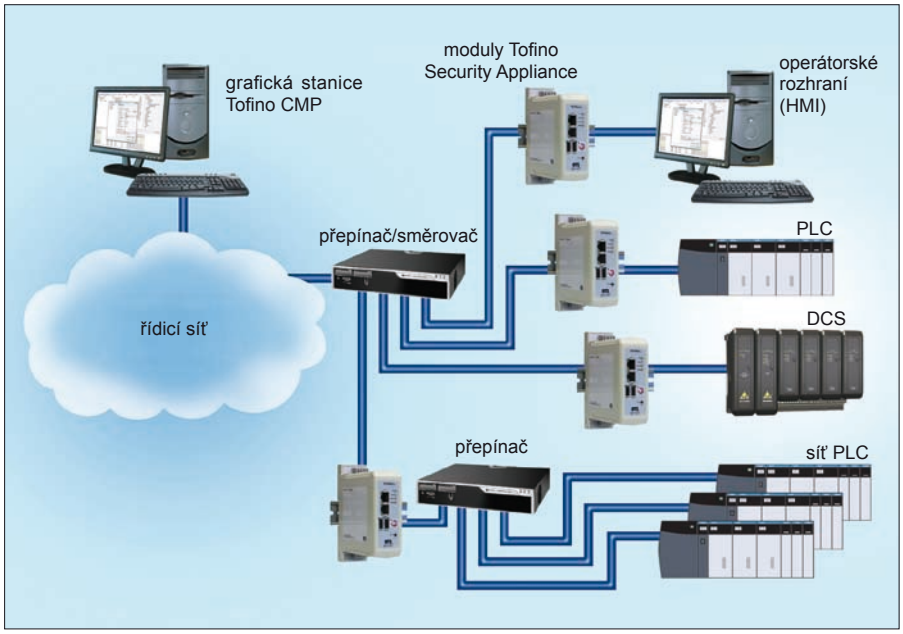
Tofino chrání průmyslové řídicí systémy

Za poslední desetiletí u řídicích systémů zdomácněly prvky informační techniky (IT) jako např. Windows, Ethernet, TCP/IP nebo webové rozhraní. To je bohužel příčinou toho, že řídicí systémy typu programovatelných automatů (PLC) a distribuovaných řídicích systémů (DCS) i monitorovací a dispečerské systémy (SCADA) jsou nyní vystaveny nebezpečí útoků virů, hackerů i teroristů z celého světa.



Obr. 1. Princip systému Tofino Security Solution

Slavný vojenský stratég Clausewitz kdysi řekl: „Pokud se budete bránit nepříteli tím, že se schováte za silné opevnění, donutíte jej k tomu, aby našel jiné řešení a toto opevnění obešel.“ Nepřátelé moderních řídicích systémů na bázi Ethernetu – hackeři nebo tvůrci virů – si najdou cestu, jak obejít firewall a dostat se do řídicího systému, jestliže k tomu dostanou příležitost.

Svět IT došel k uvedenému poznání velmi nákladným způsobem. Po letech milionových ztrát způsobovaných zavirovanými servery a pracovními stanicemi je teď od útvarů IT v podnicích vyžadováno, aby používané osobní počítače měly vlastní „hloubkovou obranu“ v podobě antivirových programů a firewallů, ať už jsou přitom chráněny podnikovým firewallem nebo ne.

Nesnáze s ochranou řídicích systémů

Vytvořit hloubkovou obranu řídicích systémů charakteristických pro svět automatizační techniky je ovšem problém. Ačkoliv se jejich projektanti snaží oddělit řídicí systém od okolního světa, 100% ochrana není dlouhodobě udržitelná. Tradiční firewally jsou příliš složité na to, aby je bezpečnostní odborníci správně nakonfigurovali, spustili a udržovali v provozu podle specifických potřeb řídicího systému.

Řídicí systémy nenabízejí možnost ochrany ověřováním oprávnění k přístupu nebo zajištěním jejich fyzické nedostupnosti. Mohou tedy být ovládány kýmkoliv, kdo se na ně připojí. Neexistuje ani možnost vyspravit odhalená slabá místa, jak je to běžné u osobních počítačů. Miliony řídicích systémů tak zůstávají otevřeny útokům hackerů, kteří ani nemusí být příliš zkušení.

Dalším problémem je samotné umístění řídicích systémů. Zatímco některé jsou nainstalovány ve výrobních závodech, jiné jsou provozovány na odlehlých lokalitách a obsluhovány pracovníky, kteří o problematice informační bezpečnosti a odpovídajících bezpečnostních technikách nevědí téměř nic.

Tofino Security Solution

Z uvedených důvodů přicházejí firmy MTL Instruments a Byres Security s integrovaným hardwarově-softwarovým řešením pro ochranu průmyslových sítí zvaným Tofino Security Solution. V názvu je použito jméno podle slavné surfové pláže Tofino v Britské Kolumbii. Průmyslové bezpečnostní řešení Tofino™ nabízí zajištění bezpečnosti řídicích systémů rozmístěním bezpečnostních prvků před každým řídicím systémem nebo skupinou systémů, které vyžadují ochranu. Vytváří se tím hloubková obranná strategie. Jestliže se tedy hackerovi podaří překonat hlavní podnikový firewall nebo jiný bezpečnostní prvek, narazí na další bezpečnostní prvky, bez jejichž překonání nemůže zasáhnout do funkce řídicího systému.

Kompletní systém Tofino Industrial Security Solution se skládá ze čtyř základních stavebních prvků. Jsou to (*obr. 1*):

- *Tofino Security Appliance*, což je vlastní fyzický modul v průmyslovém provedení určený k instalaci v blízkosti komunikačních přístrojů, které používají Ethernet nebo sériovou linku,
- *Tofino Loadable Security Modules* (LSM), to jsou různé softwarové bloky realizující zabezpečovací funkce, jako např. firewally, detektory narušení a kódování ve virtuálních privátních sítích (VPN); tyto bloky se nahrají do modulu Security Appliance,
- *Tofino Central Management Platform* (CPM), databázový systém určený pro tvůrce daného bezpečnostního systému k monitorování a konfigurování každého jeho bezpečnostního prvku; systém CPM se může nacházet kdekoliv v síti,
- grafická stanice určená specialistům k přístupu k CPM, a tím i k celému systému Tofino Industrial Security Solution na dálku.

Systém Tofino je něco jako osobní firewall a systém detekce narušení pro operátorské stanice, PLC, DCS a jednotky I/O. Fyzický modul Tofino Security Appliance se zapojí do průmyslové sítě před jednotku, kterou je třeba chránit, a jeho software následně vyhledá v databázi slabá místa této jednotky a nastaví se na její ochranu. Rozumí protokolům SCADA a jiných řídicích systémů, takže dokáže zabránit neautorizovaným zásahům, aniž by narušil průchod platných příkazů.

Systém Tofino Security Solution chrání technologické zařízení tím, že nejdůležitějším prvkům v systému řízení (PLC, DCS, HMI) poskytuje takovou úroveň hloubkového zabezpečení, jakou poskytuje útvar IT každému osobnímu počítači v podniku.

Systém Tofino umožňuje odborníkům na řídicí systémy věnovat se plně své odbornosti a nemuset se zabývat otázkami kódování dat či ochrany sítě před neoprávněným přístupem.

Jaromír Uher,
D-Ex Limited, spol. s r. o.

[Zpracováno podle materiálů Byres Security, Inc., a MTL Instruments Plc.]