

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

---

## **Az ellátási láncok információbiztonsággal összefüggő kihívásai és azok megítélése a munkavállalók szempontjából**

Jelige: HESOYAM

Pályamunka lezárásának időpontja:  
2023. január

2023.

## Tartalomjegyzék

|                                                                                                                                                         |           |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| Téma aktualitása .....                                                                                                                                  | 1         |
| Tudományos probléma megfogalmazása .....                                                                                                                | 2         |
| Kutatási célkitűzések .....                                                                                                                             | 2         |
| Hipotézisek .....                                                                                                                                       | 2         |
| Kutatás módszertan.....                                                                                                                                 | 3         |
| <b>1. fejezet Az ellátási láncok kibertérben felbukkanó kockázatai .....</b>                                                                            | <b>4</b>  |
| 1.1 Fogalmi meghatározás .....                                                                                                                          | 4         |
| 1.2 Potenciális információbiztonsági kockázatok .....                                                                                                   | 6         |
| 1.3 Az ellátási láncok ellen elkövetett támadások hatásai és lehetséges károk .....                                                                     | 8         |
| 1.4 Megtörtént incidensek .....                                                                                                                         | 9         |
| 1.4.1 Solar Winds-ügy .....                                                                                                                             | 9         |
| 1.4.2 Mimecast.....                                                                                                                                     | 10        |
| 1.4.3 Passwordstate esete .....                                                                                                                         | 10        |
| Következtetés.....                                                                                                                                      | 11        |
| <b>2. fejezet Az ellátási láncok információbiztonságának szabvány alapú megközelítése</b>                                                               | <b>12</b> |
| 2.1.Trusted Information Security Assessment Exchange .....                                                                                              | 12        |
| 2.2 NIST által kiadott publikációk .....                                                                                                                | 13        |
| 2.2.1 NIST Cybersecurity Framework.....                                                                                                                 | 13        |
| 2.2.2 NIST Cybersecurity Guidance for Supply Chain Risk Management .....                                                                                | 15        |
| 2.3 Az ISO 27000-es szabványcsalád.....                                                                                                                 | 16        |
| 2.3.1 ISO/IEC2700:2013 .....                                                                                                                            | 16        |
| 2.3.2 ISO 27036 .....                                                                                                                                   | 18        |
| 2.4 H1 hipotézis vizsgálata .....                                                                                                                       | 19        |
| Következtetés.....                                                                                                                                      | 20        |
| <b>3. fejezet: Az ellátási láncokkal összefüggő információbiztonsági kockázatok társadalmi megítélése, avagy a kérdőíves felmérés kiértékelése.....</b> | <b>20</b> |
| 3.1 A biztonságtudatosító oktatások szerepe .....                                                                                                       | 21        |
| 3.2 A kérdőív bemutatása és kiértékelése .....                                                                                                          | 21        |
| 3.2.1 Solar Winds kifejezés vizsgálata .....                                                                                                            | 21        |
| 3.2.2 H2 hipotézis vizsgálata .....                                                                                                                     | 24        |

|                                                                        |           |
|------------------------------------------------------------------------|-----------|
| 3.2.3 H3 hipotézis vizsgálata .....                                    | 25        |
| Következtetés.....                                                     | 27        |
| Összegzett következtetések .....                                       | 27        |
| Kutatási eredmények .....                                              | 27        |
| Eredmények hasznosíthatósága .....                                     | 28        |
| A dolgozatomban megfogalmazott eredményeim alkalmasak arra, hogy:..... | 28        |
| <b>Felhasznált irodalom.....</b>                                       | <b>29</b> |
| <b>Mellékletek.....</b>                                                | <b>31</b> |
| Rövidítések jegyzéke .....                                             | 31        |
| Ábrajegyzék.....                                                       | 32        |
| Táblázatok jegyzéke .....                                              | 32        |
| Kérdőív kérdései.....                                                  | 32        |
| Kérdőív kiértékelése .....                                             | 35        |

## Bevezetés

Téma aktualitása<sup>1</sup>

A kibertámadások fajtái és módszerei napról napra fejlődnek, újulnak meg. Az offline világhoz hasonlóan a kibertérben elkövetett bűncselekmények is egyfajta folyamatos kergetőzéshez hasonlíthatók, melyben a kiberbiztonsági szakemberek és az illetékes hatóságok üldözik a kiberbűnözőket, hackereket. A hatóságoknak és a biztonsági kutatóknak célszerű felvenni a lépést, hiszen a kiberbiztonsági incidensekből eredő gazdasági, politikai, társadalmi és következmények korántsem elhanyagolható tényezőként merülnek fel egy szervezet életében. A nagy média nyilvánosságot kapott kiberbiztonsági incidensek közül többek közt a Solar Winds-ügy is rávilágított arra a tényre, miszerint egyre növekvő tendenciáról beszélhetünk ellátási láncok elleni támadásokkal (supply chain attack), valamint a szoftver ellátási láncokkal (software supply chain attack) kapcsolatban. Ezek alapján megállapíthatjuk, hogy vállalatok belső informatikai és operatív technológiai rendszereinek védelme közel sem elegendő, egyaránt szükséges figyelmet fordítani a gyártóktól és beszállítóktól elvárható biztonsági követelményekre.

Az ellátási láncok ellen elkövetett kibertámadások azért bizonyulhatnak olykor meglehetősen szofisztikáltnak, mert nem közvetlenül a célzott szervezetet támadják, hanem a köztes feleket, ezért nem minden esetben lehet pontosan eldönteni, melyik szervezet bizonyul a támadás végső célpontjának, vagy milyen célból történt maga a támadás. Egy adott termékben (szoftver, alkalmazás vagy konkrét rendszer) található sebezhetőséget használják ki, s első lépésként célpontba vesznek egy beszállítót, gyártót, akinek termékét alkalmazza a valószínűsített végső célpont. Becslések szerint a vállalatok 56%-a tapasztalt olyan incidenst, amelyet valószínűsíthetően valamelyik szállítója okozott.<sup>2</sup> A Kaspersky kiberbiztonsági cég szerint pedig egy-egy vállalatot ért ellátási lánc elleni támadás átlagos gazdasági költsége 2021-ben 1,4 millió USD volt, ami magasabb, mint az összes többi kibertámadás esetében elköltött összeg.<sup>3</sup>

---

<sup>1</sup> A dolgozat az Innovációs és Technológiai Minisztérium ÚNKP-22-2-I-NKE-42 kódszámú Új Nemzeti Kiválósági Programjának szakmai támogatásával készült

<sup>2</sup> Zachary A. Collier és Joseph Sarkis, „The zero trust supply chain: Managing supply chain risk in the absence of trust”, *International Journal of Production Research* 59, sz. 11 (2021. június 3.): 3430–45, <https://doi.org/10.1080/00207543.2021.1884311>.

<sup>3</sup> N. Kshetri, „Economics of Supply Chain Cyberattacks”, *IT Professional* 24, sz. 3 (2022): 96–100, <https://doi.org/10.1109/MITP.2022.3172877>.

## Tudományos probléma megfogalmazása

Jelen kutatási terv tudományos problémáját a fentebb meghatározott jelenség adja: globális ellátási lánc több fronton is sebezhető és egyes ágazatokban folyamatos támadásoknak van kitéve. A sikeresen elkövetett kibertámadások jelentős reputációs, közvetett anyagi és társadalmi károkhoz vezethetnek.<sup>4</sup> A kiemelt beszállítók, gyártók felé támasztott információbiztonsági követelmények betartatása, auditálása ma már elengedhetetlen bizonyul egy szervezet hatékony működéséhez, azonban ez sok esetben csak feleslegesnek érzett plusz feladatként és nyűgként kezelik a szervezetek, munkavállalók. Tudományos problémaként kezelem továbbá azt a jelenséget, hogy a munkavállalók jelentős része a biztonság tudatosító képzések ellenére alapszinten sincsenek tisztában az éppen aktuális támadási trendekkel, annak ellenére, hogy ez hozzájárulhatnak nem csak az ellátási láncok ellen elkövetett kibertámadások megelőzéséhez, hanem más jellegű incidensek preventálásához is.

## Kutatási célkitűzések

Kutatásom során célnak tekintem feltárni a gyártók, beszállítók által lehetségesen generált kiberbiztonsági kockázatokat, valamint azt az eszközrendszert, szabványokat és ajánlásokat, amelyek implementálása esetlegesen kiegészíthetik a már meglévő jó-gyakorlatokat és hozzájárulhatnak a támadások megelőzéséhez vagy a már bekövetkezett incidensek következményeinek enyhítéséhez.

Kutatásom céljának tekintem még megvizsgálni, hogy a munkavállalók mennyire vannak tisztában azzal, hogy akár egy harmadik fél által is sújthatja szervezetét információbiztonsági incidens, továbbá, hogy milyen mértékben ítéli veszélyforrásnak, kockázatnak az ilyen jellegű támadásokat.

## Hipotézisek

A kutatásom során az alábbi hipotéziseket fogalmaztam meg:

H1: Jelenleg nem létezik olyan iparágakon átívelő szabvány, ajánlás vagy keretrendszer, amely teljeskörűen kezeli a komplex információbiztonsági kockázatokat az ellátási láncok vonatkozásában.

H2: A közszférában foglalkoztatottak átlagosan nagyobb kockázatnak minősítik az ellátási láncok ellen irányuló támadásokat, mint azok, akik a versenyszférában dolgoznak.

---

<sup>4</sup> Collier és Sarkis, „The zero trust supply chain”.

H3: Azok a munkavállalók, akik részt vesznek minimum évenkénti rendszerességgel információbiztonsági tudatosító oktatáson, valószínűbbnek gondolják, hogy az elkövetkezendő 5 évben ellátási lánc ellen irányuló támadást szenved a szervezetük.

#### Kutatás módszertan

Az adatgyűjtés fázisához egy kérdőívet hívok segítségül, mellyel célom megvizsgálnia munkavállalók hozzáállását az ellátási láncokat érintő kibertámadásokkal kapcsolatban. A kérdőív kiértékelését Mann-Whitney U teszttel valósítottam meg. Ezen felül pedig alaposan megvizsgálom azokat a szabványokat, ajánlásokat, amelyek ezt a kérdéskört dolgozzák fel és jógyakorlatokat, valamint kontrollokat fogalmaznak meg az ellátási láncok biztonságának érdekében.

## 1. fejezet Az ellátási láncok kibertérben felbukkanó kockázatai

Mindenekelőtt az első fejezetben kísérletet teszek alaposan definiálni fogalmakat, tisztázni azon a tartalmi eltéréseket, amelyek a különböző tudományágbeli értelmezések végett merülhetnek fel.

### 1.1 Fogalmi meghatározás

Az ellátási lánc fogalma a nemzetközi és a hazai szakirodalomban egyaránt viszonylag egységes, kiforrott. A fogalom szövegszerű meghatározása ugyan sokszor eltér egymástól, tartalmi vonatkozásokban azonban konszenzus van kialakulóban. Ennek a konszenzusnak alapvetően három elhanyagolhatatlan eleme van:

- az ellátási lánc alapvető célja fogyasztói igények kielégítése;
- az ellátási lánc több együttműködő piaci szereplő között értelmeződik;
- alapvetően az értékteremtésben szereplő reálfolyamatokat, illetve azok rendszerét foglalja magában.<sup>5</sup>

Ezek alapján elmondható, hogy Chickán Attila és Gelei Andrea (és rajtuk kívül még jópár nemzetközi szakirodalom szerzője) általános megközelítésben az ellátási láncot értékteremtő folyamatok és erőforrások összehangolt rendszereként értelmezi, amely több vállalatot érintve a végtermék fogyasztóhoz történő eljuttatásával fejeződik be.<sup>6</sup> Az ellátási láncok vizsgálata interdiszciplináris tématerületnek bizonyul, hiszen menedzsmenttudományi és logisztikai kötődése mellett kiberbiztonsági aspektusból is meg lehet vizsgálni azokat, dolgozatomban erre fogom fektetni a hangsúlyt.

Ha kiberbiztonsági szempontból közelítjük meg a témakört, egyfajta anomáliával találkozhatunk a definíciókkal kapcsolatban, ugyanis nem beszélhetünk egységes, kiforrott fogalom meghatározásról a nemzetközi szakirodalomban sem. Adott két angol kifejezés, ellátási láncok elleni támadások (supply chain attack, továbbiakban: SCA), valamint a szoftver ellátási láncok (software supply chain attack, továbbiakban: SSCA), amelyeket számos nemzetközi publikáció egybeemos, egyenlőként kezel. Egyes szakirodalmak szerint a határvonal a két fogalom között a célpont jellegétől függ, miszerint SCA-ról beszélhetünk, például a Maersk és a Fedex logisztikai óriások ellen elkövetett kibertámadások esetében, melynek hattárében a híres NotPetya zsarolóvírus állt.<sup>7</sup> Ezekben az esetekben maga az incidens direkt

---

<sup>5</sup> Gelei Andrea, „Az ellátási lánc típusai és menedzsmentkérdései”, *Vezetéstudomány - Budapest Management Review* 34, sz. 7–8 (2003. július): 24–34.

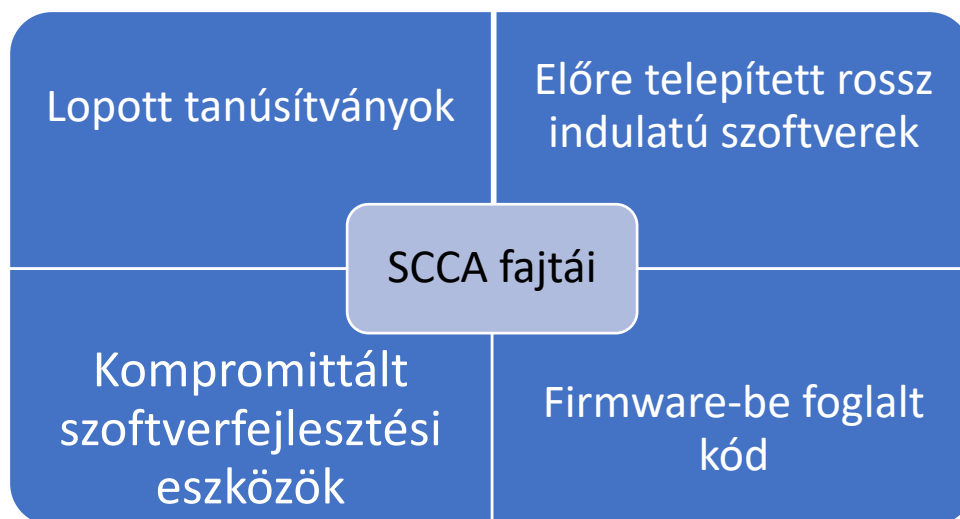
<sup>6</sup> Bányász Péter „Az ellátási lánc kiberfenyegetettsége, különös tekintettel a közlekedési alrendszer biztonságára, a szervezett bűnözés hatásai”, 2016, 643-673.

<sup>7</sup> „A háború Ukrajnában az ellátási láncokat is érinti- nem csak Ukrajnában”, Trans.INFO, elérés 2022. szeptember 4., <https://trans.info/hu/haboru-ukrajnaban-276920>.

hatásokat fejtett ki az ellátásra láncokra vonatkozóan. Eszerint az értelmezés szerint SCCA pedig akkor következik be, amikor a támadók megpróbálnak egy meglévő sérülékenységet kihasználni, hogy jogosultságot szerezzenek és hozzáférjenek egy adott gyártó vagy beszállító szoftverrendszeréhez. Tulajdonképp ez a módszer lehetővé teszi, hogy nincs szükség a hackereknek megtámadni a tényleges célpontot „csupán” elég csak egy harmadik félt, aki a végleges célpontnak terméket vagy szolgáltatást szállít be, erre a támadás típusra kitűnő példa a Solar-Winds ügy. A támadás típus olyannyira kockázatosnak bizonyult már az elmúlt években az Egyesült Államokban, hogy külön munkacsoportot hoztak a Védelmi Tudományos Testületen<sup>8</sup> belül, ahol foglalkoznak a kérdéssel.

A szervezetek, vállalkozások digitalizációja már évek óta zajlik, így beleértve az ellátási láncokat is. Az ellátási láncok egyre inkább összekapcsolt környezetben működnek, amely az emberek, folyamatok és a kétezres évektől kezdve már eszközök együttműködésén is alapul. A cégek egyre gyakrabban osztanak meg információkat, személyes adatokat, szoftver kódokat, és alkalmazás specifikációkat az általuk megbízhatónak titulált partnerekkel, beszállítókkal és alvállalkozókkal, ezáltal folyamatosan nő egy potenciális kibertámadás kockázata.<sup>9</sup>

Az SCCA-nak több fajtája létezik, amelyek mindegyike a vállalatok által megbízhatónak vélt megoldások biztonsági sérülékenységeinek létrehozásával vagy kihasználásával jár. Ezek a következők:



1. ábra SCCA fajtái (saját szerkesztés, forrás: Fortinet)<sup>10</sup>

<sup>8</sup> Civil szakértőkből álló bizottság, amelyet az USA Védelmi Minisztériumának tudományos és műszaki kérdésekben történő tanácsadására neveznek ki.

<sup>9</sup> „Who cares? Supply chain managers’ perceptions regarding cyber supply chain risk management in the digital transformation era | Emerald Insight”, elérés 2022. szeptember 4., <https://www.emerald.com/insight/content/doi/10.1108/SCM-02-2020-0073/full/html#sec001>.

<sup>10</sup> <https://www.fortinet.com/resources/cyberglossary/supply-chain-attacks>.)

Lopott tanúsítványokról beszélünk, ha egy hacker olyan tanúsítványt tulajdonít el, amelyet egy adott vállalat a saját termékének jogszerűségéért vagy biztonságának prezentálásáért használ. Ezzel a módszerrel kvázi rosszindulatú kódot terjeszthet a vállalat tanúsítványának álcája alatt. Kompromittált szoftverfejlesztési eszközök vagy infrastruktúra esetén a hackerek kihasználják a szoftverfejlesztésre szolgáló eszközöket, hogy sérülékenységeket szűrjanak be még a fejlesztés folyamatában azelőtt, hogy az adott szoftver vagy alkalmazást végleges béta verziója megjelenjen. Az eszközökre előre telepített rosszindulatú szoftverekről akkor beszélhetünk a hackerek rosszindulatú kódokat telepítenek telefonokra, USB-meghajtókra, kamerákra és más mobil eszközökre majd, amikor a célpont csatlakoztatja azt a rendszeréhez vagy hálózatához, rosszindulatú kódot juttathatnak be.<sup>11</sup> Ehhez képest az alkatrészek firmware-jébe<sup>12</sup> foglalt kódnál a hackerek rosszindulatú kódot is injektálhatnak a firmware-be, hogy hozzáférjenek egy rendszerhez vagy hálózathoz.<sup>13</sup> Természetesen ez csak egy elméleti megközelítése a jelenségnek, a gyakorlatban a támadók a legszofisztikáltabb módokon igyekeznek kihasználni a sérülékenységeket, annak érdekében, hogy elérjék kártékony céljukat. Olykor ötvözik ezeket a fajtákat, máskor pedig egy teljesen más módszert alkalmazva kísérleteznek. Az ilyen támadások során a hacker elsődleges célja, tulajdonképp ugyanaz, mint bármelyik más kibertámadás esetében: befolyásolja egy végrendszer bizalmasságát, integritását és/vagy rendelkezésre állását és végső soron az általa nyújtott folyamatokat, szolgáltatást.

A szakirodalmak vizsgálata alatt konstatáltam, hogy a különböző szakmai publikációk, ajánlások nem különböztetik meg az ellátási lánc ellen elkövetett kibertámadást, a szoftver ellátási lánc kibertámadásától, hanem egységesen beszélnek ellátási lánc ellen elkövetett kibertámadásról, így dolgozatomban én is ezt a terminológiát fogom követni.

## 1.2 Potenciális információbiztonsági kockázatok

A modern üzleti környezetben az egyes vállalkozások nem önálló entitásként versenyezhetnek, hanem a szélesebb ellátási lánc aktív tagjaként, amely több üzletből és kapcsolatrendszerből áll. Napjaink globális ellátási láncai számos különféle kockázatnak van kitéve, amelyek bármelyike

---

<sup>11</sup> . Ez a támadási típus talán már annyira nem gyakori, mint a korábbi években, hiszen számos szervezet esetében meg van tiltva a mobil adathordozók használata, sőt gyakran egyenesen a portokat tiltják le az adott számítógépeken a megelőzés érdekében.

<sup>12</sup> Olyan szoftver, amely alapvető gépi utasításokat ad és amely lehetővé teszi a hardver működését és a kommunikációt az eszközön futó más szoftverekkel.

<sup>13</sup> „Supply Chain Attacks: Examples and Countermeasures”, Fortinet, elérés 2022. szeptember 10., <https://www.fortinet.com/resources/cyberglossary/supply-chain-attacks>.

átmenetileg megzavarhatja a cég működését.<sup>14</sup> Az ellátási láncok egyik lehetségesen felmerülő kockázata az információbiztonsági kockázatok halmaza, amelyet ma már a szervezeteknek más kockázatoktól elkülönítve érdemes kezelni.

A digitalizációs folyamatok jelentősen átalakították az irodai munkakörnyezetet. Megváltoztak a pénzügyi, értékesítési, karbantartási, logisztikai folyamatok, továbbá ellátási lánc folyamatait is. Ennek következtében a munkavállalók átalakult munkafolyamatokkal szembesülnek, amelyek szélesebb körű új kompetenciákat igényelnek. Mivel munkájuk automatizáltabb, összekapcsoltabb és interdiszciplinárisabb, olyan kompetenciákat kell megszerezniük és fejleszteniük, amelyek egyre sokrétűbbek. A kompetenciák jelentős része technológiával kapcsolatosak, és az informatikai alapkészségeken alapulnak.<sup>15</sup> Ahhoz, hogy a szervezetek túléljenek és egyaránt fejlődjenek a jelenlegi összetett és folyamatosan változó piaci és globális környezetben, mára már elengedhetetlen az agilitás és a magas szintű kiberreziliencia, kockázatcsökkentési képesség, továbbá strukturális rugalmasságot kell kiépíteniük, amely lehetővé teszi a különböző kihívásokra való gyors reagálást beleértve az információbiztonsági incidensekre történő reagálást is.<sup>16</sup>

Az információbiztonsági kockázatok és hatásaik jelentősége az elmúlt néhány évben jelentősen megnőtt. Ezt az Allianz Kockázati Barométer 2022-es jelentése is hangsúlyozta, miszerint a globálisan megjelenő legfőbb üzleti kockázatok rangsorának első két helyén a kiberbiztonsági események és az üzletmenet megszakadása áll. Fontosnak tartom megemlíteni, hogy ugyanezen ranglistán 2013-ban még csak a 15. helyen tűntek fel ugyanezen kockázatok. Ahogy azt a bevezetésben is említettem, az ilyen támadásoknak az kiemelkedő tulajdonsága, hogy nincs szükség direktbe megtámadni a célpontba vett szervezetet, hanem tulajdonképp az ellátási lánc bármely részéről eredhetnek. Az aggodalomra okot adó tény, hogy az ilyen és ehhez hasonló támadások száma folyamatosan növekszik. Továbbá az ellátási láncok információ technológiától való függése jelentősen megnőtt az elmúlt években és ez nagy valószínűséggel a jövőben is így lesz. Az olyan feltörekvő technológiák és trendek, mint a 3D-nyomtatás, az e-kereskedelem, az Ipar 4.0, a dolgok internete, és az intelligens otthonok, megnövelték a sebezhetőségek számát.

---

<sup>14</sup> Jay Simon és Ayman Omar, „Cybersecurity Investments in the Supply Chain: Coordination and a Strategic Attacker”, *European Journal of Operational Research* 282, sz. 1 (2020. április 1.): 161–71, <https://doi.org/10.1016/j.ejor.2019.09.017>.

<sup>15</sup> Blandine Ageron, Omar Bentahar, és Angappa Gunasekaran, „Digital supply chain: challenges and future directions”, *Supply Chain Forum: An International Journal* 21, sz. 3 (2020. július 2.): 133–38, <https://doi.org/10.1080/16258312.2020.1816361>.

<sup>16</sup> Martin Christopher és Matthias Holweg, „Supply Chain 2.0”: managing supply chains in the era of turbulence”, szerk. Michael Crum és Richard Poist, *International Journal of Physical Distribution & Logistics Management* 41, sz. 1 (2011. január 1.): 63–82, <https://doi.org/10.1108/09600031111101439>.

Az információs technológián kívül maga a szervezet létszáma is lehet abban befolyásoló tényező. A kis-és középvállalkozások (továbbiakban: kkv) gyakran fontos szerepet töltenek be az ellátási láncban belül, mivel innovatív és/vagy réstermékeket állítanak elő, ezért megannyiszor szállítanak be terméket nagyobb vállalatok számára, így kulcsfontosságú elemnek bizonyulhatnak, azonban nagyobb kockázati tényezőként is megjelenhetnek egy szervezet életében.<sup>17</sup> Mindez szimplán annak tudható be, hogy a kisebb szervezetek jellemzően kevesebb információbiztonságra fordítható pénzügyi kerettel rendelkeznek, ezáltal sérülékenyebbé válhatnak. Fontosságuk ellenére a kkv-beszállítók gyakran a többszintű ellátási lánc leggyengébb elemei és a hackerek és hacker szervezetek gyakori célpontjai. Abban az esetben, ha egy adott kkv-nek szolgáltatói szerep jut gyakran elsőrangú beszállítóként tekintenek rá és így hozzáférhetnek olyan szenzitív adatokhoz, amelyek mind a sebesség, mind a támadás terjedésének mértéke szempontjából elősegíthetik a kibertámadást.

Az amerikai terminológiában kisvállalatnak számító szervezetekről (1-100 közé esik a foglalkoztatottak száma) a Verizon által készített jelentés alapján kiderült, hogy 2018-ban az adatszivárgási vizsgálati jelentésében elemzett számítógépes incidensek teljes számának 92 százalékát ezek a szervezetek tették ki.<sup>18</sup>

Továbbá ne felejtjük el azt a tényezőt se, hogy a végpontokon emberek végzik a mindennapi munkát, így a figyelmetlenség, gondatlanság folyamatos kockázati tényezőként szerepel.

### 1.3 Az ellátási láncok ellen elkövetett támadások hatásai és lehetséges károk

A közelmúltban történt kiberbiztonsági incidensek kiválóan rávilágítottak a gazdasági, politikai és társadalmi hatásokra, azonban a sikeresen véghez vitt támadásból eredő károk ezeken kívül még sokféle más formát is ölthetnek.

Ha a klasszikus logisztikai értelemben vett az ellátási láncok ellen elkövetett támadások hatásait vizsgáljuk, komoly fennakadásokat okozhatnak a logisztikában, a termelésben és a működésben, valamint adatvesztés is könnyen kialakulhat<sup>19</sup>. A beszállítók, gyártók ellen indított támadások megzavarhatják a működést, ami a teljes ellátási láncra negatív hatást

---

<sup>17</sup> „Supply Chain Security Guidance”, elérés 2022. szeptember 8., <https://www.ncsc.gov.uk/collection/supply-chain-security>.

<sup>18</sup> Steven A. Melnyk és mtsai., „New challenges in supply chain management: cybersecurity across the supply chain”, *International Journal of Production Research* 60, sz. 1 (2022. január 2.): 162–83, <https://doi.org/10.1080/00207543.2021.1984606>.

<sup>19</sup> Suhaiza Hanim Zailani és mtsai., „The impact of supply chain security practices on security operational performance among logistics service providers in an emerging economy: Security culture as moderator”, szerk. Dr Daniel Ekwall and Dr Bobby J. Martens Dr Jennifer Blackhurst, *International Journal of Physical Distribution & Logistics Management* 45, sz. 7 (2015. január 1.): 652–73, <https://doi.org/10.1108/IJPDLM-12-2013-0286>.

gyakorolhat. Fontos látni, hogy működés, termelés megszakítása többletköltséggel járhat az ellátási láncban nem csak konkrétan a megtámadott szervezet számára, de több más vállalat számára is, annak érdekében, hogy visszatérjenek az eredeti működési állapothoz. Ez a hatás a késéseken túlmenően készlethiányhoz, valamint a megszakítások ellensúlyozása érdekében gyorsított szállítási költségekhez is vezethet.<sup>20</sup>

Egy ellátási lánc ellen elkövetett kibertámadás gyakran generál adatszivárgásokat, amely jelentős reputációs kockázattal jár, így hatással lehet a szervezet márkájára és pénzügyi teljesítményére is, továbbá akár ügyfelek jóindulatának és bizalmának elvesztésével is számolni kell.

#### 1.4 Megtörtént incidensek

Kétségtelen, hogy a már korábban megtörtént biztonsági incidensek forgatókönyvének elemzésével tudnak a legjobban a szakemberek felkészülni egy potenciálisan bekövetkezendő új támadásra. A legideálisabb hozzáállásnak az bizonyul, ha az elemzés során szerzett tapasztalatot folyamatosan integrálják a szervezet biztonsági intézkedéseinek sorába, ezzel is frissen tartva a megelőző intézkedések, továbbá az információbiztonsági oktatásban is megjelenik egyfajta egyszerűsített formában. Ezen logika mentén igyekszem ebben az alfejezetben prezentálni pár megtörtént esetet. Az alábbi példák mindegyikében megbízhatónak titulált beszállító rendszereit vagy szoftvereit támadták meg.

##### 1.4.1 Solar Winds-ügy

A sort a korábbiakban már többször említett Solar Winds-üggyel kezdem, ezzel kapcsolatban az általam készített kérdőívben is találtak kérdést a kitöltők. A Solar-Winds egy szoftvercég, amely rendszerfelügyeleti eszközöket biztosít hálózat- és infrastruktúra-felügyelethez, valamint egyéb műszaki szolgáltatásokat nyújt szervezetek százezrei számára szerte a világon. A cég termékei között szerepel az Orion nevű informatikai teljesítményfigyelő rendszer is. Az Orion kiváltságos hozzáféréssel rendelkezik az IT-rendszerekhez, annak érdekében, hogy napló- és rendszerteljesítménnyel kapcsolatos információkat kapjon. Emiatt a kiváltságos helyzet miatt vált az alkalmazás jövedelmező célponttá.<sup>21</sup> Több mint 30 000 állami és magánszervezet használja az Orion hálózatkezelő rendszerét informatikai erőforrásaik kezelésére. Ez a

---

<sup>20</sup> Simon és Omar, „Cybersecurity Investments in the Supply Chain”.

<sup>21</sup> „SolarWinds hack explained: Everything you need to know”, elérés 2022. szeptember 10., <https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know>.

harmadik féltől származó szoftver egy úgynevezett backdoor<sup>22</sup> hozott létre, amelyen keresztül a hackerek hozzáférhetnek az áldozatszervezetek felhasználóihoz és fiókjaihoz, és megszemélyesíthetik azokat. A Sunburnst elnevezésű backdoor a SolarWinds.Orion.Core.BusinessLayer.dll nevű digitálisan aláírt SolarWinds Orion bővítmény trójai<sup>23</sup> változata. A kezdeti, legfeljebb kéthetes nyugalmi időszak után a SUNBURST olyan parancsokat hajthat végre, amelyek a hátsó ajtón keresztül fájlok átvitelére, fájlok végrehajtására, a rendszer profilozására, a rendszer újraindítására és a rendszerszolgáltatások letiltására képes. A rosszindulatú program a rendszerfájlokhoz is hozzáférhetett anélkül, hogy bármely kártékony kód elleni szoftver észlelné. A feltörés célja nagyrészt ismeretlen, egyelőre az sem világos, hogy a hackerek milyen információkat loptak el a szervektől, de a hozzáférés szintje mélynek és szélesnek tűnik.

#### 1.4.2. Mimecast

Az 1.1 pontban kifejtett SCCA fajtái közül a lopott tanúsítvány fajtára kitűnő példát jelent a Mimecast vállalat elleni megtörtént támadás. A Mimecast egy amerikai-brit vállalat, amely felhőalapú e-mail-kezelésre szakosodott konkrétan Microsoft Exchange és a Microsoft Office 365 számára, beleértve a biztonsági, archiválási és folytonossági szolgáltatásokat. A támadás során a hackerek képesek voltak kompromittálni egy biztonsági tanúsítványt, amely hitelesíti a Mimecast szolgáltatásait a Microsoft 365 Exchange Web Services-en. A szóban forgó tanúsítvány a következő 3 szolgáltatás kapcsolatának ellenőrzésére és hitelesítésére használják:

- Mimecast Sync and Recover, amely a postafiókok mappaszerkezetének, naptári tartalmának és névjegyének biztonsági mentése az Exchange On-Premises vagy Microsoft 365 postafiókokból,
- Continuity Monitor, amely e-mail forgalomban bekövetkező zavarokat keresi,
- Internal Email Protect, pedig a belsőleg generált e-maileket ellenőrzi rosszindulatú linkek, mellékletek vagy érzékeny tartalom szempontjából.

Bár a vállalat ügyfeleinek csupán 10 százaléka használja az érintett kapcsolatokat, ennek ellenére biztonsági kutatók a Solar Winds támadással húztak párhuzamot.<sup>24</sup>

#### 1.4.3. Passwordstate esete

---

<sup>22</sup> A backdoor jelentése szó szerinti jelentése hátsó ajtó. Olyan támadó program, amely összeköttetést biztosít a támadó és a megtámadott számítógép között, a megtámadott tudomása és engedélye nélkül adatokat tölthet le, ill. átveheti a megtámadott gép vezérlését.

<sup>23</sup> Rosszindulatú szoftver, amely titokban mást csinál mint amit a felhasználóknak mutat, vagy ami miatt telepítve lett.

<sup>24</sup> „Mimecast Certificate Hacked in Microsoft Email Supply-Chain Attack”, elérés 2022. szeptember 11., <https://threatpost.com/mimecast-certificate-microsoft-supply-chain-attack/162965/>.

A Passwordstate egy jelszókezelő megoldás, amelyet világszerte 29 000 vállalat több mint 370 000 biztonsági és informatikai szakembere használ.<sup>25</sup> Ügyféllistáján cégek szerepelnek az iparági vertikumok széles skálájáról, ideértve a kormányzat, a védelem, a pénzügy, a repülés, a kiskereskedelem, az autóipar, az egészségügy és a média szektort is. A Passwordstate támadója a jelszókezelő frissítési funkcióját kompromitálta és egy rosszindulatú programot illesztett a frissítésbe, amely információkat gyűjt össze például a számítógép nevét, felhasználónevét, tartománynevét, futó folyamatokat, továbbá proxykiszolgáló címét.<sup>26</sup>

#### Következtetés

Összességében elmondhatjuk, hogy legtöbb szervezet korlátozott rálátással rendelkezik az ellátási láncára, partnereire azon belül is a szoftver beszállítókra. Bármely harmadik fél, amely nincs megfelelően védve és szoftvert vagy szolgáltatásokat nyújt nagyobb szervezetek számára, már önmagába kockázatot jelent. Azt is megállapíthatjuk, hogy a támadók leggyakrabban az ellátási lánc leggyengébb láncszemeit keresik, például az olyan (kis méretű) szállítókat veszik célba, akiknek nincs, vagy meglehetősen laza biztonsági intézkedésekkel rendelkeznek. Többek között ezért a probléma miatt válnak relevánssá az információbiztonság témakörében végzett vevőauditok vagy azok az iparági szabványok, amelyek szigorú követelményrendszert állítottak fel minden egyes beszállító, gyártó számára. Az első fejezetben egyfajta betekintőt igyekeztem nyújtani a folyamatosan jelenlévő kockázati faktorra, amellyel a legtöbb szervezetnek meg kell küzdenie annak érdekében, hogy hatékony, de ugyanakkor biztonságos munkavégzésre tegyen szert beszállítóival, üzleti partnereivel folytatott közös munka során.

---

<sup>25</sup> „Supply Chain Attack Hits Passwordstate Password Manager”, Decipher, elérés 2022. szeptember 12., <https://duo.com/decipher/supply-chain-attack-hits-passwordstate-password-manager>.

<sup>26</sup> „What Is a Supply Chain Attack? Solutions & Examples | Keeper”, elérés 2022. szeptember 12., <https://www.keepersecurity.com/threats/supply-chain-attack.html>.

## **2. fejezet Az ellátási láncok információbiztonságának szabvány alapú megközelítése**

A második fejezetben a prevencióra fektetem a hangsúlyt. Igyekszem betekintést nyújtani olyan információbiztonsággal kapcsolatos szabványok, ajánlások és keretrendszerek tematikájába, amelyek kitérnek a beszállítók által esetlegesen generált információbiztonsági kockázatok elleni védelemére, s ezzel egyidőben vizsgálom H1 hipotézisemet.

Az információbiztonság területén számos olyan szabvány, keretrendszer létezik, amely olyan követelményeket, kontrollpontokat foglal össze, melynek betartása, implementálása elősegítheti az biztonságos szervezeti működést. Ezek közül néhány egyfajta útmutatót igyekszik nyújtani, mely útmutató kötelezettségeket nem keletkeztet, csupán csak a jó gyakorlatokat foglalja össze. Akadnak azonban olyanok is, amelyek olykor egy külső, független tanúsító testület auditál annak érdekében, hogy megállapítsa megfelel-e az adott szervezet a felsorolt követelményeknek. Továbbá léteznek olyan szabványok, amelyek konkrétan csak egy iparágra vonatkozóan fogalmazzak meg elvárásokat.

### **2.1. Trusted Information Security Assessment Exchange**

A sort a Trusted Information Security Assessment Exchange (továbbiakban: TISAX) modellel kezdem. A TISAX modell a német Autóipari Szövetség (Verband der Automobilindustrie, továbbiakban: VDA) által direkt az autóipar szereplői számára létrehozott követelményrendszer, amely nagymértékben támaszkodik a széles körökben elterjedt ISO/IEC27001 szabványra. A TISAX modell segítségével az autóipari beszállítók megmutathatják elkötelezettségüket az információbiztonság iránt, mindezt független fél által aláíratva.<sup>27</sup>

Az információbiztonság különösen nagy jelentőséggel bír az autóipari vállalatok számára. Világszerte lépnek kölcsönhatásba beszállítókkal és gyakran kereskedelmi szempontból érzékeny és bizalmas információkat kell kicserélniük pl. termékterveket, vagy információkat technológiai kutatási projektekké vagy üzleti tervekkel kapcsolatban. Az autóiparban új prototípusokat gyakran 3D nyomtatással készítenek, a külső információcsere alvállalkozókkal és a beszállítókkal való kommunikáció biztonsága kulcskérdés a prototípusok és a know-how védelme végett. Kezdetben a TISAX szabvány elsősorban kizárólag a német ipar vállalatait foglalta magában, mára már más európai vállalatokra is kiterjedt, a világ minden táján alkalmazzák.

---

<sup>27</sup> „TISAX - A megfelelésen túl | Deloitte Magyarország”, Deloitte Croatia, elérés 2022. szeptember 19., <https://www2.deloitte.com/hu/hu/pages/fogyasztoi-agazat/articles/tisax----a-megfelelesen-tul---deloitte-magyarorszag.html>.

A TISAX lényegében egyfajta önértékelési rendszer. A kritériumok implementálását követően úgynevezett TISAX „label” -t szerezhet meg az adott szervezet, ennek megszerzéséhez és fenntartásához az autóiipari beszállítóknak igazolniuk kell, hogy megfelelnek az információbiztonság biztosításához a kritériumoknak. Az erre vonatkozó értékelés alapja az ISA (Information Security Assessments) követelmény katalógusa, amely egy ingyenesen elérhető excel táblázatként megtalálható az ENX (European Network Exchange) platformon, amely egy olyan információcsere portál, ahol a regisztrált szervezetek tudják saját eredményeiket megosztani, vagy más beszállítót ellenőrizni.<sup>28</sup>

Általánosságban elmondható, hogy a kisebb méretű autóiipari beszállítók ugyanazon ellátási láncban szereplő nagyobb szervezet kérésére vágnak bele az önértékelési folyamatba. Ez a gyakorlat Magyarországon meglehetősen gyakori, hiszen számos magyar kis- és középvállalkozás gyárt olyan alkatrészeket, terméket, amelyeket aztán valamely német autógyártónál kötnek ki. Az adott akkreditált testület által végzett auditot követően az eredményeket a kérelmező szervezet rendelkezésére bocsátják. Az ellenőrzött vállalat különböző részletességgel elérhetővé teheti saját eredményeit a többi TISAX résztvevő számára az ENX platformon. A TISAX alapvető lényege, hogy egységsített követelményrendszert szolgáltasson az autóiipari ellátási láncok szereplőinek. Ezzel az egységsített modellel a szereplők elkerülhetik a más információbiztonsági auditok nyomán felbukkanható költségeket, továbbá az sem elhanyagolható tényező, hogy a TISAX egyfajta versenyelőnyhöz is juttathatja a szervezeteket.<sup>29</sup>

## 2.2 NIST által kiadott publikációk

### 2.2.1 NIST Cybersecurity Framework

Az amerikai Nemzeti Szabványügyi és Technológiai Intézet (National Institute for Standards and Technology, továbbiakban NIST) 2014. február 12-én kiadott egy átfogó kiberbiztonsági keretrendszert, az NIST Cybersecurity Framework-öt (továbbiakban: NIST CSF) annak érdekében, hogy önkéntes, kockázatalapú intézkedés sorozatot biztosítson, amelyeket a szervezetek a kiberbiztonságuk fejlesztésére használhatnak. Bár a keretrendszer eredeti célja a kritikus infrastruktúrák védelmének fejlesztése, rugalmas és technológiasemleges dokumentumról beszélünk, így bármilyen méretű, fejlettségi szintű szervezet tudja használni. 2018 áprilisára megjelent a keretrendszer frissített verziója. Ez az új

---

<sup>28</sup> „Downloads · ENX Portal”, elérés 2022. szeptember 19., <https://enx.com/en-US/TISAX/downloads/>.

<sup>29</sup> T. Królikowski és A. Ubowska, „TISAX - Optimization of IT Risk Management in the Automotive Industry”, köt. 192, 2021, 4259–68, <https://doi.org/10.1016/j.procs.2021.09.202>.

verzió az első kiadás végrehajtása során szerzett tapasztalatokból merített hasznot. A legújabb verzió legjelentősebb kiegészítései az autentikációval, a kiberbiztonsági kockázatok önértékelésével és a kiberbiztonsági kockázatok ellátási láncon belüli kezelésével kapcsolatos. A keretrendszer ingyenesen elérhető az NIST weboldalán.<sup>30</sup> A szervezetek iránymutatásként használhatják a keretrendszert meglévő kiberbiztonsági programjuk értékeléséhez vagy a nulláról való felépítéséhez, az üzleti környezetükkel szinkronban lévő kiberbiztonsági célok meghatározásához, a fejlesztési lehetőségek rangsorolásához, illetve a kiberbiztonság javítására vagy fenntartására vonatkozó terv kidolgozásához.<sup>31</sup> A keretrendszer értékes eszköz arra is, hogy a vezetőknek segítsen megérteni a vállalatuk biztonsági gyakorlatát.<sup>32</sup>

A dokumentum három fő összetevőből áll: a keretrendszer magjából, a profilokból és a megvalósítási szintekből. A mag további három részből áll: funkciók, kategóriák és alkategóriák. Összesen öt darab Funkcióról beszélhetünk, ezek a következők: azonosítás, védelem, felderítés, reagálás és helyreállítás. A következő szint a 23 kategória, amelyek az öt funkció között oszlanak meg. Az ellátási láncok vonatkozásában az azonosítás funkción belül találhatunk olyan kategóriát, amely relevánsnak bizonyul (eredeti rövidítése: ID-SC). Az ID-SC kategória további 5 alkategóriára oszlik, amelyek már konkrétan tartalmazznak követelményeket, javaslatokat. Az alábbi táblázat ezeket prezentálja.

---

<sup>30</sup> „Framework Documents”, *NIST*, 2018. február 5., <https://www.nist.gov/cyberframework/framework>.

<sup>31</sup> Lei Shen, „The Nist Cybersecurity Framework: Overview and Potential Impacts”, *Scitech Lawyer* 10, sz. 4 (2014. Summer): 16–19.

<sup>32</sup> Riza Azmi, William Tibben, és Khin Win, „Review of cybersecurity frameworks: context and shared concepts”, *Journal of Cyber Policy* 3 (2018. szeptember 11.): 1–26, <https://doi.org/10.1080/23738871.2018.1520271>.

| Kategória leírása                                                                                                                                                                                                                                                                                                                                                                                   | Alkategória leírása                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Ellátási lánc kockázatkezelése (ID.SC):<br/>A szervezet prioritásait, korlátait, kockázati tűréshatárait és feltételezéseit megállapítják és felhasználják az ellátási lánc kockázatainak kezelésével kapcsolatos kockázati döntések támogatására. A szervezet kialakította és végrehajtotta az ellátási lánc kockázatainak azonosítására, értékelésére és kezelésére szolgáló folyamatokat.</p> | ID.SC-1: A szervezeti érdekeltek azonosítják, létrehozzák, értékelik, kezelik és elfogadják a kiber ellátási lánc kockázatkezelési folyamatait.                                                                                       |
|                                                                                                                                                                                                                                                                                                                                                                                                     | ID.SC-2: Az információs rendszerek, komponensek és szolgáltatások beszállítóit és harmadik fél partnereit azonosítják, rangsorolják és értékelik egy kiber ellátási lánc kockázatértékelési folyamat segítségével.                    |
|                                                                                                                                                                                                                                                                                                                                                                                                     | ID.SC-3: A beszállítókkal és harmadik féllel kötött szerződéseket a szervezet kiberbiztonsági programjára és a kiber ellátási lánc kockázatkezelési tervének célkitűzéseit szolgáló megfelelő intézkedések végrehajtására használják. |
|                                                                                                                                                                                                                                                                                                                                                                                                     | ID.SC-4: A beszállítókat és harmadik fél partnereket rendszeresen értékelik auditok, teszt eredmények vagy egyéb értékelési formák segítségével, hogy megerősítsék, teljesítik-e a szerződéses kötelezettségeiket.                    |
|                                                                                                                                                                                                                                                                                                                                                                                                     | ID.SC-5: Reagálási és helyreállítási tervezés és tesztelés a beszállítókkal és harmadik fél szolgáltatókkal együtt.                                                                                                                   |

1. táblázat Az ellátási láncokkal kapcsolatos követelmények az NIST CSF-ben. (saját szerkesztés, forrás: <https://www.nist.gov/cyberframework>)

## 2.2.2 NIST Cybersecurity Guidance for Supply Chain Risk Management

Az NIST működése során megkülönböztetett figyelmet fordít az ellátási láncok kockázatkezelésével kapcsolatos kiadványok publikálására. Míg az NIST CSF jellegéből adódóan inkább egy átfogó dokumentumként funkcionál, amely ugyan sorol fel az ellátási láncokkal kapcsolatos javaslatokat (1. táblázat), továbbá több más szabvány kontrollpontját is referenciaként sorolja fel számos helyen, addig léteznek speciális kiadványok is a szervezet tollából, amelyek kizárólag az ellátási láncok információbiztonsági kockázatairól szólnak. Ilyen például a 2022. májusában kiadott Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (NIST Special Publication 800-161 Revision 1), amely ingyenesen elérhető bárki számára.<sup>33</sup> NIST alapvető kiberbiztonsági ellátási lánc kockázatkezelési (cybersecurity supply chain risk management, továbbiakban: C-SCRM) útmutatójának célja, hogy segítse a szervezetek védelmét a technológiai termékek és szolgáltatások beszerzése és

<sup>33</sup> „NIST Updates Cybersecurity Guidance for Supply Chain Risk Management”, NIST, 2022. május 5., <https://www.nist.gov/news-events/news/2022/05/nist-updates-cybersecurity-guidance-supply-chain-risk-management>.

használata során. Ez a kiadvány útmutatást nyújt a szervezetek számára a kiberbiztonsági kockázatok azonosításához, értékeléséhez és mérsékléséhez a teljes ellátási láncot beleértve, a szervezet minden szintjén. A kiadvány egy többszintű, sajátos megközelítés alkalmazásával integrálja a kiberbiztonsági ellátási lánc kockázatkezelést (C-SCRM) az információbiztonsági kockázatkezelési metódusokba. A C-SCRM olyan tevékenységeket foglal magában, amelyek a teljes rendszerfejlesztési életciklus felölelik, beleértve a kutatást és fejlesztést, a tervezést, a gyártást, a beszerzést, a szállítást, az integrációt, az üzemeltetést és karbantartást, a selejtezést, valamint a vállalat termékeinek és szolgáltatásainak általános irányítását. A dokumentum kimondja, hogy vállalkozásoknak a C-SCRM-et be kell építeni az rendszerfejlesztési életciklusba, mivel ez egy kritikus terület az információbiztonsági kockázatok kezelésében. A dokumentum továbbá konstatálja, hogy az C-RSCM kontrollok szervezeten belüli belső kommunikációján kívül a vállalkozásoknak a saját gyakorlati tapasztalatuk cseréje érdekében a partnerekkel, beszállítókkal is együtt kell működniük. Ezek a megosztott tapasztalatok, meglátások segítik a szervezeteket abban, hogy folyamatosan értékeljék, mennyire jól teljesítenek, és meghatározzák, mely területen kell javítani a működésben és hogyan tegyenek lépéseket a C-SCRM-programjuk kiforrottsága érdekében.

### 2.3 Az ISO 27000-es szabványcsalád

Az ISO/IEC 27000-es szabványcsalád az információbiztonsági irányítási rendszerekkel kapcsolatos szabványokat tartalmazza, melyek egy része előkészítés, illetve folyamatos korszerűsítés alatt áll. Alkalmazásuk lehetővé teszi, hogy a szervezetek bármilyen formában kezeljék az olyan eszközök biztonságát, mint a pénzügyi információk, a szellemi tulajdon, az alkalmazottak adatai vagy a harmadik felek által rájuk bízott információk. A következő alfejezetben egyrészt a szabványcsalád széles körben elterjedt szabványát, az ISO/IEC 27001-et fogom prezentálni, mely az IBIR követelményeit leíró normatív szabályokat tartalmazza, valamint az ISO27036 követelményeire fogok kitérni, hiszen az a publikáció a beszállítói kapcsolatok keretében az információ és az információs rendszerek biztonságának biztosításához nyújt útmutatást.<sup>34</sup>

#### 2.3.1 ISO/IEC2700:2013<sup>35</sup>

---

<sup>34</sup> „ISO - ISO/IEC 27001 — Information Security Management”, ISO, elérés 2022. szeptember 22., <https://www.iso.org/isoiec-27001-information-security.html>.

<sup>35</sup> Fontosnak tartom megemlíteni, hogy a szabvány új verziója jelenleg kiadás előtti állapotban van (2022.októberben várható a végleges megjelenés), azonban a szervezeteknek úgynevezett átállási idő áll a rendelkezésükre, amely a végleges kiadás napjától számított 3 évet jelent.

Az ISO/IEC 2700:2013 az Információbiztonsági Irányítási Rendszer (továbbiakban: IBIR) nemzetközi szabványa. Kereskedelmi, kormányzati és nonprofit szervezetekre egyaránt alkalmazható és meghatározza az IBIR létrehozásának, megvalósításának, folyamatos ellenőrzésének és fejlesztésének követelményeit. A szabvány „A” melléklete 114 kontrollpontot tartalmaz, amely átfogó követelményhalmazt nyújt az információvédelem menedzselésére és az IBIR kialakítására.<sup>36</sup> Természetesen ebből a széleskörű elvárások sorából a beszállítókkal, üzleti partnerekkel kapcsolatos kontrollok sem maradnak ki. A „Beszállítói kapcsolatok” szakasz kifejezetten az ellátási láncon belüli információbiztonság kezelésére összpontosít, ennek eredményeképp 5 kontrollpont jelenik meg a témában. A gyakorlatban ez azt jelenti, hogy a vállalatoknak ténylegesen kontrollokat kell bevezetni a beszállítókkal kapcsolatos biztonsági kockázatok kezelésére, ha el akarják érni az ISO 27001 tanúsítvány megszerzését. A szakasznak két különböző kategóriája van a beszállítói menedzsmenttel kapcsolatban, ezek az a következő:

- Információbiztonság a beszállítói kapcsolatokban
- Beszállítói szolgáltatásnyújtás menedzsmentje<sup>37</sup>

A beszállítói kapcsolatokban az információbiztonság célja, hogy biztosítsa a szervezet azon eszközeinek védelmét, amelyekhez a beszállítók hozzáférhetnek. A konkrét kontrollok, amelyeket a szervezeteknek ennek teljesítése érdekében végre kell hajtaniuk, a következők:

- a beszállítói kapcsolatokra vonatkozó információbiztonsági politikát szükséges meghatározni, amely foglalkozik a szállítók szervezet információihoz való hozzáféréssel kapcsolatos kockázatokkal;
- a szervezet információit feldolgozó minden egyes beszállítóval kössenek információbiztonsági követelményt tartalmazó megállapodásokat, szerződéseket.

A fenti pontban a beszállítói kapcsolatokra vonatkozó általános követelményeken túlmenően a megállapodásokba, szerződésekbe foglalják bele az információs és kommunikációs technológiai termékek információbiztonsági követelményeit is (ez magában foglalja felhőszolgáltatások követelményeit is). A beszállítói szolgáltatásnyújtás menedzsmentjének célja, hogy a beszállítói megállapodásokon belül fenntartsa az információbiztonság és a szolgáltatásnyújtás elfogadott szintjét. Az ehhez a kategóriához szükséges konkrét ellenőrzések a következők:

---

<sup>36</sup> Luke Irwin, „ISO 27001 Annex A Controls Explained”, IT Governance UK Blog, 2020. július 27., <https://www.itgovernance.co.uk/blog/iso-27001-the-14-control-sets-of-annex-a-explained>.

<sup>37</sup> „ISO/IEC 27001 Certification & Suppliers relationship”, Cybervadis, 2019. június 28., <https://cybervadis.com/articles/iso-iec-27001-certification-suppliers-relationship/>.

- biztosítani szükséges, hogy a beszállítókat rendszeresen figyelemmel kísérje a szervezet, felülvizsgálat és auditálás révén kövessék, hogy betartja-e a megállapodásokban meghatározott követelményeket;
- szükséges kezelni a beszállítói szolgáltatások változását, amely magában foglalja a beszállítókkal kötött megállapodások módosítását, a politikák és eljárások felülvizsgálatát és frissítését.<sup>38</sup>

Ezen 5 kontroll gyakorlati megvalósítása a való életben nem olyan bonyolult, mint amilyennek az elsőre tűnhet. Figyelnünk kell arra, hogy a megállapodások, szerződések jelentősen eltérhetnek a különböző szervezetek és a különböző típusú beszállítók között. Továbbá érdemes ügyelni arra, hogy minden releváns információbiztonsági kockázatot és követelményt tartalmazzon az adott megállapodás. A megállapodásban figyelembe kell venni a feldolgozás folytatására vonatkozó eljárásokat arra az esetre, ha a szállító nem képes szállítani termékeit vagy szolgáltatásait, hogy elkerülhető legyen a helyettesítő termékek vagy szolgáltatások megszervezésének késedelmé. A másik lényeges elem a beszállítók értékelése, amelyet minimum évenkénti rendszerrel érdemes elvégezni, ez a módszer lényegében lefedi a beszállítók teljesítésének nyomkövetését is. Érdemes a kategóriákba sorolni a beszállítókat, gyakori megközelítésnek bizonyul, hogy általános és szakmai beszállítót különböztet meg a szervezet, s mindezekon kívül az alvállalkozót is külön értékeli. A szempontok közé lehet olyan elemeket felvenni, mint például ISO27001 tanúsítvány megléte, szolgáltatási szint megállapodás (SLA) tartása vagy vevői auditok eredménye.

### 2.3.2 ISO 27036

Az ISO/IEC 27036 egy több részből álló szabvány, amely útmutatást nyújt beszállítóktól történő áru- és szolgáltatás beszerzéssel kapcsolatos információbiztonsági kockázatok értékeléséhez és kezeléséhez. Ebben az alfejezetben az alábbi szabványokat fogom bemutatni:

- ISO/IEC 27036-1:2014: Információbiztonság a beszállítói kapcsolatokban. 1. rész: Áttekintés és fogalmak
- ISO/IEC 27036-2:2022: Kiberbiztonság a beszállítói kapcsolatokban - 2. rész: Követelmények
- ISO/IEC 27036-3:2013: Információbiztonság a beszállítói kapcsolatokban. 3. rész: Irányelvek az információs és kommunikációs technológiai ellátási lánc biztonságához.

---

<sup>38</sup> „ISO/IEC 27001 Certification & Suppliers relationship”.

- ISO/IEC 27036-4:2016: Információbiztonság a beszállítói kapcsolatokban. 4. rész: Irányelvek a felhőszolgáltatások biztonságához

Az 1. rész bevezetőt nyújt, általános háttér-információkat közöl és bemutatja a beszállítói kapcsolatok információbiztonságával kapcsolatos legfontosabb kifejezéseket és fogalmakat. A dokumentum számos olyan információs kockázatot vázol fel, amelyek általában a felvásárló és a beszállítók közötti üzleti kapcsolatokból erednek, vagy azokhoz kapcsolódnak, amikor a beszerzett áruk/szolgáltatások információs tartalommal vagy információbiztonsági vonatkozással bírnak, vagy amikor a beszállító hozzáfér a felvásárló belső információihoz.<sup>39</sup>

A 2. rész a különböző termékek (árúk és szolgáltatások) szállítói és beszerzői közötti üzleti kapcsolatokra vonatkozó alapvető információbiztonsági követelményeket határozza meg. Segíti őket abban, hogy közös megegyezésre jussanak a kapcsolódó információs kockázatokkal kapcsolatban és azokat ennek megfelelően, kölcsönösen kezeljék. A 2. részben ajánlott kontroll intézkedések az irányítás és az üzleti irányítás különböző aspektusaira (pl. működés, HR-menedzsment, IT-menedzsment, kapcsolatkezelés, mérőszámok), valamint az információbiztonsági irányításra (pl. információs kockázatelemzés és kezelés, architektúra tervezés, stratégia) terjednek ki.<sup>40</sup>

A szabvány 3. része az ISO/IEC 15288, 12207 és 27002 szabványokra támaszkodva az IKT-termékek és szolgáltatások beszállítóinak és beszerzőinek egyaránt útmutatást nyújt a széles körben szétszórta és összetett ellátási láncsal kapcsolatos információs kockázatkezelésről, beleértve az olyan kockázatokat, mint a rosszindulatú szoftverek és a hamisított termékek, valamint a "szervezeti kockázatokat".<sup>41</sup>

A 4. rész pedig információbiztonsági útmutatást nyújt a felhőszolgáltatások szállítóinak és ügyfeleinek.<sup>42</sup>

## 2.4 H1 hipotézis vizsgálata

A második fejezetben arra törekedtem, hogy bemutassam az ellátási láncok információbiztonsági kihívásaival foglalkozó legelterjedtebb nemzetközi szabványokat. Ezzel egyidőben vizsgáltam egyaránt a H1 hipotézisemet is.

---

<sup>39</sup> „ISO/IEC 27036-1:2021”, ISO, elérés 2022. szeptember 25., <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/08/29/82905.html>.

<sup>40</sup> „ISO/IEC 27036-2:2022”, ISO, elérés 2022. szeptember 25., <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/08/20/82060.html>.

<sup>41</sup> „ISO/IEC 27036-3:2013”, ISO, elérés 2022. szeptember 25., <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/96/59688.html>.

<sup>42</sup> „ISO/IEC 27036-4:2016”, ISO, elérés 2022. szeptember 25., <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/96/59689.html>.

H1 hipotézisem így szól: Jelenleg nem létezik olyan iparágakon átvélő szabvány, ajánlás vagy keretrendszer, amely teljeskörűen kezeli a komplex információbiztonsági kockázatokat az ellátási láncok vonatkozásában.

A második fejezet alapján megállapítható, hogy létezik több olyan átfogó szabvány is, amely tartalmazza az ellátási láncok információbiztonságának kérdését pár kontrollpont vagy ajánlás erejéig (pl. ISO27001, NIST CSF), azonban az ISO 27036 vizsgálatát követően arra jutottam, hogy a maga 4 részes követelmény halmazával egyedi módon igyekszik az információbiztonság kérdésével foglalkozni az ellátási láncokkal összefüggésben. A szabvány 4 részre való osztása egyfajta alaposságot eredményez, valamint átláthatóbbá, emészthetőbbé válik. Az anyag nem specifikál, nem kizárólag egy iparágra íródott, mint például a korábbiakban bemutatott TISAX, sokkal inkább igyekszik az iparágakon átvélő követelmények megfogalmazására. Ezek alapján tudom azon tézisémet megfogalmazni, hogy létezik jelenleg is iparágakon átvélő szabvány, amely teljeskörűen kezeli a komplex információbiztonsági kockázatokat az ellátási láncok vonatkozásában, így a H1 hipotézisémet megcáfoltam.

#### Következtetés

A második fejezetben tárgyalt nemzetközi szabványok és szakmai ajánlások csupán egy ízelítőt hivatottak nyújtani. Számos további nemzetközi, információbiztonsággal foglalkozó szabvány létezik még, amely követelményeket vagy javaslatokat fogalmaz meg az ellátási láncokkal kapcsolatos információbiztonsági kihívásokkal kapcsolatban (pl. Cobit5). Ebben a fejezetben igyekeztem csupán csak a leglényegesebbekre és legelterjedtebbekre kitérni. A fejezet alatt megállapítottam, hogy léteznek direkt egy adott iparágra szabott keretrendszerek, továbbá megtapasztaltam, hogy szinte mindegyik olyan információbiztonsági szabvány foglalkozik egy kis részben az ellátási láncok információbiztonságával, amelyek átfogó szerepet töltenek be. Ezen kívül a H1 hipotézis vizsgálata során megállapítottam, hogy az ISO27036-os szabvány iparágakon átvélő javaslatokat nyújt az ellátási láncok információbiztonsági kihívásaival kapcsolatban.

### **3. fejezet: Az ellátási láncokkal összefüggő információbiztonsági kockázatok társadalmi megítélése, avagy a kérdőíves felmérés kiértékelése**

A harmadik, egyben utolsó fejezetben az aktuális állapotot szeretném azzal kapcsolatban prezentálni, melyhez a kérdőívem kiértékelését hívom segítségül. A kiértékelésen kívül

továbbá, javaslatokat teszek azzal kapcsolatban, hogy hogyan lenne érdemes a biztonságtudatosító program részeként közelebb hozni a kérdéskört a munkavállalók számára.

### 3.1 A biztonságtudatosító oktatások szerepe

„Az ember a leggyengébb láncszem.” Mára már közhelyként jelenik meg az információbiztonsággal foglalkozó kiadványokban, publikációkban ez a mondás, azonban az üzenete változatlanul aktuális. A munkavállalók biztonságtudatos attitűdje legalább olyan fontos tényezőként bukkanhat fel egy szervezet biztonsági stratégiájában, mint egy gondosan elkészített adatvagyonleltár és kockázatelemzés. A munkavállalók általában a biztonságtudatosító oktatások keretében találkozhatnak az információbiztonsággal, ott hallhatnak először a kibertámadások okozta károk súlyosságáról. Az biztonságtudatosító oktatások lebonyolítása és tartalma szervezetenként eltér, nincsen konszenzusos egyezmény azzal kapcsolatban, hogy mely kötelező elemeket kell tartalmaznia. Továbbá fontos megemlíteni, hogy ezen oktatások nem minden irodai munkakörnyezetben léteznek, a gyakorlat azt mutatja, hogy abban az esetben találkozhatnak a munkavállalók információbiztonsági oktatásokkal, ha a szervezet valamely jogszabályi vagy szabványi megfelelés miatt kötelező jelleggel hajtja végre. Véleményem szerint egy jó biztonságtudatosító oktatás ügyel arra, hogy tartalmazzon a mindenkori aktuális elterjedt támadási vektorokat és kitér arra is, hogy felhasználói szinten ezeket milyen módon lehet megelőzni, észre enni.

### 3.2 A kérdőív bemutatása és kiértékelése

Kutatásom központi elemét az általam készített kérdőív jelentette. A kérdőívet a H2 és a H3 hipotézisem vizsgálata során hívtam segítségül. A kérdőívet bárki kitölthette, aki irodai munkakörnyezetben dolgozik. A kérdőív alapvetően 2 részre oszlik. Az első részben a szervezettel, valamint annak információbiztonsági gyakorlatával kapcsolatban találhattak kérdéseket a kitöltők. A második részben legelőször arra voltam kíváncsi, mennyire emlékszik az adott kutatásban résztvevő alany a Solar Winds támadásra. Ezt követően ismertettem az ellátási láncokat érintő támadások fogalmát és a maradék 4 kérdés már ezzel a kérdéskörrel foglalkozik.

#### 3.2.1 Solar Winds kifejezés vizsgálata

Mindenekelőtt érdekességképp kérdőívem 8. kérdésével kapcsolatos eredményeket szeretném bemutatni. Kíváncsi voltam, hogy média által is meglehetősen felkapott Solar Winds-ügy mennyire él a köztudatban, tudják-e nagyvonalakban, hogy miről is szólt. A kérdés maga így szólt: „2020-ban a SolarWinds-ügy jelentős nemzetközi visszhangot váltott ki a médiában.

Emlékei szerint miről szólt a Solar Winds-ügy?” A kitöltők 4 fajta válasz alternatívákkal találkozhattak, melyek az alábbiak:

Több millió Facebook-felhasználó személyes adatait gyűjtötte össze a felhasználók beleegyezése nélkül egy brit tanácsadó cég, elsősorban azért, hogy azt politikai reklámozásra használják fel azokat.

Ellátási láncokat megtámadó hackertámadás, amelynek számos amerikai kormányzati szerv és piaci szereplő egyaránt áldozatául esett.

- Számítógépes vírus, amelynek lényege, hogy a megfertőződött számítógépeken tárolt fájlokat zárolja és pénzösszeg megfizetéséért cserébe lehet azokat visszakapni.
- Amerikai politikai botrány, amely Richard Nixon elnök lemondásához vezetett

Úgy gondolom, maga a kutatás címe is árulkodó lehetett a kitöltők számára, mégsem sikerült minden válaszadónak beazonosítani a helyes választ. A kitöltők (103 ember) 74,8 százaléka választotta a helyes megoldást, azaz összesen 77 ember. 15,5 százalék, azaz 16 kitöltő a Cambride Analytika botrányra utaló választ gondolta helyesnek, míg 7,8 százalék, 8 személy vélte úgy, hogy egy számítógépes vírusra utal a Solar Winds kifejezés. Végül a maradék 2 kitöltő pedig a Richard Nixonnal kötötte össze a fogalmat.

A kulcsszót megvizsgáltam egy másik módszerrel is, melynek során segítségemre volt a socialbearing.com weboldal, amely a Twitter megjelenő bejegyzéseket elemzi, többek közt a bejegyzések érzelmi töltetét is. A szentimentelemzés egy gyakorlati formája a közösségi médiáról történő adatbányászatnak, mely magába foglal olyan technológiai folyamatokat, amik segítségével meg lehet határozni a posztolt említések általános érzelmi töltetét. A weboldal ingyenes verziója a statisztikákat 100 bejegyzésre lebontva határozza meg az elmúlt 9 nap posztjaiból. Rákerestem a „SolarWinds” kifejezésre és az alábbi eredményt kaptam:

### A bejegyzések megoszlása érzelmi töltet alapján

| Érzelmi töltet | Arány |
|----------------|-------|
| Kiváló         | 25%   |
| Jó             | 14%   |
| Közömbös       | 39%   |
| Rossz          | 11%   |
| Szörnyű        | 11%   |

100% = 100 bejegyzés

2. ábra „SolarWinds „kulcsszó szentiment alapú elemzése 2022.10.08-án (saját szerkesztés, forrás: socialbearing.com)

– 23 –

A kulcsszó felhőn látszik, hogy számos összeesküvésre utaló kifejezés jelenik meg, ilyen például a „Trump” „Putin” kulcsszavak, amely ismét súlyos reputációs károkra utalhat.

### 3.2.2 H2 hipotézis vizsgálata

Kutatási eredményeim szöveges, statisztikai kiértékeléshez Németh Anikó: Adatelemzés statisztikai módszerekkel<sup>43</sup> című publikációt hívtam segítségül. A H2 és a H3 hipotézisemet az SPSS program keretein belül Mann Whitney U próba segítségével elemeztem ki. A Mann Whitney U próba ordinális (rangsorolt) adatok esetén a mediánokat hasonlítja össze. Kontrollcsoportos vizsgálatnál alkalmazzuk, amikor két részmintát vagy mintát hasonlítunk össze nagyság szintjük alapján. Arra voltam kíváncsi, hogy a két minta rangsora jelentős mértékben eltér-e egymástól. Ennél a vizsgálatnál a rang pontszámok átlagának (Mean Ranks, továbbiakban: MR) is jelentősége van, sok információt hordoz: a kisebb átlagérték az adott részminta/minta rangsorban elfoglalt jobb helyzetére utal.

A H2 hipotézisem így szól: A közsférában foglalkoztatottak átlagosan nagyobb kockázatnak minősítik az ellátási láncok ellen irányuló támadásokat, mint azok, akik a versenyszférában dolgoznak.

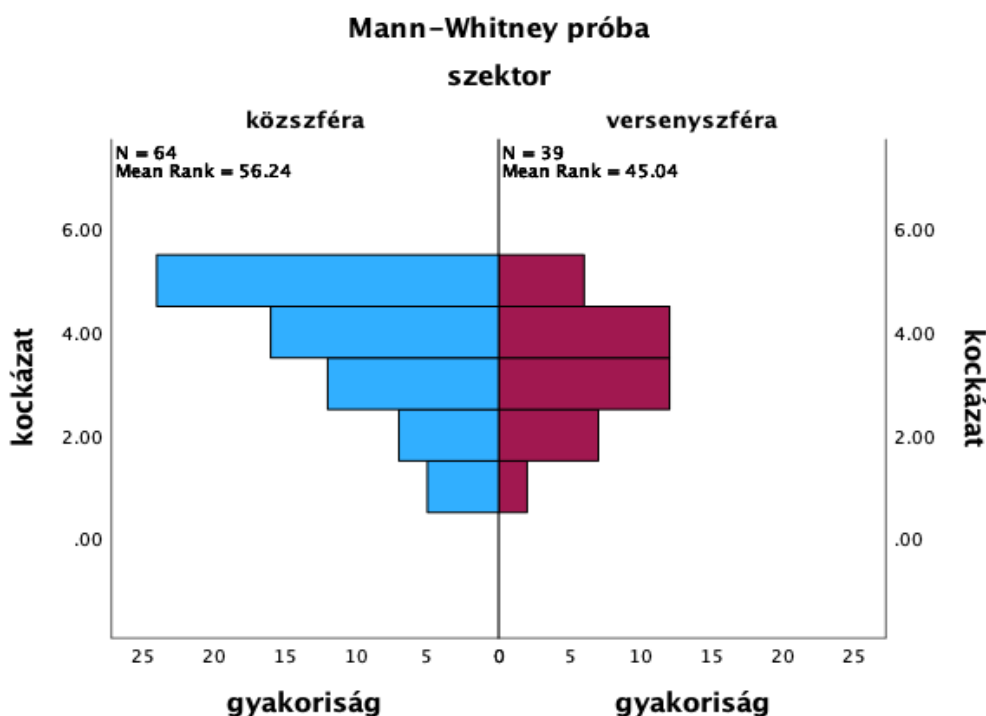
A H2 hipotézisre vonatkozó vizsgálat során kérdőívem 1. és 11. kérdését vetettem össze, melyek az alábbiak voltak:

- 1. Melyik szektorban dolgozik jelenleg?
- 11. Kérem értékelje egy 1-től 5-ig terjedő skálán, hogy mekkora kockázatnak tartja az ilyen jellegű támadásokat a saját szervezetére vonatkozóan!

Az 1. kérdésnél 2 opció közül választhattak a kitöltők, amely a közsféra és a versenyszféra volt, míg a 11. kérdés esetében egy 5 elemből álló skálát találtak a kutatásban résztvevők. Ötös értékét jelentette, ha „jelentős kockázatnak” tartja a kutatásban résztvevő az ellátási láncok ellen irányuló támadásokat, míg az egyes érték jelentette, ha „egyáltalán nem tartja kockázatnak”. Az 2. ábrán található diagramon láthatjuk az elemszámokat az elemszámokat (N) és a rangpontszámok átlagát (Mean Rank), melyek a következőképp alakultak:

---

<sup>43</sup> Anikó Németh, „Adatelemzés statisztikai módszerekkel”, Jegyzet, tankönyv, 2018. június 20., <https://eta.bibl.u-szeged.hu/458/>.



4. ábra Mann-Whitney U teszt H2 hipotézis vonatkozásában. (saját szerkesztés)

Az ábráról leolvashatjuk, hogy azok esetében, akik a közsférában dolgoznak az MR=56,24, míg az versenyszférában munkát vállalok esetében MR=45,04. A szignifikanciát, tehát azt, hogy van-e jelentős különbség a két csoport között pedig a 2. táblázatról olvashatjuk le. Szignifikanciáról akkor beszélhetünk, ha a p érték kisebb mint 0,05. A szignifikancia jelen próba esetében azt jelzi, hogy van-e a két csoport között eltérés. Estünkben a  $p=0,057$ , így nem beszélhetünk szignifikanciáról, tehát nincs jelentős különbség a két csoport között, ezzel a H2 hipotézisemet megcáfoltam

### Mann-Whitney U próba

|                                |          |
|--------------------------------|----------|
| Összes elemszám                | 103      |
| Mann-Whitney U                 | 976.500  |
| Wilcoxon W                     | 1756.500 |
| Kétoldalú szignifikancia teszt | .057     |

2. táblázat: Mann Whitney U próba eredménye a H2 hipotézis vonatkozásában (saját szerkesztés)

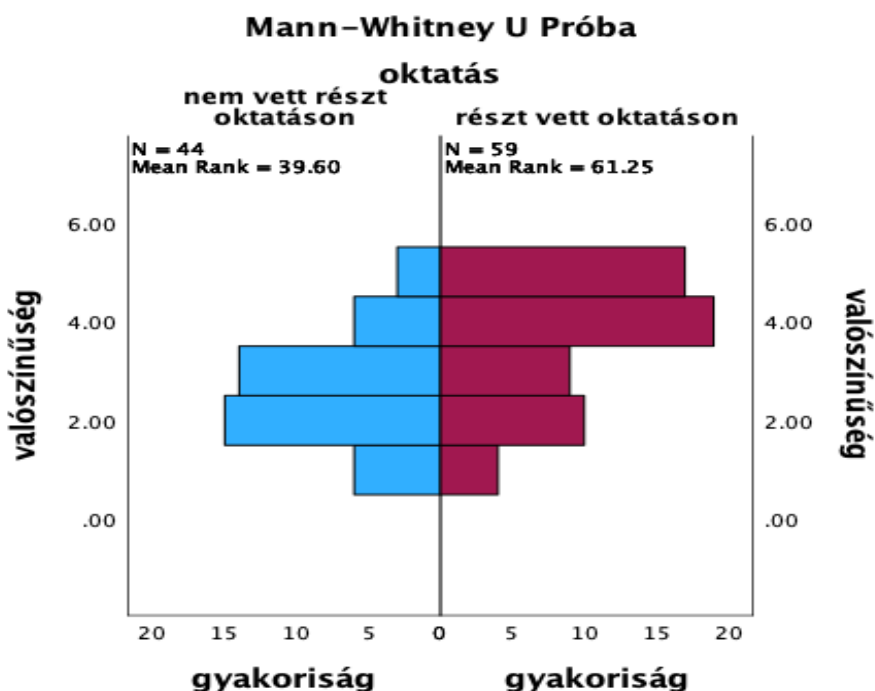
#### 3.2.3 H3 hipotézis vizsgálata

H3 hipotézisem így szól: Azok a munkavállalók, akik részt vesznek minimum évenkénti rendszerességgel információbiztonsági tudatosító oktatáson, valószínűbbnek gondolják, hogy az elkövetkezendő 5 évben ellátási lánc ellen irányuló támadást szenved a szervezetük.

H3 hipotézisem vizsgálata során kérdőívem 6. és 10. kérdését vettem össze, melyek az alábbiak:

- 6. Részt szokott-e venni a munkahelyén minimum évenkénti rendszerességgel információbiztonsági tudatosító képzésen?
- 11. Kérem értékelje egy 1-től 5-ig terjedő skálán, hogy mennyire tartja valószínűnek, hogy szervezetét ilyen jellegű támadás éri az elkövetkező 5 évben!

A 6. kérdésnél igen és nem válasz közül választhattak a kitöltők, míg a 11. kérdésnél szintén egy 1-től 5-ig terjedő skálán jelezhatték a kutatásban résztvevők, hogy mennyire tartják valószínűleg egy ellátási láncokat érintő támadás bekövetkezését a szervezetük vonatkozásában. Az 3. ábrán található diagramon láthatjuk az elemszámokat az elemszámokat (N) és a rangpontszámok átlagát (Mean Rank), melyek a következőképp alakultak a H3 hipotézis esetében:



5. ábra Mann-Whitney U teszt H3 hipotézis vonatkozásában (saját szerkesztés)

A 3. ábráról leolvashatjuk, hogy azok esetében, akik nem vesznek részt oktatáson az MR=39,60, valamint azok esetében, akik részt vesznek évenkénti oktatáson MR=61,25. A szignifikanciát, tehát azt, hogy van-e jelentős különbség a két csoport között pedig a 3. táblázatról olvashatjuk le. A szignifikanciát, tehát azt, hogy van-e jelentős különbség a két csoport között pedig a 3. táblázatról olvashatjuk le. A szignifikancia jelen próba esetében is azt jelzi, hogy van-e a két

csoport között eltérés. Estünkben a  $p=0,001$ , így beszélhetünk szignifikanciáról, tehát jelentős különbség van a két csoport között. Ezzel a H3 hipotézisemet alátámasztottam.

### Mann-Whitney U próba

|                                   |          |
|-----------------------------------|----------|
| Összes elemszám                   | 103      |
| Mann-Whitney U próba              | 752.500  |
| Wilcoxon W                        | 1742.500 |
| Kétoldalú szignifikancia<br>teszt | <.001    |

3. táblázat Mann Whitney U próba eredménye a H3 hipotézis vonatkozásában (saját szerkesztés)

#### Következtetés

A harmadik fejezetben eredményeim prezentálására helyeztem a hangsúlyt. A fejezetben a H2 és H3 hipotéziseket vizsgáltam. A H2 hipotézisem esetében felmerült bennem a gondolat, miszerint a közszférában foglalkoztatottak nagyobb kockázatnak titulálják az ellátási láncok elleni támadásokat. Ezt a feltételezést arra alapoztam, hogy közszférában munkát vállalók, nagy valószínűséggel részt vesznek évenként biztonságtudatosító oktatáson, hiszen szervezete az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L-es törvény hatálya alá esik, így ez kötelező, azonban ezt T2 tézisem megcáfolta.

T3 tézisem igazolta, hogy akik részt vesznek évente biztonságtudatosító oktatáson, valószínűbbnek gondolják, hogy az elkövetkezendő 5 évben ellátási lánc ellen irányuló támadás szenved a szervezete.

#### Összegzett következtetések

Ahhoz, hogy sikeresen kezeljék a fejlődő kiberbiztonsági kockázatokat az ellátási lánc egészében, a szervezeteknek több belső folyamatot és képességet kell bevonniuk, kommunikálniuk és együttműködniük kell a vállalati szintek és feladatkörök között, és biztosítaniuk kell, hogy a vállalatban belül minden egyes személy megértse a kiberbiztonsági kockázatok kezelésében betöltött szerepét az ellátási lánc egészében. Az ellátási láncok információbiztonságának technológiai, formális szabályozása, stratégiai és irányítási szempontjait meg kell vitatni annak eldöntésekor, hogy egy cégnek milyen stratégiát választ és testre szabnia a megoldásokat, hogy optimális megoldásokat biztosítson a kérdésben.

#### Kutatási eredmények

T1: Létezik olyan iparágakon átívelő szabvány, ajánlás vagy keretrendszer, amely teljeskörűen kezeli a komplex információbiztonsági kockázatokat az ellátási láncok vonatkozásában.

T2: A közszférában foglalkoztatottak nem minősítik átlagosan nagyobb kockázatnak az ellátási láncok ellen irányuló támadásokat, mint azok, akik a versenyszférában dolgoznak.

T3: Azok a munkavállalók, akik részt vesznek minimum évenkénti rendszerességgel információbiztonsági tudatosító oktatáson, valószínűbbnek gondolják, hogy az elkövetkezendő 5 évben ellátási lánc ellen irányuló támadást szenved a szervezetük.

Eredmények hasznosíthatósága

A dolgozatomban megfogalmazott eredményeim alkalmasak egyfajta figyelemfelhívó szerep betöltésére, továbbá eredményeim rámutatnak arra, hogy a biztonságtudatosító képzéseknek elhanyagolhatatlan tartalmi eleme az ellátási láncok elleni támadásokkal foglalkozó részek.

## Felhasznált irodalom

Ageron, Blandine, Omar Bentahar, és Angappa Gunasekaran. „Digital supply chain: challenges and future directions”. *Supply Chain Forum: An International Journal* 21, sz. 3 (2020. július 2.): 133–38. <https://doi.org/10.1080/16258312.2020.1816361>.

Anikó Németh. „Adatelemzés statisztikai módszerekkel”. Jegyzet, tankönyv, 2018. június 20. <https://eta.bibl.u-szeged.hu/458/>.

Azmi, Riza, William Tibben, és Khin Win. „Review of cybersecurity frameworks: context and shared concepts”. *Journal of Cyber Policy* 3 (2018. szeptember 11.): 1–26. <https://doi.org/10.1080/23738871.2018.1520271>.

Bányász, Péter. „Az ellátási lánc kiberfenyegetettsége, különös tekintettel a közlekedési alrendszer biztonságára, a szervezett bűnözés hatásai”, 643-673., 2016.

Christopher, Martin, és Matthias Holweg. „“Supply Chain 2.0”: managing supply chains in the era of turbulence”. Szerkesztette Michael Crum és Richard Poist. *International Journal of Physical Distribution & Logistics Management* 41, sz. 1 (2011. január 1.): 63–82. <https://doi.org/10.1108/09600031111101439>.

Collier, Zachary A., és Joseph Sarkis. „The zero trust supply chain: Managing supply chain risk in the absence of trust”. *International Journal of Production Research* 59, sz. 11 (2021. június 3.): 3430–45. <https://doi.org/10.1080/00207543.2021.1884311>.

„Downloads · ENX Portal”. Elérés 2022. szeptember 19. <https://enx.com/en-US/TISAX/downloads/>.

„Framework Documents”. *NIST*, 2018. február 5. <https://www.nist.gov/cyberframework/framework>.

Gelei Andrea. „Az ellátási lánc típusai és menedzsmentkérdései”. *Vezetéstudomány - Budapest Management Review* 34, sz. 7–8 (2003. július): 24–34.

Irwin, Luke. „ISO 27001 Annex A Controls Explained”. IT Governance UK Blog, 2020. július 27. <https://www.itgovernance.co.uk/blog/iso-27001-the-14-control-sets-of-annex-a-explained>.

ISO. „ISO - ISO/IEC 27001 — Information Security Management”. Elérés 2022. szeptember 22. <https://www.iso.org/isoiec-27001-information-security.html>.

„ISO/IEC 27036-1:2021”. ISO. Elérés 2022. szeptember 25. <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/08/29/82905.html>.

„ISO/IEC 27036-2:2022”. ISO. Elérés 2022. szeptember 25. <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/08/20/82060.html>.

„ISO/IEC 27036-3:2013”. ISO. Elérés 2022. szeptember 25.

<https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/96/59688.html>. „ISO/IEC 27036-4:2016”. ISO. Elérés 2022. szeptember 25. <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/96/59689.html>. Cybervadis. „ISO/IEC 27001 Certification & Suppliers relationship”, 2019. június 28. <https://cybervadis.com/articles/iso-iec-27001-certification-suppliers-relationship/>. Królikowski, T., és A. Ubowska. „TISAX - Optimization of IT Risk Management in the Automotive Industry”, 192:4259–68, 2021. <https://doi.org/10.1016/j.procs.2021.09.202>. Kshetri, N. „Economics of Supply Chain Cyberattacks”. *IT Professional* 24, sz. 3 (2022): 96–100. <https://doi.org/10.1109/MITP.2022.3172877>. Melnyk, Steven A., Tobias Schoenherr, Cheri Speier-Pero, Chris Peters, Jeff F. Chang, és Derek Friday. „New challenges in supply chain management: cybersecurity across the supply chain”. *International Journal of Production Research* 60, sz. 1 (2022. január 2.): 162–83. <https://doi.org/10.1080/00207543.2021.1984606>. „Mimecast Certificate Hacked in Microsoft Email Supply-Chain Attack”. Elérés 2022. szeptember 11. <https://threatpost.com/mimecast-certificate-microsoft-supply-chain-attack/162965/>. „NIST Updates Cybersecurity Guidance for Supply Chain Risk Management”. NIST, 2022. május 5. <https://www.nist.gov/news-events/news/2022/05/nist-updates-cybersecurity-guidance-supply-chain-risk-management>. Shen, Lei. „The Nist Cybersecurity Framework: Overview and Potential Impacts”. *Scitech Lawyer* 10, sz. 4 (2014. Summer): 16–19. Simon, Jay, és Ayman Omar. „Cybersecurity Investments in the Supply Chain: Coordination and a Strategic Attacker”. *European Journal of Operational Research* 282, sz. 1 (2020. április 1.): 161–71. <https://doi.org/10.1016/j.ejor.2019.09.017>. „SolarWinds hack explained: Everything you need to know”. Elérés 2022. szeptember 10. <https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know>. Decipher. „Supply Chain Attack Hits Passwordstate Password Manager”. Elérés 2022. szeptember 12. <https://duo.com/decipher/supply-chain-attack-hits-passwordstate-password-manager>. Fortinet. „Supply Chain Attacks: Examples and Countermeasures”. Elérés 2022. szeptember 10. <https://www.fortinet.com/resources/cyberglossary/supply-chain-attacks>. „Supply Chain Security Guidance”. Elérés 2022. szeptember 8. <https://www.ncsc.gov.uk/collection/supply-chain-security>.

Deloitte Croatia. „TISAX - A megfelelésen túl | Deloitte Magyarország”. Elérés 2022. szeptember 19. <https://www2.deloitte.com/hu/hu/pages/fogyasztoi-agazat/articles/tisax----a-megfelelesen-tul---deloitte-magyarorszag.html>.

„What Is a Supply Chain Attack? Solutions & Examples | Keeper”. Elérés 2022. szeptember 12. <https://www.keepersecurity.com/threats/supply-chain-attack.html>.

„Who cares? Supply chain managers’ perceptions regarding cyber supply chain risk management in the digital transformation era | Emerald Insight”. Elérés 2022. szeptember 4. <https://www.emerald.com/insight/content/doi/10.1108/SCM-02-2020-0073/full/html#sec001>.

Zailani, Suhaiza Hanim, Karthigesu Seva Subaramaniam, Mohammad Iranmanesh, és Mohd Rizaimy Shaharudin. „The impact of supply chain security practices on security operational performance among logistics service providers in an emerging economy: Security culture as moderator”. Szerkesztette Dr Daniel Ekwall and Dr Bobby J. Martens Dr Jennifer Blackhurst. *International Journal of Physical Distribution & Logistics Management* 45, sz. 7 (2015. január 1.): 652–73. <https://doi.org/10.1108/IJPDLM-12-2013-0286>.

## Mellékletek

### Rövidítések jegyzéke

| Rövidítés | Magyar nyelvű kifejezés                        | Idegen nyelvű kifejezés                                  |
|-----------|------------------------------------------------|----------------------------------------------------------|
| C-SCRM    | kiberbiztonsági ellátási lánc kockázatkezelési | cybersecurity supply chain risk management               |
| IBIR      | Információbiztonsági Irányítási Rendszer       | Information Security Management System                   |
| KKV       | kis-és középvállalkozás                        | small and medium sized business                          |
| MR        | rang átlag                                     | Mean Rank                                                |
| NIST      | Nemzeti Szabványügyi és Technológiai Intézet   | National National Institute for Standards and Technology |
| SCA       | ellátási lánc elleni kibertámadás              | supply chain attack                                      |
| SCCA      | szoftver ellátási lánc elleni kibertámadás     | software supplychain attack                              |
| TISAX     | -                                              | Trusted Information Security Assessment Exchange         |
| VDA       | Német Autóipari Szövetség                      | Verban der Automobilindustrie                            |

## Ábrajegyzék

|                                                                                                                                                                                                                     |    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 1. ábra SCCA fajtái (saját szerkesztés, forrás: <a href="https://www.fortinet.com/resources/cyberglossary/supply-chain-attacks.">https://www.fortinet.com/resources/cyberglossary/supply-chain-attacks.</a> ) ..... | 5  |
| 2. ábra SolarWinds kulcsszó szentiment alapú elemzése (saját szerkesztés, forrás: <a href="https://socialbearing.com">socialbearing.com</a> ) .....                                                                 | 23 |
| 3. ábra Kulcsszó felhő (forrás: <a href="https://socialbearing.com">socialbearing.com</a> ) .....                                                                                                                   | 23 |
| 4. ábra Mann-Whitney U teszt H2 hipotézis vonatkozásában (saját szerkesztés).....                                                                                                                                   | 25 |
| 5. ábra Mann-Whitney U teszt H3 hipotézis vonatkozásában (saját szerkesztés).....                                                                                                                                   | 26 |

## Táblázatok jegyzéke

|                                                                                                                                                                                                        |    |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 1. táblázat Az ellátási láncokkal kapcsolatos követelmények az NIST CSF-ben. (saját szerkesztés, forrás: <a href="https://www.nist.gov/cyberframework">https://www.nist.gov/cyberframework</a> ) ..... | 15 |
| 2. táblázat: Mann Whitney U próba eredménye a H2 hipotézis vonatkozásában (saját szerkesztés).....                                                                                                     | 25 |
| 3. táblázat Mann Whitney U próba eredménye a H3 hipotézis vonatkozásában (saját szerkesztés).....                                                                                                      | 27 |

## Kérdőív kérdései

1. Melyik szektorban dolgozik jelenleg?

- közszféra

- versenyszféra

2. Az Európai Bizottság 14 kulcsfontosságú ipari ökoszisztémát azonosított Európában. Az Ön szervezete az ellátási lánc(ok)on keresztül valószínűleg kapcsolódik egy vagy több ilyen ökoszisztémához. Melyekhez? (több válasz is lehetséges)

- Idegenforgalom (személyszállítás és utazás; szállodák és rövid távú szállások; éttermek és étkeztetés; rendezvények és élményparkok)

- Kreatív, kulturális iparágak (újságok, könyvek és folyóiratok; film, videó és televízió; rádió és zene)

- Repülés és védelem (beleértve a légi járművek és űrhajók gyártását, a katonai felszereléseket és a fegyvergyártást, a műholdakat)

- Elektronika (nyers kiindulási anyagok (félvezető szeletek); Félvezető-gyártó eszközök; Félvezető alkatrészek tervezése és gyártása)

- Mobilitás - közlekedés - autóipar (gépjárművek, hajók, vonatok és alkatrészek gyártása; ezek javítása és karbantartása; szállítás)

- Energiaigényes iparágak (fosszilis tüzelőanyagok kivonása; finomítás; nagy környezeti hatással járó termékek - műanyagok, vegyi anyagok, műtrágyák, vas és acél, papír stb - gyártása)
- Megújuló energia (elektromos motorok, erőgépek és turbinák; villamosenergia-termelés; gázgyártás és -elosztás)
- Agrár-élelmiszeripar (növénytermesztés és állattenyésztés; élelmiszer-feldolgozás; állategészségügyi tevékenységek)
- Egészségügy (gyógyszerészeti termékek és berendezések; kórházak, időotthonok, bentlakásos ellátás)
- Digitális ágazat (távközlés; szoftver és programozás; internetes portálok; számítógépek és berendezések gyártása)
- Építőipar (lakóingatlanok és nem lakáscélú ingatlanok építése; út- és vasútépítés; közművek építése és mélyépítés; a kapcsolódó szolgáltatások aktiválása)
- Kiskereskedelem (kiskereskedelmi értékesítés; fogyasztókhoz kapcsolt nagykereskedelmi szolgáltatások)
- Lokális és szociális gazdasági szervezetek (szociális vállalkozások; szövetségek és szövetkezetek)
- A fentiek közül egyik sem
- Egyéb

3. Mennyire ért egyet a következő kijelentéssel? A szervezetben az információbiztonsági kockázatokat minden működési folyamat kapcsán azonosítják és figyelembe veszik.

- Nincs róla információ/Nem értelmezhető a szervezetben
- Egyáltalán nem értek egyet
- Nagyrészt nem értek egyet
- Közömbös számomra
- Nagyrészt egyetértek
- Teljes mértékben egyetértek

4. Tapasztalt-e az Ön szervezete valamilyen kiberbiztonsági incidenst az elmúlt 12 hónapban? (több választ is megjelölhet)

- Az üzletmenet folytonosság megszakításával járó támadást tapasztaltunk
- Olyan támadást tapasztaltunk, amely az adatok megsértésével járt és nyilvánossá váltak ezen adatok
- Nem szándékos eseményt tapasztaltunk, amely üzletmenet folytonosság megszakításával járt
- Nem szándékos eseményt tapasztaltunk, amely adatmegsértést vont maga után

- Tudomásom szerint nem tapasztaltunk incidenst az elmúlt 12 hónapban

5. Milyen intézkedéseket hajtott végre korábban a szervezete a kiberbiztonság javítása érdekében? (több választ is megjelölhet)

- A szervezet kiberbiztonsági stratégiával rendelkezik, külön dokumentumként vagy egy másik stratégia részeként.

- A szervezet folytonossági tervvel rendelkezik olyan események kezelésére, amelyek üzleti megszakítással vagy adatmegsértéssel járnak.

- Kötelező rendszabályokat és folyamatokat vezettünk be az alkalmazottak számára, például a jelszó előállításával, a magántárhely vagy a digitális magánszolgáltatások használatával, a biztonsági mentésekkel és a hálózati hozzáféréssel kapcsolatban.

- Alkalmazunk olyan technikai megoldásokat, mint például szoftverfrissítések, biztonsági mentések készítése, kommunikáció titkosítása és a hálózati hozzáférésre vonatkozó szabályok alkalmazása.

- A szervezet tanúsított például: Az ISO27000 sorozat szerint.

- A szervezet rendelkezik a kiberbiztosítás valamilyen formájával (ideértve a számítógépes bűnözéssel vagy az adatvédelemmel kapcsolatos biztosításokat), amely lefedi például az üzleti tevékenység megszakítását, az adatok megsértését és az eseménykezelés támogatását.

- Nincs tudomásom ilyenről

6. Részt szokott-e venni a munkahelyén minimum évenkénti rendszerességgel információbiztonsági tudatosító képzésen?

- igen

- nem

7. Ön mit gondol jelentős információbiztonsági kockázatnak szervezetére vonatkozóan?

8. 2020-ban a SolarWinds-ügy jelentős nemzetközi visszhangot váltott ki a médiában. Emlékei szerint miről szólt a Solar Winds-ügy?

- Több millió Facebook-felhasználó személyes adatait gyűjtötte össze a felhasználók beleegyezése nélkül egy brit tanácsadó cég, elsősorban azért, hogy azt politikai reklámozásra használják fel azokat.

- Ellátási láncokat megtámadó hackertámadás, amelynek számos amerikai kormányzati szerv és piaci szereplő egyaránt áldozatául esett.

- Számítógépes vírus, amelynek lényege, hogy a megfertőződött számítógépeken tárolt fájlokat zárolja és pénzösszeg megfizetéséért cserébe lehet azokat visszakapni.

- Amerikai politikai botrány, amely Richard Nixon elnök lemondásához vezetett

A második részben a supply chain attack, azaz az ellátási láncokat érintő kibertámadásokkal kapcsolatban talál kérdéseket. A SolarWinds hackertámadásában alkalmazott módszert nevezik ellátási lánc ellen elkövetett támadásnak. Az ellátási lánc elleni támadás olyan kibertámadás, amely a szervezetek ellátási láncának gyengébb láncszemeire összpontosítva célozza a szervezeteket. Tulajdonképp ez a módszer lehetővé teszi, hogy nincs szükség a hackereknek megtámadni a tényleges célpontot, „csupán” csak egy harmadik felet, aki a célpontnak terméket vagy szolgáltatást szállít be.

9. Érthető volt Ön számára a fogalom meghatározás?

- Teljesen
- Többé-kevésbé
- Nem

10. Kérem értékelje egy 1-től 5-ig terjedő skálán, hogy mennyire tartja valószínűnek, hogy szervezetét ilyen jellegű támadás éri az elkövetkező 5 évben!

1-től 5ig terjedő skála

12. Kérem értékelje ezek alapján egy 1-től 5-ig terjedő skálán, hogy mekkora kockázatnak tartja az ilyen jellegű támadásokat a saját szervezetére vonatkozóan!

1-től 5ig terjedő skála

13. Kérem értékelje egy 1-től 5-ig terjedő skálán, hogy mennyire tartja fontosnak, hogy szervezetének partnerei, beszállítói és alvállalkozói bizalmasan kezeljék akár az Ön személyes adatait, akár munkahelyével kapcsolatos információkat.

1-től 5ig terjedő skála

Kérdőív kiértékelése

### Independent-Samples Mann-Whitney U Test Summary

|                               |          |
|-------------------------------|----------|
| Total N                       | 103      |
| Mann-Whitney U                | 976.500  |
| Wilcoxon W                    | 1756.500 |
| Test Statistic                | 976.500  |
| Standard Error                | 142.584  |
| Standardized Test Statistic   | -1.904   |
| Asymptotic Sig.(2-sided test) | .057     |

### Independent-Samples Mann-Whitney U Test Summary

|                                  |          |
|----------------------------------|----------|
| Total N                          | 103      |
| Mann-Whitney U                   | 752.500  |
| Wilcoxon W                       | 1742.500 |
| Test Statistic                   | 752.500  |
| Standard Error                   | 146.361  |
| Standardized Test<br>Statistic   | -3.727   |
| Asymptotic Sig.(2-sided<br>test) | <.001    |