Wat moet er in mijn IT-calamiteitenplan staan?

Waarom maakt u als ondernemer een IT-calamiteitenplan?

De wereld om ons heen verandert. Waar in het verleden alles met de post ging, gaat bijna alles nu digitaal. Dit brengt voor ondernemers risico's met zich mee. Om die risico's (IT-calamiteiten) te beperken, of misschien wel te voorkomen, maakt u een IT-calamiteitenplan. Een IT-calamiteit kan zijn dat u niet meer bij uw essentiële digitale gegevens kunt, waardoor het dagelijkse werkproces stil komt te liggen. Deze handleiding is bedoeld om bedrijven te helpen een IT-calamiteitenplan op te stellen.

Hoe maakt u als ondernemer een IT-calamiteitenplan?

Een IT-calamiteitenplan is niets anders dan een vastlegging van protocollen om uw bedrijfsproces na een calamiteit zo snel mogelijk weer op de rit te krijgen. Een IT-calamiteitenplan bevat naast technische aspecten, ook informatie over personeel, externe leveranciers en licenties. Maar denkt u ook na over;

- Zijn wij goed beveiligd?
- Wat is ons meest kwetsbare punt?
- Welke data is het meest interessant voor criminelen en/of concurrenten?
- Is dat onderdeel of onderdelen extra goed beveiligd?

Offline back-up

Een offsite locatie of offline back-up is essentieel bij ieder herstelplan. Dit houdt in dat u zorgt dat back-ups, licentiegegevens, installatiebestanden en een kopie van het calamiteitenplan buiten de bedrijfsmuren opgeslagen worden. Zorg dat deze back-ups niet aangesloten zijn op het internet (offline back-up), zodat ransomware uw back-up niet kan infecteren.
Bewaar back-upgegevens bovendien veilig en toegankelijk, 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 IT-infrastructuur

Een goed uitgangspunt voor een herstelplan is het maken van een inventarisatie 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, bestanden 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;
- IP-adressen;
- mobiele telefoons met bedrijfsgegevens;
- clouddiensten;
- tablets;
- printers, scanners, kopieer- en faxapparaten.

Inventarisatie bedrijfsprocessen

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?
- Wie is er verantwoordelijk voor de veiligheid van persoonsgegevens?
- 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: draaiboek voor herstel

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.
- Maak duidelijk wie communiceert naar buiten.
- Maak duidelijk wie de medewerkers, klanten en/of media informeert.
- Zorg ervoor dat ieder lid weet welke taak hij/zij heeft als er een calamiteit is.
- Bepaal wie er besluit dat het herstelplan in werking moet treden.
- Beschrijf welke interne functionarissen ingeschakeld moeten worden.
- Beschrijf welke externe partijen/leveranciers moeten worden ingeschakeld (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 webmail?
- 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.

Informeer en instrueer uw medewerkers

Informeer uw medewerkers wat te doen als er zich een cybercalamiteit voordoet. Leg deze afspraken met elkaar vast, zodat het ook beleid wordt. Informeer ze verder over de do's en dont's:

- **Do's:**
  1. Meld het onmiddellijk als een PC vreemd doet.
  2. Meld het altijd onmiddellijk als een apparaat is kwijtgeraakt of gestolen.
  3. Organiseer een goed wachtwoordbeleid, bijvoorbeeld door middel van een wachtwoordmanager.
- **Dont's:**
  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. Maak nooit gebruik van onbeveiligde apparaten of (wifi) netwerken.
  6. Gebruik nooit zomaar een USB-Stick of externe harde schijf in de PC of laptop.

Testen

Cruciaal om uw calamiteitenplan goed te kunnen uitvoeren, is het plan van tevoren te testen. Stel hiervoor een Service Level Agreement (SLA) op. We testen ook het brandalarm, test dan ook jaarlijks de verschillende IT-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.
- Test bij het terugzetten van de back-up ook de nieuwe systemen.
- Laat een ethisch hacker uw systemen ‘hacken’.
- Laat een ethisch hacker een phishingmail-actie als test uitvoeren.
- Laat een ethisch hacker bekijken of ongeautoriseerde mensen alleen naar binnen kunnen lopen.
- Laat een ethisch hacker een USB-drop uitvoeren (leg ergens in uw bedrijf een USB-stick neer en bekijk vervolgens of iemand deze – zonder controle - uitleest).

Betalingen

Als er binnen uw bedrijf betalingen verricht worden door medewerkers, maak hierover dan afspraken. Bijvoorbeeld:

- Tot welk bedrag mag er zonder controle geld overgemaakt worden door uw medewerkers?
- Vanaf welk bedrag geldt het ‘vier ogen principe’?
- Mag er geld overgemaakt worden naar willekeurige rekeningnummers of alleen naar de rekeningnummers in uw adressenboek? Maak vervolgens een adressenboek in uw bankomgeving.
- Welke stappen doorlopen uw medewerkers als er naar een onbekend rekeningnummer een bedrag moet worden over gemaakt?
- Wat is het protocol bij een verzoek per e-mail voor het wijzigen van een rekeningnummer? Advies is om de verzender te bellen om het verzoek en het rekeningnummer te verifiëren.
- Wat is het protocol voor het betalen in opdracht van een e-mail?

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.