Jak zabezpečit průmyslovou síť před kybernetickými útoky

Průmyslové technologie IP přinášejí do průmyslové automatizace řadu výhod, ale jejich využití rovněž způsobuje zvýšení bezpečnostních rizik. V minulosti se provozovatelé sítí, které byly součástí průmyslové automatizace, mohli domnívat, že jejich sítě jsou bezpečné, protože použité proprietární sériové technologie komunikace nebyly propojeny s okolním světem. Tento pohled na bezpečnost byl vždy poněkud iluzorní, ale moderní průmyslová automatizace se přesunula do IP ethernetových sítí, u kterých si provozovatelé aplikací nemohou dovolit ani podobné iluze o zabezpečení sítě.

Bezpečnostní hrozby jsou v IP sítích velmi reálné a mohou mít pro automatizační systémy katastrofální důsledky. V některých ohledech jsou průmyslové sítě ještě zranitelnější než podnikové IT sítě. Pokud dojde k výpadku IT sítě, může být ovlivněna produktivita zaměstnanců v kancelářích, protože ztratí přístup k Internetu. Na druhou stranu při poruše komunikace v průmyslové automatizaci může dojít k vážným škodám a značným materiálním ztrátám, pokud je průmyslový proces nečekaně přerušen nebo dojde k dlouhé odstávce montážní linky.

Bezpečnostní rizika a požadavky trhu

Že je zranitelnost průmyslové IP sítě velmi reálná, dokazuje nedávná studie CERN (The European Organization for Nuclear Research), která zjistila, že pouze 66 % PLC bylo schopno odolat jednoduchým útokům provedeným volně dostupnými hackerskými nástroji, jako jsou Netwox nebo Nessus. Ani prosté oddělení sítě od vnějšího světa není dostačující. Výzkum společnosti AT&T zjistil, že většina bezpečnostních útoků na sítě pochází od vnitřních uživatelů se zlými úmysly. V samostatné studii amerického ministerstva vnitřní bezpečnosti z roku 2007 byl proveden experimentální kybernetický útok, který měl za následek zničení generátoru.

Ohrožení průmyslových systémů není pouze hypotetické. Databáze průmyslových bezpečnostních incidentů zaznamenala nespočet prostupů do SCADA systémů, ke kterým často došlo u důležitých zařízení, jako jsou čistírny odpadních vod, elektrárny nebo chemické provozy. V současné době si trh začíná uvědomovat tyto hrozby a počítačová bezpečnost se stává hlavní prioritou. Velcí zákazníci nyní staví požadavky na počítačovou bezpečnost na přední místo, a proto byl vytvořen standard ISO99 schválený společností

Obr. 1 Průmyslový zabezpečovací router Moxa EDR-G903

ANSI (The International Society for Automation), který přesně popisuje prvky kybernetického zabezpečení. Ve veřejném sektoru a vládních institucích vznikají vlastní normy, jako jsou NERC-CIP a CPNI, definující postupy pro zabezpečení sítě. Zabezpečení sítě je důležité například při těžbě a distribuci plynných a kapalných paliv, v chemickém průmyslu, energetice a dalších systémech, které si nemohou dovolit být ohroženy útočníky.

Za účelem ochrany své sítě se provozovatelé průmyslové automatizace spoléhají na kombinaci firewallu a virtuálních veřejných sítí (VPN). Firewall je bariéra, která brání přístupu neoprávněných zařízení do systému. Firewall kontroluje příchozí komunikaci a ověřuje, že pochází z autorizovaného zdroje. VPN slouží k vytvoření tunelu pro bezpečnou privátní komunikaci ze vzdálených zařízení v síti WAN bez zabezpečeného přístupu do průmyslové sítě.

Bezpečnost bez kompromisů

Zabezpečení sítě v průmyslových automatizačních systémech míří k dosažení dvou cílů. Bohužel se u těchto cílů někdy stává, že stojí proti sobě. Zaprvé musí síťové zabezpečení chránit systém a jeho kritické prvky před neoprávněným přístupem. Zadruhé ale systém síťového zabezpečení musí pracovat tak, aby neohrožoval průmyslové provozy.

Skloubení těchto dvou cílů může být obtížnější, než se na první pohled zdá. Například routery s aktivními firewally často trpí výkonovými omezeními. Pokud si router není schopen ověřit všechny pakety dostatečně rychle a podávat adekvátní výkon, nastane vyšší latence a propustnost sítě bude trpět. Časově závislé průmyslové procesy mívají požadavky na minimální výkon, aby fungovaly spolehlivě.

Zabezpečení sítě může taky narušit její normální provoz zavedením dalších architektonických požadavků. Podle nejlepších bezpečnostních zkušeností by mělo být nasazeno více firewallů mezi jednotlivými síťovými vrstvami. Tato „hloubková ochrana“, přináší větší celkovou bezpečnost v porovnání se systémem, který se spoléhá na ochranu před průnikem do sítě jen v jedné vrstvě.

Bohužel, i když jsou bezpečnostní doporučení důkladně dodržovány a je využito několika bezpečnostních firewallů, může každý zabezpečovací prvek znamenat velké komplikace v průmyslové síti, zejména na úrovni zařízení. Důvod je ten, že zařízení jsou obvykle nakonfigurována na provoz ve stejné podsíti, ale firewally určené pro provoz v IT prostředí jsou obvykle určeny pro ochranu samostatné podsítě a pracují jako „router mode“ firewally. Tato architektura může být problematická zejména pro řídicí systémy, které jsou konfigurovány pro provoz ve stejné podsíti jako I/O zařízení. Není jednoduché překonfigurovat průmyslové řídicí systémy pro provoz ve dvou podsítích tak, aby to vyhovovalo „router mode“ firewallům.

Další unikátní vlastností topologie mnoha průmyslových sítí je redundance. Vzhledem k tomu, že průmyslové sítě musí pracovat na vyšší úrovni spolehlivosti než podnikové sítě, využívá mnoho průmyslových sítí redundance komunikace a přenosového média. Každá komunikační cesta má také záložní cestu, která může být automaticky aktivována při přerušení primární cesty. Nicméně, komunikační redundance zdvojnásobuje počet firewallů, které jsou potřeba, protože záložní cesta taky potřebuje firewall, i když není používána.

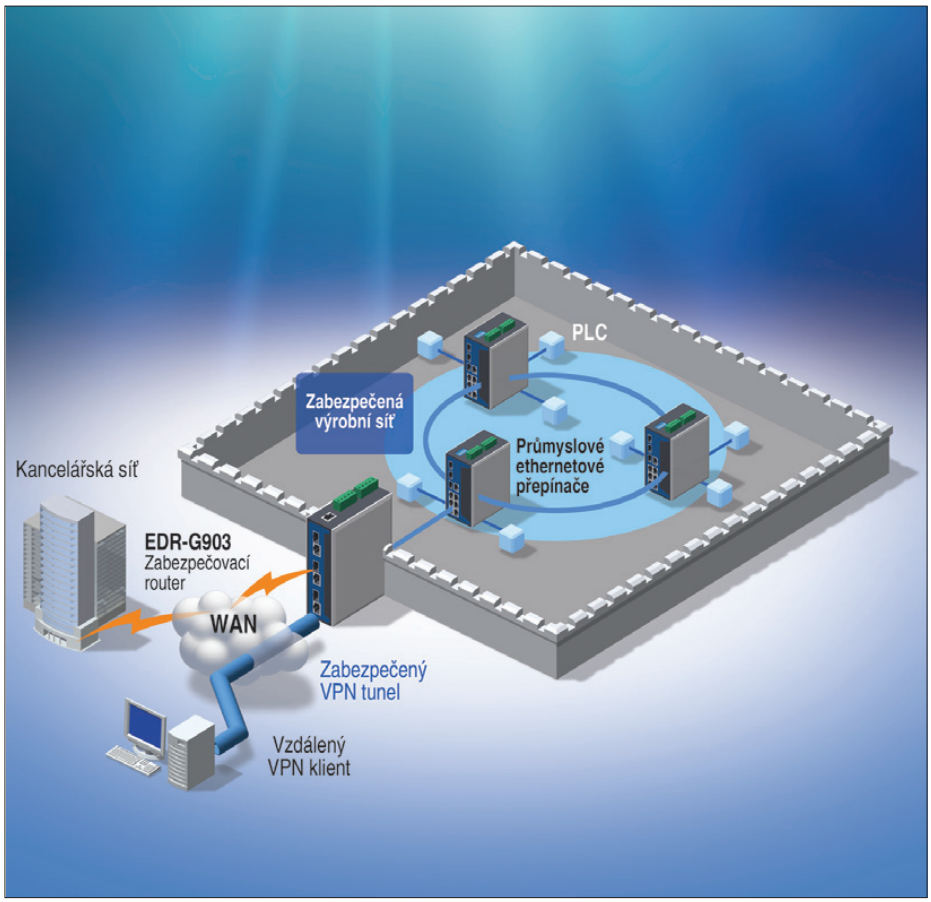
Nakonec není bezpečnost jediným požadavkem na průmyslové firewally/ VPN brány, ale musí se zajistit také dostatečný výkon pro pod-

poru časové závislých průmyslových procesů a musí být kompatibilní s průmyslovými síťovými konfiguracemi. Mnoho běžných IT bezpečnostních řešení, a to i těch které vznikly v podnikovém prostředí, má problémy splnit vyšší nároky průmyslových automatizačních sítí.

Síťová bezpečnost pro průmyslovou automatizaci

Chtějí-li provozovatelé výkonných průmyslových sítí provést jejich zabezpečení, měli by se zaměřit na zařízení vyhovující jejich specifickým potřebám. Nejprve je třeba si ověřit, že zabezpečovací síťové prvky zachovávají přiměřený výkon sítě a jejich bezpečnostní funkce splňují všechny požadavky průmyslového automatizačního systému. Router, který má vysokou latenci nebo omezuje propustnost sítě, není pro citlivou oblast průmyslové automatizace použitelný. Kromě toho je možné realizovat zabezpečení sítě bez její složité konfigurace, a to díky funkcím známým jako "bridge mode", která je podporována některými produkty.

„Bridge mode" umožňuje provoz firewallu pouze v jedné podsíti, což je ideální pro průmyslové sítě. Všechna zařízení umístěná v podsíti si mohou zachovat svou stávající konfiguraci a nový firewall může být začleněn do stávající sítě. Průmyslové procesy pak mohou využívat všech výhod zvýšené bezpečnosti, bez jakékoli změny konfigurace zařízení.



Obr. 2 Řešení bezpečného přístupu do výrobní sítě přes Internet ze vzdáleného pracoviště s využitím zabezpečovacího routeru

Mód „Dual WAN" je další vlastnost, která ušetří provozovatelům sítí mnoho komplikací při zvyšování zabezpečení sítě. Duální WAN mód umožňuje bezpečnostnímu routeru zdvojené připojení a ochranu dvou WAN linek najednou. Firewall/router s duálním WAN módem může chránit jak primární, tak i záložní spojení používané v průmyslových sítích.

Na závěr ještě jedna typická vlastnost aplikací v průmyslové automatizaci. Jsou jí extrémní provozní podmínky charakteristické velkými změnami teploty a datovými přenosy na velké vzdálenosti. IT zařízení nejsou pro provoz například v podmínkách výrobních hal vhodné. Průmyslové routery/firewally mají odolný design navržený právě pro provoz v extrémních podmínkách s širokým rozsahem teplot a komunikaci po optických vláknech.

I v průmyslové automatizaci je síťová bezpečnost důležitá

Každý rok se objevují nové zprávy o útocích na nezabezpečené systémy v průmyslové automatizaci. Zákazníci a vládní orgány zjišťují, že průmyslová automatizace vyžaduje stejné zabezpečení, jako je běžné v IT sítích, ale zároveň přizpůsobené jedinečným podmínkám průmyslových provozů. Ať už se zabýváte budováním nových průmyslových automatizačních systémů, nebo chcete modernizovat stávající sítě doplněním zabezpečení, je důležité najít řešení, které vyhovuje požadavkům průmyslu a splňuje přísné bezpečnostní nároky.

Dodavatelem ethernetových prvků Moxa a dalších zařízení pro průmyslovou komunikaci je společnost ELVAC IPC s.r.o. Podrobnější informace je také možné získat na internetových stránkách (viz níže).

www.moxa.cz.