1 KOH Cyber Incident Response Plan

1.1 Voorkomen mogelijk incident

Heb je per ongeluk een actie uitgevoerd waaruit een mogelijk incident kan ontstaan? Denk aan:

1. Verdachte email en/of bijlage(s) geopend
2. Mogelijk schadelijke URL geopend
3. Mogelijk schadelijke bestanden gedownload
4. Mobiel/tablet/laptop verloren/gestolen

Neem zo spoedig mogelijk contact op met de afdeling ICT.

1.2 Identificeren mogelijk incident

Zie je bij jezelf of andere collega's verdachte of onverklaarbare bewegingen op de computer en/of mobiele apparaat, ontkoppel (indien mogelijk) direct het betreffende apparaat van het netwerk en neem zo spoedig mogelijk contact op met de IRP beheerder. Leg het incident duidelijk uit:

Wat is er precies gebeurd?

1. Persoonlijke inloggegevens ingevuld/uitgegeven bij een niet door KOH toegestane (web) applicatie
2. Plotseling groot aantal bestanden verdwenen
3. Melding geencrypt apparaat of bestanden

Waar is het precies gebeurd?

1. Locatie/vestiging
2. Mobiel apparaat
3. Laptop/desktop
4. Serversessie (Metacom omgeving)

1.3 Insluiten incident

De IRP beheerder beoordeelt vervolgens de ernst van de situatie en neemt indien nodig vervolgstappen:

1. Ontkoppelen/uitschakelen van alle (eventueel) getroffen netwerk apparaten
2. Scannen van de complete netwerkomgeving
3. Formatteren getroffen apparaat
4. Terugzetten back-up

Heeft het incident plaatsgevonden op, of toegang gehad tot de servers in het datacenter, dan:

5. Neemt de IRP beheerder zo snel mogelijk contact op met VH ICT diensten
6. Schakelt de beheerder in overleg met VH ICT eventueel over op de replica omgeving

1.4 Nazorg incident

In alle gevallen evalueert de IRP beheerder met alle betrokken personen het incident:

1. Waar is het misgegaan
2. Hoe had het voorkomen kunnen worden
3. Welke maatregelen kunnen/moeten er genomen worden

Afdeling ICT	**IRP Beheerder**	**VH ICT**
0594-283599	0594-283598	-bekend bij ICT-