HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

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

A Military Scrum követelményelemző módszerének alkalmazása létfontosságú rendszerek fejlesztése során

The Application of Military Scrum Requirement Analysis Method during Critical Infrastructure Developments

Absztrakt

Az Európai Unió már az előző évtizedben definiálta a kritikus infrastruktúrák – a magyar terminológiában létfontosságú rendszerek – fogalmát. A dolgozat feltárja az Európai Uniós szabályozás fejlődését a 2000-es évek elejétől napjainkig, valamint a kapcsolódó hazai jogszabályokat is górcső alá veszi. Ezt követően betekintést nyerhetünk a szoftvertechnológia egy lassan húsz éves múltra visszavezethető, napjainkban meghatározó irányvonalára az agilis szoftverfejlesztésre is. A tanulmány végén a kibertér szigeteiben tapasztalható külső és belső eredetű kockázatok kezelésére is használható módszert, a Military Scrum követelményelemző módszerét mutatják be a szerzők

Kulcsszavak: kritikus, létfontosságú, infrastruktúra, rendszer, agilis, követelmény, elemzés

Abstract

In the previous decade, the European Union defined the notion of critical infrastructures – vital systems in Hungarian terminology. This article explores the development process of the European Union regulations from the beginning of the 2000s to present days, as well as the related domestic legislation. After that, we can take an insight into the two decades old agile software development which has a decisive direction in the software technology nowadays. At the end of the study, we can see the requirement analysis method of the Military Scrum what

[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

can be used to decrease the external- and internal risks in the islands of the cyberspace.

Keywords: critical, vital, infrastructure, system, agile, requirement, analysis

LÉTFONTOSSÁGÚ RENDSZEREK VÉDELME AZ EU-BAN

Az infokommunikációs rendszerek biztonságával legmagasabb szinten elsőként 2001-ben foglalkozott az Európai Közösségek Bizottsága.[3] A *Javaslat egy európai hálózat- és informatikai biztonsági politikára*[4] című dokumentum „a témakör átfogó megközelítésére épült, amely abból indult ki, hogy a hálózatok, és informatikai rendszerek széles körben alkalmazott támogató infrastruktúrákká, a gazdasági és társadalmi fejlődés kulcstényezőivé váltak, így biztonságuk alapvető prioritás" – olvasható Munk Sándor kapcsolódó tanulmányában.[5] Az ezt követő években a kritikus infrastruktúrákkal kapcsolatos feladatrendszer kidolgozását tagállami és uniós szinten is megkezdték. 2006 decemberében az Európai Közösségek Bizottsága egy 3 tevékenységi irányból álló cselekvési tervet fogalmazott meg a létfontosságú rendszerek azonosítási és kijelölési folyamatának kidolgozásához.[6] Az egyes tevékenységi irányokhoz az alábbi fázisok kapcsolódtak.[7]

1. tevékenységi irány
   a Kritikus Infrastruktúra Védelem Európai Programjának (*European Programme of Critical Infrastructure Protection,* röviden: EPCIP) stratégiai aspektusai és a létfontosságú rendszerek védelmére horizontálisan alkalmazható intézkedések kidolgozása.
   - 1. fázis: a szabályozás kidolgozására vonatkozó ágazati sorrend, definíciók és fogalmak meghatározása. Létfontosságú rendszerek védelméhez szükséges azonosítási-, együttműködési-, iránymutatási-, adatmegosztási-, kockázat-elemzési- eszközök és módszerek feltárása az EPCIP megvalósításához;
   - 2. fázis: a cselekvéshez szükséges pénzügyi alapok megteremtése, melyből uniós szintű szakértői csoportok, tevékenységek finanszírozhatók;
   - 3. fázis: harmadik országokkal és nemzetközi szervezetekkel történő együttműködés megteremtése;

[3] Európai Közösségek Bizottsága – 2007-től Európai Bizottság.
[4] Network and Information Security: Proposal for a European Policy Approach; Commission of the European Communities, COM(2001) 298, Brussels, 2001. 06. 06.
[5] Munk Sándor: Kiberbiztonsági célok, jövőképek, szabályozók az EU-ban és kapcsolatrendszerük az interoperabilitással. In: *Hadmérnök,* XIII. (2018) KÖFOP különszám, 205–217. http://hadmernok.hu/180kofop_12_munk.pdf (Letöltve: 2018. 04. 05.)
[6] COMMUNICATION FROM THE COMMISSION on a European Programme for Critical Infrastructure Protection 786 final, COM(2006), Brussels, 2006. 12. 12.
[7] Uo. 4.1.

2. tevékenységi irány
az európai létfontosságú rendszerek védelme és az ágazati kérdések kezelése.
1. fázis: ágazati követelmények meghatározása az európai szintű létfontosságú rendszerek azonosításához;
2. fázis: a létfontosságú rendszerek azonosítására és vizsgálatára vonatkozó alapok kialakítása ágazatonként. Európai létfontosságú rendszerek kijelölése, sérülékenységek, kockázatok azonosítása. Szabályozások és biztonsági szintek harmonizációja;
3. fázis: európai létfontosságú rendszerek minimális védelmi képességére vonatkozó javaslatok kidolgozása és a megfelelő intézkedések foganatosítása.

3. tevékenységi irány –
tagállamok támogatása a saját nemzeti létfontosságú rendszereikkel kapcsolatos tevékenységük során.
1. fázis: nemzeti létfontosságú rendszerek azonosításához használt követelmények megosztása a tagállamok között;
2. fázis: a létfontosságú rendszerek azonosítására és vizsgálatára vonatkozó alapok kialakítása ágazati szinten, tagállami szintű létfontosságú rendszerek kijelölése, biztonsági rések elemzése;
3. fázis: tagállami szintű létfontosságú rendszerekre vonatkozó védelmi programok kialakítása és fejlesztése, védelmi intézkedések kialakítása, valamint a tulajdonosok, illetve üzemeltetők felügyelete.

A cselekvési terv megjelenése után két évvel, 2008. december 8-án a kritikus infrastruktúrák azonosításával, kijelölésével, valamint védelmük értékelésével és javításával foglalkozó 2008/114/EC számú Európai Tanács által meghatározott irányelv[8] fektette le és kötötte határidőhöz a létfontosságú rendszerek európai szintű nyilvántartásba vételét, melynek végrehajtására 2011. január 12-ét szabta határidőként a tagállamok számára. Első lépésben az energetika és a szállítmányozás[9] jelent meg kiemelt területként, ugyanakkor az infokommunikációs szektor már itt is említésre került, mint vizsgálandó terület. Az irányelv az alábbiak szerint definiálta a kritikus infrastruktúra védelemmel kapcsolatos fogalmakat:[10]

1. Kritikus infrastruktúra (*Critical Infrastructure*, röviden: CI) – Egy adott Európai Uniós tagállam területén működő létesítmény, rendszer vagy rendszerelem, amely alapvetően szükséges a létfontosságú társadalmi, egészségügyi, biztonsági, védelmi, gazdasági és szociális jóléti funkciók ellátásához. Egy kritikus infrastruktúra sérülése vagy megsemmisítése esetén az adott tagállam nem tudná megfelelően ellátni a funkcióit az érintett területeken.

[8] COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.
[9] Uo. 5. pont.
[10] Uo. 2. cikk.

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

2. Európai kritikus infrastruktúra (*European critical Infrastructure*, röviden: ECI) – olyan kritikus infrastruktúra, melynek sérülése vagy megsemmisülése legalább 2 tagállamra hatással van.
3. Kockázatelemzés – egy kritikus infrastruktúra sérülésének vagy megsemmisülésének hatásvizsgálata.
4. Védelem – olyan tevékenység, amely a fenyegetések megelőzését, enyhítését, illetve semlegesítését célozza meg egy adott létfontosságú rendszer vagy rendszerelem folyamatos fenntartása, működtetése, és integritásának megőrzése céljából.
5. Védelemi tevékenység során keletkező érzékeny információ – olyan tények és adatok, melyek felhasználásával célzott támadás indítható egy adott kritikus infrastruktúra ellen.
6. Európai kritikus infrastruktúra tulajdonosa, illetve üzemeltetője – azok az érintett felek, akik valamilyen formában (anyagi vagy üzemeltetési) felelősséggel tartoznak egy adott kritikus infrastruktúrára vonatkozóan.

A további cikkelyekben (3–9 cikk) az európai kritikus infrastruktúrák azonosítása, kijelölése, a védelemhez szükséges biztonsági tervek és a biztonsági összekötő tisztviselők (*Security Liaison Officer*) szerepe, a védelmi tevékenységről készült beszámolók és a védelmi tevékenység során keletkező érzékeny adatok kezelése került tárgyalásra. Az azonosítási eljárás során az adott ECI sérülése vagy megsemmisülése következtében bekövetkező halálesetek vagy sérülések száma, a gazdasági-, illetve társadalmi hatás került meghatározásra kijelölési szempontként. A kijelölés támogatását a tagállamok közötti együttműködés megszervezésével, két- illetve többoldalú szerződések megkötésével javasolta az Európai Tanács. A kijelölési folyamat tárgyalását követően a biztonsági terveknek megfelelő üzemeltetés fenntartása kapott hangsúlyt.

Elmondható, hogy az Európai Tanács egy átgondolt, jól strukturált és következetes előkészítést követően megalapozta a létfontosságú rendszerek védelmének szabályozását az Európai Unió egészére és a tagállamokra vonatkozóan is. Ennek az előkészítési folyamatnak eredménye a magyar szabályozás is, melyről az alábbiakban olvashatunk.

LÉTFONTOSSÁGÚ RENDSZEREK VÉDELME MAGYARORSZÁGON

Mielőtt a létfontosságú rendszerekkel kapcsolatos magyar szabályozást áttekintenénk, érdemes rövid pillantást vetni a jelenleg érvényes hazai biztonsági stratégiákra a biztonság és ezen belül is a kiberbiztonság szemszögéből. Az alábbiakban a tanulmány szempontjából lényeges pontokat, gondolatokat olvashatjuk, némi magyarázattal kibővítve.

MAGYARORSZÁG NEMZETI BIZTONSÁGI STRATÉGIÁJA[11]

1. fejezet:

Magyarország biztonságpolitikai környezete. A dokumentum leszögezi, hogy a „21. század elején is előfordulhat, hogy a katonai erő kap elsődleges szerepet egy

[11] 1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.

regionális konfliktusban", ugyanakkor „a biztonság katonai szegmense is új hangsúlyokkal jelenik meg". Az iménti két megállapítás a hagyományos értelemben vett katonai fenyegetéseken túl, a kibertérben megjelenő fenyegetésekre is teljes mértékben értelmezhető. A hibrid hadviselés[12] szerves részeként megjelenő kiberhadviselés[13] erre a legjobb példa. Ezen túlmenően a terrorizmus és az illegális bevándorlás napjainkban is valós és folyamatosan jelenlévő fenyegetést jelent, ezért gondoljuk úgy, hogy a Biztonsági Stratégiában tett megállapítás manapság megállja a helyét, miszerint „globalizált világunkban a biztonság nem a határainknál kezdődik" – legyen az a valóság vagy a kibertér.

2. fejezet:

Magyarország helye és biztonságpolitikai érdekei a világban. A Biztonsági Stratégia megállapítja, hogy „Az Észak-atlanti Szerződés 5. cikke, a kollektív védelem Magyarország biztonságának sarokköve" [13], valamint „Magyarország NATO- és EU-keretekben folytatott biztonságpolitikai tevékenysége globális és átfogó jelleget ölt" [18]. A különböző missziós tevékenységen túl a nemzetközi- és különösen a magyar kibertér biztonságának óvása is nemzeti ügy. Még nagyobb jelentőséggel bír a kibertér védelme 2016 júliusát követően, amikor is a NATO a kiberteret hadszíntérré nyilvánította. Így a NATO-nak ugyanolyan hatékonyan meg kell tudnia védenie magát a kibertérben, mint a levegőben, a szárazföldön vagy a tengeren.[14]

3. fejezet:

A Magyarországot érintő biztonsági fenyegetések, kihívások és azok kezelése. A klasszikus fenyegetéseken túl megjelenik a Kiberbiztonság megóvásának kérdése is a Biztonsági Stratégiában. A dokumentum úgy fogalmaz, hogy „egyre sürgetőbb és összetettebb kihívásokkal kell számolnunk az informatikai- és telekommunikációs hálózatok, valamint a kapcsolódó kritikus infrastruktúra fizikai és virtuális terében" [31]. Az infokommunikációs hálózatok, informatikai szolgáltatások sérülékenységeit kihasználva ellenségesen fellépő államok, terrorista csoportok jelentős

[12] Hibrid hadviselés: „a hibrid fenyegetések a hadviselés számos formáját magukban foglalják, beleértve a konvencionális képességeket, irreguláris harceljárásokat és képződményeket, valamint a válogatás nélküli erőszakot alkalmazó terrorista akciókat és bűnözői tevékenységeket. Hibrid háborúkat egyaránt folytathatnak állami és a legkülönfélébb nem állami szereplők. Az egymástól elszigetelten működő egységek, vagy akár ugyanaz a csoport is folytathat »multimodális« tevékenységeket, de ezek általános, műveleti, valamint harcászati irányítása és koordinálása a fő hadszíntéren megy végbe, annak érdekében, hogy a szinergikus hatások bekövetkezzenek a konfliktusok pszichológiai és fizikai dimenzióiban. Ezen hatások a háború valamennyi szintjén jelentkezhetnek." Rubin K. S.: Essential Scrum. Pearson Education, Inc., Ann Arbor, Michigan, USA, 2013.

[13] Kiberhadviselés: a (kritikus) információs infrastruktúrák bizalmasságának, sértetlenségének és rendelkezésre állásának befolyásolására irányuló tevékenység informatikai, fizikai és emberi eszközökkel. Gerevich János: Az agilis szoftverfejlesztés alkalmazásának lehetőségei a Magyar Honvédség számára. *Hadmérnök,* XII (2017/1). 170–181.

[14] NATO Cyber Defence Topic. https://www.nato.int/cps/en/natohq/topics_78170.htm (Letöltve: 2018. 03. 20.)

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

károkat okozhatnak. A dokumentum a hazai kibervédelem megteremtésén túl a nemzetközi védelemben történő részvételt határozza meg elérendő célként.

4. fejezet:

A Nemzeti Biztonsági Stratégia végrehajtásának eszközrendszere: a felbukkanó fenyegetések ellen történő hatékony fellépés érdekében „erősíteni kell a honvédelmi, nemzetbiztonsági, rendvédelmi, igazságszolgáltatási, katasztrófavédelmi és polgári válságkezelési intézmények szoros és hatékony együttműködését" [43]. Az említett együttműködés magas szintű támogatása többek között a kibertér egy speciális, védelmi célú szektorában valósulhat meg az érintett szereplők közötti magas szintű információcsere révén – az együttműködést támogató védelmi célú informatikai szolgáltatások segítségével.

Habár a dokumentum 2012-ben lépett hatályba, és lényeges biztonsági kérdéseket tárgyalt a kiberbiztonság témakörében, az alkalmazható eszközrendszerre még nem tért ki megfelelő mélységben. A Nemzeti Biztonsági Stratégia megjelenését követően egy új katonai stratégia is napvilágot látott, a dokumentum kiberbiztonságot érintő pontjait az alábbiakban olvashatjuk.

MAGYARORSZÁG NEMZETI KATONAI STRATÉGIÁJA[15]

A Katonai Stratégia bővebben tárgyalja Magyarország biztonsági környezetét, hasonlóan a Biztonsági Stratégiához a NATO-és az EU tagságot határozza meg Magyarország biztonságának zálogaként, különös tekintettel a NATO Washingtoni Szerződés 5. cikke alapján megvalósuló kollektív védelemre és az EU Lisszaboni Szerződés kölcsönös segítségnyújtási és szolidaritási klauzuláira. A Magyar Honvédség működési környezetén belül is megjelenik a kibertér fogalma, mely új kihívások és potenciális veszélyek forrása lehet [33]. A haderő várható alkalmazási területei között megjelenik a kibertérhez kapcsolódóan a hálózatalapú hadviselés a különböző válságok kezelése során [41]. A technikai területen túlmutatva az információs műveletek súlya drasztikusan növekedik, a megfelelő tájékoztatás, a média, a digitális információáramlás eszközeinek magas szintű felhasználása kulcsfontosságúvá válik [51]. A Katonai Stratégia megállapítja, hogy a digitális eszközök, szolgáltatások, a lakosság vagy akár a védelmi feladatot ellátó erők ellen elkövetett, nem kimondottan fegyveresen – inkább technikai-, digitális eszközökkel – végrehajtott támadások aránya növekedik. Ezt a fajta új hadviselés jelentős anyagi károkat és káoszt okozhat, megközelítve a hagyományos fegyverek potenciálját [52].

A Magyar Honvédség kialakítandó képességeivel kapcsolatban a stratégia valamennyi hadrendi elemre vonatkozó legalább alap szintű támadási képesség meglétét célozza meg [69]. A Katonai Stratégia végén a hálózatalapú hadviselés feltételeinek megteremtése jelenik meg célként, mely a kibertér egy speciális katonai célú alkalmazását jelenti, ahol már nem csak a védelmi feladatok ellátása a cél, hanem különböző jellegű műveletek ki-

[15] 1656/2012. (XII. 20.) Korm. határozat Magyarország Nemzeti Katonai stratégiájának elfogadásáról.

bertérben történő támogatása is. Ezen a területen a technikai eszközök beszerzése, fejlesztése, valamint az állomány felkészítése, továbbképzése egyaránt feladat.[16]

A Katonai Stratégiában megjelenik kibertér és a kiberhadviselés fogalma. Napjainkra a stratégiában említett védelmi képességeken túl az alapszintű támadási képességek fejlesztése is cél lehet. A megfelelő követelmények megfogalmazása és a technológiai eszközök kiválasztása a hálózat alapú hadviselés, az információs műveletek és a kiberhadviselés területén is kulcsfontosságú kérdésnek tekinthetők.

A bemutatott két stratégia lényeges gondolatokat tartalmaz a kibervédelem témakörében, de ahhoz hogy teljes képet kaphassunk a létfontosságú információs rendszerek védelméről röviden érdemes néhány szót ejteni a 2012. évi CLXVI. Törvényről [8], mely a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről rendelkezik, a törvény végrehajtását a 65/2013. (III. 8.) Korm. Rendelet[17] szabályozza. Az alábbi főtevékenységek jelennek meg az imént említett két dokumentumban a létfontosságú rendszerekre vonatkozóan:

1. Azonosítási eljárás – „az a folyamat, amely során a lehetséges létfontosságú rendszerelemeket kockázatelemzés, valamint az ágazati és horizontális kritériumok alapján meghatározzák” [1.1];
2. Kijelölés eljárás – a nemzeti és az európai létfontosságú rendszerelemmé történő nyilvánítás folyamata. Abban az esetben indítható, ha az azonosítási eljárás eredménye pozitív, tehát az adott rendszerelem megfelel valamely ágazati és horizontális kritériumnak.
3. Visszavonási eljárás – a nemzeti és az európai létfontosságú rendszerelem státusz megszüntetésére vonatkozó folyamat, melyet nemzeti szinten a kijelölő hatóság folytat le, pozitív eredmény esetén az adott létfontosságú rendszerelem törlésre kerül a nyilvántartásból. Európai szinten egy EGT tagállam kezdeményezheti, és a Kormány dönt a státusz megszüntetéséről.
4. Nyilvántartás – a kijelölt nemzeti és európai létfontosságú rendszerek nyilvántartása.
5. Üzemeletetői biztonsági terv [9; 2. melléklet] – a létfontosságú rendszerelemek nyilvántartásba vételéhez szükséges dokumentum, melynek tartalmaznia kell az általános-, a környezeti- és a kijelölt rendszerelemre vonatkozó leírást. A biztonsági terv további fejezetei a kockázatelemzés, a kockázatkezelés és megvalósításhoz szükséges eszközrendszer bemutatása.

[16] Négyesi Imre.: Die überprüfung der voraussetzungen COTS system. *Hadmérnök,* VII (2012/2). 371–376. http://hadmernok.hu/2012_2_negyesi.pdf (Letöltve: 2018. 04. 30.); Uő: Informatikai rendszerek a védelmi szférában. In: Informatika korszerű Technikái Konferencia. DUF Konferencia kiadvány, 2010, 1–10. ISBN: 978-963-9915-38-1, http://www.duf.hu/fooldal/2010-februar/ikt-2010-konferencia (Letöltve: 2018. 04. 30.)

[17] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. Vö. Négyesi: Informatikai rendszerek a védelmi szférában. i. m.

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

A bemutatott folyamatos tevékenységeken túl, a Kormány éves jelentést nyújt be az Európai Bizottságnak az európai létfontosságú rendszerekkel kapcsolatos statisztikai adatokról, valamint a kapcsolódó sebezhetőségi pontokról. [8; 13] Megállapítható, hogy a bemutatott eljárási rend a 2008/114/EC számú Európai Tanács által meghatározott irányelv magyar leképezése.

Az eddig szemléltetett létfontosságú rendszerekre vonatkozó folyamatok alapvetően fizikai infrastruktúra védelemre vonatkoznak, és nehéz ebben a formában interpretálni őket az infokommunikációs rendszerekre. Ezt a problémát az Európai Unió is külön kezelte, külön szabályozást hozott létre a kibertér védelmére vonatkozóan. A létfontosságú infokommunikációs rendszerek és a kibervédelem témakörének további részletes elemzése meghaladja jelen tanulmány kereteit, ugyanakkor ezen a ponton célszerű egy pillantást vetni az informatikai rendszereket önálló modulként, szolgáltatásként használó létfontosságú rendszerekre. A kérdés az, hogy létezik-e olyan módszer, mellyel hatékonyan lehet támogatni a tervezés, kockázatelemzés és a kockázatkezelés feladatait?

AGILIS KRITIKUS INFRASTRUKTÚRA VÉDELEM

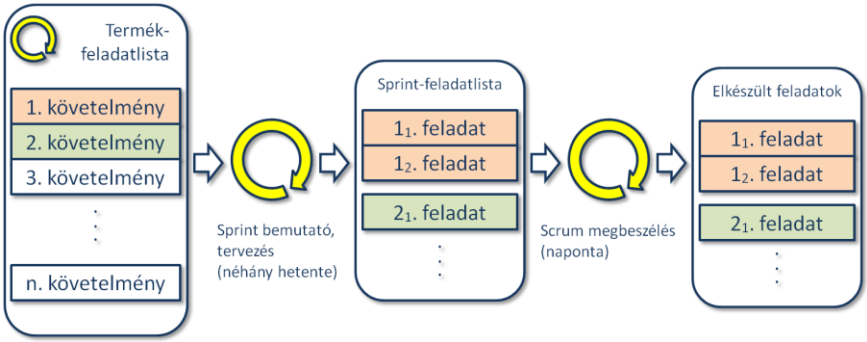
Mit értünk agilis kritikus infrastruktúra védelem alatt? A törvényi háttér feldolgozása során jól meghatározott követelményekhez jutottunk a létfontosságú rendszerek azonosítását, kijelölését és nyilvántartásba vételét illetően. Minden esetben szükséges az üzemeltetői biztonsági terv megléte, melyet akár iteratív követelményelemzés segítségével is el lehet készíteni. Itt jön képbe az agilitás, konkrétan az agilis szoftverfejlesztés és a hozzá kapcsolódó dokumentációs technikák. Az említett módszerek alkalmazási lehetősége a szoftverfejlesztést részben, illetve azt egyáltalán nem érintő területeken is lehetséges az alábbiak szerint.

Az agilis szoftverfejlesztés egy iteratív szoftverfejlesztési technológia, ahol egy terméket – alapvetően szoftvert – 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. A termék fejlesztése során kiemelt szerepet kap a folyamatosan működő szoftver és az ügyféllel tartott szoros kapcsolat. A folyamatos működést automatizált tesztelés segítségével lehet elérni, az elérendő cél, hogy minden funkcióhoz automatizált tesztek tartozzanak. Az egyik legelterjedtebb agilis szoftverfejlesztési módszertan a Scrum.[18] A témakörről részletesebb leírást Gerevich János munkájában találhatunk.[19]

[18] Rubin K. S.: Essential Scrum. Pearson Education, Inc., Ann Arbor, Michigan, USA, 2013.
[19] Gerevich: i. m. 172–175.

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám



1. sz. ábra: A Scrum folyamata[20]

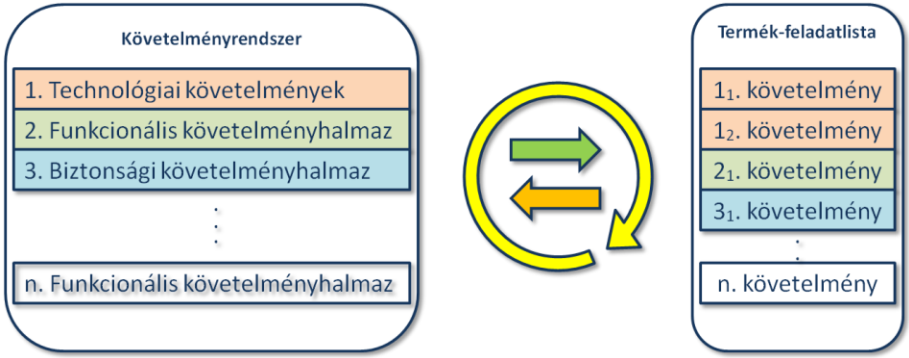
A *Scrum* és a *Military Scrum*[21] alapvetően szoftverfejlesztést támogató módszerek, ugyanakkor mindkét módszer használja a termékre vonatkozó feladatlista – Scrum terminológiában *product backlog* – fogalmát. Ha a Scrumot tekintjük, akkor a product backlog egyfajta rendszerfejlesztés-indító projektdokumentumként is felfogható. Ezzel az agilis technikával hardver- és szoftverkomponenseket tartalmazó rendszerfejlesztést is lehet támogatni, csak a product backlogban megfogalmazott követelmények finomsága határozza meg a felhasználás lehetőségeit. Azokban az esetekben, ahol fizikailag létező egységek jelennek meg, nem értelmezhető az automatizált tesztelés, így ezekben az esetekben más projektmódszertan szükséges a megvalósításhoz. Ezzel párhuzamosan egyéb műszaki specifikációs módszerekre van szükség. A hagyományos Scrum kapcsán elmondható, hogy alap szinten használható a követelmény-elemzéshez bármilyen rendszer esetében.

A Military Scrum kiegészíti a Scrum feladatrendszerező és feladatrendező módszerét, azzal, hogy a követelmények elemzését a követelményhalmazok összeállításával kezdi meg. A Military Scrum az egyes követelményhalmazokat hozzárendeli a követelmény formálójához, ennek akkor van jelentősége, ha egy nagyobb hierarchikus szervezet fogalmazza meg azokat, ugyanis ekkor az egyes témakörökben keletkező követelmények tisztázása alapvető jelentőséggel bír.

[20] Uo. 174. o.
[21] Uo.; Hoffman, Frank G.: Conflict in the 21st Century: The Rise of Hybrid Wars. Wars. 8.; Krasznay Cs.: A Kiberhadviselés elvei és gyakorlata előadás, 2011, 2
http://krasznay.hu/presentation/kiberhadviseles2011_krasznay.pptx

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám



2. sz. ábra: A Military Scrum követelményhalmazainak és követelményeinek kapcsolata (saját szerkesztés)

A *2. ábra* a követelmények azonosításának, illetve finomításának folyamatát mutatja be. Egy biztonsági követelményhalmaz egy vagy több követelményt jelenthet a termékre vonatkozó feladatlistában, ugyanakkor a termékre vonatkozó feladatlista összeállítása során egy biztonsági követelmény alapján szükségessé válhat a követelményhalmazok áttekintése és tisztázása a követelményt megformáló entitások között. A Military Scrum követelményelemzési módszerének sikere a követelményhalmazok és termék-feladatlista közötti logikai ellentmondások iteratív feloldásán alapszik. Ha szoftverfejlesztést érintő kérdésekről beszélünk, akkor az automatizált tesztelés segítséget nyújthat a problémák feloldásában. Ekkor, de egyéb esetekben is a követelményrendszer – a követelményhalmazok és a termékre vonatkozó feladatlista – megértése, feltárása és tisztázása a siker záloga.

Egy önállóan működő, fizikailag létező létfontosságú rendszer esetében is kiemelt fontossággal bír az általa használt informatikai rendszerek megfelelő működése. Példaként gondolhatunk egy vízszolgáltatást biztosító vízhálózati vezérlő rendszerre. Egy ilyen rendszer esetében a háttérben nagy valószínűséggel megjelenik valamilyen vezérlési feladatokat ellátó célszoftver. Általában ez egy szeparáltan működő informatikai rendszer, amely különböző programozható eszközök vezérlésére alkalmas.

Egy ilyen rendszer tervezésénél, továbbfejlesztésénél, illetve létfontosságú rendszerré nyilvánításakor is alkalmas választás lehet a Military Scrum követelményelemző módszere a szükséges dokumentációk elkészítéséhez, mert a módszer lehetőséget biztosít a követelmények strukturált gyűjtéséhez és az iterációk révén egy kifinomult, minden követelményformáló által teljesnek vélhető feladatlista összeállítását teszi lehetővé.

Az üzemeltetői biztonsági tervek kötelező elemei kockázatelemzés, kockázatkezelés és megvalósítás eszközeire vonatkozó fejezetek. A Military Scrum fázisai párba állíthatók az üzemeltetői biztonsági terv fejezeteivel az alábbiak szerint.

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

1. kockázatelemzés → biztonsági követelményhalmazok meghatározása
2. kockázatkezelés → biztonsági követelmények és reagálás meghatározása
3. eszközrendszer → automatizált tesztelés, szakterület specifikus eszközök

ÖSSZEGZÉS

A létfontosságú rendszerek védelme és ezen belül a kibertérben megjelenő kockázatokra való felkészülés az Európai Unióban két évtizedes múltra tekint vissza, a folyamat hatásait Magyarországon is érezhetjük. A fizikailag létező és az infokommunikációs létfontosságú rendszerek védelme külön szabályozás alá esik, de az előbbi esetében is jellemző az elkülönülten működő informatikai rendszerek megléte. Mindez azt jelenti, hogy a kibertér szeparált szigetein is szükségesek a megfelelő informatikai követelményelemzést, dokumentációt támogató eljárások.

Ha van ilyen jellegű kapcsolódási pont, akkor lehetőség nyílik az agilis szoftverfejlesztésből eredeztethető, termék-feladatlista igénybevételére. A létfontosságú rendszerek biztonsági terveinek elkészítésénél hasznos lehet a Scrum által nyújtott product backlog vezetése. A product backlog nyújtotta lehetőség kimerül a követelmények egyetlen listában történő felsorolásában. Ezen túlmenően a Military Scrum nyújt egy kétszintű, iteratív követelményelemző módszert a követelmények és a kockázatok gyűjtéséhez és azok együttes megértéséhez is. A bemutatott módszer lehetővé teszi az együttműködést a tervezést és kockázatelemzést folytató műszaki és biztonsági szakemberek számára, így egy teljes követelményrendszert létrehozva.

Ha a biztonsági követelmények megjelennek a követelményhalmazokban és a termékre vonatkozó feladatlistában, akkor a külső és belső eredetű kockázatok csökkenthetők, mert kialakított rendszerek tartalmazni fogják a megfelelő biztonsági követelmények kielégítéséhez szükséges funkciókat, illetve fizikai elemeket. Végső következtetésként levonható, hogy a létfontosságú rendszerek védelme, ezen belül a biztonsági tervek előállítása agilis eszközök segítségével magas szinten támogatható.

FELHASZNÁLT IRODALOM

1. COMMUNICATION FROM THE COMMISSION on a European Programme for Critical Infrastructure Protection 786 final, COM(2006), Brussels, 2006. 12. 12.
2. COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.
3. Gerevich J.: Az agilis szoftverfejlesztés alkalmazásának lehetőségei a Magyar Honvédség számára. *Hadmérnök,* XII (2017/1) 170–181. http://hadmernok.hu/171_14_gerevich.pdf (Letöltve: 2018. 04. 26.)
4. Gerevich J.: Híradó-informatikai fejlesztést támogató agilis dokumentációs módszerek. 1. rész. *Hadmérnök,* XII (2017/3). 210–222. http://hadmernok.hu/173_19_gerevich.pdf (Letöltve: 2018. 04. 28.)

5. Gerevich J., Négyesi I.: Híradó-informatikai fejlesztést támogató agilis dokumentációs módszerek. 2. rész. *Hadmérnök,* XIII (2018/1). 230–244. http://hadmernok.hu/181_18_gerevich.pdf (Letöltve: 2018. 04. 30.)
6. Hoffman, Frank G.: Conflict in the 21st Century: The Rise of Hybrid Wars. Wars. 8.
7. Krasznay Cs.: A Kiberhadviselés elvei és gyakorlata előadás, 2011, 2. http://krasznay.hu/presentation/kiberhadviseles2011_krasznay.pptx
8. Munk S. Kiberbiztonsági célok, jövőképek, szabályozók az EU-ban és kapcsolatrendszerük az interoperabilitással. *Hadmérnök,* XIII (2018) KÖFOP különszám 205–217. http://hadmernok.hu/180kofop_12_munk.pdf (Letöltve: 2018. 04. 05.)
9. NATO Cyber Defence Topic. https://www.nato.int/cps/en/natohq/topics_78170.htm (Letöltve: 2018. 03. 20.)
10. Network and Information Security: Proposal for a European Policy Approach; Commission of the European Communities, COM(2001) 298, Brussels, 2001. 06. 06.
11. Négyesi I.: Die überprüfung der voraussetzungen COTS system. *Hadmérnök,* VII (2012/2). 371–376. http://hadmernok.hu/2012_2_negyesi.pdf (Letöltve: 2018. 04. 30.)
12. Négyesi I.: Informatikai rendszerek a védelmi szférában. In: Informatika korszerű Technikái Konferencia. 2010, DUF Konferencia kiadvány, 1–10. http://www.duf.hu/fooldal/2010-februar/ikt-2010-konferencia (Letöltve: 2018. 04. 30.)
13. Rubin K. S.: Essential Scrum. Ann Arbor, Michigan, USA, Pearson Education, Inc., 2013.
14. 1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.
15. 1656/2012. (XII. 20.) Korm. határozat Magyarország Nemzeti Katonai stratégiájának elfogadásáról.
16. 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.
17. 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról.
18. Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény.