advenica

LÖSNINGSBESKRIVNING

Säkra uppdateringar

Uppdateringar av Windows- och Linux-system är en viktig del i att kunna upprätthålla säkerheten för den digitala information som finns i dessa system. Uppdateringen kan dock innebära en säkerhetsrisk och för att undvika det samt för att upprätthålla integriteten och tillgängligheten i systemen krävs speciella lösningar.

Utmaning

Säker uppdatering av Windows- och Linux-system

Sedan man började med Windows- och/eller Linux-baserade system inom ICS/SCADA har behovet av att kunna uppdatera dessa system ökat. Detta behov beror på att komplex mjukvara ofta innehåller buggar som bör rättas till för att säkerställa stabilitet i systemen. Men förutom att korrigera buggar så driver tillverkarna bakom operativsystem och applikationer på en funktionstillväxt som innebär att operativsystem och applikationer successivt blir föråldrade om de inte uppdateras.

Säkerhetsbrister, eller i vissa fall buggar, kan utnyttjas av någon som vill åsamka skada, stjäla information eller kartlägga system, och detta är den ur säkerhetssynpunkt främsta anledningen till att uppdatera sina system. Men att göra dessa uppdateringar är något som i sig kan innebära en säkerhetsrisk om det inte görs på rätt sätt. Integritet och tillgänglighet till systemen måste upprätthållas och de flesta systemuppdateringar är normalt sett inte tillräckligt utvärderade i den miljö de används eller i kombination med de applikationer som körs. Dessutom innebär en uppdatering att information importeras eller tillförs till systemet och det i sig kan medföra att man får in oönskad malware in i systemet.

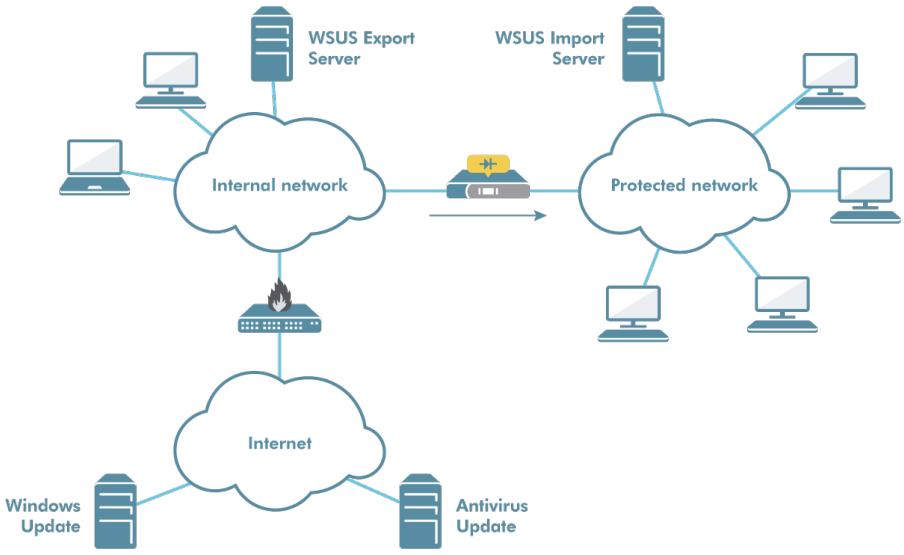
Lösning 1

Datadiod säkerställer enkelriktad kommunikation

Uppdateringen kan göras på ett säkert sätt genom att använda en datadiod som säkerställer enkelriktad kommunikation. Datadioden kopplas så att information kan importeras till systemet men eftersom ingen trafik kan överföras i motsatt riktning omöjliggörs informationsläckage.

Det man måste komma ihåg är att en datadiod inte har någon funktion som hindrar godtycklig information från att komma in i det skyddade systemet. Den uppgiften har den server som tar emot uppdateringspaketen inne i den skyddade miljön och som med hjälp av digitala signaturer säkerställer korrektheten i uppdateringspaketen innan de tillåts distribueras ut till andra system i miljön.

Kontroll av vilka uppdateringar som installeras har man i WSUS Export Server där man har möjlighet att välja ut de uppdateringspaket som ska installeras efter att man säkerställt att dessa kan importeras och installeras i de olika systemen i ICS/SCADA. Detta säkerställande uppnår man antingen genom att testa systemen i en egen testmiljö eller genom att de underleverantörer som levererat system till ICS/SCADA tillhandahåller denna information. Uppdateringar kan schemaläggas till ett tillfälle då tillgängligheten är mindre kritisk och eventuell nertid kan accepteras om något oförutsett skulle inträffa trots att man testat och kvalificerat uppdateringen.

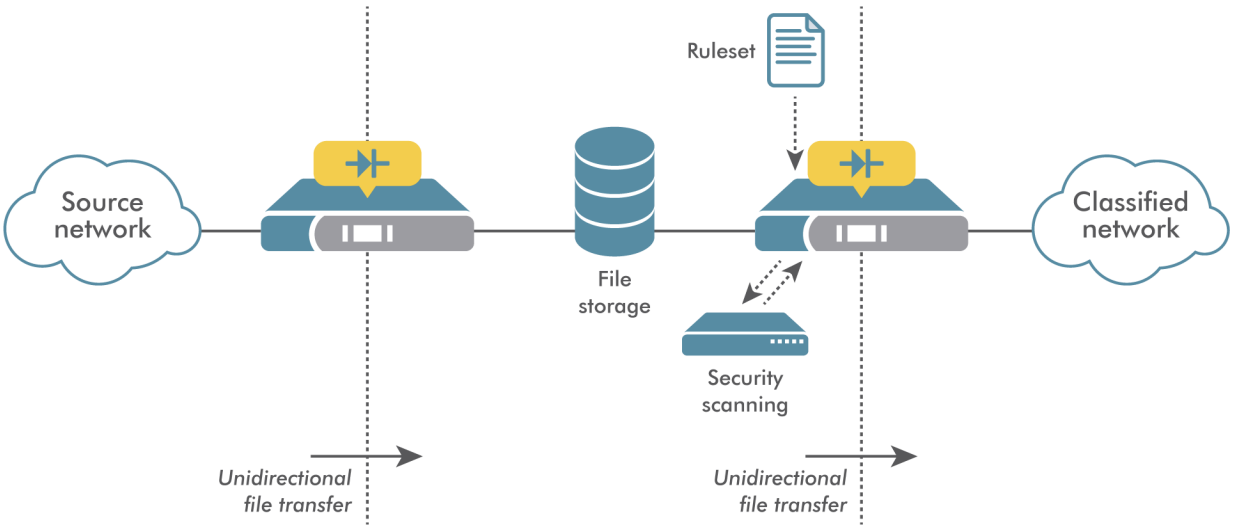


Lösning 2

Filtvätt säkerställer att uppdateringen är fri från skadlig kod

Vill man ytterligare säkerställa att uppdateringen inte blivit manipulerad kan importen av uppdateringsfiler göras via en så kallad filtvätt bestående av två datadioder och en server för antivirusskanning. Filtvätten utgör en oberoende kontroll av att uppdateringen är äkta. Dock så bör man även i detta fall låta mottagande WSUS Import Server verifiera signaturen och på så sätt få ytterligare en kontroll av uppdateringens riktighet.

Filtvätten kan även användas för import av andra typer av filer, t.ex. signaturfiler för antivirusmjukvara, uppdateringspaket för Linux-baserade system och import av helt godtyckliga filer. Kontroll och styrning av vilka uppdateringspaket som installeras utförs i WSUS Export Server på samma sätt som när man importerar över en datadiod (se lösning 1).



Fördelar

Bibehållen integritet och full kontroll

Denna lösning möjliggör import av uppdateringspaket utan att riskera informationsläckage. Eftersom uppdateringspaketens integritet kontrolleras i en skyddad miljö minimeras risken att få in oönskad skadlig kod i systemen. Väljer man att importera via en filtvätt så kontrolleras uppdateringens integritet av två oberoende säkerhetsmekanismer vilket ger ett bra djupförsvar.

Eftersom man endast släpper in de uppdateringar som testats och godkänts har man fullständig kontroll över vilka uppdateringar man tillåter. På detta sätt slipper man uppdateringar som annars riskerar att störa tillgängligheten av systemet.

advenica

Advenica tillhandahåller expertis, hög assurans och cybersäkerhetslösningar i världsklass för kritisk data-inmotion upp till Top Secret-klassning. Med oss stärker länder, myndigheter och företag informationssäkerheten och digitaliserar ansvarsfullt. Bolaget grundades 1993 och har EU-godkännande på högsta säkerhetsnivå. Våra unika produkter designas, utvecklas och tillverkas i Sverige.

Läs mer på advenica.com

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED