

Strategier för att utforma ett incidentskydd

Erika Stockinger, Sitic



Sveriges IT-incidentcentrum

- Sitic har till uppdrag att stödja samhällets arbete när det gäller skydd mot IT-incidenter.
- Sitic sprider snabbt information om nya problem som kan störa IT-system och lämnar information och råd om förebyggande åtgärder.
- Målet för Sitics arbete är att höja säkerhetsmedvetandet i samhället genom att förmedla fakta och kunskap och på så sätt öka skyddandet mot IT-incidenter.

Agenda

- Vad är det egentligen som kan hända?
- Och om det värsta ändå inträffar – vad gör du då?
- Vilka åtgärder bör en verksamhet vidta för att skydda sig mot allvarliga incidenter?

Vad är en incident?

En verklig eller uppfattad händelse av säkerhetskritisk karaktär i en dator eller ett nätverk.

Varför är det viktigt med en incidenthanteringsfunktion

- Syftet med en effektiv incidenthantering är att varje incident i så låg grad som möjligt ska påverka verksamheten negativt. Då måste alla aspekter av verksamheten beaktas, inte bara de tekniska.
- Värdefullt att strukturerat samla in erfarenheter kring säkerhetsbrister för att på detta sätt se till att organisationen lär sig att hantera framtida säkerhetsproblem.

Vad kan hända?



1. Upptäcka

- Har du blivit utsatt för ett angrepp? Eller är det ett handhavandefel som orsakat problemet?
- Ligger problemet egentligen här?
- Börja dokumentera allt som sker

2. Avbryta

- Rör det sig om ett angrepp - Minimera skadan.
- T.ex. stänga en port i brandväggen.

3. Analysera

- Ta reda på hur angreppet gick till samt vilken skada som kan ha uppkommit på de egna systemen.
- T.ex. gå igenom loggar från servrar, brandväggar och routrar för att hitta och granska den skadliga koden.

4. Spåra

- Inuti den skadliga koden finns ofta ledtrådar som kan visa med vilka andra system den kommunicerar.
- Genom analys av kommunikationskanalerna, finns det möjligheter att göra goda gissningar om vilka som ligger bakom angreppet.
- Kontakta polisen om du tror att du har blivit utsatt för ett brott.

5. Återställa

- Systemen ska upp igen, helst med all ursprunglig data, men utan tidigare sårbarheter.
- Utan att veta, via steg 3 (analys) och kanske 4 (spåra), vad som hänt, är risken stor att man tar upp sina system i ett sårbart skick igen.

6. Förhindra

- Vid det ideala fallet lär man sig så mycket vid en incident att man vet hur man skyddar sig mot både samma och även liknande angrepp efteråt.
- En viktig del i detta steg är att sammanställa hur incidenten hanterades och lära sig av bra och dåliga grepp, gå igenom dokumentationen.

FRÅGOR?

Läs gärna mer på:

- www.sitic.se
- Telefon: 08-678 57 99

- www.pts.se
- Telefon: 08-678 55 00 (vx)