Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Omgaan met risico's in de toeleveringsketen

Good practices van Nederlandse organisaties

Publicatiedatum: 15 augustus 2023

Toegestane verspreiding
TLP:CLEAR (Traffic Light Protocol)

Deze publicatie bevat het label TLP:CLEAR en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven op de website van het NCSC (https://www.ncsc.nl/onderwerpen/traffic-light-protocol)

Met TLP:CLEAR zijn er geen beperkingen om de informatie verder te delen.

Uw reacties zijn welkom op info@ncsc.nl

Inhoud

Introductie

Uitdagend. Dat is zicht en grip houden op cybersecurity risico's in de toeleveringsketen zeker. Maar hoe doe je dat? Producten en diensten bereiken Nederlandse organisaties immers vanuit de hele wereld. Deze internationale verwevenheid komt met kansen én risico's.

Onlangs sprak het NCSC met Nederlandse publieke en private organisaties over de vraag: "Hoe gaat u om met cybersecurity risico's uit uw toeleveringsketen?" Dit document geeft concrete handvatten als antwoord op die vraag.

Verschillende perspectieven en de gehanteerde definitie

Het NCSC heeft op 11 april 2023 een workshop uitgevoerd met afgevaardigden van publieke en private organisaties om *good practices*[1] ten aanzien van omgaan met risico's in de toeleveringsketen te delen.

De toeleveringsketen kan uit verschillende perspectieven worden bekeken. TNO heeft in opdracht van het NCSC deze verschillende perspectieven in kaart gebracht.[2]

Bij de workshop is de volgende definitie aangehouden*:* "Het potentieel voor schade of compromittatie dat kan voortvloeien uit leveranciers, hun toeleveringsketens, hun producten of hun diensten".[3]

Lessen uit Log4j

Toeleveringsketens zijn technisch complex en het is lastig om zicht te houden op afhankelijkheden. Dit bleek toen een ernstige kwetsbaarbaarheid werd gevonden in Log4j.

Log4j bleek het digitale equivalent van zout te zijn, het aantal applicaties waar Log4j-componenten in zaten bleek uitzonderlijk groot.[4] Kwetsbaarheden in Log4j werden vervolgens snel misbruikt door cybercriminelen en statelijke actoren.[5]

Geopolitieke ontwikkelingen

Ook geopolitieke ontwikkelingen kunnen zorgen voor nieuwe risico's in de toeleveringsketens van Nederlandse organisaties.

Zo kan een internationaal conflict invloed hebben op de veiligheid van een toeleveringsketen. Producten zijn mogelijk niet verkrijgbaar door sancties of exportrestricties, en ook kunnen internationale toeleveringsketens het doelwit worden van politiek gemotiveerde digitale aanvallen.[6]

Doelgroep

Dit document richt zich op CIO's, CISO's en risicomanagers die zicht en grip willen krijgen op risico's in de toeleveringsketen.

Totstandkoming

Dit document is tot stand komen in een workshop met de voorzitters en vicevoorzitters van de ISAC's[7] waarbij het NCSC betrokken is.

In deze workshop zijn door de deelnemers good practices ten aanzien van omgaan met risico's in de toeleveringsketen gedeeld. Het NCSC heeft de uitkomsten verrijkt en verwerkt in deze publicatie.

Overzicht

Zonder zicht op uw toeleveringsketen is het lastig om daadwerkelijk grip te krijgen. In dit hoofdstuk gaan we verder in op best practices die uw organisatie kunnen helpen inzichtelijk te krijgen wie uw toeleveranciers zijn en hoe uw organisatie daarvan afhankelijk is.

GP[8] 1.1: Zorg voor een actueel overzicht van uw assets[9]

Zicht op uw toeleveringsketen begint met een actuele lijst van uw assets. Hierbij is van belang om de kroonjuwelen van uw organisatie scherp in beeld te hebben. Kroonjuwelen zijn informatie en informatiesystemen die het allerbelangrijkst zijn voor een organisatie.[10]

- Uw ICT-afdeling onderhoudt een lijst met assets. Uw kroonjuwelen heeft u mogelijk al geïdentificeerd in uw risicomanagementproces of bedrijfscontinuïteitsplan. Maak gebruik van deze bestaande informatie om de belangrijkste assets binnen uw organisatie te identificeren. Hoe zijn uw kroonjuwelen en uw assets aan elkaar verbonden?
- Aantasting van de beschikbaarheid, integriteit en vertrouwelijkheid van belangrijke assets en kroonjuwelen kunnen organisatie belangen schaden. Door deze te beschermen organisatie belangen in kaart te brengen, en hoe deze verbonden zijn aan uw assets, creëert u een goed uitgangspunt voor risicomanagement.
- U kunt in een asset overzicht ook gebruik maken van *Software Bills of Materials* (SBOMs). Een SBOM beschrijft de componenten waaruit een stuk software is opgebouwd en de relaties tussen deze componenten.[11] Door SBOMs krijgt u overzicht de software die uw organisatie gebruikt en waar de verschillende softwarecomponenten vandaan komen.
- Neem ook *shadow IT*[12] mee in uw overzicht. Shadow IT blijft veelal onder de radar en kan grote gevolgen hebben voor uw organisatie, omdat u in dit geval geen zicht heeft op deze producten en diensten heeft. Er zijn technische mogelijkheden, zoals het uitvoeren van een scan, om aanwezige shadow IT te identificeren.

GP 1.2: Maak een leveranciersoverzicht

Binnen uw organisatie hebben alle verschillende afdelingen te maken met een deel van uw toeleveranciers. Door regelmatig langs deze afdelingen te gaan kunt u een actueel totaaloverzicht van toeleveranciers maken.

- Afdelingen binnen het primaire proces, maar ook ondersteunende afdelingen zoals ICT of marketing en communicatie of stafafdelingen, maken gebruik van toeleveranciers. Per afdeling kunnen toeleveranciers verschillen.
- Het crediteurenoverzicht van uw inkoopafdeling kan een belangrijke bron van informatie zijn. Dit crediteurenoverzicht kan naast een geïnventariseerd overzicht van uw ICT-afdeling worden gelegd om deze te controleren op volledigheid. Het kan bijvoorbeeld voorkomen dat u lopende onderhoudscontracten voor bepaalde software tegenkomt die nergens anders in beeld zijn.

GP 1.3: Classificeer en prioriteer uw leveranciers

Leveranciers kunnen diensten, goederen (zoals hardware) of software aanbieden. Om uw aandacht te kunnen richten op de belangrijkste leveranciers, is het van belang om uw leveranciers te classificeren en prioriteren. U kunt dit doen vanuit verschillende invalshoeken:

- Welke leveranciers zijn verbonden aan uw kroonjuwelen? Bepaalde leveranciers zijn van direct belang zijn voor het ongestoord functioneren van uw primaire en/of kritieke bedrijfsprocessen. Door vanuit kroonjuwelen te kijken naar de afhankelijkheden van leveranciers komt u tot een selectie.
- Welke leveranciers hebben toegang tot vertrouwelijke systemen en/of data? Bepaalde leveranciers leveren een niet-kritieke dienst aan uw organisatie, maar hebben wel toegang tot vertrouwelijke systemen en/of data.

  Denk hierbij aan leveranciers die die persoonsgegevens van uw medewerkers, klanten of relaties verwerken ten behoeve van marketing en communicatie. Soms heeft een leverancier direct toegang tot een dataset of informatiesysteem van uw organisatie.
- Over welke leveranciers maakt u zich zorgen vanwege een slechte reputatie? Deze leveranciers verdienen mogelijk extra aandacht omdat er binnen uw organisatie, of bij uw partners, slechte ervaringen mee bestaan. Ook als een leverancier betrokken is bij een informatiebeveiligingsincident zoals een datalek kan dat een aanleiding zijn om deze leverancier te bekijken.
- Verschillende methodes, zoals de Kraljic Matrix, zijn waardevol bij het inzichtelijk maken en prioriteren van risico's in de toeleveringsketen.[13]

GP 1.4: Ken, doorzie en begrijp uw belangrijkste leveranciers

Een veilige toeleveringsketen begint bij het kennen van uw belangrijkste toeleveranciers. Investeer in een goede relatie met uw belangrijkste leveranciers. Dit geeft een goede basis om het gesprek aan te gaan over cybersecurity en de manier waarop de leverancier zelf omgaat met zijn eigen leverancierssketen. Zo ontstaat een beeld van de cybervolwassenheid van een leverancier en kunnen ook kritieke afhankelijkheden van onderaannemers in beeld komen die van belang zijn voor uw organisatie.

Er zijn verschillende methodes waarmee u de cybersecurity status van uw (eventuele) leverancier kunt beoordelen:

- Gesprek: Faciliteer een gesprek tussen de security experts van de verschillende organisaties. Door de juiste vragen te stellen, kan er een beeld gevormd worden van de cybervolwassenheid van de toeleverancier.[14]
- Uitwisselen ervaring: Wissel waar mogelijk ervaringen uit met sectorgenoten om samen een beter beeld te krijgen bij de weerbaarheid van (sectorspecifieke) toeleveranciers.
- Cybersecurity ratings: Maak gebruik van de verschillende raamwerken en modellen die beogen om de cyber-security rating van een organisatie te profileren. In praktijk wordt er gebruik gemaakt van commerciële ratingbureaus (bijv. voor ISO 27001 en 28000-ratings).
- Ook raamwerken zoals CYRA kunnen een oplossing bieden.[15] Een instrument als CYRA is een laagdrempelig hulpmiddel voor organisaties in alle sectoren om cyberweerbaarheid in kaart te brengen. CYRA geeft middels een self-assessment en/of een certificering ook inzicht het niveau van cyberweerbaarheid van een organisatie.

Geopolitiek

Hoe hebben geopolitieke ontwikkelingen invloed op uw toeleveringsketen? In dit hoofdstuk gaan we verder in op risico's die voortkomen uit geopolitieke ontwikkelingen.

GP 2.1: Inventariseer welke risico's voortkomen uit geopolitieke ontwikkelingen

Wereldgebeurtenissen kunnen invloed hebben op uw toeleveringsketen. Risico's die hieruit voortkomen kunnen van geopolitieke, economische, sociologische, technologische en ecologische aard zijn.[16]

Want waar komen de producten en diensten waar u van afhankelijk bent vandaan? En via welke logistieke lijnen komen ze bij u terecht?

- Neem in uw periodieke risicoanalyse ook sabotage en spionagerisico's mee. Zo is in 2023 binnen de Rijksoverheid besloten dat applicaties, die afkomstig zijn uit landen met een offensief cyberprogramma gericht tegen Nederlandse belangen, worden ontraden op mobiele werkapparatuur. Dit besluit is genomen op basis van een risicoafweging.[17]
- Toenemende geopolitieke spanningen hebben mogelijk invloed op *insider* risico's[18]. Dit betreft dreiging vanuit personeel van uw toeleveranciers die wellicht ook bij u werkzaamheden verrichten.[19]

GP 2.2: Breng potentiele doelwitten in kaart vanuit het perspectief van een aanvaller

Inzicht in uw dreigingslandschap en aanvalsoppervlak zijn belangrijk om een inschatting te kunnen maken of uw organisatie en uw toeleveringsketen interessant zijn voor statelijke actoren.

Leveranciers kunnen worden gebruikt als tussenstap om uiteindelijk uw systemen, of die van andere klanten, te bereiken. Het uitvoeren van deze analyse is extra interessant als u afhankelijk bent van diensten en/of producten uit een land met een offensief cyberprogramma dat de Nederlandse belangen raakt.[20]

- Om deze analyse uit te voeren kan het waardevol zijn het perspectief van een aanvaller te nemen, en vanuit die blik te bepalen welke informatie en processen een interessant doelwit zijn.
- Neem uw leveranciers mee in dit dreigingslandschap en aanvalsoppervlak. In veel voorkomende gevallen worden leveranciers misbruikt als tussenstap om toegang te krijgen tot uw informatie en processen. Als uw vertrouwelijke informatie opgeslagen is bij een leverancier hoeft een aanvaller niet direct toegang te krijgen tot uw systemen om de vertrouwelijkheid van uw informatie te schaden.
- Voorkom tunnelvisie door het betrekken van externe experts bij het uitvoeren van een dreigingsanalyse. Zo zorgt u ervoor dat u geen belangrijke dreigingen over het hoofd ziet.[21]

Weerbaarheid

Nadat u risico's in de toeleveringsketen in kaart heeft gebracht, kunt u maatregelen nemen ten aanzien van geidentificeerde risico's. In dit hoofdstuk gaan we verder in op mogelijke maatregelen en hoe deze zich verhouden tot het door u geïdentificeerde risico.

GP 3.1: Digitale weerbaarheid begint bij uzelf

Een compromittatie in uw toeleveringsketen kan een direct effect hebben op uw eigen organisatie. Zorg er daarom voor dat u een aantal maatregelen treft die ervoor zorgen dat uw organisatie slechts beperkt risico loopt bij een eventuele compromittatie van een organisatie in uw toeleveringsketen.

GP 3.1.1: Voer periodiek een risicoanalyse uit

Zorg voor een gedragen risicoanalyse die door uw organisatie breed wordt opgepakt, Dit kan onderdeel zijn van een jaarlijkse risicomanagement cyclus. Neem hierin risico's ten aanzien van (logistieke) processen, dienstverlening (support), personen (inhuur, onderhoud, medewerkers) en producten (hard- en software) mee.

- Zorg ervoor dat u duidelijk hebt op welke manier de afgenomen dienst of apparatuur verbonden is met de rest van uw netwerk. Bepaal de risico's die deze met zich meebrengen en mitigeer deze door passende maatregelen te treffen. Maak hiervoor bijvoorbeeld gebruik van de basismaatregelen cybersecurity[22].

GP 3.1.2: Maak uw medewerkers bewust van risico's van derde partijen

Niet iedereen in uw organisatie zal een expert zijn op het gebied van cybersecurity. Inkopers zijn niet altijd op de hoogte zijn van de cybersecurity eisen die u wilt stellen aan toeleveranciers.

- Neem uw inkoopafdeling mee in verschillende cybersecurityeisen voor toeleveranciers en verschillende cybersecuritystandaarden.
- Het komt voor dat medewerkers hun eigen netwerken of systemen aanleggen, zonder dat u hier centraal regie op kan voeren (Shadow IT).[23] Maak medewerkers bewust van de risico's die gemoeid zijn met het gebruik van third-party diensten en apparaten om dergelijke situaties zo veel mogelijk te voorkomen.

GP 3.1.3: Doorloop een worst-case scenario

In het ergste geval wordt uw leverancier getroffen door een ernstig cyberincident dat grote impact heeft op de bedrijfsvoering van uw organisatie.

- In een table-top oefening kunt u een scenario doorlopen waarin een belangrijke toeleverancier getroffen raakt door een cybersecurity incident.[24] Dit kan u helpen in de voorbereiding voor een worst-case scenario.

GP 3.2: Goede afspraken maken met toeleveranciers voorkomt gedoe

Ook als u de basis van uw cybersecurity op orde heeft, wilt u aanvullende garanties dat uw toeleveranciers aan uw weerbaarheidsverwachtingen voldoen. Door te weten hoe uw toeleverancier omgaat met cybersecurity en hier afspraken over te maken, weet u hoeveel grip u echt heeft op risico's.

Mocht u in zee willen gaan met een leverancier, dan doet u er goed aan afspraken te maken en deze op papier te

zetten. Maak bijvoorbeeld afspraken over het uitvoeren van (onaangekondigde) security audits of security tests, of over het melden en verhelpen van beveiligingsincidenten. Maak hiervoor gebruik van een Service-level-agreement (SLA) en borg contractueel dat deze afspraken afgedwongen kunnen worden.

- Weet hierbij wat u vraagt en kunt vragen. Hecht u bijvoorbeeld veel waarde aan de beschikbaarheid van de dienstverlening en/of juist de vertrouwelijkheid van gegevens? In hoeverre zijn zaken als digitale soevereiniteit van belang voor uw organisatie? En vraag u om een maatwerkpakket – waar u aanvullende eisen kan stellen –, of om een standaarddienst en -overeenkomst? Wees op deze punten ook kritisch naar uw eigen organisatie en bedenk of uw organisatie de weerbaarheid op die punten ook voldoende op orde heeft.
- Zorg er tenslotte voor dat het afstemmen van security wensen een standaard onderdeel wordt van uw eigen inkoopprocedure en dat inkopers de juiste informatie en/ of expertise kunnen vinden om passende afspraken te maken.

GP 3.3: Wissel kennis en ervaringen uit

Cybersecurity risico's zijn vaak niet exclusief voor een individuele organisatie. Soms kan samenwerken met 'concullega's' in een sector of ketenverband waardevol zijn om kennis en expertise uit te wisselen.

GP 3.3.1: Weet elkaar te vinden en bouw aan vertrouwen

De belangrijkste vereiste om kennis onderling te delen, is vertrouwen. Zorg dat mensen elkaar kennen en weten te vinden. Een ISAC is een voorbeeld van een gremium waar mensen elkaar treffen en een vertrouwensband kan ontstaan, doordat steeds dezelfde personen aanschuiven en elkaar zo leren kennen en vertrouwen.[25]

- Zorg dat informatie op een gemakkelijke en vertrouwelijke manier met elkaar gedeeld kan worden. Een ISAC is een samenwerkingsvorm waarin informatie gedeeld kan worden in vertrouwen en op periodieke basis. Een platform of portaal waarin informatie/bestanden ook digitaal vertrouwelijk met elkaar gedeeld kunnen worden, zou hier ook aan bijdragen. Bijvoorbeeld om te zorgen dat niet alles via de mail verloopt.
- Vertrouwen creëren is niet altijd eenvoudig. Het NCSC heeft de Haagse Hogeschool in 2020 gevraagd succesfactoren voor cybersecurity informatiedeling tussen organisaties in kaart te brengen.[26] In dit document staan verdere handreikingen over hoe samen te werken met andere organisaties in uw sector of keten.

GP 3.3.2: Geef elkaar tips over leverancierslijsten, inkoopeisen en veiligheidsnormen

Verkrijg inzicht in het inkoop-aanbestedingsbeleid van elkaar. Deel kennis over welke eisen worden gesteld en welke onderdelen zijn getest. Dit kan de gehele keten versterken. Een toevoeging voor het eigen inkoop- en aanbestedingsbeleid is te leren van anderen.

- Geef elkaar bijvoorbeeld inzage in leverancierslijsten van bepaalde producten. Indien dezelfde producten aangeschaft moeten worden, is het handig om van elkaar te weten, welke leveranciers al zijn goedgekeurd door anderen. Dit kan het proces mogelijk versnellen.

GP 3.3.3: Samen invloed uitoefenen op internationale leveranciers

Het kan lastig zijn invloed uit te oefenen op internationale leveranciers. Door samen te

werken bij de inkoopprocessen kunt u een gezamenlijke wensen- en eisenlijst ontwikkelen.

- U kunt bijvoorbeeld vragen om transparantie omtrent de producten die u wilt inkopen. In groepsverband kan er meer invloed worden uitgeoefend op de leveranciers om aan kwaliteitseisen te voldoen. Toets deze kwaliteitseisen periodiek.

GP 3.4: Bereid een exit-plan voor

Het kan voorkomen dat u afscheid wilt nemen van een leverancier na zorgen over de veiligheid van uw toeleveringsketen. Een uitvoerbaar stappenplan kan u in dit geval veel helpen, zeker als daarin ook de benodigde juridische stappen verwerkt zijn. Zo kunt u tijdig afscheid nemen van een leverancier voordat u onnodig risico loopt.

Het helpt hierbij als u in een eerder stadium duidelijke afspraken hebt gemaakt met de leverancier in kwestie (zie GP 3.2). In dit geval kunt u terugvallen op deze afspraken als deze niet worden nagekomen.

- Bepaal hierbij wat de drempelwaarden zijn om ook juridisch de exit strategie voort te kunnen zetten en een contract te beëindigen. Laat u juridisch bijstaan in de afwikkeling van een overeenkomst.
- Houd hierbij rekening met de continuïteit van de dagelijkse (bedrijfs)processen. De organisatie moet goed blijven functioneren als u wisselt van leverancier. Denk hierbij bijvoorbeeld ook aan de overdracht van kennis en informatie als er een wisseling van personeel gaat komen.
- Maak een exit-plan al voordat een contract wordt afgesloten. Zo voorkomt u ongewenst afhankelijk te raken van een toeleverancier.
- Geef geen data of intellectueel eigendom weg. Als u het exit-plan in werking stelt, moet ook worden gezorgd voor de informatie die de leverancier over uw organisatie bezit en daar weer afstand van doet. Daarnaast moet deze informatie ook bij een nieuwe partij terecht komen. Denk hierbij o.a. aan intellectuele eigendomsrechten, beheerrechten, logs, broncode, softwarelicenties en de beschikbaarstelling van relevante data.

GP 3.5: Neem geopolitieke risico's mee in uw inkoopstrategie

GP 3.5.1: Zorg voor een gedegen inkoop- en aanbestedingsbeleid

Maak een gedegen aanbestedingsbeleid en/of stel een inkoopstrategie vast voor de organisatie waarin rekening is gehouden met geopolitieke risico's, zoals geopolitieke spanningen en digitale spionage, en deel dit onderling.

- Het goedkoopste product, of de goedkoopste dienst, hoeft niet altijd de beste keuze te zijn voor uw organisatie. Test de producten vooraf op veiligheid en kwaliteit en beoordeel de documentatie daaromtrent alvorens de organisatie akkoord gaat met de aankoop.

GP 3.5.2: Voorkom een te grote afhankelijkheid van specifieke toeleveranciers

Voorkom dat uw organisatie afhankelijk wordt van een specifieke (toe)leverancier. Zeker als deze leverancier gevestigd is in een gebied waarin geopolitieke spanningen kunnen ontstaan of zich in een instabiele regio bevindt. Dit kan tot leveringsproblemen leiden.

- Weet welke leveranciers nog meer op de markt zijn en waar zij zich bevinden. Denk hierbij ook aan welke moederbedrijven of aandeelhouders betrokken zijn. Ook hier kunnen geopolitieke ontwikkelingen en sancties gevolgen hebben voor uw toeleveringsketen.

Meer lezen?

SBOM Startersgids

In 2023 heeft TNO in samenwerking met het NCSC de startersgids SBOM uitgebracht. Hierin hebben TNO en het NCSC gekeken naar hoe organisaties de verwerking van *Software Bill of Materials* (SBOMs) in hun organisaties kunnen inrichten.

Startersgids: "Software Bill of Materials: Hoe, wat en waarom", TNO & NCSC, juni 2023

Good Practices for Supply Chain Cybersecurity, ENISA

In juni 2023 heeft ENISA vanuit het perspectief van Europese organisaties good practices voor supply chain cybersecurity in kaart gebracht. Hiervoor heeft ENISA 1081 organisaties uit de 27 leden van de EU geënquêteerd.

"Good Practices for Supply Chain Cybersecurity", ENISA, juni 2023

Supply chain security guidance, NCSC-UK

NCSC-UK heeft 12 principes in kaart gebracht om bedrijven in staat te stellen overzicht en controle te krijgen over hun toeleveringsketen.

"Supply chain security guidance", NCSC-UK, bezocht op 5 juli 2023

Dreigingsbeeld Statelijke Actoren, AIVD, MIVD en NCTV

Een aantal landen hebben een offensief cyberprogramma dat is gericht tegen Nederlandse nationale veiligheidsbelangen. Dit zijn onder andere China, Rusland, Iran en Noord-Korea.

In het Dreigingsbeeld Statelijke Actoren (DBSA) gaan de AIVD, MIVD en NCTV dieper op deze dreiging in. Dit document maakt eventuele risico's inzichtelijk wanneer u afhankelijkheden in deze landen heeft.

Rapport: "Dreigingsbeeld Statelijke Actoren 2", AIVD, MIVD en NCTV, november 2022

Vraagstukken en perspectieven voor ICT SCRM – een initiële verkenning, TNO

In 2021 heeft TNO in opdracht van het NCSC een publicatie uitgebracht over supply chain management in het digitale domein. Hierin gaat TNO dieper in op *supply chain risk management* (SCRM) en verschillende perspectieven daarop.

Rapport: "Vraagstukken en perspectieven voor ICT SCRM – een initiële verkenning", TNO, april 2021

Using the Software Bill of Materials for Enhancing Cybersecurity, Capgemini

In 2021 heeft Capgemini in opdracht van het NCSC een publicatie uitgebracht over SBOM en hoe dit te gebruiken om cybersecurity te bevorderen.

Publicatie: "Using the Software Bill of Materials for Enhancing Cybersecurity" (Engelstalig), Capgemini, februari 2021

5 adviezen voor veilige inkoop van clouddiensten, NCSC

Veel organisaties overwegen, of zijn al bezig met de inkoop van clouddiensten. Clouddiensten kunnen een grote functionele aanvulling vormen voor organisaties, mits er afgewogen maatregelen zijn genomen voor de inkoop van clouddiensten. In dit document gaat het NCSC verder in over hoe

organisaties clouddiensten veilig kunnen inkopen.

Factsheet: "5 adviezen voor veilige inkoop van clouddiensten", NCSC, oktober 2020

Start een ketensamenwerking, NCSC

Het NCSC heeft in 2018 een handreiking uitgebracht over het starten van een ketensamenwerking. In dit document gaat het NCSC verder in over hoe organisaties kunnen samenwerken in een keten en gezamenlijk risico's kunnen herkennen en verkleinen.

Handreiking: "Start een ketensamenwerking", NCSC, november 2018

Ketenweerbaarheid tegen cyberdreigingen, TNO

TNO heeft in 2017 een whitepaper uitgebracht met achtergrondinformatie, good practices en een stappenplan om de cyberweerbaarheid van een keten te verhogen.

Whitepaper: "Ketenweerbaarheid tegen cyberdreigingen", TNO, februari 2017

CYRA

Cyber Weerbaarheidscentrum Brainport, FERM Rotterdam, MKB Cyber Campus en TŰV NORD Nederland hebben CYRA opgezet. CYRA staat voor CYberRAting en is een methode om kleinere bedrijven perspectief en handvatten te geven in het realiseren van digitale weerbaarheid. Ook draagt CYRA bij aan transparantie van ketenpartners.

Website: "Jouw route naar digitaal weerbaar ondernemen", CYRA, bezocht op 10 augustus 2023

Referenties

[1] Good practices in dit document zijn werkwijzen, gebruiken en methodes die vanuit praktijkervaring effectief blijken in het benaderen van een vraagstuk.

[2] "Vraagstukken en perspectieven voor ICT SCRM – een initiële verkenning", TNO, februari 2021

[3] Deze definitie van *supply chain* risico is overgenomen van NIST en door het NCSC vertaald; "Security and Privacy Controls for Information Systems and Organizations", NIST SP 800-53 Rev. 5, September 2020

[4] Dit bleek uit het overzicht voor kwetsbare applicaties met Log4j-componenten op Github. Dit overzicht heeft het NCSC bijgehouden samen met nationale en internationale partners.

"Log4j", NCSC, bezocht op 28 juni 2023

[5] "Log4Shell Initial Exploitation and Mitigation Recommendations", Mandiant, 15 december 2021

[6] "Vier cybersecuritylessen uit een jaar oorlog in Oekraïne" , NCSC, DTC en CSIRT-DSP, februari 2023

[7] ISAC staat voor Information Sharing and Analysis Centre (ISAC). Dit is een overlegvorm over cybersecurity waarin organisaties uit dezelfde sector gevoelige en vertrouwelijke informatie uitwisselen over incidenten, dreigingen, kwetsbaarheden en maatregelen.

"Samenwerking in een ISAC", NCSC, bezocht op 8 augustus 2023

[8] In dit document duiden de we verschillende door de deelnemers geïdentificeerde *good practices* aan met "GP".

[9] Assets zijn, in cybersecurity-termen, informatie of digitale systemen die van waarde zijn voor een organisatie. Voorbeelden zijn: intellectueel eigendom, een klantendatabase, personeelsinformatie en dergelijke. Deze en andere gehanteerde definities in deze publicatie zijn, tenzij anders aangegeven, overgenomen uit het Cybersecurity Woordenboek.

"Cybersecurity Woordenboek 2021", Cyberveilig Nederland, december 2021

[10] Kroonjuwelen zijn informatie en informatiesystemen die het allerbelangrijkst zijn voor een organisatie. Het heeft grote gevolgen voor de organisatie als men niet meer bij deze informatie kan komen wanneer men dat wil. Of als de informatie niet meer klopt, of als die ongewild bij anderen terechtkomt.

[11] "Startersgids Software Bill of Materials: Hoe, wat en waarom", TNO & NCSC, juni 2023

[12] Shadow IT is hardware of software binnen een onderneming die niet ondersteund wordt en opgezet is door de IT-afdeling, maar wel een rol speelt in de bedrijfsvoering.

[13] "What is the Kraljic Matrix?", Forbes, 28 februari 2017

[14]

[15] "Jouw route naar digitaal weerbaar ondernemen", CYRA Cyber Rating, bezocht op 23 juni 2023

[16] "The Global Risks Report 2023", World Economic Forum, januari 2023

[17] "Apps uit landen met een offensief cyberprogramma tegen Nederlandse belangen", NCSC, bezocht in juni 2023

[18] Een insider threat is een dreiging die zijn oorsprong heeft binnen de organisatie. Bijvoorbeeld doordat medewerkers, oud-medewerkers en leveranciers bij informatie kunnen komen. Of doordat zij weten hoe zaken zijn beveiligd. Er is sprake van een insider threat als zo'n medewerker, oud-medewerker of leverancier zijn positie misbruikt voor kwaadwillende activiteiten.

[19] Zie bijvoorbeeld de publicaties van CISA over het beheersen van insider threat risico's;

"Insider Threat Mitigation", CISA, bezocht op 7 juli 2023

[20] Een aantal landen hebben een offensief cyberprogramma gericht tegen Nederlandse nationale veiligheidsbelangen. Dit zijn onder andere China, Rusland, Iran en Noord-Korea. In het Dreigingsbeeld Statelijke Actoren (DBSA) gaan de AIVD, MIVD en NCTV dieper op deze dreiging in.

"Dreigingsbeeld Statelijke Actoren 2", AIVD, MIVD en NCTV, november 2022

[21] Het NCSC voert met geprioriteerde sectoren MASKeR uit. MASKeR is een risicomanagement methode waarbij aan de hand van scenario's dreigingen, te beschermen belangen en weerbaarheid in kaart worden gebracht. Neem met

uw relatiemanager contact op als u geïnteresseerd bent in MASKeR.

[22] "Basismaatregelen cybersecurity", NCSC, bezocht op 23 juni 2023

[23] Denk bij Shadow IT ook aan het gebruik van cloudoplossingen zoals DropBox, WeTransfer en GoogleDrive. Deze oplossingen zijn populair bij medewerkers in de privésfeer om bestandsoverdracht te faciliteren. Zakelijk gebruik van deze oplossingen buiten het zicht van uw organisatie zorgt voor een extra risico. Zie voor meer informatie over Shadow IT: "Shadow IT: Hoe voorkomen we het?", KPN, december 2018

[24] "CISA Tabletop Exercise Package", CISA, 17 december 2020

[25] "Samenwerking in een ISAC", NCSC, bezocht op 23 juni 2023

[26] "Succesfactoren voor het delen van cybersecurity informatie", Haagse Hogeschool, augustus 2020

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

15 augustus 2023

TLP:CLEAR