HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 4. szám

GEREVICH JÁNOS[1] – **NÉGYESI IMRE**[2]

A Military Scrum szoftverfejlesztési módszertan alkalmazása létfontosságú infokommunikációs rendszerek fejlesztése során

Application of Military Scrum Software Development Method During Critical Information Infrastructure Developments

Absztrakt

Jelen tanulmány feltárja a létfontosságú infokommunikációs rendszerek védelmével kapcsolatos hazai és Európai Uniós szabályozás lényegi elemeit, bemutatásra kerül Magyarország Nemzeti Kiberbiztonsági Stratégiája. Ezt követően betekintést nyerhetünk az elektronikus információbiztonság hazai törvényi szabályozásába. A tanulmány végén az informatikai rendszerek kialakítására és bevizsgálására alkalmas Military Scrum szoftverfejlesztési módszertan felhasználási lehetőségei kerülnek bemutatásra.

Kulcsszavak: kritikus, létfontosságú, információs, infrastruktúra, rendszer, agilis, szoftver, fejlesztés

Abstract

This paper explores the essential elements of domestic and EU regulation on critical information infrastructure protection and presents the National Cyber Security Strategy of Hungary. After that, we can gain insight into the national legal regulation of electronic information security. At the end of the study, the Military Scrum software development methodology application possibilities are shown for IT systems during their development and inspection.

Keywords: critical, vital, information, infrastructure, system, agile, software, development

[1] Nemzeti Közszolgálati Egyetem, Hadtudományi Doktori Iskola, doktorandusz hallgató – National University of Public Service, Doctoral School of Military Sciences, PhD student, E-mail: gerevich.janos@agilexpert.hu; ORCID: 0000-0001-7236-4514

[2] Nemzeti Közszolgálati Egyetem, tanszékvezető – National University of Public Service, E-mail: negyesi.imre@uni-nke.hu; ORCID: 0000-0003-1144-1912

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 4. szám

LÉTFONTOSSÁGÚ INFOKOMMUNIKÁCIÓS RENDSZEREK

Ahhoz, hogy megértsük a fizikailag létező kritikus infrastruktúra védelem magyar szabályozását, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. Törvényt [1], valamint a törvény végrehajtását szabályozó 65/2013. (III. 8.) Korm. Rendeletet [2] célszerű górcső alá venni. Az azonosítási-, kijelölési-, visszavonási eljárás, a kijelölt létfontosságú rendszerek nyilvántartása, valamint a kapcsolódó üzemeltetői biztonsági tervek tartalmi követelményei és a végrehajtás menete az imént említett jogszabályokból megtudható. A meghatározott fogalmak és folyamatok az Európai Unió létfontosságú rendszerek védelmére vonatkozó hatályos előírásainak magyar leképezéseként tekinthetők. A témáról részletesebben Gerevich János és Négyesi Imre tanulmányában olvashatunk a Hadtudományi Szemle XI. évf. 3. számában [3].

	Ágazat	*Alágazat*
24	Infokommunikációs technológiák	információs rendszerek és hálózatok
25		eszköz-, automatikai és ellenőrzési rendszerek
26		internet-infrastruktúra és hozzáférés
27		vezetékes és mobil távközlési szolgáltatások
28		rádiós távközlés és navigáció
29		műholdas távközlés és navigáció
30		műsorszórás
31		postai szolgáltatások
32		kormányzati informatikai, elektronikus hálózatok
.	.	.
38	Jogrend – Kormányzat	kormányzati rendszerek, létesítmények, eszközök
39		közigazgatási szolgáltatások
40		igazságszolgáltatás
41	Közbiztonság – Védelem	rendvédelmi szervek infrastruktúrái
42		honvédelmi rendszerek és létesítmények

1. táblázat – 2012. évi CLXVI. Törvény, 3. melléklet, részlet

A hazai ágazati besorolások felépítését az 1. táblázat mutatja be. Az alábbiakban egy rövid példával szeretnénk szemléltetni az infokommunikációs rendszerek bonyolultságát. Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény [4] értelmében 2018. január 1-től a kormányzati és a gazdasági szereplőknek elektronikus úton kell kapcsolatot tartaniuk egymással. Az 1. táblázat sárga színnel kiemelt sorai egyenként érintettek az említett elektronikus kormányzati szolgáltatás megvalósítása során. Bármelyik kiesése a szolgáltatás teljes, illetve részleges kiesését okozhatja,

ezzel komoly gazdasági károkat okozva. Az ilyen jellegű összetett szolgáltatások védelméhez a fizikai védelmen túl további szabályozásra és intézkedésekre van szükség.

A létfontosságú rendszerekre vonatkozó jogszabályok alapvetően fizikai infrastruktúra védelemre vonatkoznak és nehéz interpretálni őket infokommunikációs rendszerekre. Ezt a problémát az Európai Unió is külön kezelte, külön szabályozást hozott létre a kibertérre vonatkozóan. A továbbiakban az EU-s és a magyar szabályozás kerül bemutatásra.

LÉTFONTOSSÁGÚ INFOKOMMUNIKÁCIÓS RENDSZEREK VÉDELME AZ EU-BAN

2011-ben az Európai Bizottság a kritikus információs infrastruktúrák védelméről szóló közleményében [5] már kimondottan a kiberbiztonság kérdésével foglalkozott. A közlemény az elért eredmények bemutatásán túl a globális kiberbiztonság elérését tűzte ki célul. A végrehajtásért többek között az ENISA[3] felelt. A meghatározott cselekvési terv 5 pilléren állt az alábbiak szerint [5; 2. old].

1. Felkészültség és megelőzés
    a. tagállamok közötti együttműködés megteremtése hálózatbiztonsági reagáló csoportok segítségével (Computer Emergency Response Team, röviden CERT);
    b. a közszféra és a magánszféra közötti együttműködés erősítése az infokommunikációs infrastruktúrák ellenálló képességének fokozása érdekében;
2. az alapképességek, szolgáltatások és kapcsolódó szabályok meghatározásával a jól működő tagállami CERT-ek együttesen alkotják az európai információmegosztási és figyelmezető rendszer (European Information Sharing and Alert System, röviden EISAS) gerincét;
3. Észlelés és reagálás
    a. az EISAS rendszer alapvető működésének megvalósítását tűzték ki célul 2013-ig a tagállami CERT-ekre alapozva, a személyes adatok védelmét határozták meg az egyik célterületnek;
4. Enyhítés és helyreállítás
    a. az ENISA által szervezett nagyszabású hálózati incidensekre történő reagálás és helyreállítás témakörében szervezett gyakorlatok; tagállami szintű iránymutatás;
    b. nagyszabású hálózati incidensekre történő felkészülés páneurópai gyakorlatok segítségével;
5. Nemzetközi együttműködés – az európai alapelvek egyeztetése a különböző nemzetközi szervezetekkel G8, OECD, NATO és partnerekkel, többek között az

[3] ENISA – European Network and Information Security Agency, azaz Európai Hálózatbiztonsági Ügynökség, a szervezetet 2004-ben hozták létre, elsődleges célja a hálózat- és információbiztonság növelése az Európai Unió határain belül.

Egyesült Államokkal; hosszú távon egy nemzetközi keretrendszer kialakítása az ellenálló és biztonságos Internet érdekében;

6. Infokommunikációs szektorra vonatkozó ECI követelmények meghatározása – a tagállamok által meghatározott infokommunikációs szektorra vonatkozó kritérium célterülete a hagyományos- és mobil telefonhálózat, valamint az Internet szolgáltatás volt;

A közlemény 2. pontjában [5; 3-4. o.] a lehetséges fenyegetések számát, hatókörét, kifinomultságát és potenciális hatását vizsgálták az infokommunikációs technológia (röviden: ICT) terjedéséből kifolyólag. Az Európai Bizottság megállapította, hogy az új és technológiailag fejlettebb fenyegetések felbukkanása tisztán mutatja, hogy az ICT segítségével politikai-, gazdasági- és katonai erőfölény teremthető meg. Megállapították, hogy be kell sorolni a lehetséges tevékenységeket az alábbiak szerint.

1. adatlopás – gazdasági, illetve politikai kémkedés. Gazdasági és kormányzati infokommunikációs rendszerek támadása;
2. zavarkeltés – DDoS[4] támadások végrehajtása botnet hálózatok segítségével;
3. megsemmisítés – az infokommunikációs technológia terjedésével ez a forgatókönyv is egyre valószínűbbé válhat különböző létfontosságú rendszerek esetében, például: intelligens hálózatok, vízhálózat-irányítási rendszerek

Az Európai Unió által foganatosított intézkedések hatásai megjelennek a magyar szabályozásban is. A kormányzati információbiztonság javítására való törekvések, a megfelelő eseménykezelő központok létrehozása és a jogi háttér megteremtése többek között az EU által kidolgozott és meghatározott követelményeknek köszönhető. A továbbiakban a hatályos magyar szabályozás áttekintése következik, ezen belül is a szoftvertechnológiai, minőségi szempontok figyelembe vétele.

LÉTFONTOSSÁGÚ INFOKOMMUNIKÁCIÓS RENDSZEREK VÉDELME MAGYARORSZÁGON

A Nemzeti Biztonsági Stratégia elveit követő és a kibertérre kiterjesztett stratégiai szintű dokumentum Magyarország Nemzeti Kiberbiztonsági Stratégiája [6]. A Kiberbiztonsági Stratégia magát a következő módon határozza meg: „a nemzeti vagyon részét képező nemzeti adatvagyon, valamint a kapcsolódó létfontosságú rendszerek és létesítmények kiberbiztonságának dokumentuma” [6; 2]. A stratégia deklarálja, hogy igazodik az Európai Unió Kiberbiztonsági Stratégiájához [7] és a NATO Kibervédelmi Politikájához [8] és a lisszaboni, valamint a chicagói NATO-csúcsokon megfogalmazott kibervédelmi elvekhez és célokhoz. A stratégia a magyar kiberbiztonsági környezetet a következő módon mutatja be: nagy fenyegetést jelent a kibertérben megvalósuló információs hadviselés, ugyanakkor „a külső károkozások mellett további kockázatot jelent, hogy a kibertér alkotóelemeiként szol-

[4] DDoS - Distributed Denial of Service - elosztott szolgáltatásmegtagadással járó támadás, más néven túlterheléses támadás, hatására célba vett informatikai szolgáltatás megbénul vagy helytelenül működik.

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 4. szám

gáló informatikai és hírközlési rendszerek üzembiztonsági szabályozása sem kellően rendezett." … „Jelen stratégia fő célja annak a döntéshozó politikai és szakmai figyelemnek és képességnek a kiépítése, mely rugalmasan reagálva lehetővé teszi a belátható jövőben a technológiai fejlődésből fakadó új kiberbiztonsági problémák kezelését." [6; 4] Az idézett gondolatok alapján azt a következtetést lehet levonni, hogy egyaránt fel kell készülnünk külső és belső eredetű kockázatokra a magyar kibertér biztonságának megteremtése és megóvása érdekében – tehát kijelenthető, stratégiai cél a megfelelő eszközök, módszerek kiválasztása és olyan szabályok alkalmazása, amelyekkel a kívánt biztonsági szint elérhető. A stratégia megállapítja, hogy a biztonságos kibertér megteremtése az egyének, közösségek, gazdasági szereplők, kormányzati szervek és a jövő generációi számára egyaránt stratégiai cél Magyarországon [6; 8].

A meghatározott célok eléréséhez összkormányzati koordinációra, a civil, a gazdasági és a tudományos területek együttműködésére, valamint a szakosított intézmények (GovCERT) hatékony fellépésre van szükség a Kibervédelmi Stratégia alapján [6; 10; a)-h)]. A gazdasági szereplők motivációja [6; 10. i)] jelen tanulmány szemszögéből kiemeltem hangsúlyos követelmény, ugyanis ebben a pontban stratégiai célként jelenik meg a kiberbiztonsági követelmények meghatározásához, a kiberbiztonság fokozásához a szükséges módszerek, technológiák alkalmazásának elősegítése.

A Kibervédelmi Stratégia végrehajtásához szükséges eszközrendszerben számos politikai, illetve adminisztratív kormányzati teendő jelenik meg [6; 11. a)-h)], ám ezt követően külön pont foglalkozik a műszaki szempontokkal, konkrétan megjelenik „a kiberbiztonsági szempontok érvényesítése az állami műszaki fejlesztési feladatok, valamint a kormányzati információs rendszerek fejlesztésével és üzemeltetésével kapcsolatos feladatok ellátása során" [6; 11. i, 19]. Az utolsó feladat ellátásához megfelelő módszertani, technológiai háttérre van szükség, ahol már szükségesek a felhasznált technológiákkal szemben alkalmazható követelmények és mérőszámok.

A Kibervédelmi Stratégia véleményünk szerint megfelelően helyezi el a magyar kiberteret a nemzetközi kibertérben és jó alapot teremt a XXI. század kihívásaira való felkészüléshez. Erre a stratégiára épül a 2013. évi L. törvény [9] és a 185/2015. (VII. 13.) Korm. rendelet [10]. Előbbi az állami és önkormányzati szervek elektronikus információbiztonságát, utóbbi a kormányzati eseménykezelő központokkal kapcsolatos feladatokat és eseményeket tárgyalja. A 2013. évi L. törvény 1. fejezetében átfogó fogalomjegyzékkel találkozhatunk, az alábbiakban néhány fontos definíció található:

1. kiberbiztonság: *„a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez"* [9; 1.26]
2. kibervédelem: *„a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését"* [9; 1.27]

3. logikai védelem: „*az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem;"* [9; 1.34]
4. sérülékenységvizsgálat: „*az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági események feltárása;"* [9; 1.41]

A törvény hatálya alá eső elektronikus információs rendszerek esetében biztosítani kell a kezelt adatok és információk bizalmasságát, sértetlenségét és rendelkezésre állását és az adott rendszer zárt, teljes körű, folytonos és kockázatokkal arányos védelmét [9; 5]. Eme követelmény teljesülését a Kormány által kijelölt hatóság ellenőrzi. Az adott hatóságnak tevékenysége során még ellenőriznie kell egy adott szervezet által használt elektronikus információs rendszer osztályba sorolását és biztonsági szintjét, valamint az adott osztálynak és biztonsági szintnek megfelelő követelmények teljesülését. A hatóság feladata az ellenőrzés során feltárt biztonsági hiányosság elhárításának elrendelése [9; 14]. A felügyeletet ellátó hatóság elrendelheti egy elektronikus információs rendszer sérülékenységvizsgálatát, valamint egy biztonsági esemény kivizsgálását is [9; 18]. A törvény ezen kívül részletesen tárgyalja a kormányzati eseménykezelő központ hazai- és nemzetközi feladatait, valamint a polgári, nemzetbiztonsági és honvédelmi célú eseménykezelő központok hatáskörét. A 185/2015. (VII. 13.) Korm. rendelet konkretizálja az egyes eseménykezelő központokat, hatásköröket, valamint a sérülékenységvizsgálatot végezhető gazdasági szervezetek és személyek körét. A tárgyalt kormányrendelet konkrét követelményeket fogalmaz meg a sérülékenységvizsgálatra vonatkozóan:

1. vizsgált területek:
    a. „külső informatikai biztonsági vizsgálat
    b. webes vizsgálat
    c. belső informatikai biztonsági vizsgálat, illetve
    d. vezeték nélküli hálózat informatikai biztonsági vizsgálata" [10; 16 (1)]
2. jogosultsági fázisok
    a. „regisztrált felhasználói jogosultság nélküli vizsgálat
    b. regisztrált felhasználói jogosultsággal rendelkező vizsgálat és
    c. adminisztrátori jogosultsággal rendelkező vizsgálat" [10; 16 (2)]

A sérülékenységvizsgálat eredményét az érintett szerv és a hatóság is megkapja, amely alapján mindketten kötelesek eljárni. A tárgyalt két dokumentum a sérülékenység-vizsgálat és biztonsági esemény kivizsgálás eljárását és a kapcsolódó határidőket írja le, de további technológiai követelményeket nem fogalmaz meg.

AGILIS KIBERVÉDELEM

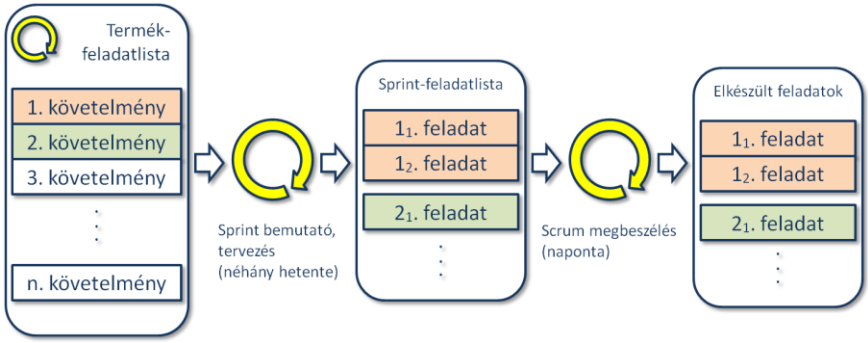
A törvényi háttér feldolgozása során jól meghatározott követelményekhez jutottunk egy alkalmazott informatikai rendszer felülvizsgálatának menetét illetően. Felmerülhet az olvasóban, hogy ezen ellenőrzések egy részét az adott informatikai rendszer alkalmazásba

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 4. szám

vétele előtt is el lehetne végezni, ezzel is javítva az adott elektronikus információs rendszer biztonságát. A megismert intézkedések alapvetően a külső eredetű kockázatokra való felkészülést tárgyalják, pedig hasonló kockázatokat rejthetnek a belső eredetű tervezési, megvalósítási és integrációs hibák is.

Az előzetesen megismert és feltárt követelmények, feladatok, problémák és hibák kezelésére kiválóan alkalmasak az agilis szoftverfejlesztési módszerek. Az agilis szoftverfejlesztés egy iteratív szoftverfejlesztési technológia, ahol egy adott terméket – informatikai rendszert – rövid megvalósítási időszakokkal, folyamatosan állítanak elő. A rendszerrel szemben támasztott követelmények egy termékre vonatkozó feladatlistában, fontossági sorrendben kapnak helyet. A fejlesztési iterációkban implementálandó feladatok a követelmények apró részekre bontásával jönnek létre. Az informatikai rendszer kialakítása során kiemelt szerepet kap a folyamatosan működő szoftver, magas színvonalú technológiai háttér és az ügyféllel tartott szoros kapcsolat. A témakörről részletesebb leírást a Hadmérnök XII. évf. 1. számában Gerevich János munkájában [11; 172-175 o.] találhatunk.



1. ábra: A Scrum folyamata [11; 174. o.]

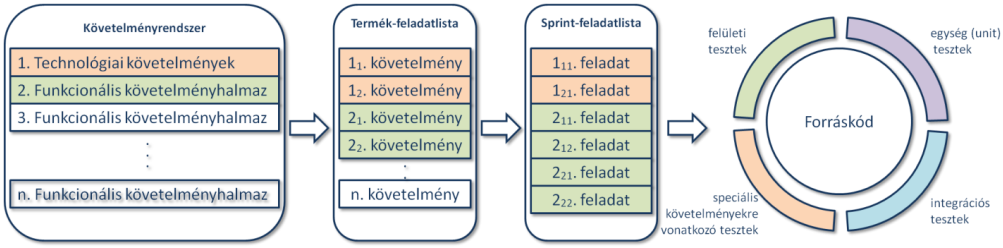
A *Scrum* [14] módszertan alapvetően a termékre vonatkozó feladatlista meglétét írja elő, nem szól a különböző jellegű szoftverfejlesztési projektek dokumentációs módszereiről. A *Scrum* szoftverfejlesztési módszertan katonai, illetve védelmi célú kiterjesztése a *Military Scrum*. A Military Scrum [12, 13] a védelmi célú szoftverek követelményelemzését különböző dokumentációs technikákkal támogatja. [14] A technika célja, hogy a lehető legbővebb, legjobb minőségű termékre vonatkozó feladatlista alapján indulhasson el egy rendszer fejlesztése. A dokumentációs technika az alábbi területeken alkalmazható

1. Új szoftver fejlesztése [12; 215-220 o.]
2. Alkalmazott szoftver cseréje új szoftver fejlesztésével, adatmigrálás nélkül [13; 235-237 o.]
3. Adatmigrálás [13; 237-241 o.]
4. Rendszerek közötti integráció [13; 241-242 o.]

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 4. szám

Mind a négy esetben alkalmazható a Military Scrum követelményelemzést támogató módszere, az egyes követelményhalmazok technológiai és funkcionális követelményhalmazokra történő szétválasztásával. Ha a katonai alkalmazást nézzük, akkor a stratégiai, a hadműveleti és a harcászati szintű követelményekhez kapcsolhatók a követelményhalmazok, ugyanakkor ez a fajta besorolás tetszőlegesen változtatható, alkalmazási területhez igazítható, itt kizárólag a követelmények forrásának azonosítása a cél.



2. ábra: A Military Scrum és az evolúciós szoftverfejlesztés kapcsolata (saját szerkesztés)

Ahogy a Scrum módszertan esetében a siker kulcsa az automatizált tesztelés, a Military Scrum kötelezően előírja a lehető legmagasabb szintű automatizált tesztlefedettséget az azonosított követelmények vonatkozásában – egyébként fölösleges lenne szofisztikált dokumentációs technikák alkalmazása, ugyanis az azonosított követelmények eltűnhetnek a fejlesztés alatt, a követelményekhez tartozó funkciók kimaradhatnak az szoftverből vagy szoftver-komponensből, ezáltal a teljes informatikai rendszerből is. Alapvetően minden követelményhez legalább egy tesztesetnek kell kapcsolódnia.

Alapesetben a fejlesztés menete a követelmények tesztesetekbe, majd tesztekbe foglalásával indul, ezt követi a kapcsolódó fejlesztés elvégzése, a fejlesztés akkor ér véget, amikor az elkészített tesztek helyes eredményt mutatnak. Egy ilyen módon felépített rendszerben minden lényegi változtatást jelez az automatizált tesztek futtatására alkalmas környezet. Még lényegesebb, hogy egy új követelménynek való megfeleléshez szükséges változtatásokat is jelzi a 2. ábrán látható tesztelési környezet. A fejlesztők ekkor eldönthetik, hogy a teszteseteket vagy a forráskódot kell megváltoztatni. Utóbbi esetén egy a szoftverekre értelmezett evolúciós folyamat jön létre, ugyanis ebben az esetben a környezethez alkalmazkodik a fejlesztés alatt álló szoftver és a helytelenül működő forráskód megváltozik, illetve eltűnik a rendszerből – a szoftverfejlesztők által. Ezt a folyamatot nevezik evolúciós szoftverfejlesztésnek, a bemutatott technika egyaránt alkalmazható a belső- és külső kockázatok kezelésére.

1. Belső kockázatok
    a. követelmények konzisztenciájának ellenőrzése;
    b. üzleti folyamatok, jogszabályi követelmények ellenőrzése;

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 4. szám

c. interfésszel illesztett belső rendszerekkel való kommunikáció;

2. Külső kockázatok
   a. terheléses tesztelés;
   b. interfésszel illesztett külső rendszerekkel való kommunikáció
   c. sérülékenységvizsgálat;

ÖSSZEGZÉS

A kibertér az infokommunikációs rendszerek fejlődésének hatására egyre több és bonyolultabb biztonsági kockázatot rejt magában. Az infokommunikációs biztonság kérdéskörével számos törvény és kormányrendelet foglalkozik. A létfontosságú infokommunikációs rendszerek védelme egyre nagyobb hangsúlyt kap nemzetközi szinten is, ezt mutatják a NATO és EU által meghatározott kibervédelmi stratégiák. A hazai Kibervédelmi Stratégia a nemzetközi irányelvek magyar leképezése. A kormányzati eseménykezelő központ és a nemzetbiztonsági- és védelmi szektor eseménykezelő központjai a hazai-, majd a globális hálózatfelügyeleti rendszerbe tagozódnak be. Úgy gondoljuk, hogy ezzel az eredeti célként kitűzött védelmi alapképesség kialakítása az infokommunikációs szektorban megtörtént.

A jövőre nézve a hazai és a nemzetközi kibertér biztonságának fenntartása továbbra is kihívásokkal teli feladat lesz. A technológia fejlődésével a szabályozás és a követelmények további fejlődése is várható. A zavarkeltés, az adatlopás és megsemmisítésre való törekvés jelenléte a kibertérben az infokommunikációs rendszerek építőelemeit képező szoftverekkel szemben újabb és újabb védelmi követelmények megjelenését fogják eredményezni. A bemutatott agilis technikákkal fejlesztett szoftverek az új biztonsági követelményeknek való megfelelést hatékonyan tudják kezelni – az evolúciós szoftverfejlesztésnek, a gyors reagálásnak köszönhetően.

Ha a hálózat alapú hadviselés, az információs műveletek vagy a kiberhadviselés képességeinek fejlesztése a cél, akkor a Military Scrum megfelelő választás lehet az egyedi szoftverek kialakításához ezeken a területeken, mert a követelmények elemzésétől kezdve figyelembe veszi a védelmi szektor felépítését és nagy hangsúlyt fektet a sok elemből álló és változó követelmények karbantartására. A módszer lehetővé teszi a belföldi know-how kialakítását a fejlesztett védelmi ágazatokban.

A kormányzati szektorban a mindenkori törvényhozó hatalomnak célszerű lenne a nagyobb információtechnológiai hatással bíró törvényeknek való megfelelést műszakilag ellenőrizni és támogatni. Megoldás lehetne ilyen esetekben egy kormányzati szintű műszaki bevizsgálás. Példa lehetne erre az elektronikus ügyintézés [4] biztosításához szükséges rendszerelemek szoftveres bevizsgálása. A vizsgálat hatásköre lehetne egy rendszerelem esetében a nyújtott és elérendő interfészekkel való kompatibilitás, valamint a kezelt adatok struktúrája, helyessége. Ezt azt jelentené, hogy a manuális auditálás mellett a műszaki ellenőrzés is megjelenhetne közigazgatásban használt rendszerek számára, ezzel a közigazgatás által használt kibertérben megjelenő rendszerelemek minősége jelentősen javulna.

Végezetül, úgy gondoljuk, hogy a biztonságosabb kibertér kérdése műszaki tervezési feladat is, melyhez a Military Scrum szoftverfejlesztési módszertan alkalmas választás lehet a követelményelemzés és a megvalósítás során is.

FELHASZNÁLT IRODALOM

1. 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
2. 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról
3. GEREVICH J., NÉGYESI I.: A MILITARY SCRUM KÖVETELMÉNYELEMZŐ MÓDSZERÉNEK ALKALMAZÁSA LÉTFONTOSSÁGÚ RENDSZEREK FEJLESZTÉSE SORÁN. In: Hadtudományi Szemle XI. 3. (2018)
4. Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény
5. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security' 163 final, COM(2011), Brussels, 2011. 03. 31.
6. 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
7. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 2013. 02. 07.
8. Defending the networks The NATO Policy on Cyber Defence, 2011. 08. 19. https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf (letöltve: 2018. 03. 22.)
9. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
10. 185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól
11. GEREVICH J.: Az agilis szoftverfejlesztés alkalmazásának lehetőségei a Magyar Honvédség számára. In: Hadmérnök XII. 1. (2017) 170-181. o. http://hadmernok.hu/171_14_gerevich.pdf (letöltve: 2018. 04. 26.)
12. GEREVICH J.: Híradó-informatikai fejlesztést támogató agilis dokumentációs módszerek. In: Hadmérnök XII. 3. (2017) 210-222. o. http://hadmernok.hu/173_19_gerevich.pdf (letöltve: 2018. 04. 28.)
13. GEREVICH J., NÉGYESI I.: Híradó-informatikai fejlesztést támogató agilis dokumentációs módszerek - 2. rész In: Hadmérnök XIII. 1. (2018) 230-244. o. http://hadmernok.hu/181_18_gerevich.pdf (letöltve: 2018. 04. 30.)

14. NÉGYESI I.: Informatikai rendszerek és alkalmazások a védelmi szférában (in.: Informatika Korszerű Technikái konferencia kiadvány, 1-10. o., Dunaújváros, 2010)
15. RUBIN K. S.: Essential Scrum. Ann Arbor, Michigan, USA, Pearson Education, Inc., 2013.
16. Az Európai Parlament 2012. november 22-i állásfoglalása a kiberbiztonságról és -védelemről (2012/2096(INI)) http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52012IP0457 (letöltve: 2018. 04. 15)
17. HOFFMAN, Frank G.: Conflict in the 21st Century: The Rise of Hybrid Wars.Wars. p. 8.
18. Krasznay Cs.: A Kiberhadviselés elvei és gyakorlata előadás, 2011, 2. old. http://krasznay.hu/presentation/kiberhadviseles2011_krasznay.pptx
19. NÉGYESI I.: COTS rendszerek alkalmazási lehetőségeinek vizsgálata (in.: Hadtudományi Szemle, IV. évf. (4), 111-116. o., Budapest, 2011)