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)