HADMÉRNÖK

VI. Évfolyam 1. szám - 2011. március

Kovács László
kovacs.laszlo@zmne.hu

Sipos Marianna
sipos.marianna@zmne.hu

A STUXNET ÉS AMI MÖGÖTTE VAN II.:
CÉLOK ÉS TEENDŐK

Absztrakt

A Stuxnet nevű féreg hatalmas riadalmat okozott 2010 nyarán illetve kora őszén. A riadalom oka elsősorban az volt, hogy ez volt az első olyan rosszindulatú program, amely ipari létesítmények vezérlő szoftvereit támadta meg. Jelen írás első része nagyon röviden bemutatta magát a Stuxnet-et, és elemezte azokat a várható hatásokat, amelyek az információbiztonságban e féreg után felmerülhetnek. Az írás második részében a komplex információbiztonság és a kormányzat - a védelemben betöltendő - szerepe kerül bemutatásra.

A worm called Stuxnet caused great alarm in summer and the early autumn of 2010. The main reason of the panic was that it was the first malicious program, which challenged the software to control industrial plants. The first part of this paper briefly described itself the Stuxnet, and analyzed the potential effects that may arise after this worm on the field of information security. In this paper the authors focus on the complex information security and the role of government on this field.

Kulcsszavak: *Stuxnet, információbiztonság, ipar, SCADA ~ Stuxnet, information security, industry, SCADA*

BEVEZETŐ

Jelen cikk első része a Stuxnet nevű féreg megjelenését és azokat a főbb informatikai – programozási kérdéseket járta körül, amelyek lehetővé tették a féreg elterjedését. [1]

Ugyanakkor az azóta eltelt időben számos olyan technikai elemzés látott napvilágot, amelyek további részleteket és adalékokat szolgáltatnak a világhírnevet szerzett féreggel kapcsolatban. A cikk első részének megírása és publikálása idején még csak sejtések voltak az igazi célokról, illetve arról, hogy ki, vagy kik is állhatnak a program mögött.

Bár egyértelmű bizonyíték még ma sincs a „gyártóról", a nemzetközi szaksajtóban egyre többet lehet olvasni arról, hogy az USA hathatós segítségével Izrael állt a háttérben.

A Stuxnet megjelenése rávilágított egy eddig nem, vagy nem elég jól kezelt problémára. Ez pedig nem más, mint az, hogy az ipari rendszerek vezérlése, automatizálása ma alapvetően olyan informatikai eszközökkel és rendszerekkel történik, amelyek hasonlóan az egyéb rendszerekhez, igen komoly mértékben sérülékenyek lehetnek.

Mindezeken túl azonban számos olyan terület is felbukkan, amelyek hasonló informatikai eszközöket használnak a működés biztosítására. A repüléstől kezdődően a hétköznapi közlekedésben használt járművek elektronikai és informatikai rendszeréig számos olyan területet találunk, ahol a sérülékenységek, és az ezzel járó veszélyek jelen vannak.

Az információbiztonság az elmúlt években hatalmas fejlődésen ment keresztül, ugyanakkor még ma is nagyon sokszor találkozni azzal az általánosítással, amely az informatika területére egyszerűsíti ezt a kérdést.

A Stuxnet pedig rávilágított, hogy az eddig igencsak marginálisan kezelt területeken, mint például az ipari vezérlő rendszerek ugyanolyan, ha nem nagyobb veszélyeknek vagyunk kitéve, mint a hagyományosnak tekintett internet és infokommunikációs hálózatok esetében.

Természetesen a védelemnek ezeken az új (régi) területeken is komplexnek, mindenre kiterjedőnek kell lennie, hiszen – ha száz százalékos biztonság nem is érhető el –, csak így garantálható a veszélyekkel arányos, azok kockázatait figyelembe vevő – viszonylagosan magas szintű – biztonság.

Jelen írás bemutatja, hogy a cikk első részének megjelenése óta, milyen új részletek kerültek napvilágra a Stuxnet működéséről.

Írásunk arra is választ keres, hogy milyen teendőink vannak az ilyen és hasonló veszélyek kivédése, vagy esetleges bekövetkezésük esetén a veszteségek minimalizálása érdekében.

A STUXNET ÉS MŰKÖDÉSE

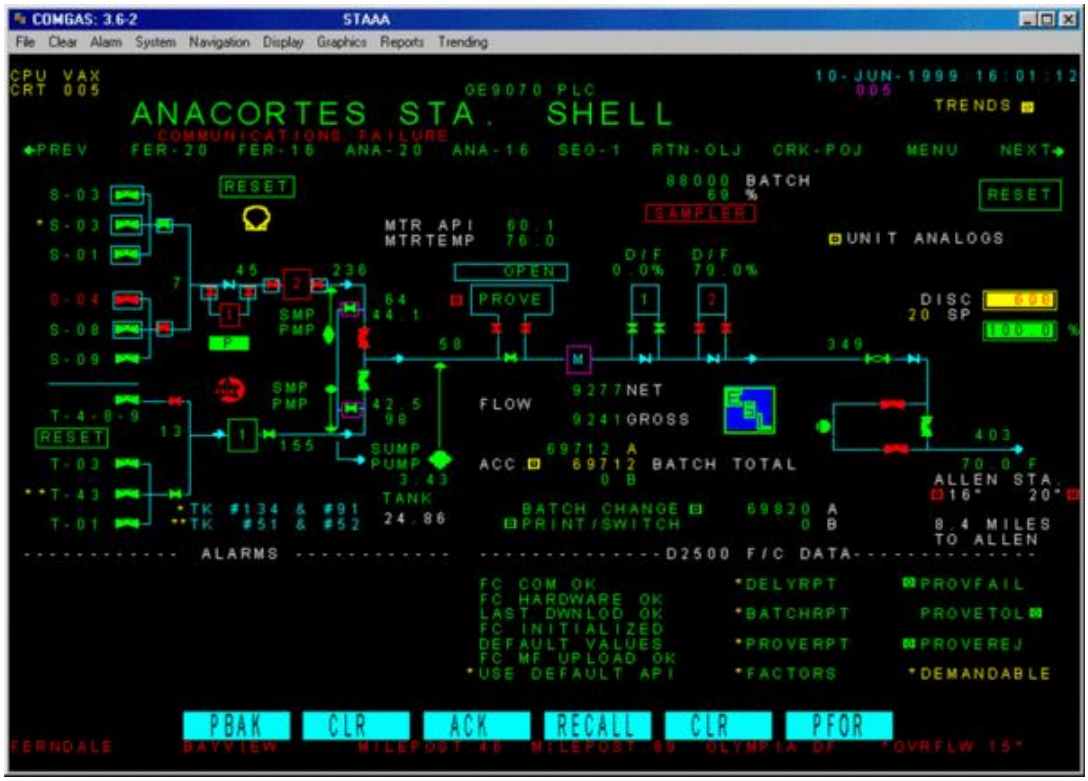
A PLC-k módosítása

Mint ahogy cikkünk első részében bemutattuk, a Stuxnet támadást elsősorban az ipari vezérlő rendszerek ellen fejlesztették ki. A támadás végső célja az ICS (Industrial Control Systems) újraprogramozása volt. [1] A PLC-k (Pogrammable Logic Controllers) kódjának módosításával azt kívánták elérni, hogy a támadó szándékának megfelelően működjenek, miközben a módosítások rejtve maradnak az eszköz kezelője előtt.

A cél érdekében a fejlesztők támadásoknál használatos eszközök sokaságát vetették be, és javítatlan biztonsági réseket támadtak (zero-day exploit). A támadók egy Windows rootkit segítségével képessé váltak a fertőzött gép adatainak elérésére és rendszergazdai jogosultságok megszerzésére. Elkerülték, hogy az antivírus programok és a számítógép kezelői felfedezzék jelenlétüket. A következő lépésben létrehozták a világon az első PLC rootkit szoftvercsomagot, mellyel kódblokkokat rejtettek a PLC-k programjaiba és az eredeti

kód végrehajtása helyett ezeket futtatták, valamint megszakították a vezérlés visszajelzését, hogy a hamis adatok elrejtsék a féreg tevékenységét.

Olyan rutinokat használtak, amelyek a hálózaton és USB-n keresztül is fertőztek, illetve peer-to-peer frissítést alkalmaztak a vírus példányai közt. Ellenőrző és vezérlő interfészeket alkalmaztak, melyek lehetővé tették a csatlakozást az úgynevezett C&C (Command and Control) szerverekhez. Így a C&C szerverekről frissítések letöltésével a vezérlő programok további módosítása is lehetővé vált.



1. ábra. Egy tipikus SCADA rendszer képernyőképe. [9]

Előző cikkünk a Stuxnet terjedését és elrejtését elemezte. [1] Az már a féreg felfedezését követő első pillanatokban kiderült, hogy a Stuxnet célját a PLC-ken keresztül éri el.

Nagyon leegyszerűsítve a PLC programozók egy külön számítógépen, meghatározott nyelveken pl. STL vagy SCL megírják a kódblokkokat, és lefordítják egy MC7 nevű assemblybe. Ezt követően ezeket a kódblokkokat feltöltik PLC eszközökre, és ezek futtatásával vezérlik és monitorozzák az ipari folyamatokat.

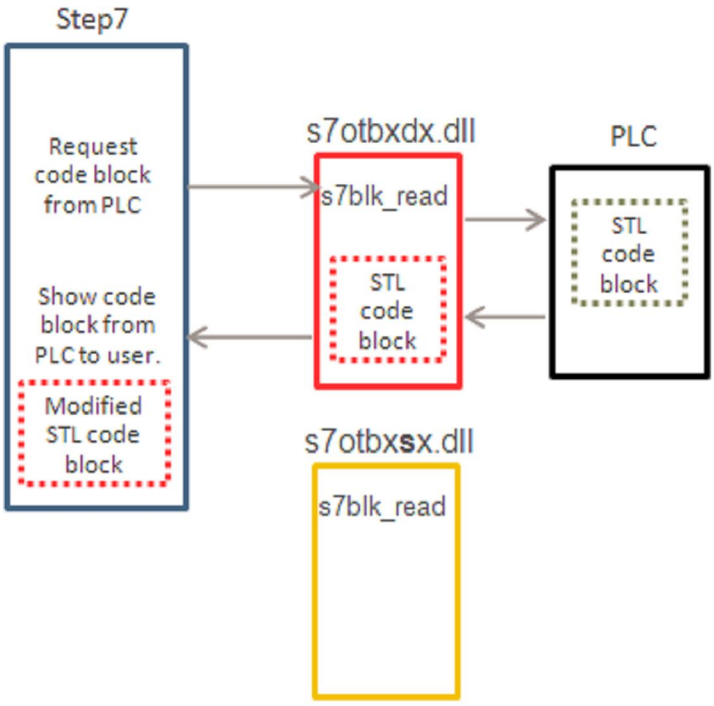
A PLC eléréséhez egy speciális szoftver szükséges, melynek telepítésével lehet a PLC-hez kapcsolódni egy adatkábel segítségével. A Stuxnet valójában ezt a szoftvert, azaz a Siemens Simatic WinCC/Step7-et támadta meg. A Step7 fejlesztői környezete képes rekonfigurálni a PLC-t, feltölteni a programot, képes nyomon követni a végrehajtást és ellenőrizni memóriát. A konfigurált és beprogramozott PLC-t ezt követően lekapcsolják a Windows gépről, hiszen az már a továbbiakban képes önállóan működni.

A PLC konfigurálást és programozást a 2. ábrán követhetjük végig.

2. ábra. A PLC konfigurálása és programozása [2]

A Simatic s7otbxdx.dll-je felel a PLC blokk cseréért a programozó eszköz és a PLC között. A Stuxnet ezt a dll-t előbb átnevezte s7otbxsx.dll-re majd feltöltötte a saját s7otbxdx.dll-jét. A helyettesítésnek köszönhetően képes volt monitorozni a PLC-re írt és onnan olvasott blokkokat. A Step7 program az s7otbxdx.dll különböző rutinjait pl. az s7blk_read rutint hívja, ha el akarja érni a PLC-t. A féreg képes volt megfertőzni a PLC-t saját blokkjainak rátelepítésével, vagy létező blokkok helyettesítésével, megfertőzésével. A folyamatot a 3. ábra mutatja.

A 109 különböző kérés lekezelése során 93 esetben a fertőzött dll egyszerűen továbbítja a kérést az eredeti, most már s7otbxsx.dll-nek nevezett komponensnek. A maradék 16 az, amit nem továbbít, hanem megszakít, és így képes módosítani a PLC által küldött adatokat anélkül, hogy a PLC-t kezelő operátor észlelné az eltérést. A Stuxnet ezeken a rutinokon keresztül éri el azt is, hogy elrejtse a rosszindulatú kódot a PLC-n. [2] A Stuxnet az első ismert féreg, mely nem csak a Windows-on rejti el magát, de a PLC-n is. [3]



3. ábra. A PLC konfigurálása és programozása fertőzött s7otbxdx.dll-el. [2]

A STUXNET KÉSZÍTŐI ÉS A FÉREG CÉLPONTJAI

Előző írásunkban már utaltunk rá, hogy 2011 januárjában a New York Times (NYT) adott elsőként hivatalosan hírt a Stuxnet eredetéről. Azóta többször és több helyen is megjelent, hogy a Stuxnet mögött Izrael áll, természetesen nem kevés USA segítséggel. [1] [8]

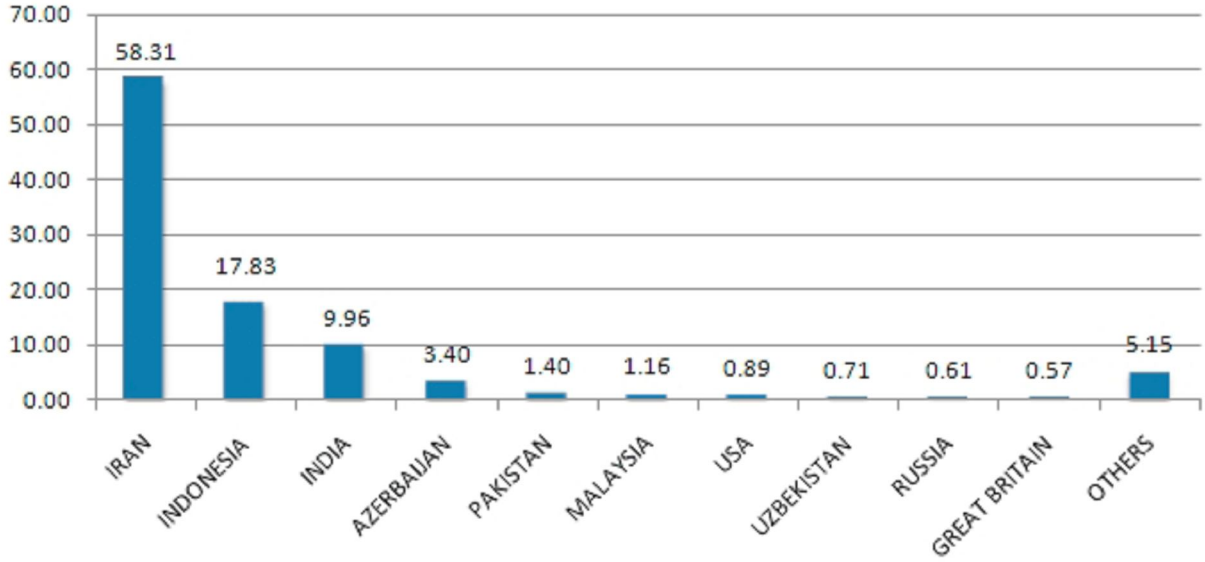
A Stuxnet előzőekben ismertetett működése mellett természetesen a kulcskérdés, hogy pontosan milyen ipari vezérlőegységekre is specializálódott a féreg. A Symantec és a Dutch Profibus szakemberei szerint ezek egy finnországi és egy iráni gyártó által készített frekvenciakonverterek voltak, melyeket villanymotorok sebességvezérléséhez használnak. A Stuxnet csak akkor módosítja a működést, ha bizonyos ideig extrém magas, (807-1210 Hz) frekvenciát adnak kimenetként. Egyik jellemző felhasználási terület a gázcentrifugák meghajtása, melyeket radioaktív izotópok szétválasztásához használnak. A közbeavatkozás ráadásul az uránfeldolgozás korai szakaszára esik, ami egybevág Irán első atomerőművének jelenlegi életszakaszával. [4]

Mindezen tények rendkívül figyelemre méltóak, hiszen ahogy korábban is utaltunk rá, bár nincs egyértelmű bizonyított tény a célpontokra, mégis arra utalnak az ismertetett adatok, hogy a Stuxnet elsődleges céljai (iráni) atomlétesítmények voltak.

Ugyanakkor érdemes végignézni, hogy a féreg, milyen úton is jutott el a végső céljáig. Egyes nemrégen megjelent elemzések szerint, a Stuxnet, és így a mögötte álló támadók öt konkrét iráni szervezetet céloztak, melyekről feltételezték, hogy kapcsolatban állnak az atomlétesítményekkel.

A Stuxnet 2010 nyarán került az újságok címoldalaira, de számos bizonyítékot tártak fel a különböző vizsgálatok, amelyek arra engednek következtetni, hogy a féreg már 2009-ben is fertőzött. A támadás három – viszonylag jól elkülöníthető hullámban – zajlott le. Első körben öt célpontot egymással párhuzamosan támadott. Ezek a támadások esetenként több hónapig is tartottak, mígnem 2010 nyarán nyilvánosságra került maga a féreg. A Stuxnet ezekből a szervezetekből kezdett el továbbterjedni más szervezetekre, hogy végül elérje végső célját, az eddigi legvalószínűbb információk szerint, az iráni urándúsító centrifugákat. [2]

Ugyanakkor érdemes további pillantást vetni a Symantec elemzésére. Az elemzés során, amely a Stuxnet terjedését hivatott felfedni, a cég 40 ezer olyan IP címet talált, amelyek 155 országban találhatóak, és amelyek valamilyen módon a Stuxnettel fertőzöttek . Az Iránt, mint célpontot feltételező elméteket támasztja alá ez az elemzés is, hiszen a felfedett IP címek 60%-a Iránban található. A 4. ábra mutatja be a Symantec országokra lebontott elemzését. . [2]



4. ábra. A Stuxnettel fertőzött gépek IP címei országokra lebontva. [4]

ÚJ TERÜLETEK?

Az elmúlt évek számítógépes, illetve számítógép-hálózatokkal szemben bekövetkezett támadásai új trendet mutattak a korábbi időszakhoz képest. Az elmúlt időszakban a támadók rájöttek, hogy a felhasználók számítógépei, az azokon futó alkalmazások sokkal gyengébben védettek, mint a nagy – pl. banki, vagy pénzügyi szolgáltatók – rendszerei. Ennek megfelelően a támadások zömmel ezeket a számítógépeket és az ezeket futó alkalmazásokat érték. Ezeken keresztül jutottak olyan adatokhoz, amelyek a nagyobb rendszerekbe való behatolásokat lehetővé tették. Az adatlopás, ideértve a social engineeringet is, sokkal kifizetődőbbé vált, mint az említett nagy rendszerek közvetlen támadása. Ezzel párhuzamosan a támadások célja az esetek nagy többségében anyagi haszonszerzés volt. Ezek után érte igencsak váratlanul a szakmát és a közvéleményt is a Stuxnet megjelenése.

A féreg rávilágított, hogy számos olyan kritikus infrastruktúránk van, amely sérülékeny információs (informatikai) rendszereket használ. Ezáltal a kritikus infrastruktúrák egyik legkritikusabb része maga az infrastruktúrát irányító, vagy az azt ellenőrző és vezérlő információs rendszer.

Ilyen kritikus információs infrastruktúra lehet (a teljesség igénye nélkül):

- energiaellátás rendszerirányítása;
- közúti-, vasúti-, légi közlekedés irányítása;
- élelmiszergyártás irányítása;
- gyógyszergyártás irányító, ellenőrző rendszere;
- vízellátás irányítása;
- ipari termelés rendszerirányítása.

Ezek közül a kritikus rendszerek közül vitathatatlanul az egyik legfontosabb az energiatermelő, szállító, tároló és ellátó rendszerek rendszerirányítása. Ráadásul az itt felsorolt rendszerek közül több is valamilyen SCADA-t használ. A Stuxnet láz elülte után már egyértelműen nem maga a féreg a legérdekesebb, hanem az általa támadott SCADA rendszerek. Az elmúlt néhány hónapban számos olyan jelentés látott napvilágot, amely magára a SCADA rendszerekben lévő sérülékenységek jelentett veszélyeire hívja fel a figyelmet. 2011 márciusában elemzők 52, a SCADA rendszereket érintő sérülékenységet jelentettek, amelyek mindegyike most került napvilágra.

Az energiaszektor mellett talán az egyik legneuralgikusabb terület, amelyre pont a Stuxnet jelenség hívta fel a figyelmet az a polgári légiközlekedés irányítása. Amennyiben itt egy Stuxnethez hasonló féreg, vagy egyéb malware hatására – akár időszakos – működésképtelenség, vagy működési zavar támad, akkor már nem csak az ellopott adatok vagy információk anyagi eszközökben mérhető káraival, hanem emberéletekben mérhető hatalmas károkkal is számolnunk kell.

Mindezekkel összefüggésben egyre több jel mutat arra, hogy a SCADA rendszereknek gyakran nagyobb a kockázata, mint egy átlagos informatikai rendszernek, mert ezek ma még mindig össze vannak kapcsolva régebbi operációs rendszereket (pl.: Windows 95) futtató gépekkel. Ezekhez az operációs rendszerekhez pedig ma már nincsenek sem automatikus sem kézi frissítésű szervizcsomagok. [7]

KOMPLEX INFORMÁCIÓBIZTONSÁG, MINT A LEHETSÉGES VÉDELEM

Kérdések

Ki a felelős, hogy a Stuxnet, illetve az ehhez hasonló jelenségek bekövetkezhetnek? Ki a felelős a védekezésért?

Az első ránézésre rendkívül egyszerűnek tűnnek a kérdések, hiszen a válasz nagyon gyakran az, hogy természetesen mindazok a vállalatok és szervezetek, amelyek ilyen – a Stuxnet esetében ipari vezérlő – eszközöket használnak.

Azonban ha csak egy kicsit is mélyebbre tekintünk, akkor rendkívül összetett és bonyolult kérdésekkel találjuk magunkat szemben.

Napjainkban a Stuxnet által is érintett ipari vállalatok szerves részei a már említett kritikus infrastruktúráknak, ezek vezérlő rendszerei pedig részei lehetnek a kritikus információs infrastruktúráknak. Ezek a között a kritikus rendszerek között pedig olyan nagyfokú interdependenciát, azaz egymástól való kölcsönös függőséget figyelhetünk meg, amelyek még tovább bonyolítják – az egyébként első ránézésre valóban rendkívül egyszerű – kérdések megválaszolását.

Természetesen jelen írás nem tud választ adni a kritikus infrastruktúrák, illetve a kritikus információs infrastruktúrák védelmének problémájára. Ez nem is volt célja jelen írásnak, hiszen születtek már itthon is átfogó művek, amelyek az említett rendszerek azonosításának módszertanától kezdve a védelem lehetséges megvalósításáig számos ezzel a kérdéssel összefüggő területet kutattak. [5]

Komplex információbiztonság

A fenti kérdésekre az egyik válasz a komplex információbiztonság értelmezése és megvalósítása lehet. Korábban utaltunk már rá, hogy még napjainkban is nagyon gyakran azonosítják az információbiztonságot úgy, mint kizárólag informatikai kérdést. Arra, hogy ez hibás megközelítés, pont a Stuxnet a legjobb példa. A minden területre, azaz a fizikai-, személyi-, dokumentum- (vagy adminisztratív), illetve az elektronikus biztonság területeire egyforma és megfelelő hangsúlyt fektető védelem, mint tevékenység, vagy tevékenységek sorozata érheti csak el azt, hogy rendszereinket biztonságosnak tekinthetjük. (Természetesen a kockázatokkal arányos védelem megvalósítása a cél, és azt is ki kell jelenteni, hogy nem létezik 100 %-os biztonság). A Stuxnet, mint példa azért illik ide tökéletesen, mert bár alapvetően egy zseniálisan megírt szoftverről van szó, mégis terjedéséhez kellettek azok a személyi, fizikai és adminisztratív területeken meglévő hiányosságok, amelyek cikkünk első részében már elemeztünk. [1]

Az elmúlt évtizedekben pedig születtek olyan ajánlások, amelyek a komplex információbiztonságot, illetve ennek egyes elemeit hivatottak szabályozni. Néhány ezek közül az ajánlások közül (a teljesség igénye nélkül):

- CC (Common Criteria for Information Technology Security Evaluation), azaz közös követelmények az információtechnológia biztonságának fejlesztéséhez: az informatikai termékek gyártóinak nyújt támogatást. Részletes és megbízható követelményeket, valamint eljárásokat biztosít az informatikai eszközök biztonsági minősítésére. A CC egységes, a megvalósítás módjától független követelményeket határoz meg, és egységes kiértékelési módszertant ad az informatikai rendszerek, termékek informatikai biztonsági értékeléséhez, tanúsításához. Meghatározza az informatikai rendszerek biztonsági követelményeinek többszintű kategóriákból álló katalógusát. [10]

- COBIT (Control Objectives for Information and Related Technology), azaz Informatikai Irányítási és Ellenőrzési Módszertan: nemzetközi módszertan az informatikai alkalmazások hatékony üzleti felhasználására. A vállalat vagy szervezet vezetése részére segítséget nyújt egy kontrollrendszer felállításához és fenntartásához, valamint a változó körülmények között a kockázatok megfelelő kezeléshez.

- ITIL (Information Technology Infrastructure Library), azaz Informatikai Szolgáltatás Módszertana: Költséghatékony, jó minőségű, informatikai szolgáltatások támogatására fejlesztették ki, mely végigkíséri a teljes életciklust, beleértve a tervezés, a bevezetés, a működtetés és az újabb szolgáltatások bevezetésének szakaszait. A legjobb gyakorlati módszertanok, valamint az informatikai iparágban elfogadott eljárások gyűjteményét foglalja magába. [11]

- ISO/IEC 27001 (Information technology. Security techniques. Information security management systems. Requirements), azaz Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények[1]: az információbiztonsági irányítási rendszer (ISMS - Information Security Management System) kialakításához, megvalósításához, működtetéséhez, figyelemmel kíséréséhez, átvizsgálásához, fenntartásához és fejlesztéséhez szükséges követelményeket írja le. [12]

Természetesen ezek közül az ajánlások, illetve az ebben foglaltak közül annyi valósul meg – azaz annyit ér maga a szabályozás egy adott szervezetnél –, amennyit be is tartanak ezekből.

A kormányzat szerepe [13]

Mindenképpen fel kell hívni a figyelmet két további tényezőre a Stuxnet ügy kapcsán. Az egyik az állami szerepvállalás mind a védelemben, mind a cyber térben történő egyéb (támadó) tevékenységek kapcsán. Ezzel összefüggésben a *Ki a felelős?* kérdés abban a tekintetben is helyénvaló és megválaszolandó, hogy, amennyiben adott országok kormányai állnak a Stuxnet mögött, akkor hol van az ő felelősségük? A Stuxnet nyilvánosságra kerülése után egyre-másra kapta fel a szakmai és a világsajtó is azokat a híreket, amelyek a féreg illetéktelen kezekbe kerüléséről szóltak. Ennek megfelelően a kormányok részéről ez egy hallatlanul veszélyes tevékenység, hiszen lehet olyan terrorista szervezet, illetve egyéb politikai, vallási vagy ideológiai alapon szerveződő csoport, amely anyagi lehetőségek birtokában – a piacon egyébként már megjelent Stuxnetet, vagy az ahhoz hasonló programokat – meg tudja vásárolni, akkor az állam a saját farkába harapó kígyóhoz hasonló helyzetbe kerül. [6]

Természetesen a kormányzat szerepe elsősorban a védekezésben, a védelemre való felkészülésben, a védelem koordinálásban kell, hogy tetten érhető legyen.

Mindezek alapján a védelmének területén a következő kormányzati feladatok válnak szükségessé a már említett neuralgikus, kritikus infrastruktúra és kritikus információs infrastruktúra védelem területén hazánkban:

- meg kell határozni a kritikus információs infrastruktúra pontos fogalmát;
- az ágazati kritikus infrastruktúrák mellett meg kell határozni azokat az elemeket, amelyek kritikus információs infrastruktúraként jelentkeznek;

[1] A magyar fordítás a szabvány magyar változatában, azaz az MSZ ISO/IEC 27001-ből származik.

- létre kell hozni egy olyan központi szervezetet, amely vészhelyzet esetén képes mind a kritikus infrastruktúra, mind a kritikus információs infrastruktúra területeken a védelmet koordinálni;
- a központi szervezetnek hatósági jogköröket kell adni az információbiztonság kialakítása, fenntartás és ellenőrzése területeken (ez a jogkör nem csak a közigazgatási és állami szervezetekre, hanem a magánszektor vonatkozásában is meg kell, hogy legyen);
- fel kell tárni a hazai a kritikus információs infrastruktúrákat fenyegető konkrét veszélyeket, függetlenül attól, hogy az adott rendszert állami, vagy magántulajdonosi körben lévő szervezet üzemelteti;
- elemezni kell, hogy a feltárt veszélyforrások közül, melyik és milyen mértékben érinti a meghatározott kritikus információs infrastruktúrákat, illetve azok egyes elemeit;
- konkrét szimulációkat kell tervezni és szervezni, nem csak hazai, hanem nemzetközi együttműködésben az információs infrastruktúrák körében, amelyek alapján fel lehet tárni azokat a pontokat, kulcsfontosságú elemeket, amelyek a gazdaság, a társadalom és a kormányzat szempontjából létfontosságúak, valamint ezekkel választ lehet kapni a védelem hatékonyságára és a védekezésben részt vevő szervezetek közötti együttműködés milyenségére, valamint a koordináció esetleges hiányaira;
- meg kell határozni, és fel kell térképezni a hazai információs infrastruktúrák egymásra, illetve a kritikus infrastruktúrákra gyakorolt közvetlen és közvetett hatásait;
- meg kell határozni, és fel kell térképezni a hazai információs infrastruktúrák környező országok infrastruktúráira gyakorolt hatását;
- a kormányzati koordináló szerv feladatait és résztvevőit ki kell egészíteni a kritikus információs infrastruktúra tulajdonosainak, üzemeltetőinek, illetve a hazai CERT-ek (valamint a Nemzeti Hálózatbiztonsági Központ) képviselőivel;
- meg kell vizsgálni, hogy alkalmas-e egy esetleges támadás esetén a hazai információs és kommunikációs infrastruktúra a riasztás és a jelzés, majd a vészhelyzeti kommunikáció menedzselésére;
- a tudatos és biztonságos internet-, illetve infokommunikációs eszközhasználatának oktatása, az erre való lakossági felkészítés az eddiginél hatékonyabb és nagyobb szerepet kell, hogy kapjon.

Összefoglalás

Írásunk két részében bemutattuk a Stuxnet nevű féreg működését és terjedését. Válaszokat kerestünk arra, hogy ki állhat a féreg mögött, illetve, hogy mi is lehetett az igazi célja a támadónak. A nemzetközi hírekből leszűrhető összegzett következtetés az, hogy egy rendkívül jól megírt, nagyon sok új, eddig nem ismert sérülékenységet kihasználó olyan rosszindulatú programról beszélünk, amely ha nem is forradalmasította a területet, mindenképpen felhívta a figyelmet a kritikus infrastruktúráink illetve kritikus információs infrastruktúráinkra. Mindezidáig nem, vagy csak elvétve hallhattunk híreket arról, hogy egy rosszindulatú program képes fizikai károkat okozni. A Stuxnet után már kétségünk sem lehet erről, hiszen az iráni izotópcentrifugák meghibásodása kétséget sem hagy afelől, hogy ezen a területen is valami új kezdődött.

Mindezek arra is felhívják a figyelmet, hogy ezen a területen sem elegendő csak egy nézőpontból szemlélni a biztonság kérdését. A komplex, minden területre kiterjedő védelemre van szükség, a melyben a kormányzatnak is igen komolyan ki kell vennie a mag részét a fent ismertetett lehetséges módokon.

Felhasznált irodalom

[1] Kovács László - Sipos Marianna: A Stuxnet és ami mögötte van: Tények és a cyberháború hajnala. in: Hadmérnök 2010/4.

[2] Falliere, N. – Murchu, L. O. – Chien, E.: W32. Stuxnet Dossier, Symantec Security Response Version 1.3 (February 2011). http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (2010. március 1.)

[3] W32.Stuxnet, Symantec Security Response, http://www.symantec.com/business/security_response/writeup.jsp?docid=2010-071400-3123-99&tabid=2 (2010. március 1.)

[4] Mit buherál a Stuxnet? http://buhera.blog.hu/2010/11/14/mit_buheral_a_stuxnet (2010. március 1.)

[5] Haig Zsolt - Hajnal Béla - Kovács László - Muha Lajos - Sik Zoltán Nándor: A kritikus információs infrastruktúrák meghatározásának módszertana. Tanulmány a Puskás Tivadar Közalapítvány részére (2009)

[6] Kiley, Sam: Super Virus a Target for Cyber Terrorists. http://news.sky.com/skynews/Home/World-News/Stuxnet-Worm-Virus-Targeted-At-Irans-Nuclear-Plant-Is-In-Hands-Of-Bad-Guys-Sky-News-Sources-Say (2010. március 1.)

[7] Muncaster, Phil: Stuxnet-like attacks beckon as 50 new Scada threats discovered. http://www.v3.co.uk/v3-uk/news/2045556/stuxnet-attacks-beckon-scada-threats-discovered (2010. március 1.)

[8] W. J. Broad, J. Markoff, D. E. Sanger: Israeli Test on Worm Called Crucial in Iran Nuclear Delay. In: New York Times, 2011. január 15. http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1&scp=2&sq=stuxnet&st=cse (2010. március 1.)

[9] Kim Zetter: Attack Code for SCADA Vulnerabilities Released Online. in: WIRED, 2011. március 22. http://www.wired.com/threatlevel/2011/03/scada-vulnerabilities (2010. március 1.)

[10] http://www.commoncriteriaportal.org (2010. március 1.)

[11] http://www.itil-officialsite.com/AboutITIL/WhatisITIL.aspx (2010. március 1.)

[12] ISO/IEC 27001:2005

[13] Kovács László: Az információs terrorizmus elleni tevékenység kormányzati feladatai. in: Hadmérnök, 2008/2. http://www.hadmernok.hu/archivum/2008/2/2008_2_kovacsl.pdf (2010. március 1.)

Jelen írás a Magyar Tudományos Akadémia Bolyai János Kutatási Ösztöndíjának támogatásával készült.