Ikt. sz.: Nbb-40/37-3/2016.

Nbb-3/2016. sz. ülés
(Nbb-52/2014-2018. sz. ülés)

J e g y z ő k ö n y v

az Országgyűlés **Nemzetbiztonsági bizottság**ának
2016. március 9-én, hétfőn 9 óra 39 perckor
az Országgyűlés Irodaháza I. emelet III. számú tanácstermében
megtartott üléséről

Tartalomjegyzék

Napirendi javaslat

1. Tájékoztató a Nemzeti Kibervédelmi Intézet tevékenységéről
2. Tájékoztató aktuális nemzetbiztonsági kérdésekről (Zárt ülés!)
3. Döntés a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 72/D. § (9) bekezdése alapján benyújtott panaszügyekben (Nbb-40/35-1/2016., Nbb-40/36-1/2016.) (Zárt ülés!)
4. Egyebek

Az ülés résztvevői

A bizottság részéről

Megjelent

Elnököl: Dr. Molnár Zsolt (MSZP), a bizottság elnöke

Németh Szilárd István (Fidesz), a bizottság alelnöke
Csizi Péter (Fidesz)
Lezsák Sándor (Fidesz)
Mirkóczki Ádám (Jobbik)
Dr. Szél Bernadett (LMP)

Helyettesítési megbízást adott

Móring József Attila (KDNP) Németh Szilárd Istvánnak (Fidesz)

A bizottság titkársága részéről

Dr. Imre Bernadett, a bizottság munkatársa
Ácsné Kovács Katalin

Meghívottak

Hozzászóló(k)

Tasnádi László rendészeti államtitkár (Belügyminisztérium)
Dr. Szabó Hedvig nb. dandártábornok, főigazgató (Nemzetbiztonsági Szakszolgálat)
Dr. Bencsik Balázs, a Nemzeti Kibervédelmi Intézet vezetője

Megjelent(ek)

Bodnár Zsolt dandártábornok, főigazgató-helyettes (Terrorelhárítási Központ)
Dr. Kiss Zoltán dandártábornok, főigazgató (Alkotmányvédelmi Hivatal)
Papp Károly r. altábornagy, országos rendőrfőkapitány
Dr. Bordás Tímea nb. ezredes, főosztályvezető (Belügyminisztérium)
Dr. Büki János r. ezredes, a Rendészeti Információs Iroda vezetője (Belügyminisztérium)
Dr. Tóth Szabolcs nb. dandártábornok, mb. főigazgató (SZEBEK)
Dr. Balogh András ezredes, főosztályvezető (Honvédelmi Minisztérium)
Samu Attila r. dandártábornok, sajtófőnök (Belügyminisztérium)
Havasi Zsófia szakértő (Fidesz)
Tóth Károly szakértő (MSZP)
Sas Zoltán szakértő (Jobbik)
Káncz Csaba József szakértő (LMP)

(Az ülés kezdetének időpontja: 9 óra 39 perc)

Az ülés megnyitása, a határozatképesség megállapítása, a napirend elfogadása

DR. MOLNÁR ZSOLT, a bizottság elnöke, a továbbiakban ELNÖK: Tisztelt Bizottság! Kedves Vendégeink! Elkezdenénk a mai ülést. Tisztelettel köszöntök mindenkit, a sajtó jelen lévő képviselőit, várhatóan az 1. napirend keretében tudnak majd velünk maradni.

A kiküldött meghívó és a jelenlét ismertetése következik. A bizottsági ülésen Móring képviselő urat Németh alelnök úr helyettesíti, és Szél Bernadett képviselő asszony jelezte, hogy késik. A bizottság határozatképes.

A kiküldött napirend szerint a Nemzeti Kibervédelmi Intézet tevékenységéről szóló tájékoztatóval kezdenénk, majd az aktuális nemzetbiztonsági kérdéseknél és a nemzetbiztonsági szolgálatokról szóló törvény alapján benyújtott panaszügyeknél azt a javaslatot teszem, egyeztetve az államtitkár úrral, hogy cseréljük meg a két napirendet, tehát az eredeti 3. lenne a 2. napirend és az eredeti 2. lenne a 3. napirend, majd az egyebek. A javaslat szerint az 1. napirendet nyílt, a többi napirendet a minősített adatokra tekintettel zárt ülésen tárgyaljuk, a 2. és 3. pont felcserélésével folytatnánk. Aki támogatja a napirendet, kérem, szavazzon! *(Szavazás.)* Köszönöm szépen, egyhangúlag elfogadtuk a napirendet.

Tájékoztató a Nemzeti Kibervédelmi Intézet tevékenységéről

Kérném tisztelettel, államtitkár úr, hogy akkor ezt a Kibervédelmi Intézet tevékenységéről szóló tájékoztatót kezdje el, vezesse fel.

TASNÁDI LÁSZLÓ államtitkár (Belügyminisztérium): Elnök Úr! Tisztelt Bizottság! Köszönjük a lehetőséget. A Kibervédelmi Intézet négy hónapja alakult, és négy hónap után a kellő tapasztalatok megszerzésével szeretnénk bemutatni a bizottságnak a tevékenységet, annál is inkább, hiszen elég sok olyan cikk jelent meg a sajtóban, amely szerint nem működik a kibervédelem. Azt kérném, hogy akkor a főigazgató asszony, illetve a kollégája, a Kibervédelmi Intézet vezetője adjon egy rövid áttekintő tájékoztatást. Köszönöm szépen. *(Csizi Péter megérkezik az ülésre.)*

ELNÖK: Parancsoljon!

DR. SZABÓ HEDVIG, a Nemzetbiztonsági Szakszolgálat főigazgatója: Köszönöm. Tisztelt Bizottság! 2013-ban megszületett Magyarország kibervédelmi stratégiája, ekkor 2013. július 1-jével a Szakszolgálathoz került a GovCERT működése, és 2015-ben felül lett vizsgálva ismételten az információbiztonsági jogszabály. Ekkor már a hatósági tevékenység is a Szakszolgálathoz került, illetve a sérülékenységvizsgálat, és így tudta 2015. október 1-jével megkezdeni működését a Kibervédelmi Intézet. Megkértem az intézet vezetőjét, Bencsik Balázs kollégámat, hogy egy prezentáció keretében mutassa be ezt a fejlődést, illetve az elért eredményeket. Köszönöm.

ELNÖK: Tessék, parancsoljon!

Dr. Bencsik Balázs, a Nemzeti Kibervédelmi Intézet vezetőjének tájékoztatója

DR. BENCSIK BALÁZS, a Nemzeti Kibervédelmi Intézet vezetője: *(Tájékoztatójához kivetítőt használ.)* Köszönöm. Jó napot kívánok! Tisztelt Bizottság!

Ahogyan a főigazgató asszony elmondta, a tavalyi év a kibervédelem átalakításáról, legalábbis a szervezeti átalakításáról szólt. 2015. október 1. óta működik intézet néven az állami és önkormányzati szervezeteket védő Kibervédelmi Intézet, amelynél a tavalyi évben az átalakítást a szervezetrendszer tekintetében az indokolta, hogy a 2013-ban létrejött struktúra operatív szinten rendkívül széttagolt volt. Mint ahogy a slide-on is látszik, több minisztériumhoz, több intézményhez kapcsolódtak feladatok, hatáskörök, és ezek a feladatok és hatáskörök ebben a heterogén szervezetrendszerben azt eredményezték, már eleve a szervezetek száma okán, hogy az együttműködés nehézkes volt, szakemberhiány is jelentkezett az egyes intézményeknél, és a kibervédelem egyik legeslegfontosabb tényezője az idő, hogy milyen gyorsan tudunk reagálni a kihívásokra.

Látni kell azt, hogy 2014-ben az elektronikus közigazgatás fejlesztési feladatai, valamint az információbiztonság feladatai a Belügyminisztérium keretében kerültek jogszabályi szinten létrehozásra, és a 2015. évben történt meg az információbiztonsági törvény felülvizsgálata, amely ezt a fajta feladatkoncentrációt az intézet manifesztálódásában megtette.

Az új struktúrában, legalábbis operatív szinten, az látszik, hogy egy rendkívül letisztult szervezetrendszer jött létre, a Belügyminisztérium irányítása alatt, a Szakszolgálat szervezeti kereteiben működik a Kibervédelmi Intézet, és három speciális ágazati eseménykezelő központ működik még a kormányzati intézményrendszerben.

A Nemzetbiztonsági Szakszolgálaton belül az intézetnek három fő feladatköre van, és ezért a szervezeti felépítés is e köré szerveződik. Az első elem az úgynevezett GovCERT működtetése. Ez egy olyan technikai szolgáltatási platformot jelent, ahol a bekövetkező biztonsági események kezelése, koordinálása, kivizsgálása zajlik. A második elemet az említett nemzeti elektronikus információbiztonsági hatósági tevékenység jelenti, amelynek a legfőbb feladata a jogszabályban rögzített információbiztonsági követelmények teljesülésének az ellenőrzése. A harmadik szervezeti elem pedig egy olyan biztonságirányítási és sérülékenységvizsgálati feladatcsoport, ahol technikai vizsgálatok végrehajtása zajlik, illetve az egyes állami, kormányzati szervezeteknek az üzemeltetői felé egy biztonsági szaktanácsadási tevékenység történik.

Hogy ez miért jó? Miért kellett ezt így létrehozni, illetőleg amikor létrehoztuk mi volt a cél? Hogyha a kormányzati intézményeket helyezzük a központba, akkor egy információtechnológiai vagy IT-technológiai vagy IT-biztonsági életciklust föl lehet vázolni az egyes kormányzati intézmények tekintetében. Mi történik? Egy intézmény fejleszt egy informatikai rendszert, ott ki kell alakítani egy szabályozást, egy védelmet, azt fenn kell tartani, és amikor bekövetkezik egy incidens, márpedig minden esetben be fog következni egy incidens, akkor azokra valamilyen megoldást kell találni. E köré a megoldás köré az intézet kialakította a szolgáltatásportfólióját, amelynek eredményeképpen minden egyes informatikai státuszhoz kapcsolódik valamilyen szolgáltatás. Ezek a szolgáltatások egymásra épülnek, illetve kiegészítik egymást, és minden egyes momentumban képesek támogatni a kormányzati intézmények üzemeltetőit és fejlesztőit.

Mi történt a tavalyi évben? Ehhez érdemes megnézni, hogy 2013 óta hogyan változtak a kibertámadások számai, illetőleg a kezelt események. Ugye az látszik, hogy 2013-ban, a második félévben kezdte el a Szakszolgálat a GovCERT-tevékenységet, és 2014 volt az első olyan év, amikor egy teljes évet tudtunk biztonsággal, illetőleg védelemmel tölteni. Látszik az adatokból, hogy a honlaprongálások, illetőleg az úgynevezett robothálózati tevékenységek, amelyekről majd később szót fogok ejteni, azok minden évben döntő többségét tették ki a biztonsági eseményeknek és incidenseknek. Jelentős számot képvisel - és sajnos azt kell mondjam, jelentős számot

képvisel - a célzott támadásoknak a megjelenése, a száma. Ezeknek a célzott támadásoknak - ezeket szoktuk mi, szakemberek csak egyszerűen hírszerző tevékenységnek vagy információgyűjtő tevékenységnek nevezni - a száma ugyancsak emelkedő tendenciát mutat. *(Dr. Szél Bernadett megérkezik az ülésre.)* Idén január-februárban a lezárt incidensek tekintetében látszanak a hasonló tendenciák, nagyjából ugyanazt tudjuk elmondani, mint ami tavaly történt, vannak kisebb, alacsonyabb fokú, alacsonyabb kockázatú incidensek, amelyek számosságát tekintve jelentősnek mondhatók, és bár ezen a slide-on nem látszik, mert ez csak a lezárt incidenseket tartalmazza, de már arról be tudok számolni, hogy célzott támadások is voltak ebben az évben.

A Kibervédelmi Intézet alapfeladata az, hogy az állami és önkormányzati szervezetek informatikai rendszerei tekintetében biztosítson biztonsági szolgáltatásokat, azonban, mivel a Kormányzati Eseménykezelő Központ vagy GovCERT működtetőjeként nemzetközi kapcsolati pont szerepét is betöltjük Magyarországon, ezért hozzánk nemcsak kormányzati, hanem kormányzaton kívüli incidensbejelentések is érkeznek.

Az arányok tekintetében, azt kell hogy mondjam, semennyivel nem kitettebb a kormányzati intézményrendszer, mint a civil intézményrendszer. Tehát, ha az arányokat megnézzük, akkor sok esetben megállapíthatjuk, hogy nagyjából azonos arányban éri támadás a civil szférát, mint a kormányzati szférát az egyes támadástípusok tekintetében.

És hogy mik voltak a legjelentősebb támadások tavaly? A számosságát tekintve - mint ahogy említettem - a weboldalrongálások tették ki a döntő hányadát ezeknek az informatikai incidenseknek. Ezek azért is különösen érdekesek, mert egyrészt nagy sajtóvisszhangot kaptak, és számos önkormányzat, kormányzati intézmény és a civil szférában is rengeteg honlaptulajdonos élt át ilyen támadásokat. Ezeknek egy része az Iszlám Államot támogatók tevékenységéhez köthető.

A Kibervédelmi Intézet minden esetben lefolytatta a vizsgálatokat, és megállapítottuk, hogy ezeknek a honlaprongálásoknak egy sablonos lefolyása zajlik. A sablonos lefolyás alatt azonban azt kell értenünk, hogy az esetek 90 százalékában valamilyen nem képzett, tehát hangsúlyozni szeretném, hogy szakmailag nem képzett támadók azok, akik ezeket a honlaprongálásokat végrehajtják. Ennek egyetlenegy oka van, hogy miért tudják ezt szakmailag kevésbé képzettek is végrehajtani: kialakult a világban ezen sérülékenységek kihasználására vonatkozóan egy olyan feketepiac, ahol tulajdonképpen ezeket az eszközöket és ezeket a sérülékenységeket meg lehet vásárolni. Tehát tulajdonképpen egy nem képzett, nem kvalifikált, pizsamás hekker is képes egy hazai weboldalt feltörni abban az esetben, ha annak a weboldalnak valamilyen sérülékenysége létezik és ez kihasználható.

A sablonos lefolyás - technikai részletekkel nem szeretném a bizottságot untatni, minden esetben valamilyen kártevő bejuttatásával történik a weblapok átírása, illetőleg lecserélése. Ha a tavalyi évet nézem, akkor több mint ötezer esetben történt ilyen weblaprongálás. Jelentős sajtóérdeklődés követte ezt, és történt mindez addig, tehát ezeknek a nem kvalifikált, vagy mi úgy gondoljuk, hogy nem kvalifikált hekkereknek - hívjuk hekkereknek - a tevékenysége zajlott mindaddig, amíg nem jött a migrációs válság. Amikor a migránsválság megjelent, akkor a honlaprongálások tekintetében is történt egy változás. Ez részben mennyiségi változást takart, tehát egyrészt megnőtt majdnem 10 százalékkal ezeknek a weblaprongálásoknak a száma, és történt egyfajta minőségbeli változás is, azaz most már nem az egyszerű, a sérülékenységek automatikus kihasználásával történtek a honlapfeltörések, hanem kifejezetten célzott támadások zajlottak. Ezek egyébként magukon a weblapokon megfigyelhetők, például a magyar kormánynak címzett üzenetek jelentek meg ezeken a weblapokon.

Technikai szempontból külön kell választani azt, amikor valaki automatikus módszerekkel tör fel honlapokat, hiszen akkor nem tud specifikus üzeneteket megfogalmazni, és külön kell választani azt, amikor kifejezetten valamilyen magyar kormányzati honlapokat keresnek; ebben az esetben ez történt. Azt hiszem, a képeket nem kell senkinek magyaráznom.

Nemcsak a honlaprongálások jelentették a döntő többségét az incidenseknek a tavalyi évben, hanem megjelentek az úgynevezett túlterheléses támadások is. A túlterheléses támadások lényege abban rejlik, hogy valamilyen elektronikus közszolgáltatást vagy elektronikus szolgáltatást megpróbálnak ellehetetleníteni, azaz például egy internetbanki szolgáltatást nem lehet elérni, egy adott weblapot nem lehet elérni, egy valamilyen elektronikus közigazgatási szolgáltatást nem lehet elérni. A tavalyi évben tíz fölött volt az ilyenfajta támadások száma. Itt minden esetben a Kibervédelmi Intézet támogató tevékenysége folytán sikerült ezeket a támadásokat rövid úton elhárítani, rendkívül gyors reagáló képességünk folytán volt olyan eset, ahol gyakorlatilag egy órán belül sikerült a támadást megszüntetni és helyreállítani.

Ki szeretném emelni, hogy bár ezt a fajta szolgáltatást az állami és önkormányzati szervezeteknek nyújtja a Kibervédelmi Intézet, azonban a tavalyi évben volt példa arra is, hogy egy nem állami intézmény, tehát egy piaci szolgáltató fordult a Kibervédelmi Intézethez, mert több napja szenvedett el túlterheléses támadásokat, aminek folytán nem volt elérhető az adott szolgáltatása. Jegyzem meg, egyébként az a szolgáltató egy önkormányzati weblapot is üzemeltetett, és ez a weblap napok óta nem volt elérhető. Ebben az esetben a kollégák természetesen, mivel önkormányzati érintettsége volt, segítettek az adott szolgáltatónak, pár órán belül megszüntették ezeket a támadásokat, és újra elérhetőek voltak a szolgáltató szolgáltatásai. Bátorító e-mail érkezett a cég vezetőjétől, hogy nem gondolta, hogy Magyarországon is van ilyen.

Az év vége sem telt el eseménytelenül. Ugyancsak nagy sajtóérdeklődést keltett az Anonymousnak tulajdonított fenyegetés. Azért mondom, hogy az Anonymousnak tulajdonított fenyegetés, mert az elsődleges információkból nem volt arra való utalás és arra való bizonyíték, hogy ez valóban az Anonymous fenyegetése. A Nemzeti Kibervédelmi Intézet volt az a szervezet, amely felvette ennek a fenyegetésnek a fonalát, és megpróbálta visszavezetni a fenyegetőt. Az egyik lényeges momentum az volt, hogy hiteles kommunikációt kívántunk folytatni e tekintetben, tehát a sajtómegkeresésekre válaszoltuk, és minden esetben elmondtuk, hogy a fenyegetést mindaddig, amíg ez validálva nincsen, fenntartásokkal kezeljük. Ennek ellenére természetesen, mint minden fenyegetést, ezt is komolyan vettük, és a megelőző védelmi intézkedésekre a kormányzati szervezetek figyelmét felhívtuk, megerősítették az informatikai rendszerek védelmét. Vagy emiatt, hogy a védelem megerősítésre került, vagy amiatt, hogy egyébként nem is szándékoztak komolyabb támadást végrehajtani, végül is arról tudok beszámolni, hogy az intézetünk nem kapott olyan jelzést, hogy sikeres támadást hajtottak volna végre.

Mint ahogy említettem, nemcsak az önkormányzati, állami szervezeteknek nyújtunk szolgáltatást, hanem mindazon intézmények számára, akik segítségért fordulnak ma Magyarországon a Nemzeti Kibervédelmi Intézethez. Ez azért lényeges, mert rajtunk kívül, mármint a Kibervédelmi Intézeten kívül, nincs olyan más szervezet ma Magyarországon, aki centralizáltan, a szakmaiságot szem előtt tartva, technikai felkészültséggel tudna bármiféle szolgáltatást nyújtani a piaci szereplőknek. Ilyen például a banki szféra. A banki szféra rendkívüli módon kitett az adathalász támadásoknak. Ha bekapcsoljuk a tévét, rádiót, biztos, hogy minden héten fogunk hallani valamilyen banki adathalász tevékenységéről. A bankok előszeretettel fordulnak hozzánk segítségül, ugyanis mi a nemzetközi kapcsolatrendszerünk okán, illetőleg a szakmai kapcsolatrendszerünk okán el tudjuk azt érni, hogy gyakorlatilag

órákon belül a leginkább használt böngészőkben ez az üzenet, tehát a slide-ban is látható üzenet jelenjen meg egy adathalász oldal kapcsán. Tehát órákon belül azt meg tudjuk tenni és el tudjuk érni, hogy az ügyfelek nem lesznek kitettek ezeknek a fenyegetéseknek, tehát az adathalász oldalak gyakorlatilag hamisított webhelyként jelennek meg az egyes felhasználók számítógépein.

Hogy milyen büntetőjogi vetületei vannak a Kibervédelmi Intézet tevékenységének, arra hoztam egy példát, amikor is a CERT-EU, tehát az európai intézmények eseménykezelő központja fordult hozzánk, miszerint észlelt egy olyan támadást, ami Magyarországról indul, Magyarországról történik, és segítsünk ennek a felderítésében vagy legalábbis a károk enyhítésében. A Kibervédelmi Intézet felvette az internetszolgáltatóval a kapcsolatot, amire az teremtett alapot, hogy a tavalyi törvénymódosítás során bekerült a jogszabályba az internetszolgáltatók együttműködési kötelezettsége a Nemzeti Kibervédelmi Intézettel, illetőleg a Kormányzati Eseménykezelő Központtal. A jogszabályalkotásnak kézzel fogható eredménye volt, hogy ugyancsak rendkívül gyorsan fel tudtuk deríteni az internetszolgáltatónál lévő fertőzött gépeket, és az elemzés során további támadásokat is felderítettünk, amelyeket a CERT-EU-nak a jogszabályok mentén átadtunk. A CERT-EU koordinált módon hat tagállamban tudott feljelentést tenni az adataink alapján. Ebben az ügyben még ezekben a tagállamokban nyomozás zajlik, és hírzárlatot rendeltek el, tehát most én sem tudom megmondani, hogy éppen hol tart az ügy.

A tavalyi évben egy rendkívül súlyos fenyegetettséggel néztünk szembe az elektronikus aláírások tekintetében. Magyarországon alapvetően mi egy speciális megoldást alkalmazunk, már úgy értem, hogy Magyarország az elektronikus aláírások tekintetében, hiszen számos esetben kötelező az elektronikus ügyintézés, ilyen például a cégalapítás, és az ehhez használt úgynevezett e-akta szolgáltatásban, amit két cég nyújt ma Magyarországon, keletkezett egy hiba. Ez a hiba olyan mérvű volt és olyan mértékű volt, hogy tulajdonképpen bármelyik elektronikusan aláírt dokumentumot meg lehetett hamisítani. Ez azzal a potenciális veszéllyel járt, hogy aki megismeri ezt a sérülékenységet, megismeri ezt a hibát, gyakorlatilag bármilyen céget létre tudott volna hozni, bármilyen cég nevében tudott volna hitelt felvenni, és adott esetben utána órákon belül úgy meg tudta volna szüntetni annak a cégnek a tevékenységét, hogy semmilyen nyom nem marad utána. Miért volt ez fontos, illetőleg a Kibervédelmi Intézetnek mi volt itt a szerepe? Ebben a szolgáltatásban a hibák javítását csak és kizárólag a gyártó tudja elvégezni. Na most, Magyarországon csak a Kibervédelmi Intézet volt az a szerv, amely ki tudta a gyártóktól kényszeríteni ezeknek a hibáknak a javítását, illetve az információk kezelése tekintetében egy rendkívül bizalmas információcserét tudtunk folytatni, illetőleg tudtak velünk a gyártók folytatni, aminek eredményeképpen rövid időn belül javították ebben az e-akta szolgáltatásban megjelenő hibákat. Fel is települtek ezek a hibajavítások minden egyes olyan intézménynél, amely ezeket az elektronikus aláírási szolgáltatásokat használta. Azonban akadt még egy feladat, hogy vissza kellett ellenőrizni, hogy vajon ezt a sérülékenységet nem használta-e ki valaki. Erre a Kibervédelmi Intézet fejlesztett egy saját ellenőrző szoftvert, ami több mint tízmillió elektronikus aktát vizsgált át, és szerencsére nem találtunk semmilyen hibát, azaz arra utaló nyomot vagy körülményt, hogy az elektronikus aláírások tekintetében ezt a hibát rosszindulatúan valaki kihasználhatta.

Az egyik leglényegesebb és legnagyobb fenyegetést jelentenek a célzott támadások, ezeket szoktuk kiberhírszerző-tevékenységeknek hívni. A tavalyi évben is több hullámban érkeztek ilyen támadások. Egyébként a Nemzetbiztonsági bizottságban is már elhangzott az úgynevezett APT28 támadási hullám, amely mögött az egyik kiberhírszerző-nagyhatalmat sejtik. Magyarországon több célpontja is volt,

többek között a Honvédelmi Minisztérium, a Külügyminisztérium, de a Belügyminisztériumban is találtunk arra utaló nyomokat, hogy ez a fajta támadástípus megjelent a Belügyminisztérium számítógépein is.

Amit itt el lehet mondani, hogy ezek a fajta támadások a legszofisztikáltabb támadástípusok, tehát itt olyan kártevőket használnak, amelyeknek a detektálása rendkívül nehéz. Általában több hónap, de akár több év is eltelhet, amíg egy kártevőt tudunk azonosítani. És ezzel nem vagyunk egyedül, ezzel minden nagy vírusirtó cég a világban küzd, illetőleg a nagyobb államok is hasonló helyzetben vannak.

Annak érdekében, hogy a felderítések idejét lerövidítsük, a tavalyi évben technikai fejlesztések zajlottak. Amikor 2013-ban elkezdtük a Kormányzati Eseménykezelő Központ működtetését, akkor viszonylag szerény technikai képességek álltak rendelkezésünkre, csak az incidenskezelés, illetőleg a sérülékenységpublikáció létezett szolgáltatásként, azonban a tavalyi év fejlesztései eredményeként egy rendkívül komoly elemző kapacitás került kiépítésre, amelynek egyik eleme például az általam korábban említett kártevőelemzés, illetőleg a naplóelemzés, amellyel ezt a fajta felderítési időt tudjuk lerövidíteni.

A fenyegetettségek, illetőleg a sérülékenységek kezelésére kialakítottunk egy fenyegetettségmenedzsment szolgáltatást, amelynek az a lényege, hogy a prevencióra helyezzük a hangsúlyt, tehát az informatikai rendszerek üzemeltetői azt megelőzően, hogy bármilyen biztonsági esemény náluk bekövetkezne, kapnak arra vonatkozóan információt, hogy az ő rendszerükben mit kell javítani. Ha ezt megteszik, ha ezzel az információval élnek és ezeket az információkat beépítik a rendszerükbe, akkor nagy eséllyel a bekövetkező incidenseket megelőzhetik. Ezt hívjuk fenyegetettségmenedzsment szolgáltatásnak. Egyébként részben a piac és a lakosság számára is elérhető a Kormányzati Eseménykezelő Központ honlapján keresztül.

De hogy a fejlesztések ne álljanak meg, a jövőben tervezünk további fejlesztéseket, amelynek egyik célja az, hogy egy központosított detektáló technikai elemző képesség álljon rendelkezésünkre, azaz hogy egy olyan technikai rendszert állítsunk fel, amely centralizált módon képes a kormányzati informatikai rendszerekben a bekövetkező incidenseknek a felismerésére és detektálására.

A Kibervédelmi Intézet tevékenysége és az említett incidensek feltárása és kivizsgálása elképzelhetetlen anélkül, hogy a nemzetközi együttműködésben, a szakmai együttműködésben részt vennénk. A Kibervédelmi Intézet több globális, regionális, európai uniós információbiztonsági szervezetnek a tagja. Itt csak párat hozok fel példaként, és kiemelném a visegrádi országok és Ausztria együttműködésében működő kiberbiztonsági platformot; és számos más munkacsoportnak is tagja vagyunk, amelyeknek az ülésein alkalom nyílik az operatív információk cseréjére is.

Regionális tekintetben a tavalyi évben soros elnökségét adtuk a kiberbiztonsági platformnak, ahol is a visegrádi országok, illetőleg Ausztria képviselőivel együtt tudtunk gondolkozni, illetőleg információt cserélni a kiberbiztonsági információvédelmi kérdésekről. De hogy ne elméleti legyen ez a fajta együttműködés, ezért szerveztünk egy kibervédelmi gyakorlatot is ezen országok számára, amely hasznos tapasztalatokkal zárult, és úgy gondolom, hogy alkalmas volt arra, hogy rávilágítsunk az információmegosztás hatékonyságában rejlő problémákra, amire vonatkozóan javaslatokat is tettünk.

De nemcsak a regionális együttműködésre fókuszálunk, hanem a globális együttműködésre is. Itt ugyancsak élen jártunk és vezető szerepet vállaltunk egy globális kibervédelmi gyakorlat lefolytatásában. Ez az IWWN szervezet keretében zajlott, amelynek tagállamait felsoroltam a slide-on.

A kibervédelmi gyakorlat technikai részletekkel is színeződött, és lehetőség volt arra, hogy az egyes tagállamok saját képességeiket csillogtassák ezen a gyakorlaton.

Az idei évben is számos nemzetközi gyakorlatban veszünk részt akár játékosként, akár csak megfigyelőként. Több olyan együttműködési platformnak is tagjai vagyunk, ahol a jövőre vonatkozó információbiztonsági kérdések zajlanak. Itt kiemelném, hogy az Európai Unió elfogadta az európai hálózat- és információbiztonsági irányelvet, amely a nyelvészeti egyeztetést követően idén májusban fog megjelenni a hivatalos lapban, és két év áll a tagállamok rendelkezésére, hogy ezt átültessék a hazai jogszabályokba.

Jelentem, befejeztem.

ELNÖK: Köszönöm szépen. Azt gondolom, hogy egy nagyon áttekinthető tájékoztatást hallottunk. Köszönöm szépen önnek is, illetve államtitkár úrnak is, főigazgató asszonynak is, hogy ebben segítettek, hogy ezt értsük. Ezt figyelemmel fogjuk kísérni, hiszen ezek a kihívások, azt gondolom, amit ön elmondott, illetve ahogy mi látjuk, vagy ahogy én látom, nem megszűnnek, hanem adott esetben szaporodni fognak.

Kérdések, válaszok

Van-e kérdés? *(Nem érkezik jelzés.)* Ilyet nem látok, akkor nagyon szépen köszönöm… *(Dr. Szél Bernadett: Bocsánat!)* Parancsoljon, képviselő asszony!

DR. SZÉL BERNADETT (LMP): Én is köszönöm a beszámolót. Egy kérdésem lenne, hogy arra van valamilyen iránymutatás, tud nekünk bármit mondani, hogy főként mely országok vagy államok részéről érzékelhetők ilyen kibertámadások, van-e ebben valamilyen tendencia vagy változás az elmúlt időszakhoz képest, ami nyílt ülésen elmondható.

ELNÖK: Parancsoljon, államtitkár úr!

TASNÁDI LÁSZLÓ államtitkár (Belügyminisztérium): Köszönöm szépen. A kérdés teljesen jogos, de erről most nem szeretnénk beszélni. Köszönöm.

ELNÖK: Köszönöm. Szerencsére lesz zárt ülésen adott esetben lehetőségünk, hogy erre visszatérjünk. Köszönöm szépen.

Akkor az 1. napirendet ilyen értelemben lezárom. Köszönöm szépen a nyílt ülés résztvevőinek, hogy itt voltak velünk. Természetesen, ha a sajtó képviselőinek lesz türelme, akkor a bizottsági ülés után adunk tájékoztatást arról, amit elmondhatunk.

Áttérünk majd zárt ülésre. Kérném szépen a kollégákat, segítsenek abban, hogy a zárt ülés feltételei megteremthetőek legyenek.

(Az 1. napirend tárgyalása befejezésének időpontja: 10 óra 11 perc
A bizottság rövid technikai szünet után zárt ülésen folytatta tovább a tárgyalást, amelyről külön jegyzőkönyv készült.)

Dr. Molnár Zsolt
a bizottság elnöke

Jegyzőkönyvvezetők: Podmaniczki Ildikó és Szűcs Dóra