Aby MaR nepřišel nazmar

Bezpečnostní analytici varují – sítě měření a regulace a zařízení využívající protokol SCADA mají tragicky podhodnocené zabezpečení.

FILIP WEBER

Sítě MaR vznikaly většinou přechodem od sériových přenosů k Ethernetu pouhým propojením měřicích a regulačních systémů přes přepínače. V naprosté většině případů postrádají jakákoliv pravidla IP architektury a jsou postaveny na nejhloupějších přepínačích bez podpory bezpečnostních funkcí (VLAN, 802.1x) a základních protokolů pro stabilitu sítě (Spanning Tree Protocol). A proč se s tím také trápit, vždyť to funguje a nikdy se nic nestalo.

Bohužel málokdo ze správců MaR, což jsou většinou lidé ze světa měření a ne z IT, si uvědomuje možné hrozby. Při kybernetickém útoku hrozí odmítnutí služby, poškození připojeného zařízení, modifikace naměřených dat, změny regulace apod.

Největší hrozba

Největší nebezpečí pro útok na zařízení v síti MaR nepředstavují útoky z internetu nebo napadení, kdy by zcela cizí osoba překonala plot a získala fyzický přístup k síti. Největším nebezpečím je útok vedený červem nebo trojským koněm, který bude infikovaný v notebooku zaměstnance nebo pracovníka servisní firmy.

K infekci může dojít, když notebook bude připojen servisním technikem u jiného zákazníka, který bude mít infikovanou síť, nebo třeba při připojení notebooku doma. Červ, který se tak dostane do sítě, může ovlivňovat měřicí a řídicí systémy (PLC). Může docházet k vypínání zařízení připojeného k PLC, modifikaci nastaveného programu v PLC nebo třeba k přeměně naměřených hodnot. A to jak hodnot jako teplota, hladina, ale i hodnot rozhodných pro fiskální systémy, např. objem a průtok.

Známé útoky

Příkladem útoku na systémy SCADA je červ STUXNET, který v roce 2010 infiltroval do řídicích systémů v íránském jaderném středisku a poškodil odstředivky na obohacení uranu. Byly jím napadeny i elektrárny v USA a Rusku a šířil se přes USB paměti.

Tento útok je známý a většina systémů SCADA je proti němu ošetřena updatem softwaru.

Pokud byl ovšem update nainstalovaný na všechna zařízení v síti a update na dané zařízení vůbec existuje. Update nemusel být proveden všude a hrozba nových, zatím neznámých útoků, je reálná. Tušíte třeba, že systémy Siemens založené na SIMATIC WinCC Open Architecture byly také postiženy zranitelností Heartbleed (OpenSSL)?

Jak zabezpečit?

Smyslem zabezpečení sítě MaR je zajištění, aby se směla připojit jen ověřená zařízení, a logické rozdělení sítě MaR na podsítě (VLAN). Do těchto podsítí jsou automaticky zařazena řešení podle jejich rozdělení do skupin na ověřovacích serverech. Je libovolné, kde je které zařízení připojeno, vždy je zařazeno do příslušné VLAN.

Zabezpečení připojení pouze ověřených platforem se zajišťuje protokolem IEEE 802.1x. Přepínač, ke kterému se zařízení připojí, se dotáže řídicího serveru (Radius), zda řešení zná a do jaké VLAN patří.

Počítače zaměstnanců, které se připojují k síti, jsou zařazeny v jedné VLAN. V jiné VLAN jsou zařazeny počítače externích techniků a v další jsou ukončeny vzdáleně se připojující technici. Měřicí a regulační zařízení mají vlastní VLAN. Síť MaR je tedy segmentována a provoz mezi segmenty je směrován přes L3 router s firewallem.

Na firewallu jsou mezi VLAN vytvořena komunikační pravidla, kdy je vše zakázáno a je povolena pouze určitá činnost (podle portu, zdrojové a cílové adresy).

Intrusion prevention system

Komunikace mezi VLAN je na firewallu kontrolována systémem prevence průniku (IPS). IPS kontroluje on-line datový tok a porovnává jej se vzorky známých útoků. Škodlivý datový tok pak automaticky zablokuje, a zabrání tak útoku na zařízení. V případě, že se objeví nový útok, je velká pravděpodobnost, že bude zachycen starými filtry.

Nové útoky jsou totiž většinou jen modifikací starých útoků. A pokud by se objevil zcela nový, neznámý útok, výrobce IPS zajišťuje okamžitou aktualizaci vzorků (digitall vaccine). Výhodou pak je, že stačí aktualizovat jeden ochranný systém a není nutné řešit složitou aktualizaci jednotlivých měřicích a regulačních zařízení.

Je samozřejmostí, že řídicí síť MaR musí být zabezpečena i při připojení k internetu. A to buď zcela, fyzicky oddělena jednoduše tak, že není k internetu připojena. Nebo je připojení k internetu povoleno, je dalším segmentem na L3 směrovači sítě MaR a veškerá komunikace je filtrována firewallem a IPS. Pravidla na firewallu musí být nastavena vše zakázat, povolit pouze komunikaci vybraným zařízením nebo serverům a jenom na zvolených portech a s definovanými cíli v internetu.

Logujte!

Jak si zajistíme přehled o tom, co se v síti MaR událo? Je nezbytně nutné logovat! A logy ukládat ze všech zařízení na jedno bezpečné místo. Všechna řešení připojená do sítě MaR musí odesílat veškeré logy ve formátu Syslog na jedno bezpečné úložiště.

Úložiště logů musí zajistit nepřetržitý příjem událostí, jejich uložení a analýzu. Systém musí podporovat alespoň vyhledání a korelace logů v případě vzniku události. Sofistikovanější (SIEM) systémy dokážou sami generovat upozornění (alerty) v případě definovaných událostí. ■

Autor je síťovým architektem společnosti Compunet

Sítě MaR

Slouží ke komunikaci měřicích a regulačních zařízení v různých odvětvích průmyslu. Distribuce plynu a vody, těžba ropy, skladování plynu, transport plynu, ale také k řízení technologií budov. Sítě propojují jednotlivé řídicí systémy PLC (Programmable Logic Controller), koncentrátory sériových portů, informační panely a přenášejí od nich naměřené hodnoty do řídicího centra a zpět pokyny k regulaci.

Samostatnými sítěmi mohou být tzv. fiskální sítě, které pouze měří a z jejichž naměřených hodnot se vypočítávají platby odběratelů a daně státu. Řídicí systémy jsou obvykle postaveny na operačním systému SCADA.

Zaujal vás tento příspěvek? Čtěte související články s příbuznou tematikou on-line.