EEN VAN DE MEEST ONDERSCHATTE ONDERWERPEN BIJ IT-RISICO'S IS HET INVENTARISEREN VAN DE HARDWARE EN SOFTWARE DIE IN GEBRUIK IS. ALS JE NAMELIJK NIET WEET WAT JE BEZIT OF IN GEBRUIK HEBT, DAN KUN JE OOK DE RISICO'S DIE MET DIT BEZIT OF GEBRUIK SAMENHANGEN NIET ANALYSEREN.

Risicomanagement in een IT-omgeving

TEKST **WIM VAN DE WEG**

Stel bijvoorbeeld dat je een moderne all-in-one printer in gebruik hebt. Dan is de kans groot dat deze printer een interne harde schijf bevat waarop print- en kopieeropdrachten worden opgeslagen. Als je deze printer buiten gebruik stelt en afvoert naar een milieustraat, dan moet je je ervan bewust zijn dat deze printer een schat aan vertrouwelijke informatie bevat. Het is natuurlijk niet de bedoeling dat deze informatie in verkeerde handen valt. Je zou dan kunnen overwegen om de harde schijf voor afvoer te schonen of de harde schijf professioneel te laten vernietigen. Maar daar moet je dan wel vooraf over nagedacht hebben (het risico gemanaged hebben).

Een dergelijke moderne printer is in de praktijk aangesloten op het netwerk en verbonden met het internet. Als de printer ook verbonden is met het Wifi-netwerk, dan kan de printer een eenvoudig doelwit zijn van kwaadwillenden. Dit is dan met name het geval als de af-fabriek instellingen niet zijn aangepast en de gebruikersnaam en het wachtwoord nog 'admin', 'admin' is. Maar ook een beveiligingslek in de printersoftware kan een kwaadwillende toegang geven tot de printer en uw netwerk. Het is daarom noodzakelijk dat ook de printer meegenomen wordt in de cyclus van het verwerken van software-updates.

'Beoordeel IT-risico's aan de hand van Beschikbaarheid, Integriteit en Vertrouwelijkheid'

De inventarisatie kan vastgelegd worden in een eenvoudig Excel-bestand, maar er is ook specifieke software voor beschikbaar. Een keuze zal afhangen van de omvang van de onderneming en de inventarisatie.

UITBESTEDING

Bij het inventariseren van de hard- en software die in gebruik is moet ook beoordeeld worden in hoeverre er sprake is van dienstverlening van derden. Bijvoorbeeld de dienstverlening die wordt aangeboden als een Software as a service (SAAS)-toepassing of waarbij de infrastructuur wordt ingekocht als een Infrastructuur as a service (IAAS)-toepassing. In onze verzekeringsbranche zijn op dit gebied Missing Piece, Tribion (VPO) en Boxing IT, bekende leveranciers. Maar ook Azure (Microsoft), AWS (Amazon) en Google zijn grote bekende partijen waar data extern wordt opgeslagen.

In de Principes voor Informatiebeveiliging benoemt de AFM elf principes die van belang zijn bij informatiebeveiliging. 'Uitbesteding' en 'Ketenperspectief' zijn twee van deze principes.

De AFM is van mening dat de onderneming die uitbesteed zelf verantwoordelijk blijft voor de informatie-

beveiliging van de uitbestede processen en systemen. Gezien het belang van de data die financieel dienstverleners verzamelen en beheren, moet je die verantwoordelijkheid ook zelf willen.

Dit betekent dat je in de praktijk overleg hebt met je leverancier en bespreekt welke beveiligingsmaatregelen er getroffen zijn en hoe door de leverancier wordt bewaakt dat deze maatregelen ook worden nageleefd. Ook worden afspraken gemaakt hoe de leverancier periodiek over deze onderwerpen rapporteert. Een belangrijk punt is hier de omvang van de beveiligingsmaatregelen. Een financieel dienstverlener zal moeten beoordelen of de door de leverancier getroffen maatregelen passen bij de wensen/eisen die de financieel dienstverlener heeft. Deze wensen/eisen worden niet alleen bepaald door zijn risk appetite (welke risico's wil en kun je accepteren?) maar ook door de ideeën die een toezichthouder daar over heeft. Als je gevolmachtigd agent bent, dan heb je ook te maken met de eisen die gesteld worden in het Werkprogramma Risicobeheersing Volmachten als er sprake is van applicaties/data met een verzekeringstechnisch of financieel gevolg voor een volmachtgever. Ook kunnen er nog andere regelingen van toepassing zijn zoals bijvoorbeeld de Digital Operational Resilience Act (DORA).

BIV

Een veel gebruikte indeling voor het beoordelen van IT-risico's is het acroniem BIV. Beschikbaarheid, Integriteit en Vertrouwelijkheid. De beschikbaarheid heeft betrekking op de vraag of de data beschikbaar is voor dagelijks gebruik. Dit kan bijvoorbeeld verstoord worden door uitval van de server, waardoor medewerkers geen toegang meer hebben tot de assurantieapplicatie. De integriteit heeft betrekking op de juistheid van de informatie. Als er in de assurantieapplicatie staat dat een motorrijtuig WA + Casco is verzekerd, dan moet dat ook zo zijn en dan moet de dekking niet ongeautoriseerd aangepast zijn. Vertrouwelijkheid heeft betrekking op de vraag of onbevoegden de beschikking kunnen krijgen over de data. Bijvoorbeeld diefstal van data door een hacker of de afscherming van hypotheekadviesdossiers voor de afdeling schadebehandeling.

De afspraken die je maakt met jouw leverancier over informatiebeveiliging moeten onderdeel zijn van de formele overeenkomst die wordt opgesteld. Omdat niet alles hetzelfde blijft, is het verstandig om de risicoanalyse ten aanzien van de uitbesteding periodiek te actualiseren. Niet alleen bij ingrijpende gebeurtenissen, zoals een bedrijfsfusie, maar ook bijvoorbeeld jaarlijks beoordelen of de uitgangspunten die gehanteerd zijn nog steeds gelden, of er nieuwe risico's of eisen zijn en of voortschrijdende inzichten wellicht aanpassing vragen. Ook is het dan een goed moment om te beoordelen in hoeverre de leverancier voldoet aan de gemaakte afspraken.

Het principe 'ketenperspectief' heeft betrekking op een integrale ketenbenadering. Of er nu sprake is van een eigen IT-omgeving of van een uitbestedingssituatie, de systemen die bij financieel dienstverleners in gebruik zijn worden complexer. Onder andere doordat er meer partijen betrokken zijn in de keten. Denk hierbij aan offerteprogrammatuur van partij X die gekoppeld wordt aan de assurantieapplicatie die geleverd wordt door partij Z. Maar ook aan programmatuur die gebruikt wordt bij geautomatiseerde acceptatie en schadebehandeling en waarbij de programmatuur die dit mogelijk maakt in verschillende datacenters wordt opgeslagen.

De ketenpartijen zullen ervoor moeten zorgen dat de informatiebeveiliging in de gehele keten op het gewenste niveau is.

Als een financieel dienstverlener de informatiebeveiliging wil organiseren, dan is het handig om gebruik te maken van een format of norm. Er zou bijvoorbeeld gestart kunnen worden met een ISO 27001-certificeringstraject. ■

Wim van de Weg is partner SVC Groep en Certified Risk Manager.

NORMENKADER

Door SVC is voor financieel dienstverleners een normenkader 'Privacy en informatiebeveiliging' ontwikkeld op basis waarvan via een self assessment bepaald kan worden wat sterke punten zijn en op welke punten er nog verbetering mogelijk is. Stuur een e-mail naar info@svcgroep.nl onder vermelding van Normenkader Privacy en Informatiebeveiliging, dan worden dit normenkader en een actiepuntenregister (kosteloos) verstrekt.