Pavel Bucka, Maros Gonos

Bezpečnosť priemyselných sietí v prostredí moderných kybernetických hrozieb

Acta Scientifica Academiae Ostroviensis. Sectio A, Nauki Humanistyczne, Społeczne i Techniczne 1, 101-128

2013

Pavel BUČKA[1], Maroš GONOS[2]

Bezpečnosť priemyselných sietí v prostredí moderných kybernetických hrozieb

Industrial network security in advanced persistent threat environment

Abstract

Industrial networks are used to control processes and manufacturing operations of varying scope. Their mission is to provide automatic transfer of information within the structure of distributed control systems. To achieve this industrial networks and systems have to possess ability to withstand wide range of internal and external threats. The consequences of cyber-attacks can potentially be varied from benign traffic disruption, through interventions in the operation (the production process), to deliberate sabotage to cause maximum damage. For this reason, it is important to constantly review environment in which they operate as well as their security.

Keywords: security, industrial networks, cyber-attack, advanced persistent threat, cyber war.

Bezpieczeństwo sieci przemysłowych w środowisku stałego zagrożenia

Streszczenie

Sieci przemysłowe są używane do kontrolowania procesów i operacji produkcyjnych różnego zakresu. Ich celem jest dostarczanie automatycznego przepływu informacji w obrębie systemów sterowania. Aby to osiągnąć sieci i systemy przemysłowe muszą mieć możliwość przeciwstawienia się dużej ilości zagrożeń zewnętrznych i wewnętrznych. Konsekwencje cyber-ataków mogą zaczynać się od łagodnego zakłócenia ruchu, poprzez interwencje w pracy (w procesie produkcji), aż do sabotażu powodującego największe szkody.

Z tego powodu ważne jest, aby stale kontrolować warunki, w których działają jak również ich bezpieczeństwo.

Słowa kluczowe: bezpieczeństwo, sieci przemysłowe, cyber – ataki, stan stałego zagrożenia, cyber wojna

[1] doc. Ing. Pavel BUČKA, CSc. Katedra bezpečnosti a obrany, Akadémia ozbrojených síl gen. M. R. Štefánika, 031 06 Liptovský Mikuláš 6, Slovensko, Email: pavel.bucka@aos.sk

[2] Ing. Maroš GONOS, Ministerstvo obrany SR, Kutuzovova 8, 832 47 Bratislava, Slovensko, Email: maros.gonos@mil.sk

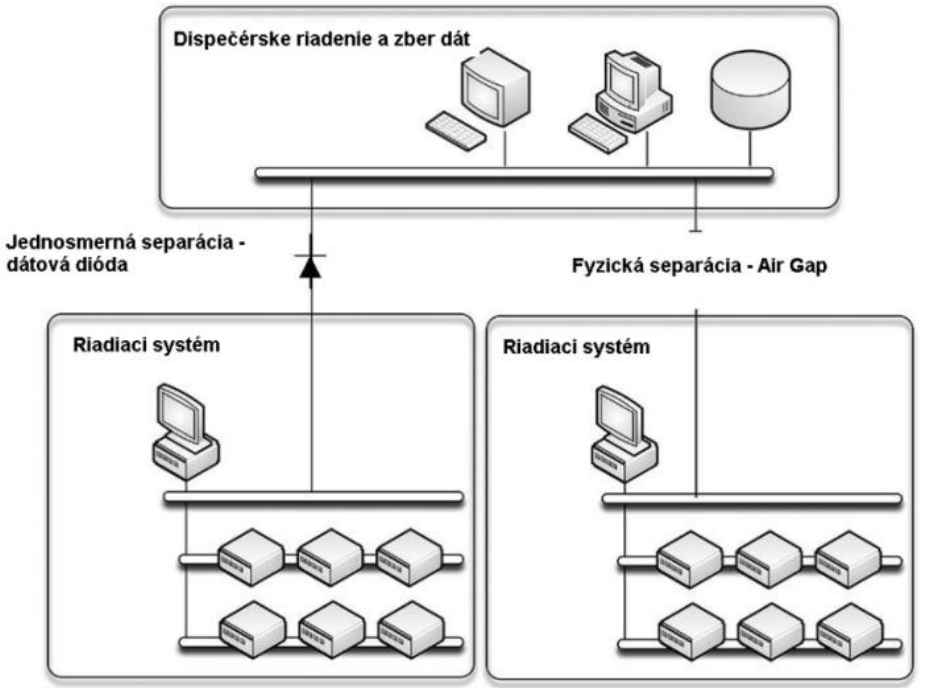
ÚVOD

Problematika ochrany priemyselných sietí je v mnohých ohľadoch podobná problematike ochrany štandardných firemných počítačových sietí, no prináša so sebou niekoľko špecifických otázok. Keďže priemyselné systémy sú budované s dôrazom na čo najvyššiu spoľahlivosť a životnosť, môžu sa stať ľahkým cieľom pre útočníka. Od priemyselných riadiacich systémov sa často očakáva nepretržitá prevádzka počas dlhých časových úsekov (mesiace, roky) a celková životnosť merateľná v dekádach. Na druhej strane útočníci majú zväčša možnosť použitia najnovších techník a technológií, ktoré môžu kedykoľvek použiť. Bezpečnostné opatrenia a postupy používané pri ochrane priemyselných riadiacich systémov často zaostávajú, čoho príčinou je zväčša skutočnosť, že použité riadiace systémy sú podstatne staršie ako moderné sieťové infraštruktúry a vždy boli chránené skôr fyzicky než digitálne. Z dôvodu vysokej dôležitosti priemyselných sietí a potenciálne devastujúcich dôsledkov možného útoku na ne, permanentne vyvstáva potreba zavádzania moderných metód ich ochrany. Známe príklady priemyselnej kybernetickej sabotáže z posledných rokov sú potvrdením toho, že priemyselné siete sú cieľom útočníkov a títo v súčasnosti využívajú vysoko sofistikované a cielené formy útokov.

1. Dôležitosť ochrany priemyselných sietí

Potreba neustáleho zdokonaľovania ochrany priemyselných sietí nesmie byť v súčasnosti podceňovaná. Mnohé priemyselné systémy boli vytvorené na báze starších zariadení a protokolov napr. *AppleTalk, DECnet, Novell IPX,* ktoré boli prispôsobené na prácu v moderných sieťach. Pred rozšírením internetového prepojenia, webových aplikácií a výrobných (obchodných) systémov využívajúcich informácie v reálnom čase, boli priemyselné systémy budované s dôrazom na spoľahlivosť. Ich fyzická bezpečnosť bola vždy predmetom záujmu, no v prípade informačnej bezpečnosti už tomu tak nebolo,

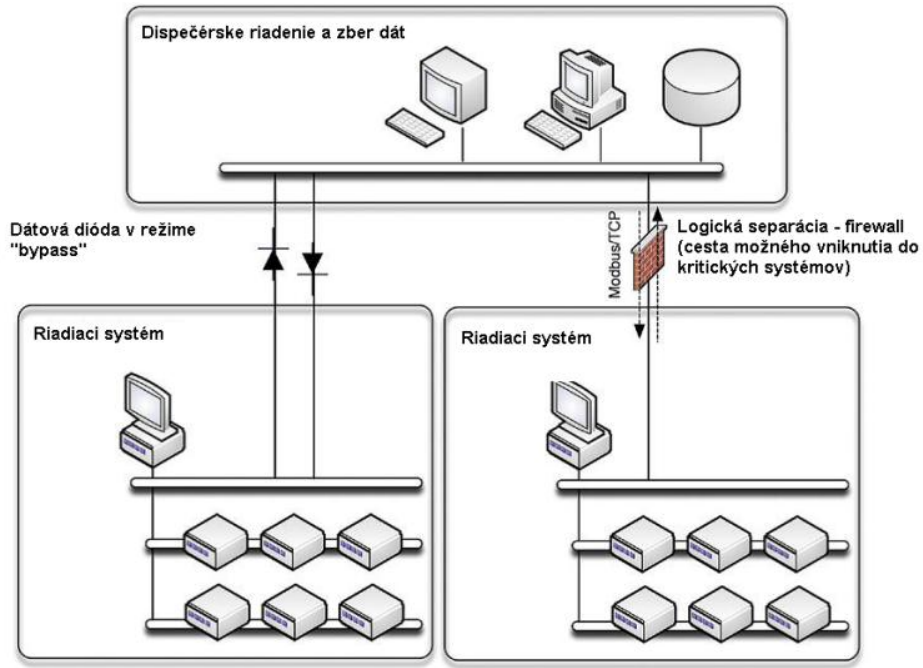
pretože riadiace systémy boli fyzicky odseparované (*Physical Air Gap*) – teda nemali spoločný žiadny (elektronický či iný) prvok, spájajúci ich s okolím (obrázok 1).



Obrázok 1: Fyzická separácia riadiaceho systému (*Air Gap*), (1, s. 32)

V ideálnom prípade by aj vo svete digitálnej komunikácie mala fyzická separácia existovať. V skutočnosti tomu však tak nie je. S postupným zavádzaním a rozvojom priemyselných sietí vo výrobnej sfére začala rovnako narastať aj potreba zdieľania informácií v reálnom čase. Keďže požadované informácie pochádzali práve „z poza tohto priestoru separácie“, bolo potrebné nájsť vhodné prostriedky, ktorými by sa tento priestor dal prekonať. Týmto prostriedkom sa stal firewall, blokujúci všetky dátové toky okrem tých, ktoré boli nevyhnutné pre zvýšenie efektivity výrobných a obchodných operácií. Problémom však zostalo, že akokoľvek dobre mienené a ospravedlnené tieto

kroky boli, fyzická separácia v podstate prestala existovať a vznikla cesta možného vniknutia do kritických systémov (obrázok 2).



Obrázok 2: Realita súčasnej separácie riadiaceho systému (1, s. 33)

Príklad: *Americká konzultačná firma Red Tiger Security, pôsobiaca v oblasti bezpečnosti priemyselných sietí a kritickej infraštruktúry prezentovala v roku 2010 závery svojho výskumu a zhodnotila stav bezpečnosti priemyselných sietí v USA. Testy prieniku do 100 priemyselných zariadení výroby elektrickej energie zaznamenali 38 000 bezpečnostných rizík a zraniteľností. Spoločnosť Red Tiger Security bola neskôr požiadaná americkým Ministerstvom pre vnútornú bezpečnosť (Department of Homeland Security) k spracovaniu analýzy získaných dát, zisteniu základných smerov možných útokov a celkovo pomôcť zvýšiť mieru bezpečnosti kritickej infraštruktúry proti kybernetickým útokom. Výsledky analýzy naznačovali, že miera bezpečnosti priemyselných sietí v skúmaných zariadeniach značne zaostávala za ostatnými odvetviami*

priemyslu. Priemerný čas od verejného odhalenia existencie zraniteľného miesta do času jeho objavenia v riadiacich systémoch predstavoval 331 dní. V niektorých prípadoch bol tento čas viac ako 1100 dní (2, s. 13).

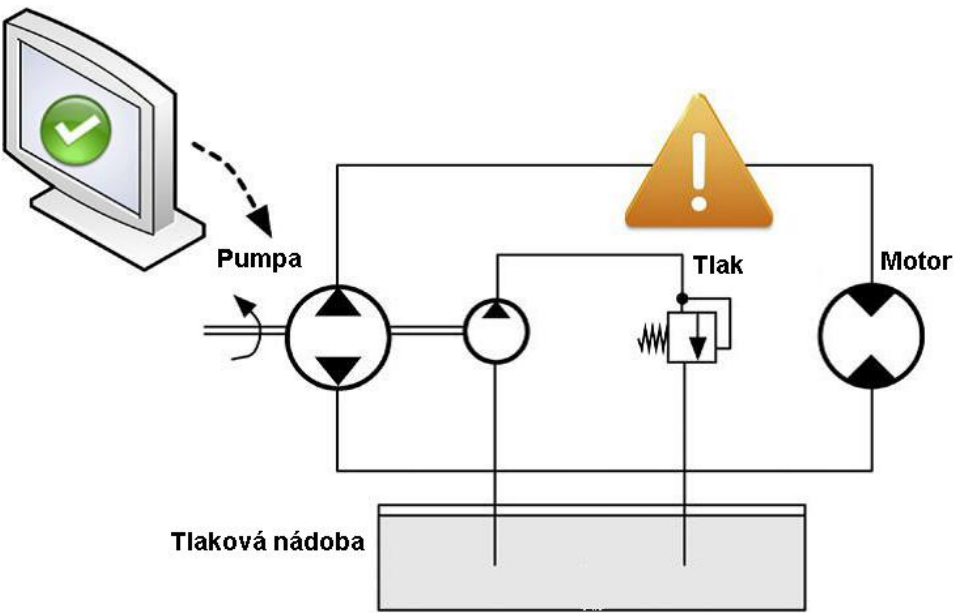
Uvedený príklad poukazuje na to, že reálne existujú zraniteľné miesta, ktoré môžu útočníci využiť na prístup do priemyselných sietí a kritickej infraštruktúry. Dostatočne dlhá verejná znalosť zraniteľností, ako to bolo napr. uvedené v príklade vyššie, určite poskytuje dostatok času na ich testovanie útočníkmi napr. open sourcovým softvérom ako typu *Backtrack* (3), alebo *Metasploit* (4), pomocou ktorých sa dajú zistiť možnosti využitia zraniteľností a penetrácie do siete.

Nemalo by byť prekvapením, že niektoré zraniteľné miesta riadiacich systémov sú všeobecne známe. Aplikácia bezpečnostných záplat v priemyselných riadiacich systémoch je veľmi náročná, čoho hlavnou príčinou je samotný spôsob ich návrhu a štruktúra. Úmyselne limitovaným (či skôr eliminovaným) prístupom do vonkajších sietí a internetu, už aj samotné získanie bezpečnostných záplat môže predstavovať značnú komplikáciu. Keďže spoľahlivosť je v tomto prípade prvoradá, aplikácia bezpečnostných záplat nie je jednoduchá a značne obmedzená na čas plánovanej údržby, či odstávky zariadenia. Výsledkom je, že môžu neustále existovať časti systému, kde ešte k aplikácii bezpečnostných záplat nedošlo.

2. Následky útokov na priemyselné siete

Priemyselné siete sa využívajú na riadenie procesov a výrobných operácií rôzneho rozsahu. Výsledkom úspešnej penetrácie siete riadiaceho systému môže byť priame ovplyvňovanie týchto procesov a operácií neautorizovanými osobami. Následky môžu byť potenciálne rôznorodé, od neškodných narušení prevádzky, cez zásahy do samotnej prevádzky (výrobného procesu), až po premyslenú sabotáž s cieľom spôsobiť čo najväčšie škody. Napríklad (pozri obr. 3) manipulácia spätnej väzby konkrétnych procesov môže

spôsobiť nárast tlaku v tlakovej nádobe nad hranicu bezpečnej prevádzky. Kybernetická sabotáž môže takto skončiť dokonca aj zraneniami osôb, obeťami na životoch a veľkými škodami na infraštruktúre (explózia) so súčasným zastavením poskytovaných služieb (napr. elektrina, voda a pod.).



Obrázok 3: Narušenie riadiaceho procesu môže mať za následok vážne poruchy (1, s. 34)

2.1 Zabezpečovacie systémy

V rámci prevencie pred haváriami sa v priemysle a v rámci priemyselných sietí využívajú rôzne automatizované zabezpečovacie systémy. Mnohé z nich však využívajú rovnaké komunikačné a riadiace protokoly, ako používajú riadiace procesy priemyselnej siete. V prípade niektorých zbernicových aplikácií dokonca zabezpečovacie systémy a riadiace procesy priemyselnej siete využívajú aj totožné fyzické médium.

Aj keď je použitie ochranných prvkov absolútnou nevyhnutnosťou, často práve oni stoja za znížením požiadaviek na bezpečnosť priemyselných

sietí. Súčasný výskum v oblasti bezpečnosti priemyselných sietí na základe simulácií ukazuje, že toto môže mať vážne následky. Simulácie vykonané *Sandia National Laboratories* (USA) ukázali, že jednoduchý až mierne pokročilý útok zo stredu (*Man-in-the-Middle Attack – MITM*), s použitím cielene vyvinutého malwaru (vo svojom scenári sa zamerali na konkrétne predradené procesory) môže byť využitý na zmeny hodnôt v riadiacom systéme a že už útok malého rozsahu na zariadenia produkcie elektrickej energie môže spôsobiť vážne výpadky (1, s. 35).

Oproti tomu, európsky výskumný tím VIKING (*Vital Infrastructure, Networks, Inormation and Control Systems Management*) sa venoval výskumu odlišných hrozieb. V oblasti riadiacich systémov zariadení výroby elektrickej energie, ktoré pracovali v úplne nezávisle na ľudských zásahoch či riadení (*Closed Loop*) iba v rámci logiky systému SCADA (*Supervisory Control and Data Aquisition System* – Dispečérsky riadiaci a informačný systém), sa namiesto snahy o prelomenie prístupu do riadiaceho systému zamerali na možnosti manipulácie vstupných dát systému a možnosti následnej zmeny normálnych riadiacich procesov.

2.2 Následky úspešných kybernetických útokov

Úspešný kybernetický útok na priemyselnú sieť môže súčasne:

- spôsobiť oneskorenie, zablokovať, alebo zmeniť konkrétny proces a spôsobiť tak výpadok prevádzky, výroby a pod.;
- spôsobiť oneskorenie, zablokovať, alebo zmeniť informácie súvisiace s konkrétnym procesom a týmto zabrániť prevádzkovateľovi zariadenia získať informácie o reálnej prevádzke, či výrobe dôležité pre následné napr. obchodné operácie.

Výsledkom môžu byť pre prevádzkovateľa napr. pokuty za nedodržanie regulačných pravidiel, dodávok, finančné dopady zo straty produkčných hodín a pod. Kybernetický útok môže riadiaci systém postihnúť v podstate

v akomkoľvek smere a spôsobiť od výpadku prevádzky, vyradenia alebo zmeny nastavenia ochranných prvkov, cez havárie s ohrozením života zamestnancov, alebo okolia, až priame ohrozenie národnej bezpečnosti krajiny. Rozsah následkov kybernetického útoku je značne variabilný a závisí od jeho typu, ako je uvedené v nasledujúcej tabuľke.

Tabuľka 1: Možné následky kybernetického útoku (1; s. 36)

Typ útoku	**Možné následky**
Zmena v systéme, operačnom systéme alebo v konfigurácie aplikácie	• Zavedenie prístupového kanálu (ovládanie, riadenie) do ináč zabezpečeného systému • Potlačenie výstrah a chybových hlásení s cieľom utajiť škodlivé aktivity • Zmeny v nastaveniach, ktoré prinášajú neočakávané a nepredvídateľné reakcie systému, či aplikácie
Zmeny naprogramovania programovateľných logických automatov *(Programmable Logic Controller - PLC)* a iných riadiacich prvkov	• Škody na vybavení a infraštruktúre • Zlyhanie procesov • Strata kontroly nad výrobnými procesmi
Úmyselná dezinformácia operátorov	• Neprimerané reakcie obsluhy na nesprávne informácie, ktoré môžu viesť k zmenám v naprogramovaní riadiacich prvkov • Skrytie škodlivých aktivít, incidentu ako celku, alebo zavedeného škodlivého kódu (napr. rootkit)
Manipulácia ochranných	• Zabránenie spustenia bezpečnostných opatrení

Typ útoku	Možné následky
(zabezpečovacích) systémov a prvkov	a procedúr, čo môže mať potenciálne ničivé dôsledky
Zavedenie škodlivého softvéru (malware)	• Možná iniciácia dodatočných incidentov • Vplyv na produkciu/výrobu, či donútenie prevádzkovateľa k jej zastaveniu z dôvodu vykonania forenznej analýzy, čistenia alebo výmeny útokom zasiahnutých zariadení • Vytvorenie prístupu do systému za účelom vykonania ďalších zásahov, krádeži informácií, či zavedeniu škodlivého softvéru
Krádež informácií	• Krádež citlivých informácií ako napr. chemické vzorce, receptúry, technologické postupy a pod.
Úmyselná zmena informácií	• Citlivé informácie sú úmyselne zmenené za účelom ovplyvnenia vlastností výsledného produktu výroby

3. Príklady útokov v oblasti priemyselných sietí

V poslednej dekáde došlo vo svete k mnohým incidentom, výpadkom, zlyhaniam produkcie a pod., ktorých príčinou boli práve kybernetické útoky. V nasledujúcich príkladoch ktoré uvádzame je možné vidieť akým prechádzajú vývojom.

3.1 Staršie prípady kybernetických útokov

V roku 2001 bol a Austrálii odsúdený muž, ktorý s použitím rádiového vysielača zasahoval do dátových tokov medzi jednotlivými prečerpávacími stanicami odpadových vôd, čo spôsobilo únik viac než 750 000 litrov splašiek do okolitých riek (5).

V roku 2007 *Idaho Natonal Laboratories* (USA) vykonávali experiment s názvom *Aurora Project*, kde úspešne demonštrovali, že obsluha zariadenia môže byť usmrtená za pomoci kybernetického útoku. Výskumníci dokázali cez zraniteľné miesto preniknúť do riadiaceho systému dieselového generátora elektrickej energie, vypnúť ochranné prvky a spôsobiť jeho explóziu. Prípad bol neskôr (2007) pomerne medializovaný televíziou CNN, ktorá poukazovala na nedostatky v oblasti bezpečnosti infraštruktúry výroby elektrickej energie v USA (6).

3.2 Kybernetické útoky na „CENTCOM“ a Operation Aurora

V roku 2008 došlo k infiltrácii do počítačov utajovanej siete veliteľstva americkej armády CENTCOM červom *agent.btz*, ktorý sa rozšíril z prenosného USB disku. Červ *agent.btz* mal schopnosti skenovať počítače a ukladať dáta cestou tzv. zadných vrátok (*backdoor)* odosielať na vzdialený server. Trvalo takmer 14 mesiacov pokiaľ boli počítače zapojené do siete vyčistené (7).

V roku 2009 zasiahli spoločnosti *Google, Symantec, Adobe* a iné útok s názvom *Operation Aurora*, ktorý priniesol na svetlo nový, vysoko sofistikovaný arzenál kybernetických útokov. *Operation Aurora* využila dovtedy neznámu zraniteľnosť (tzv. *Zero-Day Vulnerability*) internetového prehliadača Internet Explorer, na doručenie škodlivého kódu pomocou ktorého sa bolo možné dostať k chráneným informáciám (intelektuálnemu vlastníctvu) v systémoch napadnutých spoločností. Útok *Operation Aurora* bol prelomovým v histórii kybernetických útokov v tom, že predstavoval zmenu v prístupe a to prevažne od útokov typu odmietnutia služby (*Denial of Service Attack*) a zavedenia škodlivých kódov cielených na spôsobenie poškodenia alebo vyradenia siete z prevádzky, k cieleným útokom, vykonaným skryte, s úmyslom neprerušenia prevádzky napadnutých zariadení a nepozorovanou krádežou informácií. Pri útoku boli do napadnutých systémov importované viaceré škodlivé kódy (za asistencie obete – kliknutím na odkaz v prílohe

emailu), ktoré zostávali skryté v systéme a vytvorili sofistikovanú komunikáciu cestou zadných vrátok s riadiacimi servermi umiestnenými v Illinois, Texase a Taiwane (použité boli napr. aj ukradnuté webhostingové zákaznícke účty firmy *Rackspace*). Napadnuté počítače následne začali preskúmavať chránené podnikové intranetové siete, hľadať zraniteľné miesta a zdroje intelektuálneho vlastníctva – špeciálne databázy zdrojových kódov (8, 9).

Hoci popísané útoky na americké veliteľstvo CENTCOM a *Operation Aurora* neboli útokmi na priemyselné siete, sú príkladmi vývoja charekteru moderných kybernetických hrozieb. Inými slovami, špeciálne *Operation Aurora* demonštrovala existenciu tzv. **pokročilých pretrvávajúcich hrozieb** (*Advanced Persistent Threats* – APT), rovnako ako neskoršie prípady demonštrovali existenciu cielených kybernetických zbraní. Tým neskorším prípadom máme na mysli červ *Stuxnet*.

3.3 Stuxnet

Stuxnet, ako nový prostriedok kybernetickej vojny, začal infikovať priemyselné riadiace systémy v roku 2010. Prostriedok kybernetickej vojny preto, lebo akékoľvek špekulácie nad možnosťou že išlo len o cielený kybernetický útok na priemyselnú sieť boli zamietnuté komplexnosťou a sofistikovanou štruktúrou tohto súboru škodlivých kódov. Z tohto pohľadu bol *Stuxnet* „nukleárnou riadenou strelou“ kybernetickej vojny. Nebol len takpovediac výstrelom do prázdna, ale skutočným dôkazom toho, že cestou zložitých a cielených útokov je možné zasiahnuť takmer akúkoľvek priemyselnú sieť. Tu môžeme povedať, že v prípade priemyselných sietí došlo k najhoršiemu scenáru a priemyselná sieť bola reálne napadnutá útokom APT (1; s. 37).

V skutočnosti, *Stuxnet* bol prvýkrát objavený v júni 2009, no širšia diskusia o ňom nezačala skôr ako v lete 2010, kedy americký *Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)* vydal svoje

odporúčanie (10). *Stuxnet* využíval naraz štyri zraniteľnosti typu *Zero-Day*. Na svoje šírenie a infiltráciu využíval prenosné médiá, následne po infikovaní siete vyhľadával programy *SIMATIC WinCC* a *PCS 7* od firmy *Siemens* a potom s použitím defaultných SQL práv infikoval pripojené programovateľné riadiace automaty (PLC) rootkitom cez protokol priemyselnej zbernice (*Profibus*). Ďalej s použitím frekvenčného konvertora hľadal riadiace prvky, ktoré ovládali rýchlosť motorov. Ak našiel riadiaci prvok, ktorý pracoval na frekvencii medzi 800–1200 Hz, začal meniť jeho frekvenčné a následne rýchlosti ovládaných motorov, čím vlastne sabotoval činnosť celého zariadenia (1; s. 37 – 40).

Štruktúra *Stuxnetu* bola vysoko prepracovaná a v podstate bol prvým rootkitom zameraným na priemyselné riadiace systémy. Dokázal sa sám odstrániť s nekompatibilných systémov, zostať dlhodobo nečinný, obísť antivírovú ochranu, samoaktualizovať sa dokonca aj v čase ak sa nedokázal pripojiť na vonkajšiu sieť (čo malo byť základom jeho úspechu, ak by sa mal dostať do skutočne odseparovaného riadiaceho systému), komunikovať *peer-to-peer* v rámci infikovanej siete, manipulovať logické obvody programovateľných riadiacich automatov, efektívne sa maskovať v riadiacom systéme zasielaním falošných informácií obsluhe, využívať systém zložitého kódovania na systémovej úrovni a podpisovať sa certifikátmi ktoré generoval s použitím ukradnutých kľúčov (1; s. 37 – 40).

Hoci na začiatku bolo o tejto novej hrozbe známe len veľmi málo, firma *Siemens* okamžite efektívne reagovala a vydala bezpečnostné varovanie, ako aj nástroj na detekciu a odstránenie *Stuxnetu*. Na jeseň 2010 *Stuxnet*, ako jedinečná hrozba svojho druhu, ktorá cielene napádala riadiace a informačné systémy SCADA, pritiahol pozornosť médií. Následne aj v oblasti jednotlivých odvetví priemyslu došlo k zvýšeniu ostražitosti následkom reálnej existencie vyspelých hrozieb, čo dokonale potvrdilo potrebu zásadného zvýšenia a zdokonalenia bezpečnostných opatrení v oblasti priemyselných sietí.

3.4 Night Dragon, Duqu, Flame

Vo februári 2011 spoločnosť *McAfee* zverejnila objavenie série koordinovaných útokov vedených proti energetickým a petrochemickým spoločnostiam, ktoré nazvala *Night Dragon*. Útoky boli vedené pravdepodobne z oblasti Číny a pravdepodobne začali už v roku 2009. Ich dlhodobý a skrytý charakter bol indikátorom útoku APT. *Night Dragon* bol ďalším príkladom, ako sa útočníci môžu infiltrovať do systémov kritickej infraštruktúry. Aj keď v tomto prípade (na rozdiel od *Stuxnetu*) výsledkom nebola sabotáž, no došlo však ku krádeži citlivých informácií. Úmysel použitia ukradnutých informácií nie je doposiaľ známy, no použité však môžu byť na čokoľvek. Prvým krokom bola infiltrácia do podnikových serverov, cez ktoré sa útočníci dostali do serverov intranetu. S použitím prevažne štandardných a známych hackerských techník, boli dodatočne získané prihlasovacie mená a heslá do jednotlivých pracovných staníc a serverov. Nakoniec *Night Dragon* ustanovil komunikáciu s vlastnými vzdialenými servermi a možnosti vzdialenej správy útočníkmi. Aj keď v tomto prípade priemyselné riadiace systémy neboli útokom zasiahnuté, mohlo však dôjsť k nepovolanému prístupu k informáciám o ich štruktúre, dizajne a prevádzke. Toto by mohli útočníci následne využiť na ďalšie cielenejšie útoky na prevádzku konkrétnych výrobných zariadení (1; s. 41), (11,12,13).

Veľmi podobnými prípadmi ako *Night Dragon* boli škodlivé kódy z posledného obdobia ako *Duqu* (objavený na jeseň 2011) a *Flame* (objavený v roku 2012). Oba škodlivé kódy mali modulárnu štruktúru, pričom niektoré moduly obsahovali známe kódy použité už napr. v *Stuxnete*. V oboch prípadoch sa zatiaľ nepotvrdilo, že by ich cieľom boli priemyselné siete a následná sabotáž riadiacich procesov priemyselnej výroby, ale skôr špionáž, krádež informácií a pod. V každom prípade uvedené útoky APT boli aktmi kybernetickej špionáže

a môžu sa s použitím získaných informácií neskôr vyvinúť do ešte cielenejších útokov (14, 15, 16).

4. Pokročilé pretrvávajúce hrozby a kybernetická vojna

Termíny „pokročilá pretrvávajúca hrozba“ a „kybernetická vojna“ sa často krát zamieňajú medzi sebou. Aj keď môžu mať veľa spoločného, sú dosť rozdielne z hľadiska svojho prvotného úmyslu. V prípade priemyselných sietí sú hrozbou obe, no na to, aby sme boli schopní ich rozlíšiť, je potrebné chápať rozdiely medzi nimi a úmysly, ktoré môžu za nimi stáť. Rozdiel v úmysloch, môže vytvárať rozdiely v cieľoch, na ktoré sa zameriavajú. Metódy použité na krádež intelektuálneho vlastníctva s úmyslom následného získania profitu môžu byť síce totožné s prípadom krádeže intelektuálneho vlastníctva a následného využitia informácií na sabotáž priemyselného zariadenia, no presné zistenie cieľov útoku nám môže poskytnúť pohľad na samotnú povahu útoku. Útok APT môže byť využitý na prvotné získanie informácií o zariadeniach, ich zraniteľnostiach a bezpečnostných dierach (*Zero-Day Vulnerability*), ktoré môžu byť neskôr využité na vývoj škodlivého softvéru (*Zero-Day Exploits*) a na uskutočnenie kybernetickej sabotáže. Je nevyhnutné počítať s tým, že úmysly, metódy a dôsledky kybernetickej vojny budú časom dosahovať vyššiu úroveň. V nasledujúcich tabuľkách sú popísané rozdiely v niektorých aspektoch pokročilých pretrvávajúcich hrozieb a kybernetickej vojny.

Tabuľka 2 Rozdiel medzi pokročilou pretrvávajúcou hrozbou a kybernetickou vojnou (1; s. 42)

Pokročilá pretrvávajúca hrozba (APT)	**Kybernetická vojna**
Často využíva jednoduché exploity na počiatočné infikovanie	Využíva prepracovanejšie a dômyselnejšie nosiče počiatočnej infikácie cieľa

Pokročilá pretrvávajúca hrozba (APT)	**Kybernetická vojna**
Jej prostriedky sú navrhnuté tak, aby neboli detekovateľné	Jej prostriedky sú navrhnuté tak, aby neboli detekovateľné
Komunikuje a prijíma inštrukcie od útočníka cestou vytvoreného utajeného riadiaceho a komunikačného kanálu	Jej prostriedky dokážu pracovať v izolácii a nezávisia na vzdialenom riadení
Má mechanizmy na pokračovanie v činnosti aj po tom, ako bola detegovaná	Jej prostriedky majú mechanizmy na pokračovanie v činnosti aj po tom, ako boli detegované a na následné infikovanie cieľa
Nemá v úmysle narušiť sieťové operácie a sieť samotnú	Jej možným úmyslom môže byť aj narušenie sietí a zariadení

Tabuľka 3 Informačné ciele pokročilých pretrvávajúcich hrozieb a kybernetickej vojny (1; s. 42)

Pokročilá pretrvávajúca hrozba (APT)	**Kybernetická vojna**
Intelektuálne vlastníctvo	
Zdrojové kódy aplikácií	Certifikáty a právomoci
Návrhy aplikácií	Riadiace protokoly
Protokoly	Funkčné diagramy
Patenty	Kódy príkazov riadiaceho systému
Priemyselný dizajn	
Schémy produktov	Schémy riadiaceho systému
Konštrukčné nákresy	Ochranné prvky systému
Výskumné materiály/dokumenty	Zraniteľné miesta riadiaceho systému

Pokročilá pretrvávajúca hrozba (APT)	**Kybernetická vojna**
Chemické vzorce a receptúry	
Farmaceutické receptúry	Farmaceutické receptúry
Chemické vzorce	Farmaceutické bezpečnostné informácie, informácie o alergiách a reakciách na chemické látky
Chemické zlúčeniny	Chemické ohrozenia

4.1 Pokročilé pretrvávajúce hrozby

Pokročilé pretrvávajúce hrozby sa dostali do širšieho povedomia len v posledných rokoch. Veľká publicita škôr popísaných incidentov ako *Aurora Project* a *Stuxnet* zásadne zvýšili pozornosť rôznych komunít pôsobiacich v oblasti informačnej bezpečnosti ako napr. spoločností zaoberajúcich sa výskumom incidentov, regulačných úradov a softvérových výskumných ústavov, čo pomohlo zistiť mnoho o priebehu, zámeroch a spôsoboch vykonania útokov APT. Jedným z rozdielov oproti väčšine predchádzajúcich útokov, bol práve vysoko cielený charakter útoku a zameranie sa na zistenie špecifík cieľovej siete a zariadení. Prostriedky útoku APT sa rozšíria, získajú informácie a tieto zasielajú cez utajený komunikačný kanál. Vo väčšine prípadov závisia na vonkajšom riadení, no niekedy dokážu pôsobiť aj v izolácii (ako napr. *Stuxnet*).

Ďalšími z rozdielov prostriedkov útoku APT oproti bežnému malwaru alebo nástrojom infiltrácie, bola snaha zotrvať v napadnutom zariadení skryte a schopnosť sa rozširovať vo vnútri napadnutej siete. Útok typicky prebieha postupne a viacúrovňovo (*Tiered Infection Model*) a za použitia vysoko sofistikovaných metód skrytej komunikácie. Základné mechanizmy útoku APT sa snažia získať informácie z cieľa, zatiaľ čo tie zložitejšie zostávajú v nečinnosti. Tento viacúrovňový model prispieva k pretrvávajúcemu charakteru útoku, kedy v podstate nebezpečnejšie a ťažšie detekovateľné škodlivé kódy sú aktivované až po odstránení iniciačných. Týmto spôsobom v podstate „vyčistené“ zariadenia zostávajú infikované, čo len poukazuje na

dôležitosť dôsledného preskúmania útoku APT pred samotným pokusom vyčistenia napadnutých zariadení. Vytrvalý a viacúrovňový útok APT nakoniec končí prístupom útočníka k dátam cieľa. Chránené informácie môžu byť podľa svojho charakteru použité na čokoľvek od získania výhody na trhu či priameho finančného benefitu predajom konkurencii alebo na čiernom trhu a v poslednom rade aj na vývoj modernejších prostriedkov kybernetických útokov, špionáže a sabotáže (1; s. 44 – 45), (17; s. 1 – 6).

4.2 Základné metódy používané pokročilými pretrvávajúcimi hrozbami

Metódy využívané útokmi APT sa vo všeobecnosti rôznia, no analyzovaním prípadov útokov na priemyselné siete v posledných rokoch bolo možné identifikovať ich základné profily. Útočníci majú tendenciu byť priamočiari, využívajú spravodajské informácie z otvorených zdrojov (*Open source Intelligence – OSINT*) na zistenie sociálneho správania v prostredí cieľa útoku, cielený phishing (emaily navrhnuté tak, aby oklamali adresáta a naviedli ho na kliknutie na linku, otvorenie prílohy emailu, alebo spustenie škodlivého kódu iným spôsobom), prenosné médiá a nebezpečné webové stránky, ako základné prostriedky zavedenia škodlivých kódov. Samotné škodlivé programové kódy (tzv. *payload*) variujú od voľne dostupných ako napr. *Webattacker* až po komerčné ako napr. *ZeusBot, Ghostnet, Mumba a Mariposa* a ich zavedenie do systému cieľa je typicky šikovne maskované, s cieľom obísť antivírovú ochranu a iné detekčné mechanizmy (1; s 44).

Po úspešnej infiltrácii do siete sa prostriedky APT snažia pracovať skryte a prípadne sa môžu pokúsiť o deaktiváciu alebo obídenie antivírovej ochrany, nastavia komunikačné kanály vzdialenej správy útočníkom (*backdoor*) a otvoria komunikačné kanály cez bezpečnostné diery vo firewale. *Stuxnet* napríklad úspešne predchádzal detekcii obchádzaním prostriedkov ochrany a rovnako aj samostatným odstránením sa zo systému, ak tento nebol kompatibilný so súborom jeho škodlivých kódov (*payload*).

Ak sú teda techniky a prostriedky využívané pokročilými pretrvávajúcimi hrozbami známe, môžeme si položiť otázku, čo je na nich vlastne tak „pokročilé“. Jedným z takýchto faktorov je určite dokonalá znalosť cieľa – znalosť technických prostriedkov cieľa a ľudí, ktorí s cieľom prichádzajú do styku. Napríklad dobre cielený phishing môže využívať znalosti z cieľového podnikového prostredia, jeho štruktúry a zvykov pracovníkov a maskovať sa za skupinový email, vydávajúci sa za regulárny email od vedenia podniku, alebo masový email ponúkajúci pracovníkom nejaký podnikový benefit, zľavové kupóny a pod. (1; s. 44), (17; 2 – 5).

4.3 Kybernetická vojna

Oproti útokom APT, kde ako sme už uviedli iniciačná fáza útoku zvyčajne využíva síce cielené, no predsa jednoduchšie prostriedky infiltrácie (označenie „pokročilá hrozba“ je skôr spojená s ich správaním po infikovaní cieľa), pre prostriedky kybernetickej vojny sú špecifické podstatne sofistikovanejšie mechanizmy zavedenia škodlivých kódov do systému cieľa a rovnako aj samotné škodlivé kódy sú zvyčajne prepracovanejšie. Napríklad v prípade *Stuxnetu*, ktorý využíval viacero neznámych zraniteľností (*Zero-Day Vulnerabilities*). Tu je dôležité uviesť, že využitie tohto druhu zraniteľností vyžaduje značné zdroje (napr. finančné zdroje na kúpu komerčne dostupného malwaru, alebo intelektuálne zdroje na jeho vývoj). To bol rovnako jeden z dôvodov, prečo *Stuxnet* vzbudil tak veľkú vlnu špekulácií ohľadom jeho zdroja a cieľov. Jeho vysoká prepracovanosť a zameranie na konkrétny riadiaci systém vypovedala o tom, že jeho tvorcovia mali značné zdroje a prístup k rovnakému typu riadiaceho systému, na ktorom ho mohli vyvíjať a testovať, alebo mali dostatok informácií o konkrétnom systéme na to, aby ho mohli vyvíjať a testovať v simulovanom prostredí. Dostatok informácií môže vypovedať napríklad o ich predchádzajúcom nelegálnom získaní cez útok APT a neskoršom použití týchto informácií na vývoj prostriedkov kybernetickej

vojny (samozrejme, či to tak bolo aj v prípade *Stuxnetu*, nie je do súčasnosti verejne známe) (1; s. 44 – 45), (18; s, 6 - 10); (19; s. 151).

Pri porovnávaní prostriedkov útokov APT a prostriedkov kybernetickej vojny môžeme vo všeobecnosti dôjsť k dvom dôležitým skutočnostiam. Prvým je, že pre prostriedky kybernetickej vojny je charakteristická vyššia miera sofistikovanosti a možných dôsledkov útoku. Dôvodom sú značné zdroje útočníka a jasný cieľ spôsobenia škody a nie získanie profitu. Druhou je skutočnosť, že mnohé priemyselné siete oproti ostatným sieťam poskytujú útočníkom menšie možnosti profitu. Ak je priemyselná sieť súčasťou komerčného výrobného procesu, prípadné známky útoku typu APT budú pravdepodobne výsledkom pokusu o krádež intelektuálneho vlastníctva. Ak je ale priemyselná sieť súčasťou zariadenia kritickej infraštruktúry, známky útoku typu APT by mohli znamenať podstatne viac a vyšetrenie takéhoto incidentu by malo byť vedené s maximálnou obozretnosťou (1; s. 44 – 45), (18; s, 6 - 10).

4.4 Nové trendy v oblasti pokročilých pretrvávajúcich hrozieb a kybernetickej vojny

Vďaka analýzam známych kybernetických incidentov v posledných rokoch, bolo možné mapovať nové trendy v oblasti pokročilých pretrvávajúcich hrozieb a kybernetickej vojny. V prvom rade dochádza k značnému vývoju v oblasti samotného škodlivého softvéru, ktorý je prepracovanejší, schopný náročných logických operácií, mutácií a pod. V druhom rade je to vývoj v oblasti spôsobu zavedenia škodlivého softvéru do cieľa, jeho správania a spôsobe šírenia. Už v minulosti bol v tejto oblasti zaznamenaný posun a to od útokov využívajúcich zraniteľnosti na sieťovej a transportnej úrovni, na útoky využívajúce zraniteľnosti konkrétnych aplikácií. Trendy v poslednej dobe však vypovedajú o ďalšom posune a to od využívania zraniteľností produktov Microsoftu, k využívaniu zraniteľností (takmer rovnako všadeprítomného)

formátu *Adobe Portable Document Format* (PDF) a softvéru pracujúcemu s týmto formátom (1; s. 46 – 48).

Škodlivý softvér využívajúci PDF formát je takmer ukážkovým príkladom posunu od útokov na zraniteľnosti protokolov nižšej úrovne a operačného systému, k útokom a manipulácii konkrétnej aplikácie. Táto aplikácia následne zabezpečí spustenie škodlivého kódu zakomponovaného v PDF súbore, alebo pripojením sa na škodlivú webovú stránku. Táto metóda bola použitá napríklad na šírenie škodlivého kódu *ZeusBot* a hoci vyžadovala interakciu s používateľom počítača – otvorenie PDF prílohy emailu, všeobecné použitie PDF dokumentov a dôvera používateľov v kombinácii s dobre prepracovaným phishingom sa ukázali ako vysoko efektívne.

V súčasnosti hojne používanné webové aplikácie sú tiež využívané na zavádzanie škodlivého softvéru a jeho komunikáciu s útočníkom (*Command and Control*). Sociálne siete ako napríklad *Facebook, Twitter a Google Groups* sú na to ideálnym prostredím. Sú všeobecne dostupné, masovo využívané a ťažko kontrolovateľné. Mnoho spoločností využíva sociálne siete na účely marketingu a predaja a často majú tieto služby otvorený prístup cez firemné firewaly. Široká popularita a využívanie sociálnych sietí však môže predstavovať hrozbu pre priemyselné siete, aj keď tieto zvyčajne nie sú s nimi v priamom kontakte. Už vo svojej podstate sú sociálne siete navrhnuté s cieľom zabezpečovať komunikáciu medzi ľuďmi a tak, ako sú zraniteľnosti aplikácií a protokolov objektmi zneužitia útočníkmi, rovnako je to aj zo zraniteľnosťami ľudí. Na tej najnižšej úrovni môžu byť sociálne siete využívané (otvorene alebo skryte) na zhromažďovanie osobných údajov, súkromných a podnikových informácií a získanie dôvery osôb prichádzajúcich do kontaktu s priemyselnými sieťami a pod. Prepracovanejšie metódy môžu zahŕňať aktívne využitie sociálnych sietí škodlivým softvérom na komunikáciu a jeho riadenie útočníkom. Falošné účty spolupracovníkov na sociálnych sieťach môžu viesť

k sprístupneniu citlivých informácií, alebo k vyvolaniu falošnej dôvery a spusteniu internetových odkazov vedúcich k škodlivým webovým stránkam, ktoré následne infikujú počítač užívateľa, prenosné médiá a pod. Takto (nepriamo) sa môže škodlivý softvér dostať aj do zabezpečených priestorov podniku a priamo ohroziť priemyselnú sieť. Aj keď sociálne siete nie sú priamymi nosičmi škodlivého softvéru, môžu byť využité útočníkmi k zhromažďovaniu súkromných informácií, informácií o sociálnom správaní personálu podniku, organizácii práce a pod. a nakoniec k návrhu cielenej phishingovej kampane. Phishing je v tomto prípade overená taktika a v kombinácii s prirodzenou dôverou spojenou so sociálnymi sieťami, môže byť v rukách útočníkov vysoko efektívna (1; 45 – 46, 112 – 114), (18), (19; s. 146 – 148).

Tak ako v každej oblasti, aj v oblasti kybernetických útokov budúcnosť určite prinesie vývoj v jednotlivých ich aspektoch (metód zavedenia do priemyselných systémov, samotných škodlivých kódov a pod.). Môžeme očakávať vyššiu mieru v prepracovanosti individuálnych škodlivých kódov a rovnako aj ich rôzne zlúčeniny. Z dôvodu že vývoj, či zaobstaranie nových pokročilých škodlivých kódov je nákladný, v krátkodobom horizonte je možné očakávať skôr nové variácie už známych hrozieb, než novú „revolúciu“ typu *Stuxnet*.

Pochopenie ako môžu byť súčasne známe kybernetické hrozby upravené a vylepšené, môže priniesť jasnejšie svetlo do oblasti vývoja ochranných stratégií. Je možné očakávať, že kybernetické hrozby budú schopné pôsobiť širokospektrálnejšie, budú prepracovanejšie a zložitejšie, budú využívať zraniteľnosti typu *Zero-Day* vo viacerých fázach útoku (šírenie, zavedenie do systému, samotná škodlivá činnosť), budú cielenejšie a schopné sa účinnejšie maskovať v cieľovom systéme. Ak útočníci zvolia navyše obozretnú taktiku

transportu škodlivého softvéru do cieľového prostredia, pravdepodobnosť detekcie môže byť výrazne nižšia (1;, s. 49 – 50).

Už v roku 2011 boli preskúmané zverejnené viaceré neznáme zraniteľnosti riadiacich informačných systémov SCADA a programové kódy, ktoré ich využívajú (*exploits*). Napríklad takzvavé *„Luigi Vulnerabilities"* objavené talianskym výskumníkom Luigim Auriemma obsahovali celkovo 34 zraniteľností riadiacich systémov značiek *Siemens, Iconics, 7-Technologies* a *DATAC*. Podobne ruská firma *Gleg* vydala podobný balík s názvom *Agora+* pre systémy *CANVAS*. Tieto príklady poukazujú na to, že v súčasnosti sú dostupné viaceré prostriedky napomáhajúce pri zabezpečovaní ochrany proti kybernetickým útokom. Za predpokladu ich uváženého použitia (napr. penetračné testovanie systému) v kombinácii s inými bezpečnostnými opatreniami a postupmi, môžu priniesť pozitívne výsledky (20), (21).

4.5 Ochrana proti pokročilým pretrvávajúcim hrozbám

Problematika ochrany priemyselných sietí bola odjakživa vysoko aktuálna, no v súčasnom prostredí pokročilých pretrvávajúcich hrozieb či kybernetickej vojny sú nevyhnutnosťou požiadavky na zavádzanie moderných bezpečnostných mechanizmov, aplikujúcich komplexnejšie a aktívnejšie metódy ako je bežné. Je tomu tak hlavne preto, lebo pokročilé pretrvávajúce hrozby sa vyvíjajú hlavne v spôsoboch obídenia známych bezpečnostných opatrení. Rovnako, technické prostriedky ochrany dokážu sledovať a reagovať na procesy prebiehajúce v priemyselných sieťach, no nie na „ľudský element", ktorý stojí v pozadí. Kritickou súčasťou moderných bezpečnostných mechanizmov je neustály monitoring a schopnosť automatizovaným spôsobom testovať a overovať, či sú súčasné bezpečnostné opatrenia funkčné a proaktívne a včas ošetrovať zraniteľnosti (v niektorých prípadoch je tento koncept označovaný ako *Advanced Persistent Diligence – APD*). Ich úlohou je v kombinácii s prvkami viacúrovňovej ochrany (*Defence In Depth*) zmenšiť

priestor, ktorý by potenciálny útočník mohol využiť na útok a tiež poskytovať širší náhľad na činnosť jednotlivých hrozieb pre potreby ich analýz, vyšetrovania a reakcií na ne. V súčasnosti je nevyhnutné analyzovať podstatne väčšie množstvá dát z hľadiska činnosti siete a jej správania sa vo viacerých kontextoch (1; s. 23 – 24 a 50), (17; s. 9 – 10), (18; s. 10 – 11).

Tradičné bezpečnostné opatrenia používané v nedávnej minulosti dnes už nepostačujú, pretože prostriedky aktívnej sieťovej ochrany ako napríklad firewaly, antivírová ochrana, antispam, systémy prevencie do systému atď. už nie sú plnohodnotne schopné blokovať aktuálne hrozby. V prípade malwaru útočiaceho na zraniteľností typu *Zero-Day*, to v podstate ani nie je možné. Neustály prehľad o procesoch, ktoré sa pokúšajú pripojiť k systému rovnako ako sledovanie procesov vo vnútri systému, je jedinou cestou, ako systém dostať pod kontrolu. Toto zahŕňa informácie o systéme a zdrojoch, sieťových komunikačných tokoch a ich schémach a modeloch, používateľských skupinách, právach a politikách. V ideálnom prípade tieto procesy prebiehajú automatizovane a poskytujú aktívnu spätnú väzbu bezpečnostným špecialistom a priestor na ich reakciu v prípade detegovania pokročilej nepretržitej hrozby (1; s. 50), (17; 10 – 11).

4.6 Reakcia na pokročilé pretrvávajúce hrozby

Je takmer ironické, že v prípade detekcie pokročilej pretrvávajúcej hrozby, je pokus vyčistenia napadnutého zariadenia tým posledným, čo by sa malo urobiť. Už bolo spomenuté v predchádzajúcich častiach, že dôvodom je hlavne nebezpečenstvo následnej infekcie systému po odstránení iniciačného malwaru a možné spustenie škodlivých kódov, ktoré zostávali do toho času neaktívne. Je namieste začať dôsledným vyšetrením detegovanej hrozby, čo by malo byť z hľadiska komplexnosti a sofistikovanosti vedené minimálne na rovnakej úrovni, akú vykazuje zaznamenaná hrozba.

Prvým krokom je nepochybne izolácia hostiteľa a tým pádom zabránenie vzniku ďalších škôd. Detegovanej pokročilej pretrvávajúcej hrozbe sa následne ponechá možnosť komunikácie cestou kanálov, ktoré na to ustanovila. To všetko samozrejme za predpokladu, že hostiteľ bol izolovaný od zostatku siete a rovnako od prístupu k citlivým alebo chráneným informáciám. V ďalšom kroku nasleduje zber čo najväčšieho objemu informácií vo forme Log súborov, zachytenej sieťovej komunikácie, pamäťových súborov a pod. Efektívne tzv. „sandboxovanie napadnutého systému“ (prísne kontrolovanie množiny zdrojov pre spustené programy, priestoru na disku a v pamäti, prístupu na sieť atď.) môže poskytnúť dostatok potrebných informácií a výrazne napomôcť, prípadne úplne zneškodniť pokročilú pretrvávajúcu hrozbu (1; s. 50 – 51), (17; s. 7 – 11).

Zhrnutím uvedeného, v prípade podozrenia z napadnutia systému pokročilou pretrvávajúcou hrozbou, je potrebné s najvyššou obozretnosťou a dôkladnosťou:

- za každých okolností všetko monitorovať: zhromažďovať dostupné informácie (konfigurácie, firmvér, atď.),
- analyzovať dostupné Log súbory a snažiť sa identifikovať rozsah infekcie, infikovaných hostiteľov, spôsoby (nosiče) ďalšieho šírenia infekcie atď.,
- sandboxovať a preskúmať napadnutý systém,
- analyzovať pamäť a snažiť sa nájsť rootkity a iné hrozby zavedené v pamäti,
- využiť metódu reverzného inžinierstva na zistenie možného rozsahu detegovanej hrozby, spôsobov jej šírenia, spôsobov samodeštrukcie a pod.,
- odovzdať zhromaždené informácie zodpovedným autoritám.

V závislosti na závažnosti konkrétnej pokročilej pretrvávajúcej hrozby, v niektorých prípadoch bude jedinou možnosťou úplné vymazanie všetkých dát konkrétneho zariadenia a nová inštalácia systému (tzv. *Bare Metal Reload*). Pre tieto prípady je nevyhnutné mať čisté verzie operačných systémov a firmwaru na médiách v zabezpečenom priestore. Rozsah škôd v systéme je už v súčasnosti možné analyzovať viacerými druhmi nástrojov. Za voľne dostupné uvedieme napr. *Memorize* od spoločnosti *Mandiant* (22). Rovnako existuje množstvo spoločností, ktoré sa profesionálne zaoberajú problematikou analýzy pokročilých pretrvávajúcich hrozieb a odstraňovaním ich následkov (1; s. 50 – 52), (17; s. 7 – 11).

ZÁVER

Priemyselné siete sú pre súčasnú produkčnú sféru nevyhnutnosťou. Ako ukázala nedávna minulosť, sú značne zraniteľné a prípadný kybernetický útok na ne by mohol mať devastujúce účinky. V príkladoch kybernetických útokov od útoku na americké veliteľstvo CENTCOM, cez *Operation Aurora* a končiac *Stuxnetom* je viditeľný značný vývoj vo viacerých ich aspektoch. Útoky sa vyvíjajú smerom k pokročilým pretrvávajúcim hrozbám a ich úmysly od krádeže informácií, cez priemyselnú sabotáž až po narušenie kritickej infraštruktúry. Preto ochrana priemyselných sietí dnes vyžaduje prehodnotenie bezpečnostných praktík a ich preorganizovanie s cieľom lepšieho pochopenia vnútorných procesov prebiehajúcich v priemyselných sieťach, ich zraniteľností a existujúcich hrozieb.

Zoznam bibliografických odkazov

1. KNAPP, E.: *Industrial Network Security – Securing Critical Infrastructure Networks for Smart Grid, SCADA and Other Industrial Control Systems*. Elsevier, 2011. 360s ISBN 978-1-59749-645-2.
2. POLLET, J.: 2010. Electricity for free? Dirty underbelly of SCADA and Smart Meters. [online]. [cit. 2013-04-16]. Dostupnosť na internete:

<http://www.slideshare.net/the_netlocksmith/blackhat-2010-electricity-for-free-the-dirty-underbelly-of-scada-and-smart-meters>
3. BackTrack Linux – Penetration Testing Distribution: [online]. [cit. 2013-04-16]. Dostupnosť na internete: <http://www.backtrack-linux.org>
4. Metasploit – Penetration Testing Distribution: [online]. [cit. 2013-04-16]. Dostupnosť na internete: <http://www.metasploit.com>
5. The Register: Hacker jailed for revenge sewage attacks - Job rejection caused a bit of a stink: 2001, 31. Okt. [online]. [cit. 2013-04-16] Dostupnosť na internete: <http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/>
6. CNN: Staged cyber attack reveals vulnerability in power grid: 2007, 26. Sept. [online]. [cit. 2013-04-16] Dostupnosť na internete: <http://edition.cnn.com/2007/US/09/26/power.at.risk/>
7. Urban Legend Watch: Cyberwar Attack on U.S. Central Command: 2010, 31. Marec [online]. [cit. 2013-04-16] Dostupnosť na internete: <http://www.wired.com/threatlevel/2010/03/urban-legend/>
8. McAfee Labs: Operation Aurora: 2010, 14. Jan. [online]. [cit. 2013-04-16] Dostupnosť na internete: < http://www.mcafee.com/us/threat-center/operation-aurora.aspx>
9. Wired: Google Hack Attack Was Ultra Sophisticated, New Details Show: 2010, 14. Jan. [online]. [cit. 2013-04-16] Dostupnosť na internete: <http://www.wired.com/threatlevel/2010/01/operation-aurora/>
10. ICS CERT Advisory ICSA-10-272-01 – PRIMARY STUXNET INDICATORS: 2010, 29. Sept. [online]. [cit. 2013-04-16] Dostupnosť na internete: <http://ics-cert.us-cert.gov/pdf/ICSA-10-272-01.pdf>
11. McAfee Labs: Important information about Night Dragon: 2013, 7. Mar. [online]. [cit. 2013-04-16] Dostupnosť na internete: <https://kc.mcafee.com/corporate/index?page=content&id=KB71150>
12. McAfee Labs: Global Energy Cyber Attacks "Night Dragon": 2011, 10. Feb. [online]. [cit. 2013-04-16] Dostupnosť na internete: < http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf>
13. InfoWorld: Night Dragon attacks from China strike energy companies: 2011, 10. Feb. [online]. [cit. 2013-04-16]. Dostupnosť na internete: <http://www.infoworld.com/d/security-central/night-dragon-attacks-china-strike-energy-companies-057>
14. McAfee Labs: Consolidated Threat Report – Duqu: 2012. [online]. [cit. 2013-04-16]. Dostupnosť na internete: <http://download.nai.com/products/mcafee-avert/dil/Duqu_CTR_v2.2f.pdf>

15. Kaspersky Lab and ITU Research: New Advanced Cyber Threat: 2012, 28. Máj. [online]. [cit. 2013-04-16]. Dostupnosť na internete: <http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Research_Reveals_New_Advanced_Cyber_Threat>
16. McAfee Labs: "Flame Attacks" Briefing and Indicators of Compromise: 2012. [online]. [cit. 2013-04-16]. Dostupnosť na internete: <http://www.mcafee.com/us/resources/white-papers/wp-mcafee-skywiper-brief-v-1-6.pdf>
17. POLLET. J.: 2010. *Building a Better Bunker: Securing Energy Control Systems Against Terrorists and Cyberwarriors*. SANS Analyst Program. online]. [cit. 2013-04-16]. Dostupnosť na internete: <http://www.sans.org/reading_room/analysts_program/mcafee_nitro_bunker_12_2010.pdf>
18. Deloite Development LLC.: Cyber Espionage – The harsh reality of advanced security threats. 2011. [online]. [cit. 2013-04-16]. Dostupnosť na internete: <http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_aers_cyber_espionage_07292011.pdf>
19. CARR, J.: *Inside Cyber Warfare*. O'Reilly Media, Inc, 2. Vydanie. 2011. 316s ISBN 978-1-449-31004-2.
20. Digital Bond: Italian researcher publishes 34 ICS vulnerabilities. 2011, 21. Mar. [online]. [cit. 2013-04-16]. Dostupnosť na internete: <http://www.digitalbond.com/blog/2011/03/21/italian-researcher-publishes-34-ics-vulnerabilities/>
21. Digital Bond: Friday News and Notes. 2011, 25. Mar. [online]. [cit. 2013-04-16]. Dostupnosť na internete: <http://www.digitalbond.com/blog/2011/03/25/friday-news-and-notes-127/>
22. Mandiant Memorize: [online]. [cit. 2013-04-16] <https://www.mandiant.com/resources/download/memoryze>