ISZT HunCERT
2021 évi kommunikációs gyakorlat
értékelő összefoglalás

ISZT HunCERT —SZTAKI
2021. április

Összegzés

Ez a dokumentum az ***Internet Szolgáltatók Tanácsa*** – ***ISZT*** – megbízásából és érdekében a ***SZTAKI*** munkatársaiból álló, hálózati incidenskezeléssel megbízott csoportja, a ***HunCERT*** által 2021. április 6-odikai kezdettel végrehajtott, hat 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.

A lefolytatott gyakorlaton a meghívott szolgáltatók kicsivel kevesebb, mint fele tevékenyen vett részt. Idén a gyakorlatot nem előzte meg előzetes bejelentés csak az ISZT elnökségét tájékoztattuk a gyakorlat tényéről. A gyakorlatba bevontuk az ISZT tagokat és az ISZT-vel kiemelt incidenskezelési szerződésben álló, összesen 44 hazai internet szolgáltatót illetve az ISZT-vel szoros kapcsolatban lévő partnereket (hazai BIX tagok és domain regisztrátorok) és a probe eszközzel rendelkező partnereket.

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. Remél-jük, 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
Ormos Pál

Bevezetés

A ***HunCERT***, alaptevékenységi körének megfelelően és az elmúlt évekhez hasonló módon, 2021. április 6-án elindította az immár hagyományosnak tekinthető kommunikációs gyakorlatát, melyre idén munkaidőben és az elmúlt évekhez képest jelentősen bővített részvevői körben került sor.

Az ISZT HunCERT-ről

Az Internet Szolgáltatók Tanácsa hazánkban elsőként, 2001-ben 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.

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. Az előkészítés időszakában az eseménykezelő rendszerben létrehoztuk azt a ticketet, amelyhez kapcsolva tároltuk a gyakorlat során és érdekében folytatott valamennyi e-mail üzenetváltást.

A gyakorlatba ISZT tagokat és a kiemelt incidens kezelési szerződéssel rendelkező nem ISZT tagokat valamint BIX tagokat, domain regisztrátorokat és probe eszközzel rendelkező szervezeteket vontuk be.

A gyakorlat megkezdése előtt néhány héttel a gyakorlat pontos idejét és a gyakorlat témáját egyeztettük az ISZT elnökségével.

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 ***FELTÉTELEZETT*** helyzet, és ennek kapcsán megtett lépések a következők voltak:

Incidens bejelentés érkezik a HunCERT-hez, hogy ismeretlenek ddos kampányt indítottak az ISZT tag szolgáltatók valamint a többi gyakorlatban részt vevő szervezet központi domain name szerverei ellen. A szerverekre szerettek volna bejutni és azok adatait kompromittálni.

Az incidens hatásainak elhárítása érdekében a HunCERT értesíti a gyakorlat résztvevőit. Az értesítésben kéri a résztvevőket, hogy a hab.cert.hu oldalon frissítsék az adataikat, valamint adják meg az utolsó 1 hét 10 leggyakoribb támadóinak az IP címét. Az adatokat amennyiben van, akkor a probe eszközükből nyerjék ki, ha ilyen nincs, akkor pedig a központi tűzfalukból vagy IDS/IPS eszközeik logkából. Az értesítés formája az adott résztvevőhöz tartozó és a HunCERT hab rendszerében található központi cím valamint a gyakorlat kezdete előtt nyilvános oldalakról elérhető és a szolgáltatókhoz tartozó címekre küldött elektronikus levél. [***1. levél***]

1. Az értesített szolgáltatók válaszlevélben a HunCERT-et informálják, hogy az értesítő levelet megkapták, a hab rendszerben frissítették adataikat és megküldték a kért IP címeket. [1***. válaszlevél***]
2. Nagyjából az első értesítéstől számított 3 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 az incidens megszüntetését kérő, egyben a gyakorlat végét jelző HunCERT levél. Ebben mindenkinek a gyakorlat során a HunCERT által használt címre küldött levélben megköszönjük a gyakorlaton való részvételt [***2. levél***]

4. Válaszul a résztvevők nyugtázzák a gyakorlat végét és jelzik ezt a HunCERT számára [***2. válaszlevél***]

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 voltak kinyerhetők.

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 – a potenciális résztvevők neveinek felsorolását követően – 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

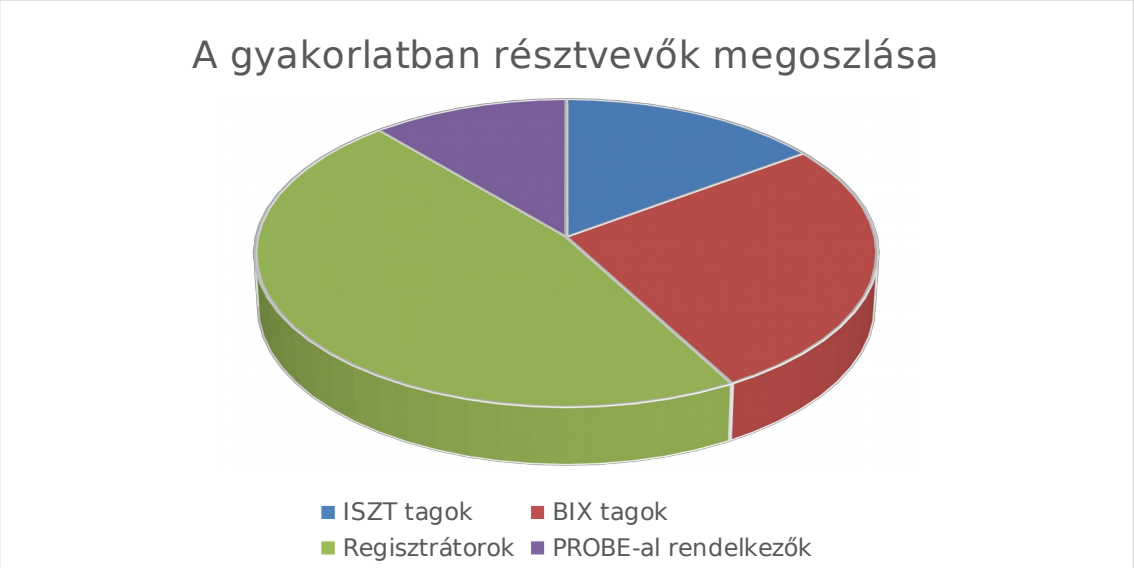
A HunCERT által vezetett gyakorlat résztvevői az ISZT tag-szervezetei a kiemelt incidenskezelési szerződéssel rendelkező nem ISZT tagok, a BIX tagok, a domain regisztrátorok és a probe eszközzel rendelkező partnerek voltak. Az ISZT tagok listája az ISZT honlapján megtalálható (http://www.iszt.hu/iszt/). 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 gyakorlatba bevontak listáját a Gyakorlatba-bevontak.pdf file-ban mellékeljük.

A gyakorlatban résztvevők és a távol maradók száma, aránya

Sajnálattal kell megállapítani, hogy a gyakorlatba bevont résztvevők közül jelentős számban nem vettek aktívan részt a gyakorlatban. Jó hír viszont, hogy a kiemelt incidenskezelési szerződéssel rendelkező szolgáltatók majdnem teljes létszámban vettek részt. Volt olyan résztvevő, aki csak a nyitó levélre reagált, de a záróra már nem. A regisztrátorok - akikkel ha nem ISZT tagok korábban semmilyen kapcsolatunk nem volt és a gyakorlatról sem tudtak – viszonylag nagy számban vettek részt. A probe tulajdonosok majdnem 60%-s részvétele nagyon jónak mondható.

Résztvevők	ISZT tagok száma	BIX tagok száma	Regisztrátorok	PROBE-al rendelkezők
Összes	*44*	*78*	*136*	*33*
Részt vett	*19*	*19*	*32*	*19*
Arány	*43,18181818*	*24,35897436*	*23,52941176*	*57,57575758*



[1]

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

Az előkészítő időszak

A gyakorlat előkészítését 2021 január végén már megkezdtük. Ekkor került meghatározásra a gyakorlat időtartama és időpontja 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 viszont kaptunk, mivel nem lett a gyakorlat előre meghirdetve, ezért voltak, akik felhívtak emiatt.

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, ill. amelyeket a kihelyezett probe eszközökkel kapcsolatban nyilvántartunk, mint kontakt adatok. 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 szerepelnek 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

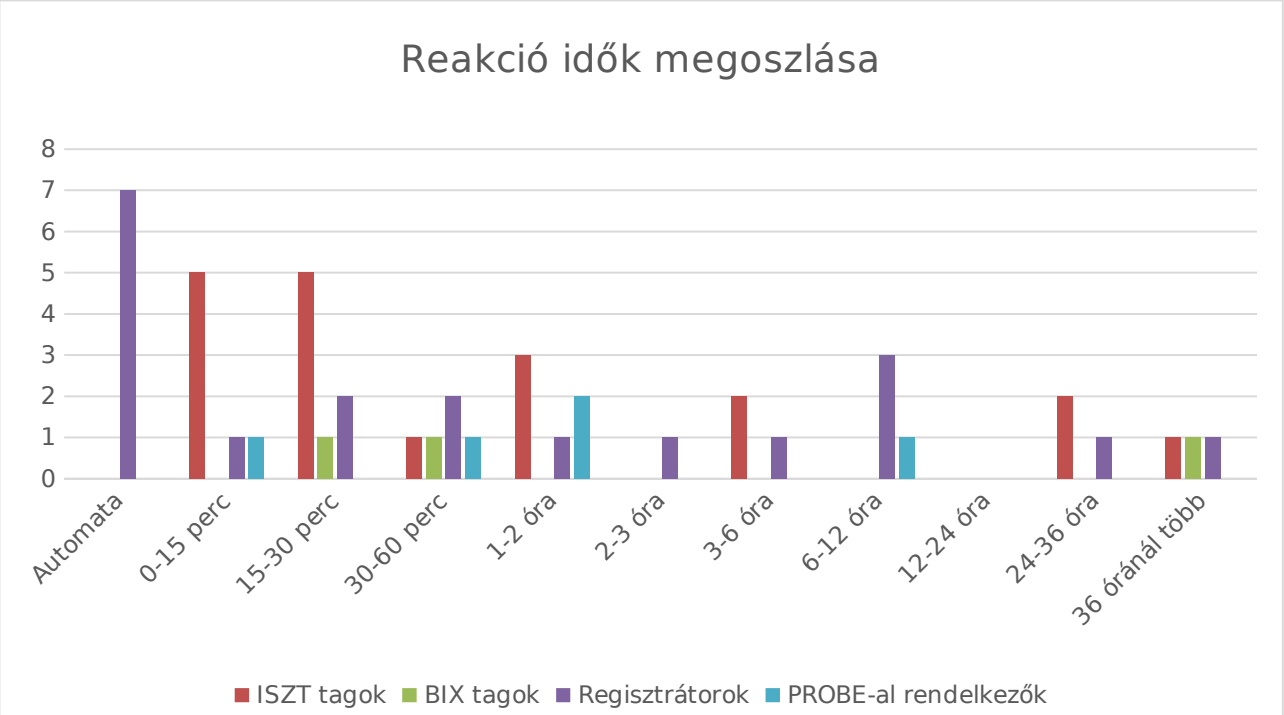
2021. április 6-án 10:17 perckor elindítottuk a gyakorlatot, vagyis kiküldtük a résztvevők ismert e-mail címére a feltételezett támadásról szóló értesítést. Ebben a levélben egyrészt arra kértük a szolgáltatókat, hogy nyugtázzák a levél vételét, módosítsák az adataikat a hab.cert.hu-n oldalon valamint küldjék meg a kért IP címeket.

Az alábbi táblázat a gyakorlat kezdetével kapcsolatosan beérkezett válaszok kiértékeléséből származó adatokat mutatja be.

Automata	0-15 perc	15-30 perc	30-60 perc	1-2 óra	2-3 óra	3-6 óra	6-12 óra	12-24 óra	24-36 óra	36 óránál több
7 db	**7 db**	**8 db**	**5 db**	**6 db**	**1 db**	**3 db**	**4 db**	**0 db**	**3 db**	**3 db**

Jól látható, hogy a leggyakoribb reakcióidők 15 – 30 perc között voltak az ISZT tagok esetében. Sőt az első 120 percben nagyon aktívak voltak a szolgáltatók. Tekintettel arra, hogy a gyakorlat 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 fenti grafikon szemlélteti, hogy az időintervallumokban miképp alakul a részvevői csoportok megoszlása. Ebből az látszik, hogy az ISZT tagok az első 30 percben voltak a legaktívabbak. Ha a regisztrátorok esetében nem vesszük figyelembe az automata válaszokat, akkor az látszik, hogy minden időintervallumban azonos gyakorisággal vettek részt. A többiek (akik csak az adott csoporthoz tartoznak) alig vettek részt a gyakorlatban, így az ő reakció idő adataik nem relevánsak egy nagyobb méretű incidens esetére vonatkozólag.

A gyakorlat folytatása– a 1. levél ismételt kiküldése

A gyakorlat során azon résztvevők számára, akik a gyakorlat kezdetét jelző e-mailre nem válaszoltak 2021. április 8-án 10:03 perckor kiküldtük a gyakorlattal kapcsolatos 1. levelet.

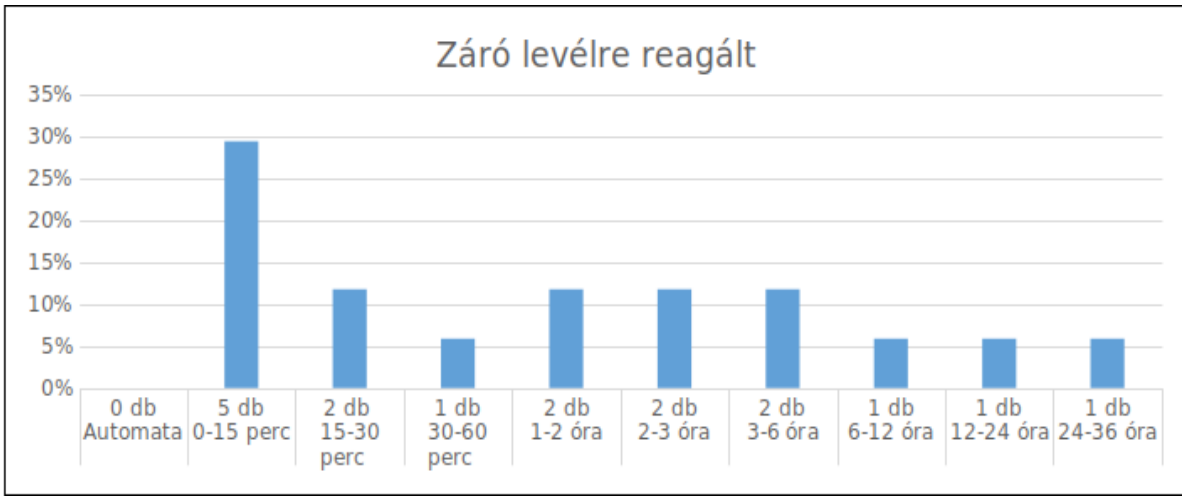
A mostani értékelésnél nem tettünk különbséget abból a szempontból, hogy az első vagy a megismételt levél hatására válaszoltak a szolgáltatók. A reakció időket ugyanúgy kezeltük és az előző pontban közölt táblázatban valamint grafikonban szerepelnek az adatok. Természetesen a megismételt esetben már 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. 2021. április 12-én 09:02-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 valamint kértük, hogy igazolják vissza a záró levél kézhez vételét is.

Visszaigazoló levelet nem kaptunk, csak ugyanazoktól jött automata válasz, akik az indító levélre is így válaszoltak.



Összefoglalás

A gyakorlat a résztvevők száma miatt nem minősíthető túlságosan sikeresnek. Abból a szempontból, hogy a http://hab.cert.hu oldalon az adatok frissítésre kerültek valamint a gyakorlat folyományaként több helyszínre is újabb probe eszközök kerültek ki sikeresnek tekinthető.

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.

A gyakorlattal kapcsolatban érkezett bejelentés melyet kezeltünk.

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

Amennyiben az elnökség is úgy gondolja előzetes egyeztetés utána a BIX tagoknak (beleértve a külföldieket is) valamint a domain regisztrátoroknak egy újabb gyakorlatot kellene tartani ősszel, a kiberhónap keretében

Tervezzük a társ CERTek 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

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

Számítástechnikai és Automatizálási Kutatóintézet
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