Skrivebordstest af beredskab

Hackerangreb

2013

Alarmering om hændelse

Scenarie – dag 1 kl.12:45

Helpdesk modtager et opkald fra en medarbejder, som har åbnet en mail med en PDF fil. Indholdet i filen vækker mistanke om et eksternt hackerangreb.

Spørgsmål

- Hvilke systemer og servere skal evt. stoppes for at undgå yderligere inficering?
- Er det nødvendigt at stoppe adgangen til internettet?
- Hvem skal kontaktes og informeres?

Afdække omfang

Scenarie – dag 1 kl.13:05

Adgangen til og fra internettet er nu blevet stoppet (inkl. e-mail).

Relevante interne servere/og eller services er stoppet, så de ikke kan viderebringe inficering via. fileshares etc.

Skadens omfang og oprindelse er endnu ukendt.

Spørgsmål

- Hvilke logfiler er relevante at gennemgå?
  - Netværkslogs?
  - Serverlogs?
- Hvem er ansvarlig for at skaffe uddybende information om angrebets oprindelse og omfang?

Eskalering

Scenarie – dag 1 kl.14:00

Det er nu blevet identificeret, hvilke systemer der er omfattet af hacking-angrebet.

Der er afstemninger af visse konti i økonomisystemet, der ikke længere passer. Banken kontaktes, og det bliver oplyst, at der mangler 1 mio. dollars.

Hændelsen skal derfor eskaleres til beredskabsorganisationen.

Spørgsmål

- Hvem skal kontaktes for eskalering til beredskabsorganisation?
- Hvilke nødplaner er relevante at tage i brug nu?

Intern kommunikation

Scenarie – dag 1 kl.14:00

De interne brugere er endnu uvidende om hændelsen og reagerer på afviste adgangsforsøg på de systemer, der er lukket ned.

Spørgsmål

- Hvem er ansvarlig for den interne kommunikation?
- Hvilke medarbejdere skal informeres om hændelsen? – skal visse grupper oplyses før andre?
- Hvilken information skal medarbejderne i organisationen have om hændelsen?
- Hvem udarbejder selve meddelelsen?

Oprydning

Scenarie – dag 1 kl.17:00

Myndighed X har nu fået viderebragt de nødvendige informationer til de nødvendige parter.

Det er nu tid til oprydning.

Spørgsmål

- Hvordan identificeres samtlige misbrugte brugerkonti, og hvordan skal de håndteres?
- Kan retablering af kompromitteret data ske indenfor den tid, der er fastlagt i SLA?
- Hvordan sikres det, at der ikke efterlades malware eller “bagdøre” på de systemer, der har været berørt.
- Skal der ske bortskaffelser af nogen flytbare medier?

Review af testen

- Hvad er de væsentligste læringspunkter fra testen?
- Hvilke ændringer skal der ske til beredskabsplanen?
- Hvilke handlingspunkter er vigtigst?

Rapportering: <dato>

<tidspunkt>	<CIO>
<tidspunkt>	<Beredskabskoordinator
<tidspunkt>	<Sikkerhedskoordinator

Skrivebordstest

Deltagere i testen:

- CIO
- Beredskabskoordinator
- HR ansvarlig
- Sikkerhedschef
- Eksterne facilitatorer
- ….

Fokusområder, særlige udfordringer og gode erfaringer fra testen: