Cyberrisk

Als uw bedrijf te maken krijgt met cybercrime staat u sterker met een Incident Response Plan. Dit plan versnelt het herstel, beperkt de schade, voorkomt mogelijk herhaling en vermindert negatieve publiciteit.

Een Incident Response Plan is geen standaarddocument. Het is belangrijk dat het op maat gemaakt wordt voor uw bedrijf. Hier hoeft u geen expert voor te zijn, u kunt het zelf opstellen, of samen met uw adviseur. Dit is hiervoor een stappenplan. Kies de elementen die voor úw bedrijf relevant zijn.

9 STAPPEN voor het maken van een Incident Response Plan

STAP 1
Stel een calamiteitenteam samen en verdeel taken

Stel een klein team samen waarbij iedereen een duidelijke taak heeft. Denk aan een leidinggevende en een systeembeheerder. En aan een communicatiemedewerker, want het is niet altijd verstandig om een ICT'er direct met klanten of de pers te laten communiceren. Zorg dat iedereen weet wat zijn taken zijn. Belangrijk is dat alle medewerkers binnen het bedrijf op de hoogte zijn van het calamiteitenteam en weten bij wie ze incidenten kunnen melden.

- ✓ Leg vast wie het **eerste** aanspreekpunt is*
- ✓ Leg vast wie het **tweede** aanspreekpunt is**
- ✓ Leg vast wie het aanspreekpunt is op **ICT-gebied**
- ✓ Leg vast wie het aanspreekpunt is op het gebied van **communicatie**

* *Deze persoon is bevoegd beslissingen te nemen die nodig zijn om de schade zo veel mogelijk te beperken. Ook als deze beslissingen op andere afdelingen betrekking hebben.*

** *Deze persoon is bevoegd beslissingen te nemen als het eerste aanspreekpunt afwezig is.*

STAP 2
Leg vast welke externe partijen ingeschakeld moeten worden

DENK AAN

- ✓ **Calamiteitennummer verzekeraar** (bijvoorbeeld 24/7 Cyberrisk-desk)
- ✓ **ICT-adviseur**
- ✓ **Telecombedrijf**
- ✓ **Internetprovider**
- ✓ **Service- of onderhoudsbedrijf printer, server etc.**
- ✓ **Andere externe partijen**

Belangrijk
Noteer van iedereen naam + telefoonnummer

STAP 3
Inventariseer uw ICT-middelen

Om snel en efficiënt te kunnen reageren bij calamiteiten moet u weten welke ICT-middelen in uw bedrijf aanwezig zijn. Noteer bij elk ICT-middel de soort, het merk, het versienummer, specificaties en wie het gebruikt.

- ✓ Computers, laptops, tablets
- ✓ Servers
- ✓ Printers
- ✓ Besturingssystemen en/of applicaties
- ✓ Internetaansluiting (IP-adres)
- ✓ Koppelingen met andere (externe) netwerken
- ✓ Overzicht van alle gebruikersaccounts en hun toegangsrechten
- ✓ Aanwezige beveiligingssystemen (firewalls, antivirus)
- ✓ Identity & Access management (wachtwoorden, tokens)
- ✓ Netwerkbeveiliging (SSL, WiFi-beveiliging)
- ✓ Overige beveiligingsmaatregelen (encryptie)
- ✓ Back-up unit of gegevens van uw online back-up account
- ✓ (Zakelijke) mobiele telefoons
- ✓ Type telefooncentrale en toestellen

STAP 4
Inventariseer uw bedrijfsprocessen

Hieronder een aantal aandachtspunten

- ✓ Welke personen, teams of afdelingen maken gebruik van welke systemen, applicaties en/of software?
- ✓ Welke systemen/websites zijn noodzakelijk voor de continuïteit van het bedrijf, welke systemen/websites moeten direct hersteld worden en welke hebben een lagere prioriteit?
- ✓ Waar worden back-ups bewaard?
- ✓ Wat is de procedure voor het terugzetten van back-ups? Neem dit op in het plan.
- ✓ Bewaar een kopie van belangrijke gegevens (zoals licentiegegevens, Incident Response Plan) buiten uw bedrijf. Leg vast waar deze kopie wordt bewaard.

STAP 5
Maak een communicatieplan

Na een incident is het niet alleen nodig om de buitenwereld te informeren, maar ook de medewerkers die niet direct betrokken waren bij het incident.

Binnen uw bedrijf

- ✓ Leg vast bij wie en hoe medewerkers incidenten kunnen melden.
- ✓ Leg vast wie het aanspreekpunt is bij vragen van medewerkers. Dit kan dezelfde persoon zijn als het aanspreekpunt voor externe partijen.
- ✓ Maak een overzicht van de teammanagers en/of senior medewerkers en hun contactgegevens.
- ✓ Maak een telefoonlijst en een telefoonketting voor het doorbellen van een calamiteit of andere belangrijke informatie. Niet alleen vaste telefoonnummers, ook mobiele (privé)nummers.
- ✓ Snt regels op voor medewerkers wanneer en waarover zij wel en niet buiten mogen communiceren. Denk aan: 'Geen contact met klanten, behalve met toestemming van directie of calamiteitenteam' en 'Geen (privé) berichten over het incident op social media plaatsen'.

Buitenwereld

Een plan voor communicatie met externe partijen, zoals klanten, potentiële klanten, leveranciers, de pers en college-ondernemers, is erg belangrijk. Wees duidelijk en eerlijk, maar speel kwaadwillenden niet in de kaart door details vrij te geven die hen mogelijk verder helpen.

- ✓ Leg vast wie het aanspreekpunt is bij vragen van klanten, pers of andere externe partijen. Laat geen IT'er of willekeurige medewerker met externe partijen of de pers praten.
- ✓ Maak een (telefoon)script voor medewerkers voor de beantwoording van vragen van klanten, leveranciers of andere betrokken.
- ✓ Deel dit script onmiddellijk met de betreffende medewerkers na een calamiteit.
- ✓ Leg vast hoe wordt omgegaan met de pers.
- ✓ Maak conceptberichten voor de pers en social media, zodat u na een calamiteit snel kunt reageren.
- ✓ Maak een overzicht van contactpersonen of gegevens van de pers.
- ✓ Maak een overzicht van de social media-accounts waarop uw bedrijf actief is.
- ✓ Maak een overzicht van de contactgegevens van (belangrijke) leveranciers, klanten en andere betrokkenen die na een calamiteit in elk geval moeten worden geïnformeerd.

STAP 6
Verdiep u in de Meldplicht Datalekken

Meld Datalekken bij de Autoriteit Persoonsgegevens

U bent wettelijk verantwoordelijk voor de privacygevoelige informatie in uw bedrijf. Bewaart of bewerkt u bijzondere persoonsgegevens of andere vertrouwelijke persoonsgegevens van gevoelige aard? Dan moet u ernstige datalekken binnen 72 uur melden bij de Autoriteit Persoonsgegevens. Denk bijvoorbeeld aan medische gegevens, informatie over godsdienst, ras, strafrechtelijk verleden, burgerservicenummers, financiële gegevens (schulden, inkomen), en inloggegevens (wachtwoorden).

Wanneer is sprake van een ernstig datalek?

Bij het melden van een datalek moet u een aantal afwegingen maken. Het onderstaande schema helpt hierbij. De meldplicht kan al van toepassing zijn op een datalek dat slechts betrekking heeft op de gegevens van één persoon.

Bron: www.autoriteitpersoonsgegevens.nl

STAP 7
Maak een actieplan

Wanneer een (vermoeden van) een cyberincident zich voordoet, is het belangrijk niet in paniek te raken of paniek te veroorzaken. Daarom is het belangrijk vooraf de acties te definiëren die nodig zijn om effectief en efficiënt te reageren.

- ✓ Bepaal wat wordt verstaan onder een cyberincident. Wanneer komt het calamiteiten-team in actie? Dit kan zijn: een verzoek om losgeld (ransomware), bestanden staan op slot of zijn niet toegankelijk, bestanden zijn verdwenen, de website is gehackt, klanten ontvangen vreemde e-mails van uw bedrijf, het netwerk functioneert niet meer of er zit een virus op de server.
- ✓ Licht uw calamiteitenteam (of uw calamiteitenpersoon) in.
- ✓ Bel bij een calamiteit het calamiteitennummer van uw verzekeraar.
- ✓ Is er sprake van een datalek? Zie stap 6.
- ✓ Noteer alles wat er gebeurt en zich voordoet. Leg hierbij ook duidelijk de eigen acties vast. Wie doet wat, waar, wanneer en waarmee. Leg ook vast met wie en wat andere personen wordt gecommuniceerd.
- ✓ Zet de communicatie in gang in overleg met uw verzekeraar/securityspecialisten. Zie stap 5.
- ✓ Zorg ervoor dat u snel weer kunt mailen (bijvoorbeeld via webmail).

STAP 8
Deel het Incident Response Plan met alle betrokkenen

- ✓ Zorg dat uw Incident Response Plan beschikbaar is voor alle leden van uw calamiteitenteam.
- ✓ Zorg dat het plan gedeeld wordt met alle betrokkenen in uw bedrijf.
- ✓ Neem het plan regelmatig door met de betrokkenen, zodat zij weten wat er van hen wordt verwacht.

STAP 9
Actualiseer uw Incident Response Plan

Bedrijven veranderen continu. Hetzelfde geldt voor cybercrime dreigingen. Een Incident Response Plan dat vandaag goed werkt, is over enkele maanden wellicht verouderd of zelfs helemaal niet meer toepasbaar.

- ✓ Herzie het plan daarom minimaal 1 keer per jaar, controleer of alle gegevens nog juist zijn en zorg dat het plan altijd up-to-date blijft.

de Goudse verzekeringen