Third-Party Assurance: nut of noodzaak?

Het outsourcen van IT-diensten naar de cloud biedt veel voordelen voor organisaties. De zorgen met betrekking tot het onderhouden en beveiligen van de IT-diensten zijn de verantwoordelijkheden geworden van de leverancier. De organisatie wordt ontzorgd en de risico's worden overgedragen met een contract.

Toch blijkt dat outsourcen van IT-dienstverlening geen garantie biedt voor een IT-omgeving zonder zorgen, zelfs dienstverlening van Microsoft, Amazon en Google kunnen verstoringen geven.

Gecontracteerde diensten blijken onderhevig aan verstoringen die een impact hebben op de dagelijkse bedrijfsvoering. Hoe kan een organisatie omgaan met de IT-risico's en risico's op reputatieschade die hiermee gepaard gaan? En welke geïmplementeerde controles mag een IT-auditor verwachten van een organisatie om de risico's te mitigeren? Om deze vraag te beantwoorden is het belangrijk om eerst te begrijpen wat het risico is en wat de kwetsbaarheden zijn van een organisatie om te komen tot een gedegen framework.

Het risico

Er bestaan verschillende studies naar verstoringen vanuit leveranciers en hun impact die kunnen helpen om te bepalen of deze verstoringen overwogen moeten worden als significant risico.

Onderzoek van het Business Continuity Institute (BCI)[1] geeft aan dat de financiële schade die bedrijven hebben geleden loopt tot in de miljoenen vanwege één of meerdere verstoringen vanuit leveranciers.

Het risico van de continuïteit van clouddienstverlening wordt ook onderstreept door onderzoek van Uptime Institute[2]. In dit onderzoek naar verstoringen die publiekelijk zijn gemeld, is te zien dat er de afgelopen drie jaar steeds vaker melding wordt gemaakt van verstoringen in de clouddienstverlening. Mogelijk neemt het aantal publiekelijk gemelde verstoringen toe door wettelijke verplichtingen. Echter, dit toont wel aan dat verstoringen nog steeds voorkomen. Daarom zullen de risico's die verstoringen veroorzaken in overweging moeten worden genomen.

Ook een onderzoek[3] van (ISC)[2] naar beveiligingsincidenten in de cloud geeft aan dat 28 procent van de onderzochte organisaties specifiek te maken heeft gehad met beveiligingsincidenten in de cloud.

Verstoringen vanuit leveranciers zijn niets nieuws en zijn een risico om rekening mee te houden. Grote cloudproviders als Microsoft[4], Google[5] en Amazon[6]

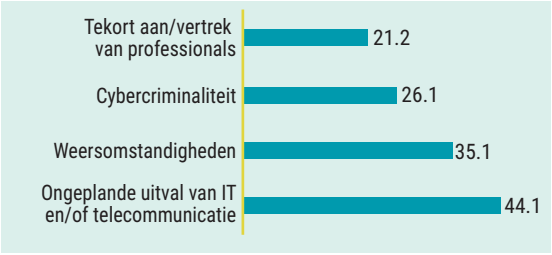
Jouke Albeda, CISA, CISSP, RE
Is een ervaren IT-auditor die bedrijven ondersteunt op het gebied van audit, risk en compliance vanuit zijn bedrijf Contrisity. Tevens is hij aangesloten bij 3angles: audit, risk en compliance. Hiervoor was hij risk en compliance manager bij Datacenter.com en heeft hij voor Binder Dijker Otte (BDO) en Ernst & Young (EY) gewerkt binnen de externe IT-audit discipline. Hij heeft reeds artikelen gepubliceerd in de magazines *Audit Magazine* van The Institute of Internal Auditors (IIA) en *de IT-Auditor* van NOREA.

zijn transparant over de regelmatige omgang met verstoringen. Het is belangrijk om te realiseren wat de impact van de risico's is op de organisatie.

Oorzaken van verstoringen

Verschillende onderzoeken onthullen verschillende oorzaken van verstoringen. Vanuit het rapport van BCI (**afbeelding 1**) blijkt dat 44,1 procent van de verstoring komt door ongeplande uitval van IT en/of telecommunicatie. Verder zijn weersomstandigheden (35,1 procent), cybercriminaliteit (26,1 procent) en een tekort aan/vertrek van professionals (21,2 procent) belangrijke factoren die de dienstverlening vanuit leveranciers aantasten. Het is een combinatie van technisch falen, externe factoren en menselijk handelen.[7]

Afbeelding 1—BCI Oorzaken van Verstoringen



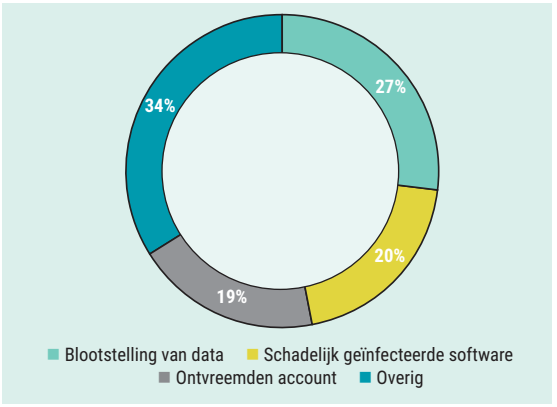
Bron: Uitkomsten van Business Continuity Institute (BCI), *BCI Supply Chain Resilience Report 2019*, United Kingdom, 5 November 2019, *https://www.thebci.org/resource/bci-supply-chain-resilience-report-2019.html*

Het onderzoek (**afbeelding 2**) van (ISC)² duidt ook externe factoren en menselijk handelen aan als oorzaken van publieke cloud-gerelateerde beveiligingsincidenten. In meer dan een kwart van de gevallen (27 procent) gaat het om data die op straat komt te liggen. Verder zien we in 20 procent van de gevallen schadelijk geïnfecteerde software en in 19 procent van de gevallen het ontvreemden van een account.[8]

Het rapport van Uptime Institute (**afbeelding 3**) geeft aan dat datacenter gerelateerde systemen de voornaamste reden van uitval is (32 procent), gevolgd door het falen van IT-systemen (31 procent) en netwerkproblemen (29 procent). Hierin is geen onderscheid gemaakt tussen technische problemen, menselijk handelen en externe factoren.[9]

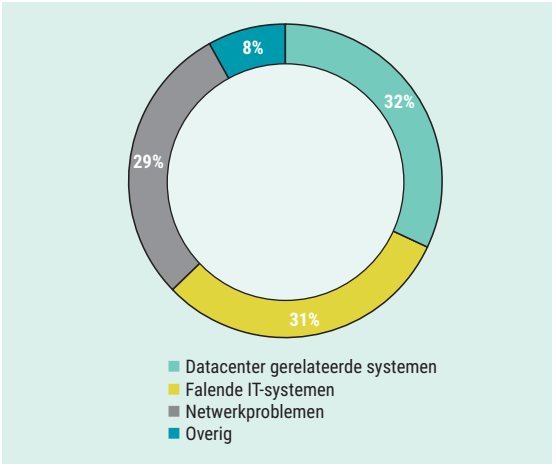
Kijkend naar de oorzaken, zal een combinatie van maatregelen moeten worden geïmplementeerd die zowel de technische risico's, operationele risico's

Afbeelding 2—(ISC)² Publieke Cloud-Gerelateerde Beveiligingsincidenten



Bron: Uitkomsten van (ISC)², *2019 Cloud Security Report*, USA, August 2019, *https://www.cybersecurity-insiders.com/portfolio/2019-cloud-security-report-isc2/*

Afbeelding 3—Uptime Institute Reden van uitval



Bron: Uitkomsten van Uptime Institute, *Publicly Reported Outages 2018-19*, USA, March 2019, *https://uptimeinstitute.com/publicly-reported-outages-2018-19*

als risico's van menselijk handelen adresseren. De bestaande kennis over het ontwerpen en gebruiken van technologie (bijvoorbeeld het COBIT®-framework, International Organization for Standardization [ISO] -standaarden, Trust Service-principes) zullen gebruikt moeten worden om onnodige zwakheden in systemen te voorkomen. Het gebruik van 'best practices' kan voorkomen dat veelgemaakte fouten worden gemaakt. Best practices en frameworks gepubliceerd door erkende beroepsgroepen zoals ISACA®, ISO, Payment Card Industry Data Security Standard (PCI-DSS) en het US National Institute of Standards and Technology (NIST) zijn beschikbaar en adresseren de menselijke factoren en andere externe en technische factoren.

Het wegen van het risico

Verstoringen hoeven niet altijd een grote impact te hebben op de afnemer van de dienstverlening. Bijvoorbeeld, het niet beschikken over een testsysteem voor een uur heeft veelal geen significant effect op de productiviteit van een eindgebruiker. Echter, het niet beschikken over een operationeel handelssysteem voor een beurshandelaar voor een kwartier zal een aanzienlijke impact hebben. Ook als het gaat om het lekken van data is de impact op een testdatabase anders dan op een database met persoonsgegevens.

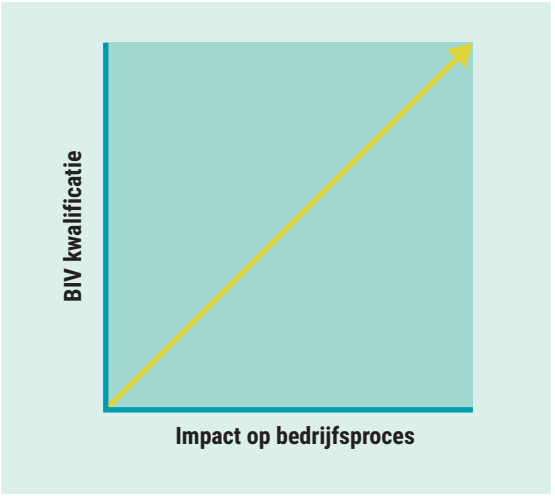
De impact van een verstoring kan gerelateerd worden aan het informatie beveiligingsmodel BIV (of CIA); de impact op de beschikbaarheid, integriteit en vertrouwelijkheid van een systeem.

- **Beschikbaarheid**—Beschikbaarheid is meestal aangetast als een verstoring zich voordoet. Dit houdt in storingen die duiden op (ongeplande) uitval van systemen waardoor ze niet gebruikt kunnen worden.
- **Vertrouwelijkheid**—Naast beschikbaarheid is het ontvreemden of ongeoorloofd toegang verschaffen tot data een veelvoorkomend incident met een negatieve impact voor de afnemer van de dienst.
- **Integriteit**—Data kan worden gemanipuleerd. Er is geen duidelijk onderscheid in de hiervoor genoemde onderzoeken naar incidenten waarbij data wordt/is gemanipuleerd in de cloud, dit is echter zeker een risico.

Als incidenten zich voordoen bij een dienstverlener hoeven deze dus niet direct een grote impact te hebben op alle afnemers in gelijke mate. Dit is waarschijnlijk ook de reden dat het onderzoek van BCI laat zien dat in de helft van de gevallen de schade minder is dan 50.000 euro, en de andere helft daarboven, reikend naar verliezen van boven de 500 miljoen.[10]

Om de impact te beoordelen zou de waarde van de afgenomen dienst gewaardeerd moeten worden. Hiervoor heeft NIST de Special Publication (SP) standaard FIPS 800-30[11] uitgegeven. Deze standaard benoemd een impactanalyse aan de hand van de BIV-kwalificatie. Het risico dat een incident een (significante) negatieve impact heeft op een organisatie neemt dus toe naarmate de BIV-kwalificatie hoger is (**afbeelding 4**).

Afbeelding 4—Invloed van BIV-kwalificatie op Impact



Om de afweging te maken welke middelen noodzakelijk zijn om de risico's te adresseren zal eerst een impactanalyse gemaakt moeten worden. Als een incident geen significante verstoring heeft op personen of op (kritische) bedrijfsprocessen, zijn mitigerende maatregelen wellicht onnodig.

Terugkrijgen van controle op de leverancier

Er zijn verscheidene manieren om organisaties te toetsen op de volwassenheid in het beheersen van de risico's. Het opvragen van derdenverklaringen en het laten uitvoeren van een self-assessment zijn veelvoorkomende toetsen. Een aantal organisaties hebben frameworks ter beoordeling van leveranciers ontworpen, zoals het Cloud Security Alliance en ISACA. CSA heeft een 'CSA STAR Level and Scheme Requirements'[12] waarbij er onderscheid wordt gemaakt tussen drie levels van assurance. Het laagste level van assurance wordt gegenereerd met self-assessments. Het tweede level van assurance wordt verkregen in de vorm van derdenverklaringen en het derde level van assurance wordt verkregen door middel van continue auditing.

Een *ISACA® Journal* artikel 'Vendor Risk Management Demystified'[13] noemt ook een framework met drie levels gerangschikt op de mate van assurance. Als laagste level wordt vendor self-assessments genoemd. Het tweede level bestaat uit een desktop-review en infrastructuurassessments en verschaft

meer assurance. Het hoogste level, een onsite-review en een infrastructuur- en applicatieassessment verschaft de meeste assurance.

Er zijn een aantal middelen die gebruikt kunnen worden om het vertrouwen in de leverancier te toetsen:

- Certificering van standaarden of raamwerken, zoals ISO 27001, Uptime Tier IV, TIA-942 en PCI-DSS
- Self-assessments – Een vragenlijst voor de leverancier, gebaseerd op standaarden en raamwerken zoals ISO 27001, Trust Service-principes en CSA
- Derdenverklaringen type II die toetsen over de werking van maatregelen over een periode aan de hand van erkende standaarden of raamwerken zoals ISAE 3402/SSAE 16 en SOC-rapporten
- Continue monitoring van maatregelen waarbij er direct inzicht is in de werking van de control-omgeving en veiligheidsmaatregelen van een organisatie

Alle genoemde middelen kunnen overlappend zijn. Het is echter niet per definitie zo dat een derdenverklaring type II beter is dan een certificering. Een SOC 2 type II-rapport (derdenverklaring type II) met betrekking tot beschikbaarheid zal vaak algemene maatregelen in helikopterview bekijken. Daarentegen zal een certificering als Uptime Tier III dieper ingaan op technische aspecten. Wanneer wordt gekeken naar een datacenter, is het voordeel van een Uptime Tier Facility certificaat dat er een meer grondige audit is uitgevoerd op de technische aspecten die de technische beschikbaarheid waarborgen, terwijl het voordeel van een SOC 2 type II-rapport is dat het zekerheid geeft op de operationele werking van geïmplementeerde controls door de organisatie. Een combinatie van beide geeft assurance over een bepaalde periode en verzekert dat onafhankelijke professionals een robuuste review en verschillende testen hebben uitgevoerd die verzekeren dat de technische infrastructuur de beschikbaarheid biedt.

Naast de diepte waarin maatregelen worden getoetst moet ook de onafhankelijkheid van de instantie en de beoordelende personen meegenomen worden voor de mate waarin de beoordeling te vertrouwen is. Een onafhankelijk bureau met professionals die zich moeten houden aan beroepsregels zal een hogere mate van zekerheid geven in de beoordeling van maatregelen dan een interne audit-afdeling die de eigen organisatie toetst.

Best Practices voor leveranciersbeoordeling

Naarmate de impact van een risico groter wordt, wordt er meer zekerheid verlangt van de volwassenheid van de control-omgeving van een leverancier. Naarmate de BIV-kwalificatie toeneemt (hoe belangrijker de beschikbaarheid, integriteit en vertrouwelijkheid voor het uitvoeren van de bedrijfsprocessen worden), moet de assurance op de leverancier ook toenemen.

BIV-kwalificatie
De BIV-kwalificatie bestaat uit drie factoren (beschikbaarheid, integriteit en vertrouwelijkheid) die geclassificeerd kunnen worden als laag, midden en hoog. Omdat we met risico's te maken hebben die de impact op de organisatie aanduiden, kan niet een gemiddelde genomen worden van de drie kwalificaties. Bijvoorbeeld, een dienst die bedrijfsprocessen ondersteunt waarbij beschikbaarheid 'uitermate belangrijk' is, maar de vertrouwelijkheid van de data die wordt verwerkt 'redelijk belangrijk' is en impact op de integriteit 'redelijk belangrijk' is, zou op een gemiddelde uitkomen van een midden-classificatie; echter de impact op bedrijfsprocessen kan even groot zijn als een dienst waarbij twee van de drie factoren ingeschaald worden op hoog. Hierom dient als algemene BIV-kwalificatie de hoogste geclassificeerde factor gebruikt te worden.

Certificeringen
Aan de hand van beoordeling van de individuele BIV-componenten, zou specifieke certificering gewenst kunnen zijn. Voor beschikbaarheid zou een Uptime Tier, TIA-942 of TSI-certificering aangeraden kunnen worden. Bij integriteit en vertrouwelijkheid zou een ISO 27001 of PCI-certificering aangeraden kunnen worden.

Naast de certificering an sich, kunnen ook eisen gesteld worden aan het certificaat zelf. Bijvoorbeeld, is het certificaat uitgegeven door een net gestarte eenmanszaak of een ervaren auditorganisatie? De omvang van het certificaat (welke processen/bedrijfsonderdelen zijn geaudit?) en gradaties van certificering (zoals meerdere gradaties van Tiers bij Uptime Institute en verschillende PCI-security-standaarden) zullen ook in overweging moeten worden genomen.

Self-assessments, derdenverklaringen type II en continue monitoring

Self-assessments, derdenverklaringen type II en continue monitoring geven veelal een meer overkoepelend inzicht in hoeverre een organisatie in-control is. Ook kunnen ze toegespitst worden op de toepasselijkheid van de wensen en eisen van de afnemer. De betrouwbaarheid van de informatie is veelal gerelateerd aan de frequentie van de toetsing en de onafhankelijkheid van de uitvoerende instantie en personen. Als voorbeeld, een jaarlijkse self-assessment rapportage van de eigen organisatie geeft minder zekerheid over hoe goed een organisatie in-control is, dan een derdenverklaring die elk half jaar wordt verstrekt.

Conclusie

Het auditen van leveranciers is noodzakelijk als (kritische) bedrijfsprocessen worden geoutsourcet. Verstoringen in de verlening van clouddiensten kunnen voorkomen, inclusief het niet beschikbaar zijn van het systeem voor een periode, en cybercriminaliteit wat vaak voorkomt. Afhankelijk van het type dienstverlening kunnen deze verstoringen een grote (financiële) impact hebben. De interne en externe auditoren moeten voor significante processen zorg dragen en toezien op een goede implementatie van monitoring van de dienstverlening.

Om voldoende grip te krijgen op leveranciers is het belangrijk leveranciers te toetsen. Hoe meer gedaan wordt om risico's te mitigeren, hoe kleiner de kans dat het risico zich voordoet. Naarmate de BIV-kwalificatie toeneemt zal meer aandacht nodig zijn. Een combinatie van assessments en certificering kan gebruikt worden voor de beoordeling van leveranciers. Het framework in **afbeelding 5** laat zien hoe de verschillende types van assessment en certificeringen te relateren zijn aan de BIV-kwalificatie.

Het type certificering zal verschillen per dienst. Bij het verwerken van transacties met betaalkaarten kan PCI-DSS benodigd zijn als de vertrouwelijkheids- en intregiteitsrisico's middel of hoog worden geacht. Bij het selecteren van een datacenter voor kritische diensten waarbij beschikbaarheidsrisico's hoog worden geacht kan een Uptime Institute Tier IV-certificaat worden verwacht.

Dit framework kan ook uitgebreid worden als er een noodzaak is om te voldoen aan wet- en regelgeving zoals de Algemene Verordening Gegevensbescherming (AVG) of California Consumer Privacy Act (CCPA). Een extra kolom voor Persoonlijk Identificeerbare Informatie (PII) kan toegevoegd worden en specifieke certificaten of contractuele verplichtingen kunnen worden geëist.

Eindnoot

1 Business Continuity Institute (BCI), *BCI Supply Chain Resilience Report 2019*, United Kingdom, 5 November 2019, *https://www.thebci.org/resource/bci-supply-chain-resilience-report-2019.html*

2 Uptime Institute, *Publicly Reported Outages 2018-19*, USA, March 2019, *https://uptimeinstitute.com/publicly-reported-outages-2018-19*

Afbeelding 5—Rancier Assessment Framework

BIV-kwalificatie	Middel assessment	Middel certificering per BIV		
		Beschikbaarheid	Integriteit	Vertrouwelijkheid
Laag	Self-assessment	Certificeringen worden belangrijker naarmate BIV-kwalificatie toeneemt. Specifieke certificering afhankelijk van de dienst		
Middel	Derdenverklaring type II			
Hoog	Continue monitoring en derdenverklaring type II			

3 (ISC)², *2019 Cloud Security Report*, August 2019, *https://www.cybersecurity-insiders.com/portfolio/2019-cloud-security-report-isc2/*
4 Microsoft Azure, "Azure Status History", *https://status.azure.com/en-us/status/history/*
5 Google Cloud, "Google Cloud Status Dashboard", *https://status.cloud.google.com/summary*
6 Amazon Web Services (AWS), "AWS Post-Event Summaries", *https://aws.amazon.com/premiumsupport/technology/pes/*
7 *Op cit* BCI
8 *Op cit* (ISC)²
9 *Op cit* Uptime Institute
10 *Op cit* BCI
11 National Institute of Standards and Technologies (NIST), NIST Special Publication (SP) 800-30, *Guide for Conducting Risk Assessments*, USA, February 2012, *https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf*
12 Cloud Security Alliance (CSA), STAR Level and Scheme Requirements, 4 September 2019, *https://cloudsecurityalliance.org/artifacts/star-level-and-scheme-requirements/*
13 Patel, D.; "Vendor Risk Management Demystified," *ISACA® Journal*, vol. 4, 2015, *https://www.isaca.org/archives*