Toenemende impact van dreigingen in de leverancierssketen

Ketenafhankelijkheden

24 december 2021

Stan van Bommel en Rob Augustinus

(Publicatiedatum: 24 december 2021)

Deze bijdrage geeft aan hoe de IT-auditor kan omgaan met de steeds grotere impact van actuele dreigingen in de leverancierssketen. Hacks via leveranciers – denk aan Solarwinds, voorjaar 2021 – onderstrepen de ernst hiervan. Wat daar nog bij komt is de trend dat cybercriminelen steeds vaker bedrijfsnetwerken binnenkomen via standaardpakketten en wijdverbreide systeemsoftware. Denk aan de recente Log4j-kwetsbaarheid.

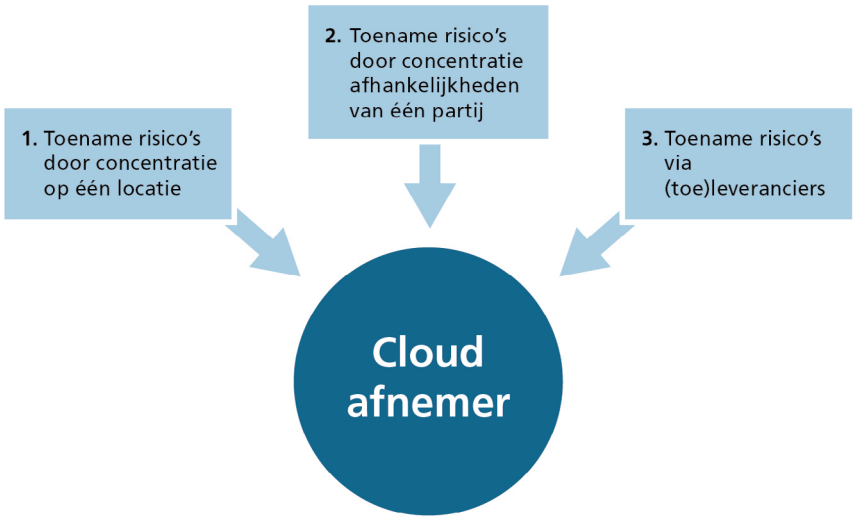
Deze dreigingen komen zowel uit het digitale als het fysieke domein. Door de coronapandemie vond een versnelling van digitalisering plaats en clouddiensten vormen nu het fundament onder allerlei digitale activiteiten. Hoewel bedrijven vertrouwen op hun cloudoplossing, brengt uitbesteding van IT-diensten specifieke dreigingen met zich mee. De toename in het aantal leveranciers van een bedrijf vergroot bijvoorbeeld het aantal aanvalsmogelijkheden van kwaadwillenden. Soms krijgt een kwaadwillende door het binnendringen bij één leverancier toegang tot duizenden bedrijven. Fysieke dreigingen ontstaan doordat datacenters waar de clouddiensten draaien steeds vaker zijn geconcentreerd in specifieke regio's en bovendien worden ze steeds groter. Zowel bedrijven als hun klanten dienen in deze gevallen rekening te houden met externe non-cyberdreigingen als gevolg van stroomstoringen, extreem weer en brand.

Bedrijven hanteren steeds vaker een *cloud native*-strategie. Hierbij besteden bedrijven complete processen of diensten uit. Leveranciers van clouddiensten spelen in op deze vraag. Zij worden steeds groter en breiden hun diensten uit, eventueel met behulp van toeleveranciers. Deze keten van leveranciers en toeleveranciers concentreert zich in specifieke regio's die technologische voordelen bieden, bijvoorbeeld dicht bij een *internet exchange*. [MILT20] Op basis van deze ontwikkelingen onderkennen de auteurs een toename van dreigingen doordat:

1. meerdere bedrijven in één locatie zijn gevestigd;
2. een organisatie (onbewust) meerdere diensten bij één leverancier afneemt;
3. aanvallen via (toe)leveranciers plaatsvinden.

Deze dreigingen worden gedreven door de laatste uitbestedingstrends. Om inzicht te krijgen in de risico's die voortkomen uit deze dreigingen en hoe deze beheerst kunnen worden, dient de IT-auditor meer te onderzoeken dan alleen de informatie-infrastructuur. [MATT16].

Figuur 1 geeft de risico's schematisch weer. In de volgende paragrafen worden deze dreigingen eerst verder uitgewerkt. Hieruit zal blijken dat het steeds belangrijker wordt om een gedegen inzicht te krijgen in de fysieke locaties en technische omgevingen van de leveranciersketen van een bedrijf. Vervolgens geven wij een handreiking om de technische architectuur van de leveranciersketen in kaart te brengen.

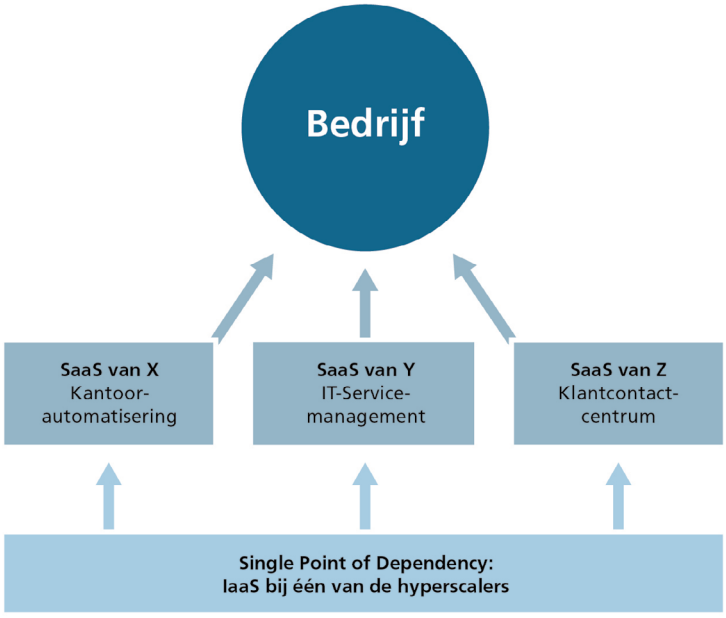


Dreiging 1: Toename risico's doordat meerdere leveranciers in één gebied zijn gevestigd

Sommige steden hebben een enorme aantrekkingskracht op datacenters. Voorbeelden van dergelijke digitale hubs zijn steden zoals Frankfurt, Parijs en Londen. Ook Amsterdam behoort tot de regio's met de meeste datacenters ter wereld. Wanneer veel datacenters dicht bij elkaar in de buurt zijn gevestigd – in Nederland is dat onder meer het geval in de Watergraafsmeer en op Schiphol-Rijk – ontstaan er clustereffecten die de individuele datacenters overstijgen. Ook wordt stroomvoorziening naar het gebied kritisch of is sprake van collectieve dreiging. In bijzondere gevallen kunnen datacenters bij uitval zorgen voor cascade-effecten waardoor ook andere datacenters geraakt worden in hun functioneren. [STRA21] Zo legde een brand bij één datacenter in Frankrijk begin dit jaar ook drie andere datacenters op dezelfde locatie stil. [HUIJ21] Deze voorbeelden schetsten de dreigingen bij een grote concentratie van datacenters in een gebied, maar dit kan natuurlijk ook gelden voor leveranciers die andere diensten aanbieden.

Dreiging 2: Toename risico's doordat een organisatie (onbewust) meerdere diensten bij één leverancier afneemt

Cloudleveranciers, die hun diensten aanbieden in de vorm van Software as a Service (SaaS), maken op hun beurt graag gebruik van de infrastructuurservices van bekende techreuzen als toeleveranciers van een *Infrastructure as a Service* (IaaS) om hun softwareapplicaties te hosten. De groei in de cloudmarkt gaat dan ook grotendeels naar de zogeheten *hyperscalers*: Amazon, Microsoft en Google. [GILS21b] Bedrijven kunnen bij gebrek aan inzicht in toeleveranciers onbewust meer afhankelijk zijn van een specifieke cloudleverancier – bijvoorbeeld een hyperscaler – dan ze in eerste instantie denken. SaaS-diensten die een bedrijf betrekt van verschillende leveranciers kunnen gebruikmaken van een grote IaaS-leverancier. Zulke leveranciers blijven vaak 'onder de radar' maar pas als ze wegvallen blijkt dat een groot aantal andere partijen daardoor wordt geraakt. Hierbij kan men spreken van *Single Points of Dependency* (SPOD). [TNO21] Een voorbeeld hiervan is te zien in afbeelding 2. Een bedrijf neemt SaaS-diensten af bij verschillende cloudleveranciers, maar al deze leveranciers hebben hun SaaS-dienst draaien op de IT-infrastructuur van een specifieke IaaS-cloudleverancier. Uitval van een dienst bij de IaaS-leverancier veroorzaakt ook uitval van alle daarvan afhankelijke SaaS-diensten. Een andere trend is 'verticale ketenintegratie'. Dat wil zeggen dat leveranciers steeds meer verschillende diensten aanbieden binnen dezelfde bedrijfskolom: van telecommunicatie tot datacenter. Ook hierdoor worden afnemers steeds vaker afhankelijk van één leverancier. Sommige leveranciers worden namelijk *too big to fail*. Ze mogen onder geen beding omvallen omdat bedrijven zo afhankelijk van hen zijn en er geen alternatief is.



Figuur 2: Onbewust afhankelijk van dezelfde toeleverancier

Dreiging 3: Toename risico's doordat aanvallen via (toe)leveranciers plaatsvinden

Hackers vallen bedrijven steeds vaker aan via hun ICT-leveranciers. Deze ontwikkeling gaat zo snel, dat zelfs wordt verwacht dat in 2021 het aantal aanvallen vier keer zo hoog zal eindigen als in 2020. [ENIS21] Deze *supply chain*-aanvallen richten zich op het verspreiden van malware of op spionage. Hierbij gebruikt de aanvaller het principe van de ketting die zo sterk is als de zwakste schakel. De aanvaller zoekt naar zwakheden in de beveiliging van leveranciers en toeleveranciers van zijn target. Denk aan het compromitteren van softwarecode om malware toe te voegen, het uitvoeren van aanvallen op zwakheden in de software of hardware en dat een hacker zich voordoet als leverancier. [GILS21], [MONT21]

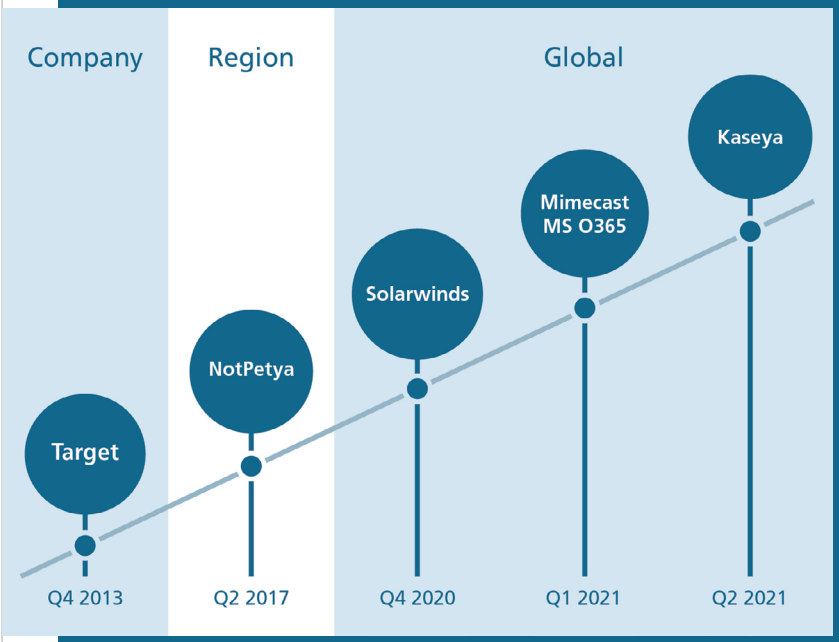
Een overzicht van vijf beruchte digitale supply chain-aanvallen tot dusver laat zien dat de aanvallen een steeds grotere reikwijdte krijgen (zie tekstkader 'Vijf beruchte digitale supply chain-aanvallen'.

Vijf beruchte digitale supply chain-aanvallen

1. **Target supermarkten in de VS.** Inbraak in het netwerk van de supermarktketen Target met behulp van netwerkreferenties die waren gestolen van een leverancier van koelapparatuur. [MELL14]
2. **Ukraine NotPetya.** In 2017 werden de regering, financiële instellingen en energiebedrijven in Oekraïne getroffen door de NotPetya-ransomware. Deze was primair gericht op bedrijven in Oekraïne maar ook bedrijven in andere landen werden zwaar getroffen, bijvoorbeeld het containervervoerbedrijf Maersk. Volgens beveiligingsexperts is de aanval afkomstig van een update van Oekraïense boekhoudsoftware genaamd MeDoc. Het automatische updatesysteem van de MeDoc software werd gecompromitteerd en gebruikt om malware te downloaden en uit te voeren in plaats van updates voor de software. [IDAG17]
3. **SolarWinds.** Eind 2020 bleek dat duizenden organisaties slachtoffer waren van een supply chain-aanval via de software van SolarWinds. Dit bedrijf levert software voor het monitoren van IT-omgevingen. Aanvallers wisten via een backdoor updates aan Solarwinds-software toe te voegen, waardoor ze toegang kregen tot de systemen van de getroffen organisaties. [WILL20]

4. **Mimecast/MS 365.** Begin 2021 werd bekend dat een certificaat van e-mailbeveiligingsbedrijf Mimecast door aanvallers is gebruikt voor het aanvallen van Microsoft 365-accounts bij klanten. Het door Mimecast uitgegeven certificaat wordt door bedrijven gebruikt om een beveiligde verbinding tussen de Mimecast-diensten en Microsoft 365 Exchange mogelijk te maken. Microsoft ontdekte dat dit certificaat door aanvallers was gecompromitteerd en waarschuwde het securitybedrijf. Het gecompromitteerde certificaat was gebruikt om toegang tot de Microsoft 365-accounts van klanten te krijgen. [SECU21]
5. **Kaseya.** Kaseya is een bedrijf dat een tool levert om software op afstand te beheren. In juli 2021 werd Kaseya gehackt, waardoor hackers via Kaseya bedrijven wisten te infecteren met malware. De aanval op Kaseya richt zich op de supply chain, maar dan twee lagen diep in plaats van slechts één. Niet alleen directe klanten van Kaseya werden getroffen, ook klanten van die klanten. Daarmee is een domino-effect ontstaan dat nooit eerder was gezien. [WHIT21]

De voorgenoemde aanvallen en hun impact zijn schematisch weergegeven in figuur 3.



Figuur 3: Schematische weergave van vijf beruchte digitale supply chain-aanvallen en hun reikwijdte

Handreiking om inzicht in de afhankelijkheden en dreigingen van de leveranciersketen te krijgen

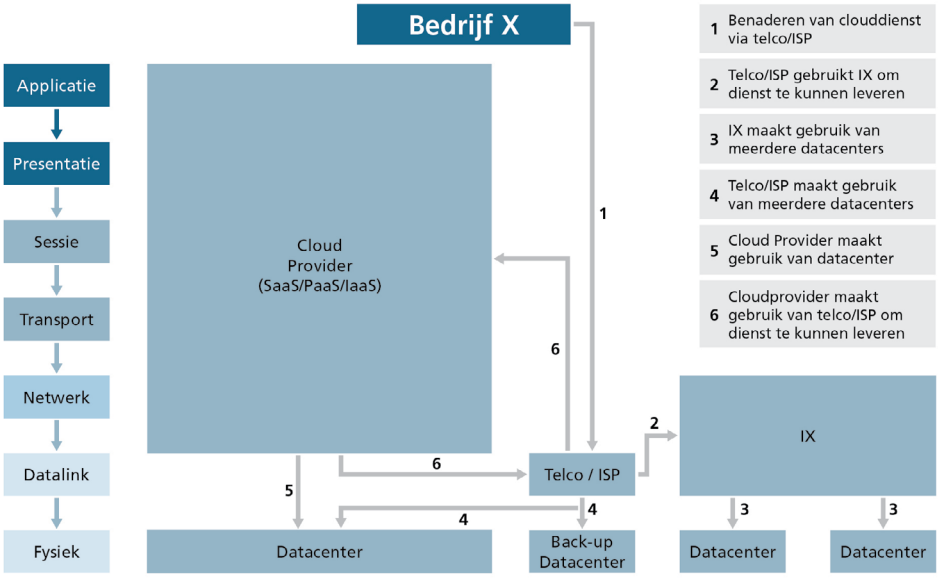
Vanuit een risicogebaseerde aanpak kan het noodzakelijk zijn dat IT-auditors zich verdiepen in de afhankelijkheden en de daarmee samenhangende dreigingen in de leveranciersketen. Hierbij dient het ecosysteem van een leveranciersketen in kaart gebracht te worden. Om inzicht te krijgen in de technische architectuur van een leveranciersketen kunnen verschillende modellen worden gebruikt die verschillende views bieden. Hieronder lichten wij enkele mogelijke views per dreiging toe.

1. Dreiging: Toename risico's doordat meerdere bedrijven in één gebied zijn gevestigd. In dit geval is een overzicht wenselijk van de fysieke locaties en geografische spreiding van leveranciers, bijvoorbeeld leveranciers onderaan de keten waar allerlei diensten samenkomen, zoals datacenters. Daarbij dient gekeken te worden naar mogelijke cascade-effecten waardoor andere leveranciers geraakt worden in hun functioneren.
2. Dreiging: Toename risico's doordat een organisatie (onbewust) meerdere diensten bij één leverancier afneemt. In dit geval is inzicht gewenst in de relaties tussen leverancier en toeleveranciers. Per leverancier is vervolgens inzicht nodig in de diensten die afgenomen worden, zodat de SPOD's kunnen worden geïdentificeerd.
3. Dreiging: Toename risico's doordat aanvallen via (toe)leveranciers plaatsvinden. Voor dit type cyberdreigingen is inzicht gewenst in het aanvalsvlak dat bepaalde leveranciers bieden voor potentiële aanvallers. Bijvoorbeeld wanneer de software van een leverancier op veel verschillende plekken en processen binnen een bedrijf gebruikt wordt of wanneer deze toegang biedt tot belangrijke bedrijfsprocessen of informatie. De gebruikte software per leverancier en de bijbehorende mogelijke impact van *vulnerabilities* dienen daarbij in kaart gebracht te worden.

Een van de manieren om de eerste twee dreigingen in kaart te brengen is via het OSI-model. [WIKI21] Dit model geeft de relaties weer vanuit het perspectief van datatransport en verbindingen en geeft een basisoverzicht. Figuur 4 bevat een voorbeeld van een leveranciersketen op abstract niveau. Door de details van alle uitbestede processen in een model op te nemen en aan te vullen met leveranciers- en locatiegegevens ontstaat een volledig en diepgaand inzicht in de samenhang van de totale leveranciersketen. Dit totaaloverzicht geeft zowel inzicht in de afzonderlijke leveranciers als de samenhang tussen hun toeleveranciers. Voor meer inspiratie verwijzen we naar het analysekader in een onderzoek van TNO dat in opdracht van NCSC is uitgevoerd. [BRIN21]

De derde dreiging is misschien wel het lastigst in kaart te brengen en te beheersen. Hierbij dient gekeken te worden of diensten dan wel software van een leverancier op veel plekken of processen binnen een bedrijf voorkomen. Ook is het zaak na te gaan of ze toegang bieden tot belangrijke bedrijfsprocessen of informatie. Impact van de vulnerabilities in de diensten van de software of diensten van deze leveranciers dient onderzocht te worden.

Daarnaast dient men inzicht in het vulnerability management-proces van de betreffende leverancier te hebben, dit kan onder andere worden verkregen door middel van assurance verklaringen – bijvoorbeeld ISAE3402.



Figuur 4: Voorbeeld van de leveranciersketen van bedrijf X op abstract niveau.

Tot slot

Dit artikel beschrijft de steeds grotere impact van drie actuele dreigingen binnen de IT-leveranciersketen die voor de IT-auditor aanleiding kunnen zijn om ketenafhankelijkheden op de auditagenda te zetten. De toenemende impact van de dreigingen wordt gedreven doordat het aantal leveranciers in één gebied groeit, doordat leveranciers steeds meer diensten aanbieden en door een toename in aanvallen via (toe)leveranciers. Om inzicht te krijgen in de risico's die voortkomen uit deze dreigingen dient de IT-auditor gedetailleerd het complexe ecosysteem van leveranciers, toeleveranciers en de samenhang en onderlinge afhankelijkheden hiertussen in kaart te brengen. Vervolgens dient bekeken te worden of deze risico's meegenomen zijn in het risicomanagementproces van het bedrijf dat diensten van deze leveranciers afneemt. Modellen zoals het OSI-model kunnen hierbij een hulpmiddel bieden. Wij zijn benieuwd welke andere modellen door IT-auditors worden gebruikt, en reacties zijn dan ook van harte welkom (zie mailadressen in cv-blok onder dit artikel). Door in ieder geval nu al aandacht te besteden aan deze dreigingen binnen de leveranciersketen, speelt de IT-auditor tijdig in op actuele trends en ontwikkelingen.

Literatuur

[BRIN21] Brink, P.E. van den, H.L. van Duijnhoven, I.N. Melman, B. Poppink, A.C.M. Smulders, *Vraagstukken en perspectieven voor ICT SCRM – een initiële verkenning,* februari 2021, https://www.ncsc.nl/onderzoek/onderzoeksresultaten/grote-verschillen-in-benadering-risico%E2%80%99s-ict-supply-chains-bij-nederlandse-organisaties, geraadpleegd op 14 september 2021.

[ENIS21] European Union Agency for Cybersecurity (ENISA), *ENISA threat landscape for supply chain attacks,* juli 2021, https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks, geraadpleegd op 14 september 2021.

[GILS21a] Gils, S., *Cyberaanval via leverancier vormt nieuwe bedreiging voor bedrijven,* 28-02-2021, https://fd.nl/futures/1374887/cyberaanval-via-leverancier-vormt-nieuwe-bedreiging-voor-bedrijven-kni1caCOAioP, geraadpleegd op 14 september 2021.

[GILS21b] Gils, S., *Cloudbedrijf Leaseweb rekent op miljardensteun in strijd tegen techreuzen*, 27-06-2021, https://fd.nl/futures/1388570/cloudbedrijf-leaseweb-rekent-op-miljardensteun-in-strijd-tegen-techreuzen-kni1caCOAioP, geraadpleegd op 14 september 2021.

[HUIJ21] Huijbregts, J., *Brand verwoest datacenter van Franse provider OVHcloud,* 10-03-201, https://tweakers.net/nieuws/179030/brand-verwoest-datacenter-van-franse-provider-ovhcloud.html, geraadpleegd op 14 september 2021.

[IDAG17] ID AGENT, *NotPetya – a Threat to Supply Chains*, 03-08-2017, https://www.idagent.com/blog/2017-08-03-notpetya-threat-supply-chains-across-ukraine/, geraadpleegd op 14 september 2021.

[MATT16] Matthijsse, R., *Informatiemanagement en control in een ketenomgeving,* 27-12-2016], https://www.deitauditor.nl/informatiemanagement/informatiemanagement-en-control-in-een-ketenomgeving/, geraadpleegd op 14 september 2021.

[MELL14] Mello, J.P., T*arget Fiasco Shines Light on Supply Chain Attacks*, 03-02-2014, https://www.technewsworld.com/story/target-fiasco-shines-light-on-supply-chain-attacks-79908.html, geraadpleegd op 14 september 2021.

[MILT20] Miltenburg, O. van, *Hoeveel datacenters kunnen we aan?*, 14-05-2020, https://tweakers.net/reviews/7722/hoeveel-datacenters-kan-nederland-aan.html, geraadpleegd op 14 september 2021.

[MONT21] Monterie, A., *Microsoft waarschuwt voor virtuele wereldramp*, 13-01-2021, https://www.computable.nl/artikel/nieuws/security/7122024/250449/microsoft-waarschuwt-voor-virtuele-wereldramp.html?utm_source=computable.nl&utm_medium=email&utm_campaign=dagelijkse_update&utm_content=topartikelen, geraadpleegd op 14 september 2021.

[TNO21] TNO, *ICT supply chain risk management – perspectieven, analysekader en toepassingen*, presentatie 13-07-2021.

[STRA21] Stratix/EZK Onderzoeksrapport Datacenters Vitaal? https://www.rijksoverheid.nl/documenten/rapporten/2020/12/10/datacenters-vitaal, geraadpleegd op 23 november 2021.

[SECU21] Security.nl, *Mimecast-certificaat gebruikt bij aanval op Microsoft 365-accounts,* https://www.security.nl/posting/685744/Mimecast-certificaat+gebruikt+bij+aanval+op+Microsoft+365-accounts geraadpleegd op 14 september 2021.

[WHIT21] Whitney, L., *Kaseya supply chain attack impacts more than 1,000 companies,*

06-07-2021, https://www.techrepublic.com/article/kaseya-supply-chain-attack-impacts-more-than-1000-companies/, geraadpleegd op 14 september 2021.
[WIKI21] Wikipedia, *OSI-model*, 29-07-2021, https://nl.wikipedia.org/wiki/OSI-model, geraadpleegd op 14 september 2021.
[WILL20] Williams, J., *What You Need to Know About the SolarWinds Supply-Chain Attack*, 15-12-2020, https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/, geraadpleegd op 14 september 2021.

C.F. (Stan) van Bommel RE CISM | specialistisch inspecteur bij *Agentschap Telecom in Amersfoort*

Stan vervult vanuit de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) een toezichtsrol op de energiesector en op organisaties die de digitale infrastructuur verzorgen. Hij heeft meerdere jaren ervaring als IT-auditor en Security Officer.

Contact: stan.vbommel@agentschaptelecom.nl

R.W.M. (Rob) Augustinus CISSP | specialistisch inspecteur bij *Agentschap Telecom te Amersfoort*

Rob vervult vanuit de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) een toezichtsrol op organisaties die de digitale infrastructuur verzorgen en op digital service providers. Hij heeft meerdere jaren ervaring in de informatiebeveiliging als onder andere Security Officer en IT Security Architect.

Contact: rob.augustinus@agentschaptelecom.nl