Swedish Civil Contingencies Agency

FAKTA

Publ.nr: MSB1344 – januari 2019

AVDELNINGEN FÖR CYBERSÄKERHET

OCH SKYDD AV SAMHÄLLSVIKTIG VERKSAMHET

Monitorerings- och övervakningssystem

En kategorisering och översikt av IDS-teknik inom ICS

I MSB:s vägledning till ökad säkerhet i industriella informations- och styrsystem (ICS) ges rådet att kontinuerligt övervaka ett ICS för att upptäcka tecken på intrång. Detta faktablad ger ICS systemägare råd samt frågeställningar som kan användas vid anskaffning av intrångsdetekteringssystem (IDS) för ICS. Faktabladet är baserat på en djupare studie som finns att läsa på MSB:s hemsida.

Frågeställningar

Vid anskaffning av IDS för ICS bör systemägaren ställa sig ett antal frågor med det framtagna ramverket som grund. Ramverket presenteras på nästa sida. Svaren på frågorna är beroende av systemägarens kännedom om systemet vilket underlättas av en uppdaterad risk- och sårbarhetsanalys.

- Vilka punkter i systemet har direkt eller indirekt kontakt med internet?
- Vilka delar i systemet utgör nyckelfunktioner med extra behörighet att modifiera och styra systemet?
- Hur pass förutsägbart beteende har systemet?
- Kan systemet, helt eller delvis, hantera att eventuella realtidskrav frångås?
- Hur homogent är systemet, det vill säga är det väl sammanhållet och enhetligt byggt (fysiskt och logiskt), eller är det distribuerat och består av flera generationer utrustning?

Ramverk för klassificering av IDS för ICS

En grundläggande skyddsfunktion för IT-system är användning av intrångsdetekteringssystem (IDS), som automatiskt ska upptäcka misstänkt aktivitet och intrångsförsök i det system som övervakas.

Här presenteras ett ramverk för klassificering av IDS för ICS. Ramverket kan till exempel användas som underlag vid behovsanalys, kravställning och anskaffning av IDS för ICS.

Några skillnader mellan IT och ICS-system

Skillnaderna beror främst på den ofta specialiserade hårdvaran i ICS och den tätare kopplingen till fysiska parametrar hos ICS. Det finns även högre krav på tillgänglighet och tidsrelevans i och med att ICS ofta utgör hårda realtidssystem. Likaså har den processnära hårdvaran ofta begränsad mängd minne och beräkningskraft jämfört med vad IT-system har.

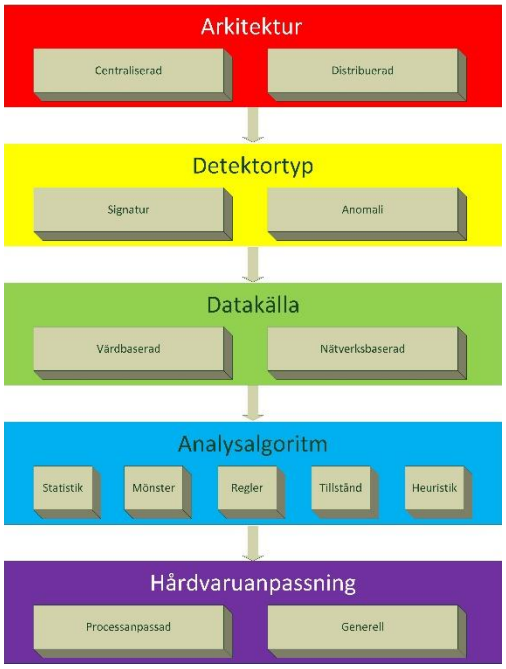
Arkitektur

Ett IDS kan ha antingen en centraliserad eller distribuerad arkitektur. De första systemen för intrångsdetektering var centraliserade, men i takt med att storleken och komplexiteten på de system som skulle skyddas ökade skiftade fokus inom forskningen till distribuerad intrångsdetektering.

Detektortyp

De två kategorier av detektorer som utgör grunden i de flesta klassificeringsramverk för IDS, signaturbaserad och anomalibaserad, skiljer sig åt vad gäller sättet att modellera systemet de övervakar. En signaturbaserad detektor bygger på modellering av angrepp, och en anomalidetektering bygger på modellering av normaltillstånd hos system.

MSB-89.8



Grunden för ramverket är de fyra första kategorierna.

1) arkitektur
2) detektortyp
3) datakälla och
4) analysalgoritm
5) anpassning för processnära hårdvara

Den sista kategorin är ny och speciellt ämnad för ett IDS för ICS. Ramverket är tänkt att ge en bättre förståelse för hur ett IDS är uppbyggt och vilken funktionalitet som är viktig.

Slutsatser

För att uppnå ett fullgott skydd så är det bra om alla delar i ett ICS övervakas av ett IDS. Det behöver däremot nödvändigtvis inte vara ett och samma system som hanterar de olika delarna i ett ICS. Om flera olika intrångsdetekteringssystem installeras så är det lämpligt om dessa samarbetar för att kunna ge en helhetsbild av de angrepp det övervakade systemet utsätts för. Lämpligt val och korrekt placering av IDS kräver god kunskap om det system som ska skyddas. En kartläggning, till exempel i form av en risk- och sårbarhetsanalys, av systemet som ska övervakas är att rekommendera. En dylik analys kan även vara till hjälp i mer generella termer. Följande rekommendationer bygger på principen att skyddet bör byggas upp av flera lager, att bygga det från ytterkant och inåt och att börja med de komponenter som det är mest troligt blir angripna (de mest skyddsvärda komponenterna) vid en incident. Generellt så är det därför en bra idé att först och främst nätverkspunkter med direkt eller indirekt koppling till internet skyddas, vilket lämpligen sker med IDS med nätverksbaserad datainsamling. Därefter rekommenderas det att nyckelfunktioner i det övervakade systemet skyddas. Det kan då handla om till exempel loggservrar och styrenheter. Principen är att först skydda de enheter som har störst förmåga att administrera, styra och kommunicera med andra enheter.

Datakälla
De datakällor som används för kategorisering av IDS-teknik är värddator och nätverk. Begreppet värddator ska ses som komplementet till nätverk, det vill säga allt som inte är nätverkstrafik är värddatorbaserad datainsamling. Ursprungligen var huvuddelen av intrångsdetekteringssystemen värddatorbaserade.

Analysalgoritm
Det är inom området analysalgoritmer som den mesta forskningen kring IDS bedrivs. Aktiviteten är konstant hög med cirka 1250 artiklar per år i medeltal de senaste 10 åren.

Hårdvaruanpassning
Utifrån det faktum att de processnära delarna av ICS ställer speciella krav på ett IDS har en kategori lagts till för att särskilja ett specialanpassat IDS från IDS för IT-system. De alternativ som kategorin innehåller är processanpassad och generell. I och med att ICS finns i en stor mängd olika miljöer och tillämpningar kan det finnas specialfall med ytterligare krav. Dessa fall får hanteras utanför det framtagna ramverket, alternativt föras in som en uppdatering av ramverket vid ett senare tillfälle. Den måste även kunna hantera aktuella protokoll.

Hela studien
Monitorerings- och övervakningssystem – en kategorisering och översikt av IDS teknik inom industriella informations och styrsystem finns att hämta på www.msb.se

Kontakta Myndigheten för samhällsskydd och beredskap

Tfn: 0771-240 240

Kontaktpersoner:
Fax: 010-240 56 00
registrator@msb.se
www.msb.se

Sabrine Wennberg
ics@msb.se

Gustav Söderlind
ics@msb.se