Richtlijn cybersecurity voor leveranciers

Vereniging voor Christelijk Voortgezet Onderwijs te Rotterdam en omgeving

Herkomst document

AUTEUR	ORGANISATIE(ONDERDEEL)
Derk Wieringa, Branko van Ormondt en Michiel van Tol	Grant Thornton Specialist Advisory B.V. Cyber Risk Services

Wijzigingshistorie

VERSIE	DATUM	TOELICHTING/WIJZIGINGEN
0.2	11-04-2024	Eerste versie door Grant Thornton
0.3	25-04-2024	Reviewcommentaar CVO verwerkt door Grant Thornton
0.9	17-05-2024	Versie ter goedkeuring (door Grant Thornton)
1.0	19-06-2024	Reviewcommentaar CVO verwerkt door Grant Thornton, versie ter goedkeuring

Goedkeuring

ORGANISATIE (ONDERDEEL)	NAAM	FUNCTIE	DATUM	HANDTEKENING
CVO	A. Bestebreur	Lid raad van bestuur	6-11-24	

Verzendlijst

ORGANISATIE (ONDERDEEL)	NAAM	FUNCTIE

Inhoudsopgave

1. Inleiding

CVO streeft naar een passend niveau van cybersecurity om ervoor te zorgen dat haar organisatie weerbaar is tegen cyberdreigingen. CVO maakt bij de ondersteuning van haar bedrijfsprocessen gebruik van applicaties en systemen die door externe leveranciers worden ontwikkeld, beheerd en/of gehost. Hierdoor is het niveau van cybersecurity van CVO afhankelijk van deze leveranciers.

CVO blijft altijd de wettelijke eigenaar van alle gegevens die worden verwerkt in zowel haar eigen systemen als die van haar leveranciers. Dit betekent dat CVO in het kader van de AVG eindverantwoordelijk is voor de bescherming van haar gegevens, ook als deze gegevens door een externe leverancier op basis van een verwerkingsovereenkomst worden verwerkt. Een aanzienlijk deel van deze gegevens is vertrouwelijk van aard. Daarom is het belangrijk dat ieder leveranciersrisico zoveel als redelijkerwijze mogelijk wordt geminimaliseerd.

CVO beoogt om het leveranciersrisico te verlagen door minimumeisen voor cybersecurity op te leggen aan leveranciers en voortdurend te controleren of leveranciers zich aan deze eisen houden. Deze richtlijn beschrijft welke aspecten van cybersecurity CVO in de overwegingen bij het selecteren van een leverancier moet betrekken en op welke criteria leveranciers in het belang van cybersecurity dan moeten worden beoordeeld. Dit document moet voor iedere leverancier in de toeleveringsketen van CVO worden gebruikt.

2. Doel van de richtlijn cybersecurity voor CVO-leveranciers

CVO moet te allen tijde weten tot welke data en tot welke onderdelen van het CVO-netwerk de leverancier toegang heeft. Dit moet duidelijk worden gedocumenteerd en regelmatig worden gecontroleerd op juiste toepassing en wijzigingen. Deze richtlijn moet in acht worden genomen bij het definiëren van rollen en verantwoordelijkheden van CVO en die van haar leveranciers.

2.1 Eigenaarschap van CVO-data

CVO zal altijd de wettelijke eigenaar blijven van alle CVO-data die wordt verwerkt door een leverancier. De leverancier heeft op basis van een verwerkingsovereenkomst de rol van gegevensverwerker en is daarom verantwoordelijk voor het veilig opslaan, verwerken en beheren van de data van CVO en het naleven van de door CVO gestelde cybersecurity-eisen. De afspraken over de gegevensverwerking worden vastgelegd in een verwerkingsovereenkomst en/of SLA.

Vervolgens is het de verantwoordelijkheid van CVO om regelmatig te beoordelen of haar leveranciers een passend niveau van cyberweerbaarheid handhaven. Deze richtlijn beschrijft de onderwerpen waarover afspraken worden gemaakt tussen CVO en haar leveranciers en de minimale eisen die CVO stelt op gebied van cybersecurity.

2.2 Verantwoordelijkheden met betrekking tot cybersecurity-incidenten

Leveranciers worden geacht om CVO te informeren in het geval van een cybersecurity-incident en zijn verantwoordelijk voor grondig onderzoek naar de onderliggende oorzaak en de verdere afhandeling van het incident binnen hun eigen omgeving.

CVO wil de mogelijkheid hebben om haar eigen onderzoek uit te kunnen voeren in het geval van een cybersecurity-incident bij de leverancier. De leverancier wordt geacht om volledig transparant te zijn over de gebruikte software, systemen en operationele procedures en om volledige medewerking aan CVO te verlenen bij het onderzoek van het incident.

2.3 Selectie en screening van leveranciers

Dit document moet worden gebruikt in de eerste fase van het selecteren van een leverancier. Dit is een van de basisbeginselen van “Security by design” en “Privacy by design” en zorgt ervoor dat cyberweerbaarheid vanaf het begin wordt geïmplementeerd. In een later stadium is het implementeren van cybersecuritymaatregelen vaak zeer inefficiënt of zelfs onmogelijk.

Leveranciers moeten een screeningsprocedure ondergaan om te verzekeren dat zij een passend niveau van cybersecurity handhaven. Deze screeningsprocedure kan ook een auditproces omvatten waarbij CVO een onderzoek mag uitvoeren om vast te stellen of door de leverancier toereikende cybersecuritymaatregelen zijn genomen.

- Onderdeel van deze screeningsprocedure is een intake waarbij de Chief Information Security Officer (CISO-rol) bepaalt of de cybersecurity ambitie van de leverancier aan de minimale eisen die CVO stelt, voldoet.
- Het uitvoeren van de screeningsprocedure en audits mag CVO deels of in geheel uitbesteden aan een derde partij, waarbij CVO vanzelfsprekend een en ander afstemt met de leverancier.
- Leveranciers worden geacht om transparant te zijn over de manier waarop ze te werk gaan, welke systemen ze gebruiken en welke data zij verwerken.
- Als de leverancier andere digitale diensten levert en/of onderdeel uitmaakt van een groep die digitale diensten levert op dezelfde infrastructuur als de geleverde dienst aan CVO, moet de leverancier CVO daarover direct informeren. Tevens moet leverancier aangeven hoe de cybersecurity omtrent deze diensten is geregeld. CVO heeft het recht om de cybersecurity-ambitie van alle entiteiten en/of diensten van leverancier die gebruik maken van dezelfde infrastructuur te beoordelen om te kunnen bepalen of zij de cybersecuritystandaarden nog steeds aanvaardbaar vindt.

- CVO moet haar visie over cyberweerbaarheid in de vroegste fase van het leveranciersselectieproces communiceren met de leverancier om te verzekeren dat de visies van CVO en de leverancier tijdig op elkaar zijn afgestemd.

Na implementatie van deze richtlijn zullen niet alleen nieuwe leveranciers aan een screening worden onderworpen, maar zullen ook bestaande leveranciers worden beoordeeld op hoe goed zij presteren op het gebied van de cyberweerbaarheidseisen van CVO. De screening wordt voor bestaande leveranciers periodiek, minimaal jaarlijks, herhaald om vast te stellen dat ze de gemaakte afspraken naleven. In het geval afwijkingen worden geconstateerd tussen de vereisten van CVO en gemaakte afspraken en het huidige niveau van cybersecurity dat de leverancier toepast, zal in overeenstemming met de leverancier een plan worden opgesteld om het niveau van cyberweerbaarheid te vergroten.

2.4 Beëindiging van dienstverlening

Bij het aangaan van een overeenkomst tussen CVO en een leverancier, met betrekking tot de diensten die deze levert, is vastgelegd onder welke voorwaarden de dienstverlening mag plaatsvinden. Wanneer de overeenkomst tussen CVO en een leverancier eindigt, gelden de voorwaarden die CVO stelt aan een goede afwikkeling van de overeenkomst:

- Bij het aangaan van een overeenkomst wordt de exit-strategie beschreven. Daarin is minimaal opgenomen dat alle data van CVO wordt teruggegeven aan CVO, onder welke voorwaarden en in welk format die overdracht plaatsvindt en dat de leverancier daarna alle CVO-data zal verwijderen.
- Het is aan de leverancier om bewijs aan te voeren dat laat zien dat alle CVO-data is overgedragen en daarna is verwijderd.
- In geval van faillissement van de leverancier moet de data worden aangeleverd aan CVO zoals vastgelegd in de exit-strategie.
- CVO heeft het recht om onderzoek uit te voeren om vast te stellen dat de data verwijderd is.

2.5 Geopolitieke spanningen

Bij de selectie van leveranciers houdt CVO rekening met politieke spanningen tussen het land waaruit de leverancier opereert en Nederland of de Europese Unie. CVO kijkt niet alleen naar de onderneming waarmee het een overeenkomst aangaat, maar naar de gehele structuur van de organisatie, bijvoorbeeld een buitenlandse moeder. Als politieke spanningen escaleren tussen Nederland, de Europese Unie en het land waar de leverancier is gevestigd, kan dat betekenen dat de leverancier niet langer zijn diensten aan CVO kan leveren wegens handelsbeperkingen of economische sancties.

3. Beheer van de toeleveringsketen

Om te garanderen dat CVO continu inzicht heeft in de cybersecurity ambitie van haar leveranciers, moet speciale aandacht worden besteed aan het leveranciersmanagement en alle relevante wijzigingen. Daarom vereist CVO volledig inzicht in relevant(e) beleid, bedrijfsstructuur en eigenaarschap van haar leveranciers. CVO verwacht om op de hoogte te worden gebracht wanneer wijzigingen worden doorgevoerd.

3.1 Verzameling, opslag en locatie van CVO-data

CVO moet kunnen controleren hoe leveranciers CVO-data verzamelen en bepalen of hun methoden veilig zijn.

- Leveranciers moeten verzekeren dat de data wordt verzameld en opgeslagen op een veilige manier. Dit omvat (fysieke) beveiligingsmaatregelen die ongeautoriseerde toegang voorkomen.
- Leveranciers moeten de data die zij verzamelen minimaliseren tot het minimum dat vereist is om hun dienst of product te leveren.
- Leveranciers moeten verzekeren dat de data zowel “at rest” als “in transit” is versleuteld met een modern en sterk encryptiealgoritme.
- CVO vereist dat al haar data blijft opgeslagen binnen de wettelijke grenzen van de EER en dat zij wordt geïnformeerd over het werkelijke land waarin de data wordt opgeslagen.
- CVO vereist haar leveranciers om de principes van ‘security by design’ en ‘privacy by design’ te hanteren.

3.2 Periodieke beoordeling van de cybersecurity-ambitie van de leverancier

CVO beoogt om regelmatig de cybersecurity-ambitie van haar leveranciers te beoordelen om te kunnen bepalen of zij de cybersecuritystandaarden van de leveranciers nog steeds aanvaardbaar vindt. Hierbij wordt gebruik gemaakt van bijlage I van dit document, waarin de minimale eisen staan beschreven. Deze beoordelingen moeten minstens jaarlijks worden uitgevoerd. Als een leverancier, of CVO, een wijziging wenst door te voeren in het beleid, organisatiestructuur, of IT-infrastructuur met mogelijke impact op de bedrijfsvoering en cyberweerbaarheid van CVO, dan wordt de wijziging vooraf beoordeeld en deze mag alleen worden doorgevoerd na instemming door CVO.

3.3 Periodieke meetings met leveranciers over cyberweerbaarheid

CVO wil periodieke sessies houden met haar leveranciers om wijzigingen bij CVO en de leverancier te bespreken die impact hebben op de cyberweerbaarheid. Deze meetings moeten minstens jaarlijks plaatsvinden, of vaker wanneer dit noodzakelijk wordt geacht door CVO of de leverancier. CVO neemt de leiding tijdens deze cyberweerbaarheid meetings en is verantwoordelijk om deze regelmatig in te plannen. Tijdens deze meetings zal CVO de cybersecuritycriteria bespreken die in bijlage I worden vermeld. Als een grote wijziging wordt doorgevoerd die impact heeft op de cyberweerbaarheid van CVO of haar leverancier, moet altijd een meeting worden georganiseerd om de mogelijke implicaties van deze wijziging te bespreken.

In het geval van een cybersecurity-incident waarbij de leverancier en/of de door leverancier geleverde diensten betrokken zijn, wordt gehandeld volgens het CVO Cybersecurity Incident Respons Plan en zal een meeting worden gehouden om mogelijke implicaties van het incident te bespreken.

Om efficiënte communicatielijnen tussen CVO en de leverancier te garanderen, vraagt CVO de leverancier een hoofdcontactpersoon aan te wijzen voor cybersecuritykwesties. Deze persoon moet in staat zijn om de vragen van CVO op het gebied van cybersecurity te beantwoorden en meldt CVO wanneer wijzigingen met betrekking tot cybersecuritystandaarden bij de leverancier worden doorgevoerd.

3.4 Minimale eisen voor leveranciers

Na het selecteren van een nieuwe leverancier is het belangrijk dat de leverancier niet alleen voldoet aan de functionele eisen die CVO stelt, maar ook aan de privacy- en cybersecurity-eisen. De CISO-rol van CVO biedt

ondersteuning bij de evaluatie van het privacy en cybersecuritybeleid van de leverancier en kan bepalen of de standaarden van de leverancier toereikend zijn. De minimale cybersecurity eisen zijn in bijlage I beschreven.

Bijlage I – Minimum eisen voor cybersecurity

De minimale eisen die CVO stelt aan haar leveranciers staan hieronder vermeld. CVO kan altijd extra eisen opleggen wanneer zij dit noodzakelijk acht. Niet alles kan worden afgevangen in deze richtlijn, sommige zaken zijn vastgelegd als onderdeel van een SLA en het (inkoop) contract.
Door een overeenkomst met CVO te ondertekenen, gaat de leverancier akkoord met deze voorwaarden:

1. Leverancier verklaart zich bereid en in staat om op proactieve wijze zorg te dragen voor een passend cybersecurityniveau voor data en systemen van CVO.
2. Leverancier beoordeelt en herziet jaarlijks de cybersecurity-onderdelen in de overeenkomst met CVO. Ook stemt de leverancier ermee in om actief deel te nemen aan periodieke cybersecuritymeetings met CVO.
3. Leverancier levert bewijs aan van certificeringen op gebied van cybersecurity, zoals ISO27001 of ISO9001. Leverancier is ervoor verantwoordelijk dat CVO op elk moment het meest actuele en geldige certificaat in bezit heeft.
4. Leverancier heeft in ieder geval passende maatregelen getroffen op de volgende acht cybersecurity aandachtsgebieden die CVO belangrijk vindt:

I. Authenticatie

- Gebruik sterke wachtwoorden met moderne versleutelingstechnieken (zoals salting).
- Sla wachtwoorden op als een hash.
- Dwing het wachtwoordbeleid actief af en voer periodieke controles uit om ervoor te zorgen dat deze goed is geïmplementeerd op de werkvloer.
- Gebruik en dwing MFA (multi-factor authenticatie) actief af als onderdeel van het authenticatie beleid.
- Controleer loginpogingen om kwaadaardige activiteiten en gelekte of misbruikte inloggegevens te detecteren.
- Zorg voor een uniek account voor iedere gebruiker binnen de omgeving.
- Maak gebruik van de SSO (Single Sign On) voorziening van CVO, als de voorziening toegankelijk is voor medewerkers en leerlingen van CVO.

II. Privileged access management

- Hanteer een beleid voor privileged access management en dwing het gebruik hiervan actief af.
- Pas de principes van ’least access’ en ‘least privilege’ toe wanneer toegang wordt verleend tot systemen en data van CVO.
- Geef alleen privileged access nadat een (vastgelegd) wijzigingsverzoek is ingediend.
- Stel MFA (multi-factor authenticatie) in en dwing MFA actief af op privileged accounts.
- Leg iedere privileged actie vast in een activiteitlogbestand.
- Gebruik alleen speciale privileged accounts voor privileged toegang en zorg voor volledige scheiding tussen privileged en normale gebruikersaccounts.
- Voer periodieke controles uit op de activiteitenlogs om kwaadaardige acties te detecteren en rapporteer de resultaten periodiek aan CVO.
- Voer periodieke controles uit om privileged accounts te toetsen op buitensporige privileges. Dit wordt tenminste iedere drie maanden gedaan, rapporteer de resultaten aan CVO.

III. Hardening

Het doel van hardening van IT-omgevingen is het verbeteren van de beveiliging van systemen, netwerken en applicaties. Door het aanvalsoppervlak te verkleinen wordt de omgeving minder kwetsbaar voor aanvallen, inbreuken en misbruik.

- Harden omgeving op basis van technische standaarden die CVO acceptabel vindt. Het doel van hardening van IT-omgevingen is het verbeteren van de beveiliging van systemen, netwerken en applicaties om zo het aanvalsoppervlak te verkleinen door het elimineren van overbodige functionaliteiten, uitschakelen van

onnodige accounts en diensten, versterken van configuraties, aanscherpen van wachtwoordbeleid, toegang tot bestanden en directories, systeemrechten, kernel-parameters, netwerkinstellingen en patchbeleid.

- Communiceer hardening-maatregelen naar CVO zodat CVO kan beoordelen of ze toereikend zijn.
- Gebruik technieken zoals: defense-in-depth, isolatie van systemen, end-point protection, firewalls, web-application firewalls (WAFs) en intrusion detection / prevention systemen om de omgeving te beveiligen.
- Implementeer additionele hardening-maatregelen voor bedrijfskritische systemen en omgevingen.
- Voer regelmatig cybersecurity (hacking) testen en scans uit op de gehardende omgeving om te garanderen dat de beschermingsmechanismen naar verwachting functioneren. De test- en scanresultaten worden periodiek gerapporteerd aan CVO.
- Implementeer fysieke beveiligingsmaatregelen om ongeautoriseerde (fysieke) toegang tot de omgeving te voorkomen.

IV. Updates

- Richt een gedocumenteerd proces in om patches en updates te beheren.
- Beoordeel wijzigingen en test ze grondig voorafgaand aan implementatie.
- Stel CVO vooraf op de hoogte wanneer een update of wijziging wordt geïmplementeerd die mogelijk impact heeft op de bedrijfsvoering en cyberweerbaarheid van CVO. Wijzigingen waarbij kans bestaat op verstoring van de bedrijfsvoering of aantasting van de cyberweerbaarheid mogen alleen worden doorgevoerd na goedkeuring door CVO.
- Scan regelmatig de omgeving op het ontbreken van patches, want dat kan een dreiging vormen voor de beveiliging van data en systemen van CVO.

V. Encryptie

- Versleutel alle netwerkverbindingen (met name de verbindingen naar het CVO-netwerk) door middel van een modern encryptiealgoritme. Deze versleuteling moet worden geïmplementeerd met een encryptieprotocol dat op minimaal TLS 1.2 (of een vergelijkbaar encryptieprotocol).
- Versleutel alle data zowel “at rest” als “in transit”.

VI. Beschikbaarheid

- Richt mitigerende maatregelen in tegen Denial of Service (DoS) aanvallen.
- Garandeer dat gegevens van CVO periodiek worden veiliggesteld via back-up in overeenstemming met de RPO.
- Minimaliseer het risico van een single point of failure door de architectuur zo in te richten dat altijd een uitwijkmogelijkheid beschikbaar is als een systeem of locatie uitvalt. De systemen van de leverancier moeten kunnen blijven functioneren en beschikbaar blijven zelfs als een centraal systeem of kantoor niet meer functioneert.
- Garandeer een minimale uptime van de dienstverlening en zorg voor een RTO waarmee in geval van een incident deze uptime kan worden gegarandeerd.

VII. Monitoring

- Controleer de omgeving continu om afwijkingen en mogelijke indicatoren van cybersecurity-incidenten te detecteren. Dit omvat automatische logging van loginpogingen en verdacht gedrag.
- Verleen CVO op verzoek toegang tot logbestanden die informatie bevatten over de toegang tot data van CVO. Op deze manier kan CVO de logbestanden controleren op verdacht gedrag dat de cybersecurity van CVO of haar data kan beïnvloeden.
- Controleer continu de technische staat van de systemen en appratuur om kwetsbaarheden te detecteren.

VIII. Incident afhandeling

- Stel een gedocumenteerd cybersecurity incident response plan in dat periodiek wordt getest en geüpdatet.
- Laat CVO het incident response plan beoordelen om vast te stellen of deze aansluit op het Cybersecurity Incident Response Plan van CVO.

- Laat CVO het incident rapport en de logbestanden onderzoeken nadat een incident heeft plaatsgevonden.
- Meld cybersecurity incidenten en/of het datalekken direct aan CVO.
- Toon aan dat passende maatregelen zijn genomen om incidenten in de toekomst te voorkomen.