Supply Chain Process
Richtlijnen 2020

CENTRE FOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

T. : +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

CHANCELLERY OF
THE PRIME MINISTER

.be

Inhoudstafel

CENTRE FOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

T. : +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

CENTRE FOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

T. : +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

1 Inleiding

1.1 Doel

Het doel van dit document is het beschrijven van controledoelstellingen om de vertrouwelijkheid, integriteit en beschikbaarheid (CIA-triade) te beschermen binnen de supply chain van netwerkassets en -diensten voor Aanbieders van Essentiële Diensten (AED's) onder de NIS-wetgeving (kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, publicatiedatum 3/5/2019, NUMAC 2019011507).

1.2 Bijdragen

Dit document kwam tot stand dankzij de gewaardeerde inbreng van het BIPT (Belgisch Instituut voor Postdiensten en Telecommunicatie), verschillende andere overheids organisaties alsook experten in (Cyber)veiligheid.

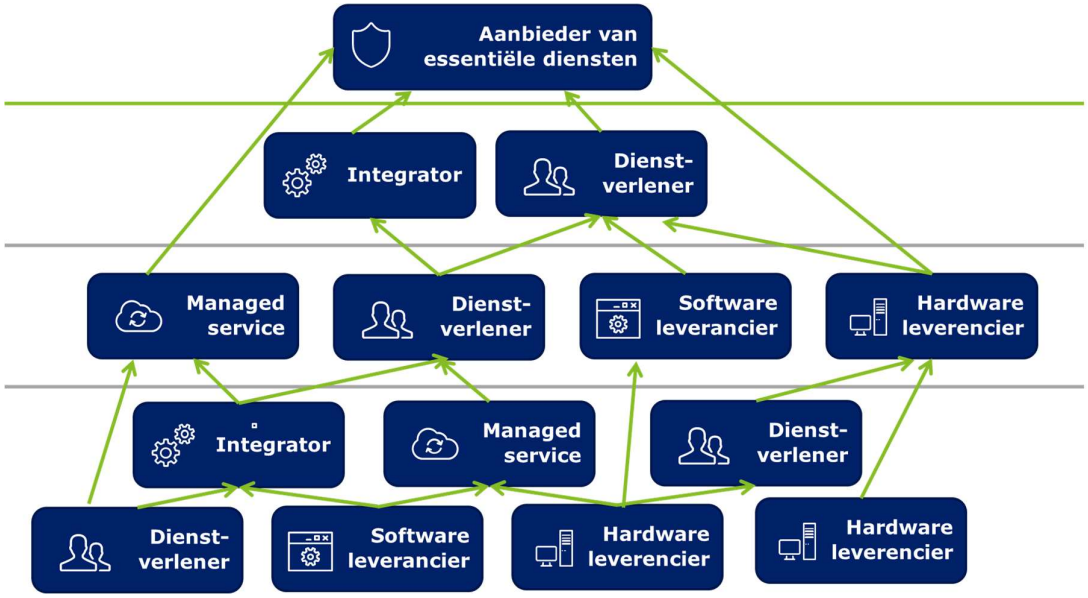
1.3 Supply chain van netwerkassets en -diensten

Doordat steeds meer op derde partijen gesteund wordt om de eigen dienstverlening te optimaliseren en kostenefficiënt te werken, wordt het steeds belangrijker om een zicht te krijgen op de beveiligingsrisico's omtrent deze derde partijen en de derde partijen daarvan. Derde partijen zijn onder meer integratoren, dienstverleners (bv. onderhoud van netwerkcomponenten), managed services, hardware- en softwareleveranciers.

Supply chain security is de beveiliging van assets en diensten gedurende de volledige levenscyclus van een systeem (ontwerp, ontwikkeling, bouw, verpakking, assemblage, distributie, systeemintegratie, operationeel beheer, onderhoud en het uit dienst nemen).

Afhankelijk van het type dienstverlener zijn de supply chain en het gebruik van derde partijen door de dienstverlener zelf, complexer en minder transparant. Zowel door de aanbieder van essentiële diensten als door de dienstverleners zelf moet er bewust worden omgegaan met de supply chain en de gerelateerde risico's teneinde de nodige mitigerende maatregelen te implementeren.

Daar aan deze maatregelen kosten zijn verbonden voor zowel de aanbieder van essentiële diensten als de derde partijen, dienen ze gebaseerd te zijn op een onderbouwde risico assessment voor zowel de dienstverlener als de derde partij.



FIGUUR 1 - COMPLEXITEIT VAN DE SUPPLY CHAIN VOOR AANBIEDERS VAN ESSENTIËLE DIENSTEN

1.4 Documentstructuur

Dit document is opgebouwd uit verschillende controledomeinen binnen het supply chain-proces. Per controledomein worden algemene controledoelstellingen opgesteld, gerelateerd aan informatiebeveiliging binnen dat domein. Een controledomein kan worden aangevuld met een of meerdere subdomeinen die specifiekere controledoelstellingen beschrijven. Om aan een controledoelstelling te voldoen, kunnen een of meerdere maatregelen worden geïmplementeerd. Een exhaustieve lijst met maatregelen valt niet binnen de scope van dit document, maar waar mogelijk wordt wel verwezen naar bestaande internationale standaarden.

De levenscyclus van een dienst of asset wordt in dit document opgesplitst in vijf controledomeinen waarbij “risicobeheer” wordt beschouwd als zesde centraal domein.

De verschillende hoofdstukken hebben betrekking op verschillende stappen binnen de levenscyclus van een asset of dienst.

CENTRE FOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

T. : +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

1.5 Gerelateerde documenten

Dit document past in het kader van ISO 28000 “Security managementsystemen voor de supply chain” als controledoelstelling voor het op te stellen en te implementeren supply chain security-plan. De scope van dit document is echter beperkt tot controledoelstellingen voor informatiebeveiliging van netwerkassets en -diensten. Meer algemene controledoelstellingen en specifieke maatregelen kunnen worden teruggevonden in standaarden zoals ISO 27000 of de “Basis Information Security Guidelines” (BSG) van het CCB.

De volgende documenten werden gebruikt als referenties voor de tekst:

- ISO/IEC 27000 – 27001 – 27002 – 27005
- ISO/IEC 27017 Cloud Security
- ISO/IEC 27036 Information security for supplier relationships
- ISO/IEC 28000
- NIST SP 800 161
- ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation
- ISO/IEC 20243:2015 Open Trusted Technology Provider Standard
- NIST Cybersecurity Framework Version 1.1 (2018)
- Baseline Information Security Guidelines (CCB editie 2019)

1.6 Termen en definities

Term	Definitie
AED	Aanbieder van Essentiële Diensten Onder de definitie van de wet “kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid” artikel 6, § 11 (publicatiedatum 3/5/2019, NUMAC 2019011507)
CERT	Cyber Emergency Response Team. Zie CSIRT.
CIA - triade	CIA staat voor Confidentiality, Integrity & Availability. In dit document verwijzen we naar de Nederlandse vertaling hiervan: vertrouwelijkheid, integriteit en beschikbaarheid.
Controle	Maatregel die het gerelateerde risico beïnvloed (conform ISO).
Controledomein	Een controledomein beschrijft een onderwerp waarvoor Controledoelstellingen worden opgesteld.
Controledoelstelling	Een controledoelstelling beschrijft een specifiek doel waartegen de effectiviteit van de te implementeren maatregelen kan worden geëvalueerd (conform ISO).
CSIRT	Computer Security Incident Response team. Zie CERT.
GDPR	Dit is de “General Data Protection Regulation”, ofwel de Algemene Verordening Gegevensbescherming. Een verordening met als doel de standaardisering van de regels met betrekking tot de verwerking van persoonsgegevens.
Niet-EU leverancier	Hiermee wordt ook bedoeld dienstverlening verleend in een niet-EU land.
KPI	KPI staat voor Key Performance Indicator. Hiermee bedoelen we een maatstaf waartegen geleverde prestaties kunnen worden geëvalueerd.
NIS-richtlijn	Verwijst naar de Europese Richtlijn 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie. Deze richtlijn werd omgezet naar Belgische wetgeving op 7 april 2019.
RTO	RTO staat voor Recovery Time Objective. Dit is de maximale tijd die vereist is om vanaf een incident terug tot een normale dienstverlening te komen.
SLA	SLA staat voor Service Level Agreement. Dit is de vastlegging van de minimale dienstverlening of kwaliteit die de klant kan verwachten.
Supply Chain	De toeleveringsketen voor diensten en assets.

Termen die niet werden gedefinieerd in de bovenstaande tabel volgen de definities van bestaande standaarden (cf. ISO en NIST).

2 Risicobeheer (Risk Management)

Identificeren en analyseren van risico's binnen de organisatie met betrekking tot de supply chain van netwerkassets en diensten.

2.1 Contextbepaling

2.1.1 Asset- en dienstenregister (asset and service inventory)

Doelstelling: Opstellen en bijhouden van een overzicht van alle netwerkassets, diensten en de kriticiteit ervan.

Leidraad: AED's stellen een proces op om assets en diensten bij te houden in een register. Dit draagt bij tot een centraal en overkoepelend overzicht. In dit overzicht kunnen kenmerken zoals eigenaarschap (ownership) worden bijgehouden.

2.1.2 Evalueer afhankelijkheid van andere dienstverleners

Doelstellingen: Evalueren van de dienstverlening naar afhankelijkheid van andere dienstverleners.

Leidraad: aanbieders van essentiële diensten dienen te evalueren in welke mate hun dienstverlening afhankelijk is van andere vitale diensten (bv. levering elektriciteit) en wat de impact hiervan is bij uitval of verstoring en hoe (preventieve) maatregelen deze impact kunnen minimaliseren.

2.1.3 Dreigingsbeeld en dreigingsscenario's

Doelstelling: bepalen en opvolgen van het dreigingsbeeld en aanverwante dreigingsscenario's voor netwerkassets en -diensten.

Leidraad: veranderingen in het dreigingsbeeld zullen worden opgevolgd door periodische review van industriebeveiligingsberichten en -aanbevelingen (security bulletins van leveranciers of nationale CERT's). Bij wijzigingen in het dreigingsbeeld, bv. nieuwe dreigingsscenario's, kan het nodig zijn om risico's binnen de supply chain opnieuw te evalueren.

2.2 Risicoanalyse (Risk Analysis)

2.2.1 Supply chain-risicoanalyse

Doelstelling: identificeren en analyseren van supply chain-beveiligingsrisico's binnen het bredere risicobeheer binnen de organisatie.

Leidraad: AED's leggen een methodologie vast van risicoanalyses inclusief gerelateerde impact- en waarschijnlijkheidsschalen.

Hier wordt er gedefinieerd welke assets deel uitmaken van de essentiële dienstverlening in de supply chain alsook de risico's die moeten worden bekeken. Het is belangrijk om de Supply chain-risicoassessment te integreren in het bredere (Enterprise) risicobeheer.

De op te stellen impacttabellen houden rekening met de impactcriteria zoals het aantal gebruikers dat door de verstoring van de essentiële dienst wordt getroffen, de duur van het incident en de omvang van het geografische gebied dat door het incident is getroffen.

Op basis van een risicoanalyse worden de te implementeren maatregelen voor een asset of dienst bepaald. Bij een asset of dienst met een hoog risico zullen striktere maatregelen nodig zijn dan voor een asset of dienst met een laag risico.

2.3 Risicocommunicatie en -monitoring

2.3.1 Risicocommunicatie

Doelstelling: delen van risico-informatie met relevante stakeholders.

Leidraad: het communiceren van risico's is belangrijk voor de opvolging van het risicobeeld en het bepalen van de te implementeren maatregelen bij derde partijen.

2.3.2 Risicomonitoring

Doelstelling: opvolgen van de bestaande risico's binnen de organisatie.

Leidraad: risico's binnen een organisatie zijn niet statisch. Het dreigingslandschap past zich continu aan en hierdoor kunnen de risico's binnen de organisatie wijzigen of kunnen er nieuwe risico's ontstaan. Een periodieke herevaluatie van de risico's binnen de organisatie is nodig voor een degelijke risicomonitoring. Hiernaast kunnen ook aanpassingen binnen de organisatie leiden tot een wijziging van risico's.

3 Beveiligingsbeheer en -architectuur (Security Management and architecture)

Algemeen beheer van informatiebeveiliging voor netwerkassets en -diensten, en beveiligingsarchitectuur van netwerkassets en -diensten.

3.1 Beheer

3.1.1 Rollen en verantwoordelijkheden

Doelstelling: formaliseren van belangrijke verantwoordelijkheden en governancestructuur bij verwerver en uitbesteder omtrent de supply chain.

Leidraad: bij uitbesteding zijn er een aantal belangrijke verantwoordelijkheden die moeten worden toegewezen, zowel bij de organisatie van de verwerver als bij de organisatie van de uitbesteder.

Identificeren welke stakeholders betrokken dienen te zijn bij beslissingsproces, wie de beslissing finaal maakt en wie aansprakelijk is voor een actie/resultaat, wie geconsulteerd of geïnformeerd moet zijn, met andere woorden het RACI-model (bv. legale dienst, HR, finance, Enterprise risk management, IT, procurement, program management etc.).

Het toekennen van de nodige resources voor het uitvoeren van processen en maatregelen relevant voor informatiebeveiliging voor de supply chain.

3.1.2 Inkoopstrategie (Procurement Strategy)

Doelstelling: definiëren van een door het management ondersteunde inkoopstrategie die betrekking heeft op bedrijfs-, operationele, wettelijke, architecturale en regelgevende vereisten.

Leidraad: de AED dient voor de essentiële diensten te bepalen wat de aankoopstrategie is en dit uit te werken in templatecontracten en aankoopmethodes.

Organisaties dienen derde partijen aan te sporen om informatiebeveiligingsmaatregelen te implementeren, transparantie te creëren in organisatorische processen, in het eigen gebruik van derde partijen en praktijken m.b.t. informatiebeveiliging, en in het voorzien van extra controle op de medewerkers en andere derde partijen gerelateerd aan dienstverlening voor de essentiële dienst.

3.1.3 Definitie en Opvolging van KPI's voor de supply chain security

Doelstelling: definiëren en opvolgen van KPI's voor de supply chain security.

Leidraad: de AED definieert interne en externe KPI's voor de opvolging van supply chain security-vereisten.

3.1.4 Risicobehandeling (Risk Treatment)

Doelstelling: behandelen van risico's met betrekking tot een netwerkasset of -dienst.

Leidraad: op basis van risicoanalyse kan de striktheid van de te implementeren maatregelen voor een asset of dienst worden bepaald.

3.1.5 Incident management

Doelstelling: voorbereid zijn voor het afhandelen en opvolgen van incidenten.

Leidraad: het definiëren van een formele incidentafhandelingsprocedure draagt bij tot de efficiëntie waarmee kan worden gereageerd op incidenten. Deze procedure bevat ten minste de volgende fases: Voorbereiding (Prepare); Detecteren en analyseren (Detection and Analysis); Inperken, bestrijden en herstellen (Contain, eradicate and recover); Post-incidentactiviteiten (Post-incident activities).

Bij definitie van deze procedure zal de AED ook de verschillende rollen en verantwoordelijkheden tijdens incidentafhandeling moeten toewijzen aan interne of externe partijen. Verder zal de AED een contractuele definitie moeten maken met zijn derde partijen wanneer de AED op de hoogte wenst te worden gebracht van incidenten bij zijn derde partijen.

De AED zal ook in zijn incidentafhandelingsprocedure de wettelijke verplichting omtrent het melden van incidenten aan de Nationale CSIRT, de sectorale overheden en het Nationaal Crisis Centrum integreren.

3.2 Netwerkbeveiligingsarchitectuur

3.2.1 Netwerkarchitectuurschema

Doelstelling: opstellen en bijhouden van een schematisch overzicht van alle netwerkassets en gerelateerde diensten, en de connecties ervan.

Leidraad: de AED bewaart een overzicht van hoe de verschillende netwerkassets en -diensten met elkaar communiceren en interageren.

3.2.2 Netwerkinformatiebeveiligingsmaatregelen

Doelstelling: bepalen van netwerkinformatiebeveiligingsmaatregelen op basis van een risicoanalyse (waarbij ten minste de verschillende informatiestromen en de gevoeligheid van de data meegenomen worden).

Leidraad: op basis van het netwerkarchitectuurschema kan er worden gekeken naar de risico's en relevante maatregelen op de netwerklaag. In de risicoanalyse dienen ten minste de verschillende informatiestromen, gekende kwetsbaarheden en gevoeligheid van de data meegenomen te worden).

3.3 Cloudoplossingen

Steeds vaker wordt gebruikgemaakt van Cloudoplossingen zoals Software as a Server (SaaS), Platform as a Service (PaaS) of Infrastructure as a Service (IaaS). Hierop zijn specifieke controledoelstellingen van toepassing.

3.3.1 Kriticiteit van de Cloud

Doelstelling: in kaart brengen van de datastromen naar de Cloudserviceprovider en de kriticiteit van de dienstverlening.

Leidraad: de AED bepaalt de impact die een Cloud service kan hebben op de volledige supply chain-keten wat de dienstverlening van een essentiële dienst betreft. Deze geeft een indicatie van de mitigerende maatregelen die door de cloud service provider en de mitigerende maatregelen die door de AED moeten geïmplementeerd worden. Risico's gerelateerd aan cloudoplossingen zullen anders moeten worden beheerd en gemitigeerd dan klassieke risico's gecontroleerd door de organisatie.

3.3.2 Beveiligingsmaatregelen voor cloudinformatie

Doelstelling: definiëren van de noodzakelijke maatregelen voor het opslaan van data in de Cloud met adequate bescherming en rekening houdend met andere richtlijnen en wetgevingen.

Leidraad: het bewaren van data in de Cloud moet aan dezelfde toegangscontroles voldoen als data die lokaal zijn opgeslagen. Daarnaast moet er gekeken worden of de geografische locatie van de data en eventuele back-ups in lijn is met wat is toegestaan door andere richtlijnen of wetgevingen (bijvoorbeeld GDPR).

3.3.3 Gegevenssoevereiniteit bij dienstverlening door niet-EU-leverancier

Doelstelling: bescherming van gegevenssoevereiniteit bij niet-EU-leverancier

Leidraad: het gebruik van IT-diensten inclusief Cloudservices door niet-EU-leveranciers brengt risico's voor de gegevenssoevereiniteit met zich mee. Dit betekent dat alle gegevens die zijn opgeslagen, verwerkt of verzonden door de service onderworpen zijn aan de wet- en regelgeving van die landen waar gegevens worden opgeslagen, verwerkt en verzonden.

Evenzo kan een niet-EU-leverancier die een dienst binnen België exploiteert, onderworpen zijn aan de wetten van het land waar zijn maatschappelijke zetel is gevestigd. Zo kan een dienstverlener door een niet-EU-beveiligingsinstantie gedwongen worden om gegevens van zijn klanten te verstrekken zonder de klant op de hoogte te stellen van het verzoek. Daarom is het van belang dat een AED de juridische regels identificeert waarin de gegevens worden opgeslagen, verwerkt of verzonden.

Verder moeten ze ook begrijpen hoe de wetten van die landen de vertrouwelijkheid, integriteit, beschikbaarheid en privacy van de informatie kunnen beïnvloeden. Wanneer een dienstverlener een aspect van de levering van de service uitbesteedt aan een derde, moet de AED ook vaststellen of dit extra risico's op het gebied van gegevenssoevereiniteit met zich meebrengt.

4 Inkoop (Procurement)

Leveranciersrelatiebeheer en aankoop van netwerkassets en diensten tot de levering en stockage.

4.1 Relatiebeheer (Relationship Management)

Het beheren van de relatie met leveranciers loopt van het eerste contact tot het afronden ervan.

4.1.1 Uitwisselen van informatie

Doelstelling: bewust omgaan met het uitwisselen van informatie met (potentiële) leveranciers tijdens het inkoopproces.

Leidraad: tijdens het inkoopproces zal er informatie uitgewisseld worden tussen de organisatie en de (potentiële) leveranciers.

Deze informatiedeling start bij het opstellen van een lastenboek of Request For Proposal (RFP). Tijdens deze uitwisseling zal er duidelijkheid moeten zijn welke informatie wordt gedeeld. Indien nodig kan er voor het delen van de informatie een bindende afspraak worden gemaakt met de (potentiële) leverancier om de gedeelde informatie contractueel te beschermen. Dit onder andere met betrekking tot het delen van informatie met onderaannemers of derde partijen van de (potentiële) leverancier. Of de toegestane bewaartijd van de informatie.

4.1.2 Contractuele nood aan informatiebeveiligingsmaatregelen van leveranciers

Doelstelling: verzamel, analyseer en rapporteer informatiebeveiligingsmaatregelen gerelateerd aan inkoop van assets of diensten om de maturiteit van informatiebeveiliging in de leveranciersrelatie te kunnen demonstreren, voor het starten van een nieuwe relatie en op regelmatige tijdstippen voor bestaande relaties.

Leidraad: bij het selecteren van een leverancier voor een asset of dienst kan een bepaalde maturiteit van informatiebeveiliging worden afgedwongen. Deze status dient ook te worden opgevolgd bij bestaande relaties. Dit kan actief (via) audit, of passief (via rapportage). Indien de securitynoden wijzigen, zal samen met de derde partij een mogelijke herziening moeten gebeuren van de informatiebeveiligingsmaatregelen.

4.1.3 Beveiligingsmaturiteit van leveranciers (Suppliers Security maturity)

Doelstelling: kiezen van leveranciers die een adequate informatiebeveiligingsmaturiteit hebben alsook het regelmatig opvolgen van deze.

Leidraad: de leverancierskeuze zal worden gemaakt op basis van verschillende parameters. Een van deze parameters is het gewenste niveau van informatiebeveiliging. De AED kan ook zelf de informatiebeveiligingsmaturiteit bepalen door het uitvoeren van een audit of maturiteitsanalyse.

4.1.4 Naleving van Europese en nationale regelgeving door leveranciers

Doelstelling: kiezen van leveranciers die de Europese en nationale regelgeving naleven.

Leidraad: de leverancier dient geëvalueerd te worden en er moet worden nagegaan of deze zich moet onderwerpen aan regelgeving die in strijd is met Europese of Belgische regelgeving.

4.1.5 In kaart brengen van alle partners en partijen betrokken bij de dienstverlening van leveranciers.

Doelstelling: in kaart brengen van alle (strategische) partners en partijen, zoals subcontractors hun dienstverlening en verhouding tot essentiële diensten.

Leidraad: de AED brengt zijn (strategische) partners en partijen in kaart, alsook de dienstverlening die ze leveren en hoe ze zich verhouden tot de essentiële dienstverlening van de AED. Deze inventaris zal een overzicht creëren van de risico's.

4.1.6 De AED houdt rekening met dreigingsgerelateerde informatie

Doelstelling: integreren van de dreigingsinformatie over niet-EU-leveranciers in het risicoanalyseproces van de AED.

Leidraad: AED's krijgen voor de dreigingsgerelateerde informatie die nodig is voor hun risicoanalyse toegang tot het centrale Cyber Threat Intelligence platform (CTI/EWS). De bevoegde inlichtingendiensten delen via dit CTI-platform hun dreigingsanalyses met betrekking tot bepaalde technische en geopolitieke risico's. Specifieke analyses worden door het CCB gecoördineerd in overleg met de bevoegde veiligheids- en inlichtingendiensten.

4.2 Verzending, levering en stockage

Assets die worden verzonden en gestockeerd kunnen tijdens deze periode worden blootgesteld aan externe dreigingen. Ook digitale downloads of files kunnen tijdens transport over het netwerk of bij opslag worden gecompromitteerd.

4.2.1 Beschermen van integriteit, vertrouwelijkheid en beschikbaarheid van een asset

Doelstelling: beschermen van assets tegen kwaadwillige aanpassing tijdens verzending, levering en stockage.

Leidraad: assets zullen worden gecontroleerd om anomalieën tijdens de verzending, levering of stockage te detecteren. Mogelijks door het vereisen van verzegelde verpakkingen tijdens transport en opslag. Er is ook controle nodig op de verzending, levering en stockage van digitale assets. De integriteit van digitale downloads en opgeslagen files zal indien nodig ook gevalideerd moeten worden vooraleer deze worden gebruikt.

4.3 Self-assessment statement voor leveranciers van IT-beveiligingsdiensten of -systemen

Doelstelling: het naleven van de supply chain proces-richtlijnen door subcontractors of de toeleveranciers van de AED.

Voor de levering of aankoop van IT-beveiligingsdiensten of -systemen zal de leverancier een self-assessment statement overmaken waarin hij verklaart conform de verschillende controledoelstellingen van deze richtlijn te zijn.

Bijlage 1 bij de richtlijn geeft een voorbeeld van een self-assessment statement.

5 Operationeel beheer (Operational Management)

Operationeel beheer omvat de terugkerende beheers- en onderhoudstaken die worden uitgevoerd door een derde partij of diensten die worden afgenomen bij een dienstverlener.

5.1 Algemene beveiligingsmaatregelen

5.1.1 Bewustmaking

Doelstelling: bewustmaking van werknemers over het delen van bedrijfsinformatie met externe partijen en de mogelijke risico's verbonden aan de supply chain.

Leidraad: informatie kan met derde partijen worden gedeeld op een "need-to-know" basis.

5.1.2 Operationele procedures

Doelstelling: opstellen en beheer van Security Operating Procedures gerelateerd aan netwerkassets en -diensten.

Leidraad: de organisatie zal een set van Security Operating Procedures opstellen en navolgen om de residuele risico's met betrekking tot de informatiebeveiliging op een aanvaardbaar niveau te houden.

5.1.3 Contracten

Doelstelling: beschermen van bedrijfsinformatie tegen diefstal en misbruik door externen.

Leidraad: het opstellen van bindende afspraken tussen alle betrokken partijen om informatie adequaat (cf. risk assessment) te beschermen en de CIA ervan te verzekeren zal in contracten met externen worden opgenomen om een juridische bescherming tegen diefstal en misbruik van bedrijfsinformatie te garanderen.

5.1.4 Toegang tot netwerkassets

Doelstelling: onbevoegde toegang tot netwerkassets voorkomen en monitoren.

Leidraad: voor werknemers, intern en extern, is een duidelijke Identity en Access Management (IAM)-levenscyclus nodig. Toegang tot netwerkassets mag enkel worden verleend indien dit nodig is voor de uitvoering van hun functie. Deze toegang dient dan ook terug worden ingetrokken eens deze niet meer nodig is.

5.1.5 Loggen & monitoren

Doelstelling: loggen en monitoren van netwerkassets en -diensten voor het detecteren van informatiebeveiligingsincidenten.

Leidraad: de verschillende netwerkassets dienen te worden voorzien van de nodige logging en monitoring voor het detecteren van informatiebeveiligingsincidenten (bv. onbevoegde toegang).

5.1.6 Informatie-encryptie

Doelstelling: zorgen voor correct en doeltreffend gebruik van cryptografie om de confidentialiteit, integriteit en beschikbaarheid (CIA) van de informatie te beschermen.

Leidraad: het gebruik van end-to-end-encryptie en -tunnels bij communicatie over toestellen die niet door de organisatie worden beheerd of waarvan de veiligheid niet voldoende kan worden gegarandeerd.

5.1.7 Informatie-uitwisseling

Doelstelling: handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe partij.

Leidraad: opstellen van duidelijke regels en maatregelen rond het mailen naar derde partijen en het delen van documenten.

5.1.8 Leveranciersafhankelijkheid

Doelstelling: het beperken van de afhankelijkheid van één leverancier.

Leidraad: de AED dient erover te waken niet afhankelijk te worden van één leverancier of fabrikant voor netwerkassets of -diensten.

Dit kan bijvoorbeeld door broncode van applicaties ontwikkeld door derde partijen onder te brengen bij een escrow service, een tweede datacenter af te nemen bij een andere leverancier Etc.

De netwerk- en cloudarchitectuur dient voldoende rekening te houden met de mate waarin deze afhankelijk is van één leverancier of fabrikant. Een modulaire architectuur met componenten die door meerdere leveranciers en/of fabrikanten geleverd worden zal de organisatie minder afhankelijk maken van één derde partij.

5.2 Consulenten/Externen

Alle externe werknemers, van lange en korte duur, worden binnen de scope van dit document als consulent aanschouwt. Bijkomend aan de maatregelen in 5.1.

5.2.1 Fysieke toegang

Doelstelling: onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatieverwerkende faciliteiten van de organisatie voorkomen.

Leidraad: een externe werknemer mag enkel toegang krijgen tot ruimten en gebouwen die nodig zijn voor het uitoefenen van zijn functie. Deze toegang kan worden voorzien op zelfstandige basis of onder begeleiding.

5.3 Derde-partijbeheerder

Een derde partij kan verschillende aspecten van de organisatie beheren. Enkele voorbeelden kunnen zijn: netwerkbeheer, serverbeheer of datacenterbeheer. Bijkomend aan de maatregelen in 5.1.

5.3.1 Toegang in de tijd

Doelstelling: beperken van toegang tot systemen en toepassingen binnen aangeduide tijdsintervallen.

Leidraad: de toegang van een derde-partijbeheerder zal beperkt worden in de tijd. De toegang kan verleend worden binnen een tijdsvenster (bv. kantooruren) of op basis van een aanvraag (bv. support-ticket).

5.4 Managed Service Providers

Een uitbesteedde dienst. Bijkomend aan de maatregelen in 5.1.

5.4.1 Extern informatietransport

Doelstelling: handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe entiteit.

Leidraad: bij het afnemen van een managed service die toegang heeft tot of controle heeft over het kernnetwerk van de organisatie moet er rekening mee worden gehouden dat de informatie die wordt gedeeld met adequate beveiliging beschermd wordt.

5.4.2 De AED houdt rekening met dreigingsgerelateerde informatie

Doelstelling: integreren van de dreigingsinformatie over niet-EU-leveranciers in het risicoanalyseproces van de AED.

Dezelfde regel geldt hier als deze bepaald bij de sectie Inkoop (4.1.6)

6 Incidentherstel en grote uitbreidingen (Recovery & Major Changes)

Uitzonderlijke ingrepen aan netwerkassets en -diensten en het wijzigen van de dienstverlening en het vervangen van netwerkassets. Deze vallen niet binnen het dagelijks operationeel beheer.

6.1 Algemeen

6.1.1 Beschermen van toegang voor uitzonderlijke ingrepen

Doelstelling: voorzien van tijdelijke autorisatie tot netwerkassets en -diensten tijdens uitzonderlijke ingrepen.

Leidraad: externe supportteams moeten de mogelijkheid hebben om tijdelijk toegang te krijgen tot de nodige netwerkassets of -diensten.

6.1.2 Noodplannen

Doelstelling: uitgewerkte noodplannen om kritieke assets en diensten te herstellen.

Leidraad: implementeer noodplannen die supply chain-aspecten meenemen zodat de integriteit en betrouwbaarheid van de supply chain gegarandeerd blijven gedurende potentiële incidenten (bv. cyberaanval of staking)

6.1.3 Veilige toegang

Doelstelling: voorzien in veilige communicatiekanalen voor remote supportteams.

Leidraad: tijdens herstellingen en grote uitbreidingen kan toegang op afstand worden verleend tot delen van de basisnetwerkinfrastructuur. Toegang op afstand kan onder verschillende vormen worden geïnstantieerd, bijvoorbeeld diensten zoals RDP of SSH.

Voor het verlenen van toegang op afstand aan externe ondersteuningsteams zal er gebruikgemaakt worden van veilige communicatiekanalen (bijvoorbeeld beschermd met VPN en multifactorauthenticatie).

6.1.4 Beveiligde gebieden

Doelstelling: onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatieverwerkende faciliteiten van de organisatie voorkomen.

Leidraad: bij herstellingen of grote uitbreidingen kan er nood zijn aan toegang tot bepaalde ruimten of faciliteiten voor het herstellen of vervangen van netwerkcomponenten.

Het verlenen van een te brede of ongeplande toegang moet worden voorkomen. Hoe wordt fysieke toegang verleend? Via aanvraag, ad hoc, in noodgevallen? Is er nood aan begeleiding?

6.2 Retourneren

Assets kunnen voor herstellingen worden teruggestuurd naar de leverancier, ook gekend als Retourneren met autorisatie (RMA).

6.2.1 Veilig terugsturen

Doelstelling: beschermen van bedrijfsdata aanwezig op assets die worden teruggestuurd naar de leverancier of fabrikant.

Leidraad: tijdens het terugsturen zal rekening moeten gehouden worden met welke partijen (koerierdienst, post etc.) toegang hebben tot deze assets en welke informatie zich op de asset bevindt.

7 Veilige buitengebruikstelling (Secure disposal)

Uit productie halen van toestellen en afsluiten of transitie van diensten.

7.1 Datadragers

7.1.1 Voorkomen van informatielekken

Doelstelling: beschermen tegen het verlies van gegevens bij het uit dienst nemen van netwerkassets.

Leidraad: bij het buitengebruikstellen van apparatuur kan de vraag worden gesteld of deze toestellen mogen worden hergebruikt of moeten worden vernietigd. Deze beslissing kan worden genomen op basis van de risicoanalyse. Wanneer een toestel wordt bestemd voor hergebruik, via verkoop of binnen de organisatie, zullen eerst alle data adequaat moeten worden verwijderd van het toestel.

7.2 Servicetransitieplan

7.2.1 Beheer van data bij leveranciers bij stopzetting

Doelstelling: beschermen van bedrijfsinformatie gedeeld met een leverancier bij stopzetting van een servicecontract.

Leidraad: bij het beëindigen van een dienst zullen alle datatransfers van/naar de leverancier worden afgesloten. Bedrijfsinformatie die opgeslagen is bij de leverancier zal moeten worden verwijderd door de leverancier en indien toepasselijk moeten worden teruggegeven aan de AED.

Bij overdracht van een dienst naar een andere leverancier zal ook de nodige bedrijfsinformatie van de originele naar de nieuwe leverancier moeten worden overgedragen. Deze overdracht zal adequaat worden beschermd.

Bijlage 1: Voorbeeld supply chain security self-assessment statement

[Leverancier]

Ik bevestig hierbij als [Leverancier] dat de security van de supply chain van het product [Product] is beoordeeld tegen de vereisten vooropgesteld door [AED].

Ik bevestig met dit supply chain security statement voor het product [Product], dat de controle objectieven worden behandeld zoals beschreven door [AED] voor de volgende controle domeinen:

Risicobeheer

- Beveiliging & Architectuur
- Inkoop
- Operationeel beheer
- Incidentherstel & Grote Uitbreidingen
- Veilige Buitengebruikstelling

Ik kan het nodige ondersteunende bewijsmateriaal aanleveren indien nodig.

Leverancier:

Handtekening

Datum

Verantwoordelijke uitgever:
Centrum voor Cybersecurity België
M. De Bruycker, Directeur
Wetstraat, 16
1000 Brussel

Wettelijk depot
D/2020/14828/001

Supply Chain Process guidelines – December 2019

CENTRE FOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

T. : +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

CHANCELLERY OF
THE PRIME MINISTER

.be