Myndigheten för samhällsskydd och beredskap

www.msb.se/ics

Programmet för säkerhet i industriella informations- och styrsystem

Kristina Blomqvist
Programansvarig

Anders Östgaard
Handläggare

MSB ska bidra till samhällets förmåga att …

Vad gäller allt från olyckor i vardagen till kriser och krig…

… förebygga händelser

Så att aktörerna bättre kan:

- bedriva brand- och olycksförebyggande arbete
- ha kontinuitet i samhällsviktig verksamhet
- hantera farliga ämnen
- hantera information säkert

… hantera händelser

Så att aktörerna bättre kan:

- genomföra räddningsinsatser
- agera samordnat vid händelser
- stödja Försvarsmakten vid höjd beredskap

Myndigheten för samhällsskydd och beredskap

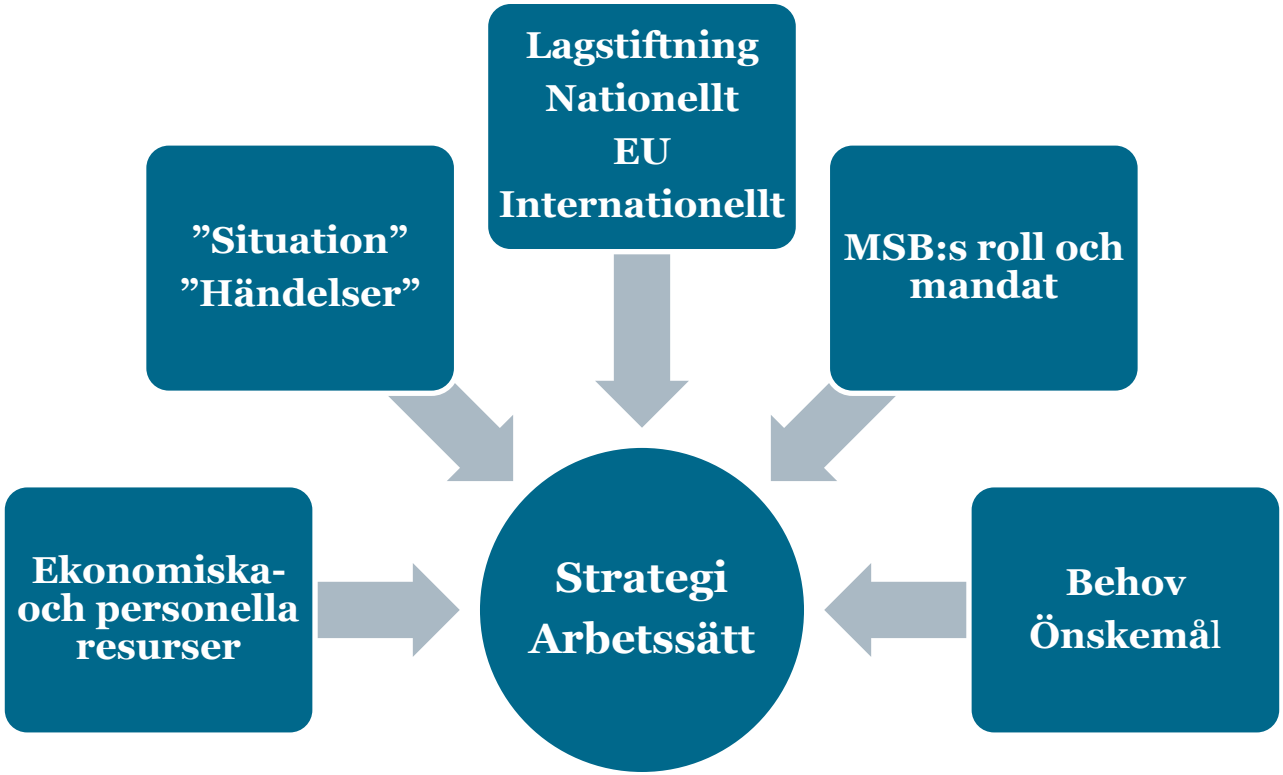
Programmet för säkerhet i industriella informations- och styrsystem

Mål

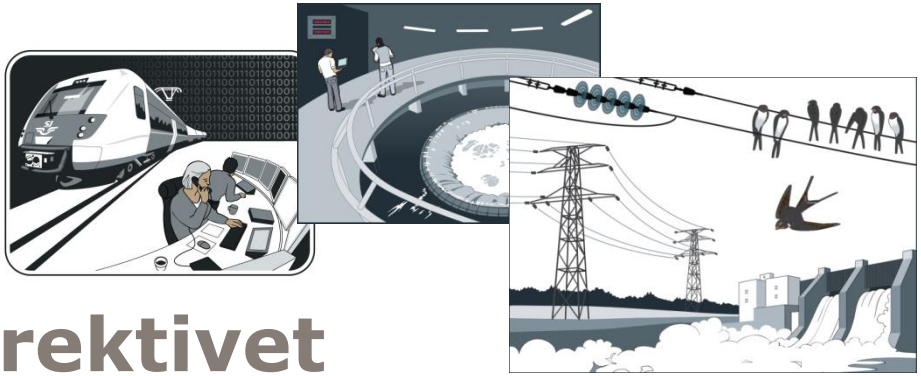
- Minska risken för att storskalig (cyber)incident inom kritisk infrastruktur/samhällsviktig verksamhet
- Bygga upp möjligheter till effektivt hanterande om detta ändå skulle inträffa

Myndigheten för samhällsskydd och beredskap

Strategi – arbetssätt?



Myndigheten för samhällsskydd och beredskap



Lagstiftning
Nationellt
EU
Internationellt

NIS-direktivet

- EU-direktiv om säkerställandet av en hög gemensam nivå av säkerhet för nätverk och informationssystem i hela unionen
- Utredning om genomförande i Sverige: Leds av lagmannen Stefan Strömberg, redovisas senast den 1 maj 2017. **Efter det en snabb process**!

Exempel på krav enligt direktivet:

  - Incidentrapportering som omfattar såväl **offentliga som privata aktörer** inom sektorerna energi, transporter, bank, finans, hälso- och sjukvård och vattenförsörjning

En konkret betydelse: För att kunna rapportera måste man kunna upptäcka!

9. Övervaka kontinuerligt anslutningar och system för att detektera intrångsförsök

Exempel på aktiviteter:

- Övervaka kontinuerligt externa anslutningar och interna system för att detektera alla former av intrångsförsök.
- Analysera kontinuerligt loggar och spårdata från intrångsdetekteringssystem.
- Spara loggar och spårdata från intrångsdetekteringssystem långsiktigt. Dessa behövs när en eventuell efterforskning påbörjas, vilket kan bli aktuellt lång tid efter det initiala problemet.
- Det bör finnas en roll med ansvar för att fånga upp eventuella varningar från de tekniska systemen.

Myndigheten för samhällsskydd och beredskap

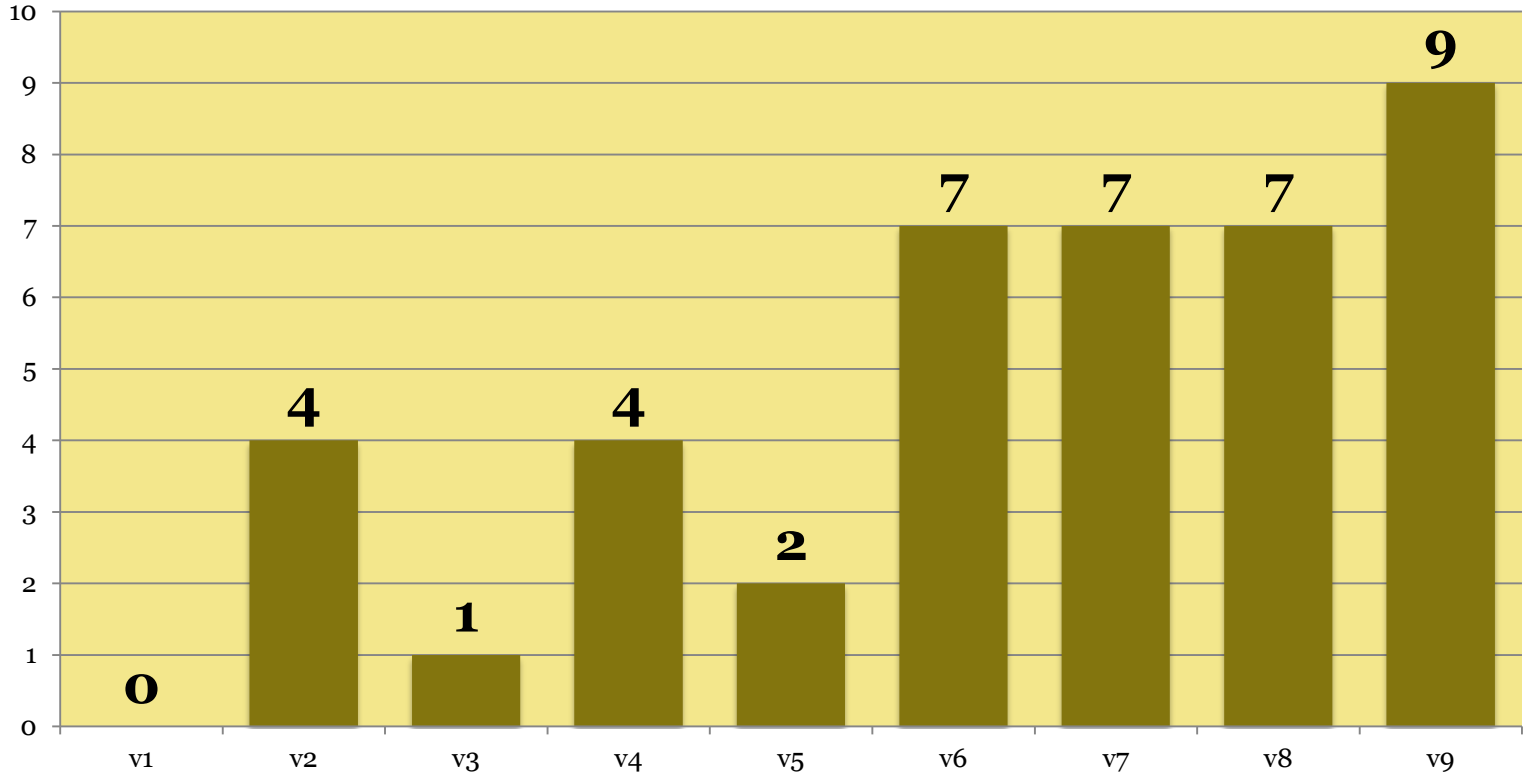
Lagstiftning
Nationellt
EU
Internationellt

Obligatorisk IT-incidentrapportering för statliga myndigheter

- Gällande sedan 4 april 2016

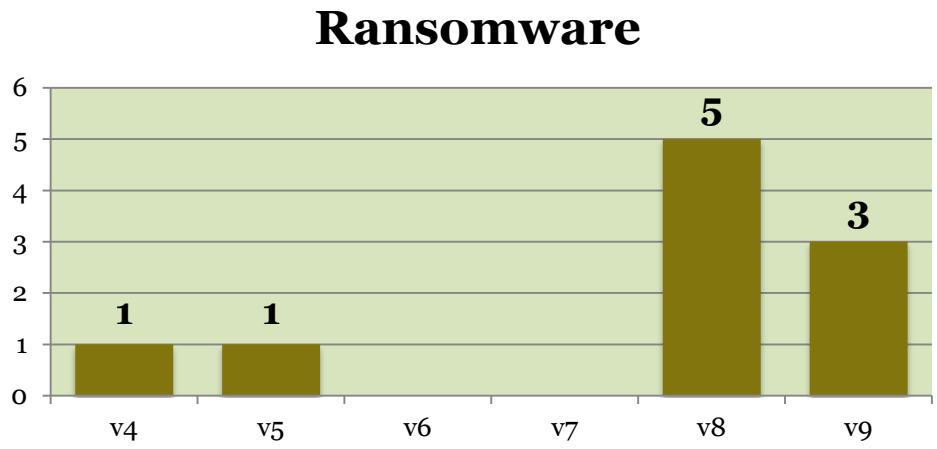
Myndigheten för samhällsskydd och beredskap

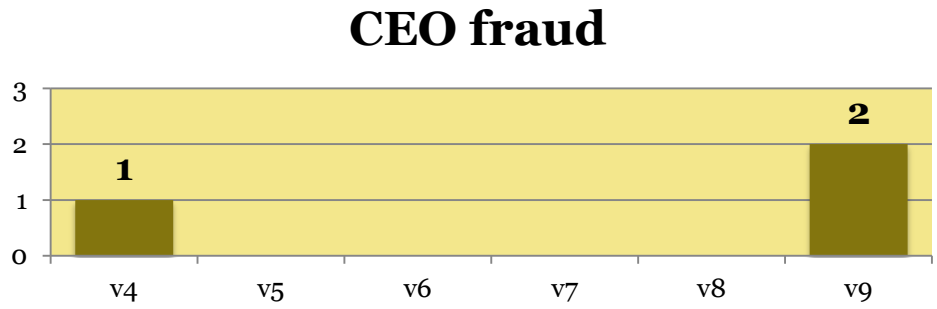
Antal inrapporterade incidenter hittills under 2017



Myndigheten för samhällsskydd och beredskap

Speciella incidentkategorier





Myndigheten för samhällsskydd och beredskap

Lagstiftning
Nationellt
EU
Internationellt

Dataskyddsförordningen - General Data Protection Regulation (GDPR)

- Gäller från maj 2018. Ersätter PUL.
- Krav på hantering av persondata under hela livscykel: administrativa, tekniska lösningar
- Omfattande arbete för många organisationer- påverkar alla branscher, företag och organisationer som hanterar personuppgifter.
- Sanktioner upp till 20 miljoner euro eller 4 % av organisationens omsättning

En konkret betydelse: För att uppfylla detta måste man veta var personuppgifter lagras, hur de överförs till andra system, parter och till länder utanför EU-området.

Myndigheten för samhällsskydd och beredskap

Lagstiftning
Nationellt
EU
Internationellt

Ny säkerhetsskyddslag?

- Utredning beslutades i december 2011. Utredning redovisades våren 2015. Ny lag våren 2018?

”*En ny lag ska svara mot de förändrade kraven på säkerhetsskyddet, bl.a. avseende utvecklingen på informationsteknikområdet, en ökad internationell samverkan, en ökad sårbarhet i samhällsviktiga funktioner och att* ***säkerhetskänslig verksamhet i allt större omfattning bedrivs i enskild regi.***

En bredare ansats för lagen innebär bl.a. att ***tillgänglighets- och riktighetsaspekterna av information och it-system lyfts fram****. På detta sätt vidgas tillämpningsområdet till att ge ett skydd för informationstillgångar i samhällsviktig verksamhet som inte behöver ett skydd från ett konfidentialitetsperspektiv.*”

En ev konkret betydelse: Mycket mer behöver skyddas – även tekniska system, inte minst informations- och styrsystem

12. Utvärdera löpande det fysiska skyddet

Exempel på aktiviteter:

- Fysiskt skydd bör utföras i flera led – även här gäller principen om djupledsförsvar – och det bör bland annat inkludera:
  - skydd av känsliga lokaler – fysiskt skalskydd, tillträdesskydd, inbrottslarm, kameraövervakning och bevakning, brandskydd och så vidare.
  - behörighetskontroll – se till att endast behöriga personer har tillgång till känslig information och viktiga driftlokaler.
  - spårbarhet som gäller personer och tillgångar – se till att både personer och utrustning stannar i behörigt område – exempelvis bör inte bärbar utrustning såsom laptops för programmering av PLC:er lämnas obevakade.
  - kablar för kommunikation – minimera risken för att kablar och korskopplingsutrymmen utsätts för avlyssning eller manipulation.
  - kontroll av miljöfaktorer – exempelvis ventilation och kraftförsörjning.

Myndigheten för samhällsskydd och beredskap

MSB:s roll och mandat

Tekniskt sensorsystem

27 februari 2017:

Regeringen föreslås ge Myndigheten för samhällskydd och beredskap rättsligt mandat att stödja vissa **offentliga och enskilda verksamhetsutövare inom samhällsviktig verksamhet med informationssäkerheten genom att, på deras begäran, tillhandahålla sensorsystem**.

Myndigheten för samhällsskydd och beredskap

MSB:s roll och mandat

MSB:s roll och mandat (1/2)

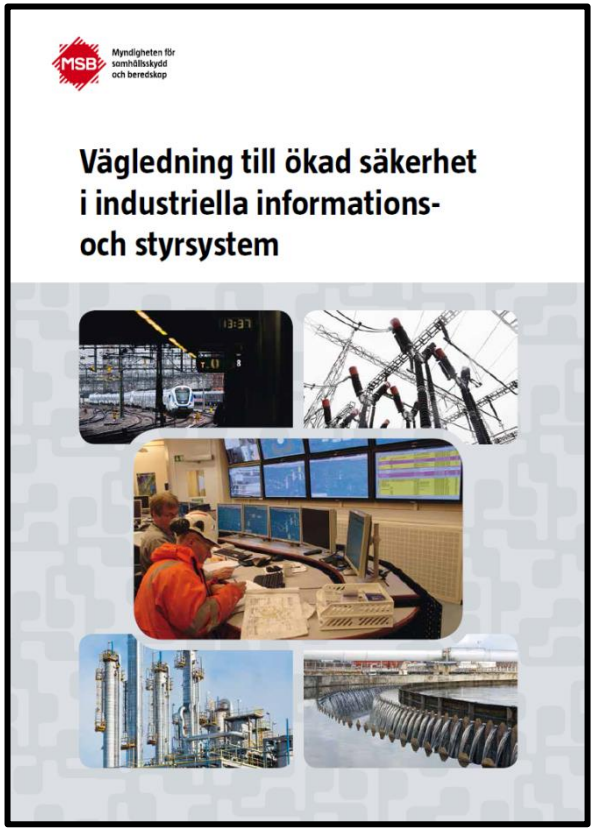
Utdrag ur förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och Beredskap:

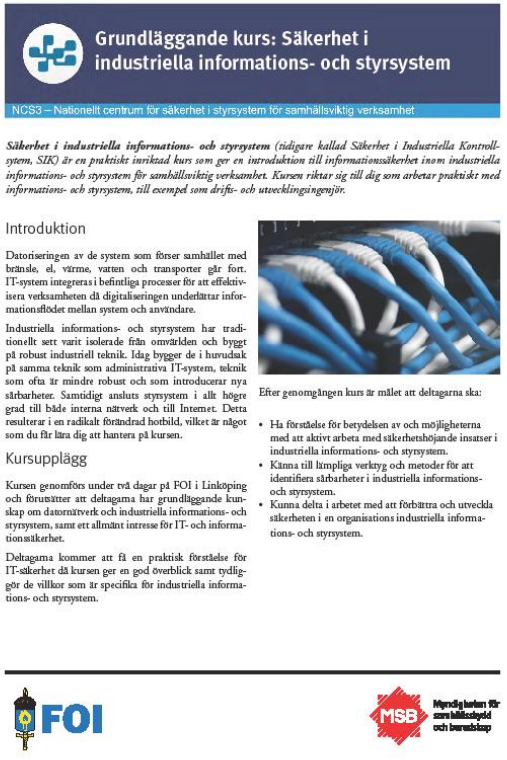
Informationssäkerhet

11 a § *Myndigheten ska stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom området. I detta ingår att* ***lämna råd och stöd i fråga om förebyggande arbete till andra statliga myndigheter, kommuner och landsting samt företag och organisationer.***

En konkret betydelse: Vi föreskriver inte inom styrsystemsområdet, utan är en diskussions- och samarbetspartner

Myndigheten för samhällsskydd och beredskap





Myndigheten för samhällsskydd och beredskap
SVENSKA KRAFTNÄT
LIVSMEDELS VERKET
Strål säkerhets myndigheten
Swedish Radiation Safety Authority
FRA
Säkerhetspolisen
FOI

- NCS3 - kompetenscentrum i samarbete med FOI. Utbildningar, övningar, studier

MSB:s roll och mandat (2/2)

Forts.

Myndigheten ska vidare svara för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera IT-incidenter.

Personlig kommentar: Detta gäller naturligtvis även inom styrsystemsområdet. Mycket arbete kvar att göra. Kontakter och samarbete nödvändigt!

5. Säkerställ systematisk kontinuitetsplanering och incidenthantering

Exempel på aktiviteter:

- Upprätta och underhåll incidenthanteringsrutiner och kontinuitetsplaner för de industriella informations- och styrsystemen.
- Analysera incidenter för att fastställa och förstå ursprungsproblem, omfattning (spridning), direkta och indirekta konsekvenser. Kontrollera till exempel om det är en klar fel och om de uppstod på grund av uppsåtliga eller ouppsåtliga händelser.

Myndigheten för samhällsskydd och beredskap

Workshop | Säkerhet i industriella informations- och styrsystem för integratörer och tekniska konsulter

Plats | MSB, Fleminggatan 14, Stockholm
Tid | 5 APRIL 2017, 0900-1500

Myndigheten för samhällsskydd och beredskap (MSB) bjuder in till en workshop om säkerhet i industriella informations- och styrsystem. Workshopen riktar sig till företag som levererar integrationstjänster inom området.

Innehåll | **Presentationer och diskussioner**

Under dagen kommer MSB bland annat att redogöra för sitt arbete inom programmet för säkerhet i industriella informations- och styrsystem.

Medverkande integratörer förväntas att inför hela gruppen göra en presentation på 15 minuter där följande frågor besvaras och tydligt fokuseras på:

1. Vad ser ni för utmaningar inom arbetet med ökad cybersäkerhet?
2. Vad är era erfarenheter av att arbeta med säkerhetsaspekter tillsammans med kunder?
3. Hur ser ni på utvecklingen framöver kopplat till säkerhetsfrågan?
4. Var har ni för erfarenhet av eget eller kunders arbete med IEC-62443 eller andra standarder och vägledningar
5. Vad har ni för önskemål gällande stöd, vägledning etc. från myndighetshåll?

Målet med workshopen är att identifiera gemensamma problemställningar ur ett integratörsperspektiv och ge svar på frågan: Hur kan förutsättningarna för säkrare industriella informations- och styrsystem på den svenska marknaden förbättras?

Myndigheten för samhällsskydd och beredskap

FAKTA

AUGUSTI 2015

VERKSAMHETEN FÖR SAMHÄLLETS INFORMATIONS- OCH CYBERSÄKERHET

Myndigheten för samhällsskydd och bered

FIDI-SCADA

Forum för informationsdelning kring säkerhet i industriella informations- och styrsystem

FIDI-SCADA är ett privatoffentligt samverkansforum som genom informationsutbyte, omvärldsanalys och framtagande av gemensamt material ökar informationssäkerheten i industriella informations- och styrsystem.

Bakgrund
Industriella informations- och styrsystem är it-baserade system som används för att styra och övervaka fysiska processer och system. Många samhällsviktiga verksamheter – såsom exempelvis dricksvattenproduktion och eldistribution – är beroende av den här typen av system.

Före utvecklingen av automationssystem så styrdes industriella processer, transportsystem och fastigheter av mekaniska eller elektromekaniska maskiner som manövrerades manuellt av operatörer. Idag är automationssystemen mycket avancerade, byggs av standardiserade grundkomponenter, kopplas ofta samman med verksamheternas administrativa system, görs tillgängliga via internet och ger möjlighet till trådlös kommunikation. Det innebär att också de industriella informations- och styrsystemen blir allt mer exponerade för traditionella it-säkerhetshot. Detta samtidigt som felaktig eller utebliven funktion i dessa system kan innebära allvarliga konsekvenser för samhället.

Ett forum för informationsdelning
Sedan 2005 driver MSB (tidigare KBM) ett forum för informationsdelning avseende säkerhet i industriella information- och styrsystem, FIDI-SCADA. SCADA är benämningen på en den typ av stora, distribuerade styrsystem som är vanliga i samhällsviktig verksamhet. Representanter för flera branscher som använder SCADA-system träffas regelbundet för att dela information kring sårbarheter, hot och möjliga åtgärder samt för att koordinera nationellt och internationellt arbete med frågorna.

Samverkande parter
E.ON
Myndigheten för samhällsskydd och beredskap
Preem AB
Stockholms Läns Landsting
Stockholm Vatten AB
Svenska Kraftnät
Sydkraft AB
Säkerhetspolisen
Trafikverket
VA Syd
Vattenfall AB

Privat-offentlig samverkan: FIDI-SC (12 år)

Myndigheten för samhällsskydd och beredskap

”Situation”
”Händelser”

”Situation” och ”Händelser”

- Säkerhetspolitiskt läge
- Inträffade incidenter nationellt och internationellt

Myndigheten för samhällsskydd och beredskap

Myndigheten för samhällsskydd och beredskap

FAKTA

Publ.nr: MSB1091 – mars 2017

VERKSAMHETEN FÖR CYBERSÄKERHET OCH SKYDD AV SAMHÄLLSVIKTIG VERKSAMHET

Viktiga lärdomar från elavbrotten i Ukraina

Skyddet av industriella informations- och styrsystem (ICS) måste stärkas

Den 23 december 2015 meddelade ett antal ukrainska elbolag via sina webbtjänster att ett större elavbrott inträffat. De indikerade samtidigt att andra störningar förekom, såsom problem att nå kundtjänstfunktioner via telefon. Senare samma dag gick ett av de drabbade elbolagen ut med att det handlade om ett IT-angrepp som innebar att understationer kopplades bort, vilket i sin tur ledde till att kunder förlorade sin strömtillförsel. I december 2016 rapporterades om ytterligare angrepp mot elbolag i huvudstaden Kiev. Vilka lärdomar kan vi dra och vilka åtgärder borde vidtas för att upptäcka och förhindra liknande händelser i Sverige?

Det som kommit fram om de tekniska lösningarna som användes i de ukrainska bolagen pekar på att förhållandena i stort liknar de svenska. Tillvägagångssätten för intrången var inte heller nya och unika och med undantag för enstaka delar av det slutliga angreppet fanns det heller ingen programvara som användes vid angreppet som var specialgjord för elsektorn. Av det dras slutsatsen att *samtliga sektorer där industriella informations- och styrsystem används i Sverige behöver fundera på huruvida de har ett tillräckligt skydd.*

I tabellen på nästa sida ges exempel på olika säkerhetsåtgärder och aktiviteter som aktualiserats i och med händelserna i Ukraina. Tre av dessa åtgärder vill vi särskilt lyfta fram:

1. **Bättre grundskydd.** ICS-miljöer är ofta dåligt uppsäkrade ur flera perspektiv. Att införa ett bra grundskydd, i form av en IT-säkerhetsarkitektur med både tekniska och andra skydd, är något som höjer säkerheten i ICS-miljöer avsevärt.
2. **Spårbarhet och övervakning.** Idag är det alltför vanligt att ICS-miljöer inte har fullgod säkerhetsövervakning. Om man inte kan upptäcka att ett angrepp påbörjats, eller lyckats och pågått under ett längre tag kan man aldrig hantera incidenten, utreda orsak och initiala intrångsvägar.
3. **Medvetandehöjning och övning.** En förutsättning för framgångsrikt säkerhetsarbete är medvetenhet och grundförståelse för hur ICS-miljöer är utsatta för hot. Medvetenhet måste finnas på alla nivåer i en organisation, såväl driftspersonal som ledning och beslutsfattare. Organisationer måste utbilda personal samt öva hantering för att kunna förebygga och hantera IT-attacker.

Vad är känt om de attackerade systemen i Ukraina?
Någon känd samlad öppen information över vilka systemlösningar som användes i de ukrainska bolagen finns inte tillgänglig. Det går dock dra en del slutsatser utifrån öppna källor.

I en amerikansk US-CERT-varning finns information om systemens människa-maskin-gränssnitt (HMI). Denna väg användes för att stänga av strömmen. Åtminstone tre skilda sådana produkter förekom hos de olika elbolagen - GE Cimplicity, Advantech/Broadwin WebAccess samt Siemens WinCC. Detta är moderna standardprodukter som används inom olika branscher och företag runtom i världen. Produkterna bygger på Microsoft Windows-plattformar, vilka även de används över hela världen.

I en rapport från E-ISAC och SANS nämns även angrepp mot andra IT-komponenter, som realtidsenheter (RTU), kommunikationsutrustning (seriell till ethernet-konverterare), servrar och reservkraftsystem. Dessa komponenter angreps för att försvåra utredning och återställning av elleverans.

Ur ett riskperspektiv är det viktigt att understryka att de drabbade ukrainska elbolagen använde kända leverantörers produkter samt hade av varandra oberoende systemutformningar och lösningar.

Mer information:
https://ics-cert.us-cert.gov/

https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Mer information om säkerhet i industriella inforamations- och styrsytem finns på www.msb.se/ics

Myndigheten för samhällsskydd och beredskap

FAKTA

DECEMBER 2015

VERKSAMHETEN FÖR SAMHÄLLETS INFORMATIONS- OCH CYBERSÄKERHET

Fastighetsautomation

Cybersäkerhet inom fastighetsautomation

Fastighetsautomation handlar om att i fastigheter styra, reglera och övervaka olika tekniska installationer och system för bland annat värme, ventilation, kyla, luftkonditionering, belysning och solskydd. Dessa system kan betraktas som en delmängd av det MSB benämner industriella informations- och styrsystem.

Egenskaper
Det finns en trend att i ökad omfattning koppla system för fastighetsautomation till administrativa nätverk och system för ta (ex uppgifter om energiförbrukning). Det erfrågan att göra styrningen centraliserad ans. Några andra egenskaper som dessa ta har en lång livscykel och begränsad ng. I ökad omfattning använder de

s i många fall under olika tidpunkter och e skapar således en komplex miljö. I de h användare ofta byts och inte tillhör apas ytterligare en komplexitet.

den med ökad uppkoppling bidrar till att tomation blir allt mer exponerade för tshot. Detta samtidigt som felaktig eller innebära stora konsekvenser för den roende av fastigheten.

edvetandegöra organisationen om ära grundläggande it-säkerhetsutbildning tar, upphandlar, installerar och underhåller

atiskt arbete kan MSBs *"Vägledning till ella informations- och styrsyste* ler 17 grundläggande reko för fastighetsautoma

Byggnadsautomation och fastighetsstyrning – Begrepp som används parallellt med fastighets-automation.

Building Automation och Energy Management Systems – Den engelska översättningen av fastighetsautomation är *Building Automation*. I många sammanhang används även det närliggande begreppet *Energy Management Systems* vilket avser system för att effektivisera energianvändningen.

Energieffektivisering - Drivkraften för de senaste årens utveckling mot mer integrerade system för styrning av fastigheter har framför allt varit energieffektivisering.

HVAC - Som ett samlingsbegrepp för funktionerna värme, ventilation och luftkonditionering används ofta den engelska förkortningen *HVAC (Heat, Ventilation and Air Conditioning)*.

Säkerhetssystem - Sy inpassering och som hand fa

Myndigheten för samhällsskydd och beredskap

Ekonomiska- och personella resurser

Ekonomiska- och personella resurser

Behov och uttryckta önskemål

Hör av er!

Information från programmet för säkerhet i industriella informations- och styrsystem – #2 2016

Inledning

Genom detta blad vill vi på enklaste sätt informera om aktiviteter, rapporter och dylikt med koppling till arbetet för säkerhet i industriella informations- och styrsystem.

Frågor, kommentarer och förslag till innehåll tas tacksamt emot via e-post till scada@msb.se.

Helt färskt medvetandehöjande material

Programmet har producerat tre små broschyrer som i "serieformat" levandegör några av vägledningens 17 rekommendationer. Broschyrerna kommer senare att gå att beställa via MSB:s hemsida. De finns inom kort även i presentationsformat på www.msb.se/ics och kan med fördel användas som diskussionsunderlag vid möten etc.

Presentation baserad på vägledningen

På programmets hemsida hittar ni numera en presentation som på torraste möjliga sätt går igenom vägledningens 17 punkter. Färdig att använda för interna utbildningar och dylikt!

Vår vägledning

Arbetet med en ny version av vår uppskattade vägledning rullar vidare. Planerat färdigställande har fått skjutas till 2018, men har ni synpunkter eller förslag så kontakta oss gärna.

Vägledningen går att beställa gratis i tryckt format, alternativt hittar ni den på https://www.msb.se/RibData/Filer/pdf/27425.pdf

SI3S-kurser 2017

Den grundläggande kursen om säkerhet i industriella informations- och styrsystem, SI3S, kommer preliminärt finansieras av MSB vid 4 tillfällen - v9, v10, v45 och v46.

Intresseanmälningar kan alltid skickas till scada@msb.se. Kontakta oss även om ni är intresserade av att själva finansiera något tillfälle.

Leverantörsmöte

Den 15 november genomfördes en workshop för leverantörer i Linköping.

MSB, FOI, NCS3 och programmet för säkerhet i industriella informations- och styrsystem vill framföra sina varma tack till alla leverantörer som ställde upp med sin tid och kunskap (i bokstavsordning):

ABB, Bombardier Transportation, Cactus Rail, Cactus Utilities, HMS, Malthe Winje Automation AB, Modio, Netcontrol, Schneider Electric, Siemens Turbomachinery, Siemens

Frågor som diskuterades under workshopen var: Vad ser ni för utmaningar inom arbetet med ökad cybersäkerhet? Vad är era erfarenheter av att arbeta med säkerhetsaspekter tillsammans med kunder? Hur ser ni på utvecklingen framöver kopplat till säkerhetsfrågan? Vad har ni för önskemål gällande stöd, vägledning etc. från myndighetshåll? Var har ni för erfarenhet av eget eller kunders arbete med IEC-62443 eller andra standarder och vägledningar?

Parallellt med workshopen genomfördes en komprimerad version av SI3S och I4S.

Möte för integratörer och tekniska konsulter

Under 2017 hoppas vi kunna anordna en workshop för integratörer och tekniska konsulter inom området. Kontakta oss om du är intresserad. Preliminärt datum för mötet är den 5 april.

Workshop med CERCES och RICS

Den 22 februari kommer de MSB-bekostade forskningsprogrammen CERCES och RICS presentera och diskutera sin forskning hos MSB i Stockholm under några timmar. Ta chansen att påverka nationell forskning inom området! Anmäl intresse via scada@msb.se med "forskningsworkshop" i ämnesraden.

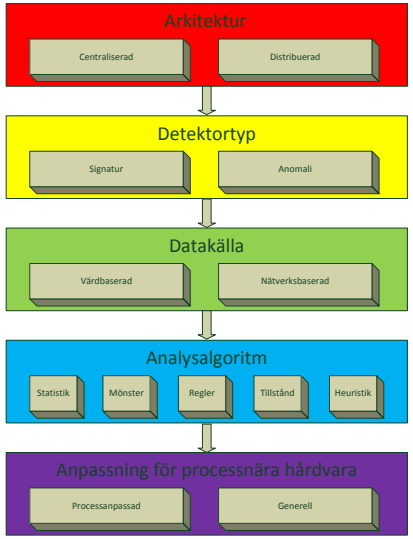
Utredningar och årsrapporter visar på vikten av säkerhet i industriella informations- och styrsystem

Såväl informationssäkerhetsutredningen (SOU 2015:23) som utredningen om en ny säkerhetsskyddslag (SOU 2015:25) betonar samhällsviktiga verksamheters beroende av industriella informations- och styrsystem och vikten av att upprätthålla en stark nationell kompetens inom området. I Myndigheten för Samhällsskydd och beredskaps Nationell risk- och förmågebedömning 2016 görs bedömningen att arbetet med informations- och cybersäkerhet behöver utvecklas ytterligare. I Svenska Kraftnäts risk- och sårbarhetsanalys 2016 redovisas hotbildsanalyser, baserade till stor del på öppna källor i form av rapporter från Försvarsmakten och Säkerhetspolisen samt det senaste årets nyhetsflöde. En av bedömningarna som görs är att resursstarka aktörer med stor förmågebredd utgör det dimensionerade hotet när ansvariga för viktiga elinfrastrukturer utformar och kravställer informations- och IT-säkerhetsfunktioner.

I de senaste årens årsöversikter från Säkerhetspolisen och Militära Underrättelsetjänsten framgår att främmande makt arbetar med kartläggning av både civil och militär svensk

Programmet för säkerhet i industriella informations- och styrsystem är ett MSB-program som arbetar sektorsövergripande med frågor om säkerhet i samhällsviktiga informations- och styrsystem. För mer information, se www.msb.se/ics. Nyhetsbladet är producerat november-december 2016.

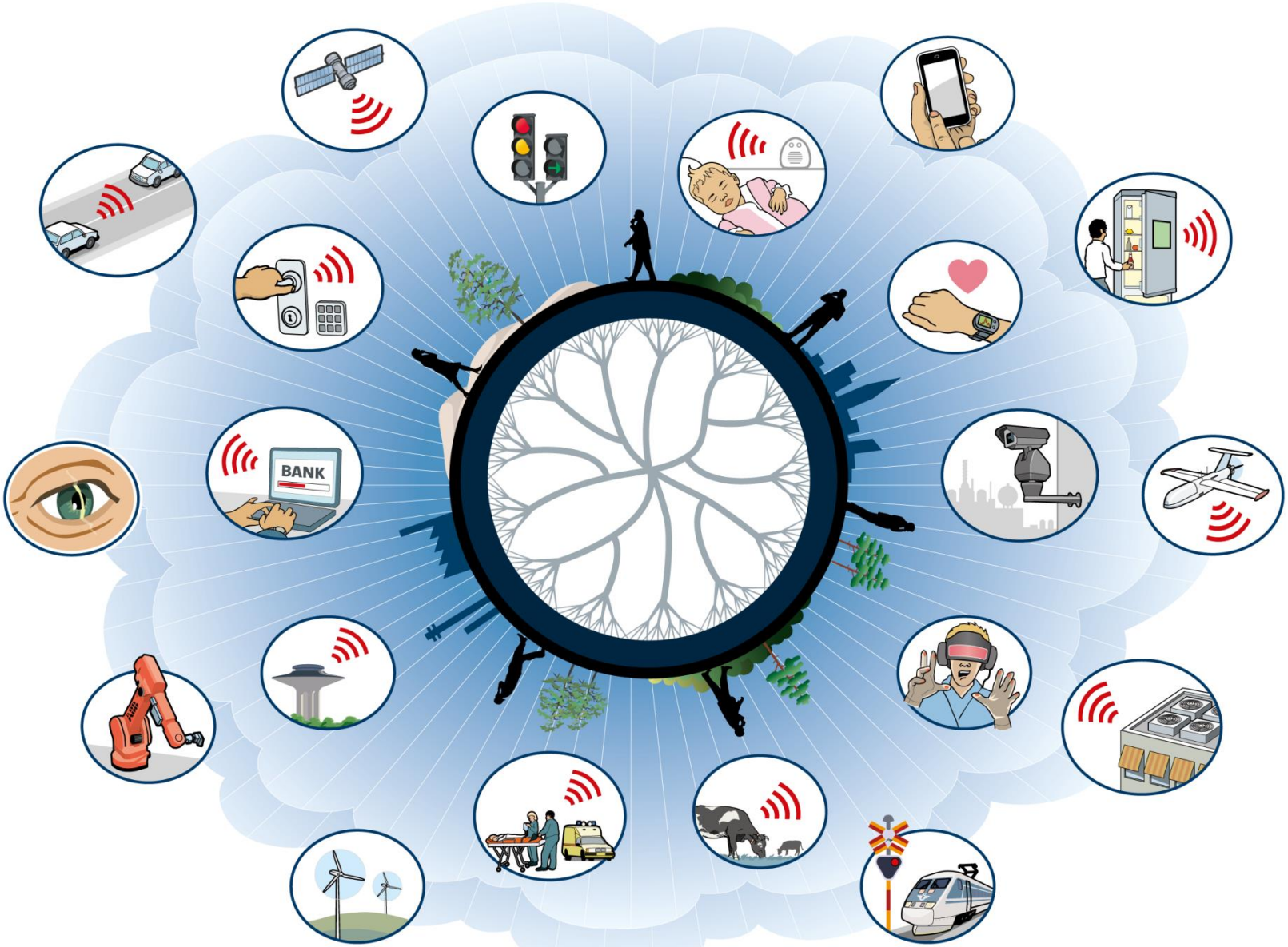
Studier gällande bland annat IEC62443, molntjänster, intrångsdetektionssystem



Vår prioritering är sådant som relaterar till operatörer av kritisk infrastruktur

Myndigheten för
samhällsskydd
och beredskap

www.msb.se/ics


BANK