Kybernetická bezpečnost průmyslových řídicích systémů (část 1)

Mario Chiock, Del Rodillas

Článek popisuje, co hrozí průmyslovým řídicím systémům z hlediska kybernetické bezpečnosti a shrnuje, jak těmto hrozbám čelit. Uvádí devět základních funkcí, které by měla splňovat moderní platforma pro zabezpečení průmyslových řídicích systémů, aby zajistila maximální dostupnost zařízení a přitom je ochránila před existujícími i dosud neznámými hrozbami.
Článek je redakčně upravenou verzí studie Defining the 21st Century Cybersecurity Protection Platform for ICS společnosti Palo Alto Networks.

Průmyslová výroba přebírá mnohé postupy a nástroje ze světa informačních a komunikačních systémů (ICT – *Information and Communication Technology*), aby využila jejich pružnost, rychlost, propojitelnost a cenovou výhodnost. Do průmyslu začíná pronikat koncepce internetu věcí – v podobě IIoT (*Industrial Internet of Things*) již dnes pomáhá zajišťovat prediktivní údržbu a v budoucnu se může stát základem zcela nových multiagentních výrobních a podnikatelských modelů.

Tento vývoj ale zanáší do řízení průmyslové výroby také slabiny ICT. Hrozí nebezpečí, že tato slabá místa se stanou vstupní bránou pro nevítané návštěvníky, kyberzločince a kyberteroristy nebo že budou využita v kybernetické válce. Rizika s tím spojená jsou o to větší, že průmyslové řídicí systémy (ICS – *Industrial Control System*) a systémy SCADA jsou často součástí kritické infrastruktury.

V současné době jsme konfrontováni nejen se zvětšujícím se počtem kybernetických útoků, ale i s jejich rostoucí důmyslností a zacílením právě na kritickou infrastrukturu a průmyslové podniky. Existují případy, kdy byly nejen přerušeny technologické procesy, ale dokonce i zničeno zařízení. Potřeba zvyšovat zabezpečení průmyslových řídicích systémů, tzv. kybernetickou bezpečnost[1)], proto ještě nikdy nebyla tak velká jako teď. Zatímco pracovníci oddělení IT mohou nová opatření ke zvýšení kybernetické bezpečnosti zavádět velmi rychle, správci provozní techniky (OT – *Operational Technology*) musí být opatrnější, protože musí respektovat extrémní požadavky na zajištění dostupnosti zařízení a kontinuity technologických procesů. V oblasti procesní techniky není výjimkou, že zařízení musí nepřetržitě pracovat mnoho měsíců či několik let. Po tuto dobu je nepřípustné provádět jakékoliv změny a aktualizovat software, byť by šlo o zabezpečení slabých míst. Jindy se administrátoři OT záměrně vyhýbají antivirovým programům a službám IPS (*Intrusion Prevention Service*) z obavy ze zablokování funkce řídicího systému nebo snížení jeho funkční bezpečnosti a výkonnosti. Tyto programy a služby tedy operátoři buď spustí pouze v režimu detekce, nebo je nepoužívají vůbec. Dokonce i metody, které jsou ve světě ICT zcela běžné, např. skenování a vyhledávání slabých míst, mohou u průmyslových počítačů PLC způsobit selhání, protože tato zařízení na takové akce nejsou stavěna. Uvedená omezení způsobují, že zabezpečení ICS je obzvlášť unikátní a obtížné.

Výsledkem je, že mnohé výrobní podniky používají pro své ICS podivný souhrn obstarožních metod zabezpečení, které je obtížné udržovat, poskytují jen velmi omezený přehled o bezpečnostní situaci a lze je jen těžko využít k preventivním bezpečnostním úkonům. Právě takové podniky jsou často primárním cílem pro útočníky – někdy čistě jen proto, aby si na nich ověřili kvalitu svých kybernetických útoků. Bezbrannost průmyslových podniků proti stále důmyslnějším útokům je varující a naléhavě vyžaduje řešení.

Pro důkladné zabezpečení ICS proti novodobým hrozbám musí vzniknout nová bezpečnostní platforma, která sloučí různé bezpečnostní technologie tak, aby ICS ochránila i proti nejdůmyslnějším útokům. Platforma musí být schopna nejen upozorňovat na útoky, ale také automaticky vykonávat příslušné akce, a to prostřednictvím svých vlastních služeb, ale rovněž prostřednictvím jiných podpůrných prostředků. Musí ochránit informace uvnitř podniku i sdílené s jinými subjekty. Stejně jako „zlí hoši“ spolupracují na přípravě kybernetických útoků, musí spolupracovat i podniky na společné obraně.

1. Úvod

1.1 Vývoj průmyslových řídicích systémů

Pro řízení technologických procesů na provozní úrovni, včetně kritické infrastruktury, např. elektrických rozvodných sítí nebo ropných rafinerií, se používají různé řídicí systémy: průmyslové řídicí systémy založené na programovatelných automatech (PLC) a průmyslových počítačích (IPC), systémy supervizního řízení a sběru dat SCADA nebo distribuované řídicí systémy DCS. V tomto článku budou pro zjednodušení souhrnně označovány jako průmyslové řídicí systémy – ICS. Tyto systémy se v posledních několika desetiletích dramaticky proměnily: od izolovaných proprietárních systémů se sériovými sběrnicemi k současným vysoce propojeným a geograficky rozsáhlým soustavám, které využívají běžně dostupné (COTS) produkty, Ethernet a internetový protokol (IP). Propojení dvou světů, informační a provozní techniky (IT a OT), umožňuje provozovatelům dosáhnout výrazného zvýšení produktivity a úspory nákladů. Další zvýšení produktivity je očekáváno s rostoucím uplatněním mobilních zařízení, virtualizace a cloudových služeb.

1.2 Nové kybernetické hrozby pro ICS

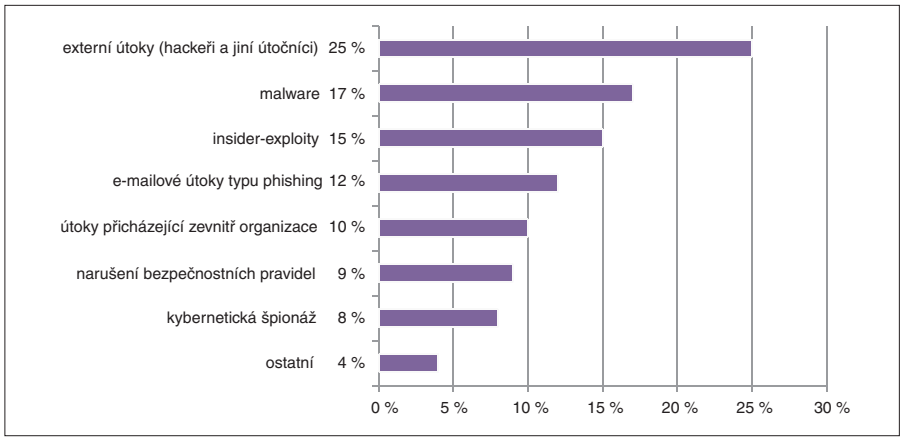
Z ekonomického hlediska je integrace IT-OT pro mnoho podniků velmi výhodná. Ovšem spolu s ní přichází i větší ohrožení různými kybernetickými útoky, které mohou snížit dostupnost zařízení, bezpečnost technologických zařízení a integritu provozních dat. Podniky tedy musí hodnotit své řídicí systémy i z pohledu, jak jsou schopny se bránit kybernetickým hrozbám.

Některé z těchto hrozeb jsou specifické jen pro komponenty ICS, jiné jsou relevantní pro IT i OT. Některé mohou pocházet ze zdrojů uvnitř podniku, jiné přicházejí zvenčí. Mohou to být náhodné incidenty i záměrné útoky. Na *obr. 1* jsou nejdůležitější vektory hrozeb podle průzkumu Institutu SANS z roku 2014 [1].

První veřejně známý virus zařaditelný do první skupiny externích útoků cílených na ICS byl Stuxnet. Využíval aplikace a soubory COTS a slabiny v softwaru určeném speciálně pro ICS. Cílem tohoto viru bylo vyřadit z provozu íránské zařízení na obohacování uranu. Skutečně se podařilo poškodit speciální odstředivky, jež jsou součástí tohoto zařízení, a poprvé tak došlo k útoku v průmyslovém kyberfyzickém prostoru. Ačkoliv Stuxnet byl již velmi důmyslný, profesionálně navržený virus, od té doby je možné pozorovat další růst propracovanosti útoků na ICS. Zpráva o útoku zvaném Energetic Bear hovoří o dvou nových metodách použitých k útoku na ICS [2]. První využívá malware ukrytý v balíčku softwaru pro ICS,

[1)] *Pozn. red.*: Pro odlišení funkční bezpečnosti a bezpečnosti strojů a zařízení (*safety*) od zabezpečení systémů (*security*, popř. *cyber security*) používáme pro *security* termíny zabezpečení, popř. kybernetická bezpečnost.

který si uživatel stáhne z webové stránky dodavatele. Dále je využívána znalost protokolu ICS, aby útočník získal přehled o prostředí dotčené organizace. Nebezpečí tkví nejen v průmyslové špionáži, ale také v tom, že prostřednictvím takto získaných znalostí lze ICS na dálku sabotovat.



Obr. 1. Nejdůležitější vektory hrozeb pro ICS (SANS ICS Survey 2014)

Další kategorií útoků jsou útoky typu phishing nebo obecněji útoky využívající sociální inženýrství. Patří sem jak útoky typu *watering hole*, kdy jsou infikovány stránky, jež jsou obětí útoku často navštěvovány, tak také např. zanechání lákavě vypadajícího infikovaného USB-sticku ve veřejně přístupných prostorách firmy, např. v recepci nebo na parkovišti. V podstatě všechny moderní útoky cílené na koncová zařízení využívají některé metody sociálního inženýrství. Například Stuxnet se šířil prostřednictvím USB-sticků, aby tak infikoval notebooky pracovníků inženýrských firem. Energetic Bear používal důmyslnější kombinaci cíleného *phishingu* (tzv. *spearphishingu*, kdy útočník pro zvýšení důvěryhodnosti používá informace, které shromáždil o své oběti), útoku *watering hole* a trojských koní. Například v rámci soustředěného spearphishingového útoku na petrochemické podniky v Norsku v srpnu 2014 [3] bylo potvrzeno padesát útoků na podniky, včetně největšího StatOil. To dokládá, že pro organizované hackery jde o základní metodu, jak se snaží proniknout do sítí provozovatelů kritické infrastruktury.

Kromě virů a phishingu je další velkou hrozbou průnik malwaru do ICS. K tomu může dojít i náhodně – stačí, když se osoba, která má k ICS přístup, připojí infikovaným mobilním zařízením nebo použije infikované přenosné paměťové zařízení. Zdrojem infekce počítačovými červy mohou být také stránky důvěryhodných dodavatelů či partnerů. Ať už jde o malware záměrný nebo nezamýšlený, může způsobit nákladné odstávky nebo bezpečnostní incidenty. Ztráty ve výrobě mohou být mnohamilionové, nehledě na možná zranění, ztráty na životech nebo poškození životního prostředí.

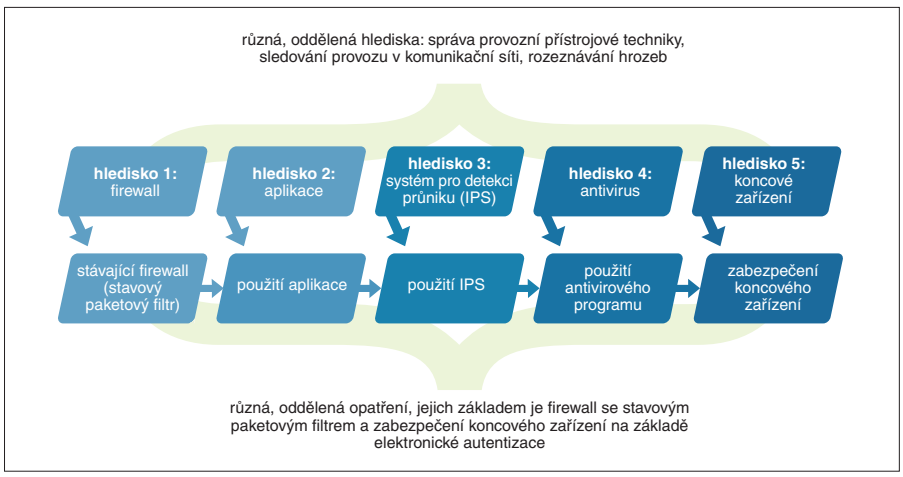
Velmi vážnou hrozbou se ukazuje být také využití exploitů navržených vlastními pracovníky – odborníky na ICS. Exploit je program, který využívá slabé místo softwaru nebo programátorskou chybu, a jeho účelem je, aby autor exploitu získal přístup do systému nebo vyšší uživatelská práva, než mu příslušejí. Veřejně známý je tzv. incident Maroochy Shire [4]. Nespokojený zaměstnanec dodavatele ICS, který řídí systém odvodu splaškových vod v rekreační oblasti Maroochy Shire v Austrálii, využil své hluboké znalosti řídicího systému a nezabezpečenou bezdrátovou síť a jako pomstu za jednání svého zaměstnavatele způsobil únik 800 000 litrů splaškových vod, která se rozlila po místních parcích, v okolí hotelů a pronikla i do řeky. Způsobil tak výraznou škodu na životním prostředí.

Jestliže se provozovatel technologického zařízení sám nebojí kybernetických útoků, může mu ochranu před nimi nařídit stát. V mnoha státech (*pozn. red.:* včetně ČR) již existují zákony o kybernetické bezpečnosti, které stanovují postihy pro ty organizace z oblasti kritické infrastruktury, které nesplňují regulatorní požadavky. Například v USA a Kanadě se v oboru elektrických rozvodných sítí používají standardy NERC CIP (*North American Electric Reliability Corporation – Critical Infrastructure Protection*). Chemické podniky v USA zase používají standardy CFATS (*Chemical Facility Anti-Terrorism Standards*). Jedním z nejnovějších standardů je NIST CSF (*National Institute of Standards and Technology – Cyber-Security Framework*), kterému podléhají vládní agentury, ale současně je i dobrovolným referenčním standardem pro posuzování kybernetické bezpečnosti v průmyslových podnicích.

1.3 Jaká je připravenost podniků na kybernetické hrozby?

V souvislosti s diskusí o kybernetických hrozbách se objevuje velmi důležitá otázka, kterou si musí průmyslové firmy položit: jak je jejich ICS proti těmto hrozbám chráněn? Je třeba se zamyslet nad těmito otázkami:

- Je komunikace v síti dostatečně transparentní, aby bylo možné co nejdříve detekovat podezřelé akce? Jak snadné je získat informace o provozu na síti?
- Používá se dostatečně silný systém pro kontrolu přístupu, který efektivně omezuje vnější i vnitřní vektory útoků, a přitom nemá negativní vliv na výkonnost ICS? Jak jednoduché je spravovat přístupová práva?
- Jak je stávající ICS, který pravděpodobně nelze aktualizovat, chráněn před exploity a malwarem a jak jsou zajištěna jeho slabá místa? Lze nějak omezit doby odstávek způsobených kybernetickými incidenty nebo nutností aktualizovat software?
- Je podnik připraven čelit kybernetickému útoku, který využívá zatím neznámé viry a malware?
- Jsou systémy ochrany koncových zařízení a komunikační sítě oddělené, nebo spolupracují, aby lépe ochránily podnik před útoky?
- Splňuje systém kybernetické bezpečnosti příslušné standardy, nebo je dokonce překračuje?
- Jestliže se používají moderní prvky jako mobilní zařízení nebo virtualizace, je zajištěna jejich kybernetická bezpečnost, nebo jsou slabým místem obrany?



Obr. 2. Typická konfigurace zabezpečení ICS

1.4 Slabá místa ICS z hlediska bezpečnosti

Řídicí systémy používané podniky působícími v kritické infrastruktuře již nyní mají určitou úroveň kybernetické bezpečnosti. Je ovšem ještě mnoho podniků, zvláště v těch oblastech průmyslu, kde není silný tlak regulatorních orgánů, jejichž dosavadní ICS jsou proti současným kybernetickým nebezpečím chráněny velmi slabě. Na *obr. 2.* je ukázána typická konfigurace zabezpečení, používaná mnoha současnými podniky.

Z hlediska zabezpečení sítě používají stávající systémy stavové firewally, tj. firewally se stavovými paketovými filtry, které pracují na síťové a transportní vrstvě, ale nevidí do vrstvy aplikační a neumožňují uživatelsky řízenou kontrolu přístupu, která je nezbytná pro efektivní detekci anomálií v komunikaci. Firmy se snaží slabá místa upravit četnými, ale vzájemně oddělenými řešeními, jako jsou systémy pro prevenci průniku (IPS – *Intrusion Prevention Systems*) nebo antivirové programy. Je zde ovšem značné riziko špatné konfigurace jednotlivých systémů, nekonzistence informací, snížení výkonnosti ICS a zvýšení nákladů, a to jak pořizovacích, tak provozních. Ke všem těmto nevýhodám přibývá ještě to, že existující systémy pro ochranu koncových zařízení nespolupracují se systémy pro zabezpečení sítě a zpravidla si poradí jen s těmi útoky, které už jsou známé a mají typické projevy. Nejsou schopny zařízení ochránit před dosud neznámými exploity nebo před napadením dosud neznámým malwarem. Systémy kybernetického zabezpečení ICS by si však měly poradit i s útoky typu *zero day*. Postupné doplňování a aktualizace takovýchto systémů skládajících se z oddělených komponent jsou nesmírně organizačně náročné, a zabezpečení ICS se proto stává velmi složitým úkolem.

(pokračování příště)

Literatura:

[1] LUALLEN, M.: *Survey on Industrial Control Systems Security* [on-line]. SANS Institute, 2014. Advisor: Harp, D. [cit. 27. 1. 2016]. Dostupné z: <http://ics.sans.org/media/sans-ics-security-survey-2014.pdf>

[2] HENTUNEN, D. – TIKKANEN, A: *Havex Hunts for ICS/SCADA Systems* [on-line]. F-Secure, 2014. [cit. 27. 1. 2016]. Dostupné z: <www.f-secure.com/weblog/archives/00002718.html>

[3] BERGLUND, N.: *Oil Industry Under Attack by Hackers* [on-line]. NewsInEnglish.no, 2014. [cit. 27. 1. 2016]. Dostupné z: <www.newsinenglish.no/2014/08/27/oil-industry-under-attack-by-hackers>

[4] WEISS, J. – ABRAMS, M.: *Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia* [on-line]. CSRC NIST, 2008. [cit. 27. 1. 2016]. Dostupné z: <http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf>

Mario Chiock, American Petroleum Institute, Del Rodillas, Palo Alto Networks

krátké zprávy

Integrace robotů COMAU do automatizačních systémů B&R

Firmy COMAU a B&R uvádějí novou funkci openRobotics, která vede k novému pojetí integrace robotů do řízení strojů a zařízení. Výrobce robotů Comau tím chce usnadnit začlenění kompletního sortimentu robotů s užitečným zatížením v rozmezí od 3 do 650 kg.

Místo dosavadního přístupu, kdy jsou pro roboty a pro stroj nezbytné samostatné řídicí systémy nebo brány, lze s použitím funkce openRobotics začlenit libovolný robot Comau do ostatního strojního vybavení provozu nebo výrobní linky, pokud jsou vybaveny automatizačními komponentami společnosti B&R. „Zákazník jednoduše zvolí příslušný robot Comau v softwaru automatizace Automation Studio a poté může pomocí mapp Technology tento robot integrovat do automatizace strojů a dokonale jej synchronizovat," vysvětluje Walter Burgstaller, obchodní ředitel pro Evropu společnosti B&R. „Toho nelze dosáhnout prostřednictvím obvyklých a často náročných řešení pomocí rozhraní."

Jednotné programování všech komponent v provozu včetně robotů dovoluje využívat ucelené koncepce diagnostiky, ovládání a údržby.

(ev)