Een Cyberincident Response Plan maken

Stappenplan

Als een cyberincident zich voordoet is tijd kostbaar. Door een goed voorbereid duidelijk plan op te stellen wat bij iedereen bekend en dat wanneer nodig kan worden uitgevoerd, zal de impact van een aanval op uw organisatie beperkt blijven.

In uw Cyberincident Response Plan beschrijft u het proces hoe als organisatie om te gaan met een eventuele cyberaanval, met daarbij de manier waarop u de gevolgen hiervan probeert zo klein mogelijk te houden. Doel van het plan is om de hersteltijd, financiële en reputatieschade te kunnen beperken tot een minimum. In het Cyberincident Response Plan beschrijft u de verschillende soorten cyberincidenten die kunnen optreden en de daar bijhorende op te volgen processen.
Wanneer uw organisatie te maken heeft met een cyberincident kunt u handelen aan de hand van het Cyberincident Response Plan!

Stel het Cyberincident Response Plan op samen met collega's uit alle disciplines van uw organisatie. Hiermee creëert u bewustzijn onder collega's en heeft u een plan waar de hele organisatie achter staat.

Stap 1: Stel een Incident Response Team samen

Tijdens en na een cyberaanval moeten er verantwoordelijkheden en acties worden verdeeld. Doe dit over meerdere medewerkers. Zorg dat alle relevante belanghebbenden hierbij zijn vertegenwoordigd (management, security, IT, legal, public relations). Denk aan acties en verantwoordelijkheden zoals wie coördineert, wie analyseert wat er aan de hand is en wie communiceert naar klanten en andere belanghebbenden en hoe. Hou rekening met het feit dat de normale communicatie kanalen mogelijk niet functioneren.

Stap 2: Voer een risico analyse uit

Bepaal voor elk kritiek systeem en voor alle kritieke data op welke incidenten u risico loopt en hoe groot de kans is dat een incident zich voordoet: hoog, groot, midden en klein. Vervolgens categoriseert u de mogelijke incidenten op basis van ernst: hoog, midden en laag. Leer hierbij ook van het verleden door te kijken naar welke incidenten er in het verleden zijn geweest. Bepaal ook of alle medewerkers zich wel bewust zijn van de mogelijke risico's.

Laat een externe security expert u helpen met het opstellen van een risico analyse.

Stap 3: Maak een actieplan

Beschrijf voor elk in Stap 2 onderkent risico:

- Wat is het incident en wat moet er gebeuren in het geval dat een incident zich voordoet?
- Welke (externe) partijen zijn betrokken of moeten erbij betrokken worden? Zorg dat vooraf duidelijk is waar en wanneer om externe hulp gevraagd kan worden.
- Wie moet er geïnformeerd worden?
- Wie is er verantwoordelijk voor de uitvoering van het plan?

> Zorg dat *vooraf* duidelijk is bij wie om externe hulp gevraagd kan worden.

Stap 4: Zorg voor een Incidentmeldpunt

Als iemand het vermoeden heeft dat er sprake is van een incident of een dreiging, moet hij dit zo snel mogelijk kunnen melden. Zorg dat medewerkers weten dat ze een mogelijk incident moeten melden, hoe en aan wie. Denk ook aan hoe dit moet gaan buiten werktijd.

Stap 5: Communiceer het plan met alle medewerkers

Zorg dat iedereen het plan blijvend kent, weet te vinden en geüpdatet wordt over eventuele aanpassingen. Zorg dat nieuwe medewerkers geïnformeerd worden over het plan als onderdeel van de in-dienst procedure.

Stap 6: Simuleer een incident

Train medewerkers regelmatig op hoe incidenten te herkennen en wat te doen in het geval van een incident. Simuleer regelmatig één van de mogelijke incidenten uit de risicoanalyse, pas het plan toe en evalueer de resultaten met elkaar.

Stap 7: Leer van incidenten

Gebruik ervaringen met gesimuleerde en echte incidenten en de evaluaties hiervan om het Cyberincident Response Plan aan te passen en scherper te stellen.

Stap 8: Zorg dat het plan altijd beschikbaar is

Zorg dat het Cyberincident Response Plan ook beschikbaar is tijdens een incident. Dus bewaar het op meerdere plaatsen en niet alleen digitaal.

> Hulp nodig bij het opstellen van je Cyberincident Response Plan? TT3P helpt u graag. Neem contact met ons op!