advenica

ICCP/TASE.2
Säkert filter & validering

Risken för attacker mot ICCP-servrar är hög och kan få allvarliga konsekvenser. Att skydda ICCP-servern minskar angriparens möjlighet att sprida attacken via nätverket. Men att skydda den kräver speciella lösningar.

Inter-Control Center Communications Protocol (ICCP) enligt definitionen i IEC 60870-6 (TASE.2/ICCP) har specificerats för att tillhandahålla datautbyte mellan anläggningar där man kontrollerar produktion och distribution av elkraft. Att koppla samman system för produktion, överföring och distribution av elkraft möjliggör realtids- och historiskt datautbyte mellan regionala, nationella och till och med internationella elföretag. Den samordning som behövs på nuvarande och framtida energimarknader är beroende av säkert och pålitligt informationsutbyte. Dessa sammanlänkade anläggningar bildar ett nätverk som ibland täcker stora geografiska områden med miljontals invånare. Ett intrång som sprider sig över sådana nätverk kan därför påverka ett stort antal människor och organisationer. ICCP består av ett transportlager, ett sessionslager, ett presentationslager och ett applikationslager i OSI-modellen. I takt med att system och kontrollcenter blir sammanlänkade blir de också utsatta för nätverksbaserade attacker. Det finns idag ett begränsat antal implementationer av ICCP och därför använder leverantörer av ICCP-servrar ofta samma implementation. Därav kan en tidigare okänd sårbarhet i något av ICCP-protokollagren ha stora effekter på elnätet.

Utmaning

Få protokollimplementationer och ohärdade servermaskiner

Det finns flera olika attack-scenarier som är troliga mot ICCP-servrar, var och en med olika konsekvensnivå:

- Avlyssning eller manipulering av processdata.
- Denial-of-service-attacker eller fjärrexekvering av kod i ICCP-applikationen. Detta sker genom att utnyttja sårbarheter i implementationen och därmed störa tillgängligheten och/eller integriteten för servern.
- Exekvering av godtycklig kod på ICCP-servermaskinen. Genom att utnyttja sårbarheter i implementationen av ICCP-applikationen, eller i andra tjänster som körs i maskinen, körs godtycklig kod, privilegier eskaleras och följaktligen tas maskinen över. Nya attacker kan därefter startas mot antingen de lokala SCADA/ICS-systemen eller mot andra ICCP-servrar.

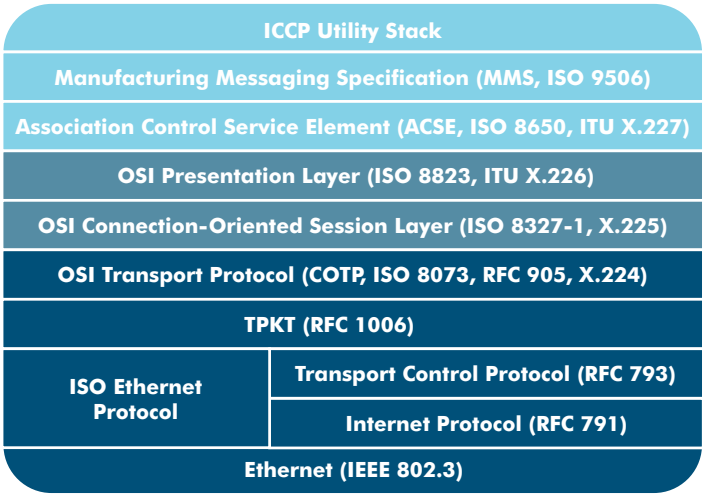
Begränsat antal implementationer

Säkerhetsproblem har rapporterats på implementationer av ICCP, men med tanke på den begränsade användningen av ICCP har detta inte fått mycket uppmärksamhet från säkerhetsforskare eller penetrationstestare. Man kan därför anta att det finns brister som ännu inte har upptäckts i implementationerna.

Betydande inverkan

En zero-day-sårbarhet skulle, på grund av det lilla antalet leverantörer av ICCP-stackar, göra det möjligt för angriparen att få en betydande inverkan på de tjänster som ICCP tillhandahåller. Angriparen skulle också bara behöva utveckla en enda exploit för att utföra attacken.

Det skulle krävas en hel del resurser för att hitta en sårbarhet, utveckla en exploit och utföra attacken. Hotagenter i form av statligt sponsrade agenter eller välfinansierade cyberbrottslingar kan dock enkelt mobilisera den mängd och typ av resurser. Med tanke på hur allvarliga effekterna är så bör ett sådant scenario inte diskvalificeras som osannolikt.



Figur 1. ICCP Utility-protokollstacken består av ett stort antal relativt ovanliga protokollager.

Brist på korrekt perimeterskydd

ICCP utbyts vanligtvis mellan organisationer på dedikerade nätverk (dvs. inte över öppna nätverk som internet). Brandväggar bör placeras mellan de olika organisationerna, men på grund av den snäva användningen och komplexiteten har dessa begränsat stöd för ICCP-protokollen och kan därför inte korrekt inspektera eller validera trafikens riktighet och släppa igenom eller avvisa felaktiga ICCP-paket. Det faktum att dessa nätverk är ”privata” ökar också risken att inte ha ett ordentligt perimeterskydd alls mellan organisationerna.

Brist på säkerhetsfunktioner

ICCP-stacken har väldigt få säkerhetsfunktioner för att adressera olika typer av hot. Säker ICCP, som ibland tas upp som botemedel, handlar om att skicka all ICCP-trafik genom en TLS-tunnel. Detta kommer att hindra alla från att avlyssna eller ansluta till ICCP-servern innan en säker TLS-session med servern upprättats. Men om någon skulle få åtkomst till någon av servrarna kan attacken ändå utföras genom de krypterade tunnlarna och fortfarande spridas okontrollerat över nätverket. ICCP-stacken måste, trots att säker ICCP är på plats, implementeras korrekt med avseende på säkerhet.

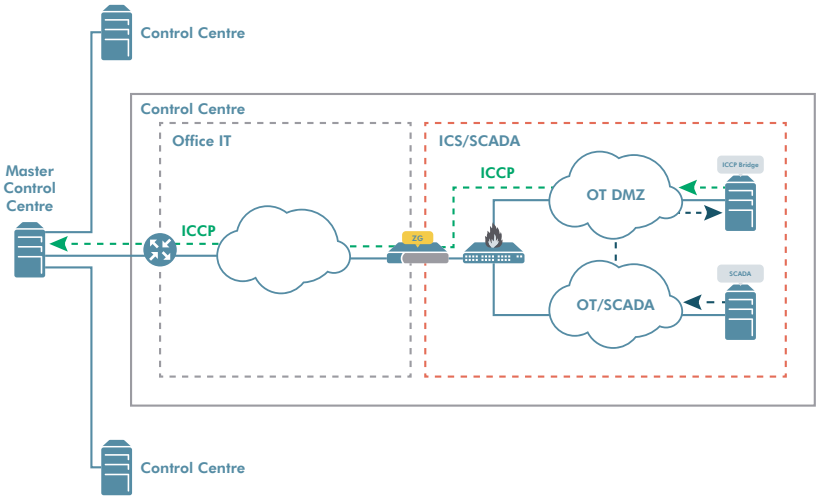
Ohärdade ICCP-servermaskiner

Operativsystemet, tjänster, processer och applikationer som finns på ICCP-servermaskinen är ofta sårbara för attacker. Opatchade och ohärdade Windows-maskiner används alltför frekvent av angripare för att få tillgång till system, inklusive ICS/SCADA.

Lösning

Skydda ICCP-applikationen och ICCP-servermaskinen med ZoneGuard

Serverns ICCP-applikation och serverplattform kan skyddas med Advenicas ZoneGuard, en fristående enhet utvecklad från grunden som en säkerhetsprodukt med en härdad säkerhetsplattform med hög säkerhet.



Figur 2. ZoneGuard med ICCP/TASE.2-protokollvalideringstjänsten validerar ICCP/TASE.2-trafikflödet mellan den lokala ICCP-servern/bryggan och kontrollcentralen.

ICCP-implementationen i ZoneGuard har inga relationer till någon av de kommersiellt tillgängliga protokollstackarna och det är därför osannolikt att en sårbarhet i en av de tillgängliga implementationerna finns i ZoneGuard. Ur ett djupförsvar-perspektiv får vi ytterligare en skyddsnivå som angriparen måste penetrera för att nå ICCP-servern. Skydd av ICCP-servern minskar angriparens möjlighet att sprida attacken över nätverket och ZoneGuards inbyggda intrångsdetekteringsfunktion kommer sannolikt att utlösas innan attacken har nått servern. ZoneGuards härdade ICCP-implementering i kombination med dess interna säkerhetsarkitektur gör det mycket svårt för en angripare att nå ICCP-servern utan att detekteras.

Fördelar

Djupförsvar genom Advenicas ZoneGuard-teknologi

Skydd av ICCP-servern med ZoneGuard-teknik mildrar attacker mot sårbara ICCP-protokollstackar och ICCP-servrar – angrepp som kan orsaka katastrofala konsekvenser om de sprids till ICS/SCADA-miljöer.

Alla system som använder ohärdade implementationer av ICCP har potentiella sårbarheter som kan utnyttjas av en angripare för att ta över system och sprida attacken över nätverket. Dessutom kan policybaserad filtrering tillämpas på innehållet i ICCP-meddelanden, vilket säkerställer att endast giltiga ICCP-data utbyts mellan kontrollcentren. Detta minskar attackvektorn, det vill säga möjliga vägar eller medel som en angripare kan använda för att få åtkomst till ICCP-servern.

advenica

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

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED