Wat moet er in mijn IT-calamiteitenplan staan?

Hoe maakt u als ondernemer een IT-calamiteitenplan?

Een back-up alleen is niet genoeg om na een calamiteit de bedrijfsprocessen van uw onderneming weer op de rit te krijgen. Om dit te kunnen herstellen, moet u zorgen voor een IT-calamiteitenplan. Deze bevat naast technische aspecten, ook informatie over personeel, externe leveranciers en licenties. Deze handleiding is bedoeld om bedrijven te helpen een IT-calamiteitenplan op te stellen.

Offsite locatie

Een offsite locatie is essentieel bij ieder herstelplan. Dat houdt in dat u zorgt dat back-ups, licentiegegevens, installatiecd's en een kopie van het calamiteitenplan buiten de bedrijfsmuren opgeslagen worden. Deze gegevens moeten veilig en toegankelijk bewaard worden, bijvoorbeeld in een kluis bij een lid van het managementteam of bij een gespecialiseerde externe partij. Zorg ervoor dat deze data ook buiten kantooruren toegankelijk is. Zorg er daarnaast voor dat de data voldoende versleuteld is. Dit om te voorkomen dat bedrijfsinformatie in verkeerde handen terecht kan komen.

Inventarisatie

Een goed uitgangspunt voor een herstelplan is een inventarisatie maken van de IT-infrastructuur. Let op: deze is omvangrijker dan alleen de pc's en servers op kantoor. Waaruit bestaat de gehele IT-infrastructuur?

- Kantoorpc's inclusief specificaties en serienummers,
- Servers inclusief specificaties en serienummers,
- Back-up unit, soort tape/disc of gegevens van een online back-up account,
- Type telefooncentrale en toestellen,
- Aantal telefoonlijnen, inclusief faxnummers en lijnen voor alarmcentrale,
- Internetverbinding, IP-adres, website, wifi en providernaam,
- Softwarelicenties voor serverapplicaties en desktopsoftware,
- Printers, scanners, kopieer- en faxapparaten.

Om een goed beeld te krijgen van de verschillende aspecten die bij een herstelprocedure aan bod komen, moet u naast de inventarisatie ook een overzicht van de verschillende bedrijfsprocessen maken. Waar moet u bij het inventariseren aan denken?

- Afdelingshoofden, wie is verantwoordelijk voor welke afdeling en wat zijn de contactgegevens?
- Welke systemen worden gebruikt door welke afdelingen?
- Welke data is noodzakelijk voor deze afdelingen?
- Welke systemen moeten direct hersteld worden en welke hebben een lagere prioriteit?

Planning

Na de inventarisatie van de IT-infrastructuur en bedrijfsprocessen, kunt u een draaiboek maken voor het herstel. Zorg hiervoor dat de volgende stappen doorlopen worden:

- Vorm een calamiteitenteam (IT-beheerder, AVG functionaris, afdelingshoofden, afgevaardigde van het dagelijks bestuur),
- Maak duidelijk wie het eerste aanspreekpunt is bij een calamiteit,

- Zorg ervoor dat ieder lid weet welke taak hij/zij heeft als er een calamiteit is,
- Wie besluit dat het herstelplan in werking moet treden,
- Welke interne functionarissen moeten ingeschakeld worden,
- Welke externe partijen/leveranciers moeten ingeschakeld worden (IT-beheerder, verzekeringsmaatschappij, facilitair bedrijf, advocaat),
- Zorg dat de telefoonnummers van de externe partijen in het calamiteitenplan zijn opgenomen,
- Is er een uitwijklocatie? Misschien kunt u hiervoor afspraken maken met collega-bedrijven of is uitwijken naar een tijdelijke online-omgeving een mogelijkheid,
- Zorg dat u bereikbaar bent. Kunt u nummers doorschakelen naar uw mobiel? Kunt u e-mailen via web-mail,
- Regel vervangende hardware. Bestelt u nieuwe of huurt u hardware? Maak hierover afspraken met uw leveranciers,
- Start het herstel: zet de back-up terug, herstel uw systemen op basis van prioriteiten.

Personeel

- Instrueer uw medewerkers over het cyberrisico, zoals:
  1. Stuur gevoelige informatie niet zomaar weg,
  2. Klik nooit op links waarvan u niet weet waar ze naartoe leiden,
  3. Download nooit e-mailbijlagen waar u niet om hebt gevraagd,
  4. Gebruik nooit torrents of websites met illegale downloads,
  5. Meld het onmiddellijk als een PC vreemd doet,
  6. Maak nooit gebruik van onbeveiligde apparaten of (wifi) netwerken,
  7. Gebruik nooit zomaar een USB-Stick of externe harde schijf in de PC of laptop,
  8. Meld het altijd onmiddellijk als een apparaat is kwijtgeraakt of gestolen,
  9. Organiseer een goed wachtwoordbeleid.
- Informeer uw medewerkers wat te doen wanneer er zich een cybercalamiteit voordoet.

Testen

Cruciaal om uw calamiteitenplan goed te kunnen uitvoeren, is het plan van tevoren te testen.
Test daarom de verschillende onderdelen van de planning steekproefsgewijs:

- Neem eens in het weekend contact op met uw leverancier(s), is deze bereikbaar,
- Weet wat u mag en kan verwachten van uw leverancier, ook buiten zijn kantooruren om,
- Welke kosten komen er dan allemaal bij kijken,
- Kunt u werken op de uitwijklocatie,
- Test het terugzetten van de back up.

Tot slot

Een herstelplan is nooit klaar, u moet er regelmatig kritisch naar kijken, om te zorgen dat het actueel blijft. Brengt u bijvoorbeeld wijzigingen aan in uw bedrijfsvoering, dan moet u het herstelplan ook weer aanpassen. Vanzelfsprekend moet u de contactgegevens en licentiegegevens regelmatig controleren en indien nodig aanpassen. Maak hiervoor een persoon binnen het calamiteitenteam verantwoordelijk, eventueel op te nemen in zijn/haar functieomschrijving.

Een generiek plan bestaat niet, een goed herstelplan is toegespitst op het herstel van uw eigen bedrijfssituatie. Bovenstaande punten zijn dan ook bedoeld als leidraad, afhankelijk van uw situatie kun u onderdelen toevoegen of weglaten.