosabb adataid tárolását?

- Publicus felhőszolgáltatónál (pl... 6
- Egyetemi felhőszolgáltatónál... 0
- Több pendrive-ra elhelyezve, a... 3
- Pendrive-ra elhelyezve egy mál... 2
- Egyéb... 3

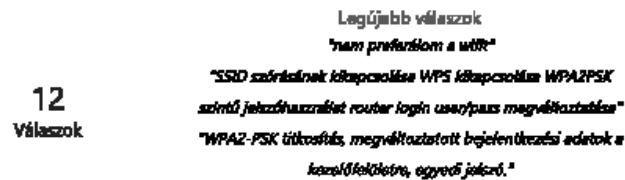


24. Miért ezt a megoldást választottad? (Kérlek foglald össze pár mondatban, vagy gondolatban!)

12
Válaszok

Legújabb válaszok
 "-"
 "Lényegében az általam használt eszközök biztonságossága miatt"
 "Rövidített időben és energiában az tűnik kivitelezhetőnek és költségtőlal irányosnak."

25. Kérek sorolj fel néhány általad preferált WI-FI hálózati biztonsági beállítást



26. Az alábbiak közül melyiket nevezzük szétszórásnak (baiting)?

- Létszálag megfigyelés perimetere... 0
- Felhasználó mégé élve ügyfélk... 0
- Jogosultsággal rendelkező usere... 0
- Egy IT eszköz (pl. táblás pendrive)... 12



27. Általánosságban hogyan biztosítod a legfontosabb digitális dokumentumaid esetében a CIA elvet? (Kérek foglald össze pár mondatban, vagy gondolatban!)



2. sz. melléklet: kérdőív szöveges válaszai

Mi alapján osztályozod, csoportosítod számítógépen adataid, dokumentumaid? (Kérlek foglald össze pár mondatban, vagy gondolatban!)

En fontosabbnak tartom a számítógémem biztonságát garantálni megfelelő vírusvedelmi szoftverrel. Sensitiv adatokat pedig próbálok nem tárolni a gépen. (Pl Jelszót, banki adatokat)

Általában a számítógépen tárolt adatokat, dokumentumokat adattartalmuk szerint csoportosítom külön mappákban. Például külön tárolok a személyes dolgaimat, külön pedig az egyetemmel kapcsolatosakat.

Elsősorban tematikai csoportosítást használok, de tevékenységi köröknek megfelelően is külön kezelem.

Dokumentumtípusok szerint. Munka, iskola, magán, játékok külön könyvtárban vannak.

Téma szerint

Év szerint, illetve azon belül topic szerint

Külön tartom a fényképeimet és a sulis dokumentumokat.

A képeimet évek, hónapok szerint mappázom, a sulis cuccokat pedig félévenként.

Lényegében nem tárolok a számítógépen semmit.

Tanulással kapcsolatos

Játékok

Filmek, sorozatok

Funkcionalitás alapján (pl. egyetemhez kapcsolódik, egy projekthez kapcsolódik), illetve vegyítem a tulajdonságot és típust (pl. családi + fotók).

témájuk és jellegük szerint

.

Kérlek 1-2 mondatban foglald össze a Social Engineering lényegét:

Az internet segítségével lényegében bármilyen adatot meg tudunk keresni, bármiről vagy bárkiről.

A Social Engineering nagyon sokféle módon is létrejöhet. A lényege a jó tulajdonságok és a jó szándék kihasználása a becsapott félben. A célja pedig adatok vagy információkat kicsalni az áldozattól.

Olyan kibertámadási fajta, amely esetén a támadó olyan viselkedésre készíti a megtámadottat, aminek következtében az önként szolgáltatja ki a támadónak a birtokában lévő adatokat és információkat.

Egy adott egyén manipulálása annak érdekében, hogy számunkra hasznos információt szerezzünk tőle.

Olyan támadási forma, mely az emberek befolyasolásán, manipulálásán alapul. Bizalmas információk megszerzésére vagy káros tevékenység elvégzésére irányul.

Az egyén befolyásolhatóságát és segítőkészségét kihasználva férnek hozzá olyan adatokhoz, infókhoz és rendszerekhez, amikhez egyébként nem lenne hozzáférésük. Főleg humán aspektusú.

Az emberek manipulálása abból a célból, hogy bizalmas információt adjanak ki illetéktelennek.

Trükkös csalás, ahol a támadó az áldozatból manipuláció segítségével nyeri ki a szükséges információt.

Egy támadó valamilyen emberi tényezőt kihasználva próbál (többnyire anyagi) haszonszerzést megvalósítani

Sérülékeny emberi tulajdonságok kihasználása manipuláció útján.

a kiválasztott célszemély pszichológiai befolyásolása különböző online tereken keresztül
humán gondolkodás sérülékenységének kihasználása

**Körülbelül hány különböző jelszót használsz?
(Kérlek szánj rá egy percet és próbáld
megközelítőleg összeszámolni - munkahely,
magánélet, minden szóba jöhet)**

**Körülbelül hány eszközre? (Kérlek írd akár egy
megközelítőleges számot, például 5-ös, vagy 10-
es kerekítéssel, számold bele az applikációk,
rendszerek jelszavait, stb.)**

4-5	25
20-30	5
6-10	25
6-10	14
11-20	5
6-10	20
6-10	25
30-50	70
11-20	10
50 felett	3
6-10	100
50 felett	80

Mit takar a https-ben az 'S'?

Az URL Titkosítását.

Azt jelenti, hogy biztonságos. Az adatátvitel titkosított csatornán zajlik.

security

Secure

Secure

Biztonságos

secure

secure

Secure

security

secured kapcsolatot

secure

Milyen logikai védelmet használsz digitális dokumentumaid megvédésére? (Kérlek foglald össze pár mondatban, vagy gondolatban!)

Elofizetett vírusirtó, jelszavas belépések. Többkulcsos azonosítás.

Jelszóval védett külső adattárolón tárolom őket, amely nem kapcsolódik online a netre. Ezenkívül van egy backup adattárolóm is.

Biztonsági mentést készítek róla időközönként, VPN, vírusirtó

Vírusirtó, tűzfal, VPN.

Több példányban tárolom őket.

.

Semmilyet

Nem tárolok semmit a számítógépen; VPN, vírusirtó, tűzfal, többkulcsos azonosítás, biztonsági mentés felhőn.

Felhasználónév, jelszóval védett programokban tárolom

Hordozható eszközön háttértár titkosítás, biztonsági mentések.

Számítógép esetlegesen merevlemez jelszavas védelme

nem szeretném megmondani ::)

Milyen fizikai védelmet használsz papír alapú dokumentumaid megvédésére? (Kérlek foglald össze pár mondatban, vagy gondolatban!)

Lakásban tárolom ahol van riasztó rendszer.

Otthon tárolom őket egy szekrényben rejtett helyen.

Zárható szekrény, zárt lakás

Semmilyet.

Bezárt, riasztóval ellátott lakásban tartom őket,

.

Semmilyet xd van riasztó és kamerarendszer a házban, de nem az én két darab papír alapú dokumentumom miatt :P

Zár, kutya, kamerarendszer, iratmegsemmisítés.

Izomerő

-

semmilyet

nem szeretném megmondani

Miért ezt a megoldást választottad? (Kérlek foglald össze pár mondatban, vagy gondolatban!)

Nem széfben de biztos helyen. Úgy gondolom ha a fizikai biztonsága megvan a hardveres eszköznek, akkor nehezen kerül illetéktelen kezekbe.

A fontosabb adatokat elrejtve kell tárolni és mindig szükséges a biztonsági mentés is, ezért kell belőle több.

Fontos a folyamatos biztonsági mentés, több eszközön való adattárolás. A felhőszolgáltatónál főként az emailben érkező adatokat tárolok.

-

Nem szeretem a felhőszolgáltatásokat

Költséghatékonyság/ráfordított energia és biztonságosság kettőssével arányos.

Mert ami egyszer az internetre felkerül, az ott is marad

Nagyon régen így alakult, s azóta elégedett vagyok vele.

Egyszerű, bárholnan hozzáférhető, viszonylag védett

Ráfordított időben és energiában ez tűnik kivitelezhetőnek és kockázatokkal arányosnak.

Lényegében az általam használt eszközök ökoszisztémája miatt

.

Kérlek sorolj fel néhány általad preferált Wi-Fi hálózati biztonsági beállítást

Router alapértelmezett jelszavainak megváltoztatása. Vendég hálózat létrehozása, mellette Mac address azonosítás az otthoni eszközökre.

Nehéz jelszót adok meg, korlátozom a Wi-Fi-re csatlakozható eszközök számát. Bizonyos portokat kikapcsolok.

Privát kapcsolat, nehéz jelszó, VPN

Erős router+hálózat pw. Guest network, ha valaki fel akar csatlakozni a hálózatomra.

Erős admin jelszó, WPA2-AES titkosítás, erős felhasználói jelszó, vendéghálózat használata a vendégeknek, tűzfal beállítása.

.

Jelszóvédelem

erős jelszó, tűzfal szabályok.

Legújabb titkosítási protokoll használata, jelszó beállítása, esetenként MAC cím alapú szűrés

WPA2-PSK titkosítás, megváltoztatott bejelentkezési adatok a kezelőfelületre, egyedi jelszó.

SSID szórásának kikapcsolása

WPS kikapcsolása

WPA2PSK szintű jelszóhasználat

router login user/pass megváltoztatása

nem preferálom a wifit

Általánosságban hogyan biztosítod a legfontosabb digitális dokumentumaid esetében a CIA elvet? (Kérlek foglald össze pár mondatban, vagy gondolatban!)
Ha például el kell küldeni valahova akkor Titkosított zip fájlban küldöm el, a jelszót pedig külön csatornán pl SMS-ben küldöm az illetőnek. Nem töltöm fel felhő alapú rendszerbe.
Csak offline kapcsolat esetén nézem meg őket. Külön adattárolón tartom ezeket jelszóval védve.
Több eszközön is tárolom, külön jelszó védi a mappát, csak biztonságos hálózaton nyitom meg
Bizalmasság, sértetlenség korábban felsorolt védelmi intézkedések halmazával.
Rendelkezésre állás: sehog. Most jöttem rá, hogy ha esetleg megadná magát valamelyik eszközöm hatalmasat szívnék.
Nem hagyom mások számára hozzáférhetően sem a digitális eszközeimet, sem a papír alapú dokumentumaimat, illetve a fontos anyagokról másolatokat készítek.
.
Bizalmasság: A számítógépet, amin a dokumentumok vannak, jelszóval védem.
Sértetlenség: Van víruskereső a gépemen.
Rendelkezésre állás: -
Magánéletben nincs olyan fontos dokumentumom, amely csak digitálisan létezne.
Munka tekintetében: VPN, tűzfal, vírusirtó, felhő backup, kettős autentikáció
Megbízható, folyamatos védelemmel ellátott szolgáltatást veszek igénybe, felhasználónév, jelszó párossal
Biztonsági mentés (A), on premise tárolás (C, érzékeny infó nem visz ki pendriveon).
.

ÖSSZEGZÉS (ANNOTÁCIÓ)

Pályafutásom során egyre több információbiztonsági tudatosító anyaggal találkozom, ami alapvetően szerintem rendkívül pozitív. Viszont szkeptikusan állok azelőtt, hogy ezek mennyire lesznek végül alkalmazva a gyakorlatban, ugyanis létezik egy úgynevezett adatvédelmi paradoxon. Dolgozatomban szerettem volna vizsgálni, hogy ez a paradoxon vajon jelen van-e egy kifejezetten erre szakosodott, kiberbiztonsági képzés hallgatói körében, emellett vajon hogyan alkalmazzák a digitális, valamint a való világban az adatbiztonsági és információbiztonsági tudásukat, intézkedéseket.

Az adatvédelem mélyebb megértéséhez előbb a releváns szakkifejezéseket ismertettem, majd különös hangsúlyt fektettem a social engineering támadások módszereibe, valamint emberközpontú és szocio-technikai alapú megközelítésébe. Ezután összegeztem a rendelkezésre álló szakirodalmat az adatvédelmi paradoxonról, megkerestem bennük a párhuzamokat, ellentéteket, valamint amiket úgy gondolom, feltétlen szükséges volt megemlítenem a megértéséhez. Vizsgáltam demográfiai tekintetben, milyen összefüggéseket lehet felfedezni, majd vizsgáltam egyéb szempontok szerint is, vajon milyen tulajdonságok lehet megmondani, hogy valaki milyen adatvédelmi beállítottsággal rendelkezik. Ezután részleteztem, mik a jelenségre a lehetséges magyarázatok, amire négy fő irányt fejtettem ki. Ezek a privacy calculus, a korlátozott racionalitás, a tapasztalat, tudás hiánya, valamint a társadalmi befolyásolás.

A kutatásom kísérlettel folytatódott, melynek 2 fő része volt. Az első egy kérdőív, melyben felmértem mind az elméleti, mind ellenőrző kérdésekkel a gyakorlati felkészültségét a célcsoportnak. A második pedig egy két részből álló adathalászat vizsgálat. A kísérlet eredménye a várakozásoknak megfelelt. A célcsoport az akadályokat legtöbbször gond nélkül, gyakran hibátlanul teljesítette. Ütköztem technikai nehézségekbe, nevesítve a spam szűrőbe, melyek áttörése komoly nehézségeket okozott, s még így sem jártam teljes sikerrel. Közben hasznos tapasztalatokat szereztem, ugyanis úgy tűnik, technikai oldalról megfelelően támogatva vannak a felhasználók, rengeteg eszköz rendelkezésükre áll, hogy biztonság tudatosan éljenek, az egyetlen dolog, ami jelenleg kérdéses, az a tényleges tudás. Ebben a célcsoportom kiemelkedően jól teljesített, ami alapján kijelenthetem, hogy rájuk tekintve az adatvédelmi paradoxon nem releváns, mind a kibertérben, mind a való világban tudatosan viselkednek, így például szolgálhatnak abban a tekintetben, hogy működh-e a tudatosítás. Ugyanis láthatólag működh.