ISZT HunCERT
2023 évi kommunikációs gyakorlat
értékelő összefoglalás

ISZT HunCERT —SZTAKI
2023. október

Összegzés

Ez a dokumentum az ***Internet Szolgáltatók Tanácsa*** – ***ISZT*** – megbízásából és érdekében a ***SZTAKI*** munkatársaiból álló, hálózati incidenskezeléssel megbízott csoportja, a ***HunCERT*** által 2023. október 25-dikei kezdettel végrehajtott, három napos átfogó kommunikációs gyakorlat összefoglaló értékelése.

A gyakorlat elsődleges célja a HunCERT ***által használt információs lánc frissítése, ellenőrzése, illetve az egységes eljárásrend gyakorlása, a HunCERT ágazati CERT szerepének erősítése*** volt.

A gyakorlat során a szolgáltatók adminisztrációs és műszaki feladatot is kaptak, melynek végrehajtása során a kommunikációs folyamatot a HunCERT eseménykezelő rendszerében rögzítettük.

Az előző évekhez hasonlóan számos szervezet 19 ISZT tag, 22 BIX tag és 41 regisztrátor és 11 kiemelt incidenskezelési szerződéssel rendelkező szolgáltató vett tevékenyen részt. Idén a gyakorlatot HUNOG-n történt előzetes bejelentés előzte meg , az ISZT elnökségét tájékoztattuk a gyakorlat tényéről, valamint csatlakozva az európai kiberbiztonsági hónaphoz, annak részeként regisztráltuk a gyakorlatot. A gyakorlatba bevontuk az ISZT tagokat és az ISZT-vel kiemelt incidenskezelési szerződésben álló, összesen 52 hazai internet szolgáltatót illetve az ISZT-vel szoros kapcsolatban lévő partnereket (hazai BIX tagok és domain

A gyakorlat, megítélésünk szerint, csak részben érte el célját, mivel a bevont szolgáltatók kis része vett csak részt benne. Ez elsősorban az újonnan bevont szolgáltatók elmaradását jelenti, a korábban is résztvevők többsége most is aktívan részt vett.

Véleményünk szerint a közös gyakorlatok hozzájárulnának a felek közti jobb megértéshez, végső soron pedig a hatékonyabb, félreértésektől mentes együttműködéshez. Ezért javasoljuk, hogy hasonló, illetve más tematikájú gyakorlatra az ISZT tagok, a BIX tagok és domain regisztrátorok, kihelyezett szenzorral (probe) rendelkezők és esetlegesen az Elnökség által még javasoltak bevonásával a jövőben is kerüljön sor.

Köszönetünket fejezzük ki mindazoknak, akik hozzájárultak munkánkhoz. Reméljük, hogy aktív támogatásukra majd az eljövendő további gyakorlatok idején is számíthatunk!

Az alábbi oldalakon a gyakorlat részletes menetét, valamint az ebből származó, anonimizált mérési eredményeket és következtetéseket ismertetjük.

Üdvözlettel,

a HunCERT csapat

Rigó Ernő
Bisztray Frigyes

Medgyesi Dorottya
Ormos Pál

Bevezetés

A ***HunCERT***, alaptevékenységi körének megfelelően és az elmúlt évekhez hasonló módon, 2023. október 25-én, az európai kiberhónap eseményeihez kapcsolódóan elindította az immár hagyományosnak tekinthető kommunikációs gyakorlatát, melyre idén munkaidőben került sor.

Az ISZT HunCERT-ről

Az Internet Szolgáltatók Tanácsa hazánkban elsőként, 2003-ban alapította meg a HunCERT-et. A kezdeményezés célja a Magyarországot érintő hálózatbiztonsági incidensek kezelése, felderítése, elemzése, valamint az ezekre adott reakciók koordinációja és értékelése. A koordinációs tevékenység mellett a HunCERT elsődleges céljai között szerepel a hazai felhasználók számítógépes biztonsági tudatosságának növelése, melynek érdekében publikációkat, oktatási anyagokat és biztonsági híreket tesz közzé, valamint workshopokat szervez különböző biztonságot érintő témákban. A HunCERT elkötelezett a fogyatékossággal élő személyek biztonsági tudatosításában is, ezért 2022-ben az ISZT-vel közösen elindította az *„Akadályok nélkül”* rendezvénysorozatot.

A gyakorlat célja, előkészítése

A gyakorlat elsődleges célja a HunCERT incidenskezelési hatékonyságának felmérése, illetve lehetőség szerinti növelése volt. A nemzetközi tapasztalatok is azt mutatják, hogy az incidenskezelésekben az egyik kritikus pont a kapcsolat felvétele az érintettekkel. Ezért kiemelt hangsúlyt kapott a kapcsolati pontok frissítése. Ennek érdekében az alábbi alapvető célokat tűztük ki:

- A HunCERT kapcsolati adatbázisának aktualizálása.
- A szolgáltatók oldalán elérhető incidens értesítési kapcsolati pontok egyértelmű meghatározása.
- A HunCERT által kiadott értesítésekre történő kommunikációs válaszidők mérése és értékelése.
- A HunCERT által kiadott kérésekre történő technikai, adminisztratív jellegű reakciók, valódi beavatkozások értékelése.
- A gyakorlatot összefoglaló értékelés összeállítása és publikálása.

A gyakorlat során a kapcsolattartás elsődleges eszközeként elektronikus levelek alkalmazását terveztük. A szolgáltatók túlnyomó többsége rendelkezik olyan e-mail címmel vagy címekkel, amelyek incidensek bejelentésére szolgálnak (példa ilyenre az „***abuse***” cím). A gyakorlat során a korábbi években egyeztetett és saját adatbázisunkban fellelhető címeket, ill. az egyes szolgáltatók (BIX tagok és domain regisztrátorok) nyilvánosan elérhető címeit használtuk.

Az adminisztratív, kapcsolati jellegű előkészítés mellett a gyakorlatot technikai oldalról is előkészítettük.

A HunCERT az incidenskezelés eseményeinek naplózott nyilvántartására hosszabb ideje egy kiterjedt képességekkel rendelkező eseménykezelő (ticketing) rendszert alkalmaz. Ez a rendszer fogadja a különféle e-mail címeinkre érkező leveleket, tárolja azokat, majd újonnan generált, illetve már létező esemény-nyilvántartó hibajegyekhez rendeli azokat.

A gyakorlatba ISZT tagokat és a kiemelt incidenskezelési szerződéssel rendelkező ISZT tagokat valamint hazai BIX tagokat és domain regisztrátorokat vontuk be.

A gyakorlat megkezdése előtt néhány héttel a gyakorlat pontos idejét és a gyakorlat témáját egyeztettük az ISZT elnökségével és bejegyeztük a 2023. évi kiberhónap eseményei közé is..

Ha megemlítettük a célokat, essen szó arról is, mi nem volt célunk a gyakorlattal.

Semmiképp sem akartuk gyakorlott kollégáink szakmai tudását ellenőrizni, mivel annak megléte nem kétséges. Ezért a forgatókönyv egy bonyolult műszaki helyzet leküzdése helyett csupán egy egyszerű *adminisztratív feladat* megoldását és egy egyszerűbb műszaki feladat kezelését célozta. De elsődlegesen ennek sem technikai megoldását vizsgáltuk, hisz a fő cél: az egymás közti kommunikáció minőségének felmérése, javítása volt.

Nem volt célunk a résztvevők között versenyt hirdetni, így személyre szóló eredményt sem közlünk. E helyett ***anonimizált***, összegző adatokat osztunk meg azt remélve, hogy a közölt adatok és tapasztalatok mindenki számára értékkel bírnak.

Nem volt célunk a partner hálózatok normális forgalmának befolyásolása. Semmiképp sem akartuk e hálózatokat megtámadni, biztonsági réseket keresni, még etikus módszerekkel sem.

Végképp nem akartuk az épp elég feladattal küzdő, elfoglalt kollégák teendőit feleslegesen szaporítani. Ezért csupán egyszerű technikai és adminisztratív lépések megtételét vártuk el, ismét hangsúlyozva: a lényeg a hírcsere, az üzenetváltások megtörténte volt.

A gyakorlat forgatókönyve

Amint azt már többször hangsúlyoztuk, a gyakorlat elsődleges célja a résztvevők közti kommunikáció jelenlegi állapotának vizsgálata, valamint hatékonyságának fokozása volt.

A gyakorlat során lépések a következők voltak:

Az értesítésben a HunCERT kéri a résztvevőket, hogy a HunCERT hab rendszerében található címeiket frissítsék, aktualizálják. Amennyiben nem rendelkeznek hozzáféréssel akkor kérésre létrehozzuk azt. Ezen kívül kértük, hogy írják meg milyen email biztonsági policy-ket alkalmaznak (SPF, DKIM, DMARC, BIMI, stb.) [***1. levél***]

1. Az értesített szolgáltatók válaszlevélben a HunCERT-et informálják, hogy az értesítő levelet megkapták, és frissítették az adataikat a hab.cert.hu oldalon és megírják az email policy-jüket is. [1***. válaszlevél***]
2. Nagyjából az első értesítéstől számított 1 nap után a HunCERT ismételten értesíti az adott résztvevőhöz tartozó értesítési címére küldött emailben azokat a szolgáltatókat, akik az első megkeresésre nem reagáltak, ugyanazt kérve, mint amit a gyakorlat indító levélben. [***megismételt 1. levél***]
3. A gyakorlat utolsó kommunikációs lépése a gyakorlat végét jelző HunCERT levél. Ebben mindenkinek megköszönjük a gyakorlaton való részvételt.[***2. levél***]

Az eredmények értékelése

A gyakorlat értékeléséhez szükséges számszerű adatok többségét az eseménykezelő rendszer szolgáltatta.

Ez a rendszer tárolta a gyakorlat során küldött és kapott valamennyi e-mailt, így az adatok a kiértékelés során innen kinyerhetők voltak.

A számszerű adatok alapján elkészült összesítéseket – legjobb tudásunk szerint – igyekeztünk az értelmezést megkönnyítő diagramok, időfüggvények és más lényegkiemelő prezentációs megoldások segítségével bemutatni.

A számszerű adatokból származó diagramokat a legtöbb esetben rövid szöveges értékelés követi, amely igyekszik felhívni a figyelmet a fontosabb körülményekre, valamint a gyakorlat lebonyolítása során tapasztalt jelenségekre.

Fontosnak ítéljük azon cél elérését, hogy a lebonyolított gyakorlat eredményei, és megfogalmazott következtetései – amely sok ember egyesített tudásának és együttes erőfeszítésének köszönhetően állt elő – a résztvevő tagok további munkáját segítse, de ne szolgálhasson felesleges ellentétek, feszültségek alapjául. Ezért az itt bemutatott adatok kizárólag ***összesített*** és ***anonimizált*** információkat tartalmaznak.

E néhány előzetes megfontolás után következzenek a feldolgozott adatok és az ezekből levont következtetések!

A gyakorlat során összegyűjtött adatokat számos szempont szerint igyekeztünk értékelni. Az elemzett és értékelt szempontok a következők:

A gyakorlat tervezett résztvevői

A HunCERT által vezetett gyakorlat résztvevői az ISZT tag szervezetei , a BIX tagok, a domain regisztrátorok voltak. Az ISZT tagok listája az ISZT honlapján megtalálható (http://www.iszt.hu/). A BIX tagok listája a BIX honlapján megtalálható (https://www.bix.hu/tagok). A domain name regisztrátorok listája pedig az alábbi linken érhető el: https://www.domain.hu/regisztratorok/

A gyakorlatban résztvevő és a távol maradók száma, aránya

Sajnálattal kell megállapítani, hogy a gyakorlatba bevont résztvevők jelentős része nem vett részt a gyakorlatban. Jó hír viszont, hogy a kiemelt incidenskezelési szerződéssel rendelkező szolgáltatók valamennyien részt vettek a gyakorlatban. A gyakorlatba bevont CERT-ek is teljes létszámban vettek részt. A regisztrátorok - akikkel ha nem ISZT tagok korábban semmilyen kapcsolatunk nem volt és a gyakorlatról sem tudtak – viszonylag nagy számban vettek részt.

Résztvevők	ISZT tagok száma	BIX tagok száma	Regisztrátorok
Összes	*52*	*63*	*120*
Részt vett	*19*	*22*	*41*
Arány	*36,53*	*34,92*	*34,16*

Meg kell jegyeznünk, hogy átfedések is vannak. Van olyan szolgáltató, aki akár kettő vagy mind a három kategóriába is beletartozik.

Az ISZT elnökség számára fontos, hogy a velük incidenskezelési szerződéssel rendelkezők milyen arányban vettek részt a gyakorlatban. Elmondhatjuk, hogy 100 %-uk részt vett és elég hamar is válaszolt a kérésre.

Az előkészítő időszak

A gyakorlat előkészítését 2023 augusztus végén már megkezdtük. Ekkor került meghatározásra a gyakorlat időtartama és időpontja is. És ekkor regisztráltuk be a gyakorlatot a kiberhónap eseményei közé is.

Kommunikációs adatok

Az incidenskezelés kapcsán alkalmazott elsődleges kommunikációs csatorna az elektronikus levelezés. Ha ez nehézkes lenne, akkor fordulunk csak a személyes – telefonos – megkeresés felé. Minderre figyelemmel alapvetően fontos, hogy ismerjük partnereink kapcsolati adatait.

A leírtakra tekintettel a gyakorlat részét képező üzenetek célba juttatásához is az elektronikus levelezést használtuk, telefonhívást mi nem kezdeményeztünk, gyakorlattal kapcsolatos hívásokat nem kaptunk.

A fentiek értelmében kiemelten fontos, hogy minden szolgáltató esetében olyan e-mail címeket ismerjünk, amely valóban azok által figyelt cím, akik az incidensek kezelésében érintettek.

Az általunk használt email címek azok a címek voltak, amelyeket az önkéntesek a hab.cert.hu oldalon a regisztrációkor megadtak. Ezen kívül a regisztrációval nem rendelkező szolgáltatók esetében a nyilvánosan elérhető oldalakról származó információk alapján gyűjtöttünk be.

Vannak olyan új ISZT tag szolgáltatók, akiknek sem az abuse-, sem pedig egyéb e-mail címei nem szerepeltek még a nyilvántartásunkban. Az ő esetükben igyekeztünk a honlapjukról megszerezni ezeket, vagy a domain-jükhöz tartozó abuse@ címet használni.

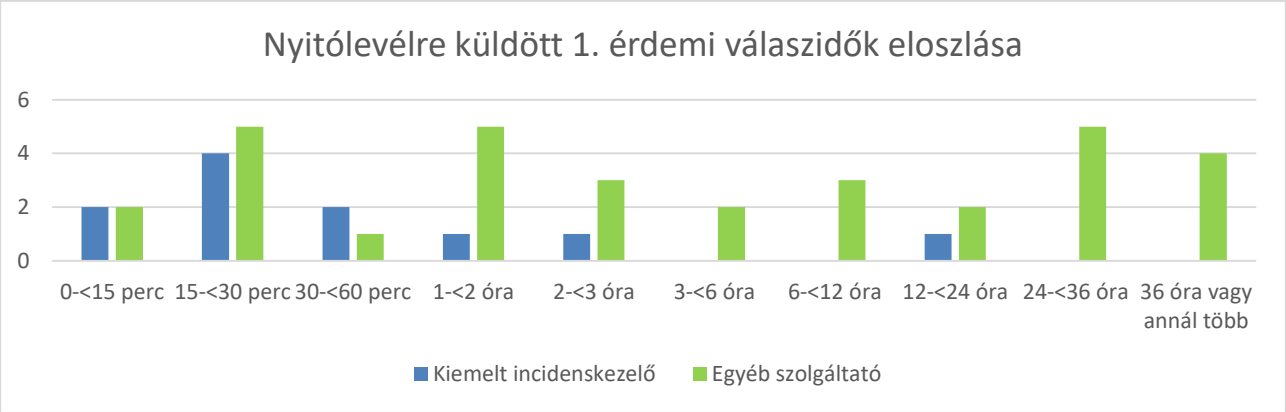
A gyakorlat kezdete – az 1. levél kiküldése

2023. október 25-én 09:55 perckor elindítottuk a gyakorlatot, vagyis kiküldtük a résztvevők ismert e-mail címére a feltételezett támadásról szóló értesítést. Ebben a levélben egyrészt arra kértük a szolgáltatókat, hogy nyugtázzák a levél vételét, aktualizálják az adataikat a hab.cert.hu oldalon és írják meg milyen email policy beállításokat használnak.

A lenti grafikonból jól látható, hogy a leggyakoribb reakcióidők 15-30 és 60 – 120 perc között voltak. Tekintettel arra, hogy a gyakorlat kezdetének időpontja nem volt előre meghirdetve ez jó reakcióidőnek számít. Persze abból a szempontból nem vonható le következtetés, hogy mi történne abban az esetben, ha munkaidőn túl történne ilyen előre nem meghirdetett gyakorlat vagy incidens.

Az is látható, hogy többen csak 24 vagy 36 óránál több idő elteltével reagáltak a megkeresésre.

A kiemelt incidenskezelési szerződéssel rendelkezők közül a leggyakoribb reakció idő 2-3 óra közé tehető.



A gyakorlat folytatása– a 1. levél ismételt kiküldése

A gyakorlat során azon résztvevők számára, akik a gyakorlat kezdetét jelző e-mailre nem válaszoltak 2023. október 26-án 09:37 perckor ismételten kiküldtük a gyakorlattal kapcsolatos 1. levelet.

A mostani értékelésnél nem tettünk különbséget abból a szempontból, hogy az első vagy a megismételt levél hatására válaszoltak a szolgáltatók. A reakció időket ugyanúgy kezeltük és az előző pontban közölt grafikonban szerepelnek az adatok. Természetesen a megismételt esetben már nem volt automata válasz, hiszen akiktől a kezdő levélre jött ilyen, azoknak nem küldtünk megismételt levelet.

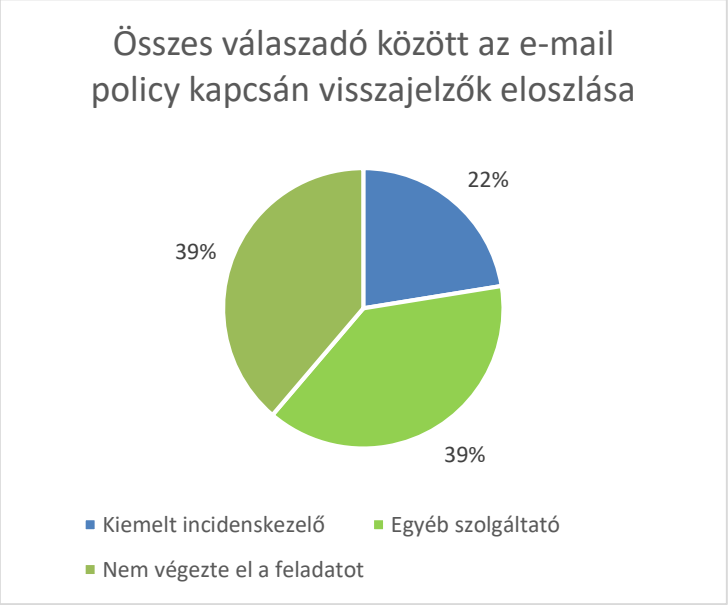
A gyakorlat zárása– a 2. levél kiküldése

Elérkeztünk a gyakorlat utolsó fázisához, a záráshoz. 2023. október 27-én 09:23-kor került sor a záró, azaz a 2. második levél kiküldésére. A záró levélben minden résztvevőt egyenként értesítettünk a gyakorlat végéről és megköszöntük a gyakorlatban való részvételüket.

A gyakorlat további feladata

Az idei gyakorlat annyiból rendhagyó volt, hogy az idei kiberhónap eseményeihez csatlakozva felmérést készítettünk arról, hogy a szolgáltatók milyen email biztonsági policyval rendelkeznek.

A grafikonon jól látszik, hogy az összes gyakorlatban résztvevő milyen %-s megosztásban válaszolt az email policy kapcsán feltett kérdésünkre.



Összefoglalás

A gyakorlat a résztvevők száma miatt alapvetően sikeresnek mondható ám célszerűnek látnánk, ha több szolgáltató aktívan csatlakozna a gyakorlathoz. Abból a szempontból is sikeresnek mondható, hogy sikerült néhány újabb szolgáltatótól konkrét elérhetőséget kapni. Elmondható, hogy a nagy szolgáltatók - szinte kivétel nélkül - nem vetek részt a gyakorlatban.

A gyakorlat során megállapítást nyert számunkra, hogy sokkal inkább működnek azok a kommunikációs csatornák, melyeket a HunCERT korábban a szolgáltatókkal folytatott személyes egyeztetések során már pontosított.

A gyakorlat során, ahogy már fentebb említettük néhány szolgáltatóval a kommunikációra használt email címeket pontosítottuk. Eredménynek tekintjük ezzel kapcsolatban, hogy 14 új szolgáltatóhoz sikerült a hab.cert.hu oldalon elérhetőséget szerezni, így a jövőben már őket is könnyebben tudjuk bármiféle biztonsági incidens esetén megkeresni.

A gyakorlattal kapcsolatban érkezett kérdés, észrevétel melyet a gyakorlat során kezeltünk.

Azon ISZT tag szolgáltatókat, akik nem vettek részt a gyakorlatban, hamarosan személyesen is fel fogjuk keresni, hogy tisztázzuk: miért nem tudtak részt venni ezen a gyakorlaton?

Tervezzük a társ CERT-ek felkeresését is a gyakorlattal kapcsolatos tapasztalatok megbeszélésére, esetlegesen közös – akár célzott szektoriális – gyakorlatok további megszervezése céljából.

A gyakorlat eredményeiről konferenciáinkon is be fogunk számolni.

A gyakorlatban részt vevőknek ezúton is szeretnénk ismételten megköszönni, hogy segítették munkánkat.

Internet Szolgáltatók Tanácsa

Cím: 1132 Budapest, Victor Hugo u. 18-22.
Telefon: (+36-1) 238-0115
Honlap: http://www.iszt.hu

HunCERT
(üzemeltető: SZTAKI)

Cím: 1111 Budapest, Lágymányosi utca 11. (telephely)
Telefon: (+36-1) 279-6222
Fax: (+36-1) 209-5288
Honlap: http://www.cert.hu

SZTAKI

Cím: 1111 Budapest, Kende u. 13-17.
Levelezési cím: 1518 Budapest, Pf. 63.
Telefon: (+36-1) 279 6000
Fax: (+36-1) 466-7503
Honlap: http://www.sztaki.hu