Auteurs: Puck van den Brink, Hanneke Duijnhoven, Ignas Melman, Bram Poppink en André Smulders zijn werkzaam bij TNO, unit Defensie en Veiligheid & unit ICT. Voor vragen is Puck van den Brink te bereiken via puck.vandenbrink@tno.nl.

ICT-supply chain risicomanagement: een veelzijdig vraagstuk

TNO doet onderzoek naar ICT-supply chain risicomanagement binnen de meerjarige onderzoeksagenda van het NCSC. Dit artikel is gebaseerd op een eerste verkenning in 2020 en gaat in op de complexiteit van het vraagstuk. Er worden vijf perspectieven beschreven om de risico's die samenhangen met ICT-supply chains beter te duiden. Deze eerste stap is een opmaat voor vervolgonderzoek naar het vergroten van het handelingsperspectief op dit thema voor overheid en bedrijfsleven.

Organisaties zijn voor de continuïteit en veiligheid van hun bedrijfsvoering in toenemende mate afhankelijk van een netwerk van ICT-aanbieders en -gebruikers, wat het aanvalsoppervlak voor cyberaanvallen met keteneffecten via derde partijen vergroot (1), (2), (3), (4). Naar schatting vindt zo'n 80% van de cyberaanvallen wereldwijd plaats via de supply chain (5). Bekende voorbeelden van ICT-supply chain incidenten zijn de ontdekte kwetsbaarheden in de systemen van Citrix (2019), waarbij een groot aantal organisaties wereldwijd – in Nederland naar schatting zo'n 3700 organisaties (6) – risico liepen om gehackt te worden en (vergaande) maatregelen moesten treffen. Ook het incident NotPetya (2018) zorgde ervoor dat via veelgebruikte administratiesoftware een wiperware zich kon verspreiden over een groot aantal organisaties wereldwijd (7). De LockerGoga ransomware aanvallen (2019) gericht op industriële controle systemen, hadden vergaande gevolgen op de logistieke en productieprocessen van de getroffen industriële organisaties (8). Deze gebeurtenissen zorgen voor steeds meer onzekerheid en zorgen over de risico's in de (digitale) supply chains en de weerbaarheid tegen deze risico's. In recente publicaties van onder andere de NCTV, de WRR, de Cyber Security Raad en het CBS wordt gewezen op de risico's die samenhangen met de steeds complexere, vaak grensoverschrijdende digitale supply chains waar wij als samenleving van afhankelijk zijn en de onzekerheid die heerst over de kennis en mate van grip die men heeft op deze risico's (6), (7), (9), (10), (11).

Omgaan met de verschillende typen risico's die voortkomen uit complexe digitale ketens vergt aandacht voor en begrip van verschillende aspecten en niveaus van de ICT-supply chain. Op basis van een verkenning naar bestaande ICT-supply chain risicomanagement methoden en gesprekken met verschillende grote organisaties onderscheiden we in dit artikel vooralsnog vijf perspectieven om naar ICT-supply chain risico's te kijken. We denken dat het onderscheiden van verschillende perspectieven kan helpen om meer grip te krijgen op ICT-supply chain risicomanagement, omdat het hanteren en bij elkaar brengen van meerdere perspectieven ervoor kan zorgen dat andere risico's of mogelijke aangrijpingspunten voor risicobeheersing in beeld komen.

Verschillende aspecten van de supply chain

Een supply chain is een systeem van organisaties, mensen, technologie, activiteiten, informatie en resources die nodig zijn om een product of dienst aan een eindgebruiker te leveren (1), (12). De verschillende aspecten in het supply chain 'systeem' bieden relevante invalshoeken om naar ICT-supply chain risico's te kijken. Met de vergaande digitalisering zijn dit in toenemende mate digitale aspecten. Een ICT-supply chain kan gaan om de productie van een ICT-product (bijvoorbeeld hardware, software of een informatiedienst), maar ook om de levering van producten of diensten die gerelateerd zijn aan deze ICT-producten, of die op basis van (de informatie uit) deze ICT-producten tot stand komen (12). Als je alleen al naar één organisatie kijkt is er dus niet zoiets als 'de' supply chain, maar is er sprake van vele verschillende ketens en relaties, waarbij de complexiteit wordt versterkt door de toenemende verwevenheid van fysieke en digitale aspecten (12). Als we grip willen krijgen op de kwetsbaarheden en risico's van de ICT-supply chains, is het dan ook van belang om naar al deze aspecten en relaties te kijken. Een eenzijdig perspectief kan er namelijk voor zorgen dat bepaalde risico's en kwetsbaarheden buiten beeld blijven of onderbelicht raken. Daarnaast is het ook van belang om naar de supply chain als geheel te kijken en de manier waarop deze samenhangt met andere supply chains op het niveau van de samenleving. Hierbij komen ook andere aspecten in beeld die van belang zijn voor het vergroten van de cybersecurity van supply chains, zoals wet- en regelgeving, het maatschappelijk belang van bepaalde supply chains voor de continuïteit van vitale processen en nationale veiligheidsvraagstukken. In dit artikel gaan we met name in op de supply chain zelf (de verschillende aspecten die een rol spelen bij het leveringsproces) om organisaties te helpen meer inzicht te krijgen in de risico's. Uiteindelijk zal dit ook aanknopingspunten bieden om op het niveau van de keten, het niveau van netwerken van ketens en de samenleving meer grip te krijgen op supply chain risico's.

Vijf perspectieven om naar ICT-supply chains te kijken

Wij zien ten minste vijf perspectieven op ICT-supply chains waarmee risico's gecategoriseerd kunnen worden. Het onderscheiden van deze perspectieven draagt bij aan het ontwikkelen van een integraal perspectief op supply chain risicomanagement omdat het de complexiteit van digitale ketens in kaart brengt. Hierdoor komen verschillende kwetsbaarheden en risico's in beeld en kunnen deze ook beter met elkaar in verband worden gezien. Hiermee ontstaan handvatten voor organisaties om hun (ICT) supply chain risicomanagement vorm te geven en aan te vullen.

1. Actorenperspectief

Wanneer men naar de ICT-supply chain kijkt vanuit het perspectief van actoren, kan men kijken naar het totaal aan organisaties (leveranciers, afnemers) dat betrokken is in een ICT-supply chain, om zo risico's in beeld te krijgen voor de continuïteit van het leveringsproces. Hierbij ligt de nadruk op het inzichtelijk krijgen in en afstemmen over de relaties tussen organisaties (afspraken tussen leverancier en afnemer, zicht op afhankelijkheden tussen verschillende leveranciers, etc.). De uitdaging hierbij is dat het afstemmen op het niveau van een keten alleen mogelijk is als de verschillende organisaties in die keten het belang daarvan voelen. Niet alle organisaties die bijdragen aan een supply chain zullen zichzelf nadrukkelijk zien als mede-eigenaar van het ketenbelang. Met name leveranciers die hun producten leveren aan heel veel verschillende partijen zullen het ketenbelang minder sterk voelen.

Een tweede manier om het actorenperspectief te hanteren is om vanuit één organisatie te kijken naar de verschillende ICT-toeleveringsketens waar de organisatie een rol in speelt (als afnemer, als leverancier, als dienstverlener, als toezichthouder, etc.). Voor elk van die rollen zal de organisatie op een andere manier maatregelen nemen. Als afnemer gaat het bijvoorbeeld om het maken van afspraken met de leveranciers (zoals SLAs). Als leverancier gaat het erom grip te krijgen op de risico's die tot gevolg kunnen hebben dat de organisatie haar afspraken met afnemers niet kan nakomen (13). Voor elke rol zijn andere aspecten van belang en komen er ook andere risico's in beeld. Een belangrijke uitdaging hier is om te prioriteren op welke ICT-supply chains men zich moet richten. De hoeveelheid aan ICT-supply chains waar één organisatie een rol in speelt is namelijk enorm. Het is dus vrijwel onmogelijk om alle ketens waar een organisatie een rol in speelt volledig in kaart te brengen. Om hier meer richting aan te geven kunnen ook de overige perspectieven een waardevolle rol spelen.

2. ICT-producten perspectief

Een andere manier om naar ICT-supply chain risico's te kijken is door te kijken vanuit de ICT-producten. Dit is het perspectief van hardware en software. Het gaat hierbij om de supply chains van ICT-producten variërend van een (relatief simpel) stuk software, zoals een telefoon, een autonoom functionerend voertuig of de automatische aansturing van operationele technologie (OT) voor vitale processen. In al deze producten komen verschillende systeemonderdelen samen vanuit verschillende leveranciers. Het kan zijn dat het product zelf (bijvoorbeeld in het geval van een softwarepakket) bij de afnemer weer wordt geïntegreerd of toegepast binnen een ander systeem. Bij het NotPetya incident (14) werd boekhoudsoftware vermoedelijk als aanvalsvector gebruikt om binnen te komen in een specifiek systeem. Maar omdat veel organisaties deze software gebruikten, werden zij meegesleept in een (geopolitiek) conflict waar ze niets mee te maken hadden. Deze organisaties namen een softwarepakket af van een leverancier zonder dat zij zicht hadden op de achterliggende leveranciers en de mogelijke risico's daarvan. Uit meerdere gesprekken komt naar voren dat het vaak een uitdaging is om inzicht en grip te krijgen op de keten van leveranciers achter een leverancier van een specifiek ICT-product. De vraag is dan ook in welke mate men zicht kan krijgen op wat er in de eigen organisatie aan ICT-producten wordt binnengehaald. Belangrijk hierbij is om zicht te hebben op de ICT-producten in de organisatie en de manier waarop zij bijdragen aan de bedrijfscontinuïteit van de organisatie. Welke producten zijn kritiek? Welke componenten horen er in het programma of systeem te zitten en wat zit er daadwerkelijk in?

3. Informatieperspectief

In het derde perspectief wordt vanuit de informatie naar een ICT-supply chain gekeken. In dit perspectief wordt gekeken naar welke informatiestromen en informatieproducten (die tot stand zijn gekomen door gebruik te maken van ICT-middelen) een rol spelen bij de toelevering van een product of dienst, of bij de ondersteuning van bedrijfsprocessen. Voorbeelden zijn de totstandkoming van rapportages van de kwaliteitscontroles die nodig zijn om de levering van een chemisch product te autoriseren, informatiestromen uit sensoren die van belang zijn bij de aansturing of controle van bepaalde OT, of het delen van klantgegevens met een bezorgdienst voor de levering van producten. Bij MAERSK werden veel systemen geraakt door de NotPetya wiperware, waardoor ook de informatievoorziening naar de klanten werd verstoord (15). Hierdoor werden ook organisaties geraakt die zelf niet geïnfecteerd waren omdat de informatie die zij voor hun processen nodig

Data is in toenemende mate niet meer in beheer van de eigen organisatie

hadden niet (volledig of tijdig) beschikbaar was. Een ander aspect van het informatieperspectief is de opslag en het gebruik van data. Data is in toenemende mate niet meer in beheer van de eigen organisatie, of meerdere organisaties maken gebruik van dezelfde data. Dit heeft als gevolg dat meerdere organisaties worden geraakt als zich een incident voordoet met deze data of de plek van opslag. Als bijvoorbeeld de patiënten data van een medisch laboratorium wordt gemanipuleerd, kunnen patiënten in ziekenhuizen vanwege onjuiste data de verkeerde behandeling krijgen (16). Hoe kan men achterhalen dat data is gemanipuleerd als deze data niet binnen de eigen organisatie wordt beheerd en hoe kan men hier op handelen? Door naar de belangrijke informatiestormen en producten te kijken.

4. ICT-diensten perspectief

In veel supply chains zullen ook ICT-diensten een rol spelen, niet alleen als onderdeel van het toeleveringsproces van een product of dienst, maar ook als eindproduct van een supply chain. ICT-diensten zijn diensten waar ICT-middelen voor nodig zijn om ze te kunnen gebruiken. Voorbeelden zijn telecomdiensten, clouddiensten of het leveren van remote onderhoud op systemen. Een voorbeeld van een supply chain incident waarbij ICT-diensten een grote rol speelden, is de DDoS aanval op de DNS provider Dyn in 2016 (17). Door de aanval op Dyn was voor een groot deel van Noord-Amerika de toegang tot het internet gedurende bijna een hele dag verstoord en veel verschillende diensten en platformen, zoals Spotify, waren daardoor niet beschikbaar. Binnen dit ICT-diensten perspectief is het feit dat heel veel organisaties afhankelijk zijn van een beperkt aantal grote ICT-dienstleveranciers een belangrijke uitdaging. Deze uitdaging geldt met name voor organisaties die van ICT-diensten afhankelijk zijn om hun bijdrage aan vitale processen te waarborgen. Denk aan de afhankelijkheid van een internet- of telecommunicatieleverancier of een leverancier van cloudopslag.

5. Productiemiddelen perspectief

Ten slotte spelen ook andere (niet-ICT-)producten of diensten een rol in ICT-supply chains die afhankelijk zijn van ICT-middelen. De bedrijfsprocessen waar deze productiemiddelen een rol in spelen hebben niet een directe koppeling met ICT-middelen, maar worden wel geleverd of aangestuurd met behulp van ICT-middelen. Denk aan een logistiek proces waarbij het transport zelf niet geautomatiseerd is, maar waarbij wel de logistieke planning met behulp van een ICT-middel wordt uitgevoerd. Om grip te krijgen op ICT-supply chain risico's is dit perspectief, samen met het informatieproducten perspectief, extra interessant omdat dit een blinde vlek kan zijn bij het identificeren van ICT-risico's, het gaat immers om risico's die niet direct gerelateerd zijn aan ICT. Het incident NotPetya en de verstoringen bij MAERSK laten zien dat het transport van fysieke goederen van andere organisaties ook stil kwam te liggen, terwijl de logistieke processen van deze organisaties in veel gevallen op geen enkele manier verbonden waren met de ICT-systemen van MAERSK (14). In dit perspectief ligt de nadruk op het in kaart brengen van producten en diensten waar bedrijfsprocessen van afhankelijk zijn en hoe die vervolgens afhankelijk zijn van andere (al dan niet ICT-) producten en diensten. Het zorgt ervoor dat niet uitsluitend naar ICT-afhankelijkheden wordt gekeken, waardoor bepaalde risico's buiten beeld zouden blijven.

Conclusie

Voor organisaties bieden de voorgaande perspectieven een bredere, meer integrale blik op ICT-supply chain risico's. Ze laten zien dat de veelzijdigheid van ICT-supply chains vraagt om een bredere blik waarmee risico's vanuit alle perspectieven inzichtelijk gemaakt kunnen worden en met elkaar gerelateerd kunnen worden. Dit inzicht kan ook aanknopingspunten bieden om bestaande ICT-supply chain risicomanagement aanpakken te versterken. Er zijn nog andere perspectieven denkbaar. Bijvoorbeeld het perspectief van de mens in ICT-supply chains (afhanke-

lijkheid van de mens (goed gebruik) of om te laten zien dat de ICT-supply chain tot daar doorloopt) of perspectieven op de manier waarop processen zijn ingericht en afgestemd in een supply chain (just-in time principes, tijdsdimensies van afhankelijkheden, redundantie die aanwezig is). Voor nu denken wij dat deze vijf een goed startpunt zijn om op een meer integrale manier naar ICT-supply chain risicomanagement te kijken. Ons onderzoek richt zich de komende tijd op het verder uitwerken van deze perspectieven en op het analyseren van supply chain risicomanagement aanpakken vanuit deze perspectieven. Het doel is om bij te dragen aan het ontwikkelen van handelingsperspectief voor het beter beheersen van ICT-supply chain risico's. Wij gaan hiervoor graag in gesprek met geïnteresseerden vanuit de overheid, het bedrijfsleven en andere onderzoeksinstituten. Daarbij dagen wij alle organisaties uit om de perspectieven die in dit artikel staan geschetst te gebruiken en om te kijken op welke punten dit een mogelijke aanvulling biedt op de huidige supply chain risicomanagement of bedrijfscontinuïteitsmanagement processen.

Referenties

(1) ENISA (2015). Supply Chain Integrity: An overview of the ICT-supply chain risks and challenges, and vision for the way forward. European Union Agency for Network and Information Security. https://www.enisa.europa.eu/publications/sci-2015

(2) AON (2019). Cyber Perils in a Growing Market. White paper. https://www.aon.com/unitedkingdom/insights/cyber-perils-in-a-growing-market.jsp

(3) Soare, B. (2020). Supply Chain Cyber Security: What are the Risks? Heimdal Security. https://heimdalsecurity.com/blog/supply-chain-cyber-security/

(4) Ghadge, A., Weiß, M., Caldwell, N.D. & Wilding, R. (2019). Managing cyber risk in supply chains: a review and research agenda. Supply Chain Management, Vol. 25 No. 2, pp. 223-240. https://doi.org/10.1108/SCM-10-2018-0357

(5) Boyens, J. (2016) in Bailey, D. (2018). Lumberjacks and Supply Chain Cybersecurity: Take Time to Prepare. Blogrige, The Offiial Baldrige Blog. https://www.nist.gov/blogs/blogrige/lumberjacks-and-supply-chain-cybersecurity-take-time-prepare

(6) NCTV (2020). Cybersecurity Beeld Nederland (CSBN) 2020. Den Haag: Ministerie van Justitie en Veiligheid. https://www.rijksoverheid.nl/documenten/rapporten/2020/06/29/tk-bijlage-2-cybersecuritybeeld-nederland-csbn-2020

(7) NCTV (2019). Cybersecurity Beeld Nederland (CSBN) 2019. Den Haag: Ministerie van Justitie en Veiligheid. https://www.rijksoverheid.nl/documenten/rapporten/2019/06/12/tk-bijlage-cybersecuritybeeld-nederland-csbn-2019

(8) Reich, J. (2020) Nearly 300 cybersecurity incidents impacted supply chain entities in 2019. TechRepublic. https://www.techrepublic.com/article/nearly-300-cybersecurity-incidents-impacted-supply-chain-entities-in-2019

(9) Wetenschappelijke Raad voor het Regeringsbeleid (2019). Voorbereiden op digitale ontwrichting. Den Haag. https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting

(10) Cyber Security Raad (2016). Digitale ketenveiligheid krijgt veel te weinig aandacht. https://www.cybersecurityraad.nl/010_Actueel/digitale-ketenveiligheid-krijgt-veel-te-weinig-aandacht.aspx

(11) CBS (2018). Cybersecuritymonitor 2018. Een verkenning van dreigingen, incidenten en maatregelen. Den Haag: CBS. https://www.cbs.nl/nl-nl/publicatie/2018/38/cybersecuritymonitor-2018

(12) Van Ruijven, T. & Keijser, B. (2017). Ketenweerbaarheid tegen cyberdreigingen. Whitepaper. Den Haag: TNO. https://www.tno.nl/nl/aandachtsgebieden/defensie-veiligheid/roadmaps/nationale-veiligheid/cybersecurity-het-belang-van-integrale-oplossingen/cybersecurity-ketens-en-processen-in-beeld/whitepaper-ketenweerbaarheid-tegen-cyberdreigingen/

(13) Joosten, H.J.M. & Smulders, A. (2014). Networked Risk Management: How to Sucessfully Manage Risks in Hyperconnected Value Networks. Delft: TNO.

(14) Crosignani, M., Macchiavelli, M. & Silva, A.F. (2020). Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains. Federal Reserve Bank of New York Staff Reports, no. 937. https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr937.pdf

(15) Greenberg, A. (2018) The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

(16) University of California - San Diego. (2018). How unsecured medical record systems and medical devices put patient lives at risk. ScienceDaily. https://www.sciencedaily.com/releases/2018/08/180829115554.html

(17) Johnson, K. (2019). What is digital supply chain management? Bitsight. https://www.bitsight.com/blog/what-is-digital-supply-chain-management#:~:text=The%20second%20definition%20%E2%80%94%20that%20the,coined%20in%20a%202001%20paper