Het Incident Response Traject

NFIR
IT FORENSICS & INCIDENT RESPONSE

Ik heb een incident, wat moet ik doen?

INCIDENT MELDING EN INTAKE

1. Bel NFIR

NFIR is 24/7 bereikbaar op 088 133 0700. Eerst volgt een telefonische intake. Op basis daarvan wordt een CERT* samengesteld.

2. Team komt in actie

Koffers worden samengesteld met internationaal goedgekeurde apparatuur en CERT vertrekt naar de klant.

3. Intake op locatie

Intake op locatie wordt uitgevoerd, waarin NFIR alle beschikbare informatie omtrent het incident verzameld.

VEILIGSTELLEN EN ONDERZOEKEN

4. Data veiligstellen

Gegevens worden veiliggesteld voor nader digitaal forensisch onderzoek.

5. Triage

Getroffen apparaten en/of systemen worden in kaart gebracht en plan van aanpak wordt opgesteld.

6. Containment

De getroffen apparaten en/of systemen worden hersteld en de beveiliging wordt geverifieerd, zodat de normale werkzaamheden zo spoedig mogelijk kunnen worden hervat.

Proces wordt herhaald indien noodzakelijk

RAPPORTAGE EN PREVENTIE

7. Post-incident

Na het verhelpen van het incident, kan digitaal forensisch onderzoek worden uitgevoerd. Het incident response traject wordt altijd afgesloten met een onderzoeksrapport, waarin adviezen om de kans op een dergelijk incident in de toekomst te verkleinen zijn opgenomen.

Preventieve maatregelen

Na het incident kan NFIR diensten zoals penetratietest en security monitoring aanbieden.

ACCREDITATIES

***CERT**

CERT staat voor Computer Emergency Response Team. Het kenmerk wordt door Carnagie Mellon University toegekend aan bedrijven en teams die zich inzetten om digitale beveiligingsincidenten te verhelpen.

POB-vergunning

Door de POB-vergunning (Particulier Onderzoeksbureau) die de Minister van Justitie en Veiligheid heeft afgegeven, mag NFIR haar werkzaamheden uitvoeren. De vergunning dekt het verwerken van bijzondere persoonsgegevens.

Toestemming Korpschef

Om vast te stellen of medewerkers mogen werken voor een recherchebureau heeft de afdeling Korpschef-taken een screening uitgevoerd op de betrouwbaarheid van alle NFIR medewerkers. Alle NFIR medewerkers hebben een dergelijke toestemming.

Voor meer informatie over Incident Response klikt u hier