Faktablad

Avdelningen för cybersäkerhet och säkra kommunikation
Publ.nr MSB1521 – mars 2020

Direkt trådlöst nätverksanslutna system

Antalet enheter i industriella informations- och styrsystem med möjlighet att ansluta till publika nätverk ökar. Detta är enheter med säkerhetsmässiga problem då dess fokus är tillförlitlighet snarare än it-säkerhet. Detta faktablad syftar till att beskriva ett antal säkerhetsaspekter som bör beaktas vid beslutsfattande, hantering och tillhandahållande av direkt trådlöst nätverksanslutna komponenter i industriella informationssystem (ICS).

Hot och risker

Majoriteten av problemen som uppstår med direkt trådlöst nätverksanslutna komponenter kan härledas till enheternas begränsade resurstillgång. Främst då säkerhetsmekanismer i regel designas och optimeras för stationära datorer och servrar med större resurstillgång. I detta faktablad lyfts sårbarheter kopplade till trådlös kommunikationsteknik, sårbarheter i hårdvara, samt administrativa problemställningar.

Trådlös kommunikationsteknik

Den trådlösa kommunikationen är angripbar från distans, då kommunikationen sker med hjälp av radiovågor och går inte att isolera likt den trådbundna. Därtill är trådlösa nätverk ofta konfiguerade ur användarsynpunkt och konfigurationen brister ofta ur säkerhetssynpunkt.

Sårbarheter i hårdvara

Hårdvarurelaterade sårbarheter kan delas in i tre typer:

Dolda kanaler, avser angrepp som utnyttjar mekanism som ej är avsedd för kommunikation, men med förmåga att kommunicera trots att det strider mot organisationens säkerhetspolicy.

Sidokanaler, en legitim kommunikationskanal som oavsiktligt avger information. Beror ofta på den fysiska implementationen av hårdvaran snarare än svagheter i teknik.

Direkt trådlöst nätverksanslutna system

I detta faktablad definierat som enheter och system med trådlös anslutningsmöjlighet som är direkt adresserabara från publika nätverk.

En enhet av mindre storlek, med begränsad beräknings- och lagringsförmåga. Exempelvis IoT-enheter, cyberfysiska system samt inbyggda system. Resurs-begränsningen innebär att enheter inte klarar av att hantera standardiserade krypterings-implementationer.

Skyddsbehov

Något som är i behov av att skyddas. Det kan vara en process, en verksamhet, information, byggnad, utrustning eller personer. Skyddsnivån och typ av skydd beror på behovet av konfidentialiet, riktighet och tillgänglighet.

Kryptering

Appliceras antingen på kommunikationsprotokoll, eller redan vara inkluderad i protokollet, genom exempelvis *Internet Protocol Security* (IPSec).

Autentisering

Används för att kontrollera identitetens riktighet vid kommunikation. Kryptografiska hashfunktioner utgör grunden i både digital signaturer och Message Authentication Codes (MAC). SHA-2 och SHA-3 är rekommenderade hashfunktioner

Kontakta oss:
Tel: 0771-240 240
registrator@msb.se
www.msb.se

Myndigheten för samhällsskydd och beredskap

Majoriteten av angrepp kräver fysisk tillgång till den enhet som avses utnyttjas.

Okänd funktionalitet, ett chipset tillverkas ofta med flera kommunikationskanaler. Stängs inte kommunikationskanaler som ej används skapas alternativa kanaler vilka kan utnyttjas för informationsläckage.

Administrativa problemställningar

När det gäller administrativa problemställningar nämns övergången från IPv4 till IPv6 samt implementation och kvalitetssäkring som exempel på administrativa problemställningar. Vid övergång till IPv6 utökas adressrymden vilket möjliggör att enheter ges unika adresser och görs direkt adresserbara. Detta resulterar i att möjligheten till åtkomst till dessa enheter ökar. När det gäller implementation och kvalitetssäkring bör det beaktas att 23 procent av alla incidenter inom ICS härleds till mjukvarufel.

Slutsats och rekommendationer

Säkerhetshoten rörande direkt trådlöst nätverksanslutna system kan till viss del hanteras. Nedan följer rekommendationer för att öka säkerheten i dessa typer av system.

- Administrativa beslut bör utgå från organisationens behov, men baseras på vedertagna standarder (IEC 62433, ISO/IEC 29191-1:2012).
- Dolda kommunikationsmöjligheter kan existera. Kartlägg därför kommunikationstekniker hos de tänkta enheterna tidigt i inköpsprocessen.
- Valet av kommunikationsprotokoll bör baseras på organisationens behov, och graden av skydd baseras på informationens skyddsbehov.
- Kvalitetssäkra och undvik fel genom att iterativt testa all kod, samt åtgärda fel, tills programmet är funktionellt korrekt.
- Beräkningssnål kryptering finns att tillgå. Ett alternativ kan vara att applicera en mellanliggande enhet vilken hanterar kryptering och dekryptering.
- Nätverkssegmentering är särskilt viktigt om säkerhetsmekanismer på enhetsnivå är begränsade eller obefintliga.

För ytterligare information och rekommendationer hänvisas till MSB:s hemsida.

Nätverkssegmentering

Minskar risken för spridning av skadlig kod mellan olika enheter. Genom att dela upp nätverket i olika zoner kan kritiska enheter isoleras från andra delar av nätverket i syfte att upprätthålla kritisk funktionalitet även under ett pågående angrepp eller störning.

Standarder

IEC 62443 erbjuder ett stöd vid kravställning och riskbedömning, snarlikt 27000-serien. Dock ställer IEC 62443 inga specifika krav på användarteknik.

Standarden beskriver istället ett antal principiella, välkända, säkerhetsmekanismer samt hur beslutsfattare och säkerhetsansvariga bör resonera kring dessa i relation till de hot och sårbarheter som identifieras.

IEC 62443 bör beaktas i alla säkerhetsrelaterade uppdrag inom ICS. Standarden presenterar åtgärder i form av krav, exempelvis:

- Nätverkssegmentering
- Isolera kritiska systemdelar
- Flerfaktorautentiseringsfunktioner

ISO/IEC 29192-1: 2012 beskriver ett antal fysiska och logiska implementeringskrav för beräkningssnåla kryptografiska mekanismer. Standarden beskriver även ett antal krav för att beräkningssnåla kryptografiska funktioner ska uppnå en minsta accepterad säkerhetsnivå (80-bitar).

Hela studien
Komponenter på avstånd Säkerhetsbeaktanden för direkt adresserbara trådlöst nätverks-anslutna komponenter i informations- och styrsystem

Rapportnr: MSB 2018-03310, finns att tillgå via www.msb.se

Kontakta oss:
Tel: 0771-240 240
registrator@msb.se
www.msb.se

Myndigheten för samhällsskydd och beredskap