CHECKLIST

# Incident Readiness

## Voorbereiding op een cyberincident

**Cyberaanvallen en datalekken zijn onvermijdelijk, dus als je door een cyberaanval wordt getroffen, moet je weten wat je moet doen. Bekijk hoe goed je organisatie is voorbereid op een mogelijke cyberaanval of datalek. Test regelmatig je reactievermogen op het gebied van cyberbeveiliging met deze checklist en synchroniseer deze met je Incident Response Plan.**

**Mogelijkheden** — Weet wat technisch gezien mogelijk is en wat niet. Noteer wat je sterke en zwakke punten zijn en weet welke beveiligingsmaatregelen al zijn genomen.

**Forensische paraatheid** — Zorg ervoor dat je bent voorbereid door na te gaan of de nodige voorbereidingen zijn getroffen. Denk hierbij aan de omvang van het netwerk, het aantal systemen en het netwerkverkeer, welke bronnen en logboeken beschikbaar zijn en welke informatie kan worden verzameld.

**Hulplijnen** — Ken de bestaande hulplijnen en zorg ervoor dat ze beschikbaar zijn in geval van een cyberincident. Neem in het geval van twijfel altijd contact op met het Incident Response Team van Eye Security om de situatie snel en correct te beoordelen.

**Crisisorganisatie** — Maak vooraf interne afspraken over wanneer escalatie plaatsvindt naar de crisisorganisatie. Bepaal hoe de crisisorganisatie eruit komt te zien en bepaal welke rollen door wie worden ingevuld. Maak afspraken over de bereikbaarheid en beschikbaarheid van het crisisteam.

**Juridische afdeling** — Weet welke autoriteiten moeten worden geïnformeerd in geval van een hack of datalek en laat de juridische afdeling de communicatie controleren.

**Communicatie** — Bedenk op welke manier je communiceert als het bedrijfsnetwerk uitvalt. Houd er rekening mee dat standaard communicatiemiddelen mogelijk niet toegankelijk zijn om te communiceren met werknemers, klanten en leveranciers. Gebruik geen systeem dat mogelijk is gehackt voor communicatie, aangezien de aanvaller je communicatie zou kunnen zien.

**Bedrijfscontinuïteit** — Ontwikkel alternatieven om de bedrijfscontinuïteit te waarborgen. Bepaal welke systemen in je netwerk het belangrijkst zijn. Een Incident Response-team kan op het moment van een incident rekening houden met deze systemen.

**Back-ups** — Ontwikkel een back-upstrategie en controleer regelmatig de veiligheid en gezondheid van back-ups. Voer periodieke tests uit op het herstellen van back-ups.

**Verzekering** — Noteer de financiële gevolgen van een cyberaanval op je bedrijf of organisatie. Onderzoek of je hiervoor verzekerd bent en in hoeverre je aan de polisvoorwaarden voldoet. Weet wie de cyberverzekeraar aanspreekt bij een cyberincident.

**Evaluatie** — bepaal wanneer de crisis eindigt en hoe dit wordt besloten en gecommuniceerd. Het is belangrijk dat de activiteiten hier niet onnodig onder lijden omdat de crisisorganisatie te lang in stand wordt gehouden.

*Wanneer je wordt getroffen door een cyberaanval of datalek, aarzel dan niet om contact met ons op te nemen. Het Incident Response Team van Eye Security is 24/7 beschikbaar en zorgt ervoor dat de bedrijfsprocessen van een slachtoffer tijdens een cyberincident snel weer op gang komen.*

**www.eye.security** info@eye.security