/// Beleid rond relatiebeheer met dienstenleveranciers

1 INTRODUCTIE

Lokale besturen en dienstenleveranciers willen bij de uitvoering van hun taken en diensten 'samen' komen tot een synergetische en veilige dienstverlening voor burgers, medewerkers en andere belanghebbenden. Ondanks dat de samenwerking tussen lokale besturen en dienstenleveranciers (meestal) goed verloopt, zijn er vaak ook verbeterpunten. Voorbeelden hiervan zijn o.a. het verduidelijken van de verdeling van verantwoordelijkheden, of het versterken van de beveiliging voor de externe accounts waarmee dienstenleveranciers toegang hebben tot de systemen van uw lokaal bestuur.

Gezien het belang van het garanderen van een veilige dienstverlening, is het belangrijk om als lokaal bestuur kritisch te kijken naar de relaties met uw dienstenleveranciers. Een beleid rond het beheer van de relaties met dienstenleveranciers kan hierbij van grote waarde zijn omdat het duidelijke kaders zet en medewerkers concrete handvaten biedt. Om een succesvol beleid te implementeren is het belangrijk dat het toezicht van dit beleid wordt toegewezen aan een beleidsmedewerker. Deze persoon heeft de verantwoordelijkheid en de bevoegdheid om de toepassing en naleving van het beleid op te volgen en eventuele inbreuken hiervan te rapporteren.

2 WET- EN REGELGEVING

Een samenwerking tussen een lokaal bestuur en een dienstenleverancier wordt vastgelegd door middel van een contract. Een contract beschrijft de rechten en plichten van de partijen en de geleverde diensten tussen de afnemer en aanbieder. Bij het afsluiten van ICT-diensten wordt extra aanbevolen om het reguliere contract uit te breiden met een Service-Level Agreement (SLA).

Een SLA is een verdere uitwerking van het originele contract betreft de kwaliteit van de diensten die een leverancier levert aan een afnemer. Een Service-Level Agreement (SLA) bevat in gekwantificeerde en meetbare termen de normen voor de dienstverlening. Denk aan beschikbaarheid, betrouwbaarheid en continuïteit.

Vergeet ook zeker niet aan de GDPR-vereisten te voldoen wanneer bedrijfsinformatie persoonsgegevens bevat (van toepassing op alle niveaus), d.w.z. dat in het contractuele kader beveiligingsmaatregelen hieromtrent moeten worden genomen.

Als u diensten afneemt via een raamcontract van de Vlaamse overheid, zitten afgesproken Service-Level Agreements (SLA's) hier deels in vervat. Ook al kunnen bijkomende afspraken rond SLA's nog steeds noodzakelijk zijn (afhankelijk van raamcontract en/of opdracht). Verder moet een lokaal bestuur ervoor zorgen dat Service-Level Agreements (SLA's) rond cyberveiligheid minstens even strikt zijn als de eigen interne

cyberveiligheidsmaatregelen. Over het algemeen zijn Service-Level Agreements (SLA's) maatwerk. Ze zijn toegespitst op de overeenkomst, de aard van de dienstverlening en de betrokken partijen. Hoofdlijnen zijn uiteraard wel te schetsen.

Typische onderwerpen die in de meeste Service-Level Agreement (SLA's) zijn geregeld:

- Een accurate omschrijving (scope) van de diensten die onder een Service-Level Agreement (SLA) vallen
- Servicelevels die behaald moeten worden
- De wijze waarop het behalen van de servicelevels wordt gemeten
- De sancties of incentives bij het niet of wel behalen van servicelevels
- De wijze van overleg en communicatie
- De wijze van escalatie, evaluatie, bijstelling en herziening van de inhoud van uw Service-Level Agreement (SLA).

Voor het opstellen van contracten geldt dat het vaak beter werkt om zelf de regie over het opstellen van de bewoording te hebben. Hetzelfde geldt voor een Service-Level Agreement (SLA). Door zelf de bewoordingen te kiezen en te bepalen is het doorgaans eenvoudiger om de betekenis en reikwijdte hiervan te doorgronden.

3 BELEID

Organisatorische maatregelen

Organisatorische maatregelen verwijzen naar het hebben van duidelijke processen, procedures en verantwoordelijkheden rond de omgang met dienstenleveranciers. Naast het belang om een Service-Level Agreement (SLA) met uw dienstenleverancier af te sluiten, moet u binnen uw lokaal bestuur ook procedures vastleggen rond de wervingsprocedure van dienstenleveranciers. Bijkomend, om de voorwaarden van uw Service-Level Agreement (SLA's) te controleren, is het belangrijk om de juistheid en de continuïteit van deze voorwaarden op te volgen en te rapporteren naar het management.

Technische maatregelen

Technische maatregelen verwijzen naar het hebben van documentatie waarin de werking, voorwaarden, verantwoordelijkheden en onderhoud met betrekking tot de diensten van uw dienstenleveranciers beschreven staan.

Idealiter staat het meeste al beschreven in een Service-Level Agreement (SLA) en wordt er voor de maatregelen gebruik gemaakt van een referentiekader zoals de ISO27002:2022 beheersmaatregel. Vanuit een authenticatie en autorisatie perspectief is het van groot belang om de nodige technische maatregelen te nemen ten opzichte van uw dienstenleveranciers.

Zorg ervoor dat dienstenleveranciers – die vaak toegang hebben tot uw computersystemen en informatie – gebruik moeten maken van multifactor-authenticatie (MFA) wanneer zij toegang wensen te hebben tot uw digitale omgeving. Het is ook belangrijk om uw IT-omgeving regelmatig te controleren op de juistheid van de autorisaties van externe accounts. Zorg ervoor dat dienstenleveranciers enkel toegang hebben tot de systemen

die zij echt nodig hebben. Het is ook belangrijk om de toegangsrechten van inactieve gastaccounts regelmatig op te schorten.

Mensgerichte maatregelen

Mensgerichte maatregelen verwijzen naar het hebben van goede onboarding processen waarin de veiligheidseisen van uw organisatie worden benadrukt bij de dienstenleveranciers die op uw omgeving werken.

4 AANBEVELINGEN

Hieronder vindt u een aantal aanbevelingen die het Cyber Response Team voor Lokale Besturen (Vo-CRT) geeft met betrekking tot een beleid rond relatiebeheer met dienstenleveranciers.

Veel van deze maatregelen (specifiek over relatiebeheer) kunt u terugvinden in het Cyberfundamentals Framework van het CCB.

Organisatorische maatregelen:

- Zorg dat u een Service-Level Agreement (SLA) afsluit voordat u zich verbindt aan een dienstenleverancier.
- Zorg dat u uw Service-Level Agreement (SLA) baseert op relevante maatregelen van een referentiekader zoals de ISO27002:2022 beheermaatregelen.
- Zorg dat er standaardprocedures en processen (bijv. een screening) bestaan voor het werven van dienstenleveranciers.
- Controleer op regelmatige basis de juistheid en de continuïteit van de voorwaarden in een Service-Level Agreement (SLA).
- Zorg voor een gedocumenteerde lijst van alle leveranciers, verkopers en partners van uw organisatie die bij een ernstig incident betrokken kunnen zijn; die lijst moet worden bijgewerkt wanneer nodig en online en offline beschikbaar zijn.
- Zorg dat ook dienstenleveranciers over de nodige crisis-, continuïteits- en herstelplannen beschikken.
- Zorg dat dienstenleveranciers incidenten correct en tijdig meedelen en escaleren volgens afgesproken procedures.
- Zorg ervoor dat het periodiek uitvoeren van audits onderdeel uitmaakt van de Service-Level Agreement (SLA), zodat u de prestaties van de leverancier kunt opvolgen.

Technische maatregelen

- Verplicht multi-factor authenticatie (MFA) voor dienstenleveranciers die toegang tot uw systemen hebben.
- Controleer de juistheid van de autorisaties van externe accounts en schort de rechten van inactieve accounts op.
- Betrek uw dienstenleveranciers en externe partners bij het uitvoeren van (test) response- en herstelplannen.

Mensgerichte maatregelen

- Zorg voor een goede on boarding wanneer dienstenleveranciers of externe partners op uw systemen gaan werken.

5 VERKLARENDE WOORDENLIJST

Term	Verduidelijking	Link naar meer informatie
SLA	Een Service-Level Agreement (SLA) is verdere uitwerking van het originele contract voor wat betreft de kwaliteit van de diensten die een leverancier levert aan een afnemer.	service level agreement (SLA) - Glossary | CSRC (nist.gov) https://overheid.vlaanderen.be/service-level-agreements
GDPR	De General Data Protection Regulation of algemene verordening gegevensbescherming (AVG) is een Europese wetgeving met doel om de privacy van burgers beter te beschermen.	AVG (GDPR) en de Vlaamse Toezichtcommissie (VTC) | Vlaanderen Intern
MFA	Multi-factor authenticatie is een elektronische authenticatiemethode waarbij gebruikers pas toegang krijgen tot een website of applicatie nadat gebruikers zich twee (of meer) keer geauthentiseerd hebben.	Toegangsbeheer | Vlaanderen.be

REFERENTIES

- CCB – Cyberfundamentals Framework – Risicobeheer van de toeleveringsketen
  - https://ccb.belgium.be/nl/cyberfundamentals-framework