

Informatiebeveiliging in de cloud

Opkomende diensten in de vorm van 'cloudservices' stellen organisaties voor nieuwe uitdagingen. Waar eerst alle informatie en diensten nog door de organisatie zelf werden beheerd en aangeboden, zullen in het geval van cloudservices de informatie en diensten worden beheerd en aangeboden door een andere partij. Deze nieuwe vorm van dienstverlening brengt specifieke risico's met zich mee ten aanzien van informatiebeveiliging.

TOM KLEIBERG *

Het internet heeft een steeds prominenter rol gekregen in zakelijke toepassingen en processen. Werknemers in alle lagen van de organisatie, van bestuurders tot het personeel op de werkvloer, gebruiken het internet of toepassingen die via in-

ternetomgeving is steeds onveiliger geworden. Cybercriminaliteit behoort tegenwoordig tot de meest lucratieve vormen van criminaliteit. Overtreders hebben eenvoudig toegang tot vele slachtoffers, terwijl het risico gearresteerd te worden of überhaupt betrappt te

stellen de organisatie voor nieuwe uitdagingen. Waar in het traditionele scenario alle informatie en diensten nog door de organisatie werden beheerd en aangeboden, zullen in het geval van cloudservices de informatie en diensten worden beheerd en aangeboden door een andere partij! Een deel van de rol van de IT-beheerder wordt hierdoor overgenomen door de cloudprovider. Deze nieuwe vorm van dienstverlening brengt specifieke risico's met zich mee ten aanzien van informatiebeveiliging. Zo is een cloudprovider een zeer interessant doelwit voor criminelen vanwege de enorme hoeveelheid informatie die voorhanden is. Daarnaast is het zaak om informatie van de verschillende organisaties die gebruikmaken van de cloudprovider, zo goed mogelijk te scheiden. Bovendien kleven er allerlei juridische kwesties aan cloudservices; wie is er bijvoorbeeld aansprakelijk wanneer een inbraak op één van de systemen van een cloudprovider ook gevolgen heeft voor andere klanten van de cloudprovider?

De afnemer van de cloudservice legt een deel van de informatiebeveiliging in handen van de cloudprovider

terne netwerken communiceren. Met deze nieuwe ontwikkelingen ontstaan ook nieuwe risico's. De bedrijfsinformatie die gedeeld wordt via deze netwerken, is doorgaans vertrouwelijk en dient binnen de organisatie te blijven. Voorheen werd deze last op de schouders van de IT-afdeling gelegd. Informatie was een IT-aangelegenheid en het was de taak van de IT-beheerder om de omgeving zo veilig mogelijk in te richten. Beveiliging werd gezien als een product: installeer een firewall, voorzie alle systemen van virusscanners en de beveiliging is in orde.

Nieuwe bedreigingen

Vandaag de dag zien we dat dit uitgangspunt niet meer toereikend is. De

worden, bijzonder laag is. Bovendien is de beloning zeer aantrekkelijk. Kortom, cybercriminaliteit is niet langer iets voor eenzame hackers op een zolderkamer, maar is verworpen tot een georganiseerde vorm van misdaad. Deze nieuwe bedreigingen vormen aanzienlijke financiële en economische risico's voor een organisatie en hebben een onmiskenbare invloed op de beveiligingshuishouding.

Nieuwe uitdagingen

Technologische ontwikkelingen vormen een andere stimulans voor het herzien van de filosofie dat informatiebeveiliging wel 'uitbesteed kan worden' aan de IT-afdeling. Opkomende diensten in de vorm van 'cloudservices'

Security in de cloud

Om deze risico's te kunnen bepalen, is het voor de cloudprovider belangrijk om te weten wat de waarde is van de informatie op zijn systemen. Dit vereist medewerking van alle betrokkenen, van zowel de cloudprovider als de afne-



mer van de cloudservices. Beiden dienen een beleidsplan in werking te hebben dat aangeeft hoe er met gevoelige informatie omgegaan dient te worden en wat de eisen zijn ten aanzien van informatiebeveiliging. De afnemer van de cloudservice legt een deel van de taak van informatiebeveiliging in handen van de cloudprovider en wil dus zekerheid hebben dat zijn informatie in veilige handen is. Een goed beleidsplan brengt structuur aan in de beveiliging van informatie en schept een kader voor het eisenpakket. Informatiebeveiliging dient als een integraal proces ingebakken te worden in de organisatie en zou een belangrijk onderdeel van de bedrijfsvoering moeten vormen. Boven-

dien helpt een beleidsplan bij het maken van afspraken en het verdelen van verantwoordelijkheden tussen een cloudprovider en de afnemer.

Beleid, techniek en de mens

Beveiliging berust op drie pijlers: beleid, techniek en de mens. Het samenspel tussen deze drie factoren bepaalt de kwaliteit van beveiliging van de IT-omgeving en zodoende de bedrijfsinformatie. Informatiebeveiliging is een integraal risicomanagementproces waaraan een visie en beleid ten grondslag liggen.

Beleid

Een informatiebeveiligingsbeleid is een op strategisch niveau vastgesteld docu-

ment waarin op hoofdlijnen doelen en richtlijnen worden geformuleerd op het gebied van informatiebeveiliging. Het schept een kader voor de tactische en operationele invulling van informatiebeveiliging. Het is een richtinggevend document voor de uitvoerders, het middenkader en de medewerkers, en beschrijft een (niet te gedetailleerde) route van de huidige situatie naar de te bereiken doelstelling. Het beleid bepaalt aan welke eisen de omgeving dient te voldoen, waarbij zowel technische als niet-technische aspecten aan de orde komen. Hoe kunnen resources optimaal worden ingezet om de beveiliging te realiseren en te garanderen, welke trainingen zijn nodig voor het



personeel en aan welke wettelijke voorschriften of regulerende normen dient te worden voldaan? Daarnaast dient een beleid te voorzien in een gestructureerd auditplan, dat de aanwezige omgeving met regelmaat controleert op gebreken. Het uitvoeren van audits of security reviews, door interne of externe partijen, is van grote waarde om de beveiliging scherp te houden en leidt vaak tot verbeteringen. Ten slotte is het volgen van technische ontwikkelingen belangrijk om op de hoogte te blijven van de ontwikkelingen in de markt en te weten waar de nieuwe mogelijkheden én bedreigingen liggen.

Techniek

Informatievoorziening en de technische infrastructuren die hieraan ten grondslag liggen, worden steeds com-

plexer, dynamischer en ingrijpender. dit stuit regelmatig op verzet en men verzandt vaak in een overvloed aan regels en overhead. Zo zou men het gebruik van cloudservices kunnen beperken tot eindstations met zeer repressieve beveiligingsmaatregelen, of alleen vanaf zeer beperkte locaties, maar dit zal frustrerend werken en de flexibiliteit van de werknemer onder druk zetten. De ervaring leert dat het belangrijk is een balans te vinden tussen beveiliging en werkbaarheid, waarbij de techniek liefst zoveel mogelijk op de achtergrond acteert en de werknemer zo min mogelijk gehinderd wordt in zijn dagelijkse bezigheden. Een voorbeeld hiervan is het gebruik van encryptie op eindstations, zoals laptops. De medewerker zal zich nauwelijks bewust zijn van deze maatregel, maar een eventueel verlies van de laptop zal zich

verliezen van een laptop of het per ongeluk e-mailen van gevoelige informatie naar een verkeerde persoon.

Technische maatregelen kunnen een belangrijke rol spelen als vangnet voor menselijk handelen, maar hier zitten grenzen aan en het aansturen van mensen vormt een belangrijk facet van een degelijk beveiligingsbeleid. Een beleidsplan is daarom niet compleet zonder de belangrijkste schakel daarin mee te nemen: de mens. De mens vormt zowel de sterkste als de zwakste schakel in het beveiligingsbeleid. Het verschil tussen deze twee uitersten wordt bepaald door bewustwording van de gevaren van het internet en het volgen van de juiste richtlijnen met betrekking tot het omgaan met informatie.

Verdeel de verantwoordelijkheden binnen de organisatie over verschillende mensen en zorg dat informatie alleen beschikbaar wordt gesteld aan degenen die het nodig hebben. Gecombineerd met de juiste training kan het personeel bewust worden gemaakt van het belang van beveiliging en krijgt het aandacht voor de risico's die met gevoelige informatie gepaard gaan.

In het geval van de cloudprovider zal de medewerker van de cloudprovider ruime kennis van zaken hebben en zich bewust zijn van de gevaren van cloudservices. Aan de andere kant zijn de belangen van de cloudprovider bijzonder groot. De impact van dataverlies bij een cloudprovider kan gevolgen hebben voor veel organisaties die bij de cloudprovider aangesloten zijn. «

* Tom Kleiberg is Security Consultant bij Pinewood in Delft

Cloud-infrastructuren zijn uitermate complex en hebben zeer specifieke eisen voor informatiebeveiliging

plexer, dynamischer en ingrijpender. Cloud-infrastructuren zijn uitermate complex en hebben zeer specifieke eisen ten aanzien van informatiebeveiliging. Vanwege virtualisatie en het delen van resources is er extra technologie vereist om de informatie veilig te houden. Het inrichten van een beveiligingsomgeving bestaat niet louter nog uit het simpel configureren van een firewall, maar is vakwerk en dient uitgevoerd te worden door experts met de focus op beveiliging. Zij beschikken over de kennis die nodig is om technische oplossingen te configureren, integreren en beheren. De impact van een falende technische oplossing is aanzienlijk. Een falende technische oplossing in een cloudomgeving heeft vaak gevolgen voor meerdere klanten. De gevolgen van een falende oplossing dienen dus geïsoleerd te worden en zoveel mogelijk beperkt te blijven. Aan de andere kant is het belangrijk dat men oog houdt voor de werkbaarheid van de cloudservices. Het is relatief eenvoudig om de hele omgeving dicht te timmeren zodat men geen enkele vrijheid meer heeft in de werkomgeving, maar

tot een klein materieel verlies beperken, aangezien de informatie die op de laptop staat niet toegankelijk is voor derden.

Mens

Het ontwerp van uw IT-omgeving maar ook die van de cloudprovider moet niet alleen bestand zijn tegen aanvallen van buitenaf, maar dient ook rekening te houden met dreigingen van binnenuit. Veel beveiligingsincidenten ontstaan door onopzettelijk dataverlies, zoals het

Samenvatting

- » Het is belangrijk dat er een **beleid** is dat aangeeft hoe men omgaat met **waardevolle informatie en objecten**.
- » Dit beleid wordt doorgevoerd in **verschillende processen**, zoals fysieke beveiliging, maar ook informatiebeveiliging.
- » **Houd criminelen op afstand** door medewerkers bewust te maken van het **belang van informatiebeveiliging** en regel de **techniek** op de achtergrond in als een **vangnet voor onbewust handelen**.
- » Zorg ervoor dat uw **cloudprovider** een **helder beleidsplan** heeft dat aansluit op uw eisen en zorg ervoor dat er **afspraken** gemaakt zijn met betrekking tot **aansprakelijkheid**.