ÖNKORMÁNYZATOK ÉS KIBERBIZTONSÁG – A SZERVEZET ÉS AZ EMBERI ERŐFORRÁS FELKÉSZÜLTSÉGE AZ ONLINE FELMÉRÉS EREDMÉNYEI ALAPJÁN

Számadó Róza

A nemzetközi és hazai tapasztalatok mind azt támasztják alá, hogy az emberi tényező szerepe meghatározó erőforrás a szervezetek életében, és ez különösen igaz az információs társadalomban, az információbiztonsági kérdésekben. Az ember–technika–környezet komplex rendszert alkot az információs társadalomban. Feltételezésem szerint a technológiai, szabályozási kérdések alapos figyelmet kapnak, ám az emberi tényező változási helyzetre való reagálásának figyelembevétele, fejlesztése, kezelése nem kap kellő hangsúlyt, nincs megfelelően a rendszerbe illesztve.

A felkészültség, az információbiztonsági kultúra kialakítása kiemelt figyelmet kapott az elmúlt húsz évben, különös tekintettel arra, hogy a különböző incidensek legnagyobb része a csekély felkészültség és információbiztonsági tudatosság hiányából következett be. Az emberi tényező fejlesztése véleményem szerint csak komplexen, a rendszer elvárásaihoz illesztve valósítható meg. Nem elfeledkezve arról, hogy ez egy olyan folyamat, amelyben eddig soha nem tapasztalt szoros kapcsolat van az élethosszig tartó tanulás koncepciójának a való élethez.

Jelen tanulmány fókuszában a helyi önkormányzatok kiberbiztonsági képességének vizsgálata áll az emberi tényező jelentőségének fokozott figyelembevételével. A kérdések, amelyekre kutatásomban a választ kerestem: Felkészültek-e az önkormányzatok a kibertérből érkező kihívásokra? Milyen fenyegetettséggel nézhetnek szembe? Tudatában vannak-e a fenyegetettség hatásainak? Rendelkeznek-e a szükséges eszközökkel, felkészült emberi erőforrással?

A tanulmány keretei nem teszik lehetővé, hogy a teljes vizsgálat bemutatásra kerüljön, így – a felmérés adatainak bemutatását követően – az önkormányzatok kiberbiztonsági helyzetének feltárását célzó online felmérésnek a fő eredményeit mutatom be, kiemelt figyelemmel az emberi tényezőre.

LOCAL GOVERNMENTS AND CYBERSECURITY – THE PREPAREDNESS OF THE ORGANISATION AND HUMAN RESOURCES BASED ON THE RESULTS OF THE ONLINE SURVEY

Számadó Róza

International and domestic experiences all confirm that the role of the human factor is a decisive resource in the life of organisations, and this is especially true in the information society, in information security issues. Humans, technology and the environment create a complex system in information society. My assumption is that the technological and regulatory issues receive careful attention, while the taking into consideration, development and management of the response of the human factor to the change situation does not receive sufficient attention, is not properly integrated into the system.

The establishment of the preparedness and information security culture has received special attention in the last twenty years, especially since most of the various incidents occurred due to the lack of preparedness and information security awareness. In my opinion, the development of the human factor can only be realised in a complex way, adapted to the expectations of the system. Not forgetting that this is a process in which there is an unprecedented tight bond between the concept of lifelong learning and real life.

The focus of this study is on examining the cybersecurity capability of local governments, paying particular attention to the significance of the human factor. The questions I was seeking answers for in my research: Are local governments prepared for the challenges of cyberspace? What threat can they face? Are they aware of the effects of the threat? Do they have the necessary tools and are their human resources prepared?

The framework of the study does not allow the full study to be presented, therefore I will present the main results of an online survey on the cybersecurity status of local governments, with a particular focus on the human factor, following the presentation of the data of the survey.

Háttér, keretek

Az önkormányzatok – az önkormányzás jogának gyakorlása során – fő felelőssége, hogy feladatvégzés közben a település lakosságának érdekeit szolgálja. Az önkormányzatok, működésük során sok szempontból állnak kettős nyomás alatt. Egyrészt azonosítható elvárás a globalitás és lokalitás kérdéseiben a nyitottság, az információ minél szélesebb körű megosztása, a XXI. század közösségi médiáinak használata. A másik oldalon pedig a kiberbiztonság biztosítása érdekében felmerülő teendők. Az önkormányzatokra a helyi igazgatás letéteményeseiként jelentős felelősség és feladatmennyiség hárul az utóbbi területen is, aminek kezelésére nem, vagy nem teljes körűen vannak felkészülve.

Az IKT[61] rendszereire épülő, összekapcsolt infrastruktúrák által alkotott globális virtuális tér: a kibertér, aminek rosszindulatú felhasználására számtalan lehetőség kínálkozik. A kibertérből érkező kihívások és fenyegetések folyamatos, dinamikus bővülése egyre szignifikánsabb veszélyt jelent. Az állami és helyi önkormányzati hivatalok hatalmas nyomás alatt vannak az adataik, infrastruktúrájuk és szolgáltatásaik biztonságossá tételét tekintve. Nagyon fontos, hogy a mérvadó döntéshozók központi és helyi szinten is felismerjék a kockázat nagyságát, rendelkezzenek stratégiával, felkészült humán erőforrással és a megfelelő eszközökkel annak érdekében, hogy időben és elvárható hatékonysággal tudjanak reagálni, amennyiben ez szükségessé válik.

A vizsgálat megközelítése, nézőpontja a szervezeti hozzáállás, tudatos működés, az emberi tényező, a humán erőforrás vizsgálata, és nem volt célja a technikai kérdések, a kiberfenyegetések kezelésének részletes kifejtése.

Trendek és kihívások, melyekkel a közszférának szembe kell néznie

2017 legfontosabb kiberbiztonság trendjei a következők voltak (Európai Hálózat- és Információbiztonsági Ügynökség jelentése) [1]:

- a támadások és az elkövetők módszereinek komplexitása egyre növekszik;
- az elkövetők egyre könnyebben tudják elfedni a nyomaikat, így a felfedésük egyre nehézkesebbé válik;
- a kártékony infrastruktúrák átalakulása többcélú, konfigurálható funkciókká, amelyek anonimizálhatók, titkosítottak és nehezebben észlelhetők;

61. Az *„information and communication technology"* kifejezés az 1980-as években jelent meg. Az angol szakirodalomban ICT rövidítéssel használják, a magyar szövegekben pedig IKT-ként. Többféle módon értelmezik, jelen esetben átfogó kifejezésként kerül használatra. Jelöli mindazon számítógépeket és elektronikus rendszereket, amelyek alkalmasak adatok elektronikus gyűjtésére, tárolására, felhasználására és továbbítására, továbbá jelenti az ezekhez kapcsolódó alkalmazásokat és szolgáltatásokat is.

Background, frameworks

The main responsibility of local governments - while exercising the right of self-governance - is to serve the interests of the inhabitants of the settlement while performing their tasks. Local governments, in their operation, are in many ways under double the amount of pressure. On the one hand, there is an identifiable expectation for openness, the sharing of information as widely as possible on issues of globalisation and locality, and the use of 20th century social media. On the other hand, they are expected to take the necessary measure to ensure cybersecurity. Local governments, as the depositories of local administration, also have a great deal of responsibility and tasks in the latter area, which they are not or not fully prepared to handle.

The global virtual space created by interconnected infrastructures based on ICT[61] systems: cyberspace, for the malicious use of which there are endless possibilities. Continuous, dynamic expansion of the challenges and threats from cyberspace pose an increasingly significant threat. State and local government agencies are under enormous pressure to secure their data, infrastructure and services. It is very important that authoritative decision-makers recognise the magnitude of the risk at both central and local levels, to have a strategy, skilled human resources and the appropriate tools in order to ensure that they can respond in time and with the expected efficiency if it becomes necessary.

The approach and viewpoint of the study is organisational attitude, conscious operation, human factor, human resource analysis, and was not intended to explain technical issues or cyber threats in detail.

Trends and challenges facing the public sector

The most important cybersecurity trends of 2017 were the following (report of the European Union Agency for Network and Information Security) [1]:

- the attacks and the methods of perpetrators are becoming more and more complex;
- the perpetrators are able to hide their tracks with increasing ease, making their detection more difficult;
- the transformation of malicious infrastructures into multi-purpose, configurable functions that can be anonymised, encrypted and more difficult to detect;

61. The term *'information and communication technology'* first appeared in the 1980s. It is used in the English literature abbreviated as ICT, and in Hungarian text as IKT. It is interpreted in several ways, however, in this case it is used as a comprehensive term. It indicates all computers and electronic systems that are capable of collecting, storing, using and transmitting data, as well as the related applications and services.

- a kibertérre a legnagyobb fenyegetést az államok által támogatott szereplők (kémek) jelentik;
- a kiberháború mint fogalom egyre dinamikusabban jelenik meg a köztudatban, és fokozott fenyegetettséget jelent a kritikus infrastruktúra operátorai felé.
- a szervezetek számára kiemelt fontosságú, hogy megfelelő készségekkel és képességekkel rendelkezzenek alkalmazottaik, azonban a képzésre és oktatásra még mindig kevés hangsúlyt fektetnek.

A Panda Security által készített 2018-as év előrejelzését tartalmazó jelentése szerint [2]:

- az adaptív elterelő hadműveletekkel operáló rejtőzködő támadások válnak gyakoribbakká;
- a mobileszközökre és az IoT-ra (Internet of Things – dolgok internete) írt kártevők további térnyerése várható;
- a védekezés tekintetében a képzés és a tudatosság a két kulcsmomentum, majd ezt követi a kiberbiztonság gyakorlata;
- az összes rosszindulatú kód 99%-a soha többé nem jelenik meg máshol (a vírusdefiníciós védekezés nem működik);
- növekvő támadási gyakoriság sokkal kifinomultabb módszerekkel.

Vizsgálat módszerei

Az önkormányzatok kiberbiztonsági kérdéseinek vizsgálatához 2018. január elején – a tesztelést követően – a teljes önkormányzati kör részére elektronikus úton került kiküldésre a kérdőív, amire 2018. február 13-ig 512 válasz érkezett. A kitöltés önkéntes és anonim volt. A kérdőív kérdéseinek leírása az 1. mellékletben található. A felmérés egy adminisztratív és három tartalmi blokkra különült el. Az első blokk a kitöltőkre vonatkozó alap adatokat tartalmazza, míg a másik három az önkormányzatok kiberbiztonsági kérdéseivel foglalkozik. A szakmai blokkok összeállítása során a célom az volt, hogy átfogó képet kapjak az önkormányzatok kiberbiztonsági kérdésekhez való viszonyulásáról, felkészültségéről és működési gyakorlatáról a beérkezett válaszokon keresztül.

A kérdőívre adott válaszok értékelése a kérdések jellegétől függően leíró statisztikai, matematikai statisztikai módszerekkel (főkomponens elemzés) és a szöveges válaszok esetében egyszerű összegzéssel készült. A főkomponens elemzés öt fő komponenst kínált fel, ebből a legerősebb magyarázó erővel az önkormányzatok felkészültségéhez, képességéhez kapcsolódott.

- the biggest threat to cyberspace are the state-supported actors (spies);
- the concept of cyber warfare is becoming more and more dynamic in public consciousness and poses an increased threat to critical infrastructure operators;
- for organisations, it is of paramount importance that their employees have the right skills;
- and abilities, however they still place little emphasis on training and education.

According to the report of Panda Security containing the 2018 forecast [2]:

- hidden attacks with adaptive diversion operations become more common;
- further spreading of malware written for mobile devices and IoT (Internet of Things) is expected;
- in terms of defence, training and awareness are the two key components, followed by the practising of cybersecurity;
- 99% of all malicious code will never appear again (virus definition protection does not work);
- increasing attack frequency with more sophisticated methods.

Assessment methods

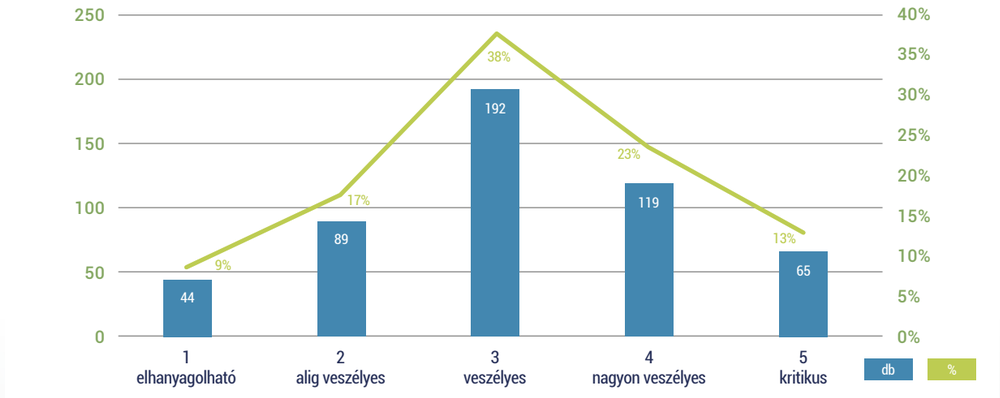
The questionnaire was sent electronically to the all local governments at the beginning of January 2018, after the testing, to investigate the cybersecurity issues of local governments, to which 512 responses were received until 13 February 2018. Its completion was voluntary and anonymous. The questions in the questionnaire are described in Annex 1. The survey was divided into one administrative and three content blocks. The first block contains basic data regarding the completing party, while the other three deal with the cybersecurity issues of the local governments. During the compilation of the professional blocks, my goal was to get a comprehensive picture of the attitude of local governments towards cybersecurity issues, their preparedness and operational practices through the responses received.

The answers to the questionnaire were evaluated using descriptive statistical, mathematical statistical methods (principal component analysis) and simple summaries in the case of written answers, depending on the nature of the questions. The principal component analysis offered five principal components, of which the strongest explanatory power related to the preparedness and capability of local governments.

A vizsgálat eredményei

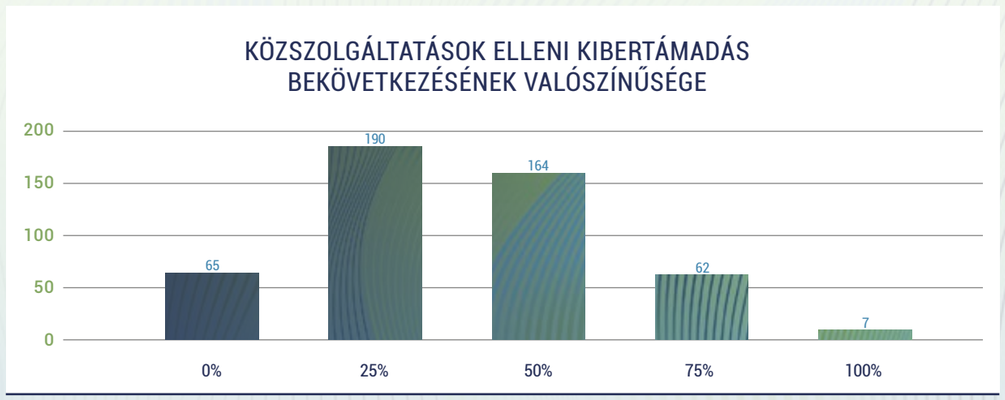
A fenyegetettség megítélése az önkormányzatok körében

A válaszadó önkormányzatok jelentős része nem tartja igazán veszélyesnek és valószínűnek egy kibertámadás bekövetkezését.



1. ÁBRA A kibertámadás bekövetkezésének veszélyessége (Forrás: [3 p. 79])

A számok további vizsgálata azt mutatta, hogy az egyenletes eloszlás csak az összes válasz egyben kezelése esetén igaz. Amikor hivataltípus bontásban néztük, akkor azt láthattuk, hogy az önálló hivatalok 90%-a, a közös hivatal székhely önkormányzatai 70%-ban, míg a közös hivatal tagok 50%-ban tarják csak közepes vagy annál jelentősebb veszélynek. Az önkormányzati hivatalok típusa szerinti megbontásnál az önálló hivatalok és a közös székhely önkormányzatok inkább ítélték veszélyesnek, sőt közel 15%-ban kritikusnak egy ilyen incidens bekövetkezését.



2. ÁBRA Közszolgáltatások elleni kibertámadás bekövetkezésének valószínűsége (összegezve) (Forrás: [3 p. 81])

Assessment results

Threat perception among municipalities

A significant proportion of responding local governments do not consider it very dangerous or likely to have a cyberattack.

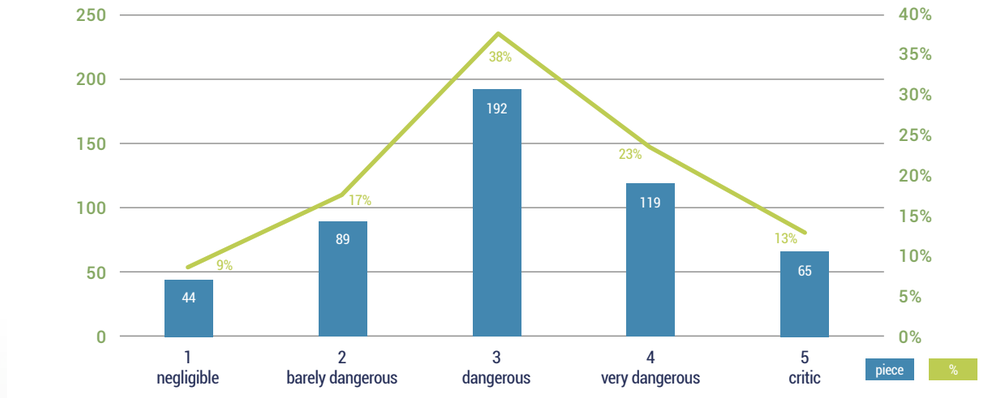


FIGURE 1 Risk of a cyberattack (Source: [3 p. 79])

Further examination of the figures showed that the uniform distribution is only true when considering all responses as a whole. When we looked at the breakdown of office types, we observed that 90% of autonomous agencies, 70% of joint office headquarters of local governments, and 50% of joint office members consider the risk to be moderate or higher. In the breakdown by type of local government office, autonomous agencies and local governments with joint headquarters were more likely to consider the risk high, in fact, nearly 15% considered the risk of such an incident to be critical.

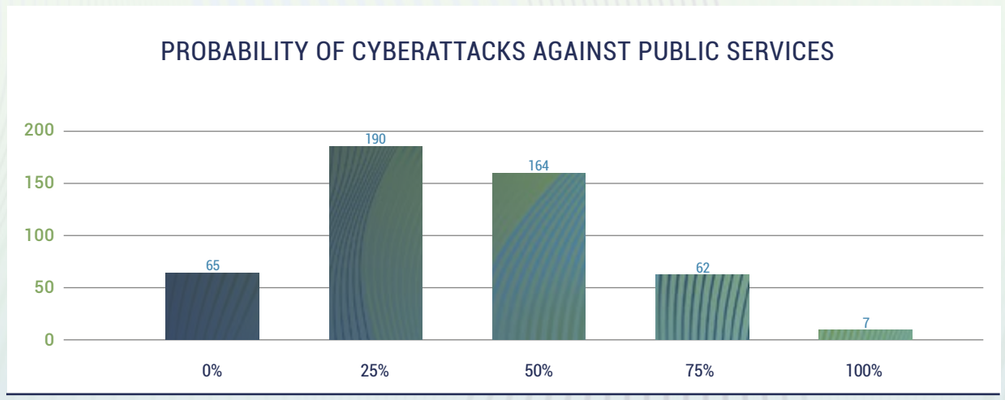
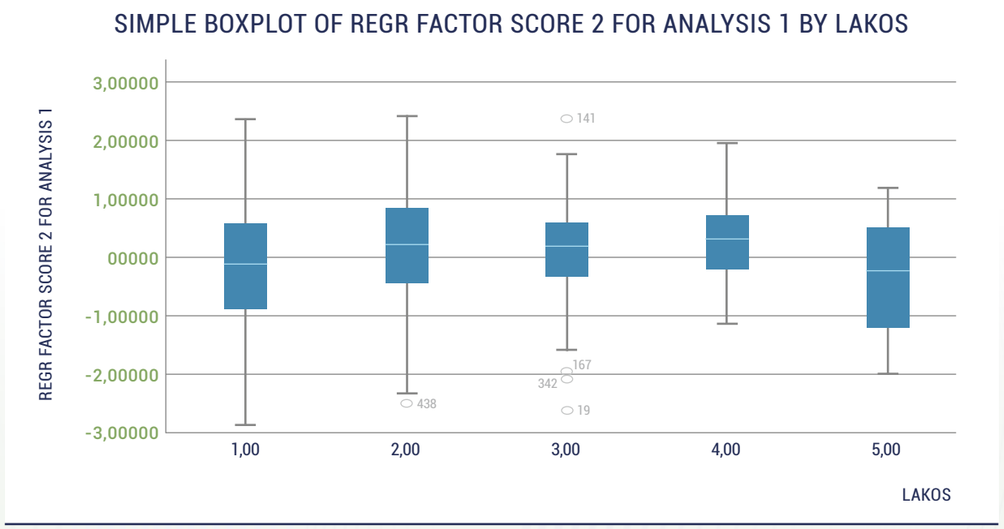


FIGURE 2 Probability of cyberattacks against public services (summarised) (Source: [3 p. 81])

Az ábrán látható, hogy 65 válaszadó (hivataltípustól függetlenül, közel azonos arányban) egyáltalán nem tartja elképzelhetőnek egy, a közszolgáltatások ellen bekövetkező kibertámadást.

Ez azért érdekes – és komoly problémaként fogalmazható meg már önmagában is –, mert a válaszadók összetételét vizsgálva azt láttuk, hogy a válaszok közel 80%-a településvezetőtől érkezett.

A főkomponens elemzés szerint a lakosságszám szerinti vizsgálat hozott szignifikáns eredményt.



3. ÁBRA Kiberfenyegetettség megítélése a különböző lakosságszám kategóriába tartozó települések esetében (Forrás: [3 p. 88])

Az elemzés eredménye alapján lakosságszámot tekintve az 1-es csoport (1000 fő alatti lakosságszám) és az 5 csoport (50000 fő feletti lakosságszám) különbözik szignifikánsan a 2–4 kategóriákba (1001 főtől 50 000 főig) tartozó lakosságszámú önkormányzatoktól a kiberfenyegetettség megítélésben. A kevés és a túl sok lakossal rendelkező települések önkormányzatai kevésbé gondolják, hogy fenyegetné őket kibertámadás. A szakirodalom, a felmérés és a fókuszcsoportos interjú eredménye alapján azt feltételezzük, hogy ezt az okozza, hogy a kistelepülések úgy, hogy kívül esnek a kibertámadásokat kezdeményezők érdeklődési körén; az általuk kezelt adatok, információk nem képviselnek olyan értéket, ami felkeltené az esetleges rosszindulatú támadó figyelmét. Az 50 001 fő lakosságszámot meghaladó települések esetében pedig egy túlzott önbizalom lehet az oka a kiberfenyegetettség alacsony értékelésének.

The figure shows that 65 respondents (regardless of the type of office, almost in the same proportion) do not consider a cyberattack against public services at all possible.

This is interesting - and can be described as a serious problem in itself - as when we examined the composition of the respondents, we found that nearly 80% of the responses came from the heads of settlements.

According to the analysis of the principal component, the population-based study produced significant results.

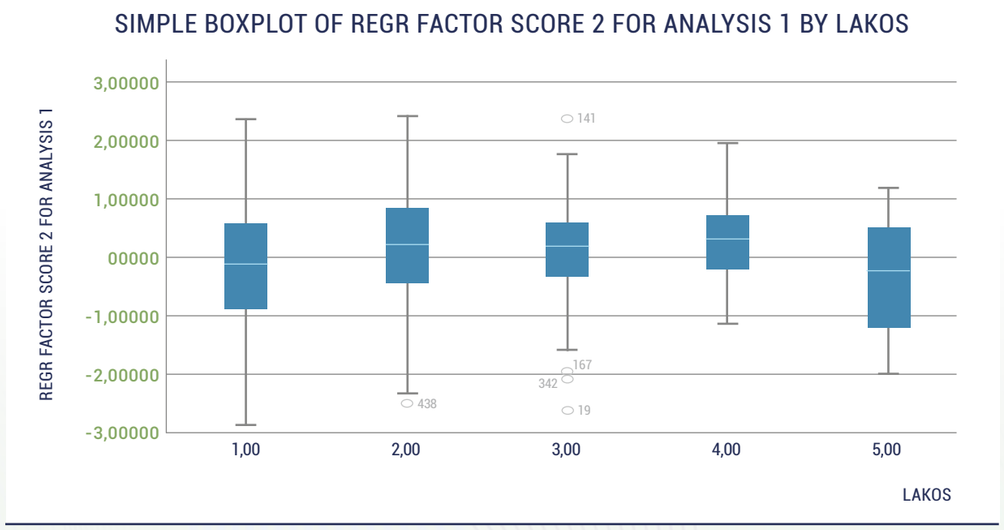


FIGURE 3 Assessing cyber threats in settlements belonging to different categories of the population (Source: [3 p. 88])

Based on the results of the analysis, looking at the population, group 1 (population below 1,000) and group 5 (population above 50,000) are significantly differ from the local governments belonging to population categories 2-4 (population between 1,001 and 50,000) in their judgement on cyber threats. The local governments of settlements with few or too many residents consider it less probable that they are exposed to the threat of cyberattacks. Based on the literature, the results of the survey and the focus group interview, we assume that this is caused by the fact that small settlements are outside the scope of cyberattacks; the data and information processed by them do not represent a value that would attract the attention of a potentially malicious attacker. In the case of settlements with more than 50,001 inhabitants, excessive self-confidence may be the reason for the low rating of cyber threats.

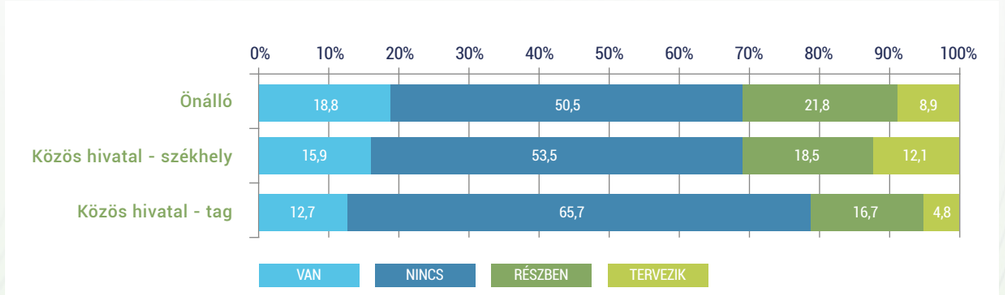
Önkormányzatok és munkatársaik felkészültsége – az online felmérés eredménye alapján

Az önkormányzatok felkészültségének elemzése szignifkáns eredményt hozott mind lakosságszám, mind hivatali státusz szempontjából.

A felkészültség inkább a nagyobb lakosságszámú, több erőforrással rendelkező települések esetében jellemző. A hivatali státusz szerinti eredmény nagyon hasonló, vagyis az önálló hivatalokra jellemző, hogy jobban fel vannak készülve egy kibertámadásra és annak kezelésére.

A munkatársak felkészültségével kapcsolatban a válaszadók véleménye szerint lehangoló a kép. A válaszok tanúsága szerint egy bekövetkezett kibertámadás alkalmával kevés olyan munkatársukra számíthatnak az egyes hivatalok, akik teljesen felkészültek és motiváltak is arra, hogy elhárítsák a fenyegetést. Általában csupán minden huszadik hivatalnál találunk ilyen munkatársi állományt. Ez az arány megközelítőleg azonos minden önkormányzati státusz esetében. A többségében felkészült hivatali dolgozók minden ötödik hivatalban tevékenykednek, legtöbben a székhelyszervezetek esetében.

Ennek ellenére a munkatársak részére rendszeresített tudatosító képzések nem jellemzőek.



4. ÁBRA Rendszeres fenyegetettséget tudatosító képzés megléte a munkatársak részére (Forrás: [3 p. 108])

A hivatalok átlagosan 60%-ában semmiféle olyan rendszeresen szervezett képzést nem jeleztek, amely témája a kiberfenyegetettség tudatosítása és az elhárítás személyes motiválása lenne. E megállapításon belül az önállóan működő és a székhelyként tevékenykedő hivatalok fele (50,5% és 53,5%), valamint a legkisebb mértékben a kirendeltséghivatalok kétharmada (65,7%) érintett a hiányolható képzések szempontjából.

Szervezett, irányított és rendszeres tematikus képzés csupán átlagosan minden hatodik-hetedik szervezet esetében figyelhető meg (14,9%). Legnagyobb arányban jellemző ez az önálló hivatalokra (ahol szinte minden ötödik szervezetre igaz: 18,8%), és legkevésbé a legkisebb hivatalokra (ahol minden nyolcadik szervezett jelezte ezt: 12,7%).

Preparedness of local governments and their employees – based on the results of the online survey

The analysis of the preparedness of local governments has yielded significant results in terms of both population and administrative status.

Preparedness is more typical for larger settlements with more resources. The result of the administrative status is very similar, that is, it is characteristic of autonomous agencies that they are better prepared for a cyberattack and its handling.

In the opinion of the respondents, the picture is depressing in relation to the preparedness of employees. According to the responses, if a cyberattack actually occurred, local governments would have only a few employees they could rely on who are fully trained and motivated to overcome the threat. Usually we only have such employees at every twentieth office. This ratio is approximately the same for each local government status. Office workers with training are located at every fifth office, mostly within headquarters.

Nonetheless, awareness raising trainings for employees is not typical.

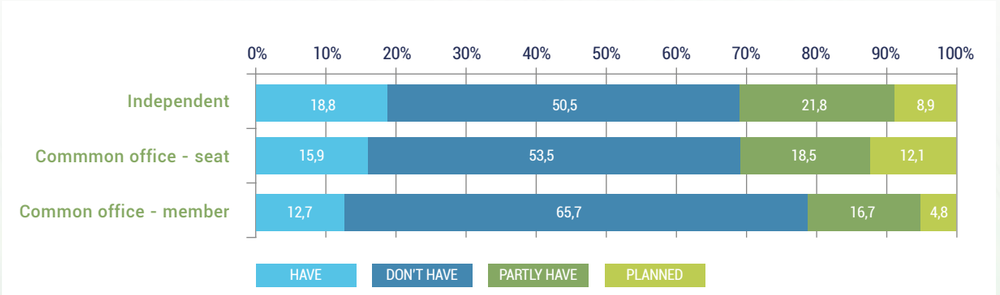


FIGURE 4 Existence of regular threat awareness training for employees (Source: [3 p. 108])

On average, 60% of the offices did not report any regularly organised training aimed at raising awareness of cyber threats and personal motivation to combat them. Within this finding, half of the autonomous agencies and the offices acting as headquarters (50.5% and 53.5%) and, to a lesser extent, two-thirds of the branch offices (65.7%) were affected by missing trainings.

Organised, managed and regular thematic training can only be observed on average for every sixth or seventh organisation (14.9%). This is the most characteristic of autonomous agencies (where it is true for almost every fifth organisation: 18.8%), and least characteristic of the smallest offices (where every eighth organisation indicated this: 12.7%).

Megállapítások

Általános megállapítás, hogy az önkormányzatok nem a megfelelő helyen és szinten kezelik az információbiztonságot.

Informatikai kérdésként kezelik, miközben a megfelelő működés érdekében az információbiztonságnak a szervezeti kultúra részének kellene lennie, vagyis tudatosság szükséges. Ez nem működik a munkatársak motivációja és a vezetők elköteleződése nélkül. A kialakított központi képzések nem illeszkednek megfelelően az önkormányzaton belül az információbiztonság biztosítása érdekében kialakítandó szerepekhez. Az online felmérés alapján az önkormányzatok vagy nem tartják fenyegetettnek, sebezhetőnek az önkormányzatok adatait és rendszereit, vagy nem gondolják, hogy célkeresztben lennének. A kiberbiztonsági kérdések kapcsán a tudatosság nagyon alacsony szintet mutat, ami a kiberbiztonsági trendeket, irányokat és technológiai fejlődést figyelembe véve (például: olyan támadások várhatók, amelyek célzottak, emberi beavatkozást már nem igényelnek) hatalmas kockázatot hordoz.

A települési önkormányzatok közül csak a legnagyobbak rendelkeznek valamelyest védekezési képességgel és információbiztonsági kompetenciákkal. A kisebb települések jellemzően nincsenek felkészülve, és szélmalomharcnak gondolják, míg a nagyok túlzottan bíznak a saját képességeikben. Az 1001–50 000 fő lakosságszámú települések értelmezik leginkább helyén a kiberfenyegetettséget.

Felhasznált irodalom

1. **European Union Agency for Network and Information Security: ENISA Threat Landscape Report 2017.** Top 15 Cyber-Threats and Trends; https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017 (letöltve: 2018. 02. 24.)

2. **Panda Security: 2017 Cybersecurity Trends; 2017.** https://www.pandasecurity.com/mediacenter/pandalabs/annual-report-cybersecurity-predictions-2018/ (letöltve: 2018. 03. 18.)

3. **Számadó R.: Önkormányzatok kiberbiztonságának és online képességének vizsgálata, figyelemmel az emberi tényező fejlesztésének kérdéseire Budapest, BTDI 2018.** Doktori értekezés https://bdi.uni-obuda.hu/sites/default/files/Doktori_(PhD)_ertekezes_-_Szamado_Roza.pdf (letöltve: 2018. 09.12.)

Findings

It is a general observation that local governments do not manage information security in the right location or at the right level.

They are treated as an IT issue, while information security should be part of the organisational culture for proper operation, i.e. awareness is required. It does not work without the motivation of employees and the commitment of managers. The central trainings developed do not fit well with the roles that need to be established to ensure information security within the local government. Based on the online survey, local governments either do not consider the data and the systems of local governments to be under threat or vulnerable, or do not think they would be a target. The awareness of cybersecurity issues is very low, which is a huge risk in terms of cybersecurity trends and tendencies and technological developments (e.g.: attacks that are targeted and no longer require human intervention are expected).

Of the local governments, only the largest ones have some level of defensive capabilities and information security competencies. Smaller settlements are typically unprepared and consider it a constant struggle, while the larger ones are over-confident in their abilities. Settlements with a population of 1,001 to 50,000 are the most likely to interpret cyber threats correctly.

Literature

1. **European Union Agency for Network and Information Security: ENISA Threat Landscape Report 2017.** Top 15 Cyber-Threats and Trends; https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017 (downloaded: 24.02.2018)

2. **Panda Security: 2017 Cybersecurity Trends; 2017.** https://www.pandasecurity.com/mediacenter/pandalabs/annual-report-cybersecurity-predictions-2018/ (downloaded: 18.03.2018)

3. **Számadó, R.: Analysing cyber security and online capabilities of local governments, considering questions of developing the human factor Budapest, BTDI 2018.** Doctoral thesis https://bdi.uni-obuda.hu/sites/default/files/Doktori_(PhD)_ertekezes_-_Szamado_Roza.pdf (downloaded: 12.09.2018)