Cyber
Weerbaarheidscentrum
Greenport

Afspraken maken met een IT-leverancier

De veranderingen in het bedrijfsleven versnellen en we doen steeds vaker een beroep op technologie. Tegelijkertijd wordt technologie steeds complexer, waardoor je als ondernemer meer tijd kwijt bent aan het onderhouden van je technische omgeving, zoals het beheren van je laptops, netwerkapparatuur en de beveiliging hiervan. In plaats van dit zelf te doen, kun je ervoor kiezen dit uit te besteden aan een externe dienstverlener. Hierbij is het belangrijk om goede afspraken te maken, zodat je zeker weet dat je een volledig werkbare omgeving met de juiste beveiligingsmaatregelen krijgt.

Uitbesteden van IT

Bij het uitbesteden van IT draag je (een deel van) het beheer van je hardware, software en IT-beleid over aan een externe dienstverlener. Je kiest zelf of je het volledige beheer wilt uitbesteden, of dat je alleen een bepaalde dienst of product wilt afnemen. Een dienstverlener heeft specialistische kennis en zorgt dat de diensten die je afneemt goed werkbaar en beveiligd zijn. Zij zorgen vaak ook voor het onderhoud en de beveiliging van deze diensten, zodat jij je volop kan richten op je bedrijfsvoering.
Uitbesteding kan flexibiliteit bieden, bijvoorbeeld als je tijdelijk extra laptops nodig hebt. Daarnaast kan het uitbesteden van IT kosten besparen doordat er geen directe kapitaalinvesteringen nodig zijn, zoals het in dienst hebben van een IT-specialist of het in één keer aanschaffen van alle laptops en netwerkapparatuur. In ruil daarvoor betaal je maandelijks een afgesproken bedrag.

Het maken van afspraken

Het is belangrijk goede afspraken te maken met je externe dienstverlener, zodat je zeker weet dat de diensten die je afneemt goed onderhouden worden en voldoende beveiligd zijn. Deze afspraken leg je vooraf vast in een zogenaamde Service Level Agreement (SLA). Dit is een type overeenkomst waarin afspraken staan tussen de aanbieder en afnemer van een dienst of product. Denk hierbij bijvoorbeeld aan de beschrijving van de dienst, de duur van de overeenkomst, informatie over eigendom en risico, beveiliging, en wat er gebeurt in het geval van geschillen.
Ieder bedrijf heeft andere wensen. Daarom moeten er duidelijke afspraken gemaakt worden over de producten en diensten je afneemt en onder welke voorwaarden. Het moet bijvoorbeeld duidelijk zijn wie verantwoordelijk is voor het uitvoeren van onderhoud, of er periodiek controles worden gedaan op kwetsbaarheden en of je data regelmatig geback-upt worden.

Checklist Service Level Agreement

Graag bieden we je een checklist aan voor het opstellen van een SLA met je IT-leverancier. Zie het als handvatten voor het maken van goede afspraken over het opzetten en beveiligen van je IT-omgeving.
Tip Bij het maken van een overeenkomst is het belangrijk dat begrippen meetbaar en eenduidig zijn, zodat de overeenkomst niet gebaseerd is op interpretatie. Gebruik het Cybersecurity woordenboek van Cyberveilig Nederland.voor heldere begrippen en definities van lastige (IT-)terminologie.

1. Producten- en dienstenoverzicht.

Wat besteed je precies uit aan de leverancier?

- Wat gaat de dienstverlener leveren? ICT-diensten, of ook ICT-apparatuur?
- Is er een duidelijke beschrijving van de producten of diensten (en waar die voor dienen) opgenomen?
- Is het helder voor welke producten en diensten je zelf nog verantwoordelijk bent?

2. Onderhoud

Wanneer, door wie en met welke regelmaat wordt onderhoud uitgevoerd?

- Welk onderhoud moet worden uitgevoerd? Denk o.a. aan updates en patches van software waarmee kwetsbaarheden worden gerepareerd.
- Door wie wordt onderhoud uitgevoerd en om welk onderhoud gaat het dan precies?
- Wanneer en hoe vaak wordt onderhoud uitgevoerd?
- Wordt het onderhoud uitgevoerd op momenten dat het geen invloed heeft op de bedrijfscontinuïteit (bijvoorbeeld 's nachts in plaats van tijdens kantooruren)?

3. Preventieve beveiliging

Welke maatregelen zijn getroffen tegen aanvallen van buitenaf?

- Zijn alle apparaten voorzien van antivirussoftware?
- Is het netwerk voorzien van een firewall en zo ja, wordt die met regelmaat getest?
- Worden kritieke systemen extra beschermd, bijvoorbeeld door middel van tweefactorauthenticatie?
- Wordt de veiligheid van de (geleverde) apparaten regelmatig getest en, zo ja, hoe vaak?
- Wie is voor welke beveiligingsmaatregelen verantwoordelijk?
- Vinden er periodieke controles plaats om zeker te stellen dat de beveiligingsmaatregelen en het beleid haar werk doen en de onderneming geen risico's loopt?

4. Werkplekken

Welk beveiligingsbeleid is van toepassing?

- Is afgesproken wie verantwoordelijk is voor het opstellen en uitvoeren van het werkplekbeveiligingsbeleid?
- Zijn er afspraken gemaakt over het gebruik van apparatuur die eigendom is van medewerkers, zoals 'Bring Your Own Device' apparatuur?
- Worden medewerkers verplicht om een sterk wachtwoord te gebruiken?
- Worden gegevens op computers, laptops en andere mobiele apparaten **versleuteld** opgeslagen?

5. Gegevensbescherming

Hoe wordt bedrijfsinformatie beschermd tegen datalekken en dataverlies?

- Weet je of de bedrijfsinformatie in de cloud of lokaal zal worden opgeslagen?
- Als het in de cloud wordt opgeslagen, is de informatie dan **versleuteld**?
- Wie heeft toegang tot de in de cloud opgeslagen data?
- Worden er back-ups gemaakt van informatie die niet in de cloud maar lokaal wordt opgeslagen?

6. Cyberaanvallen en andere incidenten

Wie is het aanspreekpunt?

- Weet je bij wie je terecht kunt als er zich een probleem voordoet?
- Is de incidentmeldingsprocedure duidelijk en niet te omslachtig?
- Is vastgelegd binnen welke tijd de dienstverlener moet reageren op een incidentmelding (response time) en binnen welke tijd een oplossing moet worden geboden (oplostijd)?
- Wat is de beschikbaarheid van de ondersteuning? Heeft de leverancier een 24x7 service?

7. Prestatie-eisen

Welke prestatie-eisen zijn nodig en hoe wordt dit gemeten?

- Wat wordt er in het SLA toegezegd over de beschikbaarheid (*uptime*) van de systemen/software?
  Let op: Als een uptime van 99,9% per jaar wordt gegarandeerd, mogen je systemen er per jaar een ruime werkdag achter elkaar niet functioneel zijn. Als dit percentage per maand wordt berekend, is het minder dan één uur.

- Wat staat er in het SLA over hoe lang een dienst offline mag zijn voor bijvoorbeeld onderhoud of door storingen (*downtime*)?
- Valt gepland onderhoud binnen de uptime of binnen de downtime?
- Wordt de beschikbaarheid van de systemen/software gegarandeerd op de relevante momenten (bijvoorbeeld updaten systemen buiten kantoortijden)?

8. Contractbreuk

Wat gebeurt er als afspraken in het SLA niet nagekomen worden?

- Wat is de vergoeding als de overeengekomen afspraken in het SLA niet worden nagekomen of niet (voldoende) worden nageleefd? Denk daarbij aan de mogelijke schade die je daardoor kan leiden.
- Wat zijn de afspraken met betrekking tot schadevergoedingen?
- Zijn er afspraken over aansprakelijkheid vastgelegd?

Dit document is gebaseerd op het document 'Afspraken maken met een IT-leverancier' van het Digital Trust Center. Het originele document is te vinden via https://www.digitaltrustcenter.nl/informatie-advies/afspraken-maken-met-een-it-leverancier