Riešenia informačnej ochrany priemyselných počítačových sietí

Security solutions for protection of Process Control Networks

Marek Šimon, Katedra aplikovanej informatiky, FPV UCM v Trnave

Robert Halenár, Katedra aplikovanej informatiky, FPV UCM v Trnave

Abstract: Security objectives can be promoted by good safety policies, safety plans and their proper implementation. For the whole process is very important to have well-defined management plans, monitoring and evaluation. To strengthen the overall protection of industrial networks is important to improve the safety characteristics of communication protocols, deploying communication encryption technology, implement appropriate authentication mechanism, firewall, antivirus and intrusion detection systems.

Key words: security policy, SCADA, PCN, IDS, firewall, encryption

Abstrakt: Bezpečnostné ciele môžu byť presadzované dobrou bezpečnostnou politikou, bezpečnostnými plánmi a ich riadnym vykonávaním. Pre celý proces je veľmi dôležité mať dobre definované plány riadenia, kontroly a hodnotenia. Pre posilnenie celkovej ochrany priemyselných sietí je dôležité zlepšiť bezpečnostné charakteristiky komunikačných protokolov, nasadiť technológie šifrovania komunikácie, implementovať vhodný autentifikačný mechanizmus, firewally, antivírusy a systémy na detekciu prieniku.

Kľúčové slová: bezpečnostná politika, SCADA, PCN, IDS, firewall, šifrovanie.

1. Úvod

Supervisory control and data acquisition (SCADA) systémy sú dôležitou súčasťou väčšiny kritických infraštruktúr. SCADA zariadenia sú spravidla nasadené pre priemyselnú automatizáciu procesov, ale svoje uplatnenie našili aj pri ovládaní kritickej infraštruktúry, ako sú vodné hospodárstvo, distribúcia elektrickej energie, distribúcia zemného plynu a podobne. SCADA systémy nasadené v priemyselných závodoch sa tiež označujú ako DCS (Distributed

Control System) a PCS (Process Control System). Ako celok sa nazývajú Control Systems. Aj keď termín DCS je v oblasti automatizácie výroby všeobecne častejšie používaný ako SCADA, termín SCADA sa používa pre systémy, ktoré sú roztrúsené na veľkých plochách s rôznymi komunikačnými linkami a protokolmi.

SCADA poskytuje zber dát v reálnom čase, umožňuje efektívnejšie riadenie, zlepšuje ochranu a bezpečnosť zariadení a obsluhy, a znižuje náklady na prevádzku. Zozbierané dáta je navyše možné ukladať do bežných dátových skladov a predspracovať pre algoritmy dolovania dát. Tieto výhody sú možné vďaka použitiu štandardného hardvéru a softvéru v systémoch SCADA v kombinácii s vylepšenými komunikačnými protokolmi a zlepšením pripojenia k vonkajším sieťam, vrátane internetu. Avšak, tieto výhody sú získané za cenu zvýšenej zraniteľnosti voči útokom a chybným krokom z rôznych externých a interných zdrojov. (1), (2), (3), (4), (11)

2. Bezpečnostný menežment

Dobrá bezpečnosť vyžaduje dobrý menežmet, správne a efektívne využívanie bezpečnostných technológií. Za poslednú dekádu spoločnosti, ktoré závisia na informačných a komunikačných technológiách, vytvorili dobré a overené bezpečnostné postupy. Svet priemyselnej komunikácie potrebuje dohnať svet informačných a komunikačných technológií a zlepšiť svoj bezpečnostný menežment.

Bezpečnostné ciele môžu byť vynútené dobrou bezpečnostnou politikou, bezpečnostnými plánmi a ich správnou implementáciou. Pre celý proces je dôležité mať dobre definované plány riadenia, kontroly a hodnotenia. Bezpečnostná politika musí byť komplexná a mať jasne definované postupy, ktoré musia byť vykonané za účelom dosiahnutia bezpečnostných cieľov. Pretože každá spoločnosť (jej sieť) má svoje špecifické požiadavky, nie je možné vytvoriť univerzálnu bezpečnostnú politiku pre všetky spoločnosti.

Bezpečnosť je kontinuálny proces, ktorý nekončí implementovaním všetkých potrebných bezpečnostných technológií. Priemyselné siete musia byť neustále monitorované a kontrolované na bezpečnostné zraniteľnosti. Ich hardvérové a softvérové prvky pravidelne aktualizované. Tento proces trvalej správy sa označuje ako konfiguračný manažment. Pre priemyselné siete obsahujúce stovky prvkov toto môže byť veľkým problémom. Na rozdiel od bežnej údržby, bezpečnostné postupy a technológie v priemyselných sieťach musia byť pravidelne kontrolované. Audity a hodnotenia tretích strán obvykle pomáhajú

odhaliť chybné postupy. Externí audítori musia však byť dôveryhodnými partnermi. Počas auditu majú k dispozícii citlivé informácie o priemyselnej sieti a jej prvkoch. (6), (8), (9)

3. Bezpečnosť HW a SW prvkov

Bezpečnosť priemyselných sietí závisí na bezpečnosti a ochrane ich koncových systémov. Na mnohých uzloch v sieti, rôznych tzv. "embedded" zariadeniach pracujúcich v reálnom čase, beží RT (Real Time) operačný systém. V porovnaní s konvenčným operačným systémom, RT operačný systém je zraniteľnejší voči DoS (Denial of Service) útokom. Aj menšie narušenie práce zariadenia môže viesť k strate schopnosti reagovať v reálnom čase.

V sieťach, ako napríklad elektrické distribučné siete, nie je prakticky možné poskytnúť fyzickú ochranu každého uzla siete. V dôsledku toho je mnoho uzlov bez fyzickej ochrany a útočníkovi stačí len nájsť takýto nechránený uzol. Kompromitovaním takéhoto uzla získa neoprávnený prístup ku zvyšku siete. Preto v prípade, že je možné fyzicky zabezpečiť zariadenie, treba tak spraviť. Vo všeobecnosti je však dôležité mať k dispozícii postupy a protokoly umožňujúce zvýšiť odolnosť siete pri kompromitácii jej uzlov. (1), (3), (5)

4. Zraniteľnosť protokolov

Na posilnenie celkovej ochrany priemyselných sietí je dôležité zlepšiť bezpečnostné vlastnosti ich komunikačných protokolov. Je nevyhnutné analyzovať používané protokoly s pohľadu bezpečnosti a identifikovať ich potencionálne zraniteľnosti. Následne bude možné vyvinúť ochranné mechanizmy, ktoré môžu byť zahrnuté do špecifikácií protokolov. Súčasné špecifikácie komunikačných protokolov priemyselných sietí sú všeobecne uznávané a používané medzinárodné štandardy spravované profesnými organizáciami. Zahrnutie bezpečnostných vylepšení do týchto protokolov môže byť časovo veľmi náročné. Je teda dôležité spraviť dôkladnú analýzu bezpečnostných slabín protokolov (alebo ich nových verzií) skôr než sa štandardizujú. Bezpečnostná analýza protokolov a pochopenie ich zraniteľností uľahčia vývoj pravidiel pre IDS. Malo by byť možné vytvoriť signatúry útokov pre každú potenciálnu zraniteľnosť a tieto signatúry implementovať do systémov na detekciu prieniku.

Pri analýze ľubovoľného protokolu treba rozlišovať dve kategórie zraniteľností, tie, ktoré sú v samotnom návrhu protokolu a tie, ktoré sú spôsobené chybnou implementáciou protokola. Aj keď je jednoduchšie riešiť zraniteľnosť spôsobenú nesprávnou implementáciou, dôležité je

ako prvé analyzovať samotnú špecifikáciu protokolu. Len čo je podstata a potenciálne následky zneužitia zraniteľnosti známa, ochrana pred útokmi je jednoduchšia.

Ohodnotenie zraniteľností je zvyčajne náročný a zložitý proces. Ukazuje sa, že je potrebné vypracovať metodológie ohodnocovania zraniteľností priemyselných sietí. Bola vypracovaná taxonómia zraniteľností v SCADA protokoloch s cieľom poskytnúť rámcovú prácu pre ohodnocovanie bezpečnosti týchto protokolov. (2), (3), (6)

5. Kontrola prístupu

Prvou úlohou pri ochrane každej siete je zabrániť neautorizovanému vstupu do siete. Je teda dôležité zlepšiť mechanizmy kontrolu prístupu v priemyselných sieťach. Bohužiaľ náročnosť definície perimetra v týchto sieťach robí vytvorenie vhodného mechanizmu kontroly prístupu skutočnou výzvou. Väčšina priemyselných sietí je pripojená do vonkajšej firemnej siete alebo cez bránu do Internetu. A zvyčajne to nie je jediné pripojenie do vonkajšieho sveta. Zabudnuté modemové spojenie, ktoré ani nie je v dokumentácii siete môže byť vstupnou bránou pre útočníka. Z tohto je zrejmé, že oddelene od riešenia kontroly technického prístupu by mala byť v bezpečnostnej politike spoločnosti jasne definovaná aj politika kontroly prístupu do siete. Samozrejmosťou by mala byť podpora tejto politiky vhodnými nástrojmi riadenia bezpečnosti.

Vhodný autentifikačný mechanizmus je prvým krokom k dosiahnutiu kontroly prístupu. Autentifikácia je zvyčajne vynútená vytvorením užívateľských účtov pre užívateľov, ktorí po autentifikovaní užívateľským menom a heslom, môžu pristupovať k zdrojom siete. Táto metóda predstavuje najrozšírenejší prostriedok autentifikácie. Heslo je ľahko prenositeľné a jeho používanie je pomerne jednoduché a pohodlné. Zároveň však existuje množstvo nevýhod a rizík spojených s používaním hesla. Heslá sú dnes už považované za slabý prostriedok k zabezpečeniu prístupu. Dôvodov je viac. Užívatelia si väčšinou ako heslo volia rôzne podoby svojho mena, iniciálky a názvy zo svojho okolia, dátumy narodenia a podobne. Rôzne štúdie dokázali, že takmer tretinu hesiel je možné uhádnuť na desiaty pokus. Heslo sa dá tiež odpozorovať počas zadávania. Alebo ho užívateľ jednoducho zabudne. Základným rozporom teda je, že heslo musí byť dlhé a komplikované, ťažko uhádnuteľné. Zároveň si ho užívateľ musí byť schopný zapamätať. Navyše, ľudia sa nechajú vcelku ľahko oklamať a presvedčiť aby prezradili svoje heslo.

V priemyselných sieťach má teda autentifikácia založená na hesle, podobne ako aj v iných sieťach, svoje nevýhody. Z toho dôvodu sa ako riešenie kontroly prístupu do priemyselných sietí navrhuje používať autentifikáciu založenú na smart kartách. Smart karty môžu bezpečne uchovávať heslo. Avšak ani smart karty neriešia kompletne problém autentifikácie. Všetky typické problémy autentifikácie ľudských užívateľov v priemyselných sieťach stále pretrvávajú rovnako ako v ktoromkoľvek inom prostredí. (3), (4), (8)

6. Šifrovanie

Protokoly priemyselných sietí typicky nepodporujú žiadne metódy kryptografie. Pritom kryptografia by mohla byť užitočná pri ochrane týchto sietí. Jedinečná charakteristika priemyselných sietí však výrazne sťažuje adaptovať existujúce kryptografické techniky. Príkladom môže byť obmedzený výpočtový výkon zariadení priemyselných sietí a často požadovaná reakcia zariadení cez sieť v reálnom čase. Toto komplikuje implementáciu komplexnej kryptografie v prostredí priemyselných sietí. Americká asociácia prepravcov plynu (American Gas Assosiation - AGA) vyvinula sadu protokolov pre komunikáciu v SCADA sieťach. Tieto protokoly by mali pokrývať všetky problémy súvisiace s implementovaním dobrej kryptografie a správy kľúčov v SCADA sieťach. Štandardy AGA-12 poskytujú prehľad problémov zapojených v implementovaní kryptografie v SCADA sieťach a tiež rozvíja techniku implementácie kryptografie do už existujúcich a používaných SCADA sietí. Účelom týchto techník je zaručenie integrity správy s ohľadom na požadovaný výkon a rýchlosť odozvy v SCADA linkách. Toto sa dosahuje zapojením prídavných kryptografických modulov na všetky koncové prvky SCADA liniek. Na vysielajúcej strane je správa zašifrovaná týmto modulom skôr ako sa ako paket odošle na prenosové médium. Na prijímajúcej strane kryptografický modul dešifruje prichádzajúce správy skôr ako sa prepošlú prijímajúcemu SCADA zariadeniu.

Kryptografické riešenia sú však neúplné bez efektívnej správy kľúčov. Toto zostáva otvoreným problémom v SCADA sieťach. Asociácia AGA v súčastnosti vyvíja štandardy pre správu kľúčov. Prostredie SCADA sietí je z pohľadu správy kľúčov jedinečné. V mnohých SCADA sieťach ako rozvody elektriny alebo plynu, sú prvky siete otvorené, bez akejkoľvek fyzickej ochrany. Kľúč uložený v takomto zariadení je veľmi zraniteľný. (3), (4), (5), (8)

7. Firewally a systémy na detekciu prieniku

Vo všeobecnosti, firewall je nástroj, ktorý oddeľuje chránenú sieť od nechránenej a v mnohých prípadoch jednu chránenú časť siete od inej nechránenej časti tej istej siete.
Firewall sa používa z dvoch dôvodov, zadržať útoky z vonku a udržať užívateľov vnútri siete. Je teda určitým škrtiacim miestom, cez ktorý prechádza všetka komunikácia z a do chránenej siete. Pomocou firewallu sa dá vynútiť určitá úroveň bezpečnosti pripojenia do ďalšej sieti (či už Internetu, alebo priemyselnej siete). Aby bol firewall účinný, organizácia ho musí zahrnúť do svojej bezpečnostnej politiky. Musia byť definované zdroje chránenej siete, ktoré budú sprístupnené z vonkajšej siete. A rovnako, ktorí používatelia, z ktorých počítačov chránenej siete môžu pristupovať k zdrojom vonkajšej siete.

Aj v priemyselných sieťach je základnou úlohou firewallu blokovať neautorizovanú sieťovú premávku medzi chránenou a nechránenou sieťou. Firewall nedovolí vytvoriť priame spojenie medzi uzlom v Internete a uzlom v priemyselnej sieti. Firewall môže byť nakonfigurovaný tak, aby povolil iba komunikáciu pomocou konkrétnych protokolov. Ak je napríklad používaný iba PROFINET, firewall môže byť nastavený tak, aby blokoval inú komunikáciu.

Firewall môže byť tiež nastavený tak, aby rozpoznával aktivitu autorizovaných entít pristupujúcich do priemyselnej siete. Niektoré entity v podnikovej sieti môžu byť autorizované pristupovať iba k niektorým zdrojom v priemyselnej sieti. Firewall teda zaručuje, že tieto entity budú svoje prístupové práva využívať správne.

Prínos firewallov je zrejmý. Napriek tomu je v súčasnosti dostupných len niekoľko komerčných firewallov pre prostredie priemyselných sietí. Spoločnosť Cisco Systems vyvinula „open source[1]“ Linuxový firewall so schopnosťou filtrovať MODBUS komunikáciu. Firewall pridáva funkcionalitu filtrovania MODBUS komunikácie do linuxového nástroja Netfilter. Projekt vyžaduje ešte veľa práce na pridaní podpory pre ďalšie protokoly (DNP3, Profinet).

Úlohou systému na detekciu narušenia bezpečnosti je identifikovať, pokiaľ možno v reálnom čase, zneužitie, neautorizované alebo nesprávne použitie počítačového systému. Pričom pôvodcom môže byť interný pracovník, alebo útočník z vonku. Problematika detekcie prieniku sa stáva veľmi dôležitou v súvislosti s nárastom počtu pripojených systémov do

[1] Všeobecne open source software, softvér s dostupným zdrojovým kódom, užívatelia majú právo ho modifikovať a šíriť ďalej

Internetu. Viac systémov znamená viac potencionálnych útočníkov a ich ťažšie identifikovanie. Systémy na detekciu prienikov (Intrusion Detection System, IDS), tak ako ďalšie nástroje počítačovej bezpečnosti by mali byť zahrnuté v bezpečnostnej politike. Bezpečnostná politika by pre IDS mala definovať aký typ IDS je potrebný, kde bude umiestnený, aký typ útokov má IDS detegovať a ako má na daný typ útoku reagovať.

S IDS je v priemyselných sieťach podobný problém ako s firewallmi. Je len málo komerčne dostupných systémov na detekciu prieniku, ktoré sú schopné pracovať s protokolmi priemyselných sietí. Vývoj IDS pre tento typ sietí je náročnejší ako vývoj firewallov. Na vývoj firewallu postačuje znalosť štruktúry komunikačných protokolov. Na druhej strane vývoj IDS schopného rozpoznať prebiehajúci útok vyžaduje znalosti aj o slabých miestach týchto protokolov a aj zariadení, ktoré tieto protokoly využívajú. Tieto znalosti sa dajú získať len intenzívnym skúmaním zraniteľností celej infraštruktúry priemyselných sietí. (3), (6), (7), (10)

8. Záver

Ak má byť kritická infraštruktúra vo svete bezpečná a spoľahlivá, tak vlastníci a prevádzkovatelia si musia uvedomiť, že ich riadiace systémy sa stali terčom sofistikovaných útokov. A podľa toho budú musieť aj upraviť svoje bezpečnostné programy. V rámci týchto bezpečnostných programov je dôležité:

- budovať robustný bezpečnostný menežment s politikou aplikovania záplat (patch policy),
- implementovať vhodný autentifikačný mechanizmus,
- implementovať kryptografické riešenie a efektívnu správu kľúčov,
- nasadiť technológie detekcie narušenia bezpečnosti, na detekciu útokov a spustenie poplachu pri ohrození zariadenia,
- nasadiť firewally a antivírusové technológie určené pre SCADA/ICS (Industrial Control System), aby sa sťažili útoky sofistikovaného malwaru,
- zahrnúť hodnotenia bezpečnosti a testovanie do procesu vývoja systému a do procesu pravidelnej údržby,

- identifikovať a opraviť prípadné chyby, čím sa znižuje pravdepodobnosť úspešného útoku,
- pracovať na zlepšenie kultúry priemyselnej bezpečnosti naprieč menežmentom a technickými tímami.

9. Zoznam bibliografických odkazov

(1) Byres, Eric – Franz, Matthew – Miller, Darrin: The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems, In *International Infrastructure Survivability Workshop (IISW'04)*, IEEE, Lisbon, Portugal, 4. decembra 2004, 9 s.

(2) Georgiev, Boris – Jurišica, Ladislav: Prevádzkové riadiace systémy 2, In *AT&P Journal 2/2006*, s. 46 - 48, ISSN 1335-2237

(3) Krutz, Ronald: *Securing SCADA Systems*, 1st ed. Wiley Pub.,Nov. 28, 2005.

(4) Byres, Eric – Ginter, Andrew – Langill, Joel: *How Stuxnet spreads – a study of infection paths in best practice systems*, Tofino security White paper, 2011

(5) Brunner, Martin, et. al.: *Infiltrating Critical Infrastructures with Next-Generation Attacks as a Showcase Threat*, Fraunhofer SIT, December, 2010, 23.

(6) Keith Stouffer, Joe Falco, Karen Kent: *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security*, NIST Special Publication 800-82, 2006

(7) Steven Cheung et al: *Using Model-based Intrusion Detection for SCADA Networks*, Computer Science Laboratory SRI International, 2006

(8) Franeková M. et al.: *Komunikačná bezpečnosť priemyselných sietí.* Žilinská univerzita v Žiline, 2007, ISBN 978-80-8070-715-6.

(9) Giani, A. et al: *A testbed for secure and robust SCADA systems.* SIGBED Rev. 5, 2 (Jul. 2008), 1-4

(10) Halenár , Igor: Secure communications in industrial data networks. In *International Doctoral Seminar 2010* : Proceedings: Smolenice, 16-19 May 2010, editorial: Alena Sucáková, Trnava : AlumniPress, 2010. ISBN 978-80-8096-118-3. S. 186-193

(11) Trnka Andrej - Proposal of application datawarehouses into control process. In *International Doctoral Seminar 2009* : Proceedings: Smolenice 17-19 May, 2009

editorial: Alena Sucáková, Dagmar Cagánová. Trnava: AlumniPress, 2009. ISBN 978-80-8096-088-9. S. 343-348.

10.Adresa autorov:

Marek Šimon, Ing.
Katedra aplikovanej informatiky FPV UCM
Nám. J. Herdu 2
917 01 Trnava
marek.simon@ucm.sk

Robert Halenár, Ing., PhD.
Katedra aplikovanej informatiky FPV UCM
Nám. J. Herdu 2
917 01 Trnava
robert.halenar@ucm.sk