advenica

Cybersäkerhet för energibolag

Så här kan energibolag säkra sin digitala infrastruktur

Med mer frekventa och alltmer aggressiva cyberattacker är IT-arkitekturens sårbarheter ett allvarligt hot för bolag idag. Hur du skyddar din digitala infrastruktur kan påverka din generella verksamhet och funktionen av fysiska processer. Energisektorn är särskilt utsatt för cyberattacker, vilket gör uppgraderad cybersäkerhet till något som behöver fokus.

Men hur går man tillväga? Vi har samlat information som hjälper dig att säkra både produktion och affärsvärde!

Artiklar

- Customer Case: Så skyddar energibolaget Wiener Netze sin infrastruktur
- Customer Case: Så säkrar stort svenskt energibolag sin drift
- Så skyddar du dina ICS- och SCADA-system
- Detta innebär standarden IEC 62443

Så skyddar energibolaget Wiener Netze sin infrastruktur

Wiener Netze, den största nätoperatören i Österrike, använder Advenicas datadioder för att kunna tillhandahålla fullständigt skydd av SCADA-system i OT-miljö.

Den största nätoperatören i Österrike har valt en produkt från det svenska cybersäkerhetsföretaget Advenica. Advenica är ett av få företag som har fått flera säkerhetscertifieringar (Secret UE/EU Secret, Swedish Hemlig/Top Secret, NATO Confidential och det nationella säkerhetscertifikatet i Österrike). Med hjälp av implementering av en högsäkerhetslösning på basis av datadioder isolerar Advenica fysiskt SCADA-systemen i Wiener Netzes OT-miljö för att kunna garantera fullständigt skydd och samtidigt garantera absolut säker kommunikation.

Datadioder säkrar envägskommunikation

Genom att garantera en hårdvarubaserad optisk separation av nätverk garanterar datadioden att informationen endast kan överföras i en riktning. Den avancerade produkten utvecklades för att uppfylla säkerhetskrav på högsta säkerhetsnivå och kan integreras i vilket system om helst.

”Eftersom lagen ålägger oss att ge bevis på vår säkerhet var det absolut nödvändigt att vi hittade en partner för denna känsliga fråga som vi kan lita blint på och som har komponenter med lämpliga säkerhetscertifikat”, förklarar Roman A. Tobler, chef för digital information och IKT-styrning vid Wiener Netze GmbH.

Wiener Netze

Wiener Netze är rankad som en av de mest innovativa leverantörerna i Europa, och levererar el, gas, fjärrvärme och data till miljontals människor i Wien och dess förorter. Produktion, handel och distribution separerades från nätverksverksamheten vid Wiener Stadtwerke när marknaden liberaliserades i början av 00-talet. Till följd av detta kombinerades el-, gas- och fjärrvärmenätet och även telekommunikationsnätet och allt integrerades i Wiener Netze. Wiener Netze har redan ett framåtriktat projekt på gång: den största utrullningen av smarta elmätare i de tysktalande regionerna.

Wiener Netze driver 47 transformatorstationer och cirka 12 000 transformatorer i Wien. En typisk applikation för datadioder är den automatiska omkopplaren i en transformatorstation, som måste styras från olika platser. Av säkerhetsskäl får den här delen av nätverket inte åtkomst till Internet och måste segregeras. Den övervakas med hjälp av ett SCADA-system. Om nätverket äventyras och mätningar manipuleras eller simuleras kan strömförsörjningen i ett helt distrikt brytas och angripare kan även orsaka en total mörkläggning.

Säker IT/OT-segmentering

På grund av konvergensen av modern IT-infrastruktur kan företag som Wiener Netze inte längre arbeta med flera olika IT-system. Därför behövs säkra luftluckor i nätverksgränssnittet, till exempel mellan kontorsnätverket och OT-nätverket, för att kvantifiera mängden el och gas som har styrts via ett specifikt rör, kontrollera var störningar uppstår och fastställa vilken information som behöver anmälas till myndigheterna. Det är just detta som datadioder används till - möjliggöra att kommunikation färdas i en riktning och förhindra att den färdas i andra riktningen med hjälp av både fysisk och galvanisk isolering. När detta har blivit säkerställt kan nätverket inte längre äventyras - inte ens vid överföringspunkter till angränsande nätoperatörer.

Så säkrar stort svenskt energibolag sin drift

Under senare år har energisektorn granskats av tillsynsmyndigheter gällande informationssäkerhet i förberedelse för exempelvis NIS-direktivet och en striktare nationell säkerhetslagstiftning. För att uppgradera säkerheten till att möta de strikt ställda kraven från tillsynsmyndigheten och samtidigt behålla tillgängligheten till digital information, kontaktade ett av landets största energibolag Advenica.

Loggdatahantering och övervakning

Med energibolagets affärsprioriteringar i åtanke beslutades det att loggdatahantering och övervakning var grundläggande för att skapa insikt och lägga grunden för ytterligare säkerhetsinsatser. Därför byggdes en ny loggmiljö för säkerhetsloggdata baserat på strikt segmentering tillsammans med godkända produkter för att skydda de olika systemen.

Datadioder med N3-godkännande

Advenicas SecuriCDS Data Diodes är nationellt godkända från försvaret och än idag ensamma om att ha godkännande på nivå N3 för användning på högsta säkerhetsnivån. De är det mest effektiva alternativet för klassificerade system. De innehåller en optisk fiber med en sändare på ena sidan och en mottagare på andra sidan vilket gör att endast ett enkelriktat informationsutbyte är möjligt. Trafik i backriktningen är fysiskt omöjlig och risken för läckage, manipulation av loggdata eller vidare förflyttning till andra nät är helt eliminerad. Advenicas SecuriCDS Data Diodes, som används på energibolaget, har integrerade proxyservrar. Dessa har utformats, utvecklats och testats för att uppfylla kraven för att interagera med känslig information i vanliga kommunikationsformer.

Säkert informationsutbyte med ZoneGuard

ZoneGuard implementerades för att ytterligare minska potentiella attackvektorer samtidigt som säker och selektiv tillgång till systemen från fjärranslutna nät tillhandahålls. Tekniken möjliggör säkert informationsutbyte mellan separata system, med tillgång som baseras på energibolagets definierade riktlinjer och inställningar för specifika system. Genom att använda ZoneGuard för att kontrollera fjärranslutningar, säkerställs korrekt åtkomst och tillåtet informationsutbyte. På så sätt säkras uppkopplingen mot både kända och okända hot som annars förknippas med en fjärranslutningslösning.

Tack vare Advenica kunde energibolaget snabbt uppnå ökad säkerhetsinsikt. De ökade sin beredskap för hot såsom Industroyer, vilket kan innebära stora konsekvenser och kostnader, inte bara för företaget, utan även för kunderna och till och med landet. Energibolaget kan nu även rapportera om godkända cybersäkerhetslösningar till tillsynsmyndigheter. Dessutom möjliggör både teknik och tjänster en kostnadseffektiv administration utan att äventyra nuvarande eller framtida tillförlitlighet och integritet.

Så skyddar du ICS- och SCADA-system

Med mer frekventa och alltmer aggressiva cyberattacker är IT-arkitekturens sårbarheter ett allvarligt hot för bolag idag. Energisektorn är särskilt utsatt vilket gör uppgraderad cybersäkerhet till en fråga inte bara om att säkra produktion och affärsvärde utan också av nationellt intresse för att hålla samhället i gång – och människor säkra.

Säkra Industrial Control Systems

För att skydda ICS-system (Industrial and Control Systems) och SCADA-system (Supervisory and Control Data Acquisition) behöver högassuranslösningar användas vid segmentering för att skydda den fysiska isoleringen och samtidigt möjliggöra en säker och pålitlig kommunikation.

Nästa prioritet är loggning. Genom att övervaka inloggningar, misslyckade inloggningsförsök, transaktioner, USB-användning etc. kan effektiva förebyggande åtgärder kartläggas och vid behov även införas omedelbart. Datans karaktär och arkitekturen kring loggdatainsamling gör emellertid loggservrar till en måltavla för attackerarna. Logghanteringssystemen blir alltså en måltavla och måste således vara tillräckligt skyddade. För att säkerställa integritet och säkerhet krävs därför hösassuranslösningar. Advenicas datadioder skapar en väg där all data endast kan flöda åt ett håll och blockerar därmed allt från utsidan. Om det är nödvändigt med ett dubbelriktat informationsflöde mellan domänerna, krävs ett högassuransfilter så som Advenicas ZoneGuard. Här inspekteras informationen i detalj och den godkänns endast om allt är enligt specifikation. Tack vare detta kan utvald information ändå överföras mellan domäner som inte får kopplas samman.

ICS & SCADA

Operational Technology (OT) är ett begrepp som innefattar alla de delsystem som behövs för att styra och övervaka en fysisk process, exempelvis ett kraftverk. OT består idag oftast av programmerbara styrsystem (PLC:er) och mätdatainsamlings- och kontrollsystem. ICS (Industrial and Control Systems) och SCADA (Supervisory and Control Data Acquisition) är benämningar som används på sådana system.

OT-system behöver kopplas 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.

Säker integration av IT/OT

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. Här är några lösningar som kan hjälpa till att skapa en säker integration av IT och OT:

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 en 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 assurans.

Tillåta viss information i zongränsen

För de dataflöden där datadioder inte är lämpliga kan man i stället 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 många av de risker som man annars skulle utsatts för.

Detta innebär standarden IEC 62443

IEC 62443 behandlar industriella styrsystem (ICS-system). Syftet med standarden är att förbättra integriteten, tillgängligheten och konfidentialiteten i komponenterna. Standarden anger även kriterier som kan styra hur man implementerar säkra system.

Vad innebär standarden?

Standarden består av fyra delar: general, policies and procedures, system och component. I stora drag kan man säga att standarden berör krav och processer för säkerhet inom ICS-system. Bland annat nämns det att användare måste autentiseras innan de får tillgång till systemet (vilket kan tyckas självklart) och att de ska få rätt grad av rättigheter, samt att deras aktiviteter ska övervakas.

Man ska även se till att systemen inte går att manipulera eller otillåtet kunna avslöja vilken slags information som finns i systemen. En annan aspekt är att tillgängligheten av systemens viktiga funktioner måste säkerställas, vilket med andra ord kallas resiliens. Systemen ska också delas in i zoner och dataflödet mellan dessa zoner ska begränsas. Det är av stor vikt att det finns ett system för incidenter, så kallad incidenthantering. Överträdelser ska alltså rapporteras till rätt instans och man ska även se till att åtgärder vidtas för att hantera överträdelsen.

Vem riktar sig standarden till?

Det kan röra sig om system- och anläggningsägare, men likväl leverantörer av både produkter och tjänster. Om du arbetar med säkerhet i industriella styrsystem är detta en standard du bör känna till!

IEC 62443

Standard IEC 62443 syftar till att förbättra industriella styrsystem och tillgängligheten, integriteten och konfidentialiteten i deras komponenter. Standarden har utvecklats av ISA (International Society of Automation) men publiceras av IEC (International Electrotechnical Commission).

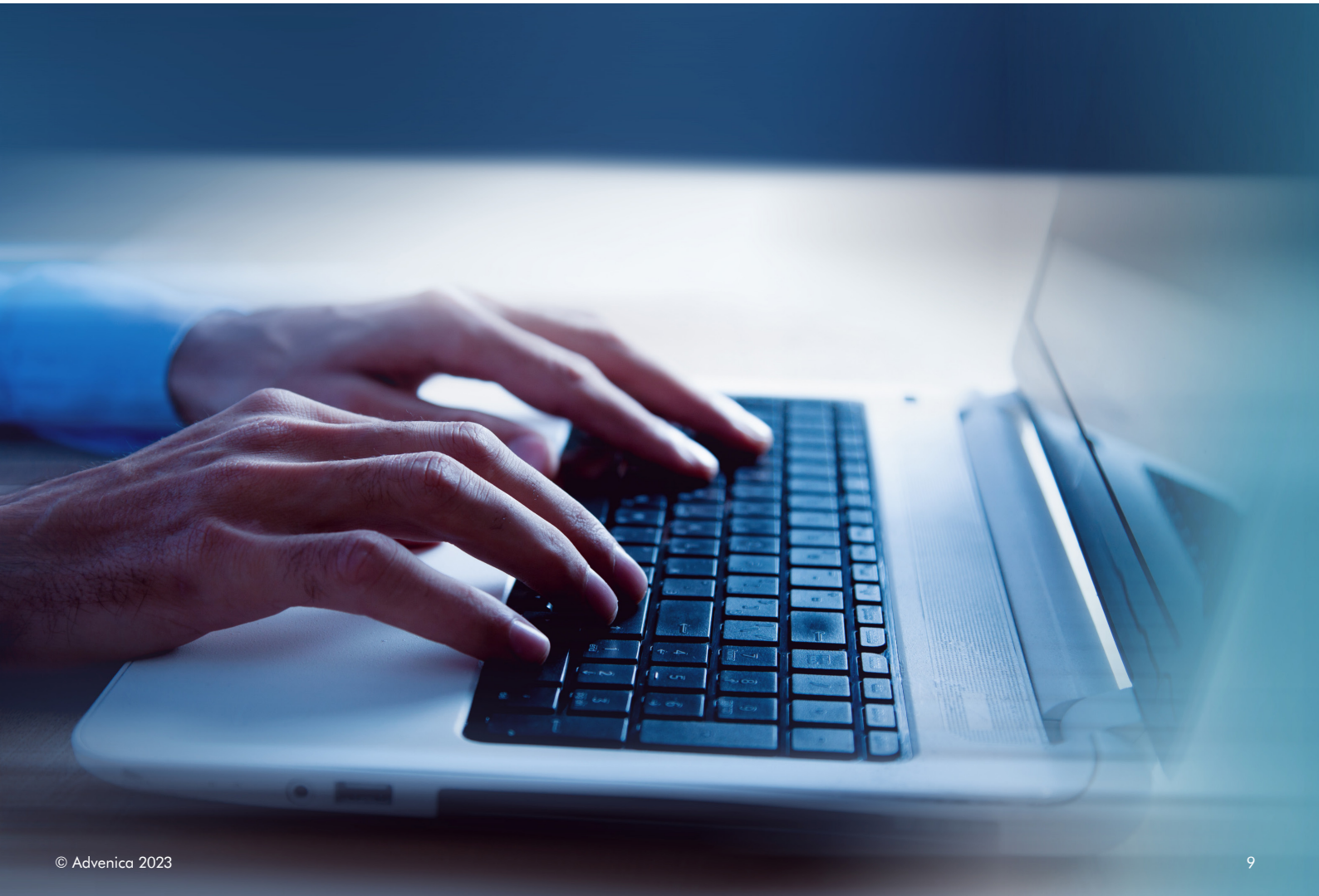
Riskanalys enligt IEC 62443

När man arbetar med cybersäkerhet och ska segmentera sina system i säkerhetszoner är det en god idé att använda sig av riskanalys. På detta sätt undviker man att säkerhetsarbetet blir utfört enligt en odefinierad ”ad hoc”-metod och dessutom blir det oftast enklare att förklara och motivera de investeringar man vill göra om man kan redogöra för vilka risker man åtgärdar eller reducerar. Standarden IEC 62443 är en bra metod att använda när man gör sin riskbaserade zonindelning.

Hur gör man en riskanalys?

I den initiala, enkla riskanalysen tittar man på ett worst case-scenario, alltså det värsta som kan hända i verksamheten. Här räknar man med att man inte vidtagit några åtgärder för att reducera de risker som finns. Man behöver en del input i denna fas, så som:

- Övergripande systemarkitektur – man behöver veta vilka system som ingår för att systematiskt kunna gå igenom dem.
- Riskkriterier och riskmatris med tolererbar risk – vilka risker kan vi acceptera och vad måste vi åtgärda? Hur mäter vi risk?
- Befintliga riskanalyser – har vi gjort någon slags riskanalys tidigare och kan använda oss av delar därifrån?
- Information om hotbild – vad skulle kunna hända? Vilka hot finns gentemot organisationen?



Advenica tillhandahåller expertis, hög assurans och cybersäkerhetslösningar i världsklass för kritisk data-in-motion 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

advenica

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED