Tři zranitelná místa v zabezpečení průmyslových sítí

Zařízení v průmyslové automatizaci mají vliv na velmi cenný majetek, a přesto se na zabezpečení průmyslových komunikačních sítí velmi často zapomíná. V minulosti se provozovatelé průmyslových systémů mnohdy spoléhali na fyzické zabezpečení svých zařízení izolací od jiných sítí pomocí „vzduchové mezery“ nebo na relativní nesrozumitelnost unikátních protokolů. Nyní v měnícím se a více propojeném světě si již provozovatelé automatizačních komunikačních sítí začínají uvědomovat, že musí čelit novým hrozbám. V nedávné zprávě vypracované pro americké ministerstvo vnitra nalezla bezpečnostní konzultační společnost InfraCritical 500 000 nezabezpečených zařízení se systémy SCADA jen pomocí vyhledávače. 7 200 takto nalezených zařízení bylo určeno pro řízení kritické infrastruktury, jako jsou vodovody, energetika a další služby. Není divu, že konzultanti charakterizovali stav zabezpečení informačních a řídicích systémů jako „směšný“.

Mnohé průmyslové podniky si ani nejsou vědomy rizika, kterému jsou vystaveny jejich systémy na internetu. Prvním a nejdůležitějším krokem pro jejich zabezpečení je přitom vůbec uznat existenci rizika. Ale stejně důležitý je i druhý krok, komplexní odstranění zranitelných míst sítě. Automatizační komunikační sítě přitom mají tři specifické typy zranitelných míst.

Zabezpečení protokolu Modbus TCP je obtížné

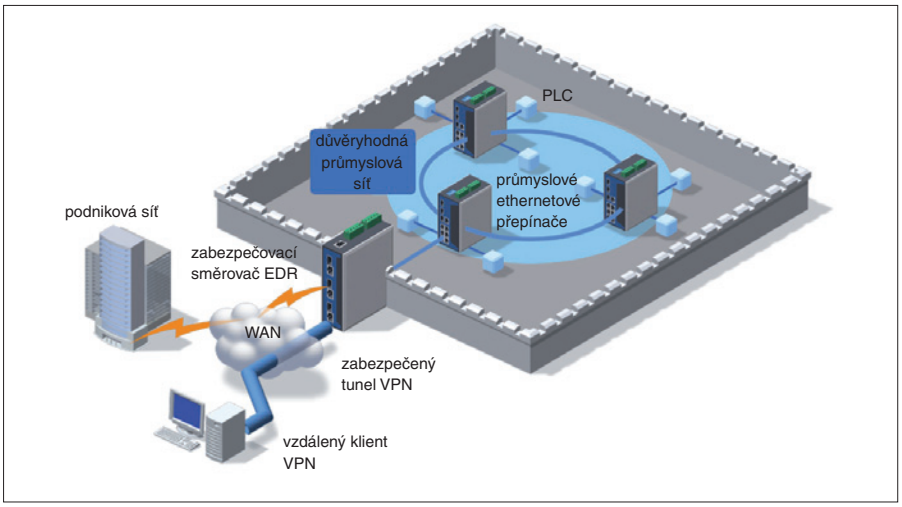
Průmyslové sítě, které přešly na ethernetovou komunikaci TCP/IP na transportní, síťové a spojové vrstvě, většinou používají na aplikační vrstvě specializované průmyslové protokoly. Nejpoužívanější z nich, Modbus TCP, je velmi zranitelný, přestože je široce používán v průmyslových komunikacích bez jakéhokoliv zabezpečení.

Paket, který se zdá být korektní při inspekci paketů TCP/IP, např. při kontrole zdrojové IP adresy, může ve skutečnosti obsahovat závadná data. Tato skutečnost by byla odhalena, kdyby bylo možné filtrovat pakety podle zdrojového ID zařízení v síti Modbus, funkčního kódu nebo jiného parametru protokolu Modbus. Vzhledem k tomu, že průmyslová zařízení jen zřídka mívají možnost zabezpečit aplikační vrstvu, jsou pro zajištění této důležité chybějící ochrany zapotřebí další zabezpečovací zařízení, např. firewally. Jenže běžné firewally málokdy dokážou hloubkově kontrolovat pakety protokolu Modbus TCP.

Průmyslové aplikace jsou časově kritické a netolerují zpoždění přenosu

Systémy SCADA a průmyslové řídicí systémy přímo řídí skutečné stroje a zařízení a často musí pracovat v reálném čase. Například na montážní lince musí všechny stroje pracovat v naprosté koordinaci, aby na sebe jednotlivé operace dokonale navazovaly. Provoz elektrických rozvoden je ještě citlivější na synchronizaci, protože zpoždění při spouštění obvodu přepínače může způsobit kolísání výkonu, nebo dokonce i výpadek.

Časově kritický charakter průmyslových provozů znamená, že průmyslové sítě musí být schopny pracovat v reálném čase. Nicméně běžné útoky DoS (*Denial of Service*), způsobené narušitelem nebo jen chybou pro-



Obr. 1. Zjednodušená struktura průmyslové sítě se zabezpečeným lokálním a dálkovým přístupem

gramu, vedou k přetížení sítě záplavou požadavků, a jestliže není firewall schopen blokovat neoprávněné požadavky, mohou mít vliv na zpoždění komunikace v síti.

Druhým problémem může být omezení šířky pásma, jestliže firewall nemá dostatečný výkon pro zpracování paketů, a stává se tak úzkým místem komunikace. To nebýval problém, když průmyslové sítě přenášely jen data nutná pro řízení. Problém vzniká až s tím, jak je do těchto sítí integrován přenos obrazu a zvuku. Přenos dat z kamer zabírá velkou šířku přenosového pásma a síťová zabezpečovací zařízení musí mít dostatečnou kapacitu, aby přenos velkého objemu dat nezpůsobil nepřípustné zpoždění.

Zabezpečovací zařízení nejsou vhodná do náročného průmyslového prostředí

Průmyslová zařízení a řídicí systémy jsou umístěny v náročnějších provozních podmínkách než většina běžných síťových zařízení v komunikačních a informačních systémech. To může být potenciálním zdrojem neshody mezi odolností průmyslových zařízení a zařízením pro zabezpečení sítě, které je chrání. Nepříznivé vlivy prostředí, jako jsou extrémní teploty nebo elektromagnetické rušení, mohou být pro síťová zařízení nebezpečnější než potenciální útočník.

Zabezpečení průmyslových gigabitových ethernetových sítí technikou Moxa

Společnost Moxa zkombinovala své zkušenosti v oblasti průmyslové automatizace se svými odbornými znalostmi v oblasti komunikačních sítí. Moxa EDR-810 (*obr. 2*) je průmyslový víceportový zabezpečovací směrovač (*router*), který obsahuje bezpečnostní funkce specificky optimalizované pro zabezpečení průmyslových komunikačních sítí. Kromě funkce VPN, která vytváří šifrovaný datový tunel pro vzdálený přístup, NAT pro skrytí IP adres lokálních zařízení a firewallu pro filtraci paketů, přidává EDR-810 funkce „šité na míru“ průmyslové automatizaci, jako jsou hloubková inspekce paketů protokolu Modbus TCP nebo velká šířka přenosového pásma.

Obr. 2. Zabezpečovací komunikační směrovač EDR-810 vhodný do průmyslových podmínek

PacketGuard™ je první funkce pro integrovanou inspekci paketů protokolu Modbus TCP. EDR-810 používá funkci PacketGuard pro kontrolu síťových paketů na všech úrovních až po aplikační vrstvu protokolu Modbus. Běžné síťové firewally přitom dokážou pakety kontrolovat jen na transportní vrstvě.

EDR-810 slučuje několik portů do jedné gigabitové ethernetové linky s mimořádně malým zpožděním, které je akceptovatelné i pro průmyslové provozy, a to i v úlohách extrémně náročných na šířku pásma, jako je např. přenos dat z IP kamer.

EDR-810 tedy kombinuje funkci směrovače i manažovatelného přepínače (*switch*) s funkcí firewallu s hloubkovou inspekcí paketů, NAT a VPN do jediného zařízení, což je velmi pohodlné a cenově efektivní pro ochranu velkého počtu zařízení.

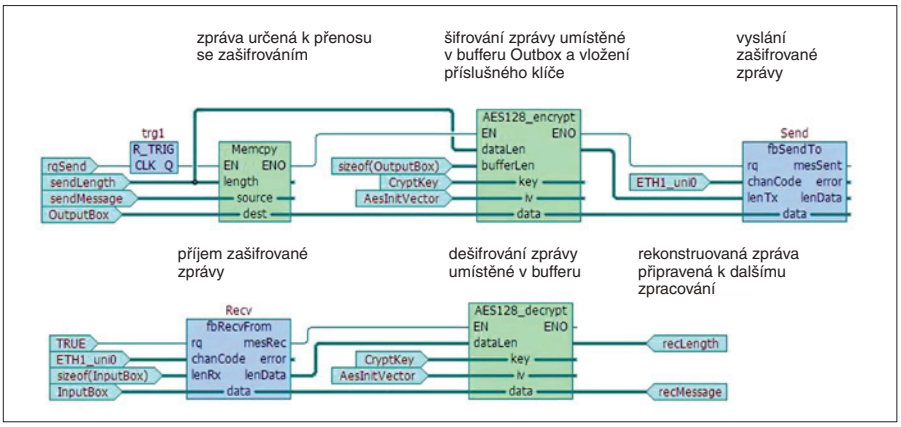
EDR-810 je nejnovější člen sortimentu zabezpečovacích síťových zařízení EDR přizpůsobených pro průmyslové subjekty. Široký rozsah provozních teplot, odolný kovový kryt a velká odolnost proti elektromagnetickému rušení umožňují zabezpečovacím zařízením Moxa EDR odolávat drsným podmínkám průmyslových provozů stejně jako ostatní robustní zařízení v průmyslových sítích.

Dodavatelem ethernetových zabezpečovacích směrovačů Moxa a dalších zařízení pro průmyslovou komunikaci je společnost ELVAC, a. s. Podrobnější informace mohou zájemci najít na internetových stránkách www.moxa.cz.

(ELVAC, a. s.)

Pokročilé šifrovací funkce pro Tecomat

Bezpečnost přenosu dat je aktuální problém při řízení technologických procesů, ale i v technice budov. Jednou z důležitých úloh zabezpečení přenášených dat je jejich šifrování. Pro programovací systém Mosaic pro systémy Tecomat byla vytvořena nová knihovna funkčních bloků s názvem encryptLib (www.tecomat.cz). Jejími funkčními bloky lze realizovat pět funkcí, které může uživatel použít ve svém aplikačním programu, potřebuje-li zvýšit zabezpečení přenášených dat. Jde především o šifrování podle symetrické blokové šifry AES128 s klíčem v délce 128 b. Šifra je (mimo jiné) od roku 2002 používána jako federální standard v USA. Je využívána i v protokolu Wireless Mbus nebo v sítích WiFi (jako zabezpečení WPA2). V knihovně jsou k dispozici funkční bloky pro šifrování i dešifrování (*obr. 1*). Dále je k dispozici funkce s proudovou šifrou RC4, která je součástí běžně používaných šifrovacích protokolů (SSL/TLS pro HTTPS nebo WEP a WPA pro bezdrátové sítě). Lze realizovat i funkci SHA (*Secure Hash Algorithm*) – rozšířenou hašovací funkci, která ze vstupních dat vytváří jednoznačný výstup (otisk) fixní délky, z nějž nelze rekonstruovat původní data, ale je možné ji použít pro zaručení integrity zprávy nebo autentizaci. Poslední je dvojice funkcí Base64_encode a Base64_decode, které převádějí libovolná binární data na řetězce znaků ASCII. Data je potom možné přenášet prostřednictvím kanálů určených pouze pro přenos textových dat, např. v e-mailech nebo sms.



Obr. 1. Ukázka části programu pro Tecomat Foxtrot s šifrováním a dešifrováním šifrou AES128, vytvořeného v systému Mosaic v grafickém editoru jazyka CFC

Ing. Jaromír Klaban, Teco, a. s.