Vlaamse overheid

Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens

Advies uit eigen beweging VTC nr. 2022/02 van 11 oktober 2022

betreffende

hosting van persoonsgegevens

AANVULLEND BIJ RICHTLIJN VTC/A/2020/05

De Vlaamse Toezichtcommissie (hierna: "de VTC");

Gelet op het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer (hierna: "het e-govdecreet"), inzonderheid artikel 10/4, §1 en 10/7;

Gelet op de 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 (hierna AVG), inzonderheid artikel 57, 1, c) en artikel 58, 2, a) en 3, AVG;

Gelet op de bespreking op de zitting van de VTC van 17 mei 2022, van 14 juni 2022, van 19 juli 2022, 6 september 2022 en 11 oktober 2022;

Brengt op 11 oktober 2022 het volgend advies uit eigen beweging uit:

A. BESTEMMELINGEN

Dit advies geldt voor alle Vlaamse instanties[1] zoals bedoeld in het e-govdecreet.

Het geldt in eerste instantie voor de Vlaamse Overheid, maar ondermeer ook voor de lokale besturen. De VTC heeft trouwens vastgesteld dat het beleid van de Vlaamse Overheid ook een impact heeft op de mogelijkheden en keuzes van de lokale besturen.

B. PROBLEEMSTELLING

Met 'hosting' wordt bedoeld het opslaan van persoonsgegevens in interne of externe datacenters. Hosting door een leverancier impliceert dat een leverancier toegang kan hebben tot de data (al dan niet in geëncrypteerde vorm).

[1] "instanties" zoals bedoeld in artikel 2, 10° van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer.

De VTC wil nogmaals uiting geven aan haar bezorgdheid dat een overheid, in casu de Vlaamse, heeft gekozen voor een beleid waarbij ze de hosting van belangrijke overheidsdata/persoonsgegevens van haar klanten-burgers frequent en op grote schaal toevertrouwt aan externe partijen waarover ze geen sluitende controle heeft.

Bovendien wordt niet alleen de VTC als toezichthouder, maar worden ook de Vlaamse overheidsinstanties, door de cloud first-strategie (de facto publieke cloud) en het elimineren van de datacenters van de Vlaamse Overheid, voor zo goed als voldongen feiten geplaatst. Instanties kunnen wel beroep doen op andere dan publieke clouddiensten, maar dit wordt nauwelijks ondersteund. (zie uitleg begrippen hierna)

De standaardoplossingen die naar voor worden geschoven zijn meestal publieke cloud oplossingen. Daardoor wordt een andere oplossing dan gebruik van de publieke cloud ontmoedigd, ongeacht de daaraan verbonden risico's. Eén van de grote risico's kan daarmee namelijk niet uitgesloten worden: de onrechtmatige toegang van de dienstverlener.

De aanleiding voor het huidige advies zijn nieuwe beveiligingsmaatregelen die aangeboden worden door de publieke cloud leveranciers en die het mogelijk maken om de data beter af te schermen van de leverancier, zoals geëncrypteerde containers en confidential computing, technieken die vooral gericht zijn op de problematiek van data in use (zie hierna).

In deze zin vormt dit advies een technische aanvulling op het advies VTC/A/2020/05.

C. CONTEXT

Als de cloudtechnieken organisatorisch en technisch veilig aangewend worden, kunnen ze zowel in een publieke, een private als een on-premise cloud opstelling, de beveiliging verhogen door het automatisch toepassen van de nodige controlemechanismen op de desbetreffende omgevingen. Maatregelen die de beveiliging van hostingoplossingen vergroten zijn vanzelfsprekend positief.

Verder stelt de VTC vast dat er enerzijds al zeker naar bijkomende technische oplossingen wordt gezocht door de aanbieders van de publieke cloud platformen (ook als navolging van de bredere Europese bezorgheden hierrond, volgend op het Schrems II-arrest); en anderzijds dat er ook navolging komt van haar advies door bepaalde VO-instanties die beslissen om niet in de publieke cloud te stappen of er uit te stappen, omdat zij van oordeel zijn dat zij de risico's niet sluitend kunnen beheersen.

Dit moet ook in het licht van de algemene verplichting vanuit de AVG om passende maatregelen te nemen rekening houdende met de stand van de technologie gezien te worden.

In het algemeen stelt de VTC vast dat de nieuwe technische oplossingen een duidelijke verbetering inhouden, maar dat de verwerkingsverantwoordelijken nog steeds structureel moeten vertrouwen op de cloud leverancier, die niet kan aantonen dat het onmogelijk is om (eventueel onder dwang) een achterpoort open te zetten. Daarom blijven keuzes voor bepaalde cloudoplossingen niet aanvaardbaar voor sommige verwerkingen, zijn bepaalde verwerkingen enkel mogelijk in een hybride of private setting, en moeten andere met extra maatregelen worden aangevuld.

De VTC geeft in dit advies een schema met controleobjectieven die minimaal moeten gerespecteerd worden. De nadruk ligt daarbij op de doeleinden die bereikt moeten worden wanneer cloudoplossingen aanvaardbaar zijn.

D. BEGRIPPEN EN AANDACHTSPUNTEN

Hierna worden een aantal begrippen verduidelijkt in de context van dit advies. Deze verduidelijking is bedoeld voor de verwerkingsverantwoordelijken en hun adviseurs voor zover die onvoldoende vertrouwd zouden zijn met deze termen (zie ook termen in bijlage).

1. Fase van de data

Daar hostingoplossingen correct begrepen moeten worden vanuit een AVG-perspectief, lijsten we enkele belangrijke fasen op waarin de persoonsgegevens zich kunnen bevinden:

- Data at Rest:
    - Wat wordt ermee bedoeld?: Het gaat bijvoorbeeld over fileshares of databases waar data **opgeslagen** worden.
    - Wat zijn de aandachtspunten?: Er dient gezorgd te worden voor gecontroleerde toegang en waar nodig bv. encryptie (zodat ongeautoriseerden zoals de leverancier geen toegang kunnen krijgen tot deze data – direct of indirect).
- Data in Motion (Transit):
    - Wat wordt ermee bedoeld? De **uitwisseling** van data tussen systemen of processen.
    - Wat zijn de aandachtspunten? Hier dient gezorgd te worden voor afdoende waarborgen m.b.t authenticiteit/integriteit en confidentialiteit. D.w.z. dat ongeautoriseerden - waarmee in het bijzonder in dit advies de leverancier wordt bedoeld, toegang kunnen krijgen tot deze data – direct of indirect.
- Data in Use
    - Wat wordt ermee bedoeld? Dit slaat op de **bewerking** van de data door applicaties.
    - Wat zijn de aandachtspunten? De persoonsgegevens waar bewerkingen op worden uitgevoerd en die beveiligd werden door encryptie, moeten daarvoor in principe gedecrypteerd worden en worden daardoor op dat moment kwetsbaar voor toegang voor onbevoegden.

2. Technieken

De beveiliging van Data at Rest en Data in Motion kan vaak reeds bogen op een hoog niveau van maturiteit. Wat de Data in Use betreft, ziet de VTC technologieën opkomen om controle te houden over welke processen[2] toegang kunnen krijgen tot bepaalde data en deze dus mogen en kunnen verwerken.

Daarnaast kan gebruik gemaakt worden van enkele additionele belangrijke technieken die een fundamentele impact kunnen hebben op het afschermen van de data tegen onbevoegden.

De in het kader van dit advies belangrijkste technieken zijn (zie uitleg in bijlage):

- Containers en Virtuele machines;
- Secure Enclaves;
- inrichten van beheersconsoles / -interfaces;

[2] of containers (zie verder).

- Privileged Access management (PAM) en Privileged Session management (PSM);
- Secret Vaults & Hardware Security Modules;
- Audit Trailing.

3. Types hosting

- **eigen datacenter** (mogelijks op basis van cloudtechnieken):
    - de infrastructuur (hardware en software) behoort toe aan de opdrachtgever-verwerkingsverantwoordelijke, al kan deze op een andere locatie / bij een hosting provider staan[3];
    - de opdrachtgever/verwerkingsverantwoordelijke beslist waar de infrastructuur zich bevindt;
    - het beheer gebeurt via een beheerdersconsole die enkel bereikbaar is voor interne of externe medewerkers van de Vlaamse instanties op het eigen netwerk;
- **private cloud** (hosted bij derde partij specifiek voor de opdrachtgever):
    - de infrastructuur (hardware en software) is ofwel eigendom van de opdrachtgever-verwerkingsverantwoordelijke ofwel van de leverancier/-verwerker;
    - wordt gehost door een externe leverancier/verwerker (privaat netwerk); de opdrachtgever-verwerkingsverantwoordelijke bepaalt zelf waar de data staan;
    - de infrastructuur (servers) wordt niet gedeeld met andere organisaties dan Vlaamse instanties[4];
    - het beheer gebeurt via een aparte beheerdersconsole op het eigen netwerk of via een VPN (of dat van de leverancier)[5];
- **publieke cloud** (gedeeld met derden):
    - de infrastructuur (hardware en software) behoort toe aan de leverancier van de cloudomgeving;
    - de leverancier-verwerker bepaalt op welke locatie de data zich bevinden tenzij contractueel afgedwongen (waarbij aandacht voor back-ups is vereist);
    - de infrastructuur wordt gedeeld met andere organisaties;
    - de data zijn enkel “logisch” afgescheiden van die van anderen waardoor het risico tot toegang tot andere klantenomgevingen veel groter is dan bij eigen of private hosting;
- **hybride cloud**:

  een combinatie van één of meerdere eigen datacenters, private clouds of publieke cloud(s). Dit kan zowel op platform niveau, waarbij een applicatie óf in het publieke óf in het private deel draait, als op applicatieniveau waarbij de applicatie in beide delen draait.

  De VTC gaat ervan uit dat hiermee de belangrijkste types zijn gevat. Deze indeling dekt wel niet alle vormen van hosting of leveranciersrelaties. In het bijzonder wat SaaS[6] betreft, wijst de VTC erop dat het aspect hosting dat erbij hoort de regels volgens de hiervoor beschreven types volgt. Daarbij moet

[3] Tegenover ter plaatse/on prem(ise).
[4] Zo bijvoorbeeld ook tussen lokale besturen.
[5] Virtual Private Network.
[6] Software as a Service.

rekening gehouden worden dat SaaS-toepassingen het minder makkelijk maken om bepaalde extra beveiliging te implementeren (omdat de leverancier externen geen toegang geeft tot zijn toepassing).

E. MAATREGELEN VOOR DE AANVAARDBARE VERWERKINGEN

1. BASISVEREISTEN

Bij elke volgens de matrix in advies VTC/A/2020/02 aanvaardbare verwerking, moet aan volgende **basisvereisten** voldaan zijn:

1. de technische en organisatorische beveiligingsmaatregelen moeten vooraf bepaald zijn en conform het **gevoeligheidsniveau** van de te verwerken informatie[7];
2. de technische en organisatorische beveiligingsmaatregelen moeten voorafgaand aan het in productie nemen **effectief aanwezig** zijn; het volstaat niet dat deze gepland zijn voor de toekomst;
3. processen/verwerkingen moeten duidelijk worden **geïsoleerd/gesegmenteerd**[8] om zodoende te kunnen bepalen welke processen wel/geen toegang krijgen tot bepaalde persoonsgegevens;
4. de technische en organisatorische beveiligingsmaatregelen moeten **op voorhand** worden **getest**. Het testen dient onafhankelijk te gebeuren (d.i. door een ander team dan deze die de toepassing heeft bedacht/gebouwd[9]). In deze test dient ook het risico op toegang door de cloudprovider tot persoonsgegevens expliciet te worden meegenomen;
5. alle datacenters waar de persoonsgegevens gehost worden, moet zich bevinden in een **EU lidstaat**[10];
6. bij elke externe hosting moet er een **recht op verificatie** (bijvoorbeeld via een audit) tijdens de loop van het contract bedongen worden. Ook hier is de bedoelde verificatie in de eerste plaats, maar niet uitsluitend, bedoeld om te verzekeren dat de encryptie en andere beveiliging niet te doorbreken is door of met medewerking van de cloudleverancier.

2. MINIMALE MAATREGELEN PER CATEGORIE VERWERKINGEN

Volgende tabellen bevatten een overzicht van de maatregelen die, op basis van de inzichten van de VTC, beschouwd moeten worden als deel van de huidige stand van de techniek bij hosting in de cloud. De VTC verwacht dan ook dat de overeenstemmende maatregelen **minimaal** worden genomen bij elke hosting in de cloud. Zonder de hiervoor vermelde beschermende maatregelen zijn de bedoelde publieke cloud toepassingen in principe onaanvaardbaar. Het zijn controleobjectieven die niet uitsluiten dat hetzelfde resultaat op andere manieren wordt bereikt. Als de voorgestelde maatregelen niet kunnen gevolgd worden, vraagt de VTC dat het project aan haar wordt voorgelegd voor advies. Ook wanneer deze maatregelen worden genomen kan er natuurlijk een advies worden gevraagd.

Als er meerdere categorieën verwerkingen van toepassing zijn, gelden de strengste maatregelen.

---

[7] Het dataclassificatieraamwerk van de Vlaamse Overheid kan daarbij gehanteerd worden. De VTC wijst er wel op dat het raamwerk, in het bijzonder de aan de classificatie gekoppelde maatregelen, door haar niet werd gevalideerd. Het is dus mogelijk dat de maatregelen vermeld in huidig advies daarvan afwijken.

[8] Bij één verwerkingsverantwoordelijke kan segmentatie o.b.v. gebruikersbeheer voldoende zijn. Als er verschillende verantwoordelijken zijn, dan is isolatie gewenst.

[9] Intern of extern volgens wat bepaald werd in de matrix van advies VTC/A/2022/05.

[10] of de EER met daarin naast de EU-lidstaten ook Ijsland, Liechtenstein en Noorwegen. Het Verenigd Koninkrijk is sinds 1 januari 2021 ook geen lid meer van de Europese Economische Ruimte.

1) Bescherming van Data at Rest

Bescherming van "data at rest" is in alle gevallen een noodzaak (en hangt samen met secrets management en gebruik van HSMs). De mate waarin hangt echter af van de gevoeligheid van de informatie:

Type informatie	Minimale maatregel
Persoonsgegevens (niet grootschalig)	Afscheiding / Isolatie noodzakelijk (+encryptie in geval v cloud)
Unieke Identificatoren[11] (niet grootschalig)	Afscheiding / Isolatie noodzakelijk (+encryptie in geval v cloud)
Gevoelige gegevens (niet grootschalig en tijdelijk)	Afscheiding / Isolatie + Encryptie noodzakelijk (BYOK[12])
Gegevens met evt. zware negatieve impact	Afscheiding / Isolatie + Encryptie noodzakelijk (BYOK)
Risico-gevoelige personen[13]	Afscheiding / Isolatie + Encryptie m.i.v. eigen HSM noodzakelijk
Grootschalige verwerking[14]	Afscheiding / Isolatie + Encryptie m.i.v. eigen HSM noodzakelijk

Met "eigen" wordt hier bedoeld dat dat niet gedeeld wordt met andere partijen dan Vlaamse instanties (eventueel wel andere Belgische overheid).

2) Bescherming van Data in Motion

Bescherming van "data in motion" is in alle gevallen een noodzaak (en hangt samen met secrets management en gebruik van HSMs). De mate waarin hangt echter af van de gevoeligheid van de data:

Type informatie	Minimale maatregel
Persoonsgegevens (niet grootschalig)	TLS en sterke authenticatie noodzakelijk
Unieke Identificatoren (niet grootschalig)	TLS en sterke authenticatie noodzakelijk
Gevoelige gegevens (niet grootschalig en tijdelijk)	TLS en sterke authenticatie noodzakelijk (BYOK)
Gegevens met evt. zware negatieve impact	TLS en sterke authenticatie noodzakelijk (BYOK)
Risico gevoelige personen	TLS en sterke authenticatie (m.i.v. eigen HSM) noodzakelijk
Grootschalige verwerking	TLS en sterke authenticatie (m.i.v. eigen HSM) noodzakelijk

Met "eigen" wordt hier bedoeld dat dat niet gedeeld wordt met andere partijen dan Vlaamse instanties (eventueel wel andere Belgische overheid).

3) Bescherming van Data in Use

:

Type informatie	Minimale maatregel
Persoonsgegevens (niet grootschalig)	Confidential computing / Secure Enclaves mogelijk
Unieke Identificatoren (niet grootschalig)	Confidential computing / Secure Enclaves mogelijk
Gevoelige gegevens (niet grootschalig en tijdelijk)	Confidential computing / Secure Enclaves aangeraden
Gegevens met evt. zware negatieve impact	Confidential computing / Secure Enclaves gewenst
Risico gevoelige personen	Confidential computing / Secure Enclaves noodzakelijk
Grootschalige verwerking	Confidential computing / Secure Enclaves noodzakelijk

[11] Identificatoren zoals het rijksregisternummer of een telefoonnummer (voor zover geregistreerd op naam van een persoon), waarmee een natuurlijke persoon over verschillende systemen heen uniek kan mee geïdentificeerd worden.
[12] Bring your own key.
[13] Zoals bedoeld in punt 9 van de DPIA-lijst van de VTC samengelezen met criterium 7 van de Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679 (WP248).
[14] Zoals bedoeld in noot 8 van de DPIA-lijst van de VTC samengelezen met criterium 5 van de WP248(ja?).

4) Beheersomgeving

Degelijke controle op wie toegang kan krijgen tot de onderliggende infrastructuur is van groot belang zodat het "omzeilen", uitschakelen of op andere wijze ondergraven van beoogde maatregelen door **instellingen** aan te passen niet mogelijk zou zijn.

Type informatie	Minimale maatregel
Persoonsgegevens (niet grootschalig)	Minimaal logische segmentatie noodzakelijk
Unieke Identificatoren (niet grootschalig)	Minimaal logische segmentatie noodzakelijk
Gevoelige gegevens (niet grootschalig en tijdelijk)	Minimaal logische segmentatie noodzakelijk
Gegevens met evt. zware negatieve impact	Aparte beheersomgeving – afgescheiden van andere klanten[15] noodzakelijk
Risico gevoelige personen	Aparte beheersomgeving – afgescheiden van andere klanten noodzakelijk
Grootschalige verwerking	Aparte beheersomgeving – afgescheiden van andere klanten noodzakelijk

5) Privileged Access Management (PAM)

Degelijke controle op **wie** toegang kan krijgen tot de configuratie van de omgeving / applicaties / toegangsregels, ed. is van groot belang zodat ongeautoriseerde wijzigingen niet mogelijk zou zijn. De mate waarin hangt echter af van de gevoeligheid van de informatie:

Type informatie	Minimale maatregel
Persoonsgegevens (niet grootschalig)	Basiscontroles m.b.t. beheerstoegangen noodzakelijk
Unieke Identificatoren (niet grootschalig)	Basiscontroles m.b.t. beheerstoegangen noodzakelijk
Gevoelige gegevens (niet grootschalig en tijdelijk)	Basiscontroles m.b.t. beheerstoegangen noodzakelijk
Gegevens met evt. zware negatieve impact	Gebruik van eigen PAM/PSM noodzakelijk
Risico gevoelige personen	Gebruik van eigen PAM/PSM noodzakelijk
Grootschalige verwerking	Gebruik van eigen PAM/PSM noodzakelijk

Met "eigen" wordt hier bedoeld dat dat niet gedeeld wordt met andere partijen dan Vlaamse instanties (eventueel wel andere Belgische overheid).

6) Secrets Management & HSMs

Gecontroleerd beheer van en toegang tot secrets en cryptografische sleutels is fundamenteel voor de beveiliging van data, toegang tot systemen, communicatie, etc. De mate van beveiliging van deze secrets en sleutels hangt echter af van de gevoeligheid van de informatie:

Type informatie	Minimale maatregel
Persoonsgegevens (niet grootschalig)	Minimaal secrets / keys afgeschermde software omgeving
Unieke Identificatoren (niet grootschalig)	Minimaal secrets / keys afgeschermde software omgeving
Gevoelige gegevens (niet grootschalig en tijdelijk)	Gebruik van secrets vaults noodzakelijk
Gegevens met evt. zware negatieve impact	Gebruik van eigen secrets vault en HSM noodzakelijk
Risico gevoelige personen	Gebruik van eigen secrets vault en HSM noodzakelijk
Grootschalige verwerking	Gebruik van eigen secrets vault en HSM noodzakelijk

Met "eigen" wordt hier bedoeld dat dat niet gedeeld wordt met andere partijen dan Vlaamse instanties (eventueel wel andere Belgische overheid).

[15] Al dan niet Vlaamse instanties.

7) Toegangs- en gebruikersbeheer

Degelijke controle van wie toegang kan krijgen tot de bepaalde acties/data is van belang zodat ongeautoriseerde toegang tot / verwerking van data niet mogelijk zou zijn. De mate waarin hangt echter af van de gevoeligheid van de informatie:

Type informatie	Minimale maatregel
Persoonsgegevens (niet grootschalig)	Sterke authenticatie en duidelijke autorisatie noodzakelijk.
Unieke identificatoren (niet grootschalig)	Sterke authenticatie en duidelijke autorisatie noodzakelijk.
Gevoelige gegevens (niet grootschalig en tijdelijk)	Sterke authenticatie en duidelijke autorisatie noodzakelijk.
Gegevens met evt. zware negatieve impact	Sterke authenticatie en eigen toegangs-/gebruikersbeheer noodzakelijk
Risico gevoelige personen	Sterke authenticatie en eigen toegangs-/gebruikersbeheer noodzakelijk
Grootschalige verwerking	Sterke authenticatie en eigen toegangs-/gebruikersbeheer noodzakelijk

Met "eigen" wordt hier bedoeld dat dat niet gedeeld wordt met andere partijen dan Vlaamse instanties (eventueel wel andere Belgische overheid). Het systeem en de processen die daarvoor gebruikt worden moeten voor 100% onder (beheers)controle van een Vlaamse instantie staan.

Opmerking: als een organisatie een toegangs-/gebruikersbeheer heeft dat meerdere (interne en externe) systemen beveiligt (bv. het ACM/IDM van Digitaal Vlaanderen), moet dat ook "apart" bekeken worden als een verwerking en moet dus ook aan de in dit advies gestelde regels voor de hosting voldoen.

8) Audit Trailing

Het kunnen volgen van toegang tot en wijzigingen van infrastructuur-configuraties, applicatie-configuraties, applicatieve toegangen, uitgevoerde wijzigingen is van groot belang. Ook hier is het minimale niveau echter afhankelijk van de gevoeligheid van de data:

Type informatie	Minimale maatregel
Persoonsgegevens (niet grootschalig)	Basis Audit Trailing (toegangen) noodzakelijk
Unieke identificatoren (niet grootschalig)	Basis Audit Trailing (toegangen) noodzakelijk
Gevoelige gegevens (niet grootschalig en tijdelijk)	Audit Trailing naar eigen omgeving noodzakelijk
Gegevens met evt. zware negatieve impact	Gedetailleerde Audit Trailing naar eigen omgeving noodzakelijk
Risico gevoelige personen	Gedetailleerde Audit Trailing naar eigen omgeving noodzakelijk
Grootschalige verwerking	Gedetailleerde Audit Trailing naar eigen omgeving noodzakelijk

Onder "eigen omgeving" wordt verstaan een omgeving die 100% onder controle van de Vlaamse Overheid staan.

3. ANDERE MAATREGELEN

In de voorgaande adviezen werden door de VTC en haar voorganger met dezelfde bezorgdheid voor ogen (afscherming van de leverancier) flankerende maatregelen voorgesteld, ondermeer[16]:
- in advies A/2016/01: algemene maatregelen voor cloudcomputing;
- in advies A/2020/05: maatregelen als pseudonimisering en inschakelen van een TTP;
- in advies A/2021/12: beperkingen bij gebruik van kantoortoepassingen.

[16] Zie https://overheid.vlaanderen.be/digitale-overheid/informatieveiligheid/andere-adviezen-en-aanbevelingen-over-cloud

Gezien het belang van de dataclassificatie en de criteria die de VTC heeft gesteld voor de aanvaardbaarheid en de maatregelen, is een voor de hand liggende (maar niet altijd gemakkelijk te realiseren) maatregel het verschillend aanpakken van de verwerkingen volgens die classificatie en criteria, m.a.w. diversifiëren (al dan niet met een hybride model).

F. BESLUIT

De VTC adviseert dat alle Vlaamse instanties rekening houden met de hiervoor vermelde eisen.

De VTC verwacht dat alle Vlaamse instanties uitdrukkelijk de hiervoor vermelde elementen opnemen in de evaluatie die bepalend is voor de keuze van verwerker, i.c. voor datacenterdiensten. Als een leverancier de maatregelen niet kan nemen, moet een andere leverancier gezocht worden.

Ze adviseert om ook dringend werk te maken van alternatieve oplossingen zoals eigen datacenters en private cloudtoepassingen. Een hybride hostingmodel is daarbij dus een mogelijkheid.

Hans Graux

Voorzitter VTC

Getekend door:Hans Graux (Signature)
Getekend op:2022-11-09 17:13:22 +01:0
Reden:Ik keur dit document goed

BIJLAGE: Lexicon

- Confidential Computing:

  Confidential Computing beschermt gegevens in gebruik door berekeningen uit te voeren in een op hardware gebaseerde Trusted Execution Environment. Deze veilige en geïsoleerde omgevingen voorkomen ongeautoriseerde toegang of wijziging van applicaties en gegevens terwijl ze in gebruik zijn, waardoor het beveiligingsniveau van organisaties die gevoelige en gereguleerde gegevens beheren, wordt verhoogd[17].

  Hardwarefuncties die gecodeerde gegevens in het geheugen isoleren en verwerken, zodat de gegevens minder risico lopen op blootstelling en compromittering door gelijktijdige workloads of het onderliggende systeem en platform[18].

- Containers

  Een methode voor het verpakken en veilig uitvoeren van een toepassing binnen een toepassingsvirtualisatieomgeving. Ook wel een toepassingscontainer of een servertoepassingscontainer genoemd[19]

- Virtuele machines:

  Een virtueel gegevensverwerkingssysteem dat ter beschikking lijkt te staan van een bepaalde gebruiker, maar waarvan de functies worden bereikt door de bronnen van een echt gegevensverwerkingssysteem te delen[20].

- Secure Enclaves:

  Een set systeembronnen die in hetzelfde beveiligingsdomein werken en die de bescherming van één gemeenschappelijke, continue beveiligingsperimeter delen[21].

- Beheersconsoles / -interfaces

  Omgeving die men hanteert voor het beheersen van zijn cloudomgeving / zijn containers / de communicatie / enz.

- Privileged Access management (PAM) en Privileged Session management (PSM)

  PAM is de omgeving die toelaat aan beperkt aantal supergebruikers om op gecontroleerde wijze toegang te krijgen tot de besturingsconsoles (niet te verwarren met de het toegangsbeheer van de gewone gebruikers).

  PSM bepaalt wat iemand mag doen die ingelogd heeft met een superuser account voor toegang tot systemen of een sessie op de server. De monitoring van zo een sessie behoort ook tot PSM.

- Secret Vaults & Hardware Security Modules:

  Faciliteiten die toelaten allerhande secrets22 en cryptografische sleutels beveiligd op te slaan (en die ervoor zouden moeten zorgen dat enkel geautoriseerde processen er toegang toe kunnen krijgen).

- Audit Trailing:

  Faciliteiten die toelaten te traceren welke toegangen / bewerkingen / wijzigingen werden toegepast op de omgeving, applicaties en data.

[17] https://csrc.nist.gov/glossary/term/confidential_computing
[18] NISTIR 8320
[19] https://csrc.nist.gov/glossary/term/container
[20] https://csrc.nist.gov/glossary/term/vm
[21] https://csrc.nist.gov/glossary/term/enclave
[22] Sleutel (niet noodzakelijk cryptografisch) die toegang geeft tot andere services bv. een API-key.