Zorgeloos online

Zo maak je een Cyber Incident Response Plan

Handig stappenplan voor mkb'ers

Incident Response beschrijft het proces hoe je als bedrijf omgaat met een datalek of cyberaanval, inclusief de manier waarop je probeert de gevolgen te beperken. Het uiteindelijke doel is om je hersteltijd, financiële en reputatieschade, tot een minimum te beperken. Het Cyber Incident Response Plan beschrijft de verschillende soorten cyberincidenten en de bijbehorende processen, zodat je hier op terug kunt vallen als je te maken hebt met een hack of datalek.

Tip! *Je kunt het plan natuurlijk zelf opstellen, maar nog beter is om een brainstorm met meerdere collega's uit alle disciplines van je organisatie te houden. Samen weet je altijd meer dan alleen. Op die manier breng je je plan naar een hoger niveau en creëer je direct awareness onder je collega's.*

Stap 1: Stel een incident-responseteam samen

Als je slachtoffer bent van een cyberaanval moeten er vaak veel verschillende dingen geregeld worden. Verdeel de acties en verantwoordelijkheden over meerdere mensen.

- Wie gaat coördineren?
- Welke mensen gaan de aanval analyseren?
- Wie is verantwoordelijk voor de communicatie richting klanten en andere stakeholders?

Stap 2: Doe een risicoanalyse

- Welke incidenten vonden er in het verleden plaats?
- Welke dreigingen bestaan er?
- Welke systemen hebben we en welke zijn kwetsbaar?
- Welke dreigingen zijn het meest waarschijnlijk?
- Zijn mijn medewerkers zich bewust van de risico's?

Bepaal per risico hoe groot de kans is dat dit gaat gebeuren op de volgende schaal: groot, midden, klein. Vervolgens categoriseer je de mogelijke incidenten op basis van ernst: hoog, midden, laag. Zo ontstaat een lijst met de grootste risico's.

Tip! *Als eigenaar van een bedrijf ben je vaak een beetje 'bedrijfsblind'.*
Het kan interessant zijn om een externe security expert eens naar jouw systemen te laten kijken.

Stap 3: Maak een actieplan

Als je weet wat je grootste risico's zijn kun je je daarop voorbereiden. Maak per risico een scenario:

- Wat is het incident?
- Wat moet er gebeuren in geval van een incident?
- Welke (externe) partijen zijn betrokken of moet je erbij betrekken?
- Wie moet geïnformeerd worden?
- Wie is verantwoordelijk voor de uitvoering?

De uitwerking hiervan geeft je houvast bij een incident.

Stap 4: Zorg voor een meldpunt

Als iemand in de gaten heeft dat er een incident of dreiging is, moet hij of zij zo snel mogelijk aan de bel kunnen trekken.

- Hoe moeten medewerkers een incident of dreiging melden en aan wie?
- En wat te doen met een incident buiten werktijd?

Stap 5: Communiceer het plan met je medewerkers

Zorg ervoor dat je de plannen intern deelt en levend houdt, want wat heb je aan een plan als je medewerkers niet weten van het bestaan of waar ze het kunnen vinden?

En vergeet nieuwe medewerkers niet: zorg dat zij bij binnenkomst in de organisatie hierover geïnformeerd worden.

Stap 6: Oefenen en herhalen

Train je medewerkers regelmatig op wat ze moeten doen bij incidenten. Vergelijk het met een brandoefening. Als je al eens een incident hebt meegemaakt – al dan niet via een simulatie – dan reageer je bij een volgend incident sneller en adequater.

Train bijvoorbeeld elk kwartaal een van de mogelijke incidenten uit je risicoanalyse. Vergeet niet te evalueren na afloop. Wat ging goed en wat kan beter? Op deze manier is de kans groter dan je medewerkers incidenten sneller signaleren en er beter op anticiperen.

Stap 7: Leer van incidenten

Jouw Cyber Incident Response Plan kan waterdicht lijken. Toch zijn er in de praktijk altijd factoren die je kunt voorspellen en die je beter, anders of sneller had kunnen doen.

Gebruik die ervaring om je plan bij te stellen en om nog beter voorbereid te zijn op toekomstige incidenten.

Stap 8: Zorg dat het plan beschikbaar is

Denk goed na waar je het plan bewaart. Aan een plan dat op SharePoint staat, heb je niks op het moment dat je hele bedrijfsnetwerk gegijzeld is door ransomware. Het kan daarom slim zijn het plan op meerdere plekken te bewaren.

- Waar bewaar ik mijn Incident Response Plan?
- Moet het hele plan voor iedereen openbaar zijn of is alleen de meldprocedure openbaar?

De 6 fases bij goede incident response

Je plan is nu bijna klaar, maar een goede incident respons is afhankelijk van het succes van het doorlopen van 6 fases. Deze leg je ook vast in je plan. Je leest er meer over op sidn.nl.

Deze checklist is samengesteld door SIDN.
Wil je meer weten over wat wij ondernemers bieden op het gebied van cybersecurity, kijk dan op sidn.nl.