Zavedenie bezpečnosti do prevádzkových riadiacich sietí (2)

Gordon Gillespie

Dodatok 1 – hypotetická infekcia

Ako príklad fungovania bezpečnosti prevádzkovej siete vyskúšame poslať vírusovú informáciu do hypotetického podniku. Zamestnanec X v takomto prípade prijme od svojho obchodného partnera e-mail obsahujúci vírus. Tento vírus začne sám seba rozmnožovať prostredníctvom rôznych metód do zariadení na sieti. Rozpošle sa na všetky adresy, ktoré má zamestnanec v adresári. Vírus podrobne prezrie lokálnu sieť s cieľom pripojiť sa na servery http a pokúsi sa skopírovať sám seba do ostatných zariadení prostredníctvom lokálne zdieľaných sietí s operačným systémom Windows. Výsledkom je, že v priebehu 2 hodín má 11 ďalších počítačov v tejto časti rovnaký vírus. Všetky tieto počítače opäť vyhľadávajú nové „ciele“, takže prevádzka na sieti sa zvýši 400-násobne oproti bežnej úrovni. Podnikový server má vyťaženú CPU na 100 %, preto nedokáže obslúžiť žiadne iné počítače.

Podľa scenára A je prevádzková sieť prepojená cez smerovač do podnikovej siete, ale nie je tam žiadna iná bezpečnosť alebo bezpečnostný server. Počítač pre konfiguráciu PLC na prevádzkovej sieti má sieťovo zdieľané pripojenie k podnikovému serveru ako systém na uchovávanie konfigurácie. Podnikový server nainfikuje tento konfiguračný počítač práve cez toto pripojenie a v priebehu hodiny je infikovaných aj 5 ďalších prevádzkových PC. Prevádzková sieť prestane správne fungovať a mnohé PLC zlyhajú v dôsledku extrémneho zahltenia siete. Počítače, ktoré slúžia ako operátorské rozhrania, nie sú schopné komunikovať so svojimi regulátormi, takže operátori sú blokovaní a výroba sa zastaví až dovtedy, kým sa systém vírusu nezbaví, čo môže trvať aj 14 hodín.

Alternatívny scenár B hovorí o tom, že v podniku je oddelená výrobná sieť pre prevádzkové riadiace systémy. Aj keď počítač na konfigurovanie PLC na prevádzkovej sieti by mohol byť aj teraz zasiahnutý vírusom a prevádzková sieť by prestala fungovať, výroba nebude postihnutá, pretože bezpečnostný server výrobnej siete neumožní zasiahnutému počítaču spojiť sa s ničím iným, len s PLC. PLC sa nemôžu nainfikovať pokiaľ nebežia na operačnom systéme, ktorý pripúšťa možnosť vírusovej infekcie. Operátorské pracovné stanice nemôžu byť zasiahnuté, pretože k nim nemožno pristúpiť z konfiguračného počítača cez bezpečnostný server. Podnik sa tak nemusí obávať žiadnych odstávok.

Dodatok 2 – návrhy pre bezpečnostnú politiku v prevádzke

Aj keď existuje veľa príkladov opisujúcich politiku bezpečnosti sietí na podnikovej (manažérskej) úrovni, je len niekoľko dokumentov, ktoré slúžia ako návod pre podniky, ktoré majú záujem spracovať bezpečnostnú politiku aj pre oblasť výroby. V nasledujúcej časti je uvedených niekoľko podnetov a príkladov pre autorov bezpečnostnej politiky prevádzkových sietí.

Zakázať všetko – základom bezpečného prístupu je, že komunikácia, ktorá nie je jednoznačne bezpečná, je zakázaná – prerušia sa všetky služby a protokoly už na začiatku. Bezpečnostná politika by sa mohla začať zakázaním všetkých prístupov ku všetkým sieťovým zdrojom, a potom sa môžu stanoviť prístupy od prípadu k prípadu.

Heslá – operačné systémy ponúkajú niekoľko funkcií, medzi iným kontrolu hesiel alebo povinné zadávanie hesiel. Dobrá metóda hesiel vyžaduje najmenej 8-znakovú kombináciu písmen a číslic v hesle používateľa, pričom každý používateľ je nútený meniť svoje heslo každých 90 dní. Operačný systém neprijme heslo, ktoré nespĺňa uvedené kritériá. Dobre spracovaná metodika hesiel by mohla vyzerať nasledovne:

- nepoužívajte meno pre prihlásenie v žiadnej podobe (tak ako je, obrátene, všetko veľkými písmenami, zdvojené a pod.),
- nepoužívajte vaše krstné meno alebo priezvisko v žiadnej forme, ani meno manžela/manželky, snúbenice alebo detí,
- nepoužívajte žiadne iné informácie, ktoré je možné o vás jednoducho získať, napr. číslo zamestnaneckej karty, telefónne číslo, čísla zo sociálnej poisťovne, značku auta, názov ulice, kde bývate atď.,
- nepoužívajte heslá zložené len z číslic, alebo všetkých rovnakých písmen,
- nepoužívajte slová nachádzajúce sa v anglickom alebo inom slovníku či v inom zozname slov,
- nepoužívajte heslá kratšie ako 6 znakov,
- používajte heslá, ktoré sú kombináciou malých a veľkých písmen abecedy,
- používajte heslá, ktoré obsahujú iné znaky ako písmená – číslice, interpunkčné znamienka,
- používajte heslá, ktoré si ľahko zapamätáte, takže si ich nemusíte zapisovať.

Dobrá metóda prihlasovacieho mena/hesla pomôže presvedčiť sa, či dotyčný je skutočne ten, za koho sa vydáva. Pri využívaní zdrojov alebo posielaní správ vo veľkej privátnej sieti (nemáme na mysli internet) je zistenie totožnosti absolútnou prioritou.

Zápis dát – ukladanie a analýza protokolov prihlásenia na serveroch a smerovačoch umožní stanoviť normálny (prevádzkový) stav a pomôže odhaliť neautorizované udalosti. Na získanie týchto informácií bude potrebný syslog server a zachytávač RMON.

Telefónne linky – modemy a telefónne linky predstavujú významné nebezpečenstvo neautorizovaného prieniku do prevádzkovej siete.

- Nepovoľte využívanie modemov na používateľských počítačoch – prevádzkujte modem na serveri, ktorý je chránený a spravovaný.
- Vzdialení používatelia zvyčajne ukladajú svoje telefónne číslo, prihlasovacie meno a heslo pre spojenie v tlačenej dokumentácii a zároveň aj ako súčasť uloženého spojenia RAS. Pri nesprávnom používaní je možné tieto informácie skopírovať.
- Používajte prenajaté komunikačné linky (bod-bod) pre systémy SCADA, kde môžete s určitosťou povedať, kto (čo) je na druhom

konci. Ak sa vyžaduje pevné pripojenie, zaveďte službu spätného volania, aby ste sa ubezpečili, že druhý koniec spojenia je v takom stave ako očakávate.
- Vždy používajte plný prístup cez meno/heslo pre spojenie s modemom buď cez funkcionalitu Windows RAS, alebo kúpou modemu so zabudovanou autentizáciou.

Sieťové zdieľanie – vyvarujte sa zdieľania diskov alebo siete do/z prevádzkovej siete okrem prípadu, keď je to nevyhnutne potrebné.

Odnímateľné disky – zakážte používať disketové mechaniky a CD ROM čítačky pre neadministratívnych pracovníkov v rámci prevádzkovej siete. Uprednostnite editáciu NT profilov na operátorských staniciach, aby ste zabezpečili ich nepožívanie alebo fyzicky zablokujte odnímateľné zariadenia.

Fyzický prístup – zamknite všetky servery, smerovače, prepínače, prepájacie dosky a horizontálne distribučné body. Každé sieťové zariadenie, ku ktorému je možné dostať sa fyzicky, môže byť narušené.

Vírusový skener – uistite sa, že všetky PC na hlavnej prevádzkovej sieti majú spustený vírusový skener a že pracujú s aktuálnymi databankami vírusov. Ak je to možné, nastavte automatickú aktualizáciu databázy vírusov a každých pár dní to kontrolujte. Ak to umožňuje dodávateľ vášho riadiaceho systému, spustite si vírusový skener aj na počítačoch v rámci prevádzkovej siete.

E-mail – neumožnite e-mailovanie v rámci výrobnej siete. Bodka. Nikdy. E-maily sú povolené na úrovni hlavnej prevádzkovej siete.

Prístup na internet – neumožnite prístup na internet z výrobnej siete. Bodka. Nikdy. Prístup na internet je možný len z úrovne hlavnej prevádzkovej siete.

Neznáme zdroje – NIKDY neotvárajte žiadny súbor alebo makrá pripojené v maili od neznámeho, podozrivého alebo nedôveryhodného zdroja. Takýto mail ihneď vymažte a druhýkrát ho vymažte vyprázdnením záložky „smetný kôš"/zmazané položky. Zmažte všetky spamy, reťazcové maily alebo iné zábavné maily bez odpovedania alebo ich ďalšieho preposielania. Nikdy nesťahujte súbory z neznámych alebo podozrivých zdrojov. Pred použitím diskety túto vždy preverte vírusovým skenerom.

Skenovanie siete – dodržiavanie bezpečnostnej politiky môže jednoznačne prekaziť monitorovanie siete, zachytávanie komunikácie, skenovanie portov alebo skenovanie bezpečnosti okrem tých prípadov, ktoré sú v súlade s povolenými právomocami niektorých zamestnancov.

Neprípustné použitie – dodržiavanie bezpečnostnej politiky môže jednoznačne zabrániť prelomeniu bezpečnosti alebo prerušeniu sieťovej komunikácie. Prelomenie bezpečnosti okrem iného znamená obídenie autentizácie alebo bezpečnosti každého počítača, siete alebo konta, získanie prístupu k údajom, ktorých prijímateľmi nie sú radoví zamestnanci alebo získanie prístupu k serveru alebo kontu, ku ktorému nemajú bežní zamestnanci autorizovaný prístup. Na účely tohto popisu „prerušenie" komunikácie okrem iného znamená prehľadávanie siete, zahltenie pingami, odmietnutie služieb a zlomyseľné falšovanie smerovania správ.

Jeden prístupový bod – bezpečnostný server musí byť jediným prístupovým miestom medzi výrobnou sieťou a ostatnými sieťami v podniku a/alebo internetom. Každá forma krížového spojenia, ktoré by obchádzalo bezpečnostný server by mala byť striktne zakázaná.

„Bezpečnostné záplaty" – pre všetky aplikácie bežiace na servery by mali byť k dispozícii aktuálne verzie „bezpečnostných záplat", t. j. doplnkov alebo aktualizácií, ktoré poskytuje dodávateľ danej aplikácie pri odhalení chyby alebo bezpečnostnej diery jej aktuálnej verzie. Administrátor (príp. skupina administrátorov) by mala mať spôsob, ako udržať jednotlivé aplikácie a bezpečnostné opravy aktuálne a to monitorovaním bezpečnostných zdrojov a sledovaním bezpečnsotných informácií predajcu softvérovej aplikácie.

Kontá – nepoužívajte privilegované (prednostné) kontá na žiadnom z prevádzkových zariadení ak vystačíte s neprivilegovanými.

Nepotrebné služby na serveroch – služby a aplikácie, ktoré neriešia požiadavky obchodného oddelenia alebo výrobných procesov musia byť zablokované. Zvláštnu pozornosť je potrebné venovať sieťovým aplikáciám na serveroch, ako napr. (ale nielen) telnet, ftp, rhost, rexec, rsh, sieťové služby, finger, gopher, lat a snmp.

Nepotrebné služby na smerovačoch – smerovače musia byť veľmi podrobne skontrolované, aby ste si boli istí, že sú bezpečné. Používateľských kont treba udržiavať len minimum a treba stále meniť ich heslá. Aktívne heslá na smerovači musia byť uložené v bezpečnej zašifrovanej forme.

Zakážte aj nasledujúce veci
- priame vysielanie na IP,
- proxy ARP,
- prichádzajúce pakety na smerovač s nesprávnou adresou, ako napr. adresa RFC1918,
- prichádzajúce pakety smerujúce do výrobnej siete,
- malé služby TCP,
- malé služby UDP,
- smerovanie každého vstupu,
- CDP na smerovačoch Cisco,
- všetky sieťové služby bežiace na smerovači.

Ďalšie odporúčania
- Používajte podnikom štandardizované reťazce SNMP – nie „verejné" alebo „privátne".
- Akonáhle vznikne požiadavka na rozšírenie výrobnej siete, budú pridané aj ďalšie prístupové pravidlá.
- Každý smerovač by mohol mať banner napr. s takýmto oznamom:
  „Neautorizovaný prístup k tomuto sieťovému zariadeniu je zakázaný. Musíte mať výslovný súhlas na prístup a konfiguráciu takéhoto zariadenia. Všetky aktivity vykonávané na tomto zariadení môžu byť zaznamenané a nedodržanie stanovenej politiky môže viesť až k disciplinárnemu postihu a prípad môže byť posunutý na právne šetrenie".

Gordon Gillespie
je vedúcim 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