Myndigheten för samhällsskydd och beredskap

FAKTA

Publ.nr: MSB1293 – oktober 2018
AVDELNINGEN FÖR CYBERSÄKERHET OCH SKYDD AV SAMHÄLLSVIKTIG VERKSAMHET

Standard: ISA/IEC 62443

Det finns flera standarder och ramverk som har relevans för industriella informations- och styrsystem (ICS). En av dessa är ISA/IEC 62443 som trots att den är under utveckling redan används. Syftet med 62443 är att förbättra ICS och ICS-komponenternas tillgänglighet, integritet och konfidentialitet, samt att ge kriterier som kan användas vid anskaffning och implementering av säkra system. Standarden vänder sig såväl till systemägarae som till produkt- och tjänsteleverantörer.

Övergripande om IEC 62443

Totalt består 62443 serien av fyra övergripande delar. Var och en av dessa innefattar standarder av relevans för såväl system- och anläggningsägare som produkt- och tjänsteleverantörer. De övergripande delarna är:

- **General:** Behandlar ämnen gemensamma för hela serien, såsom begrepp och mått.
- **Policies and procedures:** Fokuserar på policyer och procedurer kopplade till ICS-säkerhet, såsom ”patch management”.
- **System:** Behandlar krav på systemnivå, såsom systemdesign och analys av säkerhetsrisker.
- **Component:** Behandlar krav för produktutveckling och komponenter för ICS.

ISA/IEC 62443

Är en serie standarder inom industriella informations- och styrsystem (ICS) området.

Relaterade standarder och ramverk

62443 brukar kompletteras med andra standarder beroende på behov. Det finns flera standardserier, och standardliknande dokument, som ligger mer eller mindre nära 62443. Exempel är: ISO 27000, IEC 62351, NIST Cyber Security Framework (NIST CSF) och NERC CIP.

ISO 27000

Behandlar ledningssystem för informationssäkerhet. Standarderna beskriver krav på ledningssystem för informationssäkerhet och för certifieringsorgan, men beskriver även olika generella processer och ger vägledning för exempelvis införandet av sådana ledningssystem.

IEC 62351

Behandlar informationssäkerhet för styrsystem inom kraftområdet (power system control operations). Serien är utformad för att främja säkerheten i enlighet med olika kommunikationsprotokoll.

De olika delarna är strukturerade enligt samma logik. Dels finns vissa grundläggande krav för säkerhet, dels en tanke rörandes segmentering som innebär att olika delar av ett och samma system kan tilldelas olika säkerhetsnivåer och därmed olika strikta krav.

De grundläggande kraven är förenklat det följande:

- **Identifiering och autentisering:** Att identifiera och autentisera alla användare innan de ges tillträde till kontrollsystemet
- **Användningskontroll:** Att tilldela alla användare rättigheter som styr vilka åtgärder de kan utföra på systemet samt att övervaka användningen.
- **Systemintegritet:** Att säkerställa systemets integritet genom att förhindra otillåten manipulation.
- **Konfidentialitet:** Att säkerställa informationens konfidentialitet genom att förhindra att den avslöjas otillåtet.
- **Begränsat dataflöde:** Att begränsa ett onödigt flöde av data genom att segmentera systemet via zoner och kanaler.
- **Incidenthantering:** Att svara på säkerhetsöverträdelser genom att varsla rätt instans, rapportera evidens och att vidta korrigerande åtgärder.
- **Tillgänglighet till resurser:** Att säkerställa tillgängligheten av systemets viktiga tjänster, alltså att säkerställa systemets resiliens.

Användning

Det är i nuläget inte fastställt hur utbredd användningen av 62443 är i Sverige, även om man kan se att det blir mer vanligt. En intervjustudie som har genomförts visar att standarden överlag uppges fungera som en målbild då alla delar av serien inte ännu är publicerade. På grund av detta så används inte alla delar av varje enskild användare. Utan snarare väljs de delar ut fungerar som är relevanta och applicerbara. Vilka delar som används beror på om man är systemägare, produkt- eller tjänsteleverantör, samt på vad man själv eller ens leverantörer klarar av. Detta faktablad baseras på NCS3 studien ”Standardserie ISA/IEC 62443: användning och erfarenheter bland svenska ICS-aktörer”, som finns att läsa på MSB:s hemsida.

NIST CSF

NIST CSF är utgivet av National Institute for Standards and Technology (NIST) i Usa. NIST CSF behandlar cybersäkerhet inom kritisk infrastruktur. Ramverket är leverantörsneutralt och bygger på samt hänvisar till flera redan föreliggande standarder och vägledningar.

NERC CIP

NERC CIP är utgiven av North American Electric Reliability Council (NERC) och behandlar cybersäkerhet hos stamnät och produktionsanläggningar, främst på nationell nivå.

Jämförelse

Vid en jämförelse av de olika ramverken och standardena så framkommer det att 62443 är både detaljerad och heltäckande, att 62351 är detaljerad men inte särskilt heltäckande medan NERC CIP, NIST CSF och ISO 27000 är heltäckande men inte särskilt detaljerade.

En jämförelse ger även att 62443 har en tonvikt mot operatörer även om den också är relevant för leverantörer. 62351 tycks omvänt ha en tonvikt mot leverantörerna, även om den också är relevant för operatörerna. NERC CIP, NIST CSF och ISO 27000 tycks ha en klar tonvikt gentemot operatörerna.

Norska DNVGL har tagit fram en best practise guide för tillämping av 62443 inom olje och gasindustrin

http://rules.dnvgl.com/docs/pdf/DNVGL/RP/2017-09/DNVGL-RP-G108.pdf

Kontakta Myndigheten för samhällsskydd och beredskap

651 81 Karlstad
MSB1292

registrator@msb.se
www.msb.se

msb.se/ics
scada@msb.se