Kybernetická bezpečnosť systému DeltaV – prevádzková prax (1)

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. Najlepšie postupy uvedené v tomto článku môžu byť chápané ako požiadavky alebo ako základné pravidlá na zabezpečenie bezpečnosti systému DeltaV. Je to na každej organizácii – zákazníkovi či integrátorovi – aby si vytvorila súbor vhodných bezpečnostných zásad pre všetky svoje organizačné zložky alebo kvôli tomu, aby dokázala pri špecifických situáciách vhodne reagovať.

Pre potreby tohto dokumentu opisujúceho najlepšie bezpečnostné postupy a v súlade so všeobecne prijatou terminológiou bude výraz „kybernetická bezpečnosť" zahŕňať všetky útoky na sieť nefyzickej povahy. Do tejto skupiny budú patriť preniknutie hekerov do siete, každý úmyselný alebo náhodný prístup neautorizovaného používateľa a objavenie sa vírusov, červov a iných škodlivých súborov s cieľom poškodiť činnosť siete alebo získať prístup k neverejným informáciám. Pojem „útok" bude zahŕňať vírusy, červy, trójske kone, malware a iný softvér umožňujúci automatické vniknutie, ako aj priamo smerované manuálne útoky osôb pracujúcich mimo riadiacej siete.

Metodika a školenie personálu – zásady bezpečnosti systému

Okrem najlepších postupov obsahujúcich technologické riešenia a fyzické zabezpečenie sú z hľadiska vytvorenia a správy kybernetickej bezpečnosti systému dôležité aj dobrá metodika bezpečnosti a adekvátne školenie používateľa.

Kľúčovým prvkom hĺbkovej ochrany (známej tiež ako prstencová, či kruhová ochrana) je vytvorenie zásad bezpečnosti. Kybernetická bezpečnosť systému je vlastne o riadení rizika. Aké navrhneme nastavenie bezpečnosti, aký operačný systém a bezpečnostné záplaty pre jednotlivé aplikácie nainštalujeme, aký firewall a aplikácie na odhalenie prieniku nasadíme – to všetko musí byť predmetom riadenia rizika. Efektívna bezpečnosť siete závisí od životaschopných, uskutočniteľných a vzájomne súvisiacich zásad bezpečnosti. Tie budú obsahovať hrozby (riziká) pre váš systém, aké hrozby ste schopní akceptovať a ktoré musíte čo najviac eliminovať. Jedine vďaka bezpečnostným zásadám sa môžete rozhodovať, ktoré hrozby musia byť akceptované a ktoré minimalizované. Len čo budú takéto zásady vytvorené, môžete začať s náležitým aplikovaním najlepších postupov pri prevádzke vášho systému. Bezpečnostné zásady tiež osvetlia riziká, ktoré bude najlepšie riešiť použitím vhodných technológií, a riziká, ktoré bude možné riešiť inými postupmi a školením personálu, aby získali vedomosti o hrozbách a spôsoboch útokov.

Využitie tohto článku o najlepších postupoch predpokladá, že už máte spracovanú nejakú úroveň bezpečnostných zásad, aby bolo možné povedať, ako a či každé z uvedených pravidiel by bolo použiteľné aj vo vašej prevádzke.

Celková kybernetická bezpečnosť systému

Naša celková bezpečnosť systému je postavená na troch prvkoch:

- **Fyzický prístup** – fyzická izolácia systémov riadenia v uzamknutých miestnostiach alebo rozvádzačoch kvôli zabezpečeniu neautorizovaného prístupu k zariadeniam.
- **Používateľský prístup** – autentifikácia a autorizácia – implementácia vhodnej bezpečnosti používateľských hesiel a riadenie prístupu na základe pracovného zaradenia kvôli predchádzaniu neautorizovaného prístupu k používateľským staniciam DeltaV v rámci celého podniku.
- **Oddelenie siete** – oddelenia siete DeltaV Control Network od podnikovej LAN a všetkých ostatných LAN s „otvoreným prístupom".

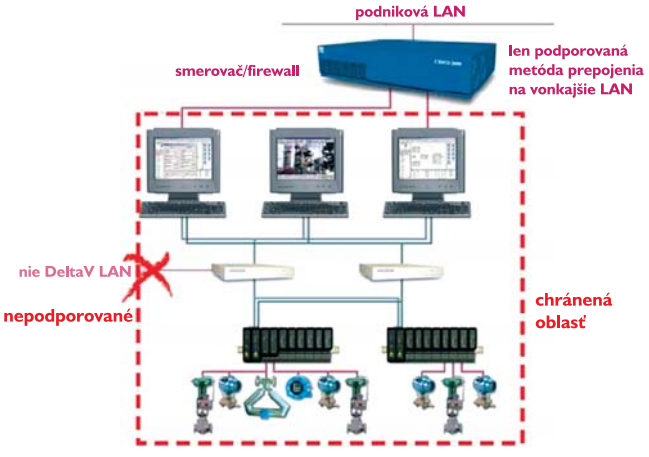
Metodológia návrhu systému

Systém DeltaV musí byť oddelený od podnikovej LAN.

1. Dodržiavajte zaužívané postupy systému DeltaV na konfiguráciu siete, v ktorej všetky prepojenia na podnikovú LAN musia byť realizované cez pracovné stanice DeltaV (obr. 1).
2. Sieťové prepojenia na podnikovú LAN by sa mali realizovať, len ak je to absolútne nevyhnutné na zabezpečenie prevádzky (procesu), údržbu systému alebo vzhľadom na opodstatnené dôvody z hľadiska povahy podnikania.
3. Zabezpečte, aby neexistovali žiadne iné siete, modemy alebo bezdrôtové spojenia zapracované do riadiacej siete okrem nevyhnutných prepojení, ktoré boli spomenuté v bode 2.
4. Každý modem, ktorý by mohol byť nainštalovaný pre potreby vzdialenej technickej podpory, musí byť identifikovaný a zabezpečený alebo vyradený z používania. Ak je modem potrebný, mal by byť nastavený na režim spätného potvrdzujúceho volania a mal by vyžadovať prístup cez používateľské heslo, keď na rozhranie modemu príde spätné potvrdzujúce volanie. Odpojenie modemu medzi jednotlivými používaniami sa neodporúča, pretože ak používateľ zabudne vypnúť zariadenie, zostáva prístup do systému otvorený.

Metódy konfigurácie a integrácie systému

Organizácie, ktoré sa venujú konfigurácii a integrácii systému DeltaV, sú zodpovedné za udržanie bezpečného prostredia pre systém DeltaV. Vírusy, červy a iný škodlivý softvér môžu útočiť na systém z ľubovoľného sieťového pripojenia. Vždy totiž možno tajne nainštalovať neočakávaný a nežiaduci softvér. Zaistenie bezpečnosti systému je teda dôležité už počas jeho integrácie. Nasledujúca časť najlepších postupov sa zvlášť venuje systému vo fáze jeho integrácie, bez ohľadu na to, kde sa táto úloha práve vykonáva.



Obr.1 Architektúra LAN systému DeltaV ho udržuje oddelený od podnikovej LAN

Ak je k dispozícii PC od Dell a boli zrealizované sieťové prepojenia do všetkých externých sietí, treba následne:

- nainštalovať posledné dostupné bezpečnostné záplaty od Microsoftu,
- nainštalovať posledné dostupné antivírusové programy do Symantec a antivírusové opisné súbory,
- aktualizovať antivírusové programy a antivírusové opisné súbory.

Operátorské stanice DeltaV možno nakonfigurovať tak, aby zabránili internetovým prehliadačom vytvoriť spojenie na internet. Používateľ pracovnej stanice nemôže mať nikdy možnosť otvoriť Internet Explorer a pripojiť sa na externú internetovú stránku.

Na žiadnej z pracovných staníc DeltaV nemôžu nikdy bežať žiadne e-mailové programy a do LAN siete systému DeltaV nemôže byť priamo pripojený žiaden počítač.

Počas inštalácie systému DeltaV by mali byť všetky pevne nastavené používateľské heslá zmenené, aby sa zabránilo prístupu neautorizovaných používateľov do systému. Jedine personál, ktorý vykonáva oživovanie systému, by mal vedieť heslá pre daný konkrétny systém. Kontá by mali byť nastavené v súlade s právami každého používateľa. Výsady administrátora by mali byť dostupné len niekoľkým ľuďom, ktorí sú za vykonávanie takýchto úloh zodpovední – vo všeobecnosti používateľom, ktorí realizujú úlohy oživovania.

Systém DeltaV by nemal byť pripojený k iným sieťam skôr, kým nie je adekvátne ochránený s korektne nastaveným firewallom. Firewall by mal presne určeným spôsobom blokovať každý z portov (všetky porty) na komunikáciu (internet) a každý port, ktorý by mohol byť využitý na e-mailovú komunikáciu. Všetky porty môžu byť blokované obojsmerne, okrem tých, ktoré sú potrebné pre aplikácie bežiace v rámci siete systému DeltaV.

Každá osoba vykonávajúca úlohy konfigurácie v systéme DeltaV by mala mať svoje jedinečné konto (špecifické používateľské meno a heslo), na základe čoho môžu byť presne kontrolované všetky aktivity daného používateľa. Všetky kontá používateľov, ktoré nie sú potrebné na nasadenie a oživenie systému, by mali byť pred odoslaním systému DeltaV zákazníkovi vymazané. Po nabehnutí systému do prevádzky by mali byť všetky kontá, ktoré nepatria používateľovi systému, zmazané.

Na zaistenie, že v systéme po implementácii budú len autorizované kontá nového používateľa, by mal nový administrátor zmeniť administrátorské heslo a zmazať všetky kontá dodávateľa systému. Ak sa v danej fáze napriek tomu vyžadujú kontá dodávateľa, používateľ by ich mal vytvoriť s príslušnými používateľskými kľúčmi. Striktne sa odporúča, aby tieto kontá mali pridelenú len obmedzenú schopnosť a po nevyhnutne potrebnom čase boli zrušené. Tieto kontá dodávateľa by mali byť prístupné len na čas nevyhnutne potrebný na vykonanie servisného zásahu a potom opätovne deaktivované.

Bežne dostupné laptopy alebo osobné počítače by sa nikdy nemali používať ako pracovné stanice DeltaV, ani by nemali byť nikdy pripojené do systému DeltaV. Prenos údajov medzi takýmito všeobecne použiteľnými laptopmi a osobnými počítačmi by sa mal uskutočniť prostredníctvom USB kľúčov alebo CD. Všetky prenosné médiá musia byť pred vložením do pracovnej stanice DeltaV zoskenované na prítomnosť vírusov.

Ak sa počas integrácie nájde počítač nainfikovaný vírusom, nemusí ho antivírusový program dokázať kompletne vyčistiť. Keďže sa mohli v rámci infiltrácie nainštalovať aj iné, neodhaliteľné zlomyseľné programy, je najlepším odporúčaním, aby sa harddisk takéhoto počítača znovu naformátoval a kompletne nainštaloval celý systém znovu. Robí sa to preto, aby bola istota, že po infekcii nezostala ani stopa a odstránili sa všetky nežiaduce zlomyseľné softvéry.

Cieľom týchto postupov je zabezpečiť, aby používateľ získal najvyššiu možnú úroveň kybernetickej ochrany a bezpečnosti systému. Integrátor musí byť schopný preukázať, že dokáže v každom čase udržať systém zákazníka v bezpečnom prostredí.

Stručný prehľad najlepších bezpečnostných postupov pre systém DeltaV

Základný systém bezpečnosti pre DeltaV možno implementovať a monitorovať relatívne jednoducho:

Fyzická bezpečnosť

- počítače a sieťové zariadenia by mali byť montované v zabezpečených rozvádzačoch,
- miestnosť riadenia by mala byť zabezpečená,
- otvorené, prihlásené pracovné stanice by nemali byť bez dozoru a bez toho, aby boli uzamknuté v pracovnom stole.

Antivírusová bezpečnosť

- antivírusové softvéry treba nainštalovať a udržiavať podľa návodu systému DeltaV,
- nepovoliť prístup k disketovej a CD mechanike,
- nepovoliť prístup k nevyužitým USB portom, špeciálne k tým na prednej strane PC (to môže vyžadovať fyzickú odinštaláciu týchto portov z počítača).

Bezpečnosť hesiel

- adekvátne udržiavajte zoznam používateľov – pridávajte len vyžiadaných používateľov a nepotrebných používateľov okamžite vymažte,
- nepoužívajte spoločne využívané používateľské mená a heslá,
- po inštalácii systému okamžite zmeňte všetky prednastavené heslá.

Sieťová bezpečnosť

- všetky podnikové LAN pripojenia do systému DeltaV musia byť realizované cez pracovné stanice,
- na oddelenie týchto pripojení z podnikovej LAN musia byť použité smerovače a firewally,
- zablokujte všetky sieťové porty okrem tých, ktoré sú nevyhnutné na prepojenie systému DeltaV,
- obmedzte počet používateľov, ktorý sa môžu pripojiť cez IP adresu, MAC adresu alebo iným podobným spôsobom,
- všetci používatelia musia mať svoje vlastné meno a heslo,
- obmedzte prístup len tým, ktorí prístup majú mať,
- rozlišujte prístup k údajom a prístup do systému, aby ste zabránili používateľom s právom len prehliadať údaje vstúpiť do systému,
- na optimálnu ochranu použite systém dvojitej firewallovej bezpečnostnej ochrany,
- pre aplikácie s vysokou prioritou bezpečnosti nainštalujte detekciu prienikov a pravidelné monitorovanie pripojení.

V ďalšej časti článku sa budeme venovať bezpečnosti systému DeltaV, kde budú uvedené prístupy opísané detailnejšie.

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