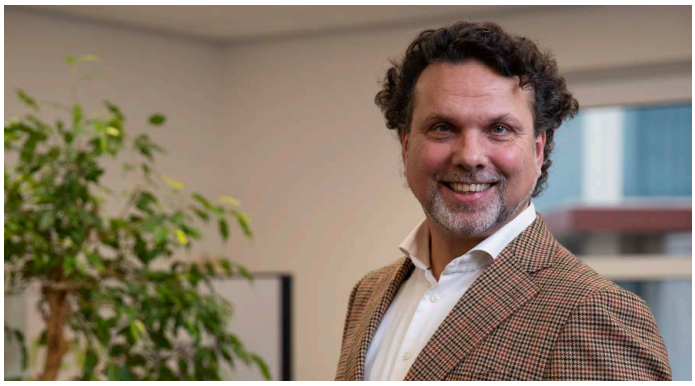

LEVERANCIERSMANAGEMENT; ONTZORGING TEGEN CYBERSECURITY?

Veel bedrijven maken gebruik van 'IT-leveranciers'. Zeker in het mkb zien we eigenlijk niet anders. Dat is ook zeer begrijpelijk. Niet elke mkb-ondernemer heeft daar interesse in of kennis van en met de huidige technologie hoeft dat ook niet altijd. Helaas zie ik dat het – ondanks de beste intenties van alle betrokken partijen – te vaak misgaat. Ook op het gebied van 'cybersecurity'. Deze tips verkleinen een mogelijke valkuil.

1. Stel een goed contract op waarbij het voor partijen en een deskundige derde klip en klaar is welke IT-dienst wordt geleverd en wie welke verantwoordelijkheden heeft. Dit klinkt simpel maar is soms door de complexiteit van de dienst en de juridificering van een contract soms toch echt lastig.
2. Neem in deze overeenkomst ook een hoofdstuk op over 'informatiebeveiliging', of iets soortgelijks.
3. Werk in dit hoofdstuk concreet uit wat partijen moeten doen en probeer weg te blijven van algemene nietszeggende juridisch vocabulaire als 'in overeenstemming met de wet' of 'marktconform'. Dit zijn termen gebruikt door juristen die helaas onvoldoende inhoudelijk zijn onderlegd om dit type overeenkomst voldoende concreet te maken.
4. Sluit bij het specificeren van deze verplichtingen met betrekking tot informatiebeveiliging aan bij een standaard voor informatiebeveiliging (zoals de ISO 27001, de NIST, OWASP, CobiT, etc), maar laat het hier niet bij. Werk in een bijlage nader uit op welke wijze door een leverancier invulling wordt gegeven aan een dergelijke standaard. Spreek bijvoorbeeld af dat een leverancier niet zonder expliciet akkoord van de klant op dat moment toestemming krijgt om bepaalde werkzaamheden uit te voeren en daarna de toegang weer goed te vergrendelen (hier ging het mis bij de hack op het Hof van Twente).
5. Dwing af dat er door de leverancier expliciete periodieke waarborgen worden verstrekt. Enkel een ISO 27001 certificaat is eigenlijk al niet meer voldoende. Denk ook aan een '3402-verklaring' of een 'SOCII/SOCIII'rapport. Maar ook meer specifiek als de resultaten van een periodiek (minstens eens per drie maanden) uitgevoerde pentest en/of vulnerability scan, de resultaten van de door de leverancier uit te voeren 'Control Risk Self Assessment'.

Deze tips helpen je niet alleen bij het verkleinen van de kans dat je het slachtoffer wordt van hackers. Ze helpen je ook om aantoonbaar te voldoen aan de verplichtingen van de privacy wet voor diegene die persoonsgegevens verwerkt. En welke organisatie doet dat feitelijk niet?

Alex Klaassen, IT Risk organisatie NewDay
newdayriskservices.nl