Incidentrapportering – lägesbild, hotbild och utveckling

MSB:s årsrapport om statliga myndigheters it-incidentrapportering 2018

SUSEC, Växjö 4 april 2019

Myndigheten för samhällsskydd och beredskap

”Publiken är mest IRT-folk, så var gärna så teknisk och nördig som möjligt!”

Myndigheten för samhällsskydd och beredskap

Vad kan en analytiker från MSB vilja snacka om?

- Krav på statliga myndigheter att rapportera it-incidenter till MSB
- Kraven på MSB
- Vad vi får in
- Lägesbilden: rapportering och slutsatser
- Hotbilden från Säkerhetspolisen, FRA och MUST
- Vad gör vi nu då?

Myndigheten för samhällsskydd och beredskap

Kravet att rapportera

- De flesta av er är statliga myndigheter
- MSB:s föreskrifter
  - Systematiskt och riskbaserat informationssäkerhetsarbete
  - Rapportering av allvarliga it-incidenter till MSB
- Inom 24 timmar

- Kategorier
  - Störning i mjuk- eller hårdvara
  - Störning i driftmiljö
  - Informationsförlust eller informationsläckage
  - Informationsförvanskning
  - Hindrad tillgång till information
  - Säkerhetsbrist i en produkt
  - Angrepp
  - Handhavandefel
  - Oönskad eller oplanerad störning i kritisk infrastruktur
  - Annan plötslig oförutsedd händelse som lett till skada

Myndigheten för samhällsskydd och beredskap

Kraven på MSB

- Årlig rapport till regeringen utifrån inrapporterade it-incidenter – Årsrapporten för 2018 nyligen släppt
- CERT-SE:s roll
- Skillnaden mellan rapportering och hantering
- Lägesbild
  - Hur ser det ut i samhället?
  - Vi är beroende av er rapportering!

Vad får MSB in?

- 297 rapporter från 87 myndigheter (av 256 rapporteringsskyldiga)
- 44 rapporter från 19 universitet, högskolor och forskningsinstitut (av 38 rapporteringsskyldiga)
- En fjärdedel angrepp, även vanligt med störningar i driftmiljö, handhavandefel och avbrott i kritisk infrastruktur
- Vad är en ”allvarlig” it-incident?

Angrepp i stora drag

- Strax över 200 angrepp sedan april 2016
- Ca ¾ av alla angrepp utförs i vinstsyfte
- Ca ¼ saknar verkan (”near misses”)
- En mycket liten andel uppnår sitt syfte

MSB Myndigheten för samhällsskydd och beredskap

Lägesbilden – rapporteringen och slutsatser

- Fler kan rapportera mer
- Rapportering kräver ett systematiskt och riskbaserat arbetssätt
- Medvetenheten om hotbilden behöver öka och skyddet anpassas
- Kontinuitetshantering och övning gör stor skillnad

MSB:s åtgärder

- MSB reviderar och kompletterar nuvarande föreskrifter, bl.a. kring säkerhetsåtgärder
- Återkoppling direkt till enskilda myndigheter utifrån rapporteringen under 2018
- Nytt metodstöd och koncept för grundläggande säkerhetsåtgärder
- NIS-rapportering från leverantörer av samhällsviktiga och digitala tjänster ger ökad kunskap och erfarenhet
- Fortsatt utveckling av samarbetet med andra aktörer

Hotbilden och utmaningarna från MSB:s horisont

- Specifika områden
  - Rymdberoendet
  - Internetexponeringen
  - Flödessäkerheten
- Omvärlden
  - Digitaliseringen
  - Samhällets beredskap och totalförsvaret
  - Juridiken
  - Kompetensförsörjningen
  - Statens roll
  - Internationellt

Myndigheten för samhällsskydd och beredskap

Vad säger övriga cybersäkerhetsmyndigheter?

- Ryssland – infrastruktur och totalförsvar
- Kina – industri- och forskningsspionage
- Iran
- Organiserad brottslighet

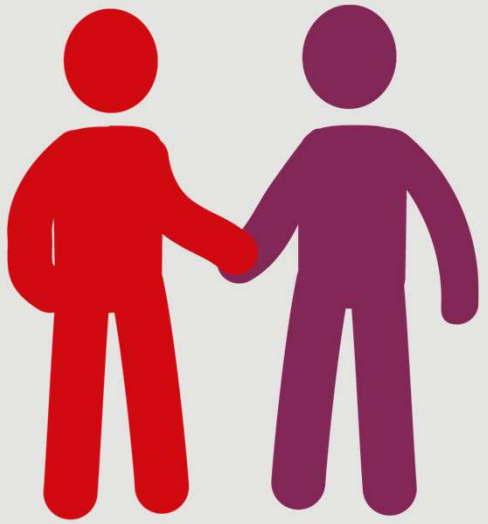
- Säkerhetspolisens årsbok
- FRA:s årsrapport
- Musts årsöversikt
- Europols Internet Organised Crime Threat Assessment (IOCTA)

Vad gör vi nu då?

- Återkoppling till alla myndigheter – informations- och cybersäkerhet är myndighetsledningens ansvar
- Återkommer till Sunet-dagarna i höst med mer info från CERT-SE
- Ber alla se över rutinerna för it-incidenthantering och -rapportering till MSB inför kommande revidering av MSB:s föreskrifter – skicka frågan uppåt i myndigheten!

Vi behöver er – vad behöver ni från MSB?

- Nån frågade om WIS?
  - Vägledning för säker och robust samverkan



Myndigheten för samhällsskydd och beredskap

Tack!

kerstin.borg@msb.se

Myndigheten för samhällsskydd och beredskap