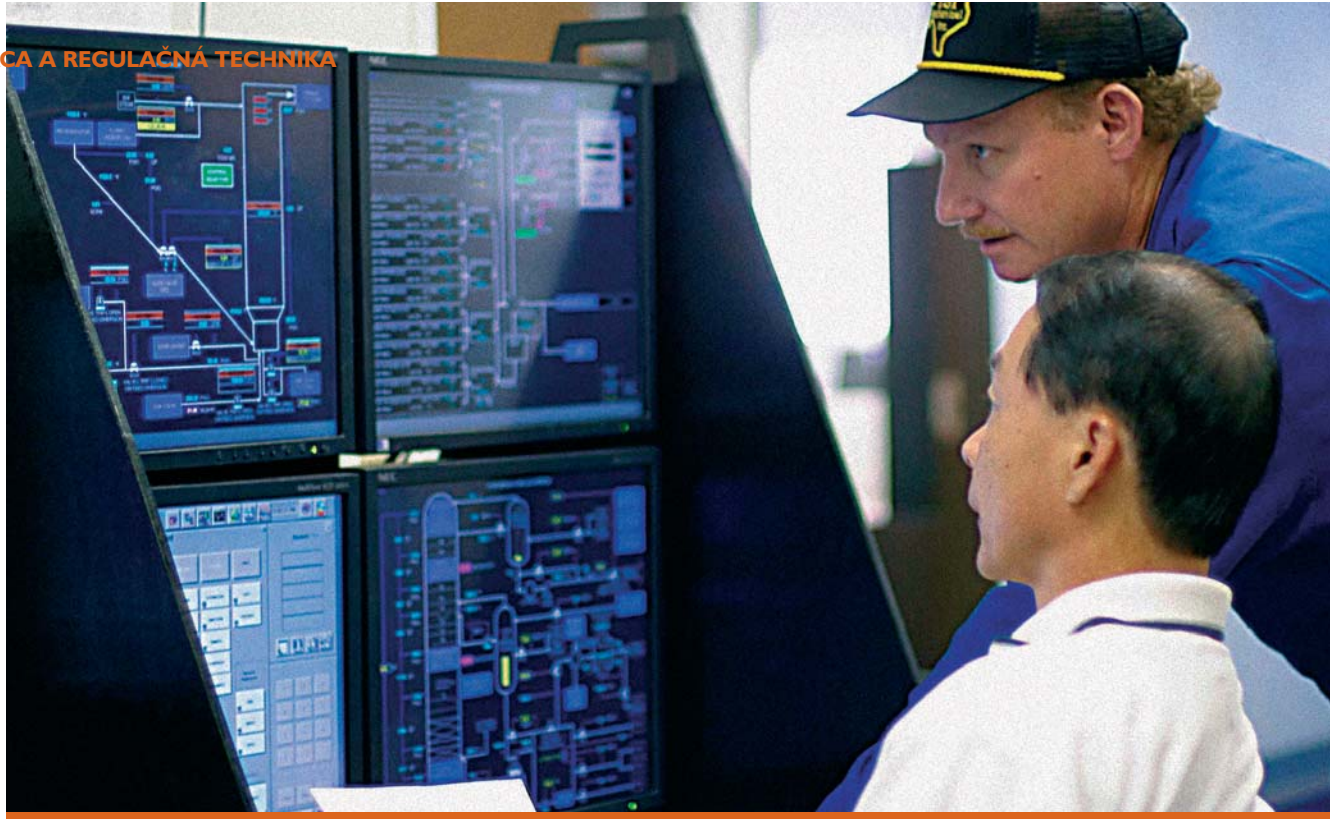
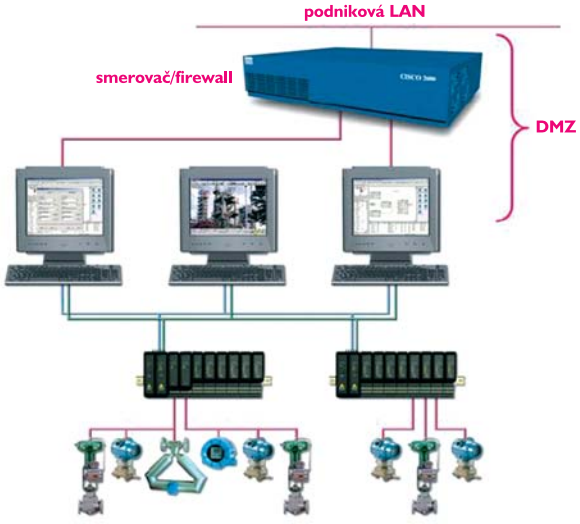


Kybernetická bezpečnosť systému DeltaV – prevádzková prax (3)

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 predchádzajúcich častiach článku sa diskutovalo o otázkach dôležitosti správnej metodiky bezpečnosti a adekvátnych školeniach používateľov, boli opísané tri prvky bezpečnostného systému pre DeltaV a najlepšie spôsoby ich realizácie, ako aj zásady ochrany nepripojeného a pripojeného systému DeltaV do vonkajšieho sieťového prostredia.

Ochrana sieťového rozhrania systému DeltaV

Spojenie medzi uzlom pracovnej stanice umiestnenom v sieti LAN systému DeltaV a externou LAN (v závislosti od toho, či je alebo nie je DeltaV inštalovaný na tomto uzle) musí byť minimálne chránené smerovačom/firewallom. Firewall by mohol byť nastavený tak, aby bol prístup do systému umožnený len konkrétnym používateľom a blokoval sa prístup cez iné porty, ktoré nie sú nevyhnutne potrebné na zabezpečenie prepojenia DeltaV na vonkajšiu LAN. Obzvlášť port 80 určený pre internet a všetky porty umožňujúce prístup e-mailovým aplikáciám



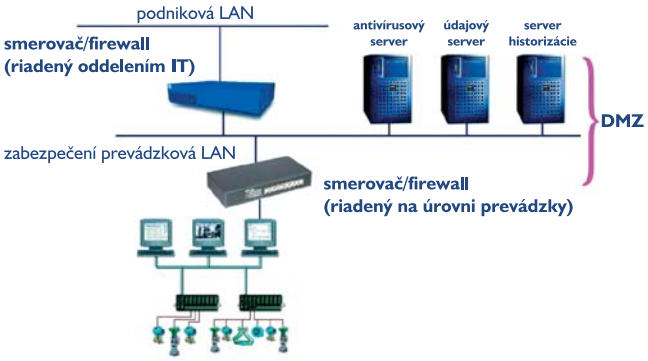
Obr.4 Všetky prepojenia musia byť realizované cez pracovnú stanicu a chránené cez firewall

musia byť uzavreté alebo blokované. Na správu prístupu cez pracovné stanice bolo vytvorené rozhranie nazývané demilitarizovaná zóna (DMZ), ktorá vytvára nárazníkovú/zásobníkovú zónu medzi LAN systému DeltaV a externou LAN.

Pracovná stanica je v tejto konfigurácii „neutrálnou zónou" medzi sieťou riadenia a podnikovou sieťou. Tým je zamedzený prístup používateľov z vrchných úrovní podniku od priameho prístupu k zariadeniam a sieti riadenia na úrovni prevádzky. Oddelenie tejto siete od podnikovej LAN výrazne znižuje možnosti neautorizovaného prístupu zvonku podniku alebo používateľov z podnikovej LAN, ktorí by nemali mať prístup do siete riadenia. Treba pritom brať ohľad na to, že ak sa používa firewall, treba vytvoriť a dodržiavať pravidlá riadenia zmien, aby sa predišlo neautorizovaným alebo neplatným zmenám, ktoré by mohli znížiť bezpečnosť prenosu príslušných údajov.

Použitie dvoch firewallov na optimalizáciu bezpečnosti

Odporúčaným riešením na dosiahnutie vysokého stavu bezpečnosti je použitie dvoch smerovačov/firewallov a vytvorenie bezpečne chránenej „prevádzkovej LAN" medzi riadiacim systémom a podnikovou LAN. Na obr. 5 je naznačené takéto riešenie. Pre optimalizáciu bezpečnosti sa odporúča, aby boli použité dva firewally od dvoch rôznych dodávateľov. Tým sa sťaží získanie kontroly nad LAN nejakému útočníkovi, pretože ak by sa mu aj podarilo prelomiť firewall na úrovni podnikovej LAN, bude nútený naučiť sa prelomenie firewallu iného typu. Tiež sa odporúča, aby bol prístup cez firewall riadiaceho systému riadený administrátorom prevádzky alebo výrobnej technológie/DeltaV, čím sa zabezpečí, že všetci jednotlivci budú mať pridelené správne systémové prístupy do pracovných staníc DeltaV.



Obr.5 Zdvojené firewally poskytujú bezpečnejší systém ako jeden firewall

Prístup k údajom vs. prístup k systému

Toto usporiadanie s dvojitým smerovačom/zabezpečenou prevádzkovou LAN prináša bezpečnosť založenú na koncepte prístupu k údajom vs. prístupu k systému. Väčšina vzdialených používateľov požaduje len prístup k údajom, aby si prezreli údaje z prevádzky, alebo aby si vedeli rady s poruchovými situáciami v prevádzke. To však nevyžaduje poskytnúť takýmto používateľom prístup k uzlu riadiaceho systému, pretože prístup k údajom na ich prácu stačí.

Prístup k údajom sa poskytuje používateľom na úrovni podnikovej LAN z údajového servera a zo servera historizácie. Systém DeltaV poskytuje prevádzkové údaje týmto serverom v reálnom čase alebo na vyžiadanie, takže používatelia na úrovni podnikovej LAN, ktorí potrebujú len prístup k údajom, sa nikdy nepripoja do uzla riadiaceho systému. Kvôli jednoznačnosti sú tieto funkcie k dispozícii na oddelených serveroch zapojených do siete LAN, avšak tieto funkcie môžu byť kombinované na jednom počítači pripojenom do LAN. Ak však možno jednoducho priradiť používateľov ku konkrétnym počítačom, je oveľa bezpečnejšie nainštalovať tieto funkcie na oddelené počítače. Tak sa používateľom povolí prístup len ku konkrétnym funkciám/údajom, ktoré potrebujú.

Antivírusový server pripojený k LAN sa používa na uchovávanie a distribúciu aktualizovaných opisov vírusov pre pracovné stanice DeltaV. Údaje o vírusoch sa na tento server prenášajú zo zabezpečeného uzla siete LAN alebo manuálne z CD. To zároveň umožňuje administrátorovi riadiaceho systému riadiť distribúciu DAT súborov pre uzly riadiaceho systému.

Vzdialeným používateľom, ktorí požadujú prístup k inžinierskym alebo administrátorským funkciám, možno prideliť systémový prístup do pracovných staníc pripojených do LAN systému DeltaV pomocou DeltaV RAS alebo DeltaV Remote Client. Aj keď je zvyčajne vzdialený prístup k týmto funkciám obmedzený len na špecifickú skupinu konečného počtu používateľov, dá sa oveľa jednoduchšie nakonfigurovať firewall do LAN siete riadiaceho systému. Tým sa umožní prístup len pre týchto jednotlivcov cez hardvérovú MAC adresu alebo statickú IP adresu a meno uzla klienta.

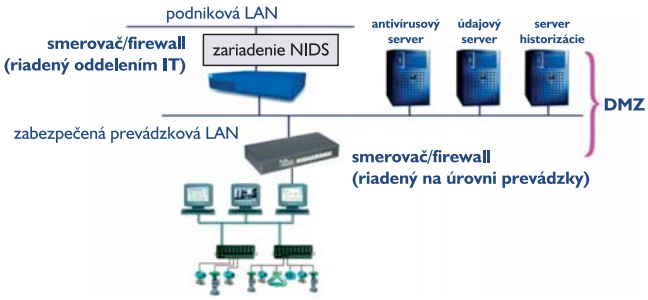
Obr.6 Sprístupnenie údajov z DMZ serverov pomáha kontrolovať nevyhnutné prístupy do riadiaceho systému

Detekcia prieniku

Systém na detekciu prieniku do siete (NIDS – Network Intruson Detection System) monitoruje pakety na kábloch siete a pokusy o prieskumy siete, ak sa útočník pokúša prelomiť do systému. Typickým príkladom je systém, ktorý sleduje veľký počet požiadaviek na TCP pripojenie na veľa rôznych portoch cieľového zariadenia, čím sa odhalí, ak sa niekto pokúša skenovať TCP port. NIDS môže bežať aj na cieľovom zariadení, čím sleduje prenosy na sebe samom (nepodporované na pracovných staniciach DeltaV) alebo na nezávislom zariadení striedavo monitorujúc celú sieťovú premávku (preferované riešenie DeltaV). „Sieťové" systémy na detekciu prieniku monitorujú mnohé zariadenia, zatiaľ čo iné systémy na detekciu prieniku monitorujú len jedno zariadenie (práve to, na ktorom sú nainštalované).

Pri väčšine sietí je NIDS umiestnený na firewallom chránenom pripojení z internetu do celofiremnej alebo podnikovej LAN. Takýmto spôsobom môžu byť votrelci odhalení predtým, ako sa dostanú do vnútornej LAN. NIDS tiež vyžaduje IT zdroje na monitorovanie komunikačných pripojení pre neštandardné aktivity, čo zvyšuje náklady na takéto riešenie. Opodstatnenosť ceny použitia NIDS medzi prevádzkovou a podnikovou LAN musí vzísť z analýzy rizika bezpečnosti riadiaceho systému, ktorú spracoval používateľ.

Ak sa NIDS používa ako súčasť riešenia ochrany systému DeltaV, možno ho nainštalovať medzi podnikovú LAN a smerovač/firewall podnikovej LAN. Záznamy z NIDS vyžadujú analýzu na odhalenie zákonitostí útokov/prienikov a toto je zvyčajne najlepšie prenechať odborníkom z IT firiem ako oddeleniam prevádzky.



Obr.7 NIDS môže poskytnúť dodatočnú bezpečnosť systému DeltaV

Zhrnutie

Vykonanie odhadu rizika systému a implementácia vhodných bezpečnostných opatrení uvedených v tomto článku umožní používateľovi vytvoriť adekvátnu a nákladovo efektívnu bezpečnosť pre automatizačný systém DeltaV. Ak by bola potrebná ďalšia pomoc pri vytváraní bezpečnosti systému DeltaV v tom-ktorom podniku, môžete kontaktovať pracovníkov implementácie z našej skupiny SureService, aby vám v tom pomohli.