advenica

Säker filtrering & validering av mätdata i GIS

Det finns en risk att OT-system (Operational Technology) och deras drift kan störas av hotagenter som riktar in sig på dataflöden mellan IT och OT. Med rätt lösningar kan man möjliggöra och tillåta en integration mellan IT och OT utan att riskera den känsliga OT-miljön.

Geographic Information Systems (GIS) kan integreras med, och hämta data från, system för övervakning, kontroll och datainsamling (SCADA). Detta möjliggör tjänster och funktioner baserade på realtidsdata som produceras av SCADA-systemet. I denna process samlas data in från SCADA och överförs till en databas varifrån data delas med andra applikationer relaterade till GIS som finns i kontorets IT-miljö. Därför finns det ett flöde av data mellan den känsliga OT-zonen och IT-zonen.

Utmaning

Attackvektor från IT till OT

Dataflöden mellan IT och OT kan potentiellt utnyttjas av hotagenter som försöker få åtkomst till, eller störa driften av, OT-systemen. Detta är särskilt relevant när det handlar om avancerade hotagenter som främmande stater eller välfinansierade och motiverade cyberbrottslingar.

IEC 62443

Standarden IEC 62443 med fokus på industriell cybersäkerhet säger att: *"Kommunikation över zongränser ska övervakas och kontrolleras för att säkerställa den zonindelning som definierats i den riskbaserade zonindelningen".*

Detta är ett krav för de som vill efterleva IEC 62443 och är ur ett säkerhetsperspektiv ett fullt rimligt krav vid skydd av en känslig OT-miljö. Så denna princip bör tillämpas oavsett om man vill efterleva IEC 62443 eller inte.

Ohärdade och opatchade servrar

Standard Windows- eller Linuxbaserade plattformar används i stor utsträckning i OT-miljöer idag. Att använda denna teknik har vissa fördelar, men kräver också kontinuerligt underhåll och patchning för att kunna fortsätta vara motståndskraftig mot nya sårbarheter som identifieras. Genom att utnyttja sårbarheter i plattformen,

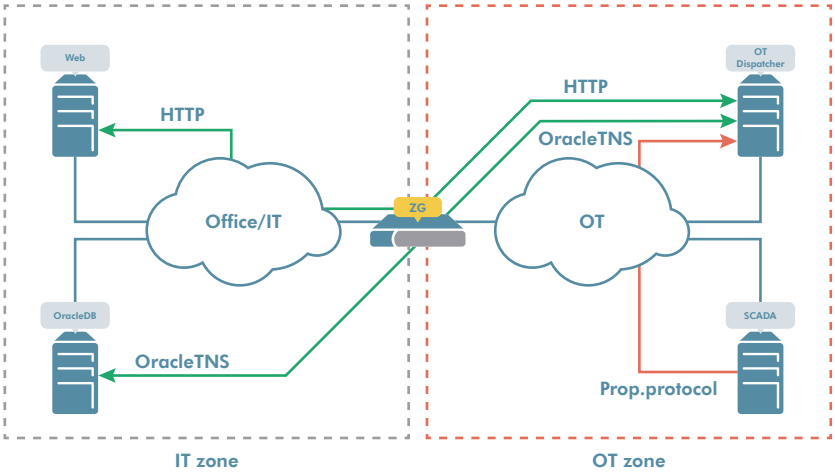
applikationen, eller i andra tjänster som körs i maskinen, körs godtycklig kod, privilegier eskaleras och på så vis tas maskinen över. Nya attacker kan därefter riktas mot SCADA och andra OT-system.

Lösning

Skydda OT-tjänsten och OT-maskinen med Advenicas ZoneGuard

OT-dispatcher-tjänsten och servermaskinen är skyddade med Advenicas ZoneGuard, en fristående enhet som från grunden utvecklats med säkerhet i fokus och har en härdad plattform och säkerhetsarkitektur med djupförsvar. Protokoll som används av GIS-applikationen är HTTP och OracleTNS. Dataflödena som består av HTTP- och OracleTNS-trafik valideras och enheten ser till att endast korrekt utformade protokollmeddelanden utbyts. Det säkerställs på så sätt att endast en godkänd delmängd (enligt specifikationen av OT-dispatcher-tjänsten) av HTTP- och OracleTNS-trafik kan komma in eller ut ur OT-zonen.

ZoneGuard with HTTP and OracleTNS protocol validation services,
validates traffic flow between the OT Dispatcher and the systems located in the IT zone



ZoneGuard utlöser ett larm och blockerar all misstänkt trafik. Den härdade implementationen i kombination med dess interna säkerhetsarkitektur gör det mycket svårt för en angripare att komma till OT-dispatcher-servern utan att bli upptäckt.

Fördelar

Djupförsvar med Advenicas ZoneGuard-teknik

Att skydda OT-servern med ZoneGuard-teknik mildrar attacker mot sårbara protokollstackar och serviceimplementationer. Dessa angrepp kan orsaka katastrofala konsekvenser om de sprids till ICS/SCADA-miljöerna. Dessutom tillämpas policybaserad filtrering på innehållet i protokollmeddelanden, vilket säkerställer att endast giltig data utbyts mellan IT och OT. Filtret anpassas enligt organisationens policy. Detta minskar hotvektorn, det vill säga möjliga vägar eller medel som en angripare kan använda för att få åtkomst till OT-servrarna. ZoneGuard stödjer hot standby mode och kan placeras i miljöer med krav på hög tillgänglighet.

advenica

Advenica tillhandahåller expertis, hög assurans och cybersäkerhetslösningar i världs-klass 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