

A female worker with blonde hair, wearing a yellow hard hat and a high-visibility yellow and blue safety vest over a grey shirt, is focused on a task. She is holding a black tool or cable and working on a piece of industrial machinery. The background shows a blurred industrial setting with blue and white structures. The overall image has a professional, industrial feel with white curved lines overlaid on the left and right sides.

axians

OT-säkerhet i praktiken

Hur Axians bygger robusta OT-miljöer

INNEHÅLL

SIDA

Sammanfattning	3
När OT och IT möts förändras riskbilden	5
Från överblick till kontroll	7
När design möter verklighet – erfarenheter från ett energiprojekt	8
Från punktinsatser till kontinuerlig insyn - därför har Axians valt Forescout	10
Slutord	12

Vill du komma i kontakt med oss?

Maila info.axiansse@axians.com
så kontaktar vi dig snarast möjligt.





SAMMANFATTNING

OT-miljöer har länge byggts med fokus på stabil drift, lång livslängd och hög tillgänglighet. I takt med att dessa miljöer kopplats ihop med IT, externa leverantörer och nya digitala tjänster har förutsättningarna förändrats radikalt. Det som tidigare kunde hållas isolerat behöver nu fungera i en mer uppkopplad och snabbföränderlig verklighet.

Här blir också skillnaden mellan traditionell företags-IT och OT som allra tydligast. Medan en IT-incident ofta handlar om administrativt avbrott eller förlorad data, sträcker sig ett intrång i en OT-miljö långt utanför företagets väggar. OT utgör ofta hjärtat i samhällskritisk infrastruktur – från energiförsörjning och vattenrening till transport och tung industri. Konsekvenserna av ett angrepp handlar därmed om omedelbar samhällspåverkan, bristande leveransförmåga och, i värsta fall, direkta hot mot människors fysiska säkerhet.

För att skydda dessa värden ökar nu kraven från regelverk och standarder som NIS2* och IEC 62443**. För verksamheter innebär det att OT-säkerhet inte längre kan hanteras som ett separat teknikområde, utan måste integreras som en del av den operativa och samhällskritiska helheten.

Axians arbetar med OT-säkerhet utifrån exakt den verkligheten. Vår roll är att skapa ordning i komplexa miljöer, bygga nätverk som håller i drift och etablera arbetssätt där hela kedjan hänger ihop. Det omfattar allt från säker design och implementation till kontinuerlig övervakning i vår SOC och effektiv incidenthantering.

För att stärka vår operativa förmåga har Axians valt Forescout som strategisk partner inom OT. Forescouts plattform gör det möjligt att upptäcka och klassificera anslutna IT-, OT, IoT och IoMT enheter med helt agentlösa och icke-intrusiva metoder. Det ger oss – och våra kunder – en kontinuerlig insyn och kontroll i miljöer där traditionella IT-säkerhetsmetoder ofta är direkt olämpliga att använda.

I detta Whitepaper beskriver vi hur vi på Axians ser på OT-säkerhet i praktiken: från den förändrade verkligheten i uppkopplade anläggningar, via konkreta arbetssätt och lärdomar från ett verkligt projekt, till varför kontinuerlig synlighet är nästa naturliga steg i ett långsiktigt säkerhetsarbete.





NÄR OT OCH IT MÖTS FÖRÄNDRAS RISKBILDEN

Operational Technology (OT) har traditionellt utvecklats i en värld där stabilitet gått före flexibilitet. System har byggts för att hålla länge, byts sällan ut och är ofta nära kopplade till den fysiska processen. När samma miljöer idag integreras med IT, fjärråtkomst, externa leverantörer och nya digitala arbetssätt uppstår en helt annan typ av beroenden – och nya sårbarheter – än tidigare.

Det märks inte alltid i teorin, men blir tydligt i praktiken. I många OT-miljöer finns äldre utrustning, många aktörer, oklar dokumentation och kommunikationsmönster som vuxit fram organiskt över tid. Här går det inte att utgå från att samma säkerhetsåtgärder som fungerar i traditionell IT också går att använda i en produktionsnära miljö.

I en traditionell IT-miljö hanteras sårbarheter rutinmässigt genom att systemen uppdateras och patchas. I en OT-miljö är detta ofta en omöjlighet. Att patcha ett äldre styrsystem, eller försöka bygga bort svagheter på komponentnivå, innebär ofta risk för kritiska driftstopp eller krav på att byta ut stora delar av OT-miljön mot helt ny utrustning.

Varje förändring måste ständigt vägas mot driftens absoluta krav på tillgänglighet, stabilitet och säkerhet. Vi måste helt enkelt kunna skydda miljöer som innehåller kända, opatchbara svagheter.

Det är därför synlighet blir en grundfråga. Den som inte vet exakt vilka enheter som finns i miljön, hur de kommunicerar och vilka berøenden som är kritiska, kan heller inte fatta välgrundade beslut om segmentering, åtkomst eller incidenthantering. Genom att få full synlighet i nätverket kan vi visualisera kommunikationen och införa kontroller som isolerar och begränsar trafiken. På så sätt minimerar vi effektivt möjligheten för en hotaktör att röra sig fritt i miljön och orsaka skada vid ett eventuellt intrång.

Vår erfarenhet är tydlig: OT-säkerhet börjar i många fall inte med nya verktyg, utan med att skapa en helt korrekt bild av verkligheten. Det är denna kontinuerliga synlighet som bygger grunden för att vår SOC ska kunna övervaka miljön och agera på hot i realtid, utan att störa den verksamhetskritiska driften.



FRÅN ÖVERBLICK TILL KONTROLL

När en tydlig bild av miljön väl finns på plats blir nästa steg att bygga in struktur och kontroll. För Axians handlar detta inte enbart om nätverksdesign, utan om att skapa en säkerhetsarkitektur som är logisk, väl dokumenterad och, framför allt, möjlig att förvalta över tid. Infrastrukturen blir i sig ett verktyg för att skapa transparens, optimera dataflöden och implementera den segmentering som krävs. Genom en genomtänkt design säkerställer vi att rätt kommunikation fungerar sömlöst, samtidigt som vi får den tekniska förmågan att effektivt isolera osäkra enheter och stoppa all oönskad trafik – utan att introducera nya risker för driften.

Men den tekniska grunden är bara halva lösningen; det operativa arbetet är minst lika viktigt. I praktiken måste ansvar, arbetsflöden och incidenthantering vara glasklara för att säkerheten inte ska störa produktionen. Det är här vår SOC knyter ihop övervakningen av arkitekturen, dygnet-runt-analys och ärendehantering till ett gemensamt, fungerande arbetssätt. Genom att integrera med ServiceNow skapar vi spårbarhet, rätt prioritering och tydlig struktur hela vägen från en upptäckt avvikelse till färdig åtgärd. Ambitionen är aldrig att lägga ett nytt, tungt lager av administration över kundens verksamhet, utan att få teknik och arbetssätt att samverka friktionsfritt.

Det är också i denna operationella vardag som skillnaden mellan tillfälliga punktinsatser och riktig, långsiktig förmåga blir som tydligast. En robust och säker OT-miljö byggs sällan i ett enda steg. Den utvecklas och stärks över tid när designval, drifterfarenhet, dokumentation och säkerhetsövervakning successivt integreras allt tätare.

NÄR DESIGN MÖTER VERKLIGHET - ERFARENHETER FRÅN ETT ENERGIPROJEKT

I ett pågående projekt inom energisektorn har Axians haft ansvar för att designa och etablera den säkra infrastrukturen för en ny digital anläggning. Projektet befinner sig just nu i testfas, där hela miljön körs under produktionslika förhållanden innan driftsättning. Det är i exakt den fasen som skillnaden mellan ritbord och verklighet blir som allra tydligast.

Under testningen har flera konkreta utmaningar uppstått. Det har handlat om buggar och fel i utrustning, där ett nära samarbete med hårdvaruleverantörer krävs för felsökning och åtgärd. Det har också uppstått oväntade beteenden i trafikflöden mellan olika delar av miljön – en tydlig påminnelse om varför full synlighet i nätverket är helt avgörande. Genom att visualisera dessa flöden har säkerhetsarkitekturen kunnat justeras, dokumenteras om och isoleras ytterligare. Den typen av arbete syns sällan i en högnivå-beskrivning, men är helt centralt för att begränsa oönskad trafik i verklig drift.

Redan i design- och planeringsfasen krävdes ett iterativt arbetssätt. Olika arkitekturvarianter testades i labbmiljö innan den slutliga lösningen fastställdes. Projektet har också inneburit att Axians behövt integrera kommunikationsmönster och standarder som skiljer sig markant från traditionella IT-miljöer, däribland det energispecifika protokollet IEC 61850***. Det har varit en central del av arbetet, eftersom OT-säkerhet inte bara handlar om teknisk kompetens, utan om djup förståelse för hur den fysiska, operativa processen faktiskt fungerar.

Axians ansvar i projektet har omfattat hela kedjan från säkerhetsdesign till implementation. Det inkluderar att ta fram en lösning som motsvarar upphandlingens hårda krav, välja rätt plattformar och mjukvaruversioner, samt leverera spårbar dokumentation för alla delar av miljön. Arbetet omfattar även uppsättning och den stundande driftsättningen.

Under testfasen har särskild vikt lagts vid att hålla miljön strikt kontrollerad och isolerad. Ingen extern access har tillåtits, all åtkomst har begränsats och hanterats genom säkra rutiner och isolerade åtkomstvägar designade för kritisk drift.

Målet har varit att leverera en robust och tillgänglig lösning med full insyn – en miljö där oönskad trafik effektivt blockeras och där det rätta fundamentet är på plats. I grund och botten handlar det om att skapa rätt förutsättningar för att på ett säkert sätt bygga optimerade OT-miljöer, samt att säkerställa att verksamheten har både rätt verktyg och en framtidssäker design för att kunna drifta och skydda anläggningen framgångsrikt över lång tid.





FRÅN PUNKTINSATS TILL KONTINUERLIG INSYN - DÄRFÖR HAR AXIANS VALT FORESCOUT

Projekt som detta visar vad OT-säkerhet kräver i praktiken: djup förståelse för säkerhetsarkitektur, disciplin i designarbetet och förmåga att hantera detaljer som bara blir synliga när miljön körs under realistiska förhållanden. Men de visar också något annat. När en stabil grund väl är etablerad uppstår behovet av mer än en korrekt design och god dokumentation. Verksamheten behöver också löpande veta exakt vad som faktiskt finns i miljön och hur den beter sig över tid.

Det är därför Axians har valt Forescout som strategisk partner inom OT. Forescouts plattform är helt inriktad på att skapa kontinuerlig synlighet och kontroll över anslutna enheter i IT-, OT- och IoT-miljöer. Plattformen använder agentlösa och icke-intrusiva metoder för att upptäcka, klassificera och följa enheter och kommunikationsmönster. Detta är särskilt kritiskt i miljöer där stabil drift alltid väger tyngre än möjligheten att installera agenter eller genomföra aktiva scannningar.



För oss på Axians är detta inte ett separat sidospår, utan en naturlig förlängning av det arbetssätt vi redan bygger upp i våra leveranser. När kontinuerlig synlighet kombineras med vår arkitekturkompetens, operativ SOC-förmåga och strukturerad incidenthantering i ServiceNow, blir det möjligt att gå från punktvisa förbättringar till en robust och långsiktig säkerhetsförmåga. Det skapar oslagbara underlag för prioriteringar, möjliggör snabbare upptäckt av förändringar och ger en helt ny nivå av kontroll i miljöer där konsekvenserna av fel beslut är oacceptabelt höga.

SLUTORD

OT-säkerhet handlar ytterst om att skapa kontroll i miljöer där teknik, drift och verksamhetskrav är tätt sammanvävda. Det går aldrig att lösa med en enskild produkt eller en copy-paste-metod från traditionell IT. Det kräver djup förståelse för hur miljön faktiskt fungerar, förmåga att bygga en säkerhetsarkitektur som håller i verklig drift, och processer som gör säkerhetsarbetet möjligt att upprätthålla över tid.

Axians bidrag är att omsätta detta i praktiken – från säker design och implementation till kontinuerlig övervakning, ärendehantering och vidareutveckling. Med Forescout som vald strategisk partner inom OT förstärks denna helhetsförmåga ytterligare genom oöverträffad synlighet och kontroll över miljön.

Tillsammans skapar vi de bästa möjliga förutsättningarna för att skydda affärs- och samhällskritiska miljöer. Allt utan att någonsin tappa fokus på det som alltid kommer först i OT: en stabil och säker drift.

Vill du komma i kontakt med oss?

Maila info.axiansse@axians.com så kontakter vi dig snarast möjligt.

OM AXIANS

Axians är en strategisk IT-outsourcing & Telekompartner som tar ett integrerat helhetsansvar för drift och cybersäkerhet hos både privata och samhällskritiska verksamheter. Som en del av den globala koncernen VINCI, har vi en unik fördel i att vi förstår och säkrar både traditionell IT och verksamhetskritiska industriella styrsystem (OT) på riktigt. Genom våra säkra svenska datacenter och vår dygnet-runt-övervakande SOC levererar vi en obruten säkerhetskedja som skyddar hela er affär, från kontorsnätverket hela vägen ut till fabriksgolvet.

Läs mer på www.axians.se

OM FORESCOUT

Forescout Technologies, Inc. är en global ledare inom cybersäkerhet som hjälper organisationer att identifiera, skydda och hantera risker i alla typer av cyberresurser – både hanterade och icke-hanterade – inklusive IT, OT, IoT och IoMT.

Läs mer på: www.forescout.com

FOTNOTER

**:NIS2 är ett EU-direktiv som syftar till att höja och skapa en gemensam, hög nivå av cybersäkerhet i hela EU. Det ställer striktare krav på företag och organisationer inom samhällsviktiga och kritiska sektorer när det gäller riskhantering, incidentrapportering och säkerhet i leverantörskedjan. <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>*

*** IEC 62443 (även känd som ISA/IEC 62443) är den internationella standardfamiljen för cybersäkerhet i industriella automations- och styrsystem (IACS). Den fungerar som ett ramverk för att skydda driftkritiska system (OT – Operational Technology) mot cyberattacker. <https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards>*

****: IEC 61850 är en internationell standard för kommunikation och system inom elkraftteknik, framför allt för transformatorstationer och ställverk. Den gör det möjligt för utrustning från olika tillverkare (som skyddsreläer, mätare och styrsystem) att "prata" med varandra och fungera sömlöst ihop (interoperabilitet). <https://energiforsk.se/program/elnatens-hallbara-teknikutveckling-och-digitalisering/projekt/iec61850-natverk/>*