Federal Information Security Policy Guideline

Handleiding voor de beveiliging in de cloud

21/11/2019

FISPDOC07 V1.2

Belangrijke opmerking: Dit document is een leidraad die het resultaat is van een samenwerking tussen informatiebeveiligingsexperts van de verschillende federale diensten (FOD, OIP, IPSS). De voorgestelde maatregelen zijn gebaseerd op internationale normen, goede praktijken op het gebied van informatiebeveiliging en de ervaringen van de deelnemers aan de FISP-werkgroep.

Indien strengere maatregelen vereist zijn voor een federale dienst omwille van reglementaire redenen of om andere formele en dwingende redenen, kan men ervan uitgegaan dat deze maatregelen voorrang hebben op de maatregelen die in deze gids worden beschreven.

FISP Werkgroep

.be

INHOUDSTAFEL

Inhoud van het document

Oriëntatie van het document

Dit document maakt integraal deel uit van methodologie voor informatiebeveiliging binnen de Federale overheid (FISP-project).

Veiligheidsdoel van het document

Dit document omschrijft de vereisten om te voldoen aan de beveiliging in de cloud.

Toepassingsgebied

Deze handleiding stelt de overheidsdiensten in staat om de risico's voor de informatieveiligheid in verband met clouddiensten systematisch te identificeren, te analyseren en te beoordelen. Ze beschrijft bovendien controles om deze risico's effectief te beheren.

Vrijwaring

Deze informatie mag niet individueel gebruikt worden als referentiedocumentatie. De lezer van dit document gebruikt dit document niet als vervanger van de wetgeving, maar als leidraad bij nemen van de gepaste beveiligingsmaatregen.

Verantwoordelijkheden

Dit document is bestemd voor de informatieveiligheidsconsulent en voor de functionaris voor de gegevensbescherming (FGB of ook wel DPO) van de openbare instelling van de federale overheid en voor andere belanghebbenden in verwante gebieden.

Eigenaar

De eigenaar van dit document is de FISP-werkgroep.

Inleiding

Cloudcomputerdiensten hebben veel potentiële voordelen voor het publiek en voor overheidsinstanties, zoals schaalbaarheid, elasticiteit, hoge prestaties, kostenefficiëntie, reactiviteit en flexibiliteit.

Het beheer van de veiligheid en het herstellingsvermogen van traditionele IT-omgevingen is meestal zeer uitdagend voor overheidsdiensten. Cloudcomputerdiensten brengen enkele bijkomende uitdagingen mee. Bijvoorbeeld:

- Een gebrek aan duidelijke definities van de cloud, haar diensten en haar verschillende architecturen
- Een gebrek aan certificering van en standaarden voor de beveiliging van de cloud en een onvolledige compatibiliteit met de huidige beveiligingsnormen
- Een gebrek aan een duidelijke taal en methodologie voor de keuze van de best passende cloudcomputerdienst.
- Een gebrek aan een duidelijk begrijp van de implicaties van cloudcomputerdiensten met grensoverschrijdende overdracht van gegevens
- Het verzekeren van de naleving van de nationale wetten en reglementen

Dit beleid is bedoeld om overheidsdiensten een overzicht te geven van de cloudcomputerdiensten en de bijbehorende uitdagingen voor de beveiliging. De unieke architectuur en de grensoverschrijdende aard van de cloudcomputerdiensten vereisen een andere benadering van de privacy- en beveiligingseisen voor persoonsgegevens en de beveiligingseisen voor overheidsgegevens, -transacties en communicatie. Dit document behandelt de dreigingen, de technologische risico's en de beveiligingsmaatregelen voor cloudomgevingen. Het wil de inzichten verstrekken die ICT-besluitvormers nodig hebben om met kennis van zaken te beslissen.[1]

Deze handleiding stelt de overheidsdiensten in staat om de risico's voor de informatieveiligheid in verband met clouddiensten systematisch te identificeren, te analyseren en te beoordelen. Ze beschrijft bovendien controles om deze risico's effectief te beheren. Hoewel dit document de meest courante problemen in verband met cloudcomputerdiensten behandelt, mogen de hier geïdentificeerde risico's niet als volledig worden beschouwd. De overheidsdiensten worden aangemoedigd om mogelijke andere risico's te identificeren en te evalueren die uniek zijn voor hun werkingscontext of voor de clouddiensten die zij van plan zijn te gebruiken.

[1] Cloudbeleid Qatar

Cloud Business Plan

Aangezien elke overheidsdienst uniek is, bestaat er geen eenvormig model voor cloudcomputerdiensten. De overheidsdiensten worden aangemoedigd om deze handleiding op zichzelf te betrekken en ze te gebruiken om hun bedrijfsmodellen voor de cloud te definiëren. Elk overheidsdepartement hoort zijn cloudbeleid individueel te bepalen. Dit moet door het topmanagement van elke overheidsdienst gebeuren, met de hulp van de CISO en de DPO. Met het oog op de bewustmaking aangaande de veiligheidseisen bij het gebruik van cloudcomputerdiensten, moeten hun beslissingen ook gebaseerd zijn op een vergelijkende risicoanalyse van de lokaal beheerde infrastructuren en de cloudsystemen. De beslissingen zullen slechts geloofwaardig zijn wanneer ze voor beide aspecten hetzelfde eisenniveau hanteren en dus van dezelfde basiselementen vertrekken.

De ontwikkeling en implementatie van een **Cloud Business Plan** is aanbevolen. De overheidsdiensten moeten over een plan voor hun gebruik van de clouddiensten beschikken. Dit gedeelte behandelt ook enkele wijzigingen van het ICT-bedrijfmodel die de overheidsdiensten dienen te overwegen. Deze aanbeveling is bedoeld om de overheidsdiensten aan te sporen tot een strategische benadering van het gebruik van cloudcomputerdiensten.

Plannen voor de cloud moeten eerst beschrijven hoe de overheidsdienst de cloudcomputerdiensten wenst te gebruiken om beduidende verbeteringen van de werking te ondersteunen om de klantbeleving te verbeteren, de effectiviteit en efficiëntie te bevorderen, de werking te stroomlijnen of nieuwe leveringsmodellen te ontwikkelen. [2] Het eerste advies voor overheidsdiensten die plannen voor hun cloud ontwikkelen, is om rekening te houden met het volgende:

- Bedrijfsstrategie: openbare clouddiensten moeten uitgelijnd zijn met de bestaande strategieën van de overheidsdienst. Het moet duidelijk zijn hoe deze diensten zullen worden gebruikt om beduidende verbeteringen van de werking te ondersteunen. Een benadering per sector moet worden overwogen.
- **Risicobereidheid:** de risicobereidheid van de overheidsdienst in het gebruik van cloudcomputerdiensten moet duidelijk zijn, in de context van de privacy, de rechtspraak, de beveiliging en de wetgevende overwegingen.
- **Governance en identiteit**: het moet duidelijk zijn hoe de gegevensgovernance, met inbegrip van identiteits- en toegangsbeheer, in meerdere cloudcomputerdiensten zal worden toegepast.
- **Overwegingen met betrekking tot de enterprise- en de technologiearchitectuur**: het moet duidelijk zijn hoe het gebruik van cloudcomputerdiensten de enterprisearchitectuur en de technologiestrategie van uw organisatie zal beïnvloeden en welke technologie- en proceswijzigingen uw organisatie nodig heeft om de veilig met cloudcomputerdiensten te werken.
- **ICT-werkingsmodel**: het nagestreefde werkingsmodel voor uw ICT-functie en het plan voor de overschakeling naar dat model moeten worden gedefinieerd.
- **Maturiteit van de organisatie**: de ondersteunende functies van uw dienst die verder moeten worden ontwikkeld om het gebruik van openbare cloudcomputerdiensten te ondersteunen, moeten worde gedefinieerd (bijvoorbeeld commerciële of juridische functies, architectuur, IT-beveiliging).

[2] Hier vindt u een voorbeeld van de ontwikkeling en implementatie van een businessplan voor de cloud: https://snapshot.ict.govt.nz/resources/digital-ict-archive/static/localhost_8000/guidance-and-resources/using-cloud-services/develop-and-implement-a-cloud-plan/implementing-the-cloud-plan/index.html
(de inhoud van 'ict.govt.nz' wordt gemigreerd naar 'digital.govt.nz', zodat de link binnenkort verouderd zou kunnen zijn)

- **Operationele processen**: de manier waarop de overheidsdienst het gebruik van openbare cloudcomputerdiensten systematisch benadert, met inbegrip van het beheer van de risico's die de diensten meebrengen, zonder een beroep te doen op een IT-team (shadow cloud) moet worden gedefinieerd.
- **Stappenplan**: de openbare cloudcomputerdiensten met de hoogste prioriteit voor de overheidsdienst moeten worden gedefinieerd, samen met het tijdskader voor hun toepassing.

Wat is de cloud?

De Belgische overheid gebruikt de definitie van cloudcomputerdiensten van het National Institute of Science and Technology (NIST):

> "Een model voor het snel beschikbaar stellen van overal beschikbare on-demand netwerktoegang tot een gedeelde pool van configureerbare IT-middelen zoals netwerken, servers, opslag, applicaties en diensten, met een minimum aan managementinspanning of interactie met de dienstverlener."

Cloud computing omvat vijf essentiële kenmerken, drie servicemodellen en vier implementatiemodellen. Dit gedeelte geeft een beknopt overzicht van de essentiële kenmerken van cloud computing, de clouddiensten en de implementatiemodellen. Het is aanbevolen dat de overheidsdiensten zich vertrouwd maken met de definities van het NITS, om te verzekeren dat zij de risico's van de verschillende clouddiensten en implementatiemodellen kunnen identificeren en gebruiken.

De cloudinfrastructuur moet worden begrepen als het geheel van hardware en software dat de vijf essentiële kenmerken van cloud computing mogelijk maakt. De cloudinfrastructuur kan worden gezien als samengesteld uit een fysieke en een abstracte laag. De fysieke laag bestaat uit de hardwaremiddelen die nodig zijn om de geleverde clouddiensten te ondersteunen. De abstracte laag bestaat uit de software die op de fysieke laag wordt toegepast.

4.1. Door het NITS gedefinieerde kenmerken van cloud computing:

On-demand selfservice	De consument kan gebruikmaken van verscheidene computerfuncties die hij nodig heeft (bv. een virtuele server of een e-mailaccount). Deze functies kunnen volledig online beschikbaar zijn, zonder interactie met personeel van de dienstverlener.
Uitgebreid netwerktoegang	De diensten zijn op het netwerk beschikbaar en de toegang wordt op meerdere platformen ondersteund (bv. mobiele telefoons, tablets, laptops en werkstations).
Pool van middelen	De middelen die de leverancier van cloud computing aanbiedt, worden samengevoegd om meerdere consumenten tegelijk te bedienen. De consumenten kunnen zich overal ter wereld bevinden. Voorbeelden van middelen zijn opslag, verwerking, geheugen en bandbreedte op het netwerk.
Schaalbaarheid	Middelen in de cloud kunnen gemakkelijk worden aangeschaft en vrijgegeven. Voor de consument kunnen de middelen onbeperkt lijken en op elk ogenblik in om het even welke hoeveelheid beschikbaar worden gemaakt.
Meetbare diensten	Cloudsystemen controleren en optimaliseren het gebruik van middelen automatisch. De consumenten betalen alleen de middelen die zij werkelijk in de dienst gebruiken. Het gebruik van de middelen kan worden gemonitord, gecontroleerd en gerapporteerd, zodat het transparant is voor zowel de leverancier als de consument.

4.2. Door het NITS gedefinieerde servicemodellen van cloud computing

Software as a Service (SaaS).	Dit model stelt de overheidsdienst in staat om gebruik te maken van de toepassingen van de clouddienstverlener die op een cloudinfrastructuur worden uitgevoerd. De softwaretoepassingen zijn via een webinterface of een desktoptoepassing online toegankelijk. De consument heeft geen controle over de onderliggende hardwareconfiguratie. **Voorbeelden van SaaS:** de Office Productivity as a Service (OPaaS) van de overheid, Microsoft Office 365, Google Apps, Salesforce.com en Oracle Applications Cloud. **Een ander voorbeeld** als Community Cloud (zie hieronder **4.3. Implementatiemodellen)**: G-Cloud "Componenten en toepassingen": https://www.gcloud.belgium.be/fr/services#service-2
Platform as a Service (PaaS).	Dit model stelt de overheidsdienst in staat om een door de overheidsdienst ontwikkelde of aangeschafte toepassingen op de cloudinfrastructuur uit te rollen of te installeren, met de voorwaarde dat de toepassing wordt ontwikkeld aan de hand van door de clouddienstverlener ondersteunde programmeertalen, bibliotheken, diensten en tools. De klant heeft geen controle over de onderliggende hardwareconfiguratie, de opslag, het netwerk, het besturingssysteem of de lagen van het beheer. **Voorbeelden van PaaS**: de Desktop as a Service (DaaS) van de overheid, Google App Engine, Microsoft Windows Azure, Force.com en Oracle Database Cloud. **Een ander voorbeeld** als Community Cloud (zie hieronder **4.3. Implementatiemodellen)**: G-Cloud "Platformen": https://www.gcloud.belgium.be/fr/services#service-3
Infrastructure as a Service (IaaS).	Dit model stelt de overheidsdienst in staat om verwerking, opslag, netwerken en andere computermiddelen te gebruiken waarbij de consument om het even welke software kan installeren en uitvoeren, eventueel met inbegrip van besturingssystemen en toepassingen. De overheidsdienst kan de onderliggende infrastructuur niet beheren of controleren, maar controleert wel de besturingssystemen, de opslag en de geïmplementeerde toepassingen. **Voorbeelden van IaaS:** de IaaS-platformen van de overheid, Amazon Web Services (AWS), Elastic Cloud Compute (EC2), Google Compute Engine. **Een ander voorbeeld** als Community Cloud (zie hieronder **4.3. Implementatiemodellen)**: G-Cloud "Harde infrastructuur": https://www.gcloud.belgium.be/fr/services#service-5

4.3. Door het NITS gedefinieerde implementatiemodellen

Private cloud.	De cloudinfrastructuur dient voor exclusief gebruik door een enkele organisatie/overheidsdienst met meerdere consumenten (bv. verschillende departementen). Ze kan eigendom zijn van, worden beheerd en uitgebaat door de organisatie, een derde partij of een combinatie van de twee, en kan zich in of buiten de lokalen van de organisatie bevinden. Ze kan zich ook in of buiten het land bevinden.
Community cloud.	De cloudinfrastructuur dient voor exclusief gebruik door een specifieke gemeenschap/sector van consumenten uit organisaties met taken en plichten van dezelfde aard (bv. dezelfde missie, ICT-veiligheidseisen, wettelijke en sectorspecifieke complianceoverwegingen). Ze kan eigendom zijn van, worden beheerd en uitgebaat door een of meer organisaties van de gemeenschap, een derde partij of een combinatie van de twee, en kan zich in of buiten de lokalen van een organisatie bevinden. Ze kan zich ook in of buiten het land bevinden. (bv. Extranet)
Public cloud.	De cloudinfrastructuur dient voor open gebruik door om het even welke organisatie. Ze kan eigendom zijn van, worden beheerd en uitgebaat door een privé-organisatie of openbare organisaties of een combinatie van de twee. Ze bevindt zich in de lokalen van de clouddienstverlener.
Hybrid cloud.	De cloudinfrastructuur is samengesteld uit twee of meer verschillende cloudinfrastructuren (private, community of public) die afzonderlijke entiteiten blijven maar met elkaar verbonden zijn door een gestandaardiseerde of eigen technologie die de draagbaarheid van gegevens en toepassingen mogelijk maakt (bv. taakverdeling tussen clouds).

Ken de Shadow Cloud!

Het begrip "shadow cloud" verwijst naar publieke clouddiensten die werknemers buiten het weten en zonder de goedkeuring van de organisatie gebruiken. Het gebruik van persoonlijke mobiele toestellen voor zakelijke doeleinden is een voorbeeld van "shadow IT". Werknemers kunnen hun eigen toestellen voor het werk gebruiken zonder dat de ICT-functie van de organisatie het weet of goedkeurt.

Een niet-beheerde shadow cloud kan net als niet-beheerde shadow IT gevaarlijk zijn voor de overheidsdiensten. Maar wanneer ze correct wordt beheerd, kan ze het engagement van de werknemers bevorderen en de efficiëntie verbeteren terwijl de bijbehorende risico's worden beheerd. De shadow cloud moet niet alleen worden beheerd om haar risico's tot het minimum te beperken maar ook om haar voordelen te benutten.[3]

Gelet op het toenemende belang en de groeiende afhankelijkheid van technologie, moeten de overheidsdiensten de omvang van de shadow cloud in hun organisatie beoordelen, de opportuniteiten en risico's meedelen en passende maatregelen identificeren om het probleem aan te pakken. Gemakkelijk te gebruiken publieke clouddiensten zoals DropBox hebben de scheidingslijnen tussen persoonlijke en zakelijke toepassingen vervaagd. Hoewel toepassingen in de shadow cloud vaak valabel kunnen worden benut, heeft hun toenemende gebruik een aantal implicaties, zoals:

- verlies of compromitteren van gegevens als gevolg van slecht ontworpen, slecht beheerde of kwaadwillige diensten die de gegevens of infrastructuur van de organisatie aan onvoorziene risico's blootstellen;
- verlies van gegevens doordat de informatie over meerdere diensten wordt verspreid en minder goed toegankelijk is voor het geheel van de organisatie (dit kan tot gegevensverlies leiden wanneer diensten worden stopgezet, werknemers vertrekken en men niet meer weet waar de gegevens zich bevinden);
- hogere kosten door het gebruik van meerdere publieke clouddiensten voor dezelfde functie; ze kunnen duur zijn en misschien geen volumeprijzen mogelijk maken (andere potentiële kosten zijn die van het herstel, de recuperatie en de remediëring indien een clouddienst de informatie of de infrastructuur van de organisatie in het gedrang brengt).

Het is mogelijk dat overheidsdiensten weinig zichtbaarheid of controle hebben op welke diensten worden gebruikt en voor welke gegevens dat gebeurt, en dat er weinig commerciële garanties van de beschikbaarheid van de gegevens zijn. Dit leidt tot onzekerheid over de bijbehorende risico's. Het is nuttig om te erkennen dat in het gebruik van de shadow cloud door werknemers van de overheid een onderscheid kan worden gemaakt tussen zakelijke en persoonlijke doeleinden.

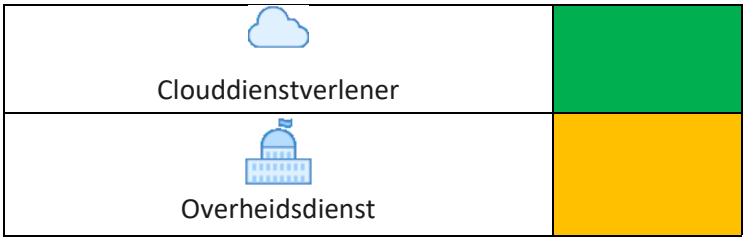
[3] Hier vindt u een voorbeeld van het beheer van de shadow cloud: https://snapshot.ict.govt.nz/resources/digital-ict-archive/static/localhost_8000/assets/Uploads/Shadow-Cloud-Guidance2.pdf (de inhoud van "ict.govt.nz" wordt gemigreerd naar "digital.govt.nz", zodat de link binnenkort verouderd zou kunnen zijn)

Aansprakelijkheid van de overheidsdienst voor de veiligheid in cloudcomputingomgevingen

Afhankelijk van het gekozen cloudmodel, kan een overheidsdienst die een IaaS-dienst gebruikt de volledig controle behouden over – en dus verantwoordelijk zijn voor – de courante beveiliging en het onderhoud van alle besturingssystemen, toepassingen, virtuele configuraties (met inbegrip van de hypervisor en de virtuele beveiligingsapparaten) en gegevens.

Het is belangrijk dat men begrijpt dat overheidsdiensten weliswaar de verantwoordelijkheid voor de toepassing, het beheer en het onderhoud van veiligheidscontroles aan een dienstverlener kan uitbesteden, maar niet hun aansprakelijkheid voor passende bescherming van hun gegevens. De clouddienstverlener draagt een adaptieve operationele aansprakelijkheid, afhankelijk van de keuze van de cloudcomputingomgeving, maar de overheidsdienst blijft de wettelijk aansprakelijke instantie voor de gegevensbescherming. De overheidsdienst moet met de clouddienstverlener een passende verdeling van de rollen en verantwoordelijkheden voor de informatieveiligheid overeenkomen en bevestigen dat de clouddienstverlener de hem toegekende rollen en verantwoordelijkheden kan vervullen. De rollen en verantwoordelijkheden voor de informatieveiligheid van beide partijen moeten in een overeenkomst worden opgenomen.[4]

Het volgende schema toont hoe de aansprakelijkheid van een overheidsdienst afhankelijk van het cloudmodel kan verschillen.



Aansprakelijkheid	Terplekke	IAAS	PAAS	SAAS
Gegevensclassificatie en -aansprakelijkheid				
Bescherming van de client en het eindpunt				
Identiteits- en toegangsbeheer				
Controles op toepassingsniveau				
Netwerkcontroles				
Hostinfrastructuur				
Fysieke beveiliging				

[4] Iso 27027

De volgende tabel geeft een overzicht van de verantwoordelijkheidsgrens voor elk van de servicemodellen:

Software as a Service (SaaS).	In het SaaS-model heeft de overheidsdienst een zeer beperkte controle over de veiligheid. Meestal is de overheidsdienst verantwoordelijk voor het beheer van zijn gebruikersaccounts, om te verzekeren dat zij uitsluitend over de machtigingen beschikken die ze nodig hebben om hun taken uit te voeren. De dienstverlener is verantwoordelijk voor de toepassing van alle andere veiligheidscontroles en voor het verzekeren van een passend beveiligingsniveau.
Platform as a Service (PaaS).	Het PaaS-model bouwt voort op het IaaS-model en breidt het uit met het gastbesturingssysteem en de toepassingsservices. De dienstverlener is bijgevolg ook verantwoordelijk voor de implementatie, het beheer en het onderhoud van de veiligheidscontroles die deze componenten beschermen. De overheidsdiensten zijn verantwoordelijk voor de veiligheid van de toepassingen die zij in de PaaS-omgeving implementeren.
Infrastructure as a Service (IaaS).	De dienstverlener is verantwoordelijk voor de toepassing, het beheer en het onderhoud van de controles voor de informatieveiligheid, tot en met de virtualisatie-hypervisorlaag (nl. de onderliggende infrastructuur). De overheidsdiensten zijn verantwoordelijk voor de toepassing van passende veiligheidscontroles voor de bescherming en het onderhoud van alle componenten boven de hypervisorlaag, met inbegrip van het gastbesturingssysteem, de toepassingsservices en de toepassingen die zij in de IaaS-omgeving implementeren.

Veiligheidslandschap van de cloud[5]

Clouddiensten en traditionele niet-clouddiensten brengen soortgelijke veiligheidsproblemen mee, maar in cloud computing worden ze versterkt door het bestaan van een externe controle over de middelen van de organisatie en het potentiële wanbeheer van die middelen. Wanneer men overschakelt naar publieke cloud computing, is er ook een overdracht aan de clouddienstverlener van de verantwoordelijkheid voor en de controle over de informatie en de systeemcomponenten die voordien rechtstreeks door de overheidsdienst werden gecontroleerd. De overheidsdienst blijft evenwel verantwoordelijk voor zijn gebruik van clouddiensten. Het is in het beste belang van de organisatie dat zij op de hoogte blijft van de situatie, alternatieven onderzoekt, prioriteiten bepaalt en haar beveiliging aanpast. Een aantal veiligheidsrisico's van cloud computing moet passend worden aangepakt:[6]

● **Verlies van eigendom van de governance**. In de publieke cloud staan de klanten de controle over een aantal zaken die de veiligheid en de privacy kunnen beïnvloeden af aan de clouddienstverlener. Soms bevatten de overeenkomsten voor clouddiensten echter geen verbintenis vanwege de clouddienstverlener om deze zaken op te lossen, zodat de veiligheid wordt verzwakt.

● **Dubbelzinnigheid over de verantwoordelijkheid.** De verantwoordelijkheid voor aspecten van de veiligheid en de privacy kunnen door de clouddienstverlener en de klant worden gedeeld, met de mogelijkheid dat vitale delen van de verdediging worden verwaarloosd als de verantwoordelijkheden niet duidelijk worden toegewezen en afgebakend. De verdeling van de verantwoordelijkheden zal waarschijnlijk verschillen volgens het gebruikte model van clouddiensten (bv. IaaS versus SaaS).

● **Authenticatie en autorisatie**. Het feit dat gevoelige middelen in de cloud van overal in cyberspace toegankelijk zijn, vergroot de noodzaak om de identiteit van een gebruiker met zekerheid vast te stellen – vooral als de gebruikers werknemers, aannemers, partners en klanten kunnen zijn. Een sterke authenticatie en autorisatie worden cruciale aandachtspunten.

● **Isolatiefalen.** Multi-tenant en gedeelde middelen zijn typische kenmerken van de publieke cloud. Deze risicocategorie omvat het falen van mechanismen voor de scheiding van het gebruik van opslagruimte, geheugen, routing en zelfs reputatie tussen tenants.

● **Compliance- en juridische risico's.** De investering van de cloudklant in certificeringen (bv. om de naleving van de industriestandaarden of regulatoire eisen aan te tonen) kan verloren gaan als de clouddienstverlener zijn eigen naleving van de relevante eisen niet kan bewijzen. De klant moet verifiëren dat de v over passende en relevante certificeringen beschikt.

● **Behandeling van veiligheidsincidenten.** De opsporing, rapportage en aansluitend beheer van veiligheidsincidenten kunnen aan de clouddienstverlener worden gedelegeerd, maar deze incidenten hebben een impact op de klant. In de overeenkomst voor de clouddiensten moeten regels voor de kennisgeving worden opgenomen, zodat de klanten niet worden verrast en niet met onaanvaardbare vertragingen te maken krijgen.

---

[5] CSCC-Security for Cloud Computing 10 Steps to Ensure Success: https://www.omg.org/cloud/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf

[6] Bron: European Network and Information Security Agency (ENISA). Bezoek http://www.enisa.europa.eu/ voor meer informatie.

● **Kwetsbaarheid van de beheersinterface.** Interfaces voor het beheer van middelen in de publieke cloud (zoals zelfvoorziening) zijn meestal via het internet toegankelijk. Aangezien ze toegang geven tot meer middelen dan traditionele hostingleveranciers, impliceren ze ook een groter risico, zeker in combinatie met toegang op afstand en beveiligingsproblemen van webbrowsers.

● **Bescherming van toepassingen.** Toepassingen worden traditioneel beveiligd met oplossingen voor bescherming in de diepte, met een duidelijke afbakening tussen de fysieke en de virtuele middelen en met veilige zones. Wanneer zij de verantwoordelijkheid voor de veiligheid van de infrastructuur aan de clouddienstverlener delegeren, moeten organisaties hun perimeterbeveiliging op netwerkniveau aanpassen en meer controles invoeren op het niveau van de gebruikers, de toepassingen en de gegevens. Een werkbelasting die in de cloud wordt uitgevoerd, moet hetzelfde niveau van controle van de gebruikerstoegang en beveiliging hebben als een werkbelasting die in traditionele datacenters wordt uitgevoerd. Dit vereist de ontwikkeling en het beheer van een op de werkbelasting gericht beleid en de toepassing van een gecentraliseerd beheer op gedistribueerde werkbelastingen.

● **Gegevensbescherming.** De belangrijkste aandachtspunten zijn de blootstelling of vrijgave van persoonsgegevens en/of gevoelige gegevens, het verlies of de onbeschikbaarheid van gegevens en een te lange bewaring van gegevens. Het kan voor de overheidsdienst (in de rol van verwerkingsverantwoordelijke) moeilijk zijn om de verwerkingspraktijken van de clouddienstverlener effectief te controleren. Dit probleem wordt verergerd in het geval van multipele gegevenstransfers (bv. tussen meerdere clouddiensten, of wanneer een clouddienstverlener onderaannemers en externe leveranciers gebruikt). Dit leidt tot een gebrek aan transparantie van de eigendom en onduidelijkheid over de doeleinden van de gegevensverwerking.

● **Regulering van de persoonsgegevens.** In de meeste jurisdicties is het gebruikelijk dat persoonsgegevens volgens wettelijke en/of reglementaire eisen moeten worden verwerkt. Dit gaat nu meestal verder dan de bescherming van persoonsgegevens en omvat ook de rechten van de betrokkenen om hun gegevens te raadplegen, te corrigeren of te verwijderen – en in sommige gevallen te eisen dat hun gegevens naar elders worden overgedragen. Elk gebruik van clouddiensten voor de bewaring of verwerking van persoonsgegevens moet aan deze eisen voldoen en tegelijkertijd de gegevens veilig houden.

● **Kwaadwillig gedrag van insiders**. Kwaadwillige handelingen van personen binnen de organisatie kan ernstige schade veroorzaken, aangezien deze personen over toegangsrechten en machtigingen beschikken. Dit wordt verergerd in de cloudcomputingomgeving, waar dergelijke activiteiten zowel in de organisatie van de klant als in die van de dienstverlener kunnen plaatsvinden.

● **Faillissement van de dienstverlener.** Een faillissement kan voor de werking van de klant essentiële gegevens en toepassingen gedurende een lange periode onbeschikbaar maken.

● **Onbeschikbaarheid van de dienst.** Ze kan worden veroorzaakt door storingen van hardware, software of communicatienetwerken.

● **Leveranciersvergrendeling.** De afhankelijkheid van de eigen diensten van een gegeven clouddienstverlener kan ertoe leiden dat de klant aan die dienstverlener gebonden is. Het gebrek aan draagbaarheid van toepassingen en gegevens tussen dienstverleners schept een risico van de onbeschikbaarheid van gegevens en diensten wanneer men van dienstverlener verandert. Dit is dus een belangrijk maar soms over het hoofd gezien aspect van de beveiliging. Het gebrek aan interoperabiliteit van de interfaces van de clouddiensten bindt de klant eveneens aan een gegeven dienstverlener en kan de overstap naar een andere dienstverlener bemoeilijken.

● **Onveilige of onvolledige verwijdering van gegevens**. Het is mogelijk dat bij de beëindiging van een contract met een dienstverlener de gegevens van de klant niet van de systemen van de dienstverlener of diens derde partijen worden verwijderd. Meestal bestaan er back-upkopieën van de gegevens, die op dezelfde media met gegevens van andere klanten gemengd kunnen zijn, zodat men ze moeilijk selectief kan wissen. Het grote voordeel van multi-tenancy (het delen van hardware middelen) vormt dus een groter risico voor de klant dan het gebruik van eigen hardwaren.

● **Zichtbaarheid en audit**. Sommige bedrijfsgebruikers scheppen een "schaduw-IT" door zonder de expliciete toestemming van de organisatie met behulp van clouddiensten IT-oplossingen te ontwikkelen. De grote uitdagingen voor het beveiligingsteam bestaan erin elk gebruik van clouddiensten in de organisatie te kennen (bv. welke middelen worden gebruikt, waarom, in welke mate en door wie), te begrijpen welke wetten, reglementen en beleidsregels op dat gebruik van toepassing kunnen zijn, en de veiligheidsaspecten van het gebruik regelmatig te beoordelen.

Minimale veiligheids- en privacyoverwegingen

Voorgestelde maatregelen om aan de overwegingen te voldoen

Overheidsdiensten kunnen ook overwegen welke certificeringen bruikbaar en relevant zijn, en of ze wel of niet hun vertrouwen vergroten in het vermogen van de dienstverlener om hun informatie te beschermen. Het is essentieel dat de overheidsdienst begrijpt of de certificering volgens een internationaal erkende standaard of een internationaal erkend kader een zekerheid geeft dat de dienstverlener aan zijn veiligheidseisen voldoet. Het bereik van de certificering moet overeenstemmen met de diensten die de clouddienstverlener de overheidsdienst aanbiedt. Verder in deze handleiding wordt voor elk specifiek veiligheidsdoel een niet-limitatief aantal maatregelen voorgesteld.

> Zo kunnen dienstverleners die als compliant met de eisen van ISO/IEC 27001 gecertificeerd zijn het bereik van de audit definiëren aan de hand van een toepasselijkheidsverklaring. Daarom moeten overheidsdiensten nagaan precies welke controles de audit omvat, door de dienstverlener een exemplaar van het laatste externe auditrapport te vragen (met inbegrip van het bereik of de toepasselijkheidsverklaring), samen met de resultaten van alle recente interne audits.
>
> Een andere potentiële bron van informatie over de veiligheidscontroles die een dienstverlener toepast is het Security, Trust & Assurance Register van de Cloud Security Alliance (CSA STAR). De mate van zekerheid hangt af van het niveau dat de dienstverlener in het Open Certification Framework (OCF) van de CSA bereikt heeft.

Enisa (het European Network and Information Security Agency) geeft een overzichtstabel die veiligheidsdoelen aan verschillende certificeringen koppelt.[7]

[7] https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers/

Details van de aansprakelijkheid voor een veiligheidsdoel

Waar mogelijk wordt meer gedetailleerde informatie gegeven over de aansprakelijkheid voor de veiligheidsdoelen op basis van ISO/IEC 27017.

Waarde, kritikaliteit en gevoeligheid van de informatie

Om de risico's van het gebruik van een clouddienst te kunnen beoordelen, moeten de overheidsdiensten de waarde, de kritikaliteit en de gevoeligheid kennen van de informatie die zij in de dienst wensten te plaatsen.

Voor deze veiligheidsdoelstelling moet men rekening houden met de volgende overwegingen:

- de eigenaar van de informatie in het bedrijf moet geïdentificeerd zijn;
- het bedrijfsproces dat door de informatie wordt ondersteund, moet geïdentificeerd zijn;
- er moet een veiligheidsclassificatie van de informatie bestaan;
- er moeten richtlijnen voor de bescherming van officiële informatie bestaan;
- specifieke aandachtspunten met betrekking tot de vertrouwelijkheid van de door de clouddienst te bewaren of verwerken informatie moeten geïdentificeerd zijn;
- het moet duidelijk zijn of de gegevens persoonsgegevens bevatten;
- de gebruikers van de informatie in het bedrijf moeten geïdentificeerd zijn;
- de machtigingen die de gebruikers voor de informatie nodig hebben (lezen, schrijven, wijzigen en/of verwijderen) moeten duidelijk zijn.
- de wetgeving die op de informatie van toepassing is, moet duidelijk zijn;
- de contractuele verplichtingen die op de informatie van toepassing zijn, moeten duidelijk zijn;
- de impact op het bedrijf van een ongeoorloofde openbaarmaking van informatie moet geïdentificeerd zijn;
- de impact op het bedrijf van een inbreuk op de integriteit van de informatie moet geïdentificeerd zijn;
- de overheidsdienst moet over plannen voor incidentrespons en -beheer beschikken om de impact van een ongeoorloofde openbaarmaking tot het minimum te beperken;
- de impact op het bedrijf van de onbeschikbaarheid van informatie moet duidelijk zijn;

Voorgestelde maatregelen om aan de overwegingen te voldoen:

- De veiligheidscontrole van de Cloud Control Matrix[8]: DSI-01, DSI-02, DSI-03, DSI-04, DSI-05,DSI-06, DSI-07

Details van de aansprakelijkheid voor deze veiligheidsdoelstelling:

Overheidsdienst	Clouddienstverlener
De overheidsdienst moet informatie en aanverwante middelen die in de cloudcomputingomgeving worden bewaard, labelen volgens de door bij de overheidsdienst toepasselijke procedures. Indien van toepassing kunnen door de clouddienstverlener voorziene functies die labeling ondersteunen worden gebruikt.	De clouddienstverlener moet elke functie van de dienst die hij levert documenteren en openbaar maken, zodat de overheidsdienst zijn informatie en aanverwante middelen kan classificeren en labelen.

[8] Geleverd door de Cloud Working Group (voorheen: Cloud Security Alliance) van de Object Management Group (OMG) https://cloudsecurityalliance.org/research/working-groups/cloud-controls-matrix/

Gegevenssoevereiniteit

Het gebruik van clouddiensten die zich buiten de Belgische jurisdictie bevinden of die eigendom zijn van buitenlandse ondernemingen impliceert risico's voor de gegevenssoevereiniteit. Dit betekent dat gegevens die door de dienst worden bewaard, verwerkt of verzonden onderworpen kunnen zijn aan wetten en reglementen in de landen waar de gegevens worden bewaard, verwerkt en verzonden. Evenzo kan een dienstverlener in buitenlands eigendom die in België een dienst verzorgt onderworpen zijn aan de wetten van het land waar zijn maatschappelijke zetel gevestigd is.

De wetten die kunnen worden gebruikt om toegang te krijgen tot door de dienstverlener gehouden informatie kunnen van land tot land verschillen. In sommige gevallen kan de wet een dienstverlener verbieden om zijn klanten te informeren wanneer een buitenlandse wetshandhavingsinstantie hem verplicht om gegevens van die klanten te verstrekken. Daarom is het van kritiek belang dat de overheidsdienst weet in welke jurisdicties zijn gegevens zullen worden bewaard, verwerkt of verzonden. Hij moet ook de impact van de wetten van die landen kennen op de vertrouwelijkheid, integriteit, beschikbaarheid en privacy van de informatie.

Als de dienstverlener enig aspect van de levering van de dienst aan een derde partij uitbesteedt of in onderaanneming geeft, moet de overheidsdienst ook nagaan of dat bijkomende risico's voor de gegevenssoevereiniteit inhoudt.

Privacy-informatie die in jurisdicties buiten België wordt bewaard, kan onderworpen zijn aan de privacy- en gegevensbeschermingswetten van de landen waar de clouddienst wordt geleverd. Ondanks de AVG kunnen de privacy- en gegevensbeschermingswetten in de Europese Unie nog altijd van land tot land verschillen. Daarom is het belangrijk dat de overheidsdienst onderzoekt hoe de wetten van die landen de privacy van de informatie van zijn werknemers en/of klanten kunnen beïnvloeden.

Voor deze veiligheidsdoelstelling moet men rekening houden met de volgende overwegingen:

- de maatschappelijke zetel van de dienstverlener moet gekend zijn;
- de landen van waaruit de clouddiensten worden geleverd, moeten gekend zijn;
- de jurisdicties waar de gegevens van de overheidsdienst zullen worden bewaard en verwerkt moeten gekend zijn;
- de dienstverlener moet toestaan dat zijn klanten specificeren op welke locaties hun gegeven wel en niet mogen worden bewaard en verwerkt;
- als de dienst afhankelijk is van een derde partij (bv. outsourcers, onderaannemers of een andere dienstverlener) die bijkomende juridische risico's meebrengt, moet de dienstverlener voor elke derde partij die bij de levering van de dienst betroken is de volgende gegevens verstrekken:
    - de maatschappelijke zetel van de derde partij;
    - het land of de landen van waaruit de diensten van de derde partij worden geleverd; en
    - de toegang die de derde partij heeft tot de door de clouddienst bewaarde, verwerkte en verzonden klantgegevens;
- de wetten van het of de landen waar de gegevens zullen worden bewaard en verwerkt, moeten worden onderzocht om te beoordelen hoe zij de veiligheid en/of de privacy van de informatie kunnen beïnvloeden;
- de wetten moeten feitelijk toepasselijk zijn op de dienstverlener en/of zijn klantinformatie;
- de manier waarop de dienstverlener omgaat met verzoeken van overheidsdiensten om klantinformatie te raadplegen, moet gekend zijn;

Voorgestelde maatregelen om aan de overwegingen te voldoen:

- ISO/IEC 27001 en ISO/IEC 27018 kunnen overheidsdiensten helpen om toereikend aan de gegeven overwegingen te voldoen.

Details van de aansprakelijkheid voor deze veiligheidsdoelstelling:

Overheidsdienst	Clouddienstverlener
De overheidsdienst moet de autoriteiten identificeren die relevant zijn voor de gecombineerde werking van de overheidsdienst en de clouddienstverlener.	De clouddienstverlener moet de overheidsdienst informeren over de geografische locaties van zijn organisatie en over de landen waar de clouddienst de gegevens van de overheidsdienst kan bewaren.

Privacy

Overheidsdiensten die van plan zijn om persoonsgegevens in een clouddienst te plaatsen, moeten een Data Protection Impact Assessment (DPIA) uitvoeren om te verzekeren dat zij mogelijke privacyrisico's die het gebruik van de dienst meebrengt identificeren en weten elke controles ze moeten toepassen om de risico's effectief te beheren.

Clouddiensten kunnen de overheidsdiensten helpen om opportuniteiten voor het delen van informatie te benutten. Zo kunnen persoonsgegevens gemakkelijk met een andere overheidsdienst worden gedeeld door in een SaaS-oplossing gebruikersaccounts met passende machtigingen aan te maken, zodat men geen interface voor de uitwisseling van informatie tussen de systemen moet implementeren.

Hoewel clouddiensten de technische barrières voor het delen van informatie kunnen verlagen, moeten de overheidsdiensten verzekeren dat zij de toegang tot persoonsinformatie passend beheren en aan de eisen van de Algemene Verordening Gegevensbescherming (AVG) en van de Belgische wet voor de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens voldoen. De overheidsdiensten moeten er zeker van zijn dat de clouddienstverlener deze verordening en wet naleeft, zo niet lopen ze gevaar op zware boetes.

Aangezien gegevensinbreuken wel degelijk voorkomen en de overheidsdienst verantwoordelijk is voor de bescherming van alle persoonsgegevens die hij houdt, is het belangrijk dat de overheidsdienst alles in het werk stelt om die gegevens te beschermen voor hij in apps en opslag in de cloud plaatst.

Zelfs als blijkt dat een clouddienst de AVG heeft overtreden, kan de overheidsdienst nog altijd aansprakelijk worden gesteld als verwerkingsverantwoordelijke. De overheidsdienst moet dus de beveiligingsmaatregelen die de clouddienstverlener in het kader van de naleving van de AVG waarborgt zorgvuldig onderzoeken.

Voor deze veiligheidsdoelstelling moet men rekening houden met de volgende overwegingen:

- Men moet weten of de gegevens die door de clouddienst zullen worden bewaard en verwerkt persoonsgegevens volgens de definitie van de AVG bevatten;
- men moet een Data Protection Impact Assessment (DPIA) uitvoeren om de privacyrisico's van het gebruik van een clouddienst en de controles voor hun effectieve beheer te identificeren;
- het gebruik van persoonsgegevens door de dienstverlener moet duidelijk uiteengezet zijn in zijn privacybeleid;
- het beleid moet consistent zijn met de wettelijke verplichtingen van de overheidsdienst volgens de AVG;

- het moet duidelijk zijn waar de overheidsdienst, zijn personeel en/of klanten klacht kunnen indienen in het geval van een inbreuk op de privacy;
- de overheidsdienst moet regelmatige audits plannen om te verzekeren dat de gebruikte systemen en diensten compliant blijven met de AVG;

Voorgestelde maatregelen om aan de overwegingen te voldoen:

- ISO/IEC 27001 en ISO/IEC 27018 kunnen overheidsdiensten helpen om toereikend aan de gegeven overwegingen en aan de Algemene Verordening Gegevensbescherming te voldoen.
- ISO/IEC 27701, Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines, bepaalt de eisen voor het ontwerp, de implementatie, het onderhoud en de doorlopende verbetering van een privacyspecifiek systeem voor het beheer van de informatieveiligheid. Het is een soort beheerssysteem voor de bescherming van persoonsgegevens.

Details van de aansprakelijkheid voor deze veiligheidsdoelstelling:

- Voor meer informatie over Privacy bevelen wij het FISP- Privacy-vademecum aan.

Governance

De voorgestelde acties voor cloudgovernance zijn:

- Een praktische gids voor cloudgovernance is hier te vinden: https://www.omg.org/cloud/deliverables/practical-guide-to-cloud-governance.pdf
- De veiligheidscontrole van de Cloud Control Matrix: GRM-01

Dienstvoorwaarden:

Anders dan in traditionele outsourcingmodellen zullen de klanten misschien niet altijd de mogelijkheid hebben om over alle contractuele voorwaarden met de dienstverlener te onderhandelen, vooral in het geval van publieke clouddiensten. De primaire governancecontrole waarover overheidsdiensten beschikken, zijn de Dienstvoorwaarden (of het contract) van de dienstverlener, de bijbehorende overeenkomst inzake dienstverleningsniveau (Service Level Agreement of SLA), en de sleutelprestatie-indicatoren (Key Performance Indicators of KPI) en metingen die de prestaties van de dienst aantonen. Men moet ze zorgvuldig onderzoeken om te verzekeren dat de dienst kan voldoen aan de verplichtingen van de overheidsdienst om de vertrouwelijkheid, integriteit en beschikbaarheid te beschermen van zijn officiële informatie en van de privacy van alle persoonlijke identificeerbare informatie die hij in de clouddienst zal plaatsen.

Om een mate van controle over de in de clouddienst bewaarde gegevens te kunnen uitoefenen, moet de overheidsdienst de eigendom van zijn gegevens behouden en weten hoe de dienstverlener de gegevens in het kader van de levering van de dienst zal gebruiken. Het is mogelijk dat dienstverleners de gegevens van klanten voor hun eigen zakelijke doeleinden gebruiken (bv. om opbrengsten te genereren door de gebruikers gerichte advertenties aan te bieden of door statistische gegevens aan andere organisaties te verkopen). Hoewel het gebruik van klantgegevens meestal beperkt blijft tot contracten met consumenten en niet met ondernemingen, is het belangrijk dat men nagaat hoe of de dienstverlener de gegevens zal gebruiken voor andere doeleinden dan het leveren van de dienst. Daarom moet men de Dienstvoorwaarden van de dienstverlener onderzoeken om te verzekeren dat zij de eigendom van de gegevens duidelijk bepalen, de manier waarop ze in de levering van de dienst zullen worden gebruikt, en of de dienstverlener ze voor andere doeleinden dan de levering van de dienst zal gebruiken.

Het is niet ongebruikelijk dat een dienstverlener een beroep doet op componenten van andere dienstverleners. Een SaaS-dienst kan bijvoorbeeld op een IaaS van een andere dienstverlener worden gehost. Het is essentieel dat men een eventuele afhankelijkheid van een dienstverlener tegenover diensten van derden identificeert, zodat men de risico's van het gebruik van een dienst ten volle begrijpt.

Voor deze veiligheidsdoelstelling moet men rekening houden met de volgende overwegingen:

- men moet weten of de dienstverlener over de contracten met zijn klanten onderhandelt, of de klanten standaard Dienstvoorwaarden moeten aanvaarden;
- de Dienstvoorwaarden en het SLA van de dienstverlener moeten duidelijk bepalen hoe de dienst de vertrouwelijkheid, de integriteit en de beschikbaarheid van officiële informatie en de privacy van alle persoonlijk identificeerbare informatie beschermt;
- de Dienstvoorwaarden van de dienstverlener moeten vermelden dat de overheidsdienst de eigenaar van zijn gegevens blijft;
- men moet nagaan of de dienstverlener de gegevens voor andere doeleinden dan de levering van de dienst gebruikt;
- het moet duidelijk zijn of de dienst van de dienstverlener afhankelijk is van diensten van derden;

Voorgestelde maatregelen om aan de overwegingen te voldoen:

- A practical guide to Cloud Service Agreements V3.0: https://www.omg.org/cloud/deliverables/practical-guide-to-cloud-service-agreements.htm
- Public Cloud Service Agreements: What to Expect and What to Negotiate V2.0: https://www.omg.org/cloud/deliverables/public-cloud-service-agreements-what-to-expect-and-what-to-negotiate.htm

Compliance:

De clouddienstverlener moet zich houden aan de Belgische wet tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, de omzetting van de Europese NIS-richtlijn (2016/1148/EU) in het Belgische recht. Clouddienstverleners kunnen worden beschouwd als digitaledienstverleners die onder het toepassingsgebied van deze wet vallen. De clouddienstverlener hoeft zijn hoofdvestiging niet in België te hebben, maar kan de dienst in België aanbieden terwijl hij een in België de gevestigde vertegenwoordiger heeft.

De NIS-richtlijn wil verzekeren dat de leveranciers van cloudcomputingdiensten technische en organisatorische beveiligingsmaatregelen nemen om incidenten te voorkomen of hun impact te beperken, en zo de veiligheid en de continuïteit van het leven van de Belgische burgers en bedrijven te verzekeren. De beveiligingsmaatregelen onder de NIS-wetgeving omvatten:

- De risicopreventie: Passende en met het risico evenredige technische en organisatorische maatregelen.
- De beveiliging van netwerk- en informatiesystemen: De maatregelen moeten een niveau van beveiliging van de netwerk- en informatiesystemen verzekeren dat is afgestemd op de risico's.
- Behandeling van incidenten: De maatregelen moeten de impact op de IT-systemen die voor de levering van de diensten worden gebruikt voorkomen en tot het minimum beperken.
- De door digitaledienstverleners genomen beveiligingsmaatregelen moeten ook rekening houden met enkele specifieke factoren:
    - de beveiliging van systemen en faciliteiten
    - de behandeling van incidenten
    - het beheer van de bedrijfscontinuïteit

- toezicht, controle en testen
- de inachtneming van de internationale normen

De verplichtingen voor cloudcomputingdiensten onder de NIS-wetgeving kunnen in principe de veiligheid van de overheidsdiensten garanderen.

Voorgestelde maatregelen om aan de overwegingen te voldoen:

- ISO/IEC 27001 kan de overheidsdiensten helpen om toereikend aan de gegeven overwegingen te voldoen;
- De aanbevelingen van ENISA, zoals de technische richtlijnen voor de implementatie van minimale beveiligingsmaatregelen voor digitaledienstverleners: https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers

Details van de aansprakelijkheid voor deze veiligheidsdoelstelling:

Overheidsdienst	Clouddienstverlener
• De overheidsdienst moet ook rekening houden met de mogelijkheid dat de relevante wetten en reglementen die van de jurisdictie van de clouddienstverlener kunnen zijn, naast die van de overheidsdienst. De overheidsdienst moet bewijzen vragen van de naleving door de clouddienstverlener van de relevante reglementeringen en standaarden die voor de werking van de overheidsdienst vereist zijn. Deze bewijzen kunnen door externe auditors verstrekte certificeringen zijn. • De installatie van software onder een commerciële licentie in een clouddienst kan een schending van de licentievoorwaarden van de software veroorzaken. De overheidsdienst moet over een procedure beschikken om voor de cloud specifieke licentievereisten te identificeren voor hij toelaat dat software onder een licentie in een clouddienst wordt geïnstalleerd. Gevallen waarin de clouddienst elastisch en schaalbaar is en de software op meer systemen of processors kan worden uitgevoerd dan de voorwaarden van de licentie toestaan, verdienen een bijzondere aandacht. • De overheidsdienst moet bij de clouddienstverlener informatie inwinnen over de bescherming van de registraties die door de clouddienstverlener worden verzameld en bewaard die relevant zijn voor het gebruik van de clouddiensten door de overheidsdienst. • De overheidsdienst moet verifiëren dat de reeks cryptografische controles op het gebruik van een clouddienst voldoet aan de relevante overeenkomsten, wetten en reglementen. • De overheidsdienst moet gedocumenteerde bewijzen vragen dat de implementatie van informatieveiligheidscontroles en richtlijnen	• De clouddienstverlener moet de overheidsdienst informeren over de jurisdictie waaronder de clouddienst valt. De clouddienstverlener moet zijn eigen relevante wettelijke vereisten identificeren (met betrekking tot de versleuteling voor de bescherming van intellectuele eigendomsrechten. Deze informatie moet op verzoek ook aan de overheidsdienst worden verstrekt. De clouddienstverlener moet de overheidsdienst bewijzen bezorgen van zijn huidige naleving van de toepasselijke wetten en contractuele eisen. • De clouddienstverlener moet over een proces voor de reactie op vorderingen inzake intellectuele eigendomsrechten beschikken. • De clouddienstverlener moet de overheidsdienst informeren over de bescherming van de registraties die door de clouddienstverlener worden verzameld en bewaard in verband met het gebruik van de clouddiensten door de overheidsdienst. • De clouddienstverlener moet beschrijvingen leveren van de cryptografische controles die hij implementeert, zodat de overheidsdienst de naleving van de toepasselijke overeenkomsten, wetten en reglementen kan nagaan. • De clouddienstverlener moet de overheidsdienst gedocumenteerde bewijzen verstrekken als staving van zijn bewering dat hij informatiebeveiligingsmaatregelen toepast. Wanneer individuele audits door de overheidsdienst niet onpraktisch zijn of de risico's voor de informatiebeveiliging kunnen verhogen, moet de clouddienstverlener onafhankelijke bewijzen leveren dat de informatiebeveiliging geïmplementeerd is en

voor de clouddienst overeenkomt met de verklaringen van de clouddienstverlener. Deze bewijzen kunnen certificeringen volgens relevante standaarden omvatten."	wordt uitgevoerd in overeenstemming met het beleid en de procedures van de clouddienstverlener. De overheidsdienst moet deze bewijzen ontvangen voor hij een contract afsluit. Een relevante door de clouddienstverlener gekozen onafhankelijke audit zou normaal een aanvaardbare methode moeten zijn om te voldoen aan het belang voor de overheidsdienst om de werking van de clouddienstverlener te onderzoeken, op voorwaarde dat de audit voldoende transparant is. Als een onafhankelijke audit onpraktisch is, moet de clouddienstverlener een zelfbeoordeling uitvoeren en zijn processen en resultaten aan de overheidsdienst bezorgen."

Vertrouwelijkheid

Veel factoren kunnen een ongeoorloofde toegang tot of openbaarmaking van in een clouddienst bewaarde informatie veroorzaken. Het is echter belangrijk om op te merken dat de grote meerderheid van deze factoren niet uniek is voor cloudcomputing.

Zoals reeds aangestipt, zal het model van de clouddienst (bv. IaaS, PaaS of SaaS) bepalen welke partij verantwoordelijk is voor de implementatie en het beheer van de controles die de vertrouwelijkheid beschermen van de door de dienst bewaarde, verwerkte of verzonden informatie. Evenzo zal het implementatiemodel van de cloud (public, private, community of hybrid) een invloed hebben op het vermogen van de klant om zijn controle-eisen op te leggen.

Authenticatie en toegangscontrole

Het gebruik van meerdere clouddiensten kan een onaanvaardbare last voor de gebruikers inhouden als de overheidsdienst geen passende strategie voor identiteitsbeheer toepast. Elke gebruikte clouddienst zou er bijvoorbeeld toe kunnen leiden dat de gebruikers telkens een andere gebruikersnaam en wachtwoord nodig hebben. Een bespreking van de benaderingen van het identiteitsbeheer valt buiten het bereik van dit document. De overheidsdiensten worden echter aangespoord om een benadering van het identiteits- en toegangsbeheer te ontwikkelen die het gebruik van clouddiensten door hun werknemers en klanten ondersteunt. Dit beheer moet rekening houden met de implicaties en risico's voor de veiligheid.

De ruimte toegankelijkheid via het netwerk die typisch is voor cloud computing vergroot de noodzaak dat de overheidsdiensten sterke praktijken voor het beheer van de levenscyclus van de identiteit hanteren. De gebruikers kunnen een clouddienst immers meestal vanop om het even welke locatie bereiken. Dit impliceert een beduidend risico, aangezien de mogelijkheid kan bestaan dat werknemers of aannemers die niet langer voor de overheidsdienst werken nog altijd toegang hebben tot de clouddienst. De overheidsdienst moet bijgevolg over een effectief proces voor het beheer van de levenscyclus van de identiteiten beschikken. Het moet verzekeren dat:

- Machtigingen op het passende niveau van de organisatie worden goedgekeurd.
- De op rollen gebaseerde toegangscontrole (Role Based Access Control, RBAC) voldoende granulair is om de machtigingen te controleren.

- De gebruiker uitsluitend de machtigingen ontvangen die zij nodig hebben om hun taken uit te voeren.
- De gebruikers geen machtigingen verzamelen naarmate zij in de organisatie van rol veranderen.
- Gebruikersaccounts stipt worden verwijderd wanneer het diensterband eindigt.

Daarnaast moeten de overheidsdiensten regelmatig audits uitvoeren van hun gebruikersaccounts en van de machtigingen die de accounts ontvangen in de clouddiensten die ze gebruiken, om te verzekeren dat redundante accounts worden verwijderd en dat de gebruikers altijd alleen de machtigingen ontvangen die ze nodig hebben om hun taken uit te voeren.

De alomtegenwoordige toegang houdt ook in dat de gebruikers met behulp van uiteenlopende toestellen vanop elke locatie de toegang kunnen krijgen tot de informatie in de clouddienst. De overheidsdiensten moeten de implicaties voor de informatiebeveiliging zorgvuldig overwegen en onderzoeken welke controles ze nodig hebben om hun informatie passend te beschermen. Zo zou een overheidsdienst die een op SaaS gebaseerde oplossing voor het beheer van de klantenrelaties (Customer Relation Management, CRM) implementeert kunnen bepalen dat hij de toegang moet beperken tot specifieke onderdelen en functies (bv. het downloaden van klantendossiers of het opslaan van rapporten) wanneer gebruikers de clouddienst raadplegen buiten de lokalen van de overheidsdienst of met een toestel dat geen eigendom is van de overheidsdienst en niet door de overheidsdienst wordt beheerd.

Een ander aandachtspunt bij het gebruik van clouddiensten is de vraag of de wachtwoorden voldoende zekerheid bieden dat de persoon die zich bij de dienst authentiseert de eigenaar van het gebruikersaccount is. De overheidsdienst moet bepalen of hij een sterker authenticatiemechanisme nodig heef(bijvoorbeeld meervoudige verificatie) die voldoende zekerheid verschaft dat de persoon die de identiteit opeist de geautoriseerde gebruiker sis.

Voor deze veiligheidsdoelstelling moet men rekening houden met de volgende overwegingen:

- de overheidsdienst moet een strategie voor identiteitsbeheer hanteren die het gebruik van clouddiensten ondersteunt;
- de clouddienst moet de strategie voor identiteitsbeheer van de overheidsdienst ondersteunen;
- er moet een effectief intern proces bestaan dat verzekert dat de identiteiten tijdens hun volledige levenscyclus worden beheer;
- er moet een effectief auditproces bestaan dat met regelmatige intervallen wordt uitgevoerd om een passend beheer van de gebruikersaccounts te verzekeren;
- de controles die nodig zijn om de risico's van de alomtegenwoordige toegang via de cloud te beheren, moeten geïdentificeerd zijn;
- de clouddienst moet aan deze controle-eisen voldoen;
- men moet weten of een grotere mate van zekerheid nodig is om te garanderen dat de partij die tijdens de authenticatie bij de dienst een identiteit opeist wel degelijk de geautoriseerde gebruiker van het account is;

Voorgestelde maatregelen om aan de overwegingen te voldoen:

- De veiligheidscontrole van de Cloud Control Matrix: AIS-03, IAM-01, IAM-02, IAM-03, IAM-04, IAM-05, IAM-06, IAM-07, IAM-08, IAM-09, IAM-10, IAM-11, IAM-12, IAM-13, ...
- Voor meer informatie over IAM en Pam bevelen wij het volgende document aan: FISP- Handleiding voor IAM & PAM

Details van de aansprakelijkheid voor deze veiligheidsdoelstelling:

Overheidsdienst	Clouddienstverlener
• Het beleid voor toegangscontrole voor het gebruik van netwerkdiensten van de overheidsdienst moet eisen voorschrijven voor de toegang tot elke afzonderlijke clouddienst die wordt gebruikt; • de overheidsdienst moet toereikende authenticatietechnieken gebruiken (bijvoorbeeld meervoudige verificatie) om de beheerders van de clouddienst van de overheidsdienst te authentiseren voor zij toegang krijgen tot de beheersfuncties van een clouddienst, in overeenstemming met de geïdentificeerde risico's. • De overheidsdienst moet nagaan of de beheersprocedure van de clouddienstverlener voor te toekenning van geheime authenticatie-informatie, zoals wachtwoorden, aan de eisen van de overheidsdienst voldoet.	• Om de toegang van de gebruikers van een overheidsdienst tot de clouddiensten te beheren, moet de clouddienstverlener functies voor de registratie en de deregistratie van gebruikers voorzien en de specificaties voor het gebruik van deze functies aan de overheidsdienst bezorgen; • De clouddienstverlener moet functies voorzien voor het beheer van de toegangsrechten van de gebruikers van de overheidsdienst tot de clouddiensten, en de specificaties voor het gebruik van die functies bezorgen; • De clouddienstverlener moet toereikende authenticatietechnieken gebruiken om de beheerders van de clouddienst van de overheidsdienst te authentiseren voor zij toegang krijgen tot de beheersfuncties van een clouddienst, in overeenstemming met de geïdentificeerde risico's. De clouddienstverlener kan bijvoorbeeld een meervoudige verificatie voorzien, of het gebruik van meervoudige verificatiemechanismen van een derde partij mogelijk maken. • De clouddienstverlener moet informatie verstrekken over de procedures die hij voorziet voor het beheer van de geheime authenticatie-informatie van de overheidsdienst, met inbegrip van de procedures voor de toewijzing van deze informatie en voor de authenticatie van de gebruikers.

Multi-tenant

Het voor cloud computing typische delen van middelen betekent dat de diensten meestal een vorm van multi-tenancy gebruiken. De risico's van multi-tenancy houden meestal verband met de virtualisering van de infrastructuur of de vermenging van gegevens. Het meest geciteerde probleem in een gevirtualiseerde omgeving is dat een kwaadwillige partij een zwakke plek in de hypervisor zou kunnen benutten om toegang te krijgen tot de informatie van andere klanten (bv. met een "guest-to-host" of "guest-to-guest" aanval). De virtualisering maakt het gemakkelijk om een momentopname (snapshot) te maken (een kopie van het geheugen en de schijf van een server op een gegeven tijdstip, voor back-up- en redundantiedoeleinden). Als de momentopnamen niet passend beveiligd zijn, zou een kwaadwillige partij ongeoorloofde toegang kunnen krijgen tot de informatie op de lokale schijven van de virtuele machine en tot alle cryptografische sleutels en gegevens in het geheugen.

Dit impliceert dat de architectuur van de dienstverlener, de implementatie en het doorlopende beheer en de monitoring van de virtualisatieomgeving, samen met de praktijken voor patches en het beheer van zwakke plekken, essentieel zijn om de veiligheid van de in de clouddienst bewaarde en verwerkte informatie te verzekeren.

Een ander courant probleem in IaaS- en PaaS-omgevingen is dat de veiligheid van de volledig omgeving kan afhangen van de klant met de zwakste veiligheidspraktijken en -controles (probleem van de kleinste gemene deler). SaaS en PaaS gebruiken logische controles in de toepassing of het platform en de ondersteunende infrastructuur om de toegang tot de gegevens van elke klant af te schermen. Meestal worden de gegevens echter vermengd in de toepassing, de database en de back-upmedia. Dat maakt de beveiliging volledig afhankelijk van de kwaliteit van het ontwerp, de implementatie en de handhaving van de toegangscontroles op de platformen en in de toepassingen.

De "zelfbediening" en de "on-demand" werking van cloud computing zijn problematisch voor de veiligheid omdat de registratieprocessen om klant te worden niet altijd de identiteit van een klant met volledige zekerheid verifiëren (bv. bij zelfregistratie op het web). Deze kwetsbaarheid kan een kwaadwillige partij in staat stellen om zich bij een dienst te registreren en hem daarna te gebruiken voor kwaadwillige of bedrieglijke activiteiten, bijvoorbeeld door te trachten te toegangscontroles te omzeilen om ongeoorloofde toegang te krijgen tot de gegevens van een andere klant. Een overheidsdienst moet er voldoende zeker van zijn dat andere klanten die een clouddienst gebruiken de controles van de clouddienstverlener niet kunnen omzeilen om toegang te krijgen tot zijn gegevens. Zoals reeds vermeld kan dat moeilijk zijn, aangezien de aard 'als een dienst' van cloud computing vaak een gebrek aan transparantie impliceert van de veiligheidscontroles en -praktijken die de clouddienstverlener toepast om de klantgegevens te beschermen. Dit leidt opnieuw tot een grote afhankelijkheid van auditverslagen en penetratietests van derde partijen.

Voor deze veiligheidsdoelstelling moet men rekening houden met de volgende overwegingen:

- de dienstverlener moet toestaan dat de overheidsdienst een externe audit laat uitvoeren met een beoordeling van de veiligheidscontroles en -praktijken voor de virtualisering en de afscheiding van de gegevens van de klant;
- de dienstverlener moet de klanten de mogelijkheid geven om veiligheidstests uit te voeren (met inbegrip van penetratietests) om de effectiviteit te beoordelen van de toegangscontroles die de scheiding van de klantgegevens verzekeren;
- de processen van de dienstverlener voor de registratie van de klanten moeten een voldoende zekerheid verschaffen in lijn met de waarde, de kritikaliteit en de gevoeligheid van de informatie die in de clouddienst wordt bewaard;

Voorgestelde maatregelen om aan de overwegingen te voldoen:

- De beveiligingstoepassing van de Cloud Control Matrix: IVS-09, IAM-01, IAM-02, IAM-03, IAM-04, IAM-05, IAM-06, IAM-07, IAM-08, IAM-09, IAM-10, IAM-11, IAM-12, IAM-13, ...

Standaard besturingsomgevingen

Hoewel de dienstverlener volledig verantwoordelijk is voor de passende configuratie en het passende beheer van zijn SaaS-oplossing, wordt in de andere cloudmodellen (IaaS en PaaS) de verantwoordelijkheid gedeeld tussen de overheidsdienst en de dienstverlener. Overheidsdiensten die geen gedefinieerde en gedocumenteerde bouw- en hardingsstandaarden hanteren voor de besturingssystemen en toepassingen die zij op IaaS- of PaaS-clouddiensten wensen te implementeren, kunnen moeilijkheden ondervinden om hun systemen effectief tegen ongeoorloofde toegang te beschermen.

Wanneer een overheidsdienst beslist om de bouw en harding van besturingssystemen en toepassingen aan de dienstverlener toe te vertrouwen, moet hij bepalen of hij de standaarden van de dienstverlener mag aanvaarden of zijn eigen standaarden moet ontwerpen. Ongeacht de benadering die de overheidsdienst kiest, is het aanbevolen dat men een penetratietest uitvoert om te verzekeren dat de eerste implementatie van de diensten veilig verloopt.

Voor deze veiligheidsdoelstelling moet men rekening houden met de volgende overwegingen:

- men moet passende bouw- en hardingsstandaarden definiëren en documenteren voor de servicecomponenten die de overheidsdienst beheert;
- de overheidsdienst moet besturingssystemen en toepassingen implementeren volgens interne bouw- of hardingsstandaarden, of moet over passende bouw- en hardingstandaarden beschikken die aan de veiligheidseisen van de dienst voldoen;
- de virtuele kopie moet een op de host gebaseerde firewall bevatten die geconfigureerd is om uitsluitend inkomend en uitgaand verkeer toe te staan dat nodig is om de dienst te ondersteunen;
- de dienstverlener moet toestaan dat in de virtuele machines op de host gebaseerde programma's voor intrusiedetectie en -preventie (IDS/IDP) worden geïnstalleerd;
- de dienstverlener moet zijn beveiligingsprocessen en -controles regelmatig testen;
- men moet een penetratietest van de dienst kunnen uitvoeren om te verzekeren dat hij goed beveiligd is;

Voorgestelde maatregelen om aan de overwegingen te voldoen:

De beveiligingstoepassing van de Cloud Control Matrix: IVS-02, IVS-07, ...

Beheer van patches en beveiligingsproblemen

Een verbeterd beheer van patches en kwetsbaarheden wordt vaak aangehaald als een van de grote voordelen van de overstap naar de cloud. Kwetsbaarheden zijn een ernstig risico voor elk informatiesysteem en vooral voor systemen die aan het internet blootgesteld zijn. Omdat clouddiensten overal toegankelijk zijn, is het buitengewoon belangrijk dat de overheidsdiensten verzekeren dat de diensten stipt met patches worden bijgewerkt. Het is belangrijk dat men weet welke partij verantwoordelijk is voor de patching van elke component van een clouddienst (bijvoorbeeld de toepassing, het besturingssysteem, de hypervisorsoftware, de Application Programming Interface (API) enz.). Zoals reeds vermeld, zal het model van de clouddienst (bv. IaaS, PaaS of SaaS) meestal bepalen welke partij verantwoordelijk is voor het beheer en het onderhoud van de individuele componenten. Als de dienstverlener verantwoordelijk is, moet de overheidsdienst verzekeren dat de

Dienstvoorwaarden en het SLA de specifieke tijdspanne vermelden die toegestaan is tussen het uitbrengen van een patch door een leverancier en zijn toepassing op alle betrokken systemen (het "maximale blootstellingsvenster").

Als de overheidsdienst verantwoordelijk is voor de patches, moet hij verzekeren dat hij over een effectief proces voor het patchbeheer beschikt en de juiste bronnen monitort op kwetsbaarheidswaarschuwingen, zodat hij kan verzekeren dat patches tijdig worden geïdentificeerd en geïmplementeerd.

Voor deze veiligheidsdoelstelling moet men rekening houden met de volgende overwegingen:

- ofwel moet de dienstverlener verantwoordelijk zijn voor de patching van alle componenten van de clouddienst, ofwel moet de overheidsdienst identificeren voor welke componenten de dienstverlener verantwoordelijk is en voor welke de overheidsdienst verantwoordelijk is;
- de Dienstvoorwaarden of het SLA van de dienstverlener moeten serviceniveaus bevatten voor het beheer van patches en kwetsbaarheden, met inbegrip van het maximale blootstellingsvenster;
- de overheidsdienst moet over een effectief proces voor het beheer van patches en kwetsbaarheden beschikken;
- de overheidsdienst moet verzekeren dat alle componenten waarvoor hij verantwoordelijk is, opgenomen zijn in zijn proces voor het beheer van patches en kwetsbaarheden;
- de overheidsdienst moet geabonneerd zijn op passende bronnen van waarschuwingen voor kwetsbaarheden en patches, of ze monitoren, voor de componenten waarvoor hij verantwoordelijk is;
- de dienstverlener moet toestaan dat zijn klanten de kwetsbaarheid regelmatig evalueren;
- de Dienstvoorwaarden of het SLA moeten een compensatieclausule bevatten voor inbreuken als gevolg van kwetsbaarheden in de dienst, of moeten ten minste een passend niveau van vergoeding voorzien in het geval van een inbreuk;

Voorgestelde maatregelen om aan de overwegingen te voldoen:

- De beveiligingstoepassing van de Cloud Control Matrix: TVM-01, TVM-02, TVM-03

Details van de aansprakelijkheid voor deze veiligheidsdoelstelling:

Overheidsdienst	Clouddienstverlener
• De overheidsdienst moet de clouddienstverlener om informatie verzoeken over het beheer van de technische beveiligingsproblemen met een potentiële impact op de geleverde clouddiensten. De overheidsdiensten moet identificeren voor welke technische beveiligingsproblemen zij verantwoordelijk zijn, en moeten hun processen voor het beheer van die problemen duidelijk bepalen.	• De clouddienstverlener moet de overheidsdienst informeren over het beheer van de technische beveiligingsproblemen die de geleverde clouddiensten kunnen treffen.

Versleuteling

Versleuteling wordt vaak voorgesteld als de oplossing voor de behandeling van vertrouwelijkheidsrisico's in de cloud. Ze heeft echter een aantal belangrijke beperkingen waarmee overheidsdiensten rekening dienen te houden wanneer ze het gebruik van clouddiensten plannen. De overheidsdiensten moeten hun specifieke eisen voor de bescherming van informatie door middel van versleuteling bepalen, en de versleuteling moet compliant zijn met het niveau van de gegevenscategorie zoals gedefinieerd in het document "FISP – Informatiecategorisatie". Men moet de volgende punten zorgvuldig overwegen:

- Welke informatie moet worden versleuteld? Betreft het alle informatie die in de clouddienst wordt gehouden of slechts bepaalde types gegevens of databaserijen, kolommen of entiteiten?
- Waarom moet de informatie worden versleuteld? Is versleuteling bijvoorbeeld vereist om een beleid of standaard na te leven?
- Hoe moet de informatie worden versleuteld? Bijvoorbeeld, welke protocollen en algoritmen moet men gebruiken?
- Wie zal de informatie versleutelen en de encryptiesleutels beheren? De overheidsdienst of de dienstverlener?
- Waar moet de informatie worden versleuteld en ontsleuteld? In de overheidsdienst, op de toestellen van de klant of in de clouddienst?
- Wanneer moet de informatie worden versleuteld en ontsleuteld? Tijdens de transit, door de toepassing (versleuteling van berichten) en/of in rust?

Versleuteling is een effectieve controle om de vertrouwelijkheid van gegevens in rust te beschermen, maar meestal moeten de gegevens ontsleuteld worden om door een bedrijfsregel in een informatiesysteem te laten verwerken. Bijgevolg kan het onpraktisch of onmogelijk zijn om gegevens te versleutelen in een clouddienst die informatie verwerkt (in plaats van ze louter op te slaan). Wanneer een clouddienst in staat is om gegevens in versleuteld formaat te bewaren, is het belangrijk dat men weet welke partij (de overheidsdienst of de dienstverlener) verantwoordelijk is voor het beheer van de encryptiesleutels. Het is belangrijk om op te merken dat als de dienstverlener toegang heeft tot de encryptiesleutel of hij ze beheert, hij de in de clouddienst gehouden informatie zal kunnen ontsleutelen en raadplegen.

De onderschepping van gegevens in transit is een inherent risico telkens als gevoelige informatie op een netwerk circuleert, vooral als dat netwerk geen eigendom is van of niet wordt beheerd door een overheidsdienst, zoals in het geval van het internet of het netwerk van een dienstverlener. De overheidsdiensten moeten verzekeren dat de clouddienst alle gevoelige gegevens in transit (met inbegrip van authenticatiegegevens) versleutelt en uitsluitend goedgekeurde encryptieprotocollen en algoritmen gebruikt. Overheidsdiensten die op versleuteling vertrouwen, moeten onderzoeken of passende versleutelingsprotocollen, algoritmen en de sleutellengten worden gebruikt.

Voor deze veiligheidsdoelstelling moet men rekening houden met de volgende overwegingen:

- de eisen voor de versleuteling van de informatie die op de clouddienst zal worden geplaatst moeten bepaald zijn;
- het moet duidelijk zijn welke partij verantwoordelijk is voor het beheer van de encryptiesleutels;

Voorgestelde maatregelen om aan de overwegingen te voldoen:

- De beveiligingstoepassing van de Cloud Control Matrix: EKM-01, EKM-02, EKM-03
- Het document ‘Handleiding voor cryptografie’ is eveneens aanbevolen

Details van de aansprakelijkheid voor deze veiligheidsdoelstelling:

Overheidsdienst	Clouddienstverlener

• De overheidsdienst moet cryptografische controles voor zijn gebruik van clouddiensten toepassen als de risicoanalyse dat verantwoordt. De controles die door de overheidsdienst of de clouddienstverlener worden voorzien, moeten voldoende krachtig zijn om de geïdentificeerde risico's te beperken. Als de clouddienstverlener cryptografie aanbiedt, moet de overheidsdienst de door de clouddienstverlener verstrekte informatie onderzoeken om te bevestigen of de cryptografische capaciteiten:
  • aan de beleidseisen van de overheidsdienst voldoen;
  • compatibel zijn met eventuele andere cryptografische beveiliging die de overheidsdienst gebruikt;
  • gelden voor statische gegevens in de clouddienst en gegevens die in transit zijn naar, van of binnen de clouddienst."
• De overheidsdienst moet de cryptografische sleutels voor elke clouddienst identificeren en procedures voor hun beheer toepassen. Als de clouddienst functies voor het beheer van de sleutels voorziet die de overheidsdienst kan gebruiken, moet de overheidsdienst de volgende informatie verzoeken over de procedures die voor het beheer van de sleutels voor de clouddienst worden gebruikt:
  • type sleutels;
  • specificaties van het systeem voor het beheer van de sleutels, met inbegrip van de procedures in elke fase van de levenscyclus van de sleutels, namelijk hun aanmaak, wijziging of update, opslag, intrekking, bewaring en vernietiging;
  • aanbevolen procedures voor het beheer van de sleutels door de overheidsdienst.
De overheidsdienst mag niet toestaan dat de clouddienstverlener de encryptiesleutels voor versleutelingsoperaties bewaart en beheert als de overheidsdienst de sleutels zelf beheert of een afzonderlijke en onderscheiden dienst voor het beheer van de sleutels gebruikt.
	• De clouddienstverlener moet de overheidsdienst informeren over de omstandigheden waarin hij versleuteling gebruikt om de informatie die hij verwerkt te beschermen. De clouddienstverlener moet bovendien de overheidsdienst informeren over eventuele capaciteiten die hij verstrekt die de overheidsdienst kunnen helpen om zijn eigen cryptografische beveiliging toe te passen.

Interne bedreigingen bij de clouddienstverlener

Ongeoorloofde toegang van werknemers van de dienstverlener tot gevoelige informatie is een courant probleem voor organisaties die van plan zijn om clouddiensten te gebruiken. De overheidsdiensten moeten nagaan of de dienstverlener passende procedures hanteert om te verzekeren dat zijn personeel betrouwbaar is en geen veiligheidsrisico voor zijn klanten vormt. De mate van zekerheid die de overheidsdienst kan verkrijgen, kan sterk verschillen afhankelijk van de fysieke locatie van de dienst en de werknemers van de dienstverlener.

De logging en monitoring van de activiteiten van de werknemers is een belangrijke controle voor het beheer van de risico's van kwaadwillige insiders. De logging moet alle relevante activiteiten bestrijken die worden uitgevoerd door werknemers van de dienstverlener die logische of fysieke toegang hebben tot uitrusting of media die klantgegevens bevatten. De dienstverlener moet de logboeken monitoren en onderzoeken om mogelijke verdachte activiteit te identificeren die verder onderzoek vereist. Bovendien moeten de taken gescheiden zijn, om te verzekeren dat de logboeken beschermd zijn tegen ongeoorloofde wijziging en verwijdering (zo mag de beheerder van een dienstcomponent geen wijzigings- of verwijderingsrechten hebben voor de Security Information Event Monitoring-dienst (SIEM).

Voor deze veiligheidsdoelstelling moet men rekening houden met de volgende overwegingen:

- de dienstverlener moet de achtergrond van alle werknemers die toegang zullen hebben tot klantgegevens passend onderzoeken voor ze worden aangeworven;
- de dienstverlener moet tijdens de tewerkstelling doorlopende controles uitvoeren;
- als de dienstverlener een derde partij gebruikt om een deel van zijn dienst te leveren, moet die derde partij de achtergrond van alle werknemers die toegang zullen hebben tot klantgegevens passend onderzoeken voor ze worden aangeworven;
- de dienstverlener moet over een SIEM-dienst beschikken die elke logische toegang tot klantgegevens registreert en monitort;
- de dienstverlener moet de taken scheiden om te verzekeren dat de auditlogboeken beschermd zijn tegen ongeoorloofde wijziging en verwijdering,
- de Dienstvoorwaarden of het SLA moeten de dienstverlener verplichten om ongeoorloofde toegang van zijn werknemers tot klantgegevens te melden;
- de dienstverlener moet verplicht zijn om de getroffen klanten details over het incident te verstrekken, zodat zij de gevolgen kunnen beoordelen en beheren;

Voorbeelden van maatregelen om aan de overwegingen te voldoen:

- De beveiligingstoepassing van de Cloud Control Matrix: HRS-01, HRS-02, HRS-03, HRS-04, HRS-05, HRS-06, HRS-07, HRS-08, HRS-09, HRS-10, HRS-11
- Het document ‘Handleiding voor logging en monitoring’ is eveneens aanbevolen.

Gegevenspersistentie

Het kan moeilijk zijn om gegevens blijvend van een multi-tenancy clouddienst te verwijderen wanneer de organisatie haar gebruik van de dienst afschaalt of stopzet. Als gegevens niet veilig verwijderd zijn, kan een toekomstige compromittering van de dienst nog altijd informatie van de overheidsdienst blootstellen. Soortgelijke problemen ontstaan wanneer de dienstverlener geen processen hanteert die verzekeren dat ICT-uitrusting en opslagmedia (bv. harde schijven, back-uptapes enz.) veilig worden gewist voor ze worden hergebruikt of opgeruimd. Daarom is het essentieel dat organisaties zich ervan verzekeren dat de dienstverlener effectieve en aantoonbare processen voor de verwijdering van gegevens en uitrusting hanteert.

Voor deze veiligheidsdoelstelling moet men rekening houden met de volgende overwegingen:

- de dienstverlener moet over een auditeerbaar proces beschikken voor het veilig opschonen van opslagmedia voor hij door een andere klant laat gebruiken;
- de dienstverlener moet over een auditeerbaar proces beschikken voor de veilige opruiming of vernietiging van ICT-uitrusting en opslagmedia (bv. harde schijven, back-uptapes enz.) die klantgegevens bevatten;

Voorgestelde maatregelen om aan de overwegingen te voldoen:

- De beveiligingstoepassing van de Cloud Control Matrix: DSI-07, DCS-05

Fysieke beveiliging

Controles van de fysieke beveiliging zijn van vitaal belang om te verzekeren dat de informatie fysiek beschermd is tegen ongeoorloofde toegang door zowel kwaadwillig personeel van de dienstverlener als derde partijen. Een effectieve informatiebeveiliging hangt af van de effectiviteit van de fysieke beveiligingsmaatregelen die men toepast om de kantoren, datacenters en fysieke middelen van de dienstverlener te beschermen. Maar zoals reeds vermeld, kan een rechtstreekse beoordeling van de fysieke beveiligingsmaatregelen die de dienstverlener gebruikt om zijn klantgegevens in een clouddienst te beschermen, onmogelijk of onpraktisch zijn. Het is mogelijk dat de overheidsdienst slechts een auditrapport van een derde partij kan onderzoeken.

Voor deze veiligheidsdoelstelling moet men rekening houden met de volgende overwegingen:

- als het praktisch haalbaar is, moet de overheidsdienst de fysieke beveiligingsmaatregelen van de dienstverlener rechtstreeks onderzoeken of beoordelen, of de dienstverlener moet ten minste toestaan dat de overheidsdienst een recent auditrapport van een derde partij onderzoekt dat een beoordeling van de fysieke beveiligingsmaatregelen omvat;

Voorgestelde maatregelen om aan de overwegingen te voldoen:

- De beveiligingstoepassing van de Cloud Control Matrix: DCS-02,DCS-07, DCS-08, DCS-09
- Het document ‘Handleiding voor de controle en de beveiliging van de fysieke toegangen’ is eveneens aanbevolen

Details van de aansprakelijkheid voor deze veiligheidsdoelstelling:

Overheidsdienst	Clouddienstverlener
De overheidsdienst moet de bevestiging verzoeken dat de clouddienstverlener over een beleid en procedures beschikt voor de veilige opruiming of het veilige hergebruik van middelen.	De clouddienstverlener moet verzekeren dat regelingen zijn getroffen voor de stipte en veilige opruiming of het stipte en veilige hergebruik van middelen.

Integriteit

De input- en outputkanalen van de cloudoplossing moeten de identificatie van de bron- en doelgegevens waarborgen en alle inkomende en uitgaande transfers beveiligen, zodat de juistheid en de betrouwbaarheid van de verwerkte gegevens van begin tot einde verzekerd zijn. Dienstverleners kunnen sterk verschillende niveaus van de beveiliging tegen het verlies of de beschadiging van gegevens aanbieden. Sommige dienstverleners nemen diensten voor de back-up van gegevens in hun basisaanbod op, andere bieden ze als een afzonderlijk te betalen dienst aan, nog andere voorzien ze helemaal niet (bv. Google Apps for Business levert geen back-updiensten zonder een afzonderlijk te betalen abonnement op Google Apps Vault). Het is bijgevolg belangrijk dat men identificeert welk beschermingsniveau de dienstverlener aanbiedt en beoordeelt of het wel of niet voldoet aan de eisen van de overheidsdienst voor het herstel na incidenten met gegevensverlies en -beschadiging.

De overheidsdiensten moeten het niveau van de granulariteit van het aangeboden gegevensherstel nagaan (bv. kunnen afzonderlijke bestanden of e-mails worden hersteld, of kan de klant alleen een volledige mailbox of database herstellen?). Bovendien moeten zij het proces voor het starten van een herstel identificeren en begrijpen. Het is belangrijk dat men beseft dat het gebruik van clouddiensten geen afbreuk doet aan de noodzaak dat de overheidsdienst zijn eigen back-upstrategie ontwikkelt, toepast en test, om te verzekeren dat hij zich voldoende kan herstellen van een incident dat tot het verlies of de beschadiging van gegevens leidt. De input- en outputkanalen van de cloudoplossing moeten de identificatie van de bron- en doelgegevens waarborgen en alle inkomende en uitgaande transfers beveiligen, zodat de juistheid en de betrouwbaarheid van de verwerkte gegevens van begin tot einde verzekerd zijn.

Voor deze veiligheidsdoelstelling moet men rekening houden met de volgende overwegingen:

- de dienstverlener moet als onderdeel van zijn standaard dienstenaanbod diensten voor gegevensback-up of -archivering voorzien, als bescherming tegen het verlies of de beschadiging van gegevens, of moet ten minste diensten voor gegevensback-up of -archivering als een aanvullende dienst aanbieden als bescherming tegen het verlies of de beschadiging van gegevens;
- men moet weten hoe de diensten voor gegevensback-up en -archivering worden verstrekt;
- de diensten voor gegevensback-up of -archivering moeten verzekeren dat de bedrijfseisen met betrekking tot gegevensverlies voldaan zijn;
- het granulariteitsniveau van het gegevensherstel dat de dienstverlener aanbiedt, moet duidelijk zijn;
- het proces van de dienstverlener voor de start van een herstel moet duidelijk zijn;
- de dienstverlener moet het herstelproces regelmatig testen om te verzekeren dat de gegevens van de back-upmedia kunnen worden hersteld;
- de overheidsdienst moet een strategie voor gegevensback-up implementeren om het herstel na een incident met verlies of beschadiging van gegevens te verzekeren;

Voorgestelde maatregelen om aan de overwegingen te voldoen:

- De veiligheidscontrole van de Cloud Control Matrix: IVS-02, IVS-07

Details van de aansprakelijkheid voor deze veiligheidsdoelstelling:

Overheidsdienst	Clouddienstverlener
• Wanneer de clouddienstverlener back-updiensten als onderdeel van de clouddienst aanbiedt, moet de overheidsdienst de clouddienstverlener om de specificaties van de back-upcapaciteit verzoeken. De clouddienst moet eveneens verifiëren of hij aan zijn back-upeisen voldoet. De overheidsdienst is verantwoordelijk voor de implementatie van back-upcapaciteiten indien de clouddienstverlener ze niet voorziet.	• De clouddienstverlener moet de overheidsdienst informeren over het beheer van de technische beveiligingsproblemen die de geleverde clouddiensten kunnen treffen. De clouddienstverlener moet de specificaties van zijn back-upcapaciteiten aan de overheidsdienst meedelen. De specificaties moeten de volgende informatie omvatten, zoals van toepassing: • het bereik en het schema van de back-ups; • de back-upmethoden en de gegevensindelingen, in voorkomend geval met inbegrip van de versleuteling; • de bewaarperiodes van de back-upgegevens; • de procedures voor de verificatie van de integriteit van de back-upgegevens; • de procedures en tijdschalen voor het herstel van gegevens uit de back-up; • de procedures voor het testen van de back-upcapaciteiten; • de locatie waar de back-ups worden bewaard. De clouddienstverlener moet veilige en gescheiden toegang tot de back-ups verlenen, zoals virtuele momentopnamen, als hij de overheidsdienst een dergelijke dienst aanbiedt.

De toewijzing van de verantwoordelijkheden voor het maken van back-ups in de cloudcomputingomgeving is vaak onduidelijk. In het geval van IaaS ligt de verantwoordelijkheid voor het maken van back-ups meestal bij de overheidsdienst. Het is echter mogelijk dat een overheidsdienst zich niet bewust is van zijn verantwoordelijkheid voor het maken van back-ups van al zijn gegevens die in het cloudcomputingsysteem worden geproduceerd, zoals uitvoerbare bestanden die door het gebruik van de ontwikkelingscapaciteiten van een PaaS-dienst worden geproduceerd.

Verschillende back-up- en herstelniveaus kunnen als een aanvullende te betalen dienst worden aangeboden en in dat geval kan de overheidsdienst kiezen wat hij back-upt en wanneer.

Beschikbaarheid

Overeenkomst inzake dienstverleningsniveau (SLA)

Het is belangrijk dat de overheidsdiensten duidelijk begrijpen wat het gedefinieerde percentage betekent en dat zij onderzoeken of dat niveau aan de beschikbaarheidseisen voldoet. Het SLA moet de details van eventuele geplande onderbrekingsperioden vermelden. Dit zal verzekeren dat de dienstverlener geen lange onderbrekingsperioden kan plannen (met inbegrip van onderbrekingen in noodsituaties) zonde of met weinig kennisgeving zonder inbreuk te maken op het SLA.

Wanneer het SLA geplande onderbrekingsperioden vermeldt, moeten ze worden onderzocht om te verzekeren dat ze geen schadelijke gevolgen voor de werking zullen hebben.

Een andere belangrijke overweging is de toereikendheid van de compensatie voor een inbreuk op het SLA en de methode om de boetes over een dienstperiode te berekenen. Meestal vermeldt het SLA voor clouddiensten een minimale compensatie, zoals servicecredits of kortingen op facturen. De overheidsdiensten moeten eventuele compensatieclausules onderzoeken en bepalen of het niveau van de vergoeding volstaat, waarbij ze rekening moeten houden met de gevolgen van een onbeschikbaarheid voor de dienst voor hun werking.

Voor deze veiligheidsdoelstelling moet men rekening houden met de volgende overwegingen:

- het SLA moet een verwacht en minimaal beschikbaarheidspercentage over een welomschreven periode vermelden;
- de bedrijfseisen voor de beschikbaarheid moeten voldaan zijn;
- het SLA moet een compensatieclausule voor inbreuken op de gewaarborgde beschikbaarheidspercentages bevatten;

Voorgestelde maatregelen om aan de overwegingen te voldoen:

- A practical guide to Cloud Service Agreements V3.0: https://www.omg.org/cloud/deliverables/practical-guide-to-cloud-service-agreements.htm
- Public Cloud Service Agreements: What to Expect and What to Negotiate V2.0: https://www.omg.org/cloud/deliverables/public-cloud-service-agreements-what-to-expect-and-what-to-negotiate.htm

Denial of Service-aanvallen

Denial of Service-aanvallen (DoS) zijn een inherent risico van alle diensten die met het internet verbonden zijn. Het gebruik van clouddiensten kan het risico van een dergelijke aanval vergroten, aangezien de verzameling van meerdere overheidsdiensten op een enkele clouddienst een aantrekkelijker doelwit voor aanvallers kan zijn. Evenzo kan een overheidsdienst aanverwante of nevenschade lijden wegens een aanval op de dienstverlener of een andere tenant.

Een DoS-aanval kan tegen de dienstverlener of tegen de overheidsdienst zelf gericht zijn. Het gebruik van clouddiensten kan de impact van sommige vormen van DoS-aanvallen beperken, aangezien de dienstverleners over een reserve aan bandbreedte en computingcapaciteit beschikken. Daarnaast gebruiken sommige dienstverleners protocollen en technologieën (bv. Anycast, Application Delivery Networks en Content Delivery Networks) en geografisch verspreide datacenters die het netwerkverkeer en de computerverwerking wereldwijd verdelen. De elastische aard van clouddiensten kan ook een financiële impact veroorzaken.

Voor deze veiligheidsdoelstelling moet men rekening houden met de volgende overwegingen:

- de dienstverlener moet protocollen en technologieën gebruiken die tegen DoS-aanvallen kunnen beschermen;
- de overheidsdienst moet limieten voor het gebruik van middelen specificeren of configureren om zich tegen EDoS (Economic Denial of Sustainability)/factuurschokken te beschermen;

Voorgestelde maatregelen om aan de overwegingen te voldoen:

- De veiligheidscontrole van de Cloud Control Matrix: IVS-13

Netwerkbeschikbaarheid en -prestaties

De beschikbaarheid en de prestaties van clouddiensten zijn in grote mate afhankelijk van de ondersteunende netwerkinfrastructuur. De overheidsdiensten moeten de netwerkconnectiviteit tussen hun gebruikers en de clouddienst onderzoeken om te verzekeren dat de beschikbaarheids- en prestatie-eisen voldaan zijn. De overheidsdiensten moeten nagaan of de netwerkdiensten die zij zelf beheren of die zij gebruiken een toereikend niveau van beschikbaarheid en bandbreedte hebben, en een voldoende lage latentie en packetverlies om aan de bedrijfsbehoeften te voldoen.

Voor deze veiligheidsdoelstelling moet men rekening houden met de volgende overwegingen:

- de netwerkdiensten die de overheidsdienst zelf beheert of zelf gebruikt, moeten een toereikend beschikbaarheidsniveau voorzien;
- de netwerkdiensten die de overheidsdienst zelf beheert of zelf gebruikt, moeten een toereikend niveau van redundantie/fouttolerantie voorzien;
- de netwerkdiensten die de overheidsdienst zelf beheert of zelf gebruikt, moeten een toereikende bandbreedte voorzien (doorvoercapaciteit van het netwerk);
- de latentie tussen het of de netwerken van de overheidsdienst en de dienst van de dienstverlener moet toereikend zijn om de gewenste gebruikersbeleving te verzekeren, of ten minste moet de latentie zich voordoen op de netwerkdiensten die de overheidsdienst zelf beheert of zelf gebruikt;
- het packetverlies tussen het of de netwerken van de overheidsdienst en de dienst van de dienstverlener moet toereikend zijn om de gewenste gebruikersbeleving te verzekeren, of ten minste moet het packetverlies zich voordoen op de netwerkdiensten die de overheidsdienst zelf beheert of zelf gebruikt;

Voorgestelde maatregelen om aan de overwegingen te voldoen:

- De veiligheidscontrole van de Cloud Control Matrix: BRC-01, BCR-02, BCR-03, BCR-04, BCR-05, BCR-06, BCR-07, BCR-08, BCR-09, BCR-10, BCR-11, IVS-04

Bedrijfscontinuïteit en rampenplan

De dienstverlener moet over toereikende plannen beschikken en de overheidsdienst moet begrijpen in welke mate de plannen het niveau van de continuïteit en het herstel verzekeren. Het is ook belangrijk dat men beseft dat het gebruik van clouddiensten geen afbreuk doet aan de noodzaak dat de overheidsdienst zijn eigen bedrijfscontinuïteitsplannen en rampenplannen ontwikkelt, toepast en test, om te verzekeren dat hij tijdens een onderbreking van de dienst kan blijven werken.

De overheidsdiensten moeten verzekeren dat de dienstverlener courante of de facto gegevensindelingen gebruikt en een methode voorziet om gegevens uit te pakken in een formaat dat de overheidsdienst kan gebruiken.

Voor deze veiligheidsdoelstelling moet men rekening houden met de volgende overwegingen:

- de dienstverlener moet over een bedrijfscontinuïteitsplan en een rampenplan beschikken;
- de dienstverlener moet toestaan dat de overheidsdienst zijn bedrijfscontinuïteitsplan en rampenplan evalueert;
- de plannen van de dienstverlener moeten het herstel van de gegevens van de overheidsdienst dekken, of alleen het herstel van de dienst zelf;
- de plannen van de dienstverlener moeten het herstel van de gegevens van de overheidsdienst dekken, met voorrang voor de klantgegevens;
- het moet duidelijk zijn of klanten op basis van het volume en de waarde van hun contract worden geprioriteerd;
- de dienstverlener moet zijn bedrijfscontinuïteitsplan en rampenplan regelmatig testen;
- de regelmaat van deze tests moet duidelijk zijn;
- Het moet duidelijk zijn of de dienstverlener de klanten een exemplaar van de bijbehorende rapporten zal verstrekken;
- de overheidsdienst moet zijn eigen bedrijfscontinuïteitsplan en rampenplan beschikken, om zijn herstel te verzekeren na een uitval van de diensten, een faillissement van de dienstverlener of een stopzetting van de dienst;
- de overheidsdienst moet zijn eigen bedrijfscontinuïteitsplan en rampenplan beschikken, om zijn herstel te verzekeren na een uitval van de diensten, een faillissement van de dienstverlener of een stopzetting van de dienst;
- de back-ups (gemaakt door de dienstverlener of de overheidsdienst) moeten versleuteld zijn aan de hand van een goedgekeurd versleutelingsalgoritme met een gepaste sleutellengte;

Voorgestelde maatregelen om aan de overwegingen te voldoen:

- De veiligheidscontrole van de Cloud Control Matrix: BRC-01, BCR-02, BCR-03, BCR-04, BCR-05, BCR-06, BCR-07, BCR-08, BCR-09, BCR-10, BCR-11

Incidentrespons en -beheer

De overheidsdiensten moeten een passende mate van zekerheid bezitten dat een dienstverlener in staat is om effectief en efficiënt te reageren op een informatieveiligheidsincident, aangezien zelfs de zorgvuldigst geplande, geïmplementeerde en preventieve controles niet altijd kunnen voorkomen dat een risico zich voltrekt. Bijgevolg moeten de overheidsdiensten de Dienstvoorwaarden en het SLA van de dienstverlener onderzoeken om te identificeren welke ondersteuning de dienstverlener zijn klanten in het geval van een informatieveiligheidsincident verleent.

Ongeacht de dienst of het implementatiemodel doet het gebruik van clouddiensten geen afbreuk aan de noodzaak dat de overheidsdienst over zijn eigen processen en plannen voor incidentrespons en -beheer beschikt.

Voor deze veiligheidsdoelstelling moet men rekening houden met de volgende overwegingen:

- de dienstverlener moet over formele processen en plannen voor de respons op en het beheer van incidenten beschikken, die duidelijk bepalen hoe hij informatieveiligheidsincidenten opspoort en erop reageert;
- hij moet de overheidsdienst een kopie van zijn processen en plannen bezorgen, zodat de overheidsdienst kan bepalen of ze toereikend zijn;
- de dienstverlener moet zijn processen en plannen voor de respons op en het beheer van incidenten regelmatig testen en verbeteren;
- de dienstverlener moet zijn klanten betrekken bij het testen van zijn processen en plannen voor de respons op en het beheer van incidenten;
- de dienstverlener moet zijn personeel passend opleiden in de processen en plannen voor de respons op en het beheer van incidenten, om te verzekeren dat zij effectief en efficiënt op incidenten reageren;
- de Dienstvoorwaarden of de SLA's van de dienstverlener moeten duidelijk vermelden welke ondersteuning de overheidsdienst zal ontvangen in het geval van een informatieveiligheidsincident. De dienstverlener moet bijvoorbeeld:
    - De overheidsdienst informeren wanneer een incident wordt gedetecteerd of gerapporteerd dat de veiligheid van zijn informatie of geïnterconnecteerde systemen kan beïnvloeden;
    - Een specifiek contactpunt of -kanaal aanduiden dat de klanten kunnen gebruiken om vermoedelijke informatieveiligheidsincidenten te melden;
    - De rollen en verantwoordelijkheden van elke partij tijdens een informatieveiligheidsincident bepalen;
    - De klanten toegang geven tot bewijzen (bijvoorbeeld auditlogs met tijdstempel en/of forensische momentopnamen van virtuele machines), zodat zij het incident zelf kunnen onderzoeken;
- er moet een geïdentificeerde partij zijn die verantwoordelijk is voor het herstel van gegevens en diensten na een informatieveiligheidsincident;
- na een incident moeten de getroffen klanten rapporten ontvangen die hen in staat stellen om de oorzaak van het incident te begrijpen en met kennis van zaken te beslissen of zij de clouddienst blijven gebruiken;
- het contract moet limieten en voorzieningen inzake verzekering, aansprakelijkheid en vrijwaring voor informatieveiligheidsincidenten bevatten; (opmerking: het is aanbevolen dat de overheidsdiensten de aansprakelijkheids- en vrijwaringsclausules zorgvuldig op uitsluitingen onderzoeken).

Voorgestelde maatregelen om aan de overwegingen te voldoen:

- De volgende beveiligingstoepassing van de Cloud Control Matrix: SEF-01, SEF-02, SEF-03, SEF-04, SEF-05, STA-02, BCR-O2

Details van de aansprakelijkheid voor deze veiligheidsdoelstelling:

Overheidsdienst	Clouddienstverlener

• De overheidsdienst moet de toewijzing van de verantwoordelijkheden voor het beheer van informatieveiligheidsincidenten verifiëren en verzekeren dat ze aan alle eisen van de overheidsdienst voldoet.
• De overheidsdienst moet de clouddienstverlener om informatie verzoeken over de mechanismen waarmee:
  • de overheidsdienst informatieveiligheidsgebeurtenissen die hij heeft opgespoord aan de clouddienstverlener meldt;
  • de clouddienstverlener informatieveiligheidsgebeurtenissen die hij heeft opgespoord aan de overheidsdienst meldt;
  • de overheidsdienst de status van een gemelde informatieveiligheidsgebeurtenis volgt."
• De overheidsdienst en de clouddienstverlener moeten de procedures overeen komen voor de respons op verzoeken om potentieel digitaal bewijsmateriaal of andere informatie uit de cloudcomputingomgeving.
	• "Als onderdeel van de dienstenspecificaties moet de clouddienstverlener de toewijzing van de verantwoordelijkheden voor het beheer van informatieveiligheidsincidenten en de procedures tussen de overheidsdienst en de clouddienstverlener definiëren.
	De clouddienstverlener moet de overheidsdienst documentatie verstrekken over:
	  • het bereik van de informatieveiligheidsincidenten die de clouddienstverlener aan de overheidsdienst zal melden;
	  • het niveau van de onthulling van de opsporing van en respons op informatieveiligheidsincidenten;
	  • de doeltijd voor de melding van informatieveiligheidsincidenten;
	  • de procedure voor de melding van informatieveiligheidsincidenten;
	  • contactinformatie voor de behandeling van zaken in verband met informatieveiligheidsincidenten;
	  • eventuele oplossingen die kunnen worden toegepast indien bepaalde informatieveiligheidsincidenten zich voordoen.
	• De clouddienstverlener moet mechanismen voorzien waarmee:
	  • de overheidsdienst een informatieveiligheidsgebeurtenis aan de clouddienstverlener meldt;
	  • de clouddienstverlener een informatieveiligheidsgebeurtenis aan de overheidsdienst meldt;
	  • de overheidsdienst de status van een gemelde informatieveiligheidsgebeurtenis volgt.
	• De overheidsdienst en de clouddienstverlener moeten de procedures overeen komen voor de respons op verzoeken om potentieel digitaal bewijsmateriaal of andere informatie uit de cloudcomputingomgeving.

Documentbeheer

Historiek

Datum	*Auteur*	*Versie*	*Omschrijving wijzigingen*
17/09/2019	BOSA	V.0.1	Eerste draft
5/10/2019	BOSA	V.1	Update op basis van het commentaar van de FISP-werkgroep
16/10/2019	BOSA	V.1.1	Update op basis van het commentaar van de deelnemers aan FISP
21/11/2019	FISP workgroup	V1.2	Publieke verspreiding

Goedkeuring

Datum	*Goedkeurder(s)*	*Versie*
21/11/2019	FISP workgroup	V1.2

Bronnen

Dit document werd samengesteld met behulp van de volgende bronnen:

- https://www.digital.govt.nz/dmsdocument/1-cloud-computing-information-security-and-privacy-considerations
- https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers/
- GEA-NZ Guide: Managing Shadow Cloud Services
- RICHTLIJN (EU) 2016/1148 VAN HET EUROPEES PARLEMENT EN DE RAAD van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie
- Wet tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&clouddiensten=2019040715&table_name=wet
- VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=NL
- Wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens https://www.timelex.eu/sites/default/files/pdf/Nieuwe-belgische-privacywet-30-07-2018.pdf
- ISO/IEC 27017/27018

Link met een ander beleid

Afhankelijkheid van interne documenten

Ref.	*Titel*
FISPDOC01	Handleiding voor informatiecategorisatie

Positionering van het beleid t.o.v. de ISO 27001-norm

Sectie	*Doelstellingen en referentiemaatregelen*	*In relatie (X = ja)*
4	Context van de organisatie	
5	Leiderschap	
6	Planning	
7	Ondersteuning	
8	Operatie	
9	Evaluatie van de prestaties	
10	Verbeteringen	

Positionering van het beleid t.o.v. de ISO 27002-norm

Sectie	*Doelstellingen en referentiemaatregelen*	*In relatie (X = ja)*	*Doelstellingen/maatregelen (detail)*
A5	Informatiebeveiligingsbeleid		
A6	Organisatie van informatiebeveiliging		
A7	Human Resources Veiligheid		
A8	Asset Management		
A9	Toegangscontrole		
A10	Geheimschrift		
A11	Fysieke en ecologische veiligheid		
A12	Operationele veiligheid		
A13	Beveiliging van communicatie		
A14	Aankoop, ontwikkeling en onderhoud van informatiesystemen		
A15	Relatie met leveranciers		
A16	Beheer informatiebeveiligingsincidenten		
A17	Informatiebeveiliging in Business Continuity Management		
A18	Conformiteit		