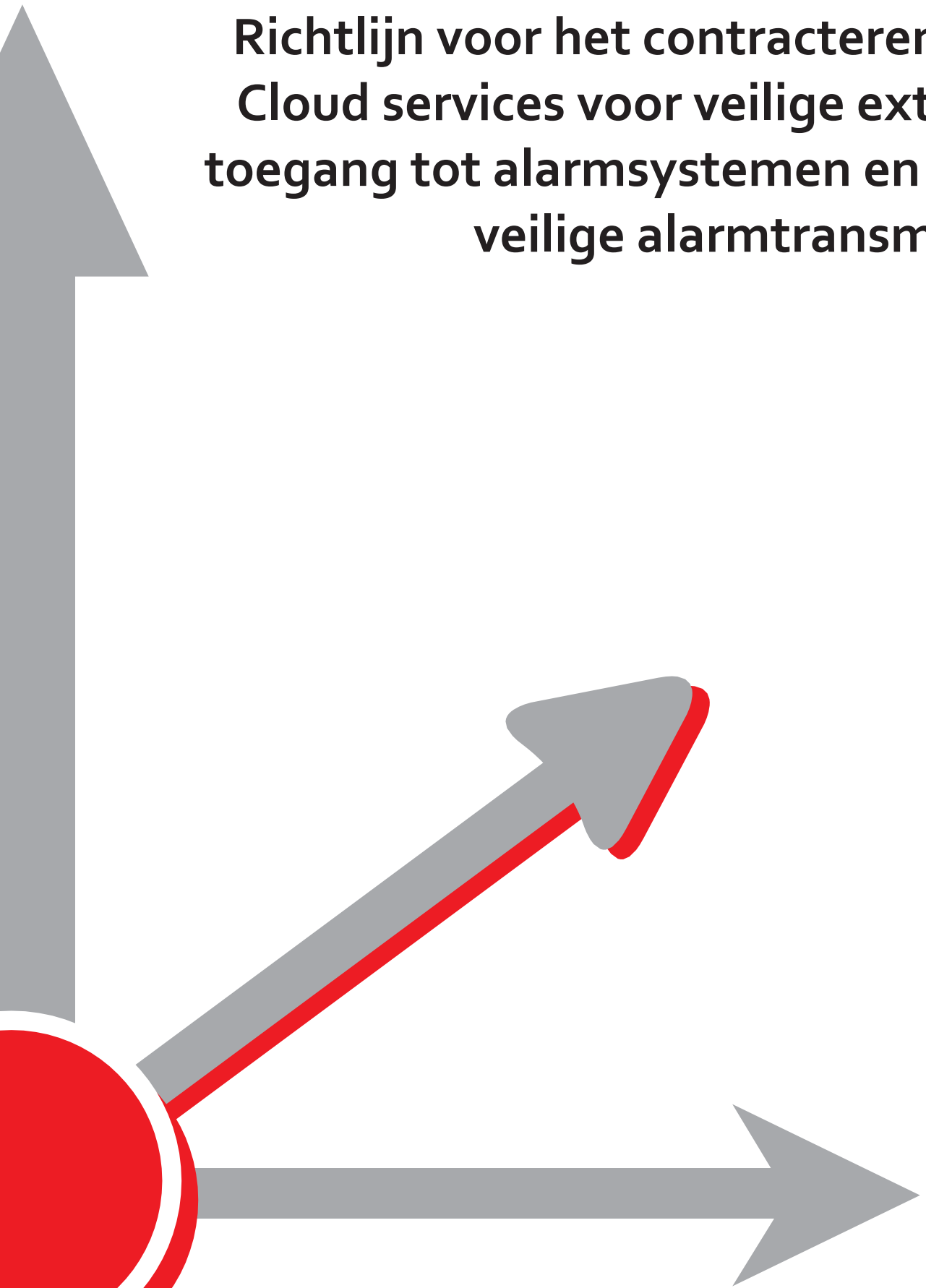
Richtlijn voor het contracteren van Cloud services voor veilige externe toegang tot alarmsystemen en voor veilige alarmtransmissie



Wijzigingstabel

Datum	Rev. #	Paragraaf/Pagina	Wijziging
Februari 2025	1.0		Eerste uitgave

VOORWOORD

Dit document is bedoeld als algemene richtlijn en is geen vervanging voor gedetailleerd advies in specifieke omstandigheden. Hoewel er grote zorg is besteed aan de samenstelling en voorbereiding van deze publicatie om de nauwkeurigheid te garanderen, kan Euralarm in geen geval aansprakelijkheid aanvaarden voor fouten, omissies of gegeven advies of voor enig verlies dat voortvloeit uit het vertrouwen op informatie in deze publicatie.

DISCLAIMER

Dit document is uitsluitend bedoeld als richtlijn voor Euralarm-leden en, indien van toepassing, hun leden, over de stand van zaken met betrekking tot het onderwerp. Hoewel alles in het werk is gesteld om de nauwkeurigheid ervan te garanderen, mogen lezers niet vertrouwen op de volledigheid of juistheid ervan, noch het beschouwen als een juridische interpretatie. Euralarm is niet aansprakelijk voor het verstrekken van onjuiste of onvolledige informatie.

Opmerking: De Engelse versie van dit document is het goedgekeurde referentiedocument van Euralarm.

Copyright Euralarm

Euralarm • Gubelstrasse 11 • CH-6300 Zug • Switzerland

E: secretariat@euralarm.org
W: www.euralarm.org

Inhoudsopgave

1. Inleiding

Het wordt steeds gebruikelijker om de nieuwste technologie te gebruiken om IP-gebaseerde alarmtransmissie en externe toegang tot brandveiligheidssystemen en/of beveiligingssystemen (FSSS) te bieden en als zodanig een deel van de apparatuur buiten de locatie van de FSSS-serviceprovider te plaatsen. Dit document zal FSSS-serviceproviders (bijvoorbeeld installateurs) ondersteunen bij het gebruik van de diensten van een datacenter om een deel van de apparatuur onder te brengen.

Twee verschillende gebruikssituaties worden hier behandeld, met hun specifieke vereisten en doelgroepen.

- Eén gebruikssituatie is alarmtransmissie via een Alarm Transmission System (ATS) dat wordt bediend en beheerd door een Alarm Transmission Service Provider (ATSP) waarbij beschikbaarheid, transmissietijd, foutmelding en bescherming tegen vervanging belangrijke kenmerken zijn. De norm voor Alarm Transmission Systems (ATS) EN 50136-1 staat gehoste configuraties toe waarbij het cloudelement zich op een beveiligde locatie moet bevinden, wat een datacenter kan zijn. De hoogste categorieën van ATS omvatten beveiligingsvereisten die in het hele systeem moeten worden nageleefd. Richtlijnen voor deze gebruikssituatie zijn gericht op elke entiteit die de rol van ATSP op zich neemt.
- Een ander gebruikssituatie is externe toegang tot de FSSS via een Remote Access Infrastructure (RAI) die wordt beheerd en aangestuurd door een Remote Access Infrastructure Service Provide (RAISP) waarbij beveiligde toegang tot de FSSS en de gegevens belangrijke kenmerken zijn, terwijl beschikbaarheid voornamelijk voor gemak is. De technische specificatie voor de Remote Access Infrastructure (RAI) CLC/TS 50136-10 vereist dat de Remote Access Server (RAS) zich op een beveiligde locatie bevindt en bevat vereisten voor de beveiliging van de overgedragen gegevens. De richtlijnen voor deze gebruikssituatie zijn gericht op elke entiteit die de rol van RAISP op zich neemt, met name op kleine en middelgrote FSSS-serviceproviders die van plan zijn de rol van RAISP op zich te nemen en niet bekend zijn met Cloud services en externe services willen leveren in overeenstemming met EN 50710.

Hoewel er verschillende goede redenen zijn om cloudoplossingen te overwegen, moeten FSSS-serviceproviders zich bewust zijn van de impact op hun bedrijf, waaronder beschikbaarheid, servicelevel agreements, gegevensbeveiliging, naleving, juridische en contractuele vereisten. FSSS-serviceproviders zullen nog steeds moeten aantonen dat ze voldoen aan bestaande normen, bijvoorbeeld prestaties en beschikbaarheid, back-ups, toegangscontrole, enz. De verantwoordelijkheden voor onderhoud moeten duidelijk worden begrepen en geaccepteerd door alle belanghebbenden. Deze omvatten levenscyclusbeheer voor besturingssystemen, platforms (bijv. database, virtualisatie, enz.) en applicaties. De FSSS- serviceprovider moet kunnen bevestigen dat deze activiteiten zijn uitgevoerd in overeenstemming met de verwachtingen van de FSSS- serviceprovider en de serviceovereenkomsten.

Het opslaan, het delen en de beveiliging van gegevens zijn van vitaal belang en vereisen juridische overwegingen die verder gaan dan wat dit document stelt. Daarom probeert dit document deze juridische vereisten niet te interpreteren of er richtlijnen voor te geven.

Belangrijke gedeelten van de huidige richtlijn zijn afkomstig uit de BSIA-richtlijn "ARC-overwegingen bij het gebruik van datacenters of Cloud services", met de nodige toestemming van BSIA. EURALARM is de British Security Industry Association, haar lid, dankbaar voor deze bijdrage.

Deze richtlijn geeft een beschrijving van belangrijke concepten met betrekking tot Cloud services, beschouwt

relevante normen en biedt een overzicht van de juridische criteria voor de keuze van de CSP. De richtlijn pretendeert echter niet alle juridische vereisten van individuele landen binnen Europa te behandelen. Er moet zorgvuldig rekening worden gehouden met de richtlijn in de context van lokale wetgevende vereisten die voorrang hebben.

2. Afkortingen

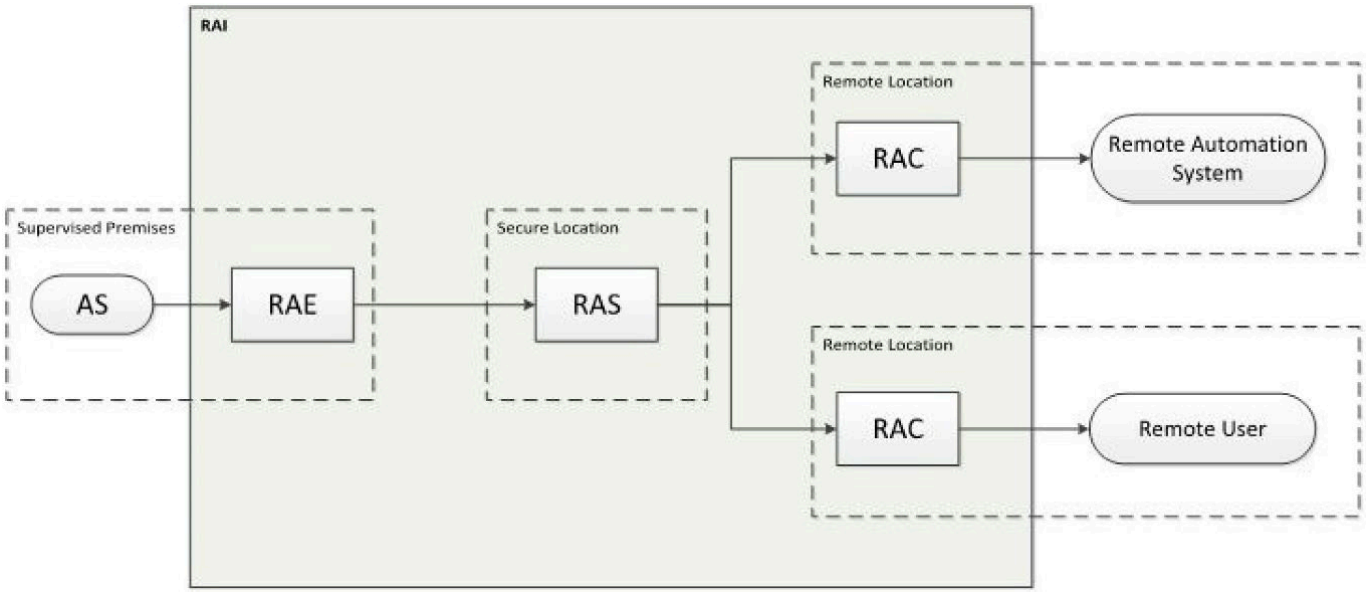
AICPA: American Institute of Certified Public Accountants (Amerikaans Instituut voor Gecertificeerde Openbare Accountants)
AMS: Alarm Management System (Alarmbeheersysteem)
ANSI: American National Standards Institute (Amerikaans Nationaal Instituut voor Standaarden)
ARC: Alarm Receiving Centre (Alarmcentrale)
AS: Alarm System (Alarmsysteem)
ATS: Alarm Transmission System (Alarmtransmissiesysteem)
BSIA: British Security Industry Association (Britse Vereniging voor de Beveiligingsindustrie)
CLC: CENELEC (Europese Commissie voor Elektrotechnische Normalisatie)
CSP: Cloud Service Provider (Cloudserviceprovider)
EN: European Standard (Norm) - (Europese Norm)
FaaS: Function as a Service (Functie als een Dienst)
FSSS: Fire Safety Systems and/or Security Systems (Brandveiligheidssystemen en/of Beveiligingssystemen)
IaaS: Infrastructure as a Service (Infrastructuur als een Dienst)
IEC: International Electrotechnical Committee (Internationale Elektrotechnische Commissie)
ISO: International Standardisation Organisation (Internationale Organisatie voor Standaardisatie)
IT: Information Technology (Informatie Technologie)
MARC: Monitoring and Alarm Receiving Centre (Monitoring- en Alarmcentrale)
PaaS: Platform as a Service (Platform als een Dienst)
PSTN: Public Switched Telephone Network (Openbaar geschakeld telefoonnetwerk)
RAC: Remote Access Client (Cliënt voor Externe Toegang)
RAE: remote Access Endpoint (Eindpunt voor Externe Toegang)
RAI: Remote Access Infrastructure (Infrastructuur voor Externe Toegang)
RAS: Remote Access Server (Server voor Externe Toegang)
RCT: Receiving Centre Transceiver (Ontvangstcentrum Transceiver)
RCT-A: RCT at the ARC (RCT in de ARC)
RCT-H: Hosted RCT (Gehoste RCT)
SaaS: Software as a Service (Software als een Dienst)
SLA: Service Level Agreement (Service Level Overeenkomst)
SOC: System and Organization Controls (Systeem- en Organisatiebeheersmaatregelen)
SPT: Supervised Premises Transceiver (Toezichthoudende Locatie Transceiver)
TIA: Telecommunications Industry Association (Telecommunicatie Industrie Associatie)
TS: Technical Specification (Technische Specificatie)

3. Onderwerp

Dit document behandelt het cloudelement van een Remote Access Infrastructure (RAI, gebruikt om externe toegang te krijgen tot functionaliteiten van de FSSS) en van een Alarm Transmissie Systeem (ATS, gebruikt om alarmen van de FSSS naar het Alarm Receiving Centre te verzenden).

3.1. Externe toegang tot FSSS

In het geval van een RAI wordt dit cloudelement geïdentificeerd als de RAS in Figuur 1.

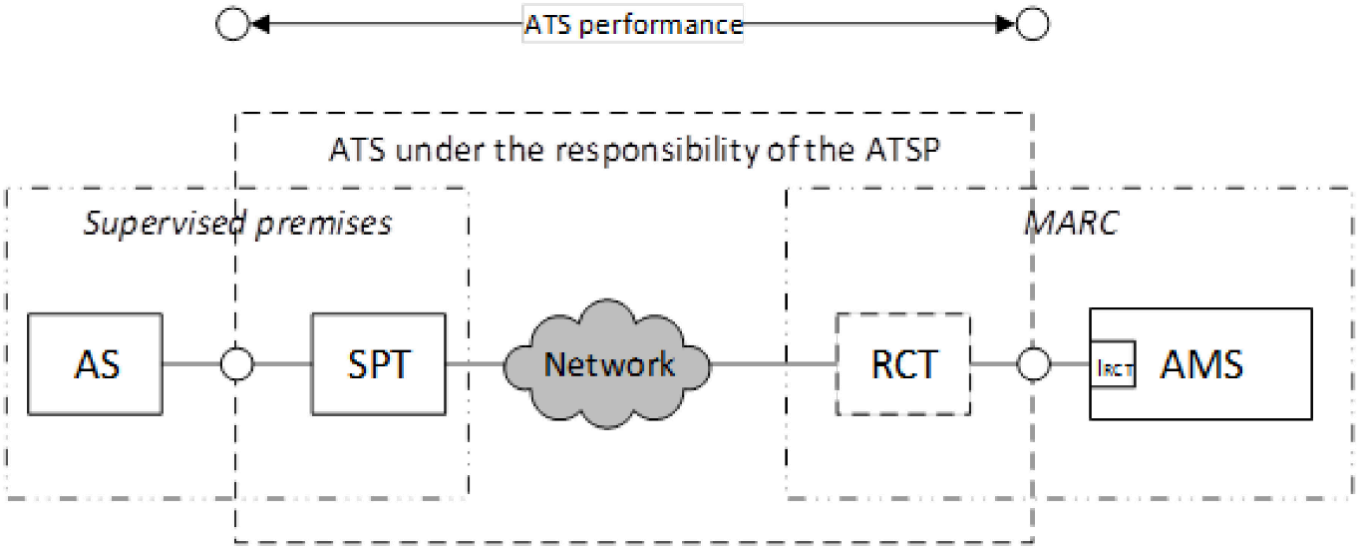


Figuur 1. Logisch diagram van de Remote Access Infrastructure (overgenomen uit CLC/TS 50136-10:2022)

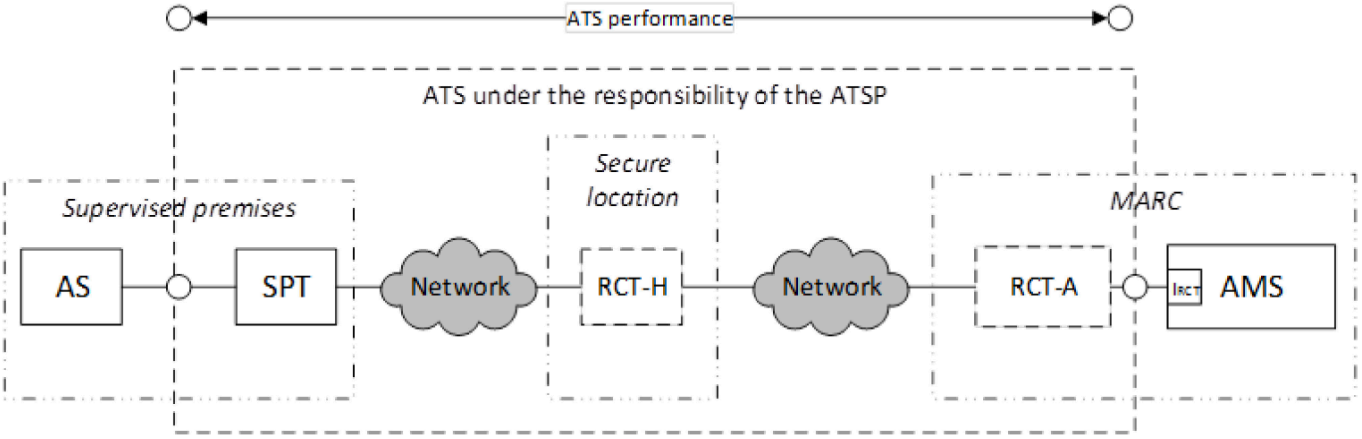
3.2. Alarmtransmissie

In het geval van een ATS staat de Europese norm een niet-gehoste configuratie toe, zoals weergegeven in Figuur 2a. In deze configuratie wordt een directe verbinding tot stand gebracht tussen het alarmsysteem (AS) en de ARC (MARC). De norm staat ook een gehoste configuratie toe, zoals weergeven in Figuur 2b. In deze configuratie komen alarmmeldingen van meerdere alarmsystemen samen in een ontvanger die is gehost in een datacenter en is geïdentificeerd als RCT-H, waar ze worden verwerkt, bevestigd en opgeslagen en de ARC er toegang toe krijgt via een beveiligd communicatiepad. Overwegingen om de veranderingen van PSTN-communicatie naar IP-alarmtransmissie aan te pakken, zijn in 2019 gegeven in een Euralarm-whitepaper: "New Generation Networks for alarm communications"[1]. De FSSS-serviceprovider moet ervoor zorgen dat de ATS voldoet aan EN 50136-1, de SPT voldoet aan EN 50136-2 en de RCT, RCT-H en RCT-A voldoen aan EN 50136-3 (zie A2.2 in Bijlage 2 voor uitleg van die normen). Dit garandeert dat de hele ATS de alarmmeldingen op tijd aflevert en wordt gecontroleerd op storingen in de alarmtransmissie.

[1] https://www.euralarm.org/resource-report/white-paper-new-generation-networks-for-alarm-communications.html



Figuur 2a. Voorbeeld van een **niet-gehost** alarmtransmissiesysteem (overgenomen uit EN 50136-1/A1:2018)



Figuur 2b. Voorbeeld van een **gehost** alarmtransmissiesysteem (overgenomen uit EN 50136-1/A1:2018)

3.3. Algemeen

De huidige richtlijn schetst de overwegingen van de FSSS-serviceprovider bij het kiezen van de services van een datacenter of Cloud services. Dit helpt bij het bepalen in hoeverre de FSSS- serviceprovider veilig en betrouwbaar gehost (of gedeeltelijk gehost) kan worden in een cloudomgeving.

Een FSSS-serviceprovider beschermt voortdurend levens en eigendommen en in dit opzicht zijn de vereisten kritischer dan bij de meeste andere organisaties.

4. Cloudomgevingen

4.1. Inleiding

Zorgvuldigheid is cruciaal bij het evalueren en selecteren van cloud serviceproviders. Zorgvuldigheid verwijst naar het grondig onderzoeken en beoordelen van potentiële leveranciers of serviceproviders voordat je een zakelijke relatie met hen aangaat. Dit proces helpt om een beter inzicht te krijgen in de capaciteiten, betrouwbaarheid, beveiligingsmaatregelen en algehele geschiktheid van de provider voor je specifieke behoeften.

Drie omgevingen worden klassiek gedefinieerd als: **Private business** cloudoplossing, Data Centre Hosted (hierna **Data Centre**) of Native Cloud (hierna **Cloud**). De FSSS-serviceprovider kan een of meer van deze omgevingen gebruiken om de technische apparatuur te bedienen die de externe toegang of de alarmtransmissie vormt, of de oplossing gebruiken die door de fabrikant van de FSSS wordt aangeboden.

Dit document impliceert niet dat Private business cloudoplossingen of Cloudomgevingen de enige operationele modus zijn voor alle toepassingen, maar er is een erkenning dat de FSSS-serviceprovider toepassingen in meerdere omgevingsmodellen kan en zal bedienen. Met andere woorden, afhankelijk van de servicevereisten kunnen zij alle drie de operationele omgevingen in meer of mindere mate benutten.

FSSS- serviceproviders moeten ook rekening houden met hun certificeringsvereisten van derden bij het kiezen van een eigen oplossing (private business), een datacentrum of een cloudoplossing.

Het gebruik van datacenters/Cloud services sluit de verantwoordelijkheden van de FSSS-serviceprovider niet uit, zoals vastgelegd in EN 16763, EN 50710 of EN 50136-1 (zie A2.2 in Bijlage 2 voor uitleg over die normen). Er is een Euralarm- richtlijn[2] gepubliceerd die speciaal is bedoeld voor de implementatie van externe diensten en die te vinden is op de Euralarm website. Deze richtlijn helpt de FSSS-serviceprovider bij het vooraf controleren van de naleving van de vereisten van deze normen.

4.2. Private business cloudoplossing

Private business oplossingen worden beheerd door de FSSS-serviceprovider. De servers worden geïnstalleerd in hetzelfde gebouw of terrein waar de FSSS-serviceprovider is gevestigd of in een ander gebouw onder de verantwoordelijkheid van de FSSS-serviceprovider. Een applicatieprovider levert het servicebedrijf de software om op servers te draaien. Servers worden aangeschaft door de FSSS-serviceprovider of gekocht als onderdeel van de service van de applicatieprovider.

Upgrades van serverbesturingssystemen, databases en de applicatiesoftware worden gecoördineerd tussen de FSSS-serviceprovider en de applicatieprovider. Beveiliging (encryptie in rust etc.) en betrouwbaarheid (zoals databasereplicatie met geografische diversiteit) zijn doorgaans oplossingen die door de applicatieprovider worden ontwikkeld.

4.3. Datacenter

Datacenteroplossingen zijn servers die zijn geïnstalleerd op een locatie die wordt beheerd door een derde partij die fysieke beveiliging, stroom en rackruimte biedt om servers te huisvesten. Deze servers kunnen specifiek voor een bepaalde FSSS- serviceprovider worden ingezet of werken in een multi-tenantomgeving. Deze servers worden onderhouden door de FSSS-serviceprovider of door de applicatieprovider als een beheerde service.

4.4. Cloud

4.4.1. Beschrijving

[2] https://www.euralarm.org/resource/guidance-on-remote-services---final-xlsx.html

Cloudoplossingen omvatten alle kenmerken van de datacenteroplossing, maar de servers en andere gerelateerde technologieën (databases etc.) worden geleverd en onderhouden door de Cloud serviceprovider (bijv. AWS - Amazon Web Services, Microsoft Azure, Google Cloud, IBM). Het Cloud Shared Responsibility Model (SRM) is een kader dat de verantwoordelijkheden tussen een Cloud serviceprovider en de applicatieprovider voor het beveiligen van de Cloud omgeving afbakent.

De Cloud serviceprovider beschermt de activa van de omgeving van de applicatieontwikkelaar. Ze bieden bijvoorbeeld fysieke beveiliging en beveiligen de virtualisatieservices. De applicatieprovider beveiligt de activa in zijn Cloud instantie, wat betekent dat de applicatieprovider het besturingssysteem beveiligt dat ze op servers installeren en beheert wie toegang heeft tot je Cloud omgeving.

Cloud computing omvat verschillende modellen die inspelen op verschillende behoeften en gebruikssituaties. Het is belangrijk om op te merken dat deze modellen niet wederzijds exclusief zijn en dat Cloud serviceproviders vaak een combinatie hiervan aanbieden om in te spelen op verschillende vereisten en voorkeuren. In de volgende secties worden 4 verschillende Cloud modellen beschreven.

4.4.2. Infrastructure as a Service (IaaS)

Dit model biedt virtuele rekeneenheden via het internet. Het biedt virtuele machines, opslag en netwerken die gebruikers kunnen inrichten en beheren. Gebruikers hebben meer controle over de infrastructuur, inclusief besturingssystemen en applicaties.

4.4.3. Platform as a Service (PaaS)

PaaS biedt een platform voor ontwikkelaars om applicaties te bouwen, implementeren en beheren zonder zich zorgen te hoeven maken over de onderliggende infrastructuur. Het biedt een vooraf geconfigureerde omgeving met tools, frameworks en runtime voor applicatieontwikkeling. Gebruikers kunnen zich richten op codering en applicatielogica, terwijl het platform zorgt voor schaalbaarheid, load balancing en implementatie.

4.4.4. Serverless Computing

Serverless computing is een model waarbij ontwikkelaars code schrijven en implementeren als afzonderlijke functies of eenheden van code. De cloud serviceprovider beheert de infrastructuur en schaalt en levert automatisch middelen op basis van de vraag. Ontwikkelaars hoeven zich geen zorgen te maken over servers of infrastructuurbeheer en kunnen zich volledig richten op het schrijven van code.

4.4.5. Software as a Service (SaaS)

SaaS is een complete softwaretoepassing die via internet wordt geleverd. Eindgebruikers van de FSSS of FSSS-serviceproviders kunnen de software openen en gebruiken zonder dat installatie of beheer nodig is. Providers van SaaS-oplossingen draaien hun servers in IaaS-, PaaS- of Serverless computing-modellen.

4.4.6. Overwegingen voor native Cloud modellen

Bij het kiezen van een omgeving voor een bedrijfskritische applicatie is het belangrijk om de specifieke vereisten en beperkingen zorgvuldig te overwegen. Factoren zoals prestatiebehoeften, schaalbaarheidsvereisten,

beheeropties en kostenoverwegingen moeten worden afgewogen om de best passende oplossing voor de doelstellingen van de applicatie te bepalen.

Zie Bijlage 1 voor meer informatie.

4.5. Oplossing van de fabrikant

Fabrikanten van FSSS hebben hun oplossingen ontwikkeld en bieden deze aan de FSSS-serviceproviders aan via hun systemen. Een dergelijke oplossing kan gebaseerd zijn op een van de 3 hierboven beschreven omgevingen. De FSSS-serviceprovider hoeft zich geen zorgen te maken over het onderhoud van de servers, software en applicatie. Hij moet zorgen voor een contractuele overeenkomst die past bij zijn behoeften en verwachtingen.

Gewoonlijk heeft de FSSS-serviceprovider geen contract met de fabrikant voor het gebruik van zijn oplossing, maar hij accepteert de voorwaarden door in te loggen op de cloudapplicatie. Daarom wordt geadviseerd dat de fabrikant een document voor de installateur opstelt waarin hij duidelijk is over zijn cloudapplicatie:

- Welke Cloud service provider wordt gebruikt,
- Waar de data zich bevindt,
- Hoe de gegevens toegankelijk zijn, inclusief beveiligingsmaatregelen,
- Serviceniveau, zoals hersteltijd en onderhoud,
- Naar welke certificering de fabrikant kan verwijzen,
- hoe de FSSS service provider de FSSS correct moet verbinden,
- ...

4.6. Overwegingen voor operationele omgevingen

Private-bedrijfscloudoplossingen en datacenteroplossingen vereisen investeringen in hardware, software en infrastructuur, evenals de expertise om deze op te zetten en te onderhouden. Cloud gebaseerde oplossingen vereisen nog steeds dat de applicatieprovider de vaardigheden heeft om de vereiste functionaliteit te begrijpen, te monitoren en op te schalen. De Cloud serviceprovider bundelt gespecialiseerde IT-services voor de implementatie en het onderhoud van de hardware, besturingssystemen en databasesoftware.

Er moeten stappen worden ondernomen om rekening te houden met de beveiliging van gegevens die toegankelijk zijn via online of Cloud gebaseerde verbindingen.

5. Juridische criteria voor de locatie van servers

5.1. Inleiding

De regelgeving voor dataservers in Europese landen wordt beheerst door een combinatie van nationale wetten en regelgeving van de Europese Unie. Hier volgt een overzicht van de belangrijkste regels in verschillende Europese landen, evenals het overkoepelende EU-kader.

5.2. European Union General Data Protection Regulation (GDPR)

De GDPR, van kracht sinds mei 2018, is de primaire regelgeving voor gegevensbescherming en privacy in de EU. Deze is van toepassing op alle lidstaten en omvat:

- beginselen van gegevensverwerking: rechtmatigheid, eerlijkheid, transparantie, doelbinding, gegevensminimalisatie, juistheid, opslagbeperking, integriteit en vertrouwelijkheid;
- rechten van betrokkenen: recht op toegang, rectificatie, verwijdering (recht om vergeten te worden), beperking van verwerking, gegevensportabiliteit en bezwaar;
- gegevensoverdracht: beperkingen op de overdracht van persoonsgegevens buiten de EU/EER, waarbij passende beschermingsniveaus worden gewaarborgd;
- meldingen van datalekken: verplichting om autoriteiten en getroffen personen binnen 72 uur op de hoogte te stellen van datalekken.

5.3. Voorbeelden van land specifieke regelgeving

Duitsland

Federale wet op gegevensbescherming (Bundesdatenschutzgesetz, BDSG): vult de GDPR aan met aanvullende vereisten, waaronder strengere regels voor gegevensverwerking voor arbeidsdoeleinden en specifieke verplichtingen voor functionarissen voor gegevensbescherming.

Frankrijk

Wet bescherming persoonsgegevens (Loi Informatique et Libertés): handhaaft GDPR-bepalingen en voegt nationale specificaties toe, zoals regels voor de verwerking van gezondheidsgegevens en extra bevoegdheden voor de nationale gegevensbeschermingsautoriteit (CNIL).

Verenigd Koninkrijk

Wet op gegevensbescherming 2018: implementeert GDPR en bevat specifieke bepalingen voor gegevensverwerking door overheidsinstanties en wetshandhavingsinstanties. Na Brexit heeft het VK de UK GDPR aangenomen, die de EU GDPR weerspiegelt maar onafhankelijk functioneert.

Italië

Gegevensbeschermingscode (Codice in materia di protezione dei dati personali): sluit aan bij GDPR, met aanvullende nationale regels voor gegevensverwerking voor wetenschappelijk en historisch onderzoek en journalistieke doeleinden.

Spanje

Organieke wet op gegevensbescherming en digitale rechten (LOPDGDD): vult GDPR aan met specifieke regels over digitale rechten en extra bescherming voor minderjarigen en kwetsbare personen.

Nederland

Uitvoeringswet GDPR: vult GDPR aan met nationale bepalingen, met name met betrekking tot de verwerking van strafrechtelijke gegevens en personeelsgegevens.

België

Belgische uitvoeringswet (Gegevensbeschermingsautoriteit GBA) kaderwet van 30 juli 2018

De gemeenschappelijke thema's in de verschillende landen zijn:

- lokalisatie van gegevens: sommige landen hebben specifieke vereisten voor lokalisatie van gegevens, met name voor gevoelige gegevens zoals medische dossiers;
- sectorspecifieke regelgeving: veel landen leggen aanvullende regelgeving op voor bepaalde sectoren, zoals financiën, gezondheidszorg en telecommunicatie;
- Gegevensbeschermingsautoriteiten (Data Protection Authorities, DPA's): elk land heeft een nationale DPA die verantwoordelijk is voor de handhaving van wetten inzake gegevensbescherming en de behandeling van klachten. Voorbeelden hiervan zijn CNIL in Frankrijk, ICO in het VK en BfDI in Duitsland;
- grensoverschrijdende gegevensoverdrachten: EU-landen volgen over het algemeen het GDPR-kader voor internationale gegevensoverdrachten, dat mechanismen omvat zoals standaardcontractbepalingen (SCC's), bindende bedrijfsvoorschriften (BCR's) en adequaatheidsbesluiten.

Deze lijst met landspecifieke wetgevingen is niet exhaustief. Voor meer specifieke regelgeving en de laatste updates is het raadzaam om de respectieve nationale DPA's en wetteksten in elk land te raadplegen.

5.4. Nuttige referenties

- Europese Commissie - Gegevensbescherming[3]
- GDPR Tekst[4]
- CNIL (Frankrijk)[5]
- ICO (Verenigd Koninkrijk)[6]
- BfDI (Duitsland)

6. Verdeling van rollen en verantwoordelijkheden

6.1. Impact van onderhoudsactiviteiten (gepland/ongepland)

De beschikbaarheid van de infrastructuur kan verschillende kritieke niveaus hebben, afhankelijk van de services die ermee worden geleverd. Alarmtransmissieservices vereisen een hoge beschikbaarheid die is gedefinieerd door de toepasselijke categorie uit EN 50136-1. Beschikbaarheid wordt over het algemeen als minder kritisch beschouwd voor services voor externe toegang.

De FSSS-serviceprovider (of de fabrikant in een oplossingsomgeving van de fabrikant)) moet beschikken over processen voor het beheren en waar nodig beperken van onderhoudsactiviteiten, bijv. secundaire systeembeschikbaarheid of gedupliceerde infrastructuur, enz.

FSSS-serviceproviders die een gehoste oplossing overwegen, moeten ervoor zorgen dat er overeenkomsten (SLA's) zijn met de Cloud serviceproviders om ervoor te zorgen dat de FSSS-serviceprovider vooraf op de hoogte wordt gesteld van de duur van offline periodes tijdens gepland onderhoud. Deze overeenkomsten moeten ook de aanpak en communicatie rondom ongepland onderhoud omvatten.

Wanneer FSSS-serviceproviders afhankelijk zijn van derden voor IT-services, moet de FSSS-serviceprovider overwegen hoe incidenten van invloed kunnen zijn op het vermogen van de IT-serviceprovider om ondersteuning te bieden.

6.2. IT- competentie

De FSSS-serviceprovider is uiteindelijk verantwoordelijk voor zijn eigen apparatuur en systemen en heeft een bepaald niveau van lokale IT-competentie nodig om ervoor te zorgen dat routinematige monitoring en onderhoudsactiviteiten van de FSSS-oplossing worden beheerd.

6.3. Beveiliging

[3] https://commission.europa.eu/law/law-topic/data-protection_en
[4] https://eur-lex.europa.eu/eli/reg/2016/679/oj
[5] https://www.cnil.fr/en
[6] https://ico.org.uk

FSSS-serviceproviders moeten overwegen wie toegang heeft tot hun systemen en gegevens en welke eisen er worden gesteld aan personeelsscreening. Er zijn verschillende opties om beveiligingsuitdagingen aan te pakken, waaronder:

- Identiteits- en toegangsbeheer (IAM)
- Encryptie
- Beveiligingsmonitoring en logging
- Naleving en certificeringen
- Netwerkbeveiliging.

Datacenteroplossingen vereisen on-site personeel en/of externe toegang om de infrastructuur te beheren en te onderhouden, inclusief hardware-onderhoud, software-upgrades en beveiligingspatches. Cloudoplossingen worden daarentegen beheerd door de Cloud serviceprovider, die al het infrastructuuronderhoud, software-upgrades en beveiligingspatches afhandelt, waardoor interne IT-personeel zich kan richten op de kernactiviteiten.

In elke Cloud omgeving is er een gedeelde verantwoordelijkheid tussen de Cloud Service Provider (CSP) en de gebruiker (FSSS-serviceprovider of fabrikant). Beveiligingsaspecten zoals gegevensclassificatie, netwerkcontroles en fysieke beveiliging hebben duidelijke eigenaren nodig. De verdeling van deze verantwoordelijkheden staat bekend als het shared responsibility model (SRM) voor Cloud beveiliging. Bekijk dit schema om te zien waar de verantwoordelijkheden liggen binnen verschillende Cloud omgevingen.

Private business cloudoplossing	**Infrastructuur als een dienst *IaaS***	**Platform als een dienst *PaaS***	**Software als een dienst *SaaS***
Gegevens & Configuraties	Gegevens & Configuraties	Gegevens & Configuraties	Gegevens & Configuraties
Applicatiecode	Applicatiecode	Applicatiecode	Applicatiecode
Schaalbaarheid	Schaalbaarheid	Schaalbaarheid	Schaalbaarheid
Runtime	Runtime	Runtime	Runtime
Besturingssysteem	Besturingssysteem	Besturingssysteem	Besturingssysteem
Virtualisatie	Virtualisatie	Virtualisatie	Virtualisatie
Hardware	Hardware	Hardware	Hardware
Beheerd door de FSSS service provider of fabrikant			
Beheerd door de Cloud serviceprovider			

Meer informatie en richtlijnen over SRM zijn te vinden op de website van het Center for Internet Security (CIS)[7].

7. Cloudservices contracteren

De Europese Commissie schreef in 2012 in haar mededeling getiteld "Unleashing the potential of cloud computing in Europe"[8]:

> *"Traditionele IT-outsourcingovereenkomsten werden doorgaans onderhandeld en hadden betrekking op gegevensopslag, verwerkingsfaciliteiten en services die gedetailleerd en vooraf werden gedefinieerd en beschreven. Cloud computing-contracten creëren daarentegen in wezen een kader waarin de gebruiker toegang*

[7] https://www.cisecurity.org/insights/blog/shared-responsibility-cloud-security-what-you-need-to-know
[8] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

heeft tot oneindig schaalbare en flexibele IT-mogelijkheden op basis van zijn behoeften. Momenteel wordt de grotere flexibiliteit van Cloud computing in vergelijking met traditionele outsourcing echter vaak gecompenseerd door verminderde zekerheid voor de klant vanwege onvoldoende specifieke en gebalanceerde contracten met Cloud providers.

De complexiteit en onzekerheid van het juridische kader voor Cloud service providers betekent dat ze vaak complexe contracten of service level agreements gebruiken met uitgebreide disclaimers. Het gebruik van "take-it-or-leave-it" standaardcontracten kan kostenbesparend zijn voor de provider, maar is vaak onwenselijk voor de gebruiker, inclusief de eindgebruiker. Dergelijke contracten kunnen ook de keuze van toepasselijk recht opleggen of het herstel van gegevens belemmeren. Zelfs grotere bedrijven hebben weinig onderhandelingsmacht en contracten voorzien vaak niet in aansprakelijkheid voor gegevensintegriteit, vertrouwelijkheid of servicecontinuïteit."

Om deze complexiteit en onzekerheid aan te pakken, kunnen gedetailleerde richtlijnen over belangrijke contractuele elementen worden gevonden in de "Guidelines on outsourcing to cloud service providers"[9] die in 2021 door de European Securities and Markets Authority (esma) in verschillende Europese talen zijn uitgegeven. Met name de volgende secties van het document kunnen relevant zijn:

- Richtlijn 3 – Belangrijke contractuele elementen
- Richtlijn 4 – Informatiebeveiliging
- Richtlijn 5 – Exitstrategieën
- Richtlijn 6 – Toegangs- en auditrechten.

OPMERKING: Vergelijkbare richtlijnen zijn ook te vinden op de website van de European Insurance and Occupational Pensions Authority (eiopa)[10].

Bovendien bereidt de Europese Commissie in het kader van de Data Act ((EU) 2023/2854) standaardcontractbepalingen voor om belanghebbenden te begeleiden bij de implementatie van de bepalingen met betrekking tot het wisselen van Cloud serviceprovider en het delen van gegevens. Deze leidraad zal naar verwachting in de loop van 2025 worden gepubliceerd.

Tot slot bevat bijlage 2 van deze Euralarm-richtlijn een verwijzing naar normen en certificeringsschema's waaraan naleving kan worden vereist in het contract met de Cloud serviceprovider.

Meer informatie over cloudcomputingcontracten is te vinden op de website van de EC:

- "Cloud computing contracts"[11]
- "Comparative study on cloud computing contracts"[12]

8. Conclusie

Aangezien er geen uniek of uniform certificeringsschema is voor datacenters en Cloud services, moet de FSSS-serviceprovider ervan verzekerd zijn dat de CSP ervoor zorgt dat het datacenter voldoet aan de benodigde betrouwbaarheids- en beveiligingsvereisten voor het overwogen gebruiksscenario. Elke nalevingsverklaring die door de CSP of fabrikant wordt geclaimd om de betrouwbaarheid en beveiliging van de Cloud service aan te

[9] https://www.esma.europa.eu/document/guidelines-outsourcing-cloud-service-providers
[10] https://www.eiopa.europa.eu/system/files/2020-04/guidelines_on_outsourcing_to_cloud_service_providers_en.pdf
[11] https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/cloud-computing/cloud-computing-contracts_en
[12] https://op.europa.eu/en/publication-detail/-/publication/40148ba1-1784-4d1a-bb64-334ac3df22c7

tonen, moet ten minste de volgende overwegingen omvatten:

- betreffende het gebruikte datacenter:
  - de naam en locatie(s);
  - het niveau van bedrijfscontinuïteitsgarantie van geen continuïteit tot volledige continuïteit in geval van een datacenterstoring (cruciaal voor alarmtransmissie en gemak voor externe toegang);
  - middelen om het risico op uitval te minimaliseren, zoals de keuze van één of meerdere locaties, de structuur van het gebouw, stroomvoorzieningssystemen, koelsystemen, mechanische systemen, architectuur, fysieke beveiliging, cyberbeveiliging, bekabelingsinfrastructuur, telecommunicatiesystemen, back-upbeleid, brandbeveiliging en veiligheid (cruciaal voor alarmtransmissie en gemak voor externe toegang);
- betreffende de Cloud service:
  - gebruikte Cloud omgeving;
  - duidelijke en begrepen verdeling van rollen en verantwoordelijkheden op de juiste manier vastgelegd in een SLA;
  - Disaster Recovery Plan (DRP) aanwezig (cruciaal voor alarmtransmissie en gemak voor externe toegang);
  - testplan na een software-update;
  - melding van de FSSS-serviceprovider in geval van systeemupdates, software-updates of verandering van providers;
- betreffende de cyberbeveiliging en privacy van datacenter en Cloud service:
  - naleving van ISO/IEC 27001;
  - certificaat onder het EUCS-certificeringsschema (indien beschikbaar, zie A2.6);
  - veilige toegangscontrolemechanismen met authenticatie om toegang te krijgen tot opgeslagen gegevens en functies;
  - encryptie van gegevens in transit;
  - beperking van de effecten van (D)DOS-aanvallen;
  - proces voor het afhandelen van kwetsbaarheden;
  - verificatie via penetratietesten;
- voor alarmtransmissie:
  - naleving van de ATS volgens de EN 50136-1 in een opgegeven categorie die geschikt is voor het beschermde risico (transmissietijd, beschikbaarheid, rapportagetijd in geval van mislukte transmissies, encryptievereiste, vervangingsbeveiliging, bevestigingsmodus enz.);
  - dual path (DP)-categorie waar hoge risico's worden gedekt of voor vitale (levensbedreigende) systemen;
- voor externe toegang tot FSSS:
  - naleving van de RAI volgens CLC/TS 50136-10.

9. Bibliografie

"ARC considerations when utilising data centre or cloud services", BSIA (British Security Industry Association), uitgave 1, oktober 2023.

Bijlage 1 - Datacenter/IaaS en serverloos

Voor een bedrijfskritische applicatie hebben zowel IaaS (Infrastructure as a Service) als serverloze omgevingen hun voor- en nadelen. Hier volgen enkele vergelijkingen tussen beide:

- Beheerscomplexiteit: in een IaaS-omgeving hebben gebruikers volledige controle over de infrastructuur, wat betekent dat ze verantwoordelijk zijn voor taken zoals het inrichten en beheren van servers, het configureren van netwerken en het garanderen van hoge beschikbaarheid. Dit vereist meer expertise, tijd en middelen vergeleken met een Serverless-omgeving, waar het infrastructuurbeheer wordt geabstraheerd. Met Serverless kunnen applicatieproviders zich uitsluitend richten op het leveren van softwareservices, maar ze hebben minder inzicht in de onderliggende infrastructuur, wat een beperking kan zijn voor bepaalde bedrijfskritische applicaties.

- Schaalbaarheid: In een IaaS-omgeving vereist het schalen van de infrastructuur om toegenomen verkeer of vraag aan te kunnen, handmatige interventie en configuratie. Aan de andere kant schalen serverless-omgevingen automatisch de resources op basis van het aantal verzoeken of gebeurtenissen die worden geactiveerd, waardoor een meer dynamische schaalbaarheid mogelijk is. Serverless kan echter bepaalde beperkingen hebben op het gebied van schaalbaarheid, zoals het maximum aantal gelijktijdige uitvoeringen of de uitvoeringsduur, wat van invloed kan zijn op veeleisende toepassingen.

- Cold start en prestaties: Serverloze omgevingen hebben vaak een concept dat 'cold start' wordt genoemd, waarbij de eerste uitvoering van een functie extra latentie met zich meebrengt vanwege de noodzaak om de runtime-omgeving te initialiseren. Deze latentie kan van invloed zijn op realtime- of low-latency-applicaties. In een IaaS-omgeving worden applicaties uitgevoerd op dedicated servers of virtuele machines, die doorgaans consistente prestaties bieden zonder koude startvertragingen. Daarnaast kunnen serverloze omgevingen beperkingen hebben op resources die zijn toegewezen aan individuele functies, wat de prestaties van resource-intensieve applicaties kan beïnvloeden.

- Vendor Lock-In: Hoewel zowel IaaS- als serverloze omgevingen een zekere mate van vendor lock-in met zich meebrengen, hebben serverloze omgevingen vaak nauwer geïntegreerde services en event-driven architecturen, wat het lastiger kan maken om applicaties te migreren tussen verschillende Cloud service providers of naar on-premises infrastructuur. In een IaaS-omgeving hebben gebruikers meer flexibiliteit om hun applicaties tussen verschillende providers te verplaatsen of zelfs naar hun eigen infrastructuur te brengen.

- Kosten en voorspelbaarheid: Serverless-omgevingen volgen een pay-per-use-prijsmodel, wat kosteneffectief kan zijn voor applicaties met sporadische of variabele workloads. De prijsstructuur kan echter soms complex en onvoorspelbaar zijn, vooral door extra kosten voor API-aanroepen, gegevensoverdracht en resourcegebruik. In een IaaS-omgeving hebben gebruikers meer controle over resourcetoewijzing en -prijzen, waardoor de kosten beter voorspelbaar zijn, maar de vaste kosten mogelijk hoger liggen.

Bijlage 2 - Normen en certificeringsschema's

A2.1. Inleiding

Hieronder staan de belangrijkste normen met betrekking tot alarmtransmissie, externe toegang en datacenters die nuttig kunnen zijn bij het bepalen van de prestaties van een systeem of dienst op gebied van veerkracht, robuustheid en betrouwbaarheid.

A2.2. Normen voor alarmtransmissie, externe toegang tot alarmsystemen en externe services

EN 50136-1 Algemene eisen voor alarmtransmissiesystemen

Deze Europese norm specificeert de vereisten voor de prestaties, betrouwbaarheid en beveiligingskenmerken van alarmtransmissiesystemen. De norm specificeert de vereisten voor alarmtransmissiesystemen die alarmoverdracht verzorgen tussen een alarmsysteem op een bewaakte locatie en de meldapparatuur in een alarmcentrale.

Deze Europese norm is van toepassing op transmissiesystemen voor alle soorten alarmmeldingen, zoals brand, inbraak, toegangscontrole, sociaal alarm, enz.

Een FSSS-serviceprovider die de rol van ATSP (Alarm Transmission Service Provider) op zich neemt, moet voldoen aan de bepalingen van deze norm.

CLC/TS 50136-10 Alarmsystemen - Vereisten voor externe toegang

Dit document specificeert minimumvereisten voor een beveiligde verbinding en sessie voor externe toegang tot een of meer alarmsystemen, bijvoorbeeld brandbeveiligingssystemen, inbraak- en overvalalarmsystemen, elektronische toegangscontrolesystemen, externe perimeterbeveiligingssystemen, videobewakingssystemen en sociale alarmsystemen.

Dit document specificeert de vereisten voor de prestaties, betrouwbaarheid, integriteit en beveiligingskenmerken van een externe toegangsinfrastructuur.

Dit document specificeert de vereisten voor een Remote Access Infrastructure tussen een Remote Access Client en een alarmsysteem op de bewaakte locatie en kan worden geïntegreerd als onderdeel van de ATS of een aparte infrastructuur.

Een FSSS-serviceprovider die de rol van RAISP (Remote Access Infrastructure Service Provider) op zich neemt, moet voldoen aan de bepalingen van deze technische specificatie.

EN 50710 Vereisten voor het leveren van beveiligde externe services voor brandveiligheidssystemen en beveiligingssystemen

Dit document specificeert de minimale vereisten voor het leveren van beveiligde externe services via een Remote Access Infrastructure (RAI), uitgevoerd op locatie of op afstand (bijv. via IP-verbindingen) voor de volgende

systemen:

a) brandveiligheidssystemen, waaronder, maar niet beperkt tot, branddetectie- en brandalarmsystemen, vaste brandbestrijdingssystemen, rook- en warmteregelsystemen;
b) beveiligingssystemen, waaronder, maar niet beperkt tot, inbraak- en overvalalarmsystemen, elektronische toegangscontrolesystemen, externe perimeterbeveiligingssystemen en videobewakingssystemen;
c) sociale alarmsystemen;
d) geluidssystemen voor noodgevallen;
e) een combinatie van dergelijke systemen;
f) beheersystemen die zijn aangesloten op systemen a) t/m e).

Deze norm is bedoeld als aanvulling op EN 16763 – *Diensten voor brandveiligheidssystemen en beveiligingssystemen.*

A2.3. Norm voor Cloud services

CEN/TS 18026 Driedelige benadering voor een set cybersecurityvereisten voor Cloud services

Deze technische specificatie (TS) biedt een set cybersecurityvereisten voor Cloud services. Deze TS is van toepassing op organisaties die Cloud services aanbieden en hun subserviceorganisaties.

Opmerking: deze nieuwe TS wordt naar verwachting in de zomer van 2024 gepubliceerd.

A2.4. Norm voor informatiebeveiligingsmanagementsystemen

ISO/IEC 27001 Informatiebeveiliging, cyberbeveiliging en privacybescherming - Beheersystemen voor informatiebeveiliging - Vereisten

ISO/IEC 27001 is een algemeen erkende internationale norm die de beste praktijken schetst voor het implementeren en onderhouden van een Information Security Management System (ISMS). Deze norm biedt een kader voor het beheer van informatiebeveiligingsrisico's, waaronder mensen, processen en technologie.

ISO/IEC 27001 dekt alle aspecten van informatiebeveiliging, waaronder vertrouwelijkheid, integriteit en beschikbaarheid, en vereist dat organisaties controles implementeren om de vertrouwelijkheid, integriteit en beschikbaarheid van hun informatiemiddelen te waarborgen.

De norm vereist ook dat organisaties een risico gebaseerde aanpak van informatiebeveiligingsbeheer hanteren, waarbij risico's worden geïdentificeerd en beoordeeld, passende controles worden geïmplementeerd om deze risico's te beperken en de effectiviteit van de controles voortdurend wordt bewaakt en beoordeeld.

Door ISO/IEC 27001 te implementeren, kunnen organisaties hun toewijding bij informatiebeveiliging aantonen en belanghebbenden de zekerheid bieden dat hun informatieactiva op een veilige en effectieve manier worden beheerd. De norm is van toepassing op organisaties van alle groottes en industrieën en wordt algemeen erkend als een benchmark voor informatiebeveiligingsbeheer.

A2.5. Normen voor datacenters

ISO/IEC 22237 (en 50600) Informatietechnologie - Datacenterfaciliteiten en -infrastructuren

ISO 22237 is de ISO-normenreeks die het ontwerp, de structuur, de werking en de fysieke en informatiebeveiliging van datacenters regelt. De bedoeling van de norm is om de noodzakelijke voorwaarden te definiëren om de doelstellingen van ISO 27001 te kunnen bereiken in een datacenteromgeving.

De EN 50600 is de EN-normenreeks die voorziet in de planning, het ontwerp, de inkoop, de integratie, de installatie, de werking en het onderhoud van faciliteiten en infrastructuren binnen datacenters. Hoewel de EN 50600-reeks vergelijkbare bepalingen biedt als de ISO 22237-normen, zijn ze niet volledig op elkaar afgestemd.

EN 50600 is een groeiende familie van normen die momenteel uit de volgende delen bestaat:

- EN 50600-1, Algemene concepten
- EN 50600-2-1, Gebouwconstructie
- EN 50600-2-2, Stroomvoorziening en -distributie
- EN 50600-2-3, Klimaatbeheersing
- EN 50600-2-4, Telecommunicatie bekabelingsinfrastructuur
- EN 50600-2-5, Beveiligingssystemen
- EN 50600-3-1, Management- en operationele informatie
- EN 50600-4-1, Overzicht van en algemene vereisten voor belangrijke prestatie-indicatoren
- EN 50600-4-2, Doeltreffendheid stroomverbruik
- EN 50600-4-3, Hernieuwbare energie-factor
-

EN 50600 voorziet in een classificatiesysteem gebaseerd op de belangrijkste criteria beschikbaarheid, veiligheid en energie-efficiëntie:

1. Beschikbaarheidsklasse (Availability Class - AC): AC-classificatie is gedefinieerd in de gebieden van stroomvoorziening, ventilatie- en airconditioningsystemen en bekabeling;
2. Beschermingsklasse (Protection Class - PC): PC is gedefinieerd voor inbraakpreventie, brandbeveiliging, rookbeveiliging en bescherming tegen milieugevaren. Er moeten minimaal drie beschermingsklassen worden gevormd;
3. Granulariteitsniveau (Granularity Level - GL): Het vermogen voor energiezuinige werking wordt gedefinieerd door middel van meetkwaliteiten en meetbereik voor de ventilatie- en airconditioningsystemen. De norm onderscheidt drie verschillende granulariteitsniveaus;

Voor een datacenterontwerp om aan deze norm te voldoen:

a. Moet er een bedrijfsrisicoanalyse worden uitgevoerd;
b. Moet er een geschikte AC-klasse worden geselecteerd met behulp van de bedrijfsrisicoanalyse;
c. Moet er een geschikte PC zijn voor de datacenterpaden en -ruimtes;
d. Moet er een geschikt energie-efficiëntieniveau, GL, worden toegepast;
e. Moeten het ontwerpproces en de ontwerpprincipes worden toegepast.

Opmerking: Momenteel houden datacenters doorgaans geen rekening met EN 50600 of ISO 22237. Datacenters (AWS, ...) zijn doorgaans gecertificeerd door het private Uptime Institute (Tier Certification) en/of volgens ANSI/TIA-942. Deze 2 certificeringsschema's worden als complementair beschouwd.

Uptime Institute Tier-certificering

Deze particuliere certificeringsinstantie hanteert haar eigen Tier-standaarden voor de beschikbaarheid en algehele prestaties van datacenters. Er zijn verschillende prestatieniveaus mogelijk die rekening houden met zowel de gebouwde omgeving als de aanpak en prestaties van het operationele team. Er zijn 4 niveaus

gedefinieerd:

- Tier I: Basiscapaciteit: Voor onderhoud of reparaties zijn volledige site-shutdowns vereist. Capaciteits- of distributiestoringen hebben invloed op de site.
- Tier II: Redundante capaciteitscomponenten: Volledige site-shutdowns voor onderhoud blijven noodzakelijk. Capaciteitsstoringen kunnen invloed hebben op de site. Distributiestoringen hebben invloed op de site.
- Tier III: Gelijktijdig onderhoudbaar: Elke capaciteitscomponent en distributie pad op een site kan op geplande basis worden verwijderd voor onderhoud of vervanging zonder dat dit gevolgen heeft voor de operaties. De site is nog steeds blootgesteld aan een apparatuur storing of een operatorfout.
- Tier IV: Fouttolerant: Een individuele apparatuur storing of onderbreking van het distributie pad heeft geen invloed op de operaties. Een fouttolerante site is ook gelijktijdig onderhoudbaar.

ANSI/TIA-942 Norm voor Telecommunicatie-infrastructuur voor Datacenters

ANSI/TIA-942 is een norm die is gepubliceerd door de Telecommunications Industry Association (TIA) en die richtlijnen biedt voor het ontwerp en de bouw van datacenters, waaronder energiesystemen, mechanische systemen, architectuur, beveiliging, telecommunicatiesystemen, brandbeveiliging en veiligheid. De norm is bedoeld om ervoor te zorgen dat datacenters betrouwbaar, veilig en schaalbaar zijn om te voldoen aan de veranderende behoeften van de IT-industrie.

ANSI/TIA-942 biedt een uitgebreid kader voor datacenterontwerp, inclusief aanbevelingen voor locatieselectie, gebouwstructuur, bekabelingsinfrastructuur, koel- en energiesystemen, beveiliging en beheer.

ANSI/TIA-942 wordt gebruikt door ontwerpers, exploitanten en auditors van datacenters om ervoor te zorgen dat datacenters worden ontworpen en gebouwd om te voldoen aan de beste praktijken en normen in de sector. De norm wordt ook vaak door regelgevende instanties en klanten aangehaald om de betrouwbaarheid en beveiliging van datacenters te evalueren.

Systeem- en organisatiecontroles (System and Organization Controls – (SOC) 2)

SOC 2 is een reeks normen die is ontwikkeld door het American Institute of Certified Public Accountants (AICPA) om de beveiliging, beschikbaarheid, verwerkingsintegriteit, vertrouwelijkheid en privacy van de systemen en gegevens van een serviceorganisatie te beoordelen en te auditen.

Opmerking: terwijl ISO/IEC 27001 algemeen toepasbaar is, is SOC 2 specifiek afgestemd voor datacenters.

SOC 2-rapporten worden door serviceorganisaties (zoals datacenters) gebruikt om aan hun klanten en belanghebbenden te laten zien dat ze effectieve interne controles hebben om hun gevoelige gegevens te beschermen.

SOC 2-rapporten zijn gebaseerd op de Trust Services Criteria (TSC), een reeks principes en criteria die worden gebruikt om de effectiviteit van de controles van een serviceorganisatie over haar systemen en gegevens te evalueren.

Er zijn twee soorten SOC 2-rapporten: Type I en Type II. Type I-rapporten evalueren het ontwerp van de controles van een serviceorganisatie, terwijl Type II-rapporten de effectiviteit van die controles gedurende een bepaalde periode evalueren.

SOC 2-audits worden uitgevoerd door onafhankelijke externe auditors, die gecertificeerd zijn door de AICPA.

SOC 2-audits zijn vrijwillig, maar ze worden steeds belangrijker voor serviceorganisaties die hun toewijding aan beveiliging en privacy willen aantonen.

Ter voorbereiding op een SOC 2-audit moeten serviceorganisaties een risicobeoordeling uitvoeren en een uitgebreide set controles implementeren om te voldoen aan de Trust Services Criteria.

SOC 2-audits omvatten doorgaans een combinatie van interviews, documentatiebeoordelingen en systeemtesten om de effectiviteit van de controles van een serviceorganisatie te evalueren.

SOC 2-rapporten bevatten een oordeel van de auditor over de effectiviteit van de controles van een serviceorganisatie, evenals een beschrijving van de controles die zijn getest en eventuele vastgestelde tekortkomingen.

SOC 2-rapporten kunnen worden gedeeld met klanten, belanghebbenden en regelgevende instanties om de zekerheid te bieden dat een serviceorganisatie effectieve controles heeft geïmplementeerd om gevoelige gegevens te beschermen.

Is SOC 2-rapport Type II De aanbeveling voor cybersecurityaspecten?

SOC 3

SOC iii is een type attestatierapport dat een overzicht op hoog niveau biedt van de beheersmaatregelen van een organisatie met betrekking tot beveiliging, beschikbaarheid, verwerkingsintegriteit, vertrouwelijkheid en privacy.

In tegenstelling tot SOC 1- en SOC 2-rapporten, die bedoeld zijn voor een specifiek publiek en gedetailleerdere informatie bieden over de controles van een organisatie, zijn SOC 3-rapporten ontworpen voor een algemeen publiek en bieden ze een samenvatting van de controles van de organisatie die openbaar kan worden gedeeld.

SOC 3-rapporten zijn gebaseerd op dezelfde controles en criteria als SOC 2-rapporten, maar ze bieden niet dezelfde mate van detail. In plaats daarvan bevatten SOC 3-rapporten een korte beschrijving van het systeem en de controles van de organisatie, samen met een verklaring van een onafhankelijke auditor die bevestigt dat de organisatie voldoet aan de SOC 2-criteria.

SOC 3-rapporten worden vaak door organisaties gebruikt om hun toewijding aan beveiliging en naleving aan klanten, partners en andere belanghebbenden te demonstreren. Omdat ze openbaar beschikbaar zijn, kunnen ze ook door potentiële klanten of investeerders worden gebruikt om de beveiligingshouding van een organisatie te evalueren voordat ze zaken met hen doen.

A2.6. Certificeringsschema's

De Cyber Security Act (CSA, (EU) 2019/881) biedt een Europees kader voor de cybersecuritycertificering van producten, processen en diensten. ENISA, het agentschap van de Europese Unie voor cybersecurity, is

gerechtigd om cybersecuritycertificeringsschema's te ontwikkelen die bedoeld zijn om op vrijwillige basis te worden gebruikt en geldig zijn in de hele Europese Unie. Het tweede schema is bedoeld om Cloud Services (EUCS) te dekken. Op het moment van schrijven van deze richtlijn is dit schema nog in voorbereiding. Verwacht wordt dat dit schema gebruik zal maken van de hierboven gepresenteerde CEN/TS 18026. Wanneer het beschikbaar is, kan het een nuttig hulpmiddel worden voor de CSP's om de beveiliging van zijn oplossing aan te tonen en voor de FSSS-serviceprovider om de CSP te vertrouwen.

Publicatie datum: 14-02-205

Euralarm
Gubelstrasse 22
CH-6301 Zug (Switzerland)

Swiss Commercial Registration No: CHE-222.522.503

E secretariat@euralarm.org
W www.euralarm.org