SCADA systémy je potrebné chrániť

Bill Holder, bezpečnostný špecialista spoločnosti Sun Water, odpovedal na niekoľko otázok na tému informačnej bezpečnosti SCADA systémov.

Otázky bezpečnosti v súčasnosti zamestnávajú odborníkov na SCADA systémy. Aké sú kľúčové zásady a postupy, ktoré by mohli poskytnúť adekvátnu bezpečnosť?

SCADA systémy sa tradične opierali o nízke povedomie o vlastnej technológii a o špecifickosť. V minulosti to prinášalo želaný efekt, nebolo to síce dokonalé, ale poskytovalo to akceptovateľnú úroveň bezpečnosti. Moderné technológie a zvýšené požiadavky na SCADA systémy však tento stav zmenili, čo znamená, že sa SCADA systémy len tak ľahko neskryjú s nádejou, že ich to ochráni.

Potreba dát reálneho času a pripojiteľnosti viedla k tomu, že SCADA aplikácie si osvojili WAN a LAN komunikáciu a vo väčšine prípadov sa pripojili ku korporatívnej sieťovej infraštruktúre. Z toho vyplýva, že SCADA systémy sú dnes vystavené všetkým rizikám a nebezpečenstvám, ktoré so sebou takéto pripojenie prináša, či už v súvislosti s internetom alebo internou súkromnou sieťou spoločnosti.

Na to, aby sa podarilo zaistiť bezpečnosť na požadovanej úrovni ako súčasť aplikácií SCADA, odborníci v tejto oblasti si musia osvojiť zásady a postupy, ktoré sa zaoberajú s aktuálnymi rizikami v súvislosti s touto novou pripojenou SCADA technológiou. Tradičné IP siete s tým majú dlhoročné skúsenosti a za ten čas si vytvorili mnohé účinné praktiky a obranné mechanizmy, pričom často sa učili za chodu pri útokoch kybernetických vírusov a červov.

Zásady okolo SCADA systémov musia nájsť rovnováhu medzi bezpečnosťou a požiadavkami na prevádzku. Z bezpečnostného hľadiska má najvyššiu prioritu zabezpečenie SCADA inštalácie pred externými útokmi (vrátane tých z internej siete spoločnosti). Takisto je potrebné mať na pamäti, že naopak, interná sieť spoločnosti musí byť chránená pred SCADA systémami. Je to veľmi dôležité, pretože SCADA systémy sú často bez obsluhy a niekedy zvyknú byť inštalované na značne vzdialených miestach. Narušiteľ vzdialeného SCADA systému má potom možnosť získať prístup aj do siete spoločnosti a prípadne ukradnúť cenné interné informácie alebo dokonca získať prístup k iným SCADA inštaláciám.

Najdôležitejšie zásady zaistenia vysokého stupňa bezpečnosti SCADA technológie sa sústreďujú na prístup do siete a riadenie. S každou SCADA inštaláciou by sa malo zaobchádzať ako s externou sieťou, dokonca by sa malo ísť ešte ďalej a mala by sa pre ňu vytvoriť osobitná sieť DMZ (tzv. demilitarizovaná zóna). Zároveň by sa obmedzil prístup do tejto siete na nutné minimum iba pre potreby dennej prevádzky. Na tomto princípe by sa zabezpečila ochrana SCADA inštalácie pred korporatívnou sieťou a naopak.

Ochrana však môže byť ešte efektívnejšia so systémom monitorovania umiestneným priamo na mieste inštalácie SCADA systému. Mal by sa monitorovať prístup, prevádzka a výkon, aby bolo možné rýchlo odhaliť neautorizovanú alebo neznámu aktivitu, čím sa maximalizuje ochrana integrity SCADA inštalácie.

Jednou z prehliadaných oblastí bezpečnosti SCADA systémov je údržba. Bezpečnostným rizikám softvéru sa je potrebné venovať pravidelne, obzvlášť keď jeho dodávatelia vydávajú informácie o konkrétnych chybách a poskytujú záplaty na ich nápravu. SCADA inštalácia bez údržby zvyšuje bezpečnostné riziká smerom ku korporatívnej sieti, nehovoriac o tom, že informácie o dierach v softvéroch sa voľne nachádzajú na internete, ktoré si môže každý prečítať.

Je zrejmé, že zodpovedné zásady prístupu k sieťovej bezpečnosti v kombinácii s monitoringom a údržbou môžu výrazne vylepšiť úroveň bezpečnosti SCADA inštalácie a minimalizovať bezpečnostné riziká korporatívnej siete ako aj inštalácie samotnej.

Aktualizácia systémovej bezpečnosti si vyžaduje nemalé náklady. Ako si môžete byť istý, že takáto aktualizácia prinesie návratnosť investícií (ROI)?

V podnikateľskom prostredí tesne po globálnej finančnej kríze, keď sa každý snaží vyťažiť z každého centu čo najviac, je naozaj ťažké obhájiť vynaloženie investície do systémovej bezpečnosti. Bezpečnosť je bežne vnímaná ako drahá réžia, na ktorú sa vynakladá veľa peňazí a nič nezarába. Z istého hľadiska to môže byť pravda, ale viete si predstaviť škody napáchané jediným prienikom do sietí spoločnosti? Tie sa môžu vyšplhať až na hranicu niekoľkých desiatok tisíc eur, takže investícia do bezpečnosti by sa mala vnímať ako spôsob úspory peňazí. Ako však získať najvyššiu možnú návratnosť investície do systémovej bezpečnosti? Je niekoľko spôsobov ako demonštrovať hodnotu takejto investície a maximalizovať ROI.

Po prvé, systémová bezpečnosť je nenápadná. Dobrý bezpečnostný systém pracuje bez toho, aby si niekto niečo všimol. Poskytuje istú úroveň bezpečnosti tak, aby neobmedzoval prácu ľudí. Napríklad firewall umožňuje používateľom kedykoľvek sa pripojiť na internet a do iných sietí a súbežne blokuje zákerné útoky a nechcenú komunikáciu. Toto všetko prebieha bez toho, aby si bežný zamestnanec vôbec niečo všimol. Bezdrôtové siete sú ďalším príkladom nenápadnosti systémovej bezpečnosti. Ľudia považujú prístup do siete za samozrejmosť a za pomoci notebookov a mobilných zariadení sa pripájajú do korporatívnej siete kedykoľvek to potrebujú. Nikto z nich si však neuvedomuje prístupové a autentifikačné procedúry, ktoré prebiehajú v pozadí, aby mali k dispozícii bezpečné pripojenie.

Toto vedie potom k otázke, či vynaloženie 500 eur za firewall je dobrá investícia alebo či takýto výdavok prinesie rozumnú návratnosť. Povedomie, že systémová bezpečnosť neponúka dostatočné ROI, sa jednoducho musí zmeniť. Efektívny spôsob, ako to dosiahnuť, je stará dobrá publicita. To neznamená zverejňovanie detailov systémovej bezpečnosti, ale osvetu u ľudí, že investície do systémovej bezpečnosti sú oprávnené.

Napríklad jeden týždeň bude korporatívny firewall blokovať mnohé pokusy o neautorizovaný prístup a zároveň bude umožňovať prístup zamestnancom. Tieto informácie sa potom budú odovzdávať manažérom a kompetentným osobám, aby názorne prezentovali, ako pracuje systémová bezpečnosť. To postačuje k zdôrazneniu efektivity a hodnoty systému.

Ďalším potenciálnym opatrením je hľadanie spôsobov na proaktívne využitie infraštruktúry systémovej bezpečnosti. Namiesto prístupu, kedy sa pasívne čaká na odozvu infraštruktúry, je lepšie zaviesť činnosti, ktoré skvalitnia vykonávanie a monitoring bezpečnosti prostredia spoločnosti. Zvyšuje to ukazovateľ ROI a demonštruje, že vynaložené investície sa používajú na ochranu a zároveň na vylepšenie bezpečnosti. Jednoduché činnosti ako monitorovanie siete schopné zachytiť neautorizované zariadenie, ako aj zabezpečenie riadenia prístupu, názorne ukazujú pridanú hodnotu investície. Ďalším príkladom je využitie systémovej bezpečnostnej infraštruktúry na zber štatistických údajov o prevádzke a aktivitách súvisiacich s bezpečnosťou siete. To umožní skvalitnenie procesov, ktoré môžu spoločnosti ušetriť nemalé peniaze – ideálny spôsob ako ukázať dobrú návratnosť investícií.

Najlepší spôsob ako dostať dobrý ukazovateľ ROI pre investíciu systémovej bezpečnosti je začať s rozumnými výdavkami. Načo platiť tisíce za bezpečnostný smerovač, keď lacnejší typ vie poskytnúť akceptovateľnú úroveň funkcionality. Pri hlbšom zamyslení sa nad požiadavkami vzťahujúcimi sa na miestnosti s diaľkovým prístupom sa ukáže, že je potrebný prepínač, smerovač, firewall, modem a dokonca zariadenie s VPN funkciou, čiže dovedna päť až šesť zariadení potrebných na vytvorenie spojenia medzi vzdialenou miestnosťou a korporatívnou sieťou. A čo tak použiť jediné zariadenie s rovnakou funkcionalitou a podobnou úrovňou bezpečnosti? Jedno zariadenie je takmer vždy lacnejšie ako niekoľko prístrojov, a pokiaľ aj nie je, tak jeho údržba istotne áno. Takéto nižšie náklady sa oveľa jednoduchšie obhajujú a reprezentujú aj zásadne lepší ukazovateľ ROI ako v prípade inštalácie niekoľkých zariadení.

Čoraz viac dát je z kategórie okamžitých a patriacich do oblasti reálneho času. Ako by sa mala spravovať taká záplava dát? Je možné predísť zahlteniu dátami?

Množstvo dát a informácií, ktoré sú v súčasnosti k dispozícii, je obrovský. Súčasné požiadavky na získavanie čo najväčšieho množstva dát, aby sa vďaka nim dospelo k tomu najlepšiemu rozhodnutiu, vedú k tomu, že sa takmer každý deň implementujú nové spôsoby získavania a zberu dát. Zvýšený dopyt sa zaznamenáva aj po dátach reálneho času. Schopnosť rýchlej reakcie na vzniknutú situáciu si vyžaduje nevyhnutnosť disponovať aktuálnymi dátami. Je čoraz očividnejšie, že príliš veľa informácií je rovnako neželané, ako príliš málo informácií. Je potrebné zrealizovať kroky, ktoré zabezpečia rozumnú správu toku informácií a neumožnia ich nekontrolovateľný príval.

Keď sa zamyslíte nad každodennými činnosťami, zistíte, že rozhodnutia si vyžadujú veľké množstvo informácií. Zoberme si jednoduchý príklad cesty do práce. Hodnotíte aktuálne počasie, aby ste zistili, či potrebujete dáždnik alebo teplejšie oblečenie. Kontrolujete príchod vlaku, či nemešká, dopravnú situáciu, aby ste boli načas na stanici, bankový účet, aby ste si mohli kúpiť lístok, cenu benzínu, či si ho môžete dovoliť. Tieto informácie sa zdajú triviálne, ale aké množstvo ich potrebujete, aby ste sa len dostali do práce. Predstavte si teraz, koľko informácií potrebujete, aby ste mohli v sieti zrealizovať implementáciu nového systému na prevenciu narušenia s redundantným zabezpečením proti výpadku.

Z toho enormného množstva informácií, o ktorých rozhodneme, že sú relevantné a iné zase nepotrebné? Ako posúdime, čo je spoľahlivý zdroj a čo nie? Čo urobíme s informáciami, keď ich dostaneme? Máme vôbec k dispozícii správne informácie? Jedna z najväčších výziev v súčasnosti je vyhodnocovanie získaných informácií a rozhodovanie, či sú použiteľné a čo s nimi potrebujeme urobiť. Príliš veľa informácií má na svedomí, že sa v nich pracovníci zúfalo prehrabávajú a náročne ich triedia a naopak, s malým množstvom informácií nie sú kompetentní ľudia v podniku schopní dospieť k adekvátnym rozhodnutiam. Informáciám je tiež potrebné dôverovať a pri nadmernej ponuke informačných zdrojov trvá príliš dlho, kým sa vyberie spoľahlivá informácia.

Situácia je zložitejšia tým, že dnes sa informácie bežne získavajú v reálnom čase, čo si vyžaduje vyhodnocovanie a analyzovanie konštantného toku dát ešte pred tým, než sa samotné dáta vôbec použijú. Množstvo zdrojov reálneho času, ktoré sú pracovníkovi k dispozícii, môže sťažovať ich schopnosť reakcie v priebehu času. Viete si napríklad predstaviť situáciu, že operátor dostáva v reálnom čase dáta z desiatich alebo tridsiatich čerpacích staníc naraz? Kvantum informácií zvyšuje pravdepodobnosť, že sa niečo prehliadne alebo pracovníka tak preťaží, že sa celá situácia stane neovládateľnou.

Informácie reálneho času sú však potrebné a medzičasom sa stali integrálnou súčasťou každodennej prevádzky. Je potrebné spravovať informácie takým spôsobom, aby sa koncový používateľ nestrácal v ich množstve. Jednou z ciest je zaobstarať systém automaticky spravujúci dáta reálneho času, monitorujúci priebehy veličín a špecifické parametre. Jeho úlohou je iba upozorňovať koncového používateľa na splnenie kritérií. Dáta reálneho času sú tak kedykoľvek k dispozícii, ale používateľ je ochránený pred veľkým objemom dát a zároveň je upozorňovaný na zásadné udalosti. Dá sa to porovnať napr. s databázou zbierajúcou všetky dáta reálneho času a vykonávajúcou analýzy priebehov. Z hľadiska SCADA systému je tok dát reálneho času podstatnou súčasťou jeho prevádzky.

Čo musia podľa vás zabezpečiť SCADA a IT inžinieri, keď chcú vytvoriť bezpečný prístup k vzdialeným SCADA inštaláciám?

Zabezpečenie prístupu k vzdialeným SCADA systémom je jednou z najprehliadanejších oblastí sieťovej bezpečnosti. V minulosti sa SCADA systémy spoliehali na to, že ako technológia boli neznáme a tým pádom bezpečné. Nikdy to nebol dobrý príklad bezpečnostných praktík, ale akceptoval sa ako možný spôsob. Dnes je čoraz viac SCADA systémov inštalovaných s podporou štandardného komunikačného protokolu akým je TCP/IP. V niektorých prípadoch sa tak SCADA inštalácie stávajú súčasťou bežnej sieťovej infraštruktúry a musia byť chránené ako ktorákoľvek iná sieť. Na vzdialený prístup ku SCADA systému sa kladú tri základné požiadavky – spoľahlivosť pripojenia, sieťová bezpečnosť a fyzické zabezpečenie. Tieto požiadavky síce nie sú pre SCADA systém nijako jedinečné, ale stávajú sa pre ne čoraz dôležitejšími.

Pravdepodobne najdôležitejšou požiadavkou je prvá menovaná. SCADA inštalácie ako elektrické rozvodne či vodné diela potrebujú mať k dispozícii vysoký stupeň spoľahlivosti pripojenia na zabezpečenie efektívnej prevádzky. V prípade ťažkostí totiž musia mať operátori vzdialený prístup na detekciu problému a prípadnú realizáciu potrebného úkonu. Z bezpečnostného hľadiska sa môže stratiť pripojenie do siete z dôvodu sabotáže alebo vandalizmu, čo v prípade poškodenia alebo krádeže zariadenia môže spôsobiť stratu tisícov eur. Spoľahlivosť zvyšujú redundantné linky, obzvlášť ak je záložná linka na báze inej technológie. Spoľahlivosť napríklad zvyšuje kombinácia ADSL telefónnej linky ako primárnej a bezdrôtového pripojenia v pozícii záložného pripojenia.

Druhá požiadavka je sieťová bezpečnosť. V IT prostredí sa infraštruktúra často skladá z interných a externých sietí, osobitnej siete DMZ a dokonca z izolovanej testovacej alebo vývojovej siete. Umožňuje to dôkladnú kontrolu prevádzky, prístupu a aktivít každej siete. Zariadenia v DMZ sieti napr. nemôžu posielať dáta do internej siete a podobne testovacia sieť môže posielať dáta iba do externej siete. Vzhľadom na to, že vzdialené SCADA inštalácie môžu byť bez obsluhy, je vhodné k nim pristupovať ako k potenciálnym narušiteľom a podniknúť opatrenia na striktnú kontrolu ich komunikácie smerom von. Takéto opatrenia sú na mieste, pretože ktokoľvek, kto prenikne do SCADA systému, môže získať prístup aj do korporatívnej siete. Rovnako to platí aj naopak, aby sa minimalizovalo riziko neautorizovaného prístupu do vzdialenej SCADA inštalácie.

Treťou požiadavkou je fyzické zabezpečenie. SCADA inštalácie disponujú výbavou v hodnote stoviek eur a tá je lákavým cieľom rôznych kriminálnych živlov. Fyzické zabezpečenie sa nachádza priamo na mieste, aby ochránilo technickú výbavu vrátane SCADA systému. To neznamená nevyhnutne napríklad elektrický plot, ale môže to byť rozvádzač odolný voči manipulácii upevnený na stene alebo plot z ostnatého drôtu okolo samotnej inštalácie. Viditeľné opatrenia ako ploty, poplašné systémy a strážne hliadky sú efektívne prostriedky fyzického zabezpečenia.

www.iqpc.com

-bb-