Öka säkerheten i OT nätverket med hjälp av segmentering

Advitum AB
Franska vägen 11
393 56 Kalmar
T:0481-480 20

Område	Skapat av	Version
Dokumentnamn	Författare	1.0

Innehållsförteckning

Allmänt

Man pratar alltmer om cybersäkerhet både inom IT och OT miljöerna men tar man hoten på allvar?

Det är viktigt att man inte underskattar behovet av att se över just säkerheten och att man förstår hotbilden. Man har kanske inte varit så uppmärksam på hotbilden inom OT då man anser att det ha varit en skyddad miljö. Men mer och mer integreras OT miljöerna med IT system och ända upp i molnet. I denna artikel ta vi upp detta med att det är viktigt att säkra både IT och OT miljöerna då de idag hänger ihop mer och mer.

Självklart finns det många sätt och produkter att hantera/göra det med. Men i denna artikel ta vi upp det i allmänna termer.

Ett sätt att åstadkomma detta är att använda sig av nätverkssegmentering, övervakning och bra larmhantering.

Vad är nätverks segmentering

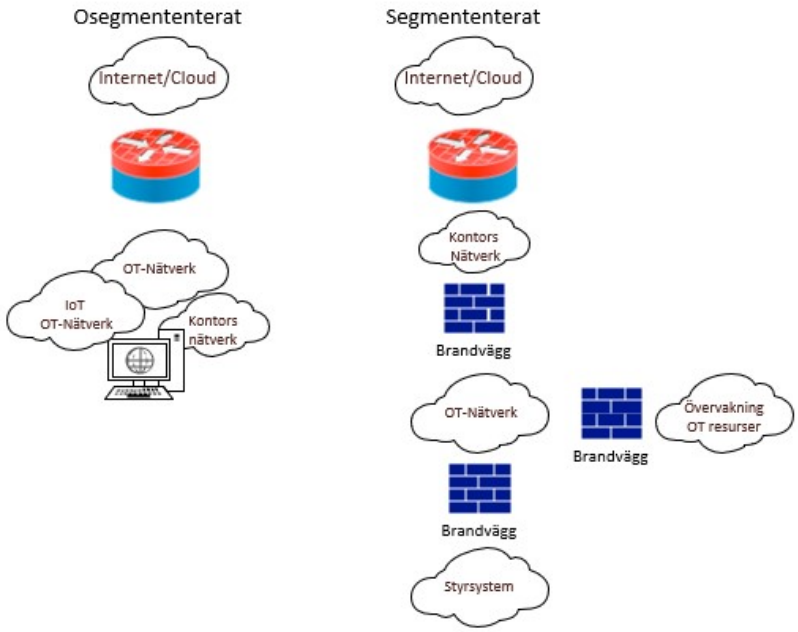
Närverkssegmentering är precis som namnet säger. Man segmenterar nätet. Man gör det genom att identifiera och analysera risker i sin infrastruktur och därmed klassificera de olika segmenten i sin IT/OT miljö.

Segmentering innebär att man helt enkelt delar upp nätverket i separata segment eller subnät och sära OT och IT miljön från varandra genom att skapa virtuella barriärer.
Detta tillåter då varje segment att fungera oberoende och skapar på detta sätt ett skydd mellan de olika nätverken.

Huvudsyftet med nätverkssegmentering är att förhindra säkerhetshot och spridning av dessa inom nätverket. Man kan på detta sätt isolera ett eventuellt hot inom ett segment utan att det skall påverka hela miljön genom att anpassa säkerhetsåtgärderna för att möta varje unik process/behov och sårbarhet i den sammansatta IT- och -OT-Miljö.

Design

Genom en tydlig strategi och balans i designen av infrastrukturen mellan säkerhet och tillgänglighet, möjliggörs att man bevarar de kritiska system och dess tillgångar inom de segment som kräver detta. Samtidigt som andra områden/segment har konfigurerats för mer anpassad åtkomst. Figur 1 visar en enkel bild på skillnaden på osegmenterat och segmenterat



Figur 1 Osegmenterat och Segmenterat nätverk

Segmentering i OT -Miljöer

Genom att segmentera inom industrin i s.k. OT-nätverk som i sin tur kan vara flera stycken baserade på funktion/process etc. Fördelen med att segmentera dessa är att skapa en motståndskraft och robusthet i den digitala infrastrukturen. Det är viktigt att organisationen förstår de fördelar det bär med sig att skapa denna segmentering för att på så sätt få kontroll över Cybersäkerheten, som innefattar regelöverenskommelse, incidenthantering, den operativa effektiviteten och den långsiktiga skalbarheten. Detta skapar många fördelar och motståndskraft på den digitala infrastrukturen som skall stå emot Cyberattacker och samtidigt kunna möjliggöra en säker produktion.

Genom att segmentera kan man begränsa de eventuella attackerna så att de inte drabbar hela nätverket. Detta gäller även om man skulle drabbas av en intern attack, vilket då kan isolera detta till enbart ett segment, vilket kan minska störningar och därmed bevara den övergripande produktiviteten. Avbrutna operationer i en process/verksamhet kan/är ofta kostsam, därav är det viktigt att man har full koll på sin infrastruktur i OT miljöerna.

Genom segmentering kan man även skapa en optimerad nätverksprestanda och säkerställa dataflödena på ett effektivt sätt.

Hantering underhåll och skalbarhet

En högre säkerhet kräver en hantering med mer precision och förvaltning. Detta p.g.a. att man måste genomföra uppdateringar, säkerhetsåtgärder samt konfigurationsändringar. Att en förvaltningsorganisation som ser till att detta fungerar garanterar och underlättar ett effektivt underhåll.

Vilka utmaningar finns då?

I befintliga miljöer är det oftast stora utmaningar som man måste hanteras i samband med att man vill införa segmentering av infrastrukturen. Problem som kan uppstå är.

Begränsning i äldre system/produkter, begränsad budget, och komplexiteten samt samsynen mellan OT och IT samt verksamheten kan göra att en implementation av segmentering är en utmanande och komplex process. Men med noggrann planering och strategier och en helhetssyn på cybersäkerhet blir det ett gemensamt mål för verksamheten och därmed skapande av en motståndskraftig infrastruktur.

Gamla system och infrastruktur

Hur hanterar man denna problematik?

Man bör göra en noggrann utvärdering för att identifiera de system som kan vara problematiska och som kan skapa kompabilitetsproblem med den nya tänkta lösningen. Det gäller att man identifierar dessa system i ett tidigt skede. Undersöka om det går att uppgradera till en nivå som är acceptabel eller om det går att virtualisera dem och på så sätt kunna isolera dem.

Implementation av segmentering

Ofta kan sådana projekt skapa en oro för driftstörningar i verksamheten vilket kan påverka produktionen.

Åtgärd för att minimera detta är noggrann planering, tester, se saker och ting i sitt sammanhang, försöka identifiera problemområden i ett tidigt skede och ta fram åtgärdsplaner för att minska riskerna.

Förändringsarbete

Oftast möts man av ett motstånd i en organisation när det kommer till förändringar. Detta avhjälper man med att ha med rätt resurser i ett projekt samt att involvera verksamheten i ett tidigt skede. Informera och utbilda personal för att få förståelse för processen.

Få med verksamheten, OT och IT organisation samt ledning för att på detta sätt få samsyn.

Samverkan mellan OT och IT

Att hitta rätt balans kring hur man skall hantera och driva cybersäkerhets frågor och som i detta fall att bygga en nätverkssegmentering kan vara en utmaning i en organisation.

Hur hanterar man då detta?

Genom att uppmuntra till en öppen kommunikation och samarbete mellan IT och OT team är avgörande. Se till att man har ett bra utbyte mellan organisationerna genom gemensamma system/utrustning. Regelbundna gemensamma möten och workshops och att man har en kunskapsöverföring mellan teamen. Detta kan underlätta och på så sätt skapa en bra harmoni i gruppen.

Utmaningen i de industriella miljöerna

Att införa en segmentering i de industriella miljöerna kan variera väldigt mycket mellan de olika industrierna gällande konfiguration, maskiner och processer.

Här är det viktigt att man försöker hitta och följa branschstandarder/regler. Det kan krävas experter på olika områden beroende på vilka lagkrav som organisationen kan drabbas av. Idag kan det handla om NIS och imorgon om NIS2 exempelvis. Processer etc måste ses över och tas hänsyn till. Ta hjälp av externa experter både för de efterlevnadsregler som kan finnas och designen av just den tekniska segmenteringen.

Underhåll och förvaltning

Underhåll, anpassning och övervakning kräver dock en större kunskap samt processer och rutiner.

Detta kan man hantera genom ett tydligt ägarskap av nätverket och dess processer och rutiner. Genom att ha en tydlig förändringsprocess och policys kan man effektivisera underhåll av dessa system. De är även viktigt att man har tydligt ansvar och mandat och att man hantera reguljära kvalitéts granskningar och riskbedömningar detta för att bibehålla och säkerställa att infrastrukturen/nätverket förbli säkert.

Sammanfattning

Att genomföra en nätverkssegmentering i den industriella miljön kan bestå av många olika utmaningar. Men om organisationen använder lämpliga strategier och metoder kan man på övervinna de hinder som kan finnas.

För att övervinna hindren måste man göra omfattande utvärderingar, se till att samarbetet fungerar och investera i utbildning och ha tydliga operativa mål. Genom att ha en proaktiv strategi säkerställer man att man kan genomföra en förändring i sin nätverksmiljö som då ger fördelar såsom förbättrad säkerhet, operativ effektivitet och efterlevnad av regelverk

Hur gör man då?

Förenklat är det som i de flesta projektet att man arbeta strategisk med detta och ha en tydlig bild av vad man vill åstadkomma, det som oftast kallas för effektmålen i samband med projekt.

I ett projekt för implementation av en segmenterad infrastruktur i en industriell miljö handlar det om ett antal steg.

Personen/Människan: identifiera vem och hur individen drabbas och se till att man har en tydlig information och utbildning för att få förståelse och ett bra samarbete, det måste vara ett gemensamt mål man strävar efter. Se till att ha tydliga roller, behöver organisationen ses över etc.

Analys och dokumentationsfasen: Se till att ha ett underlag som stämmer med verkligheten så som nätbeskrivningar, uppdatera anläggningsregister (assets), IP-planer att de är uppdaterade, nätstrukturer, brandväggar etc.

- Vilka svagheter/risker finns det i miljöerna?
- Vilka informationsflöden finns det?
- Analysera
- Dokumentera/dokumentera/dokumentera det är vad det hela handlar om

Man skall veta inte tro

Design: När det gäller design så kan man självklart göra det på många sätt men försök att hålla det till standarder så som IEC 62443. Eller rekommendationer så som ENISA tagit fram och föreslagit som en reviderad version av Purdue modellen. Good Practices for Security of the Internet of Things in the context of Smart Manufacturing. Vilken lösning man väljer skall framkomma i kravbilden på vad man kommer fram till i analysfasen och vilka effektmål man har att uppnå.

Implementationsfasen: Om man har gjort läxan i analys/dokumentations fasen och i Designfasen då skall man ha kommit fram till ett antal aktiviteter. Dessa aktiviteter kan vara enbart aktiviteter men kan också vara delprojekt i ett större implementations projekt.

Här gäller det att man följer en tydlig projektmodell som exempelvis Wenells projektmodell som vi på Advitum valt att arbeta med.

I implementationsfasen är det också viktigt att man har med utbildning av personal som skall hantera/övervaka anläggningen/nätverket.

Överlämning: När projektet lider mot sitt slut måste det finnas en mottagarorganisation som skall förvalta och vidareutveckla det projektet lämnar över. Det är mycket viktigt att denna organisation finns och är med i delar av projektet. Förvaltningsorganisationen är den som tar

emot och skall vara en del av organisationen som godkänner projektöverlämningen förutom diverse andra organisatoriska funktioner som redan innan projektet startas är utsedda för detta.

Sammanfattning

Ta Cyberhoten på allvar, de ökar väldigt mycket och även på OT system har man sett stor ökning av attacker. Se till att vara steget före. Man kan aldrig vara 100% säker men man kan göra så gott man kan. Ta kommandot och ha kontrollen. Att se över OT och IT miljöerna och identifiera riskerna, ta fram åtgärdsplan och se till att implementera dem, då har du kommit en bra bit på vägen. Det är inte bara en persons ansvar, det är hela organisationens ansvar. Var rädda om er.