



LÖSNINGSBESKRIVNING

Säker IT/OT-integration

Digitaliseringen innebär att IT- och OT-system behöver kopplas samman. Denna integration är en utmaning ur säkerhetssynvinkel och kräver speciella lösningar.

Utmaning

Integrera IT och OT på ett säkert sätt

Operational Technology (OT) är ett begrepp som innefattar alla de delsystem som behövs för att styra och övervaka en fysisk process, exempelvis ett kraftverk eller en fabrik. OT består idag oftast av programmerbara styrsystem (PLC'er) och mätdatainsamlings- och kontrollsystem (SCADA). IT refererar till de affärs- och kontorsnära system som de flesta organisationer använder.

Historiskt har OT-system ofta varit helt frikopplade från omvärlden. I takt med samhällets digitalisering har behovet att koppla samman OT med omvärlden ökat. IT och OT kopplas därför samman, och ofta använder man samma typ av teknik inom IT och OT. De skilda behoven inom IT och OT leder lätt till tekniska konflikter som kan vara utmanande att hantera.

Lösning

Separera och kontrollera dataflöden

Separera IT och OT fysiskt med Zonindelning

Genom att separera IT och OT i separata segment kan man undvika att sårbarheter eller störningar inom IT påverkar OT. För att undvika risker som följer av misstag i konfiguration eller funktion bör man använda fysisk segmentering (Zonindelning). Det innebär att det är separat hårdvara som används för IT respektive OT.

Använd datadiod i Zongränsen för dataflöden ut från OT

Det säkraste sättet att koppla samman ett datanät, som inte skall kunna påverkas utifrån, med omvärlden är att använda datadioder. Alla dataflöden ut från OT som kan hanteras med datadioder medför en förenklad säkerhetsanalys, helt enkelt därför att datadioden är så lättanalyserad och säker, eller mer korrekt: har så hög assurances.

- **Speglning av databaser:** En metod att exportera data ut från OT-zonen är att spegla innehållet i en databas ut från OT-zonen. Genom att skapa en kopia av databasens innehåll på IT-sidan kan man tillåta läs rättigheter för alla de system som behöver ta del av databasinnehållet.
- **Export av XML:** En annan metod är att sätta samman en XML-fil inom OT-zonen med alla data som behövs utanför OT. Denna fil sänds sedan regelbundet med ftp/sftp till en mottagare i IT-zonen.
- **Speglning av skärmbild:** Ett vanligt behov är att kunna övervaka en process i OT-zonen från IT-zonen. Genom att skapa en skärmbild inne på OT-zonen och låta en kopia av bilden exporteras över zongränsen via en datadiod skapas realtidsobservation helt utan risk för att forbindelsen skall kunna utnyttjas för attacker mot OT-zonen. En identisk skärmvy visas även inom IT-zonen.

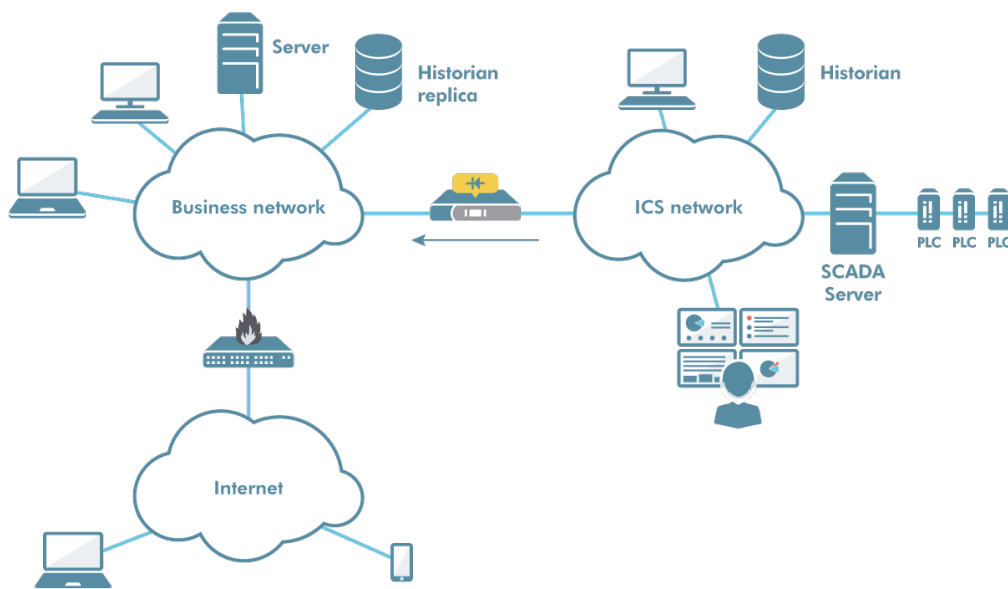
Tillåta viss information i zongränsen

För de dataflöden där datadioder inte är lämpliga kan man istället använda system som säkerställer informationsflödet, som till exempel ZoneGuard. För att undvika att skadlig kod kan komma in och påverka processen gäller det att strikt separera och kontrollera alla dataflöden över zongränsen. Den säkraste metoden är att strikt styra den information som tillåts passera zongränsen. Genom att förhindra till exempel transportprotokoll undviker man helt många av de risker som man annars skulle utsatts för.

Fördelar

Optimal avvägning mellan funktion och säkerhet

Genom att fysiskt zonindela IT och OT och utnyttja datadioder och ZoneGuards i zongränsen uppnår man en optimal avvägning mellan funktion och säkerhet. Digitaliseringen kan därmed accelereras utan att man äventyrar OTs tillgänglighet, samtidigt som man slipper lägga tid och kraft på att analysera de flöden som riktar sig ut från OT. Genom valet av Datadiod och ZoneGuard uppnår man en framtidssäker lösning som är avsevärt mindre sannolikt att den behöver korrigeras över tid, jämfört med en lösning baserad på traditionella brandväggar och intrångsdetekteringssystem. Läs mer om våra datadioder och ZoneGuard på advenica.com.



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

© Copyright 2020 Advenica AB. All rights reserved. Advenica and the Advenica logo are trademarks of Advenica AB. All registered and unregistered trademarks included in this publication are the sole property of their respective owner. Our policy of continuous development may cause the information and specifications contained herein to change without notice. Doc. no.: 18110 v1.1

ISO 9001
CERTIFIED
ISO 14001
CERTIFIED