Kybernetická bezpečnosť systému DeltaV – prevádzková prax (2)

Aby bolo možné ochrániť systém DeltaV pred útokmi hekerov, vírusov, červov a iných nežiaducich aktivít a útokov na bezpečnosť, je potrebné, aby každý, kto prichádza do kontaktu s týmto systémom, dodržiaval definovanú množinu najlepších bezpečnostných postupov. V prvej časti článku bola diskutovaná téma dôležitosti správnej metodiky bezpečnosti a adekvátne školenie používateľov, opísané boli tri prvky bezpečnostného systému pre DeltaV a najlepšie spôsoby ich realizácie.

Detaily bezpečnosti systémy DeltaV

V tejto časti článku budú uvedené podrobnejšie informácie o bezpečnosti systému DeltaV. Informácie sú uvedené v logickej následnosti, kde základom je zabezpečenie systému v rámci nezávislej implementácie skôr, ako je do systému zavedený sieťový prístup.

Zabezpečenie samostatného systému DeltaV

Dokonca aj keď je systém izolovaný a nepripojený k iným komunikačným systémom, existujú bezpečnostné riziká, ktorými sa treba zaoberať. Primárnym krokom v rámci bezpečnosti je v takomto prípade zabezpečenie fyzickej vrstvy a prístupu lokálnych používateľov.

Obr.2 Uzamknutie pracovných staníc ako ochrana pred neautorizovaným prístupom

Prvá úroveň a primárny systém bezpečnosti je založený na obmedzenom fyzickom prístupe k pracovným staniciam DeltaV, sieťovým zariadeniam a regulátorom a V/V jednotkám. Myslíme si, že ako je nevyhnutné zabezpečiť bezpečnosť riadiacieho systému, podobne aj používateľ musí zabezpečiť prevádzku riadeným prístupom k fyzickým zariadeniam, miestnosti riadenia a prostrediu výroby, kde sú systémy rozmiestnené.

V rámci týchto priestorov najlepšie riešenia bezpečnosti odporúčajú:

- Regulátory a sieťové zariadenia by mali byť inštalované v uzavretých alebo zaplombovaných rozvádzačoch, ktoré neumožnia prístup neautorizovanému personálu. Sieťové prepínače by mali deaktivovať nepoužívané sieťové porty. Tak možno ochrániť interný prístup odpojením sieťového zariadenia pred prístupom alebo jednoduchým pripojením do nepoužívaného portu sieťového zariadenia.
- Aj keď sú počítače fyzicky zabezpečené v uzavretých rozvádzačoch, disketové a CD mechaniky by mali byť blokované alebo odpojené, aby sa zabránilo používateľom vniesť do systému vírusy a iný nevyžiadaný softvér.
- Aj v rozvádzači je možné, že personál údržby vyrobí problém tým, že použije neotestované CD alebo disketové nosiče. Každý takýto softvér musí byť chránený, a teda by mali existovať postupy na poriadnu verifikáciu, že daný softvér je bez vírusu.
- USB porty (okrem tých, ktoré sa používajú pre klávesnice, myši alebo periférie) by mali byť fyzicky odpojené, takže nemôžu byť prístupné pre neautorizovaných používateľov.
- Trasy sieťových káblov, obzvlášť vo vzdialených oblastiach, by mali byť tiež chránené pred ľahkým prístupom.

Prístup do miestnosti riadenia, v ktorej sú umiestnené operátorské konzoly, by tiež mal byť riadený – prinajmenšom z toho pohľadu, že zamestnanci v miestnosti riadenia majú kontrolovaný prístup k pracovným staniciam. Operátori by nemali opustiť otvorenú konzolu, ak je miestnosť riadenia bez dozoru. Konzoly by mali byť vždy zablokované, ak nie sú pod dohľadom.

Pri konzolách, ktoré sú umiestnené na vzdialenom mieste mimo miestnosti riadenia, by mali prevádzkové predpisy nariadiť odhlásenie sa alebo zamknutie konzoly, ak sa nepoužíva. Minimálne by mali byť konzoly nastavené tak, že v prípade krátkeho času nečinnosti sa automaticky obrazovka vypne – v tomto prípade sa odporúča ako hranica 2 minúty nečinnosti. Všetky počítače alebo iné inteligentné zariadenia pripojené do siete systému DeltaV pre účely údržby by mali byť skontrolované priamo na mieste, aby bolo zaistené, že skôr, ako budú pripojené, sú preskúšané na prítomnosť vírusov a nevyžiadaných programov.

Okrem toho by bolo potrebné vyžadovať autorizáciu aj od zamestnancov a návštevníkov prinášajúcich do podniku notebooky alebo iné prenosné zariadenia s možnosťou sieťového pripojenia (vrátane bezdrôtového ethernetového prístupu). Prostredníctvom takýchto nezabezpečených prenosných zariadení možno vykonať neautorizovaný prístup do siete a systémy sa môžu nakaziť vírusmi a nevyžiadanými softvérmi. Pomôckou pre zamestnancov podniku pri identifikovaní a ohlasovaní neautorizovaných zariadení môže byť napríklad to, že všetky autorizované zariadenia budú veľmi jednoducho identifikovateľné (vyhotovené v nápadnej farbe alebo označené nejakým viditeľným spôsobom), takže neautorizované zariadenia bude možné ľahko rozlíšiť. Aby sa zabránilo pripojeniu neautorizovaných bezdrôtových prístupových bodov do systému, malo by sa na miestach, kde sú inštalované sieťové zariadenia, zabezpečiť periodické skenovanie bezdrôtových signálov pomocou nenákladných monitorovacích zariadení bezdrôtového signálu.

Ak sú laptopy používané ako pracovné stanice DeltaV (ako riešenie nepodporované DeltaV), mali by sa využívať len pre funkcie DeltaV a nikdy by nemali byť pripojené do otvorených LAN. Aby sa zabezpečila izolácia systému, laptopy, ktoré sa zároveň používajú na všeobecné podnikové úlohy (s pripojením k internetu a e-mailu), by nikdy nemali byť použité ako pracovné stanice priamo pripojené do LAN siete systému DeltaV.

Prístup používateľov – bezpečnosť hesiel

Po zabezpečení fyzického prístupu je druhou úrovňou bezpečnosti systému DeltaV riadenie prístupu používateľov prostredníctvom schémy heslovej ochrany. Zaheslovaný prístup do DeltaV je viacúrovňový a poskytuje dve úrovne bezpečnosti a možnosť nastaviť bezpečnostné privilégiá pre každého používateľa podľa jeho pracovného zaradenia. Každý používateľ s autorizovaným prístupom do systému DeltaV musí mať používateľské konto Microsoft, ako aj používateľské konto DeltaV.

Obr.3 Laptopy môžu byť zdrojom nevyžiadaného softvéru a neautorizovaných sieťových pripojení

Heslá musia byť precízne spravované, aby sa zabránilo neautorizovanému prístupu ľudí, ktorí majú fyzický prístup k systému:

- prednastavené heslá musia byť zmazané,
- každému pracovníkovi musí byť pridelená presná úloha (rola),
- prístup používateľov musí byť precízne spravovaný,
- používatelia, ktorí už viac nepotrebujú prístup, musia byť zrušení,
- používatelia bez vážnych obchodných dôvodov nesmú mať do systému prístup,
- prístup do systému a politika hesiel by mali byť dostupné a povinné,
- nechránené alebo spoločne využívané používateľské mená a heslá by sa nemali používať.

Operačný systém Microsoft poskytuje bezpečnostné nastavenia, ktoré umožňujú každému používateľovi (alebo skupine používateľov) nastaviť špecifické Microsoft privilégiá pre prístup k určitým funkciám (napr. prístup k spusteniu, mazaniu alebo úprave súborov), aby sa zabránilo neautorizovaným používateľom pristupovať k súborom, programom a informáciám na pracovných staniciach. V rámci systému DeltaV je na administrátoroch individuálnych používateľov nastaviť správne tieto bezpečnostné funkcie, aby sa zabezpečila správna úroveň prístupu pre každého používateľa. Potom je už na samotnom používateľovi správne nastaviť privilégiá pre prístup k súborom a aplikáciám.

V každom prípade by nemali operátori poskytovať svoje osobné mená a heslá nikomu inému vrátane inžinierov a vedúcich pracovníkov. Podniky dbajúce na bezpečnosť by nemali používať nezabezpečené používateľské mená a heslá pre každého používateľa. Každý používateľ by mal mať osobné, privátne prihlasovacie nastavenia. Používateľ s autorizovaným prístupom k pracovnej stanici, ktorý však nie je používateľom DeltaV, nemôže mať prístup k softvéru a funkciám DeltaV. Možno teda poskytnúť administrovaný prístup do systému bez toho, aby bol poskytnutý akýkoľvek prístup k funkciám DeltaV.

Zabezpečený prístup – základ pracovného zaradenia

Systém DeltaV ponúka aj bezpečnosť na základe pracovného zaradenia. Každému používateľovi musia byť pridelené špecifické privilégiá na prístup do DeltaV aplikácií. Operátorom možno prideliť celopodnikovú autorizáciu alebo ich dosah riadenia môže byť obmedzený na priestor prevádzky s prístupom len k špecifickým funkciám prislúchajúcim ich pracovným úlohám alebo zaradeniu v rámci podniku. Inžinierom môžu byť pridelené len konfiguračné privilégiá bez možnosti sťahovania súborov alebo ovládania. Je na vlastníkovi podniku, aby zaškolil operátorov a ostatných používateľov do používania a aktualizácie hesiel.

Prevencia pred vírusmi a ich detekcia

Na základe skúseností z najlepších riešení odporúča Emerson Process Management minimálne nainštalovať antivírusový softvér na všetky pracovné stanice pripojené do vonkajších LAN. Na ďalšiu ochranu by mohli byť na každej pracovnej stanici v sieti DeltaV nainštalované antivírusové programy. Emerson Process Management podporuje aktuálnu verziu programu Symantec (Norton) Anti-Virus. K tejto téme je spracovaný samostatný článok „Symantec Anti-Virus and DeltaV“, zahŕňajúci špecifické hľadiská rozmiestnenia antivírusového softvéru v systéme DeltaV.

Softvér schválený pre pracovné stanice DeltaV

Bezpečnosť môže byť znížená aj inštaláciou neschváleného softvéru na pracovných staniciach DeltaV. Pod pojmom neschválený softvér máme na mysli každý softvér, ktorý nebol schválený administrátorom DeltaV systému pre inštaláciu na strane používateľa. Najlepším riešením je, aby len veľmi obmedzený počet pracovníkov zaradených do podpory systém mal práva pre nahrávanie softvéru a iné práva prislúchajúce administrátorovi. DeltaV si nevyžaduje prihlásenie pre získanie administrátorských práv pre konfiguráciu, prevádzku alebo nahranie systému DeltaV.

Zabezpečenie pripojeného systému DeltaV

Ako náhle používateľ vytvorí sieťové prepojenie na vonkajšie systémy, je potrebné brať do úvahy ďalšie doplňujúce aspekty bezpečnosti. Tieto sú doplnkom bezpečnostných opatrení, ktoré boli popísané v kapitole „Zabezpečenie samostatného systému DelteV“.

Všetky sieťové prepojenia medzi systémom DeltaV a podnikovými systémami alebo vonkajšou LAN musia byť realizované cez pracovné stanice DeltaV chránené smerovačom/firewallom. Priame prepojenie medzi vonkajšou LAN a sieťovými rozbočovačmi a prepínačmi systému DeltaV nie sú povolené alebo podporované. Prepojenie systému DeltaV využíva pre komunikáciu špecifické porty a všetky ostatné porty nevyužívané pre aplikácie DeltaV by mali byť uzavreté alebo nepovolené. Tým sa zabráni vytvoreniu možného spojenie cez ďalšie otvorené porty. V prípade, že ostatné porty sú požadované pre softvér inštalovaný používateľom, je možné povoliť otvorenie len týchto portov. Každé pripojenie k DeltaV aplikácii si vyžaduje istú úroveň autentifikácie používateľa (rovnako to platí pre pripojenie k DeltaV WebServer). Nakoľko prístup k systému je umožnený len pre určené osoby s právom pripojenia, nastavenie smerovača/firewallu by malo byť urobené tak, aby umožnilo pripojenie do systému len týmto určeným osobám alebo počítačom. Toto nastavenie by bolo možné pre zamedzenie neautorizovanému prístupu vykonať aj na nižšej úrovni, nakoľko pripojenia k DeltaV by nemali byť nastavené pre všeobecný prístup.

Všetky spojenia z vonku k systému DeltaV musia byť nastavené pre heslá špecifické pre jednotlivých pracovníkov. Bezpečnosť je možné ľahko dosiahnuť, ak pre prístup budú prideľované generické mená a heslá.

Väčšina spoločností alebo podnikov má definované isté pravidlá vytvárania a správy hesiel a tieto možno využiť aj pre používateľov riadiacich systémov. Odporúčame zaviesť prísne pravidlá vytvárania a správy hesiel, aby sa zabránilo jednoduchému odhaleniu hesla. Výmeny hesiel by sa mali pridŕžať celofiremných pravidiel, alebo by mali byť meniteľné s periódou 90 dní. Pevne stanovené heslá by sa nemali používať a počas implementácie systému by mali byť zmenené.

Za žiadnych okolností nesmie na pracovnej stanici systému DeltaV bežať e-mailová aplikácia alebo nezabezpečené, otvorené prepojenie na internet. Prepojovací firewall by mal blokovať všetky výstupné prepojenia alebo e-mailové prepojenia portu 80. Ak sa však ale požaduje pre operátorov prístup k e-mailu alebo internetu, je potom nevyhnutné pre takéto aplikácie využiť oddelené sieťové podnikové počítače nepripojené do LAN systému DeltaV.

V poslednej časti článku sa budeme zaoberať ochranou rozhrania do systému DeltaV ako aj použitím dvoch firewallov na zabezpečenie optimálnej bezpečnosti.

Pokračovanie v budúcom čísle.

EMERSON
Process Management

Emerson Process Management, spol. s r. o.

Železničiarska 13, 811 04 Bratislava
Tel.: 02/52 45 11 96, fax: 02/52 44 21 94
http://www.emersonprocess.com/SIS