DOI: 10.53020/IME-2024-KSZ-203

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet kibervédelmi gyakorlata az egészségügyi szektor számára

The cybersecurity exercise for the healthcare sector of the National Cyber-Security Centre of the Special Service for National Security

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet cikke.

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) által 2023-ban szervezett HunEx kibervédelmi gyakorlat az egészségügyi szektor számára nyújtott lehetőséget a résztvevők kibervédelmi képességeinek felmérésére, belső eljárásrendjeik tesztelésére, valamint az ágazatok közötti együttműködés erősítésére. A gyakorlat során a résztvevők 14 technikai és 5 kommunikációs feladatot oldottak meg, amelyek célja valósághű szituációk szimulálása és a résztvevők készségeinek próbára tétele volt. A technikai feladatok között szerepelt a logelemzés, káros kódok elemzése, valamint a virtuális gépeken történt incidensek kivizsgálása. Különösen fontos volt a zsarolóvírus-támadások kezelése, mivel ezek súlyos következményekkel járhatnak az egészségügyi szektor számára.

A kommunikációs feladatok során a résztvevőknek sajtómegkeresésekkel és közösségimédia-kihívásokkal kellett szembenézniük, amelyek révén a szervezet belső és külső kommunikációs stratégiáit tesztelték. A gyakorlat során a vezetői döntéshozatal, a szervezeti eljárásrendek követése és a hatóságokkal való kapcsolattartás szintén központi szerepet játszott. A résztvevők visszajelzései szerint a gyakorlat jelentősen hozzájárult kibervédelmi készségeik és szervezeti kommunikációjuk fejlesztéséhez, miközben azonosította a további fejlesztésre szoruló területeket, mint például az adathalász támadások felismerésének javítása és a hatóságokkal való gyorsabb kommunikáció. A gyakorlat összességében sikeres volt, és nagymértékben hozzájárult az egészségügyi szektor kibervédelmi képességeinek erősítéséhez, valamint a jövőbeni kibertámadásokra való felkészüléshez.

A cikk célja, hogy bemutassa a lezajlott gyakorlatot és a szervezés közben, valamint a gyakorlat lebonyolítása során keletkezett tapasztalatokat, és ezáltal segítse az egészségügyi intézményeket a hasonló gyakorlatokra történő felkészülésben.

Kulcsszavak: kiberbiztonság, gyakorlat, incidens, technikai feladatok, kommunikációs feladatok

The National Cyber-Security Centre of the Special Service for National Security (SSNS NCSC) organized the HunEx cybersecurity exercise in 2023, specifically targeting the healthcare sector. The primary objectives of this exercise were to evaluate the cybersecurity capabilities of participating institutions, to test internal procedures, and to strengthen intersectoral cooperation. Given the critical nature of healthcare systems, ensuring that these institutions are well-prepared to handle cyber incidents is of utmost importance. The HunEx exercise provided a controlled environment in which participants could engage with realistic scenarios designed to test their readiness and response to cyber threats.

The exercise involved 14 technical and 5 communication tasks, each designed to simulate real-life situations that the participants might face in the event of a cyberattack. The technical tasks included activities such as log analysis, malware analysis, and incident investigation on virtual machines. These tasks were crucial in assessing the participants' ability to identify and mitigate cyber threats. For example, participants were required to analyse logs and identify indicators of compromise, investigate the presence of malicious code, and determine whether data breaches had occurred.

One of the most significant challenges presented during the exercise was the handling of ransomware attacks. Given the increasing prevalence of ransomware incidents globally, this aspect of the exercise was particularly important. In addition to technical tasks, the exercise placed a strong emphasis on communication. The participants faced various challenges related to media relations and social media management, testing the organization's internal and external communication strategies.

Moreover, the exercise highlighted the importance of leadership decision-making and adherence to organizational procedures. Participants were tasked with making strategic decisions in response to the incidents, coordinating their teams' efforts, and ensuring that all actions were in line with the organization's internal protocols.

Communication with authorities also played a key role in the exercise. Participants were required to prepare legal documents and reports and ensure that these were submitted to the relevant authorities in a timely and correct manner.

The feedback from participants indicated that the exercise was highly beneficial in improving their cybersecurity skills and organizational communication. However, the exercise also identified areas that need further development. One of the most frequently observed issues was the inadequate communication with both internal and external stakeholders. In many cases, communication was either insufficient or entirely lacking, which could lead to significant problems in a real incident.

Another significant area for improvement was the communication with authorities and the Computer Security Incident Response Team (CSIRT). During the exercise, there were instances where participants failed to report incidents to the authorities in a timely and correct manner. This is a critical weakness, as timely and accurate reporting to authorities is essential for coordinating an effective response to a cyber incident.

Phishing attempts were also a common problem among participants. Many participants failed to recognize phishing emails, highlighting the need for further training and awareness in this area.

Despite these challenges, the exercise also highlighted several positive outcomes. One of the most notable achievements was the proactive reporting of phishing attempts. Although many participants initially fell victim to these attempts, the majority recognized the threat and reported it. This proactive attitude and adherence to reporting protocols demonstrate that participants are aware of the dangers of phishing and are capable of responding quickly to such threats. The exercise also demonstrated the high level of technical competence among participants. They successfully completed complex technical tasks, such as forensic analysis, log analysis, and malware identification.

Another positive outcome was the quality of communication with senior management. Participants were able to effectively inform leadership about the incidents, providing clear and comprehensive updates that enabled management to make informed decisions.

The aim of this article is to present the exercise that took place and the lessons learnt during the organisation and conduct of the exercise, and thus to help health care institutions prepare for similar exercises.

Keywords: *cybersecurity, exercise, incident, technical tasks, communication tasks*

BEVEZETÉS: MIRŐL SZÓL A HUNEX?

A HunEx egy olyan, a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) által már 2017 óta szervezett komplex kibervédelmi gyakorlat, amelyet a valós infrastruktúra veszélyeztetése nélkül, saját fejlesztésű platformon keresztül végeznek a résztvevők. A valós életből vett vagy fiktív kerettörténet és a különböző feladatok révén a gyakorlatok célja a résztvevők képességeinek felmérése, belső eljárásrendek tesztelése, valamint az ágazatok közötti kapcsolatok elmélyítése.

Ezen célok kerülnek részletes bemutatásra a következőkben:

- A gyakorlat során a résztvevők különböző technikai és kommunikációs feladatokat oldanak meg, amelyek révén felmérhető, hogy mennyire felkészültek a valós kibertámadások kezelésére. Az értékelési szempontok és pontszámok alapján részletes visszajelzést kapnak teljesítményükről, ami segít azonosítani a fejlesztendő területeket.
- A gyakorlatok során lehetőség nyílik a szervezetek belső eljárásrendjeinek tesztelésére és finomítására. A résztvevők megtapasztalhatják, hogyan működnek ezek az eljárások egy szimulált vészhelyzetben, és azonosíthatják azokat a pontokat, ahol szükség van javításokra vagy átdolgozásokra.
- Az esemény célja, hogy erősítse az együttműködést és a kommunikációt az ágazati szereplők és a különböző ágazatok között. A gyakorlatban részt vevő szervezetek különböző szektorokból érkezhetnek, ami lehetőséget teremt az ágazatközi kapcsolatok építésére és a közös gyakorlatok révén szerzett tapasztalatok megosztására.
- A gyakorlat során a résztvevők olyan szituációkkal találkoznak, amelyek elősegítik a valós incidensek kivizsgálására való felkészülést. Az incidenskezelési feladatok megoldása során fejlesztik képességeiket az adatok gyűjtésében, elemzésében és a megfelelő válaszintézkedések kidolgozásában.
- A résztvevők gyakorolják a különböző incidensek kezelését, beleértve a technikai és menedzsmentszintű feladatokat. A gyakorlatok során szerzett tapasztalatok hozzájárulnak ahhoz, hogy a résztvevők jobban felkészüljenek a valós kibertámadások kezelésére.
- A résztvevők menedzsmentfeladatokat is ellátnak, beleértve a vezetői döntések előkészítését és végrehajtását, valamint a szervezet belső eljárásrendjeinek követését. Ez lehetőséget ad a menedzsmentképességek fejlesztésére és a vezetői szerepek gyakorlására.
- A gyakorlat során a résztvevők tesztelik és fejlesztik technikai és sajtókapcsolati repertoárjaikat. A belső és külső kommunikációs csatornák tesztelése, valamint a sajtóval és egyéb szereplőkkel való kapcsolattartás során szerzett tapasztalatok hozzájárulnak a kommunikációs stratégia fejlesztéséhez.

A feltárt hiányosságok és gyenge pontok azonosítása lehetőséget ad a folyamatos fejlesztésre. A résztvevők visszajelzései és a gyakorlat során szerzett tapasztalatok alapján a szervezetek javíthatják belső eljárásrendjeiket és felkészültségüket.

HOGY LEHET VALÓSÁGHŰ SZITUÁCIÓKAT SZIMULÁLNI? MI AZ INJECTEK SZEREPE?

A HunEx kibervédelmi gyakorlat során a résztvevők különféle feladatokkal és ún. „inject”-ekkel találkoztak, amelyek célja a valósághű szituációk szimulálása és a résztvevők készségeinek tesztelése volt. Az injectek olyan, a szimuláció során – például üzenet vagy hír formájában – érkező információk, amelyek a játék folyamatához és aktuális helyzethez alkalmazkodva befolyásolják az aktuális döntéseket és ezáltal a játék menetét. Tipikusan ilyen például a gyakorlat közben a kommunikációra használt platformon történő technikai jellegű adat, feladat vagy a gyakorlat háttértörténetéhez kap-

csolódó részlet megosztása, amely elősegíti a gyakorlat dinamikáját vagy könnyítést adhat egy nehéz feladathoz. Ezek a feladatok különböző típusú kihívásokat tartalmaztak, amelyek különböző területeken és szinteken mérték a résztvevők képességeit.

- A sajtó injectek célja a résztvevők sajtókommunikációs képességeinek tesztelése volt. Különböző hírek formájában megjelenő sajtóanyagokat kaptak, amelyekre megfelelően kellett reagálniuk. A feladatok között szerepelt sajtóközlemények kiadása, sajtómegkeresésekre való reagálás, és a nyilvánosság tájékoztatása.
- A platform közösségimédia-felületén megjelenő injectek a résztvevők közösségimédia-menedzsment képességeit tesztelték. Feladatuk volt az online megjelenő információk monitorozása, gyors és pontos válaszok kidolgozása, valamint a közösségimédia-csatornák kezelése. A gyakorlat közösségimédia-platformja az 1. ábrán látható.
- A technikai injectek célja a résztvevők technikai készségeinek felmérése és fejlesztése volt. Ezek többek között tartalmazták a káros kódok elemzését, logelemzést, és a virtuális gépeken történt incidensek kivizsgálását. A technikai feladatok keretében a résztvevők igazságügyi hatósági (forensics) jellegű elemzéseket is végeztek, hogy megállapítsák, milyen események és incidensek történtek, és hogy történt-e adatszivárgás.
- A menedzsment injectek a vezetői döntéshozatal és a szervezet belső eljárásrendjeinek tesztelésére irányultak. A résztvevőknek döntéseket kellett hozniuk az incidensek kezelésével kapcsolatban, és tájékoztatniuk kellett a vezetőséget az incidens alakulásáról. A szervezet vezetésével együttműködve kellett kidolgozniuk és végrehajtaniuk az ellenintézkedéseket.
- Az irányító hatósági injectek a jogszabályoknak és hatósági előírásoknak való megfelelést tesztelték. A résztvevők feladatai közé tartozott a megfelelő formában és időben történő jelentések megküldése a hatóságok részére, valamint a hatóságokkal való folyamatos kommunikáció fenntartása.
- Az adatvédelemmel kapcsolatos injectek a résztvevők adatvédelmi incidenskezelési képességeit tesztelték. A feladatok között szerepelt az adatvédelmi incidensek megfelelő kezelése, az érintettek tájékoztatása, és a hatóságok felé történő bejelentés.

Az alábbi példán keresztül bemutatásra kerül, hogyan történik a sajtómegkeresés a gyakorlat során.

„EXERCISE EXERCISE EXERCISE

Tisztelt Játékos Szervezet!
Lapunk információi szerint online rendszereikben tapasztalható fennakadás oka egy kibertámadás. Kérjük, válaszoljanak néhány, ezzel kapcsolatos kérdésre a lakosság tájékoztatása érdekében!
– Milyen támadás történt pontosan?
– Milyen intézkedéseket hoztak a támadás hatásának megszüntetésére?
– Bejelentették-e az incidenst a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet CSIRT-jének?
– Betegadatokat érintett-e a támadás?
– Hogyan állnak jelenleg a kivizsgálással?

Kérjük, hogy sajtóközleményüket lehetőleg a következő 30 percen belül juttassák el szerkesztőségünknek, hogy azt érdemben fel tudjuk használni!

Üdvözlettel,
Kovács Péter
Kiber Nemzet

EXERCISE EXERCISE EXERCISE”

1. ábra
Bleeter – a gyakorlat közösségimédia-felülete (saját szerkesztés)

A CSAPATOK ÖSSZEÁLLÍTÁSA ÉS FELADATKÖREIK

A HunEx kibervédelmi gyakorlat során a résztvevő csapatok tagjai különböző szerepkörökre oszlottak, amelyek mindegyike egy-egy speciális feladatkört látott el. A csapatok tipikus összetétele változatos volt, és a különböző szerepkörökben dolgozó tagok szoros együttműködésben végezték feladataikat. Az alapvető csapatösszetétel általában egy vezetőből vagy csapatkoordinátorból, két incidenskivizsgálóból, egy sajtószóvivőből és egy jogászból állt. Az egyes szerepkörökben dolgozó tagok különféle feladatokat láttak el, amelyek hozzájárultak a gyakorlat sikeres végrehajtásához.

A csapat vezetője, aki egyben a csapat koordinátora is volt, irányította a csapat munkáját, biztosította a feladatok megfelelő elosztását, és gondoskodott a különböző szerepkörök közötti hatékony kommunikációról. Ő felelt a stratégiai döntéshozatalért és az incidensek kezelésére irányuló tervek kidolgozásáért. A vezető feladata volt továbbá a felsővezetés tájékoztatása és a vezetői döntések végrehajtásának koordinálása is.

A két incidenskivizsgáló fő feladata a technikai incidensek kezelése és a fenyegetésmenedzsment volt. Ők végezték a logelemzéseket, káros kódok elemzését, valamint a virtuális gépeken történt incidensek kivizsgálását. Az incidenskivizsgálók munkája kulcsfontosságú volt a technikai feladatok sikeres megoldásában, mivel ők azonosították az eseményeket és az incidensek forrásait, valamint meghatározták a szükséges ellenintézkedéseket.

A sajtószóvivő szerepe szintén meghatározó volt a gyakorlat során. Ő kezelte a sajtómegkereséseket, sajtóközleményeket adott ki, és gondoskodott a nyilvánosság megfelelő tájékoztatásáról. A sajtószóvivő feladata volt továbbá a közösségi médiában megjelenő információk monitorozása és a közösségimédia-csatornák kezelése. A szóvivő közvetítette a szervezet hivatalos álláspontját, és biztosította, hogy a kommunikáció összhangban legyen a szervezet eljárásrendjeivel.

A jogász feladata az incidensekkel kapcsolatos jogi kérdések kezelése volt. Ő biztosította, hogy a szervezet minden tevékenysége megfeleljen a jogszabályoknak és a hatósági előírásoknak. A jogász koordinálta a hatóságokkal való kapcsolattartást, előkészítette a szükséges jogi dokumentumokat, és gondoskodott arról, hogy a jelentések és bejelentések megfelelő formában és időben történjenek.

A csapatokban dolgozó további munkatársak száma nem volt limitálva, így szükség esetén több szakember is bevonható volt a feladatok megoldásába. A csapatok rugalmasan alkalmazkodtak a felmerülő kihívásokhoz, és együttműködve oldották meg a különböző technikai és kommunikációs feladatokat. Az egyes szerepkörök közötti szoros együttműködés biztosította, hogy a gyakorlat során minden terület hatékonyan működjön, és a résztvevők sikeresen teljesítsék a rájuk bízott feladatokat.

A HunEx kibervédelmi gyakorlat során kialakított csapatstruktúra és a különböző szerepkörök együttműködése hozzájárult ahhoz, hogy a résztvevők átfogó képet kapjanak a kibervédelmi kihívásokról, és hatékonyan felkészülhessenek a valós incidensek kezelésére. A csapatok előzetes feladatai között szerepelt a kommunikációs csatornák tisztázása, mely során a belső és a külső kommunikációs csatornák kerültek meghatározása annak érdekében, hogy biztosítsák a hatékony információáramlást az incidensek során.

Főbb feladatok, melyeket a gyakorlat során a résztvevőknek teljesíteniük kellett:

- Feladatok és bejelentések fogadása: a résztvevőknek folyamatosan fogadniuk kellett a különböző feladatokat és bejelentéseket, és megfelelően kellett reagálniuk ezekre.
- Sajtó monitorozása és fenyegetettségmenedzsment: a sajtóban megjelenő információk folyamatos nyomon követése és a fenyegetettségmenedzsment szintén a gyakorlat része volt, annak érdekében, hogy a résztvevők gyorsan és hatékonyan reagálhassanak a médiában megjelenő információkra.
- Logelemzés és károskód-elemzés: a technikai feladatok közé tartozott a logelemzés és a káros kódok elemzése, hogy a résztvevők azonosítani tudják az esetleges támadásokat és azok forrásait.
- Reaktív incidenskezelés: a résztvevőknek az összefüggéseket vizsgálva kellett reaktív incidenskezelési feladatokat végrehajtaniuk, amelyek célja az incidensek hatékony kezelése volt.
- Kapcsolattartás és ellenintézkedések kidolgozása: a résztvevők folyamatosan kapcsolatban álltak az eseménykezelő központtal, és kidolgozták az ellenintézkedéseket, amelyeket meg is küldtek az érintetteknek.
- Elemzőcsapat koordinálása: az elemzőcsapat koordinálása a szervezet belső eljárásrendje szerint történt, a résztvevőknek a csapat munkáját kellett összehangolniuk.
- Vezetői döntések előkészítése és végrehajtása: a vezetői döntések előkészítése és végrehajtása is része volt a gyakorlatnak, a résztvevőknek ebben az esetben is a szervezet belső eljárásrendje szerint kellett cselekedniük.
- Sajtómegkeresések fogadása és válaszadás: a sajtómegkeresések fogadása és válaszadása szintén fontos feladat volt, amelynek során a résztvevőknek a szervezet belső eljárásrendje szerint kellett eljárniuk.
- Incidenskezelési feladatok: a technikai feladatok között szerepeltek az incidenskezelési feladatok, amelyek célja a résztvevők technikai készségeinek tesztelése volt.
- Vezetői tájékoztatók készítése: a vezetői tájékoztatók készítése során a résztvevőknek átlátható és érthető módon kellett összefoglalniuk az incidensekkel kapcsolatos információkat.
- CTF (Capture The Flag) feladatok: a CTF feladatok során a résztvevőknek „flag”-eket kellett keresniük a virtuális

gépeken és dokumentálniuk kellett az útjukat, amely a technikai készségeik fejlesztését szolgálta.
- Technikai adatok kinyerése: a technikai adatok kinyerése során a résztvevőknek adatokat kellett gyűjteniük és elemezniük az incidensekkel kapcsolatban.

A feladatok célja a kommunikációs csatornák tisztázása, a sajtó folyamatos monitorozása, logelemzés, károskódelemzés, valamint a reaktív incidenskezelés volt. A résztvevők emellett az eseménykezelő központtal is kapcsolatot tartottak, és ellenintézkedéseket dolgoztak ki.

A kibervédelmi gyakorlat során a feladatok két nagy csoportra oszthatók. Az egyikben a fő hangsúly a technikai feladatokon van, a másikban pedig a döntéshozatal és a kommunikáció játszik főszerepet.

TECHNIKAI FELADATOK

A HunEx kibervédelmi gyakorlat technikai feladatai kiemelkedő jelentőséggel bírtak, mivel ezek segítségével mérték fel a résztvevők technikai készségeit és képességeit a kibertámadások kezelésében. Ezek a feladatok különböző szintű és típusú kihívásokat tartalmaztak, amelyek valósághű szimulációk révén tesztelték a résztvevők felkészültségét. A technikai feladatok központi eleme volt a virtuális gépek incidenskivizsgálása. A résztvevőknek előre megadott adatok alapján kellett kivizsgálniuk, hogy milyen események és incidensek történtek ezekben a gépekben. A vizsgálat során a résztvevőknek azonosítaniuk kellett a káros kódokat, elemezniük kellett a logokat, és meg kellett állapítaniuk, hogy történt-e adatszivárgás. Ez a feladat lehetőséget adott a résztvevőknek, hogy alkalmazzák a forensics-technikákat és -módszereket, valamint fejlesszék elemzőképességeiket.

A feladatok között szerepelt továbbá a zsarolóvírus-támadások kezelése, ahol a résztvevőknek részletes jelentést kellett készíteniük a támadásról. Ennek során fel kellett térképezniük az érintett rendszereket, leírniuk a támadás menetét, azonosítaniuk a károkat és meghatározniuk a szükséges ellenintézkedéseket. A zsarolóvírus-támadások kezelése különösen fontos volt, mivel ezek az incidensek súlyos következményekkel járhatnak, így gyors és hatékony reagálást igényelnek.

A technikai feladatok közé tartozott a káros kódok elemzése is, amelynek során a résztvevőknek azonosítaniuk kellett a rosszindulatú szoftvereket, és meghatározniuk, hogy milyen intézkedéseket szükséges tenni a fenyegetés elhárítására. Ez a feladat segítette a résztvevőket abban, hogy fejlesszék az ilyen szoftverekre vonatkozó elemzési képességeiket, és megértsék, hogyan működnek ezek a kártékony programok.

A technikai feladatok megoldása során a résztvevőknek továbbá be kellett azonosítaniuk a támadások forrásait és összefüggéseit. Ez magában foglalta a különböző események közötti kapcsolatok feltárását, és a reaktív incidenskezelési intézkedések kidolgozását. A résztvevőknek folyamatosan figyelemmel kellett kísérniük a beérkező jelentéseket és bejelentéseket, és gyorsan kellett reagálniuk a felmerülő problémákra.

DÖNTÉSHOZATAL ÉS KOMMUNIKÁCIÓS FELADATOK

A döntéshozatal és a kommunikációs feladatok központi szerepet játszottak a HunEx gyakorlat során, mivel ezek révén tesztelték a résztvevők képességeit a vezetői döntéshozatalban és a hatékony kommunikációban. Ezek a feladatok széles spektrumot öleltek fel, a stratégiai döntéshozataltól kezdve a sajtókommunikáción át a hatóságokkal való kapcsolattartásig.

A döntéshozatal során a résztvevőknek számos vezetői feladatot kellett ellátniuk. Ezek közé tartozott a szervezet belső eljárásrendjeinek követése és a vezetői döntések előkészítése. A résztvevőknek gyorsan kellett reagálniuk a felmerülő incidensekre, és hatékonyan kellett koordinálniuk a csapatok munkáját. A vezetői döntések meghozatalakor figyelembe kellett venniük az aktuális helyzetet, a rendelkezésre álló információkat és a lehetséges következményeket.

A kommunikációs feladatok közé tartozott a sajtómegkeresések kezelése, sajtóközlemények kiadása és a nyilvánosság tájékoztatása. A résztvevőknek biztosítaniuk kellett, hogy a kommunikáció összhangban legyen a szervezet eljárásrendjeivel, a közlemények pontosak és időszerűek legyenek. A sajtóval való kapcsolattartás során a résztvevőknek válaszolniuk kellett a média kérdéseire, és biztosítaniuk kellett, hogy az információk megfelelően és érthetően kerüljenek közlésre.

A hatóságokkal való kapcsolattartás szintén fontos része volt a kommunikációs feladatoknak. A résztvevőknek elő kellett készíteniük a szükséges jogi dokumentumokat és jelentéseket, és gondoskodniuk kellett arról, hogy ezek időben és megfelelő formában kerüljenek megküldésre a hatóságok részére. A hatóságokkal való folyamatos kommunikáció biztosította, hogy az incidensekkel kapcsolatos információk eljussanak a megfelelő szervekhez, és a szükséges intézkedések megtörténjenek.

A döntéshozatal és kommunikációs feladatok során a résztvevőknek továbbá a belső és külső partnerekkel is kapcsolatot kellett tartaniuk. Ez magában foglalta a szervezet vezetésének tájékoztatását, a belső kommunikációs csatornák tesztelését, valamint a külső partnerek, ügyfelek és érintettek tájékoztatását. A résztvevőknek biztosítaniuk kellett, hogy a kommunikáció minden szinten hatékony és összehangolt legyen, és az információk gyorsan, pontosan eljussanak a megfelelő helyekre.

A HunEx gyakorlat során a döntéshozatal és kommunikációs feladatok végrehajtása kulcsfontosságú volt a gyakorlat sikeréhez. Ezek a feladatok segítettek a résztvevőknek fejleszteni vezetői és kommunikációs képességeiket, és biztosították, hogy a szervezet hatékonyan tudjon reagálni a felmerülő kibertámadásokra és incidensekre.

MIBEN SZÜKSÉGES MÉG FEJLŐDNI?

A HunEx kibervédelmi gyakorlat során feltárt hiányosságok és gyenge pontok rávilágítottak a résztvevők és a szervezetek azon területeire, amelyek további fejlesztésre és javításra szorulnak. Az egyik leggyakrabban tapasztalt probléma a külső és belső ügyfelek megfelelő tájékoztatásának hiánya volt. Számos esetben előfordult, hogy a kommunikáció nem volt elégséges vagy teljesen elmaradt, ami komoly problémákat okozhat egy valós incidens során. Az ügyfelek, partnerek és érintettek időben történő és pontos tájékoztatása elengedhetetlen a bizalom megőrzéséhez és a helyzet hatékony kezeléséhez.

Egy másik jelentős hiányosság a hatóságokkal és a CSIRT (Computer Security Incident Response Team) irányába történő kommunikációban mutatkozott meg. A gyakorlat során többször előfordult, hogy a résztvevők nem tudták megfelelően, időben és formailag helyesen jelenteni az incidenseket a hatóságoknak. Ez a gyenge pont különösen kritikus lehet egy valós támadás esetén, mivel a hatóságokkal való gyors és pontos kommunikáció elengedhetetlen a megfelelő válaszintézkedések meghozatalához.

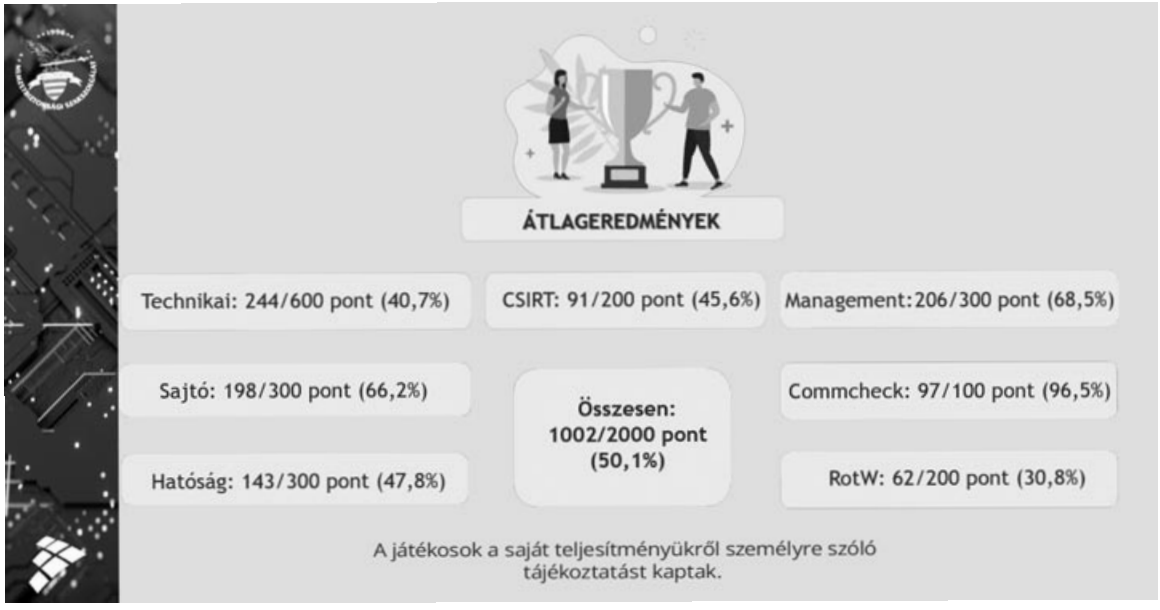
Az adathalász (phishing) próbálkozásokra való „rámozdulás" szintén gyakori probléma volt a résztvevők körében. Sok esetben a résztvevők nem tudták felismerni az adathalász e-maileket, ami azt jelzi, hogy további képzésre és figyelemfelhívásra van szükség ezen a területen. Az adathalászat elleni védekezés kulcsfontosságú a szervezetek számára, mivel ezek a támadások gyakran a leggyengébb láncszemre, az emberi tényezőre irányulnak.

MI VOLT AZ, AMI A GYAKORLAT SORÁN KIEMELÉSRE MÉLTÓ?

A HunEx gyakorlat pozitívumai között számos olyan eredményt és tapasztalatot lehet kiemelni, amelyek hozzájárultak a résztvevők készségeinek és képességeinek fejlődéséhez. Az egyik legjelentősebb pozitívum az adathalászat felismerése és jelentése volt. Bár sok résztvevő vált adathalász próbálkozások áldozatává, pozitívumként említhető, hogy a legtöbben jelezték ezeket az incidenseket. Ez a proaktív hozzáállás és jelentési fegyelem azt mutatja, hogy a résztvevők tisztában vannak az adathalászat veszélyeivel, és képesek gyorsan reagálni az ilyen típusú fenyegetésekre.

A technikai hozzáértés is kiemelkedő pozitívum volt a gyakorlat során. A résztvevők bizonyították, hogy magas szintű technikai ismeretekkel rendelkeznek, és képesek komplex technikai feladatok megoldására. A forensics elemzések, logelemzések és káros kódok azonosítása során szerzett tapasztalatok hozzájárultak a résztvevők technikai készségeinek továbbfejlesztéséhez.

A felsővezetés megfelelő minőségű értesítése szintén pozitív eredmény volt a gyakorlat során. A résztvevők képesek voltak átlátható és érthető módon tájékoztatni a vezetést az incidensekről, ami kulcsfontosságú a gyors és hatékony döntéshozatalhoz. Az érthető és részletes tájékoztatás lehetővé tette, hogy a vezetők megfelelő intézkedéseket hozzanak és irányítsák a válaszintézkedéseket.



2. ábra
A gyakorlat eredménye (saját szerkesztés)

Az ábrán szereplő rövidítések:
Commcheck: a gyakorlatot megelőző, a kommunikációs csatornák ellenőrzésére használt üzenetváltás.
CSIRT: a gyakorlat ideje és keretei között megjeleníti a hatályos jogszabályok által előírt, az NKI által működtetett Nemzeti Eseménykezelő Központot.
RotW: a szerepkör ellátója az összes, a gyakorlatban nem szereplő intézményt helyettesíti. Ha a gyakorlat résztvevőinek egy olyan partnerrel kell kapcsolatot létesíteni, aki egyébként nem vesz részt a játékban, akkor ezt az elérhetőséget kell megszólítania.

LEGFONTOSABB EREDMÉNYEK ÉS KONKLÚZIÓ

Összességében a HunEx gyakorlat során szerzett pozitív tapasztalatok és eredmények hozzájárultak a résztvevők felkészültségének növeléséhez és kibervédelmi képességeik fejlesztéséhez. A gyakorlat során feltárt hiányosságok és gyenge pontok pedig lehetőséget adtak a résztvevőknek és a szervezeteknek arra, hogy javítsák belső folyamataikat és felkészültségüket a jövőbeni kihívásokra.

A gyakorlat során szerzett tapasztalatok és eredmények alapján megállapítható, hogy a résztvevők technikai és kommunikációs képességei jelentősen fejlődtek. A gyakorlatok révén feltárt hiányosságok és gyenge pontok lehetőséget adnak a folyamatos fejlesztésre és a jövőbeni incidensekre való jobb felkészülésre.

Az egészségügyi szektor számára szervezett gyakorlatokon összesen 26 egészségügyi szervezet vett részt, több mint 160 játékossal. A feladatok megoldása közben több mint 1000 e-mail került kiküldésre a 350-nél is több levélváltás során. A kibervédelmi gyakorlat összesített eredményét a 2. ábra szemlélteti.