Zavedenie bezpečnosti do prevádzkových riadiacich sietí (1)

Gordon Gillespie

Úvod

Prepojenie podnikových sietí s modernými prevádzkovými sieťami otvorilo dvere pre hackerov a vírusy, ktoré sa môžu jednoducho dostať do prostredia výrobnej technológie. Takýto vstup môže spôsobiť chybu prevádzkovej siete alebo neoprávnenú modifikáciu výrobného systému, ktorý je na takúto sieť napojený. V záujme dosiahnutia čo najdlhšieho času bezporuchovej prevádzky a využiteľnosti prevádzkovej siete, ako aj na elimináciu prekážok v prípade poruchy procesu, je na mieste uvažovať o takých bezpečnostných postupoch, ktoré zabránia nežiaducemu prieniku do výrobného systému.

Takáto bezpečnosť by mohla byť reprezentovaná oddelenými sieťami, pričom prístup do prevádzkového systému je striktne obmedzený smerovačmi (routermi) a ochranným serverom (firewallom). Podobne aj všetky aplikácie a všetci používatelia sú v rámci výrobných sietí obmedzení špecifikami, ktoré sa pre proces vyžadujú: žiadne e-maily, žiadne hry, žiadne prehliadanie internetu. Takáto filozofia môže viesť k požiadavke paralelnej inštalácie viacerých sietí na rovnakom mieste. Napríklad velín (miestnosť riadenia) si pravdepodobne bude vyžadovať podnikovú sieť pre e-maily a obchodné aplikácie, a tiež chránenú prevádzkovú sieť pre riadiace systémy. Správne nainštalované siete v prostredí súčasných výrobných podnikov môžu nielen zabezpečiť zneškodnenie vírusov, ale i to, že na výrobnej sieti budú „prítomní“ len oprávnení používatelia. V tomto článku sa budeme zaoberať zabezpečením ochrany výrobných systémov pred poruchami siete, ktoré bývajú zapríčinené vonkajšími vplyvmi.

Prepojte svoje siete

Vo väčšine priemyselných podnikov sa možno stretnúť s požiadavkou poskytovať vedeniu, manažérom a obchodníkom informácie z výroby a naopak, podnikové aplikácie sprístupniť používateľom z výrobných prevádzok. Často sú však tieto systémy vybudované na už historickom toku procesných informácií od riadiacich systémov k používateľom na najvyššej podnikovej úrovni a/alebo prístupe k súborom podnikových aplikácií a na e-mailovom prístupe pracovníkov velína (miestnosti riadenia). Bez ohľadu na uvedenú skutočnosť takáto filozofia umožňuje sieťové prepojenie medzi výrobou a manažmentom podniku. Pretože veľa riadiacich systémov používa sieť ethernet ako rozhodujúci prvok svojej systémovej architektúry, problémy na úrovni podnikovej siete sa môžu preniesť do prevádzkovej siete práve cez údajovú linku spájajúcu manažment s výrobou, čo môže mať vážny dopad na produkciu.

Problémy, ktoré môžu postihnúť prevádzkové siete, sa dajú rozdeliť do dvoch základných kategórií: neúmyselné (náhodné) a úmyselné. Medzi neúmyselné problémy možno typicky zaradiť chybu káblovania či konfigurácie siete, alebo chybu sieťového zariadenia. Naopak, úmyselné chyby sú tie, ktoré zapríčiní jednotlivec so zlomyseľným zámerom. Môže ísť pritom o nespokojných zamestnancov, sieťových hackerov alebo o osoby šíriace počítačové vírusy. V oblasti priemyslu je podľa našich skúseností viac neúmyselných ako úmyselných útokov, ale premnožovanie sa vírusov a stúpajúci počet riadiacich systémov na báze PC vedie k nárastu počtu úmyselných narušení systémov.

Neúmyselné a systematické problémy v prevádzkových riadiacich sieťach často predstavujú jeden z troch nasledujúcich typov:

- **Porušené alebo zlé pakety** – chybná sieťová karta alebo zlé káblové spojenie môžu „zaplavovať“ sieť zlými údajovými balíkmi, čo môže viesť k spomaleniu alebo dokonca k prerušeniu komunikácie.
- **Zdvojenie IP adresy** – tento bežný problém sa dosť ťažko diagnostikuje a výsledkom môže byť dočasná strata komunikácie alebo údajov.
- **Zahltenie prenosu** – keďže vysielané pakety sú bežnou súčasťou akejkoľvek siete, v enormnom množstve môžu spomaliť či pozastaviť jej normálny chod. Vtedy všetky sieťové zariadenia musia venovať zálohu CPU na interpretáciu každého paketu. Jednoduché zasunutie koncovky kábla do nesprávneho portu môže zapríčiniť „búrku vo vysielaní“, a tá preruší akúkoľvek sieťovú komunikáciu.

Úmyselné udalosti v rámci prevádzkovej riadiacej siete možno zaradiť do jednej z nasledujúcich kategórií:

- **Vírusová infekcia** – „červy“ a „trójske kone“ sú vo všeobecnosti vytvárané tak, aby sa množili prostredníctvom reťazcového mechanizmu, obľúbeného v prostredí Microsoft Windows, Internet Explorer a Outlook E-mail na počítačoch s procesorom Intel. Šanca infikovania sa takýmito vírusmi sa vo výrobnom prostredí zvyšuje, pretože spomenuté technológie sa veľmi často využívajú v riadení procesov vďaka ich nízkej cene a možnosti splnenia požiadavky vzájomnej spolupráce v otvorených systémoch. Vírusy môžu zaplniť disk buď cez sieť, alebo priamo z diskety, alebo z podomácky napáleného CDROMu, takže politika bezpečnosti sa musí sústrediť nielen na ochranu siete (firewallu), ale aj na fyzickú ochranu (uzavretie takého servera).
- **Prienik zvonka** – prerazenie do sietí prevádzkového riadenia sa doposiaľ vyskytovalo zriedka. Stále viac podnikov sa však už navzájom spája prostredníctvom internetu alebo podnikových sietí WAN (wide area network), čo zvyšuje výskyt neautorizovaných prienikov. Hacker väčšinou získa prístup do podnikovej siete a pokúsi sa napadnúť lokálne počítače. Servery (tak na báze Windows, ako aj multipoužívateľské platformy ako Unix a Linux) sú najčastejším cieľom takéhoto sieťového prieniku. Slabým miestom v mnohých aplikáciách v priemysle sú interné webové prehliadače. Využívajú sa najmä ako efektívne nástroje na prenos údajov. Málokedy sú však vybavené aktuálnymi bezpečnostnými prvkami a verziami bezpečnostných programov. Aj http sa často prenáša cez ochranný server (firewall) na zabezpečenie funkčnosti prehliadača, ale potom z nedostatočne nakonfigurovaného webového servera robí lákavý cieľ.
- **Prienik zvnútra** – v poslednej dobe stúpa množstvo neautorizovaných priesku-

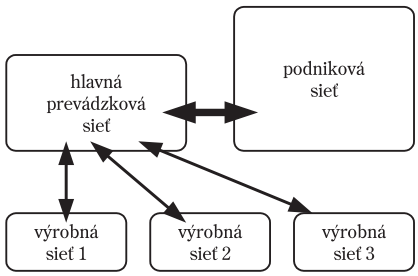
mov siete a zariadení zamestnancami. Deje sa tak následkom toho, že ľudia sú už počítačovo gramotnejší a zariadenia sú stále viac konštruované na báze PC. Bežným problémom je, že zamestnanci, ktorí počítačom rozumejú, nevedomky zmenia konfiguráciu zariadenia, čo znamená prerušenie procesu. Ochrana heslom poskytuje len obmedzenú ochranu proti hackerom, pretože väčšina skupín prevádzkového riadenia používa v im zverených systémoch ľahko zapamätateľné (a ľahko uhádnuteľné) heslá, ktoré ani pravidelne nemenia.

Vypracovanie bezpečnostnej politiky

Aj keď väčšina podnikov má (mala by mať?) vypracovanú politiku bezpečnosti informačných systémov, ktorá definuje kto komu udeľuje prístup do siete, mnohé z nich však nemajú v týchto dokumentoch obsiahnutú oblasť výroby. Je jasné, že väčšina zamestnancov by nemala mať prístup k databázam účtovníctva, ale vo výrobnom podniku sa často nerešpektuje skutočnosť, že väčšina zamestnancov by nemala mať prístup k prevádzkovým riadiacim systémom. Vypracovanie bezpečnostnej politiky by malo začať definovaním typov používateľov na základe ich funkcie a pozície a následne špecifikovaním, aký druh počítačov, siete a prístupu k aplikáciám sa pre každého používateľa vyžaduje. Politika bezpečnosti by mala byť súborom detailných smerníc. Môže obsahovať nariadenia typu: „PC a používatelia z oddelenia účtovníctva nebudú mať prístup k sieti vo výrobe." Alebo „Zákaz používať disketové mechaniky pracovníkmi, okrem administratívnych, vo všetkých PC, ktoré sú nasadené na riadenie procesov." Špecifické výnimky sa riešia od prípadu k prípadu a nemusia byť súčasťou politiky bezpečnosti.

Oddeľte svoje siete

Bezpečnostná politika by mohla zariadeniam s rôznymi funkčnými úlohami nariadiť použitie oddelených (zvláštnych) sieťových segmentov. Podniková sieť môže byť rozdelená prinajmenšom do troch úrovní dôležitosti. Patrí sem hľadisko celistvosti (integrity) a prístupu, pri ktorom sa zabezpečuje, že vysielanie, sieťové problémy a/alebo narušitelia sa nedostanú až ku kritickému procesnému zariadeniu. Na rozdelenie siete do menších komunikačných okruhov možno použiť smerovače. Manažment prístupu založený na stupni kritickosti pripojeného zariadenia môžu zabezpečiť bezpečnostné servery. Obmedzený prístup ku kritickým sieťam a lokalizácia väčšiny používateľov na úrovni podnikovej siete môže maximalizovať čas bezporuchovosti výrobnej prevádzky. Na obr. 1 vidieť, že používatelia a servery vyžadujú komunikáciu s obidvoma sieťami



Obr.1

– s výrobnou aj podnikovou, takže títo by boli umiestnení na procesnej sieti. Z obrázka je zrejmé aj to, že neexistuje priame komunikačné spojenie medzi podnikovou a procesnou sieťou. Okrem toho môže byť prístup medzi procesnou a výrobnou sieťou obmedzený len na podporu takých protokolov a počítačov, ktoré sú nevyhnutné pre konfiguračné funkcie a funkcie zhromažďovania údajov.

Presuňte kritické výrobné zariadenia do sietí s vyššou bezpečnosťou mimo ostatných podnikových sietí. Minimalizácia prístupu, najmä zo strany podnikovej siete, môže maximalizovať čas bezporuchovosti prevádzky (obr. 1). Jednotlivé siete z obr. 1 možno zadefinovať nasledovne:

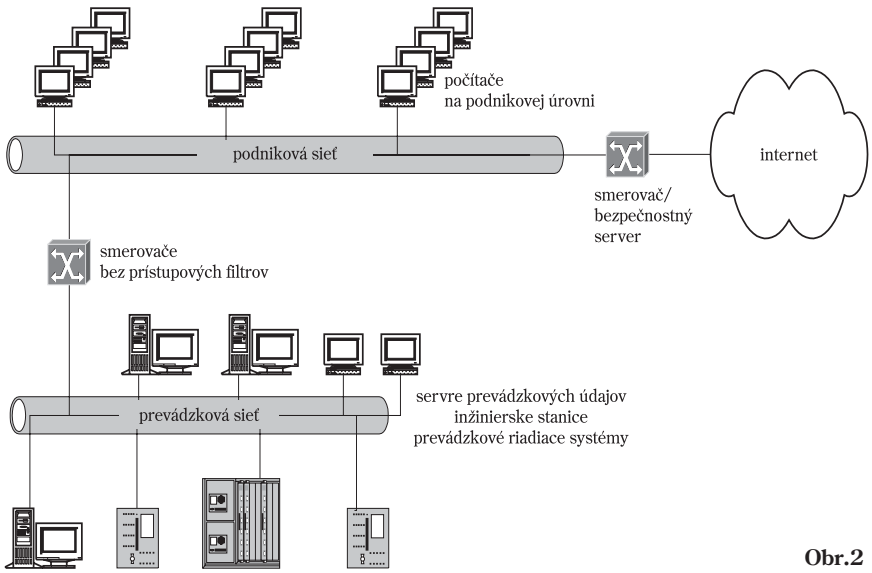
Výrobná sieť – je pre výrobný podnik kritická, a musí fungovať za každých okolností. Príkladmi sú siete pre distribuované systémy riadenia (DCS) a programovateľné logické automaty (PLC). Tieto siete môžu zahŕňať minimum zariadení, ktoré by mohli byť chránené pred neautorizovaným prístupom. Bežné PC alebo tlačiarne by nemali byť pripojené do kritických sietí s výnimkou situácie, ak je takéto zariadenie predpísané jeho výrobcom. Sieťový prístup ku kritickým sieťam by mohol byť na smerovači obmedzený len pre špecifické uzly, ako napr. inžinierska konfiguračná stanica alebo uzly zberu dát pre podnikový informačný systém. Na takejto sieti by mali byť PC fyzicky oddelené a mali by mať obmedzený prístup k disketovým mechanikám a CD ROMom.

Hlavná prevádzková sieť – využíva sa na komunikáciu na úrovni prevádzkového personálu, ale z hľadiska fungovania podniku nie je kritická. Prevádzková sieť zahŕňa PC, tlačiarne a spúšťajú sa na nej bežné kancelárske aplikácie ako MS Office a sieťové aplikácie ako e-mail. Prevádzková sieť sa často využíva na zabezpečenie prístupu z velína (riadiacej miestnosti) k sieťovým aplikáciám, ako sú napr. informácie ISO a WHMIS alebo trendy a archivované údaje v podnikovom informačnom systéme. Najdôležitejšou vlastnosťou prevádzkovej siete je, že jej uzly môžu mať obmedzený prístup ku kritickým výrobným sieťam. Úlohou údajových serverov podnikového informačného systému by bolo zbierať údaje z kritických sietí a poskytovať ich podnikovej sieti. Prevádzková sieť by mohla byť poškodená vírusom, ale táto chyba by sa nepreniesla do výrobnej siete.

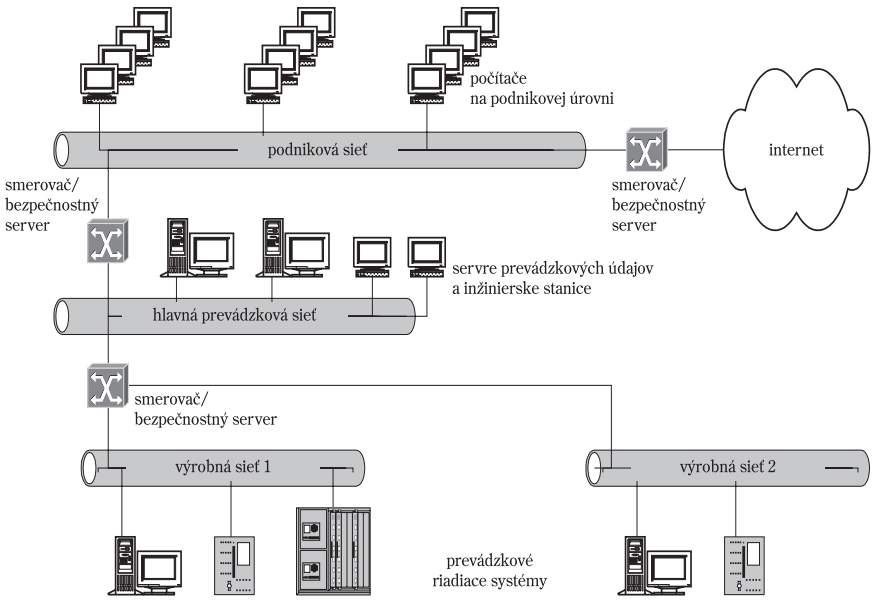
Podniková sieť – túto sieť najčastejšie využívajú pracovníci oddelení informatiky a pracovníci prevádzky. Zvyčajne je v takejto sieti zabezpečený aj prístup na internet, a tak sa môže vyskytovať aj nákaza vírusom. Kancelárska sieť by mala mať zakázaný prístup do výrobných sietí, no mohla by mať prístup k serverom hlavnej prevádzkovej sieti. Cez podnikovú sieť prichádza väčšina sieťových prienikov, takže je mimoriadne dôležité udržiavať izoláciu medzi touto a výrobnou sieťou.

Topológia siete

Usporiadanie siete na obr. 2 je typické pre mnohé priemyselné výrobné podniky dneška. Aj keď má podnik nainštalovaný smerovač medzi podnikovými a prevádzkovými sieťami v záujme prevencie pred zahltením siete, stále neexistuje žiadne vhodná ochrana obmedzujúca priamu komunikáciu cez smerovač. Používatelia na prevádzkovej sieti stále dostávajú svoje e-maily a často majú aj spojenie na podnikové servery, pričom obidve tieto „možnosti" sú takmer s určitosťou potenciálnym



Obr.2



Obr.3

zdrojom vírusovej infekcie. Mnohé osoby na podnikovej sieti, resp. na internete, sú schopné sledovať prevádzkové riadiace zariadenia hľadajúc slabé miesto takéhoto systému.

Mnohé podniky inovovali svoje siete oddelením prevádzkovej riadiacej siete. Nanešťastie, takéto riešenie často nezahŕňa žiadnu kontrolu a riadenie prístupu alebo funkciu bezpečnostného servera (firewallu). V najlepšom prípade sa tu môžeme stretnúť s bezpečnosťou na báze zisťovania chýb (obr. 2).

Aby sme si boli istí, že hackeri a vírusy nedokážu lokalizovať a napadnúť kritické prevádzkové riadiace zariadenia, odporúča sa vytvoriť tretiu úroveň siete. Takáto ochrana výrobnej siete ťaží z riadenia prístupu na smerovači, ktorý oddeľuje výrobnú sieť od hlavnej prevádzkovej siete.

Dodávatelia prevádzkových riadiacich zariadení často preferujú umiestnenie svojich zariadení na oddelených ethernetových sieťach. Jeden smerovač s funkciou bezpečnostného servera a schopnosťou kontrolovať stav prichádzajúcich paketov môže ochrániť niekoľko oddelených a kriticky bezpečných výrobných sietí. Tento typ blokového smerovača kontroluje prichádzajúce prístupy (okrem špecificky dovolených) a odchádzajúcu komunikáciu v záujme zvýšenia bezpečnosti, a to pri minimálnej potrebe svojej údržby (obr. 3).

Obr. 3 zobrazuje takú štruktúru, kde na výrobnej sieti sú pripojené len vyhradené prevádzkové riadiace zariadenia. Bezpečnostná politika by mala zakázať všetky akcie na sieti, e-maily, sieťové tlačiarne, prístup na internet a všetky počítače, ktoré nie sú špecificky požadované dodávateľom prevádzkového riadiaceho systému. V mnohých prípadoch je vhodné mať k dispozícii samostatné siete pre rôzne typy zariadení, ako napr. sieť pre DCS, sieť pre PLC, sieť pre bezdrôtové zariadenia či inteligentné meracie zariadenia a pod.

Záver

Na záver možno povedať, že bezpečnosť výrobnej siete znamená trvalé úsilie o navodenie stavu, v ktorom bezpečnostná politika zakazuje všetky prístupy okrem tých, ktoré majú na to špecifický dôvod. Návrh, implementácia a riadenie prevádzkových sietí má vyššie vstupné náklady ako ekvivalentná podniková sieť IT, pretože sa vyžaduje hlbšie zaškolenie a externá podpora. Návratnosť takejto investície sa dosahuje práve znížením času odstavenia prevádzky z dôvodu prerušenia siete alebo zlyhania počítača.

V ďalšom pokračovaní sa zameriame na demonštráciu fungovania bezpečnosti prevádzkovej siete a uvedieme niekoľko návrhov, ako vybudovať bezpečnostnú politiku pre prevádzku.

Gordon Gillespie
je vedúci návrhu sietí v spoločnosti Artemis Industrial Networks, ktorá sa špecializuje na návrh prevádzkových sietí a komunikačných sietí na úrovni procesov.

Publikované so súhlasom autora.

Článok bol po prvýkrát publikovaný v časopise Sensors Magazine, júl 2003, www.sensorsmag.com

Gordon Gillespie

Artemis Industrial Networks
7500 Winston Street
Burnaby, B.C.
Kanada, V5A 4X5
e-mail: ggillesp@artemisnetworks.com