WWW.MINDYOURSTEP.INFO

Crisiswoordvoering

wat doe je in het geval van een incident?

De vraag

Het is tegenwoordig niet meer de vraag óf je organisatie slachtoffer wordt van incidenten op informatieveiligheidsvlak, maar vooral 'wanneer'. 100% veilig bestaat immers niet, want ook 'cybercrime' is inmiddels de hobbyfase voorbij. Maar als er zich dan een incident op informatieveiligheidsvlak voordoet, wat doe je dan? Het minste wat je kunt doen is goed voorbereid zijn, zeker op woordvoeringsvlak.

De uitdaging

De media berichten bijna wekelijks over incidenten op informatieveiligheidsvlak. Of het nu gaat om het lekken van data, cyberaanvallen, digitale fraude, cyberspionage, phishing, de kranten staan er bol van. Zeker sinds de Meldplicht Datalekken van kracht is, en organisaties verplicht zijn om een incident te melden, is het noodzakelijk dat je als organisatie je crisiswoordvoering goed op orde hebt. Zeker bij organisaties die zich in een politiek-bestuurlijke omgeving bevinden en waarbij transparantie en verantwoording cruciale uitgangspunten zijn. Het ontbreken van gerichte crisiswoordvoering kan immers leiden tot materiële en immateriële schade voor je organisatie. Reputatieschade is de meest voorkomende vorm van schade, maar ook de vorm die het meest eenvoudig te voorkomen is. Effectieve woordvoering helpt daarbij. Het staat of valt bij het hebben van informatie en vooral het op een succesvolle wijze gebruiken ervan. Maar hoe doe je dat?

De oplossing

Voor effectieve woordvoering in het geval van een incident is het belangrijk om rekening te houden met de volgende zaken:

- Zorg dat er een draaiboek Informatieveiligheid klaarligt op het vlak van crisiswoordvoering, inclusief alle (privé) contactgegevens van verantwoordelijken.
- Zorg dat deze verantwoordelijken weten wat er van hen verwacht wordt in geval zich een incident voordoet en dit ook naleven.
- Communiceer met regelmaat intern over het feit dat er een draaiboek Informatieveiligheid aanwezig is binnen de organisatie. Communiceer ook in het kort wat de procedure is in geval zich een incident voordoet.
- Maak het draaiboek onderdeel van een groter calamiteiten handboek van de organisatie.
- Wijs één persoon (bij voorkeur in het draaiboek al benoemd) aan als crisiswoordvoerder. Zorg ervoor dat dit nooit de hoogste bestuurder in rang is. Zo mist een logische escalatie lijn. Een professionele crisiswoordvoerder heeft in het algemeen de voorkeur boven een bestuurder.
- De crisiswoordvoerder is de enige persoon die zowel in- als extern over het incident communiceert. Zijn er derde partijen bij betrokken? Wijs dan één crisiswoordvoerder aan die namens alle bedrijven de externe communicatie verzorgt.
- Kies vooraf een heldere consistente woordvoeringslijn met één kernboodschap en pas deze aan al naar gelang de oplossingsrichting van het incident. Informeer collega's en direct betrokkenen over deze woordvoeringslijn.
- Breng altijd de risico's in kaart die betrekking hebben op het specifieke incident en bepaal wat de impact hiervan is.
- Zorg dat je, indien er persoonsgegevens zijn gelekt, het incident zo snel als mogelijk meld bij de Autoriteit Persoonsgegevens (AP).
- Stel een lijst met Q&A's op. Elk publiek moment biedt kansen maar ook risico's. Zorg dus dat je goed voorbereid bent op de antwoorden die je namens jouw organisatie wil geven.
- Kom zelf naar buiten met informatie over het incident, hierdoor bepaal je zelf het frame in plaats van dit aan anderen (journalisten) over te laten. Dit hoeft geen gedetailleerde informatie te zijn, maar communicatie over het proces kan altijd.
- Zorg voor de juiste feiten en communiceer ook alleen deze feiten. Vermijd percepties en verwijzingen naar derden. Acteer vanuit de eigen kracht van de organisatie.
- Weet je niet direct het antwoord? Geen probleem. Geef dan aan dat je er op een later moment op terug komt. Kom deze belofte vervolgens altijd na.
- De reputatie van je organisatie staat of valt bij de juiste wijze van optreden tijdens het incident. Stel daarom dus altijd het perspectief van de gedupeerden of slachtoffers centraal en niet de eigen organisatie.
- Tenslotte; Zorg dat je goed voorbereid (of getraind) bent op alle mogelijke soorten incidenten.

Let op! Houd ook je omgeving goed in de gaten, via sociale media verspreiden berichten zich razendsnel. Waardoor vaak veel speculaties en geruchten ontstaan en feiten snel 'op straat' komen te liggen. Anticipeer hierop indien noodzakelijk.

Meer weten?

Bezoek onze website www.mindyourste.info voor meer tips en tricks op informatieveiligheidsvlak of neem contact op met Sonja Kok via sonja@soulmade.nl of door te bellen naar 0162-430345 voor meer informatie over wat wij voor jouw organisatie kunnen betekenen.