HADMÉRNÖK

XIII. Évfolyam 1. szám – 2018. március

TECHNIKAI KIBERBIZTONSÁGI GYAKORLATOK – NEMZETKÖZI KITEKINTÉS

TECHNICAL CYBER SECURITY EXERCISES – INTERNATIONAL OVERVIEW

SZABÓ András

szabo.andras@uni-nke.hu

Absztrakt

Ebben a cikkben a technikai jellegű kiberbiztonsági gyakorlatok jellemzőit, az IT biztonsági képzésben betöltött helyét és szerepét mutatom be az olvasónak. Ezen gyakorlatok egy része a támadásokra való felkészüléssel, és az informatikai rendszerek védelemével foglalkozik (olyan kibergyakorlatok, melyekben a védőknek az ellenerő támadásait kell detektálni és kivédeni), a másik része a biztonsági rések keresésére fókuszál (ezek az úgynevezett zászlófoglaló, másnéven CTF (Capture The Flag) gyakorlatok. Napjainkban mindkettőre szükség van, hiszen az elméleti tudás a gyakorlatban való alkalmazhatóság nélkül hasztalan, illetve, ha nem ismerjük a támadó gondolkodásmódját, akkor védekezni sem tudunk ellene. A technikai gyakorlatok célja lehet a motiváció (érdeklődők szakmai orientációja), a képzés, a kiválasztás (szakmailag kompetens személyek), a validálás (rendszerek és procedúrák megfelelőségének ellenőrzése), demonstráció (egy-egy új támadási/védelmi módszernek), vagy a kutatás és fejlesztés támogatása (innovatív megoldások keresése).

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett Ludovika Kiemelt Kutatóműhely keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

Kulcsszavak: *Kiberbiztonság, gyakorlat, oktatás, képzés*

Abstract

This article is deal with the main reasons why and how should organizations use technical cyber security exercises to challenge their cyber security experts. A part of these exercises deals with cyber defence (also known as Red team/blue team exercises), the other part is about the offensive operations (the so called Capture the flags - CTF). Nowadays we need both, because we won't be able to create an effective cyber defence, without knowing the capabilities of the attackers. There can be multiple reason to organize such an exercise: to motivate (orientate people), to train the audience, to select competent persons, to validate (by checking the suitability of systems and procedures), to demonstrate Proof of concept of novel attack / defence methods, or to conduct a research (by finding innovative solutions to a problem).

The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance” in the Ludovika Workshop.

Keywords: *cybersecurity, exercise, education, training*

A kézirat benyújtásának dátuma (Date of the submission): 2018.10.02.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.03.20.

BEVEZETÉS

A kibertér egy újfajta dimenzió, a maga nemében egyedülálló, hiszen a fizikai térrel (szárazföld, tenger, légtér, űr szegmenssel) ellentétben ez az első, melyet az emberiség teremtett. Így azt feltételezhetnénk, hogy a kibertér szabályai és törvényszerűségei adottak, az itt bekövetkező események számíthatóak, könnyen megérthetőek. Azonban a használt technológia komplexitása és globális kiterjedése, valamint a gyors, szabályozatlan kialakulása következtében ez sajnos nem igaz[1]. Problémája, hogy az ebben a térben bekövetkező események sok esetben a felhasználók számára láthatatlanul zajlanak, illetve hatásaik közvetlenül nem érzékelhetőek. Például egy adatlopás, vagy adatszivárgási incidens nem okoz közvetlenül érzékelhető veszteséget, hiszen az adatok az eredeti tulajdonos számára továbbra is elérhetőek maradnak (nem úgy, mint a fizikai térben, ahol jól érzékelhető a hiánya annak, amit elloptak).

"Vírusok", "férgek", "trójai programok", "tűzfalak", "demilitarizált zóna" és még sorolhatnánk azokat az analógiákat, amit a valós, fizikai világból vettünk át, hogy a kibertérben jelentkező fenyegetéseket, és védekezési módokat elnevezzük. Ez a jelenség azt tükrözi, hogy az érthetőség érdekében meg akarjuk feleltetni ezt az absztrakt világot a már ismert, kézzelfogható környezetünkkel, ismert fogalmainkkal. Azonban az analógiák sosem tökéletesek, ezért a kibertér megértéséhez újszerű megközelítésekre és naprakész szaktudásra van szükségünk. Ezt a fenyegetések és a védekezési módok alapját képező műszaki háttér megismerésével tudjuk megszerezni.

A számítógépes hálózatok és rendszerek már a 1990-es évekre olyan komplexitást értek el, melyet egyetlen személy már képtelen volt teljes egészében átlátni. A rendszerek összekötésére és az informatikai szolgáltatások biztosítására felhasznált technológiákat így különböző szakterületekre osztották. Napjainkban az egyes szakterületek specialistái sokszor nem ismerik a másik területek kihívásait és technológiai megoldásait. Eltérő védelmi eljárásokat lehet alkalmazni például Windows és Linux rendszerek eseten, a mobiltechnológia megint más megközelítést igényel, nem is beszélve az ipari folyamatirányító rendszerekről vagy a beágyazott rendszerekről). Tovább árnyalja ezt a komplexitást az, hogy az informatikai rendszerek biztonsága mára már nem pusztán technológiai kihívás, így egyre több polgári, és kormányzati szervezet ismeri fel a biztonságot érintő egyéb szakterületek szerepét (pl.: jog, diplomácia, köz-, és nemzetbiztonság, katasztrófavédelem). A tudás és szakértelem így különböző szervezetek szakembereinél oszlik meg.

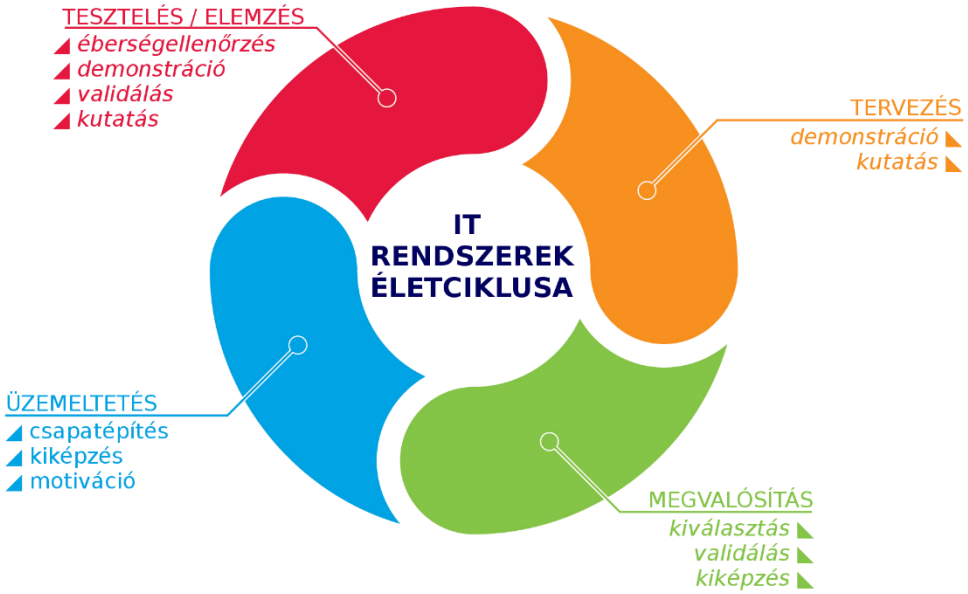
A kiberbiztonság fent említett összetettsége miatt napjainkra a szakértők nélkülözhetetlen tulajdonságává vált a csapatmunka. Az informatikai biztonsági incidensek kezelése szempontjából kiemelten fontos az együttműködésre való felkészítés, hiszen a több szakterület közös munkája nem lenne zökkenőmentes a biztonsági esemény okozta stresszhelyzetben. A szakterületek együttműködése az adott probléma több nézőpontból való megvizsgálását is lehetővé teszi, ezzel is bővítve az egyes szakértők látásmódját és tudását.

Jelen cikk a technikai kihívásokra való felkészítés egyik csoportos formájával, a technikai kiberbiztonsági gyakorlatokkal foglalkozik. Ezek egy része a támadásokra való felkészüléssel (a kiberbiztonsági "hadijátékokkal", más néven a *Red team - Blue team* gyakorlatokkal) foglalkozik. A másik típus a biztonsági rések keresésére fókuszál, ezeket nevezzük

[1] Összehasonlításképpen, a tengeri jog alapjait már az ókorba lefektették. Rhodoszon az ie. XI. évszázadban hozták létre az első szabályzókat, melyeket az egész ókori Görögország, majd később a Bizánci birodalom is átvett. Foglalkoztak a tengeri kereskedem, a szállított áruk biztosításával, és a kalózkodás kérdésével is. Forrás: https://www.britannica.com/event/Rhodian-Sea-Law
Ehhez képest a kibertér jogi szabályozása még nemzeti és nemzetközi szinteken sem teljes, annak ellenére, hogy ezt a teret teljes egészében az ember alkotott, és ha az internet alapjait képező ARPANET-et vesszük kialakulásának dátumául, akkor közel fél évszázada létezik.

zászlófoglaló (CTF[2]) gyakorlatoknak. Napjainkban mindkettőre szükség van, hiszen ha nem ismerjük a támadó gondolkodásmódját, akkor hatékony védelmet sem tudunk kialakítani ellene. Ezek egymást kölcsönösen ki is egészítik, hiszen a védők gyakoroltatása szimulált támadások nélkül lehetetlen lenne. A támadások végrehajtásához szintén gyakorlás kell (melyet védelem nélküli rendszereken végrehajtani megint csak értelmetlen). A katonai kiképzés során az ellenség harcmodorát és eszközeit használó ellenerőkkel (un. OPFORCE[3]), ismerik fel a saját harceljárások hiányosságait. A kibergyakorlatok során a Red team ugyanezt a szerepet tölti be.

Számtalan oka lehet annak, hogy egy információbiztonsági szempontból érett szervezet felismerje az informatikai rendszereit fenyegető tényezőket (és számít is a biztonsági események bekövetkezésére) és ezért felkészülésképpen ilyen gyakorlatokat szervezzen[4].



1. ábra A technikai gyakorlatok alkalmazásának céljai

A célok csoportosíthatóak ha az informatikai rendszerek életciklusának fázisai szerint (Lásd: 1 Ábra).

Ezek alapján a technikai gyakorlatok célja lehet:

- motiváció (érdeklődők szakmai orientációjának elősegítése),
- kiképzés (oktatási célból),
- csapatépítés (egy szervezeti egység trenírozása, adott feladatra való felkészítése),
- kiválasztás (szakmailag kompetens személyek felvétel előtti értékelése céljából),
- validálás (rendszerek és procedúrák megfelelőségének ellenőrzése céljából),
- "éberségellenőrzés" (az üzemeltető, és az incidenskezelő állomány figyelmének és felkészültségének, teherbírásának tesztelése valósághű körülmények között),
- demonstráció (egy-egy új támadási/védelmi módszernek az alkalmazhatósága, valamint a kialakított védelem hatékonyságának megítélése céljából),
- kutatás (innovatív megoldások keresése).

Lévén, hogy ezek a célok a már meglévő tudásra alapoznak, azokat mélyítik, vagy naprakész ismeretekkel egészítik ki, ezért mielőtt rátérnénk a gyakorlatokban rejlő potenciálok bemutatására, ismertetni szeretném a technikai jellegű tudás átadására és az

[2] *Capture the Flag*
[3] opposing force
[4] akár a saját szakértői, vagy külső érdeklődők számára

innovatív gondolkodás fejlesztésére szolgáló egyéni és csoportos IT biztonsági képzési módszereket.

AZ IT BIZTONSÁG OKTATÁSÁNAK SZINTEREI

A korai szakmai orientációt már a médiaügynökségek, és a filmkészítők is segítik, hiszen egyre közkedveltebb téma a kiberbiztonság. Az ezzel kapcsolatos napi hírek mellett számtalan film[5], sorozat[6], novella és regény[7] [8] [9], valamint számítógépes játék[10] készült ebben a témában. A 2000-es évek ilyen témájú filmjei mellőzték a szakmai alapokat, azonban az utóbbi években a téma popularitásának növekedése mellett megfigyelhető, hogy egyre realisztikusabban ábrázolják a hackerek módszereit (például a Mr. Robot sorozatban a támadók által használt szoftverek és támadási módszerek a valóságban is léteznek). Fontos azonban megértetni az érdeklődőkkel, hogy a valóság mellőzi a filmszerű jeleneteket, illetve a szaktudás megszerzése hosszú, kitartó tanulást igényel.

Ha belegondolunk mennyire meghatározó és hatékony tud lenni a fiatal korban elkezdett nyelvtanulás vagy sportolás, nem lepődünk meg azon, hogy a nagyobb kiberbiztonsági konferenciákon[11] már gondolnak az utánpótlásnevelésre is, és kiberbiztonsági gyereksarkokat alakítanak ki a jövő generációinak. Ezeken a gyerekek játékos módszerekkel ismerik meg az informatika lehetőségeit és veszélyeit. Nem feltétlenül az ekkor elsajátított szaktudás, hanem inkább az ezek hozadékaképpen kialakuló innovatív gondolkodásmód, a tudás iránti vágy, a szokványostól eltérő megoldások keresése az, amit ezek a fiatalok elsajátítanak.

Az online életünk biztonságáról korán - lehetőleg már az általános iskolában [1] - beszélni kell a fiatalokkal, annak érdekében, hogy felhívjuk a figyelmüket a veszélyekre, és így tudatos online életet alakítsanak ki. Például, hogy odafigyeljenek arra, hogy a közösségi hálókon milyen információkat adnak meg, hogyan védjék profiljukat, hogyan szeparálják a magánéletüktől a munkával kapcsolatos tevékenységüktől, hogyan válasszák ki, hogy mely online szolgáltatásokban bíznak, milyen forrásból telepítsenek alkalmazásokat, hogyan kezeljék az online zaklatást stb. Ezek mindenki számára fontos alapismeretek, ezen felül fel kell ismerni a műszaki beállítottságú érdeklődet is, akik a jövő mérnökeivé és informatikusaivá válhatnak. Az általános iskolás korosztályoknál a tudatosítás mellett a szakmai orientáció is megkezdődhet (pl.: programozás alapjai, 3D nyomtatás, hálózatok, robotika játékos bemutatása).

A megfelelő motivációt, és a szakmai ismereteket már középiskolában meg lehet alapozni (pl.: szakkörök, versenyek, nyári táborok formájában). Az Egyesült Államokban, valamint az Egyesült Királyságban több középiskola is orientálja tanulóit az informatika, azon belül pedig kifejezetten a kiberbiztonság irányába[12]. Nyári táborok[13], és versenyek (un.Challenge-ek[14]) formájában államilag is támogatják a fiatalok ezirányú orientációját .

---

[5] Ezekre láthatunk példát az IMDB adatbázis egyik tematikus ajánlásában, mely elérhető ezen a linken: http://www.imdb.com/list/ls055167700/

[6] Pl.:Mr Robot, The LoneGunman, vagy akár a magyar Hacktion

[7] Tom Clancy – Threat Vector 2012, G. P. Putnam's Sons ISBN 0425262308

[8] Johnny Long, Ryan Russell, Timothy Mullen – Stealing the Network: The Complete Series Collector's Edition ISBN 159749299X

[9] Mark Russinovich - Zero Day: A Jeff Aiken Novel ISBN 9780312612467 és Mark Russinovich – Rogue Code: A Jeff Aiken Novel ISBN 9781250035387 valamint Mark Russinovich – Operation Desolation: A Short Story ISBN 9781466821552

[10] Például a Watchdogs I. és II. részeBővebben: https://www.ubisoft.com/en-us/game/watch-dogs/

[11]Pl.aDefconconferencián Forrás: http://money.cnn.com/2017/07/29/technology/culture/r00tz-def-con-kids-army-hacking/index.html

[12] Az ISECOM orientációs anyag, mely kifejezetten középiskolásoknak szól elérhető az alábbi linken:http://www.hackerhighschool.org/books.html

Véleményem szerint az erkölcsi fejlődés korai szakaszában nem javasolt még a kiberbiztonságra fókuszálni, inkább az azt megalapozó általános műszaki érdeklődést, a programozói alapismereteket, a probléma felismerő, elemző és megoldó készséget, és a tudásvágyat kell kialakítani. A közép- és felsőfokú tanulmányok alatt ezek kiegészülhetnek a kiberbiztonsággal kapcsolatos ismeretekkel, mint például hálózati technológiák, hálózatbiztonság, biztonságos programozás, szoftver és hardverfejlesztés, biztonságos üzemeltetés, kriptográfia stb. A szakmai kompetenciák mellett fontos az etikai hozzáállás formálása is, e nélkül ugyanis a fiatalkori identitáskeresés során tévútra kerülhetnek (pl.: a kíváncsiság, vagy a társaiknak való bizonyítási kényszer miatt mások informatikai rendszerében okoznak kárt). A kiberbiztonsággal kapcsolatos mély szakmai ismereteket nem lehet pusztán "klasszikus" oktatás módszerekkel, tantermi körülmények között a középiskolai, vagy a felsőfokú tanulmányok során elsajátítani (azonban a műszaki érdeklődést, a mérnöki alapismereteket, és a gondolkodásmódot ekkor kell a leendő szakembereknél kialakítani).

Az "élethosszig tartó tanulás" koncepciója arról szól, hogy a tudás utáni vágyat egész életünkben fenn kell tartanunk, és újabb és újabb ismereteket kell elsajátítanunk. A mély technikai ismeretekkel rendelkező szakemberek "nem teremnek", hanem a korai szakmai orientáció, mentori[15] útmutatás, és a konstruktív közösség segítségével fejlődnek [2].

Az IT biztonság mély technikai ismereteinek oktatása egészen az utóbbi néhány évig még a legnagyobb egyetemeken [3] is csak a hallgatók kis csoportjának volt elérhető. Ugyanakkor hatalmas igény van a szakmai tapasztalattal rendelkező, képzett, praktikus tudással rendelkező IT biztonsági szakemberekre. Az oktatási intézmények módszereinek is változnia kell annak érdekében, hogy piaci igényeket ki tudják elégíteni, és a nagyobb létszámú képzések lehetővé váljanak. A Budapesti Műszaki és Gazdaságtudományi Egyetemen például ezért alakították ki a nagy hallgatói létszám kiszolgálására alkalmas online kiberbiztonsági labort, az Avatao[16] rendszert, melyben párhuzamosan akár több száz hallgató is képes a laborgyakorlatokat elvégezni.

A graduális képzés mellett az önálló tanulás is egyre hangsúlyosabbá válik. Már nem az a kérdés, hogy egy-egy szakkönyvhöz, szoftverhez, hardveres eszközhöz hogyan férünk hozzá, hanem hogy a számtalan információforrás közül melyiket válasszuk. Ezen a téren változott az oktatók, mentorok szerepe, az alapismeretek átadása mellett a szakmai orientáció és az útmutatás jelentősége növekedett. A csoportos önképzés lehetőségei is bővültek a számtalan rendelkezésre álló kommunikációs szolgáltatás (pl.: chat, VoIP[17], felhő alapú fájl- és tartalommegosztás, közösségi hálózatok stb.) segítségével. A BME CrySyS Lab[18] közössége [2] bizonyította ennek a módszernek a sikerességét több rangos nemzetközi versenyen elért eredményeivel[19].

---

[13]Néhány példa erre a Gen Cyber Summer Camphttps://www.nsa.gov/resources/students/summer-camps/gencyber/ National Cyber Warrior Academyhttps://ung.edu/cyber-operations-education/national-cyber-warrior-academy.php és a USCC Summer Campshttps://www.uscyberchallenge.org/cyber-camps/ valamint GCHQ által szervezett Cyber Summer Schools

[14] Pl.HighSchool Forensics (HSF) Challenge https://csaw.engineering.nyu.edu/hsf vagy a NCL - National Cyber League https://www.nationalcyberleague.org/

[15] aki a megfelelő motivációt-, és szakmai ismereteket átadja

[16] Elérhető: https://avatao.com/

[17] Voice over IP

[18]CrySyS Student Core http://core.crysys.hu/

[19]Médiamegjelenéseik: http://core.crysys.hu/media/ és aktuális eredményeik a nemzetközi listán https://ctftime.org/team/5347

Módszer[20]	**Jellemző**		**Példa**
Online tananyagok			
elearning[21]	Strukturált ismeretanyag	logikai láncba kapcsolt tudásanyagok, kiegészítő anyagokkal, ajánlott irodalommal, interaktív feladatokkal	*CyFor – Cyberforensics oktatási anyagok*[22] *Cyber Defence Awareness Course*[23] *CYBER502x Computer Forensics*[24]
Tutorial[25]-ok („hogyan kezdjek neki” anyagok) *101* anyagok[26] *Whitepaper*[27](leírások)	könnyű elsajátíthatóság	egy-egy specifikus terület megismerésére használhatóak, az anyagok sokszor nincsenek összefüggésben (nincs kapcsolat köztük)	*Cybersecurity 101*[28] *Nova Lab oktatási anyaga*[29] *MIT Cybersecurity Whitepaper*[30] SANS Cyber Aces[31]
Video tananyagok	rugalmas idő kihasználás	a klasszikus tantermi előadás rögzítése, és az interneten történő megosztása segítségével a tanulás egyszerűsödik, és a hatásfoka javul	*MIT Computer Systems Security Egyetemi kurzus*[32]
IT biztonsági *konferenciák* és *workshop*[33]-ok	újdonságok megismerése	trendek megismerése és szakmai kapcsolatok kialakítása	*Defcon*[34] *Blackhat*[35] *CCC*[36] *Hacktivity*[37]

1.Táblázat Újszerű egyéni és csoportos tanulási módszerek, és azok jellemzői

A világon több helyen is kialakultak szakmai közösségek (pl.: az un. Hackerspace-ek[38]), amelyek tagjai közösen dolgoznak egy-egy projekten. Itt laborkörnyezetet, hardvereket

[20] Az internetes források kereshetősége érdekében az angol kifejezéseket jelenítettem meg
[21] interaktív, online tananyagok és tanulást támogató rendszerek
[22] Elérhető:https://cyfor.engineering.nyu.edu/modules/
[23] Elérhető:https://ccdcoe.org/awareness-e-course.html
[24] Lásd: https://courses.edx.org/courses/course-v1:RITx+CYBER502x+2T2017/course/
[25] Kezdők számára részletes oktatási anyagok
[26] 101 jelentése: az adott terület egy szer egye, alapvető ismeretek halmaza
[27] Szakmai kiadvány
[28] Elérhető:https://www.khanacademy.org/partner-content/nova/cybersecurity/cyber/v/cybersecurity-101
[29] Lásd: http://www.pbs.org/wgbh/nova/labs/about-cyber-lab/educator-guide/
[30] MIT ENERGY INITIATIV E UTILITY OF THE FUTURE (whitepaper) https://energy.mit.edu/wp-content/uploads/2016/12/CybersecurityWhitePaper_MITUtilityofFuture_-2016-12-05_Draffin.pdf
[31] LÁSD: https://tutorials.cyberaces.org/tutorials
[32] Forrás: https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-858-computer-systems-security-fall-2014/video-lectures/
[33] Műhelymunka
[34] Elérhetősége: https://www.defcon.org/
[35] https://www.blackhat.com/
[36] Elérhetősége: https://www.ccc.de/en/
[37] Elérhetősége: https://hacktivity.com/en/
[38] http://hackerspaces.org/

(pl.:3D nyomtatók, szoftverrádiók, mérőműszerek, forrasztóállomások stb.) és szoftvereket biztosítanak a fejlesztőknek.

A kiberbiztonsággal foglalkozó konferenciák száma is jelentősen ugrott az utóbbi évtizedben. Ezek az új módszerek, technológiák megismerésének, a közös ötletelésnek, és a szakmai kapcsolatok építésének egyik legjobb formája. A workshopok kifejezetten a praktikus ismeretek elsajátítására jók, sokszor gyártók, vagy a szoftverek fejlesztői szervezik.

A graduális képzésben lehetőséget kell teremteni arra, hogy a hallgatók megismerjék ezeket a tanulási módszereket, azok előnyével és hátrányával együtt.

Élethosszig tartó tanulás (Life long learning)

A szakmai fejlődésünk érdekében napjainkban egyre többet tudunk tenni, mivel az utóbbi években a tanulási módszerek reformálódtak köszönhetően az online kurzusoknak[39], a számtalan ingyenesen elérhető forrásnak, az egyre közkedveltebb "alternatív" tanulási módszereknek (pl.: projekt alapú tanulás, játék alapú oktatás ~ Gamification, közösségi hálózatok felhasználása az oktatásban, szituációs/szerepjáték módszerek alkalmazása stb.). Napjainkban rengeteg lehetőség érhető el ingyenesen a tanulni vágyok számára. Ezek előnye, hogy felépített tematikájuk és ajánlott forrásaik irányítják a hallgatókat a tanulási folyamat során, és így nem vesznek el a keresőmotorok (Google, Yahoo, Bing) sokszor irreleváns, vagy téves találatai között. Előnyük, hogy munkája és egyéb elfoglaltsága mellett a hallgató maga osztja be, mennyi időt tud a tanulásra fordítani, és ennek függvényében halad az anyag feldolgozásával. Egyetlen problémája, hogy a hallgatók jelentős része számára szükség van egy oktatóra (vagy egy mentorra), mert önállóan nem kezdenek neki a tanulásnak, vagy halogatják a továbblépést. A BME CrySyS Lab hallgatói közösségének kialakítása során éppen ezért törekedtek arra, hogy a tapasztalt tagok támogassák az újakat és időszakosan mini workshop-ok segítségével rákényszerítsék a hallgatókat az önképzésre, és a megszerzett ismeretek társaiknak való átadására [2].

A tanulás, önképzés az IT technológia területén most már nem egy lehetőség, hanem kötelező feladatunk, ha követni kívánjuk a folyvást változó trendeket és gyorsan piacra kerülő innovációkat. A kiberbiztonság területén ez a gyorsuló tudásfejlesztés (és egyben a tudásavulás, melyet a technológiák gyors cseréje okoz) praktikus módszereket követel meg.

Az elméleti tudás megszerzésével párhuzamban, gyakorlati ismereteket is el kell sajátítani, melyeket követően önálló munka formájában kell bizonyítani azok bevéső dését. Az IT biztonságban érintett szakembereknek más és más oktatási módszerre van szükségük. Ez egyrészt az egyének eltérő tanulási stílusai (vannak vizuális, auditív stb. típusú tanulók, akiknek célszerű ennek megfelelő formában hozzáférhetővé tenni a tananyagot). A különböző szakterületek eltérő tudásbázisa (szoftverfejlesztés, üzemeltetés, rendszerintegráció, incidens kezelés, vezetői feladatok ellátása, felhasználók tudatosság, szabályzatok készítése stb.) is más és más oktatási módszer használatát indokolja. Mindenkinek a munkájához, céljainak eléréséhez szükséges tudást kell átadni (lehetőleg az esetében alkalmazható ideális módszerek felhasználásával).

A felhasználók képzése során a különböző fenyegetések vizualizálhatóak, és demonstrációs videókkal kézzelfoghatóvá tehetőek. A döntéshozóknak a kiberbiztonság és a szervezeti célok közötti összefüggés társasjátékokkal[40] és döntéshozatali gyakorlatokkal (TTX) mutatható be. A fejlesztők és az üzemeltetők számára kiberbiztonsági fejtőrök (un.

[39]Massive Open Online Courses

[40]KasperskyInteractiveProtectionSimulationhttp://media.kaspersky.com/en/business-security/enterprise/KL_SA_KIPS_overview_A4_Eng_web.pdfhttps://www.youtube.com/watch?v=XkzMi1dmULQ&feature=youtu.be&t=23m51s

challange-ek[41]) alakíthatóak ki, amelyekkel inspirálják őket a folyamatos tanulásra és javítja a problémamegoldó készségüket.

Az egyéni tudás fejlesztése mellett a csoportos munkavégzést is meg kell tanulni. Jellemzően eltérő tudással és tapasztalattal rendelkező egyének alkotják a munkacsoportokat. Ők akkor tudnak hatékonyan együtt dolgozni, ha ismerik a saját- és társaik képességeit, határait, és képesek felosztani a munkát egymás között, valamint képesek kommunikálni, és közlik egymással az elért részeredményeket.

A technikai gyakorlatok a meglévő elméleti és gyakorlati tudásra építenek, így a tanulási folyamat második lépcsőjében alkalmazhatóak (az ismeretek elsajátítását követően, a készségszint elérésére, és a tudás karbantartására használható).

TECHNIKAI KÖRNYEZET

Ezek a gyakorlatok egy valós informatikai rendszert, vagy virtuálisan kialakított hálózatokon játszódnak. Ezek lehetnek az internettől szeparáltak, vagy akár azzal összekapcsoltak. Mindegyiknek van előnye és hátránya is, döntően a gyakorlat célja határozza meg, melyiket alkalmazzuk.

A fizikai eszközök (pl. routerek, switchek, IoT eszközök, stb.) használata lehetővé teszi a valósághű játékot, azonban sokszor körülményes és nehéz a különböző résztvevő csapatoknak egyforma rendszereket kialakítani. A virtualizáció használatával viszont gyorsan üzembe helyezhető, flexibilis, hiba esetén gyorsan újraindítható/javítható kiberbiztonsági gyakorlóteret hozhatunk létre[42]. A skálázhatóság (a résztvevők számának és a feladatoknak növekedéséhez való illeszkedés) is könnyebbé válik.

Ha az internettől szeparált a kibergyakorlótér, akkor az azon használt támadási módszerek és eszközök véletlenül sem okozhatnak kárt produktív rendszerekben (pl. kártékony kódok nem fertőzhetnek meg más rendszereket). Az internetre kapcsolt gyakorlatoknak viszont az az előnye, hogy valósághű legitim forgalom (pl. felhasználók internetes böngészése, frissítések települése stb.) és realisztikus támadások generálhatóak [4].

Hátránya, hogy fennáll a veszély a külső rendszerek kompromittálásának (pl.: egy, a gyakorlaton részt vevő támadó rossz IP címet ad meg, és a kártékony kód külső rendszereket fertőz meg), továbbá a sokszor szándékosan sérülékenynek beállított rendszer külső, valós támadások célpontjává válhat (mivel a „kiberlőtéren” sok rendszert szándékosan elavult operációs rendszerrel, frissítések nélkül üzemeltetünk).

A kialakított infrastruktúra mintázhatja a szervezet saját rendszereit (operációs rendszerek, szolgáltatások, használt alkalmazások tekintetében), vagy olyan technológiákat, melyek számukra ismeretlenek (így kizökkentik a résztvevőket a napi rutinból), ezzel új ismeretek tanulására sarkaljuk őket, továbbá inspiráljuk a megszokott megoldásoktól való elvonatkoztatást is.

Valós időben játszott, vagy Offline gyakorlatok

A gyakorlatok kivitelezése szempontjából lehetnek offline feladványok (pl.: egy virtuális gép formájában elemzésre átadható számítógép, kártékony kód minta, memóriakép, merevlemez másolat, napló fájlok, hálózati forgalmak stb.), illetve valós időben játszva (un. Live fire) egy előre kialakított hálózaton. Utóbbi előnye, hogy az incidenskezelési ismeretek mellett a

[41] Néhány példa: Honeynet Project Challenges (https://www.honeynet.org/challenges), ENISA EU CyberChallange (https://www.enisa.europa.eu/topics/cybersecurity-education/eu-cyber-challenge), CyPhinx (https://www.cybersecuritychallenge.org.uk/competitions/play-demand-cyphinx), Network Forensicspuzzles (http://forensicscontest.com/puzzles)

[42] Pl. a Észt Hadsereg Cyber Range-t, bemutató videó:
Estonian Defence Forces' Cyber Range https://www.youtube.com/watch?v=5pYNVzKmnTc

valósághoz hasonlóan mindennapos üzemeltetési feladatokkal[43] is meg kell birkózniuk a résztvevőknek.

Pontozó rendszer

Módot kell találni a csapatok hatékonyságának értékelésére. Ez egyrészt számukra is egy visszacsatolás (jó úton haladnak), másrészt összehasonlíthatóvá teszi munkájukat a gyakorlat szervezői számára (akiknek ez egyfajta helyzetértékelést nyújt). A katonai terminológiából származtatott Műveleti helyzetkép (Common Operational Picture) a parancsnokok, és vezetők döntéshozatalát támogató összefoglaló információhalmaz, melyet egyetlen képernyőn jelenítenek meg, és a helyzet változásával folyamatosan aktualizálnak. A Situational Awareness (SA) segítségével a döntéshozó ismeri a rendelkezésre álló erőforrásokat, az alkalmazásának lehetőségeit, és az azokat fenyegető tényezőket. A kiber SA három tényezőt foglal magába: a saját hálózatok és IT rendszerek állapotát, a fenyegetési információkat, és a műveleti dependenciákat (azok a tényezőket amelyektől függ a szervezet céljainak megvalósítása során). A gyakorlat céljainak függvényében ezek determinálják, hogy milyen szempontokat kell mérni, értékelni. Egy technikai kiberbiztonsági gyakorlat során minimum a saját hálózatok és IT rendszerek állapotát, és a fenyegetési információkat kell monitorozniuk a szervezőknek annak érdekében, hogy objektíven tudják értékelni a résztvevők teljesítményét.

Ezt az értékelést jellemzően a pontozó rendszer (un. Scoring system) végzi, mely sokszor a legkritikusabb eleme az egész gyakorlatnak. IT biztonsági gyakorlat révén arról is gondoskodni kell, hogy a résztvevők ne találhassanak a versenyszabályban, vagy a pontozásra használt informatikai rendszerben kiskapukat (sokszor ezért a pontozás során mért paraméterek, és a mérés módszereit nem ismerik a résztvevők).

A nemzetközi gyakorlatokon megfigyelhető, hogy először csak néhány csapatnak szervezik eseti jelleggel (pl.: a Locked Shields gyakorlatsorozat elődjének tekinthető Baltic Shields-en csak 6 védő csapat vett részt [5]), majd idő múlásával újabb és újabb résztvevők csatlakozását teszik lehetővé (bővítik az infrastruktúrát és bonyolultabb feladatokkal egészítik ki a gyakorlatot). Azonban komplexitás növekedésével a technikai környezet, és a pontozó rendszer (az un. "scoring") előbb utóbb korlátossá válik.

A technikai incidenskezelési gyakorlatok egyik mérőszáma lehet a szolgáltatások elérhetősége. Annak érdekében, hogy megállapítható legyen, hogy a gyakorlat infrastruktúrájának hibája, vagy a sikeres szolgáltatás bénítás okozza a pontvesztést, olyan rendszert kell kialakítani, ami monitorozza a szolgáltatások elérhetőségét, és az aktuális mellett képes a múltbeli statisztikákat is megjeleníteni, továbbá képes összehasonlító kimutatásokat készíteni (pl.: az egyik csapat összes elérhető szolgáltatását mérni, vagy az összes csapat azonos típusa szolgáltatásainak elérhetőségét kimutatni). Az idővonalon horizontálisan és vertikálisan jelentkező hibajelzések mást, és mást jelenthetnek (pl. az egy időben elérhetetlenné vált szolgáltatások jelezhetik a router hibáját, vagy annak kompromittálodását).

A tevékenység nyomon követhetősége érdekében szubjektív és objektív módszerek alkalmazhatóak. A védő oldalon szubjektív mérőszám lehet a szervezők felé jelentett támadások típusa, azok súlyossága, objektív lehet a kézi, vagy automatizáltan gyűjtött technikai adatok (pl.: Indication of Compromise[44] mutatók).

[43] felhasználók elfelejtették a jelszavaikat, munkájukhoz szükséges programok vagy hardverek, pl.: hálózati nyomtatók telepítését kérik, problémáznak, hogy nem érnek el egyes kiszolgálókat, vagy a céges weblapon kérnek változtatás stb.

[44] IoC kártékony kód esetén pl.: a futtatható állomány hash lenyomata, a település, vagy futás során létrehozott, megváltoztatott fájlok, konfigurációs változások, a merevelemezen vagy memóriában tárolt kódrészek azonosítható karaktersorozatai stb. A támadási módra, vagy a kártékonykódra jellemző hálózat forgalom pl.: használt protokollok, azok paraméterei, a kommunikáció gyakorisága, a forrás/cél IP címek stb.

Az incidensek szabályszerű kezelése (amennyiben van előre definiált incidenskezelési terv), a fals pozitív (tévesen támadásnak vélt esemény) és fals negatív arány (fel nem ismert események), valamint a reakcióidő (támadás bekövetkezte, detektálás, annak jelentése, és a probléma elhárítása között eltelt időintervallumok) is vizsgálható egy gyakorlat során.

Ezekhez azonban a támadásoknak is előre tervezetnek, illetve végrehajtásuknak megfelelően dokumentáltnak kell lennie. Ez a támadó oldaltól nem spontán próbálkozásokat, hanem pontos, lepróbált forgatókönyvet követel meg. A végrehajtást pedig lehetőleg automatikus módon dokumentálni kell (mit futtattak, illetve milyen eredményre jutottak). Az objektív értékelhetőség érdekében célszerű rögzíteni a "támadók" forgalmát [6]. Illetve a célok elérését jól azonosíthatóvá tenni (pl.: weblap defacement-ről pillanatkép a böngészőben látható URL címmel és időbélyeggel, számítógép jogosulatlan elérése esetén a felhasználó adatbázis, jelszófájlok másolata stb.).

A fentiekben említett pontozási rendszer a "mérhető", technikai szempontok értékelésére kiváló, azonban a védelmi stratégiák és módszerek, a csapatkohézió mellett a résztvevők véleményét is vizsgálni kell (a gyakorlat előtt, közben és után). Ez alapján lehet a gyakorlat oktatási / képzési céljainak elérését értékelni. Erre felelet választós online kérdőíveket célszerű használni, és csak indokolt esetben, célzottan kérni hosszabb kifejtést (pl.: a szervezők, infrastruktúra üzemeltetők, a csapatvezetők, és egyéb kulcspozíciókat betöltőktől) [7].

NEMZETKÖZI KÖRKÉP

Több, a NATO által szervezet katonai gyakorlatnak is részét képezi a kiberbiztonság, ezzel is felhívva a figyelmet arra, hogy a szövetséges erőknek a C4ISR[45] rendszerek megbízhatóságának tesztelése [8][9], valamint a kommunikációs rendszerek interoperabilitásának ellenőrzése mellett a kibertérből érkező fenyegetésekre is készülniük kell. Napjaink fegyveres konfliktusai [10] során a rádiófrekvenciás spektrum és a kibertér [11] felől is számítani kell ellenséges tevékenységre, így a katonai gyakorlatokon fel kell készíteni a parancsnokokat és az üzemeltetőket ezekre a veszélyekre is. Az ilyen gyakorlatok lehetőséget kínálnak, az un. kiber-fizikai[46]eszközök [12], pl. pilóta nélküli rendszerek sebezhetőségének tesztelésére [13], vagy a navigációs rendszerek elleni támadások demonstrálására [14]. Ezek mellett a gyakorlatok mellett azonban van néhány olyan, melyek célközönsége kifejezetten az informatikai rendszerek üzemeltető-, és az incidenskezelő állománya. Az alábbiakban ezek jellegzetességeit mutatom be.

CYBER DEFENSE EXERCISE (CDX)

A CDX[47] (Cyber Defence Exercise) versenyt 2001-ben rendezték meg először az Egyesült Államok katonai, majd szélesebb körben a kormányzati szervek számára képzést folytató akadémiák végzős kadétjai között. Ez az első olyan katonai kiberbiztonsági technikai gyakorlat[48], melyet részletes háttérinformációkkal, mérési eredményekkel publikusan elérhető formában dokumentáltak. Az ellenerőt minden évben az NSA biztosítja, és más gyakorlathoz

[45]Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance – Katonai felhasználású informatikai célrendszerek a vezetés, irányítás, kommunikáció, hírszerzés és felderítés támogatására

[46]olyan rendszerek, melyek a fizikai valóságban működnek, azonban vezérlésük, vagy szenzorjaik miatt informatikai rendszerek részét is képezik.

[47] Lásd: https://www.usma.edu/crc/SitePages/CDX.aspx

[48] A 2009 évi gyakorlat során generált hálózati forgalom és naplóállományok az alábbi linkről letölthetőek: https://www.usma.edu/crc/SitePages/DataSets.aspx

hasonlóan az évek során ez is sokat bővült a feladatok szempontjából. A résztvevők száma is jelentősen növekedett. A gyakorlat során a csapatoknak saját magunknak kell kialakítani hálózatukat, azon a biztonsági beállításokat elvégezni, majd várni a támadásokat. A biztonsági kihívások megértése és az incidensekre való reagálás mellett a csapatmunka, és a folyamatosan növekvő terhelés is célja ennek a zárógyakorlatnak[49]. Napjainkra ez a red team-blue team gyakorlat kiegészült számos "kihívással", mint például malware elemzés/visszafejtés, hálózati, és hoszt oldali forensics, és offenzív, un. "ethikus hack"-eléssel kapcsolatos feladványok[50]. Ezeknek célja ellenőrizni a résztvevő csapatok a technológiai sokrétűségét, illetve az újabb és újabb kihívásokkal nyomás alatt tartják a résztvevőket.

LOCKED SHIELDS

A NATO tagországok [15] [16] [17] katonai rendszereinek üzemeltetőinek továbbképzését célozza a Locked Shields gyakorlatsorozat, melyet évente rendez a NATO Kibervédelmi Kiválósági Központja. A 2010-ben 6 résztvevővel megrendezett első gyakorlat (amelyet Baltic Shieldsnek neveztek) folytatásaként minden évben bővül a résztvevők köre, és a feladatok komplexitása. A Magyar Honvédség 2014 óta vesz részt a gyakorlaton, a Budapesti Műszaki Egyetem és az Nemzeti Közszolgálati Egyetem közös csapata pedig 2016 óta teszteli a gyakorlat főpróbájának a virtuális gyakorlótér infrastruktúráját.

A gyakorlatsorozat szándékosan nyomás alá helyi a résztvevőket. Ezt egyrészt azzal érik el, hogy a résztvevők számára ismeretlen, rosszul dokumentált, nagy kiterjedésű hálózatot (több mint 100 végpont) kell minimális idő alatt felügyeletük alá vonni. Ezt nehezíti, hogy külső és belső elkövetők kártékony kódokkal is megfertőztek egyes rendszerelemeket, illetve szándékosan kikapcsoltak bizonyos védelmi funkciókat. A felügyelt infrastruktúra inhomogén (Windows, Linux, Android, Mac OSX, BSD, továbbá eltérő gyártmányú hálózati eszközök, és beágyazott rendszerek célszoftverei futnak rajta), sok esetben elavult (vagy javítócsomagok nélküli futó) operációs rendszereket használnak, valamint régi, sérülékeny vagy hibás konfigurációval futó szolgáltatásokat (a web, DNS, fájltranszfer, VoIP, Chat és email mellett különböző forgalomirányító protokollok) tartalmaz.

A résztvevőknek az egyes támadások kivédése mellett képesnek kell lenniük csapatukon belül hatékonyan kommunikálni, és megosztani a támadóról és a támadási módszerről szerzett információt, képesnek kell lenni priorizálni a feladatokat, és a párhuzamosan bekövetkező események közül megállapítani melyikkel kell elsődlegesen foglalkozni (a célpont prioritása, a támadás súlyossága, a támadók feltételezett célja, valamint a szakértők leterheltségének függvényében). Fontos továbbá, hogy párhuzamosan több dologra is képesek legyenek figyelni, hiszen a támadások mellett különböző üzemeltetési, (felhasználóknak segítségnyújtás, új szerverfunkció beüzemelése, konfiguráció változtatása stb.), igazságügyi szakértői feladatokat, továbbá jogi, és média megjelenéssel, valamint stratégiai döntéshozatallal kapcsolatos kihívásokat adnak a gyakorlat szervezői. Ezek helyes megoldása mellett a határidők betartását, a szakmai hitelességet, az érthetőséget, és a prezentálás módját is figyelembe veszik.

A gyakorlat fontos üzenete, hogy az egyes technikai problémákra fókuszáló szakembernek csapatban kell dolgoznia, és az információt meg kell osztaniuk a szervezetén belül horizontálisan (a csapattagok között), és vertikálisan (a szervezeti vezetőkkel) is[51]. A

[49] Erről láthatunk egy összefoglalót az alábbi rövidfilmben:BraggingRights: CyberDefense 2012 https://www.youtube.com/watch?v=aoG1XzUk7sU

[50] A 2016 évi verseny részleteiről az alábbi online kiadványban tájékozódhatunk: https://www.nsa.gov/news-features/press-room/press-releases/2016/16th-annual-cyber-defense-exercise.shtml

[51] 2015-ben egy közös német-holland csapat is részt vett a gyakorlaton, akiknél a közös munka megszervezése, és a kommunikáció bonyolultsága egy magasabb szintre lépett.

gyakorlat végrehajtás során jelentéseket kell készíteniük a résztvevőknek, mely célja a lényeglátás, és a megfelelő szaknyelv használata (a felsővezetőknek az adott fenyegetésnek a szervezetre gyakorolt hatását, és az ellenintézkedésekhez szükséges pénzügyi, szervezeti döntéseket kell bemutatni).

A csapatoknak lehetőségük van az előre kialakított infrastruktúra biztonságát saját védelmi megoldásokkal fokozni (amennyiben azt a hálózati topológia átalakítása nélkül képesek integrálni). Ez lehetőséget kínál például újfajta megoldások (pl.: hálózati forgalomelemző, IDS, kliens oldali biztonsági szoftverek stb.) tesztelésére is.

CROSS SWORDS [18]

A *blue team – red team* jellegű technikai gyakorlatokon a „vörös csapat" az informatikai ellenerő[52] szerepét játssza el. Feladatuk az ellenség Taktikák, Technikák és Eljárások (TTP[53]-ék) biztosítása a gyakorlatokon. A valósághűség érdekében az ellenerő tudását és szervezettségét is folyamatosan fejleszteni kell. A Cross Swords gyakorlatnak célja, hogy a résztvevők megismerjék az aktuális támadási TTP-ket és azokat minél hatékonyabban tudják szimulálni más kiberbiztonsági gyakorlatokon. A 2017 évi gyakorlat egyik fókuszterülete a megtévesztésen alapuló védelmi technológiák (pl.: honeypotok, honeytokenek) detektálása volt [19]. Érdekes, hogy az egyetemeket és kutatóintézeteket is egyre nagyobb mértékben vonják be a szervezők [20] . A résztvevők és a feladatok folyamatos bővülésének eredményeképpen 2017-ben már 350 szakértő vett részt a gyakorlaton[54].

CYBER COALITION [21]

A Cyber Coalition elnevezésű gyakorlatot 2009 óta rendezik a NATO tagállamok számára. A fő célja az incidenskezeléssel kapcsolatos nemzeti szintű feladatok gyakoroltatása. A Locked Shields-hez hasonlóan ez is az Észt Cyber Range-et használja fel. A résztvevők számában itt is folyamatos növekedés figyelhető meg. 2017-ben a 3 napos gyakorlaton közel 900-an vettek részt, többségükben saját hazájukból [22][23]. A gyakorlat a technikai kihívásokkal az incidenskezelésben résztvevő szakemberek tudását és felkészültségét vizsgálja, illetve lehetőséget kínál a nemzeti incidenskezelési módszerek és akciótervek tesztelésére is [24] [25]. A szakértők közti technikai jellegű információk megosztását, illetve a szervezeten belüli, és azon kívüli szereplőkkel folytatott hatékony kommunikációt is gyakorolják a résztvevők. A hazai részvétel összetétele az évek során formálódott egyrészt a jogszabályi körülmények változása miatt, másrészt mivel a gyakorlat évente változó forgatókönyve más és más célpontokat érint, így mindig az aktuális történet incidense kapcsán "érintett" szervezetek kerülnek bevonásra.

A gyakorlat az esemény- és incidenskezelő, IT nyomozati-, és elemzői feladatokra fókuszál [26], de a műszaki feladványok mellett a műveletre gyakorolt hatást, és a technikai kihívásokra adható jogi válaszokat is vizsgálják (hasonlóan a Locked Shields-hez).

Ezeknek a "nagyobb" nemzetközi gyakorlatoknak a hatására több hadsereg is kialakított saját gyakorlóteret. A helyi sajátosságok figyelembevételével kialakított technikai kihívások gyakoroltatása mellett további előny, hogy a nemzeti szereplők bevonásával a tudás a hazai egyetemeknél, és a kritikus infrastruktúrák üzemeltetői számára is hasznosul.

[52] Nevezik még őket tigerteam-nek, vagy OPFOR-nak (opposingforce-nak) is.
[53]Tactics, Techniques and Procedures
[54] Lásd:https://www.information.dk/udland/2017/06/natos-cyberkrigere-ruster-verdens-stoerste-krigsspil

CYBER PERSEU

2017-ben a Portugál hadsereg a nemzeti szintű kiberbiztonsági gyakorlatát az Indra cég Minsait rendszerének segítségével bonyolította le [27]. A gyakorlat tervezésében, kialakításában, és végrehajtásában közel 60 kormányzati-, katonai-, piaci- és akadémiai szereplő vállalt részt. A gyakorlat a blue team-red team koncepciójú megvalósítása mellett egy Capture The Flag feladványt is tartalmazott. A portugál erők mellett Spanyol és Brazil résztvevői voltak a gyakorlatnak.

PANOPTES

A Görög hadsereg a saját kiberbiztonsági gyakorlatának tervezése és megvalósítása során szintén a Locked Shields-et vette mintául [28]. 2016-ban ezen a gyakorlaton 200 fő vett részt. A résztvevő csapatok a katonai és rendvédelmi egységektől, egyetemekről, kormányzati és piaci szereplőktől érkeztek (elsősorban a nemzeti kritikus infrastruktúráktól).

CYBER CZECH [29]

2015-ben a nemzetközi tapasztalatok (Cyber Coalition, Cyber Europe, Locked Shields) alapján a Cseh Kiberbiztonsági központ elhatározta, hogy nemzeti sajátosságait figyelembe véve saját technikai gyakorlatot szervez a közigazgatásban dolgozó IT üzemeltetők számára. A technikai infrastruktúrát a Masaryk Egyetem incidenskezelő csoportja (CSIRT-MU[55]) által fejlesztett KYPO kiberbiztonsági gyakorlatszervező platform adta.

Feladatok és az ütemezés terén ez a gyakorlat is a Locked Shields-et mintázza. A csapatok létszáma (4 fős csapatokban összesen 20-30 fő), és a technikai infrastruktúra is a nemzeti lehetőségekhez mért. A létszám lehetővé tette, hogy a résztvevők egy helyszínen dolgozzanak a feladatokon. Ez könnyítette a szervezést, és javította a gyakorlat hatékonyságát az oktatás/kiképzés terén.

NEMZETKÖZI EGYÜTTMŰKÖDÉS

A jövő a különböző kiberbiztonsági gyakorlóterek összekapcsolása felé mutat. Ez egyrészt a technikai infrastruktúra szintjén a hálózatok, illetve az egyes feladványok integrálását, valamint szervezési szinten a kiberbiztonsági hadijátékok közös végrehajtását jelenti. A gyakorlatok többsége valamilyen virtualizált infrastruktúrát alkalmaz, és a gyakorlat elérésére gyakran az internetet használják. Így azt gondolhatnánk, hogy az együttműködés csak szervezési kérdés. Azonban a különböző gyakorlóterek összekapcsolása esetén a rendszerek közti üzenetváltások a menedzsment forgalomnál[56] jóval nagyobb terhelést jelentenének, továbbá az üzemeltetőknek, és a gyakorlat szervezőinek is kisebb ráhatása lenne a rendszerre (pl. hálózati hibák okozta kiesések detektálása, és javítása terén). Az összekapcsolt rendszereken szervezett gyakorlatokon többen vehetnének részt és komplexebb játékteret lehetne kialakítani, illetve a szervezési feladatok, anyagi terhek is eloszlanának, azonban a korábbiakban említett pontozási rendszer, illetve a kiszolgáló infrastruktúra is bonyolódna.

KÖVETKEZTETÉSEK

A technikai gyakorlatok komoly felkészülést igényelnek, azonban a technikai feladatokat ellátó szakállomány (üzemeltető-, incidenskezelő-, igazságügyi szakértői állomány) képzése e

[55] https://csirt.muni.cz/

[56] ti. a távoli elérés esetén csak a távmenedzsment (pl.:ssh, rdp, vnc protokoll alapú) megoldások forgalmát kell csak az interneten keresztül felépített VPN csatornán továbbítani.

nélkül nem lehet teljes. Az ilyen jellegű gyakorlatok a technológia ismeretek bővítése mellett a kommunikációs készséget, illetve a csapatmunkával, a munkamegosztással és a feladatok menedzselésével kapcsolatos képességeket is fejleszti. A NATO által szervezet gyakorlatok jó lehetőséget kínálnak az ismeretek bővítésére, és a nemzetközi bevált gyakorlatok megismerésére. Követve más nemzetek kezdeményezéseit (például a Cseh Kibervédelmi Központ Cyber Czech gyakorlatát) hazánkban is szükséges lenne ilyen technikai kiberbiztonsági gyakorlatokat szervezni, és végrehajtani. Így a hazai jogi-, és technológia környezetben készülne fel a szakállomány, és készségeik az aktuális nemzeti kihívásokhoz illeszkednének.

FELHASZNÁLT IRODALOM

[1] MATTHEW, J.: *Winning the Cyber Security Game* (online Tanterv) Forrás:http://mediasmarts.ca/sites/mediasmarts/files/lesson-plans/lesson_winning_cyber_security_game.pdf (Letöltve:2017.08.15)

[2] BUTTYÁN L., FÉLEGYHÁZI M., PÉK G.: *Mentoring talent in IT security*, 2016 Usenix Workshopon Advances in Security Education Forrás: http://www.crysys.hu/publications/files/ButtyanFP16ase.pdf Letöltve:2017.08. 15

[3] BISHOP, M.: *U.S. Universities Get "F" For Cybersecurity Education* Forrás: https://blog.cloudpassage.com/2016/04/07/universities-fail-cybersecurity-education/ Letöltve:2017.08. 15

[4] CAPUANO, E: *Go Beyond Tabletop Scenarios by Building an Incident Response Simulation Platform Defcon* 25 Konferencia előadás anyaga Forrás: https://www.wallofsheep.com/pages/dc25#ecapuano2

[5] CCD COE – *Baltic Cyber Shield Cyber Defence Exercise 2010 After Action Report* Forrás: https://ccdcoe.org/publications/BCS2010AAR.pdf Letöltve:2017.08. 15

[6] KONT, M., PIHELGAS M., MAENNEL, K., BLUMBERGS, B. AND LEPIK T.: *Frankenstack: Toward Real-time Red Team Feedback 2017* IEEE Military Communications Conference
Forrás:
https://ccdcoe.org/sites/default/files/multimedia/pdf/Frankenstack_MILCOM_IEEE_2017_CCDCOE.pdf Letöltve:2017.08. 15

[7] SZALAI, F.: *Does cyber security exercise information sharing work*? Forrás:https://digi.lib.ttu.ee/i/file.php?DLID=7110&t=1 Letöltve:2017.08. 15

[8] Szabó L.: *Átalakulóban a Combined Endeavor gyakorlat* Forrás: http://2010-2014.kormany.hu/download/c/0f/50000/CE_fejlodes (1).pdf Letöltve:2017.08. 15

[9] NATO ACT - CWIX 2017: *NATO Tests Cyber, Innovation and Adaptation* Forrás:http://www.act.nato.int/cwix-2017-nato-tests-cyber-innovation-and-adaptation Letöltve:2017.08. 15

[10] US EUCOM - *Cyber Endeavor seminars during Exercise Combined Endeavor 2014* Forrás:http://www.eucom.mil/media-library/photo/26809/cyber-endeavor-seminars-during-exercise-combined-endeavor-2014 Letöltve:2017.08. 15

[11] *The Guardian Nato countries begin largest war game in eastern Europe since cold war* Forrás:https://www.theguardian.com/world/2016/jun/06/nato-launches-largest-war-game-in-eastern-europe-since-cold-war-anaconda-2016 Letöltve:2017.08. 15

[12] Scott D. A.: *The Dawn of Kinetic Cyber*
Forrás:https://ccdcoe.org/cycon/2013/proceedings/d2r1s4_applegate.pdf
Letöltve:2017.08. 15

[13] FERDINANDO, L. – DoD Officials Observe Counter-Drone Demoin California Forrás:https://www.defense.gov/News/Article/Article/612734/ Letöltve:2017.08. 15

[14] *BBC GPS to be jammed in Scotland during Nato wargames* Forrás:http://www.bbc.co.uk/news/uk-scotland-highlands-islands-34413696
Letöltve:2017.08. 15

[15] *NATO Cooperative Cyber Defence Centre of Excellence –Cyber Defence Exercise Locked Shields2012 After Action Report*
Forrás:https://ccdcoe.org/sites/default/files/multimedia/pdf/LockedShields12_AAR.pdf
Letöltve:2017.08. 15

[16] *NATO Cooperative Cyber Defence Centre of Excellence –Cyber Defence Exercise Locked Shields 2013 After Action Report* Forrás:
https://ccdcoe.org/publications/LockedShields13_AAR.pdf Letöltve:2017.08. 15

[17] *NATO Cooperative Cyber Defence Centre of Excellence –Cyber Defence Exercise Locked Shields 2014 - After Action Report Executive Summary* Forrás:https://ccdcoe.org/sites/default/files/documents/LS14_After_Action_Report_Executive_Summary.pdf Letöltve:2017.08. 15

[18] *NATO Cooperative Cyber Defence Centre of Excellence – Crossed Swords Exercise* Forrás:https://ccdcoe.org/crossed-swords-exercise.html Letöltve:2017.08. 15

[19] SYSMAN, D.: *The Crossed Swords wargame: Catching NATO red teams with cyber deception*
Forrás: http://blog.cymmetria.com/nato-crossed-swords-exercise Letöltve:2017.08. 15

[20] *NATO Industry Relations - An Exercise before the Exercise: Student "Hack" of Locked Shields*
Forrás: http://ncia.nato.int/NewsRoom/Pages/160628_Locked_Shields-students.aspx
Letöltve:2017.08. 15

[21] *NATO Cyber Defence Fact Sheet*
Forrás:
https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_201_03/20170331_1704-factsheet-cyber-defence-en.pdf Letöltve:2017.08. 15

[22] *NATO exercise Cyber Coalition 17 underway in Estonia* Forrás: https://shape.nato.int/news-archive/2017/nato-exercise-cyber-coalition-17-underway-in-estonia

[23] *NATO - NATO's flagship cyber exercise begins in Estonia (2017)*
Forrás: https://www.nato.int/cps/ic/natohq/news_149233.htm Letöltve:2017.08. 15

[24] SZŰCS L.: *Sikeres volt a kibervédelmi gyakorlat* (2011) https://honvedelem.hu/cikk/29471/sikeres-volt-a-kibervedelmi-gyakorlat
Letöltve:2017.08. 15

[25] *A Felügyelet sikeres szerepvállalása a második NATO kibervédelmi hadgyakorlaton* Forrás: http://www.nbf.hu/20121119.html Letöltve:2017.08. 15

[26] SZALAI M.: *Cyber Coalition 2017 – kibervédelmi gyakorlat* Forrás: http://bhd.honvedseg.hu/cikk/cyber_coalition_2017_kibervedelmi_gyakorlat

[27] INDRA - *The Portuguese Armed Forces complete Cyber Perseu, the National Cyberdefense exercise, using Indra's Minsait Cyber Range platform* Forrás: https://www.indracompany.com/en/noticia/portuguese-armed-forces-complete-cyber-perseu-national-cyberdefense-exercise-using-indras Letöltve:2017.08. 15

[28] GRITZALIS, D., SPYROS, P.: *Panoptes: The Greek National Cyber Defence Exercise* Forrás: https://www.infosec.aueb.gr/Publications/CEER-ENISA-2016%20Gritzalis%20Papageorgiou.pdf Letöltve:2017.08. 15

[29] VYKOPAL, J., MOKOŠ, O.: *Czech cyber defence exercise* Forrás:https://www.terena.org/activities/tf-csirt/meeting47/J.Vykopal-O.Mokos-Czech-lessons.pdf Letöltve:2017.08. 15