Myndigheten för samhällsskydd och beredskap

Samhällets informationssäkerhet – utveckling och nya krav

Myndigheten för samhällsskydd och beredskap

På EU-nivå..

- **Dataskyddsförordning**
  - Träder ikraft 2018
  - Förstärkning av enskildas rättigheter och tydliggörande av skyldigheter för de som behandlar personuppgifter
  - Några nyheter: rätt att bli glömd, anmäla dataskyddsincidenter, privacy by design m fl
  - Skadeståndsansvar, böter 10 – 20 milj €
- **NIS-direktivet (Nät- och informationssäkerhetsdirektiv)**
  - Träder ikraft 2018 (förmodligen)
  - Ta fram strategier, policys och regelverk i syfte att uppnå och bibehålla en hög nivå av nät- och informationssäkerhet.
  - Nationellt system för incidentrapportering (offentliga och privata aktörer inom sektorerna energi, transporter, bank, finans, hälso- och sjukvård och vattenförsörjning) samt för digitala samhällstjänster.
  - Funktioner för tillsyn och sanktioner kopplat till direktivet.

Myndigheten för samhällsskydd och beredskap

På nationell nivå …

- Förslag på ny säkerhetsskyddslag
- Obligatorisk it-incidentrapportering
- Nya krav på systematiskt informationssäkerhetsarbete

Myndigheten för samhällsskydd och beredskap

Obligatorisk it-incidentrapportering

Myndigheten för samhällsskydd och beredskap

Agenda

- Syfte och innebörd för berörda aktörer
- Vad ska rapporteras, hur och när?
- MSB:s roll och uppgifter
- MSB:s återkoppling till aktörer
- Säkerhet, sekretess och kryptolösning
- Tillgängligt stöd och kontaktvägar
- Nästa steg, pågående arbete?
- Frågestund

Myndigheten för samhällsskydd och beredskap

Syftet med den obligatoriska it- incidentrapporteringen är att skapa en bred och samlad rapportering av it-incidenter i samhället

Syfte:
Att skapa en systematisk, bred och samlad rapportering av it-incidenter i samhället. Detta för att öka samhällets förmåga att förebygga, motstå, återhämta och lära av it-incidenter och it-relaterade kriser.

Ett nationellt system för it-incidentrapportering möjliggör att:

Skapa en samlad lägesbild
- Rättvisande och aktuell lägesbild på nationell nivå
- Skapar beslutsunderlag

Avvärja och begränsa
- Säkerställa snabbt agerande vid inträffade it-incidenter genom att sprida information i samhället
- Samordna åtgärder
- Lindra effekter

Lära och återföra
- Kanalisera information till berörda myndigheter
- Ge underlag för rapportering till regeringen

Arbeta förebyggande
- Ge stöd för internt informations-säkerhetsarbete
- Skapa underlag för långsiktigt förebyggande och ökad krisberedskap

Ovanstående fördelar kommer att realiseras successivt

Obligatorisk it-incidentrapportering för statliga myndigheter

What's in it for us? Vad får vi som organisation ut i gengäld?

Första året
- Inte så mycket, tyvärr. Lägesbild huvudsakligen till regeringen. Sannolikt statistik i höst samt årsskiftet.

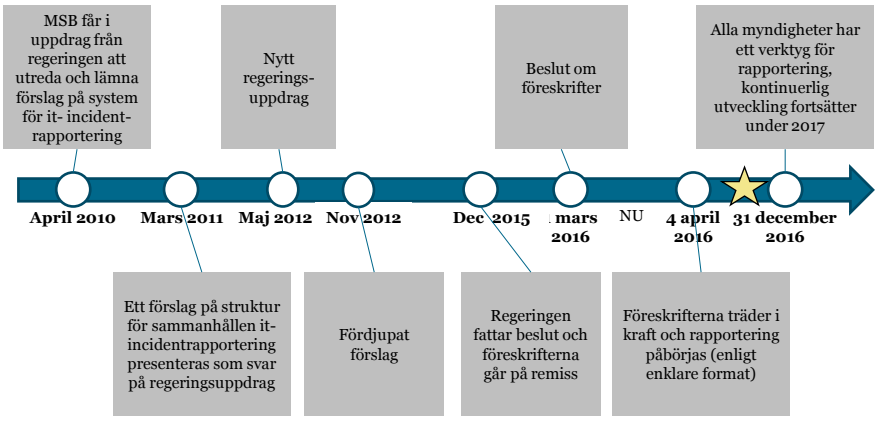
Senare
- Information och tidiga varningar
- Statistik, trender och återkoppling
- Möjlighet att upptäcka allvarliga hot som drabbar många

I framtiden hoppas vi också på
- IOC-er (indicators of compromise)

Redan idag – assistans när det gäller angrepp och analys

Bakgrund och viktiga datum

Arbetet med den obligatoriska it- incidentrapporteringen har pågått under en längre tid



Vilka ska rapportera enligt förordningen?

- Alla statliga myndigheter under regeringen med undantag för:
  - Regeringskansliet, kommittéväsendet,
  - Säkerhetspolisen,
  - Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt och Totalförsvarets forskningsinstitut.
  - För utlandsmyndigheterna tillämpas bestämmelserna endast i den utsträckning som bestäms i föreskrifter som meddelas av Regeringskansliet

Vilka it-incidenter ska rapporteras enligt förordningen?*

- **It-incidenter** som inträffat i myndighetens informationssystem och som *allvarligt kan påverka säkerheten* i
  - den *informationshantering* som myndigheten ansvarar för eller
  - i tjänster som myndigheten *tillhandahåller åt en annan organisation*

- **Inte it-incidenter** som ska rapporteras till Säpo eller FM enligt 10 a § säkerhetsskyddsförordningen (1996:633).
  - system som hanterar hemliga uppgifter (ej ringa mängd)
  - system som behöver särskilt skyddas mot terrorism
  - it-incidenter som upptäckts genom FRA:s arbete

** Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap*

Det är allvarliga it-incidenter som ska rapporteras

Vad ska rapporteras?

Från förordningen (2015:1052)
"...it-incidenter som inträffat i myndighetens informationssystem och som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för eller i tjänster som myndigheten tillhandahåller åt en annan organisation"

Från föreskrifterna och allmänna råden (2016:2)
"Med "it-incident" bör förstås en oönskad och oplanerad it-relaterad händelse som kan påverka säkerheten i organisationens eller samhällets informationshantering och som kan innebära en störning i organisationens förmåga att bedriva sin verksamhet"

En utmaning för myndigheter och MSB kommer att vara att hitta rätt nivå på vad som ska rapporteras, samt att kommunicera kring detta.
"Allvarligt"

Vilka kategorier av it-incidenter ska rapporteras enligt föreskrifterna:

1. störning i mjuk- eller hårdvara, såsom fel i system, komponent eller programvara samt oväntad funktion i system eller komponent eller systemkrasch,

2. störning i driftmiljö, såsom haveri i tekniskt system eller komponent, förlust av tillgänglighet i system samt störningar i säkerhetsfunktioner (ex. säkerhetskopiering), eller

3. informationsförlust eller informationsläckage, såsom förlust av tillgänglighet till eller läckage av information i myndighetens informationssystem, felaktig avyttring av teknisk utrustning som innehåller information som inte ska vara allmänt tillgänglig, eller otillåtet offentliggörande av sådan information,

4. informationsförvanskning, att informationen helt eller delvis har blivit korrumperad eller att det inte går att säkerställa dess riktighet,

Myndigheten för samhällsskydd och beredskap

Kategorier av it-incidenter forts.

5. *hindrad tillgång till information,* att informationen eller ett system där informationen finns inte kan användas på avsett sätt.

6. *säkerhetsbrist i en produkt,* såsom säkerhetslucka eller annan sårbarhet i tekniskt hjälpmedel som används av myndigheten,

7. *angrepp,* såsom överbelastningsattack, införande av skadlig kod, intrång i informationssystem (s.k. hackning), olovligt nyttjande eller annat missbruk av lösenord, olovlig åtkomst till information genom skadliga program och obehörig användning av informationssystem,

8. *handhavandefel,* såsom internt felaktigt bruk eller felaktig implementering av tekniskt system eller komponent,

9. *oönskad eller oplanerad störning i kritisk infrastruktur*, såsom elektriskt fel, vattenskada eller störning i funktioner för avbrottsfri kraftförsörjning, säkerhetskopiering, kylning eller ventilation, eller

10. *annan plötslig oförutsedd händelse som lett till skada,* it-incidenter som orsakats av annan händelse än de som omfattas av kategorierna som nämnts ovan men som av rapporterande myndighet inte bedöms kunna sorteras in i någon av dessa kategorier.

Myndigheten för samhällsskydd och beredskap

Vad ska rapporteras inom 24 timmar?

En rapport ska innehålla:

1. myndighetens namn,
2. en beskrivning av it-incidenten,
3. den exakta eller uppskattade tidpunkten för när it-incidenten inträffade,
4. när myndigheten upptäckte it-incidenten och om den alltjämt pågår eller är avslutad,
5. till vilken eller vilka kategorier enligt 3 § som it-incidenten hör, samt
6. myndighetens initiala bedömning av it-incidentens omfattning och konsekvenser.

Utkontraktering

9 § Ansvaret för att rapportera it-incidenter gäller oavsett om informationsbehandlingen sker inom myndigheten eller är utkontrakterad till annan än statlig myndighet.

Ansvaret i första stycket gäller inte för sådan informationsbehandling som är utkontrakterad om åtgärden skulle strida mot avtal som ingåtts före denna författnings ikraftträdande.

Återkoppling

- Leveranserkännande
- Varningar
- Ytterligare information
- Stöd i det enskilda fallet
- etc

- Rapport till regeringen

Obligatorisk it-incidentrapportering för statliga myndigheter

What's in it for us? Vad får vi som organisation ut i gengäld?

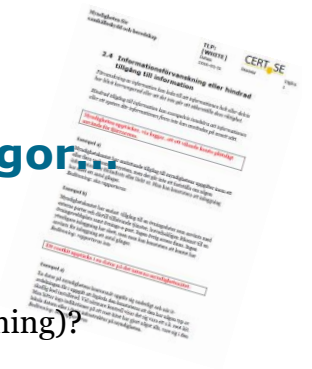
Första året
- Inte så mycket, tyvärr. Lägesbild huvudsakligen till regeringen. Sannolikt statistik i höst samt årsskiftet.

Senare
- Information och tidiga varningar
- Statistik, trender och återkoppling
- Möjlighet att upptäcka allvarliga hot som drabbar många

I framtiden hoppas vi också på
- IOC-er (indicators of compromise)

Redan idag – assistans när det gäller angrepp och analys

Vanliga rapporteringsfrågor...



- Vad är allvarligt?
- Om it-driften är outsourcad?
- Om it-incidenten polisanmälts (bedömning)?
- 24 timmar från upptäckt?
- Rapportering av incidenter om personuppgifter?
- Hantering av personuppgifter?
- Korrigering av uppgifter?
- MSB:s tillsynsansvar?
- Kontaktfunktion och kontaktperson?
- Begäran om kompletterande uppgifter?

Myndigheten för samhällsskydd och beredskap

Kryptolösningen Kurir och sekretess

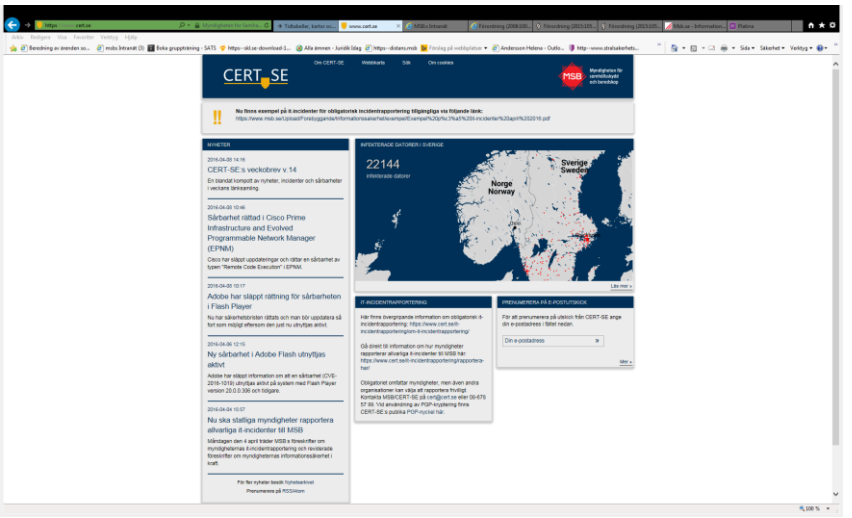
- Egen bedömning av skyddsvärde

- Utskick till registratur och kontaktperson
- 18:8 sekretess, ej rikets säkerhet
- KSU-produkt med förenklat regelverk

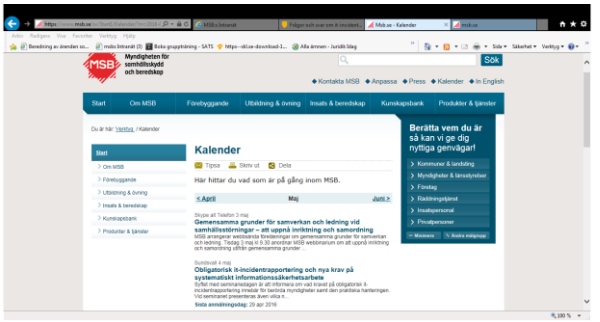
- Juridisk PM – fördjupning om sekretess

Myndigheten för samhällsskydd och beredskap

Tillgängligt stöd



Regionturné



- 12-13 april Kristianstad
- 27 april Stockholm
- 4 maj Sundsvall
- 16 maj Göteborg:
- 17 maj Malmö
- 2 juni Stockholm Arlanda

Anmälan på :
https://www.msb.se/sv/Start1/Kalender/

Informationssäkerhetskonferensen för offentlig sektor – presentation av rapporteringsresultat

Kontaktvägar

- Kontakta MSB/CERT-SE på:
- **cert@cert.se** eller på telefon 08-678 57 99

Myndigheten för samhällsskydd och beredskap

Nya krav på systematiskt informationssäkerhets arbete


Myndigheten för samhällsskydd och beredskaps författningssamling

Myndigheten för samhällsskydd och beredskaps föreskrifter[1] om statliga myndigheters informationssäkerhet;

beslutade den 1 mars 2016.

Myndigheten för samhällsskydd och beredskap föreskriver följande med stöd av 21 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

Tillämpningsområde

1 § Denna författning innehåller föreskrifter som ansluter till bestämmelserna om statliga myndigheters informationssäkerhet i 19 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

2 § Om det i en annan författning finns något bestämmelse om statliga myndigheters informationssäkerhet som avviker från denna författning, gäller den bestämmelsen.

3 § I 19 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap finns föreskrifter om varje myndighets ansvar för säker informationshantering. Ansvaret gäller även när myndighetens information hanteras av en extern aktör eller när myndigheten tillhandahåller externa aktörer tjänster för informationshantering inom e-förvaltning eller motsvarande.

I de fall en myndighet anlitar en annan myndighet för att fullgöra uppgifter som regleras i denna författning ska de berörda myndigheterna tydliggöra dokumentens ist samarbete. Det ska i dokumentationen tydliggöras vilken myndighet som är ansvarig för att uppfylla kraven som ställs i denna författning. Informationsklassning enligt 9 § p.1 ska utföras av den myndighet som äger informationen.

[1] Föreskrifter och allmänna råd som innehåller till föreskrifterna finns på sid 5.

Myndigheten för samhällsskydd och beredskap

Fokus för regelverken

- Statliga myndigheter
- Systematiskt informationssäkerhetsarbete – ledningssystem för informationssäkerhet
- Obligatorisk it-incidentrapportering – förtydliga vad, hur och när

- Inbördes koppling

- Träder ikraft 4 april 2016

Myndigheten för samhällsskydd och beredskap

Bakgrund - nya föreskrifter om statliga myndigheters informationssäkerhet

- Nu gällande föreskrifter MSBFS 2009:10
- Nya versioner av standarderna
- Enkätundersökningen visar på brister
- Riksrevisionen pekar på brister och vill att MSB agerar
- Analysunderlag
- Delvis förändrade villkor/miljö för informationshantering sed
- Utkontraktering och gemensamma tjänster
- Föreskrifterna ska vara ett praktiskt stöd

Myndigheten för samhällsskydd och beredskap

Portalparagraf 5 §

Varje myndighet ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet. I detta arbete ska standarderna ISO/IEC 27001:2014 och ISO/IEC 27002:2014 beaktas.

Tillräckliga resurser ska tilldelas för informationssäkerhetsarbetet samt löpande och regelbunden information lämnas till myndighetsledningen.

Föreskrifternas upplägg

- Tillämpningsområde (1 – 3§§)
  - Ansvarsområde
  - Ansvar om administreras av annan myndighet
- Begreppsförklaring (4§)
  - Informationsklassning, informationsmängd, informationssäkerhet, ledningssystem för informationssäkerhet
- Ledningssystem för informationssäkerhet (5– 6 §§)
  - Systematiskt och riskbaserat, verksamhetens behov, tydliggöra ansvar och resurser, löpande utvärdering och uppföljning.

Föreskrifternas upplägg forts.

- Närmare krav på myndigheternas informationssäkerhetsarbete (7 - 8 §§)
  - styrande dokument, ansvar för informationsmängder, god säkerhetskultur, (informera, övningsplan, utbildningsplan)
- Processarbete (9 §)
  - Med stöd av beslutade modeller: 1 informationsklassning, 2 analysera hot och risker, 3 identifiera åtgärder, 4 följa upp åtgärder och bedömningar, 5 kontinuerligt utveckla, 6 dokumentera.
  - Modellerna ska visa ansvar och tidpunkt/situation då infoklassning respektive hot- och riskanalys ska göras
- Incidenthantering och kontinuitetshantering (10 - 11 §§)
  - krav på rutiner för identifiera, rapportera, bedöma, hantera och dokumentera incidenter samt rutiner för att lära av incidenter
  - Krav på rutiner för kontinuitetshantering som tydliggör hur verksamheten upprätthålls vid större störningar och avbrott.

Myndigheten för samhällsskydd och beredskap

Vad innebär det nya regelverket?

- Tydliggör ansvar vid organisationsöverskridande samarbeten och outsourcing
- Definition av ledningssystem
- Tydliga krav på ledningssystemets utformning (inkl extern granskning i AR)
- God säkerhetskultur
- Processinriktat arbete med stöd av modeller
- Incidenthantering
- Kontinuitetshantering

Myndigheten för samhällsskydd och beredskap

Frågor och tack!

Helena Andersson och Svante Nygren
Verksamheten för cybersäkerhet och skydd av samhällsviktig verksamhet
Helena.andersson@msb.se
Svante.nygren@msb.se