Bespreek digitale veiligheid met jouw IT- dienstverlener

Jouw bedrijf is afhankelijk van digitale systemen zoals software en websites. Als bedrijf is het belangrijk om je eigen data en systemen en de data van je klanten goed te beschermen. Een bestaande of toekomstige IT-dienstverlener is daarin een belangrijke partner.

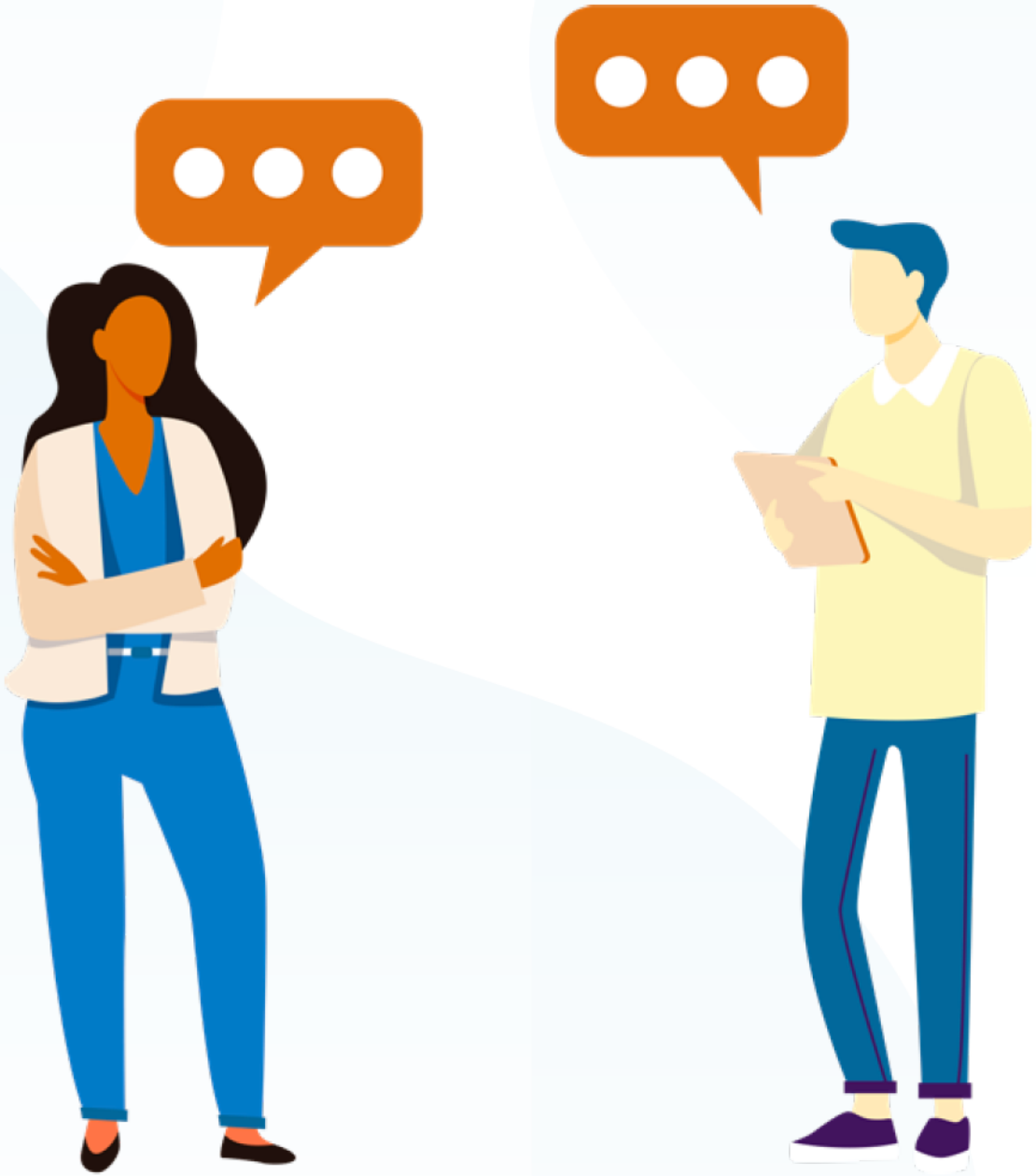
Het uitbesteden van IT betekent niet automatisch dat digitale veiligheid geregeld is. De bescherming van jouw data en continuïteit van jouw bedrijfsprocessen, is een gezamenlijke verantwoordelijkheid.
Om duidelijk te krijgen waar de verantwoordelijkheden liggen zal je in gesprek moeten gaan en blijven met je IT-dienstverlener.

Door in gesprek te blijven met je IT-dienstverlener krijg je inzicht in:

- Afspraken over rollen en verantwoordelijkheden
- De volledigheid van de IT-dienstverlening
- Potentiële aanpassingen die nodig zijn
- De verdeling van verantwoordelijkheden voor digitale veiligheid

In gesprek blijven met jouw IT-dienstverlener over digitale veiligheid is belangrijk maar waar begin je? Zie ommezijde voor de onderwerpen die kunnen helpen als leidraad in het gesprek.

Deze praatplaat is een initiatief van en mogelijk gemaakt door Cybersecurity Alliantie



Belangen van jouw bedrijf

✔ Ga na welke data en bedrijfsprocessen belangrijk zijn voor jouw bedrijf. Bespreek met je IT-dienstverlener welke processen en data beschermd moeten worden.

ⓘ Risico's kunnen op basis van dat gesprek worden geïdentificeerd.

Resultaat:
Gezamenlijk beeld van digitale dreigingen

Inventariseren verantwoordelijkheid

✔ Wat houdt de dienstverlening in, waar ben je zelf verantwoordelijk voor en welke verantwoordelijkheden liggen bij jouw IT-dienstverlener?
Zijn die verantwoordelijkheden voldoende om je bedrijf digitaal veilig te houden?

ⓘ Het is belangrijk om een beeld te hebben van de verantwoordelijkheden van jouw IT-dienstverlener en inzicht in wie wat doet.

Resultaat:
Overzicht dienstverlening en verantwoordelijkheden

Maatregelen tegen digitale dreigingen

Noodzakelijke digitale veiligheid maatregelen kunnen verschillen op basis van specifieke belangen voor jouw bedrijf.

Vraag je IT-dienstverlener welke maatregelen zij nemen en waarom.
Bespreek tenminste de volgende maatregelen:

✔ **Back-up** - Hoe gaat jouw IT-dienstverlener met back-ups om?

ⓘ Heb je een automatische back-up?
Een back-up kan je laatste redding zijn. Dat kan alleen als hier van te voren goed over nagedacht is. Zo moet een back-up de juiste data bevatten, veilig worden opgeslagen en in geval van een incident moet je er tijdig over kunnen beschikken.

✔ **Updates** - Hoe gaat jouw IT-dienstverlener om met updates?

ⓘ Installeert jouw IT-dienstverlener de updates tijdig?
Het tijdig installeren van beveiligingsupdates is belangrijk voor de veiligheid en het functioneren van jouw software. Bespreek met jouw IT-dienstverlener hoe zij er voor zorgen dat alle systemen op tijd en juist worden geüpdatet.

✔ **Wachtwoordbeleid** - Welk wachtwoordbeleid wordt er door jouw IT-dienstverlener gehanteerd?

ⓘ Heb jij al tweefactorauthenticatie ingesteld?
Toegang tot systemen en software moet worden beheerd om basale veiligheid te garanderen. Bespreek tweefactorauthenticatie om ongewenste indringers buiten jouw netwerk te houden.

✔ **Antivirus** - Welk antivirus beleid hanteert jouw IT-dienstverlener?

ⓘ Hoe voorkomt jouw IT-dienstverlener geïnfecteerde computers door een virus?
Bescherming tegen malafide software, beter bekend als 'malware' is actueel. Denk bijvoorbeeld aan ransomware aanvallen. Bespreek met je IT-dienstverlener hoe zij jouw bedrijf beschermen en hoe ze dit monitoren.

Resultaat:
Basismaatregelen

Rapportage

✔ Vraag de IT-dienstverlener om structureel een rapportage te leveren van de dienstverlening.

ⓘ Hoe vaak ontvang jij een rapportage van jouw IT-dienstverlener?
Deze rapportages geven jou de mogelijkheid te controleren, bij te sturen en input te geven in een volgend gesprek. Zo'n rapportage bevat minimaal de genomen maatregelen (back-ups, updates etc.) en het effect hiervan over een bepaalde tijd.

Resultaat:
Controle en verantwoording

Wil je meer weten over digitale veiligheid, bezoek dan de website van het DTC: digitaltrustcenter.nl.

digital trust center.