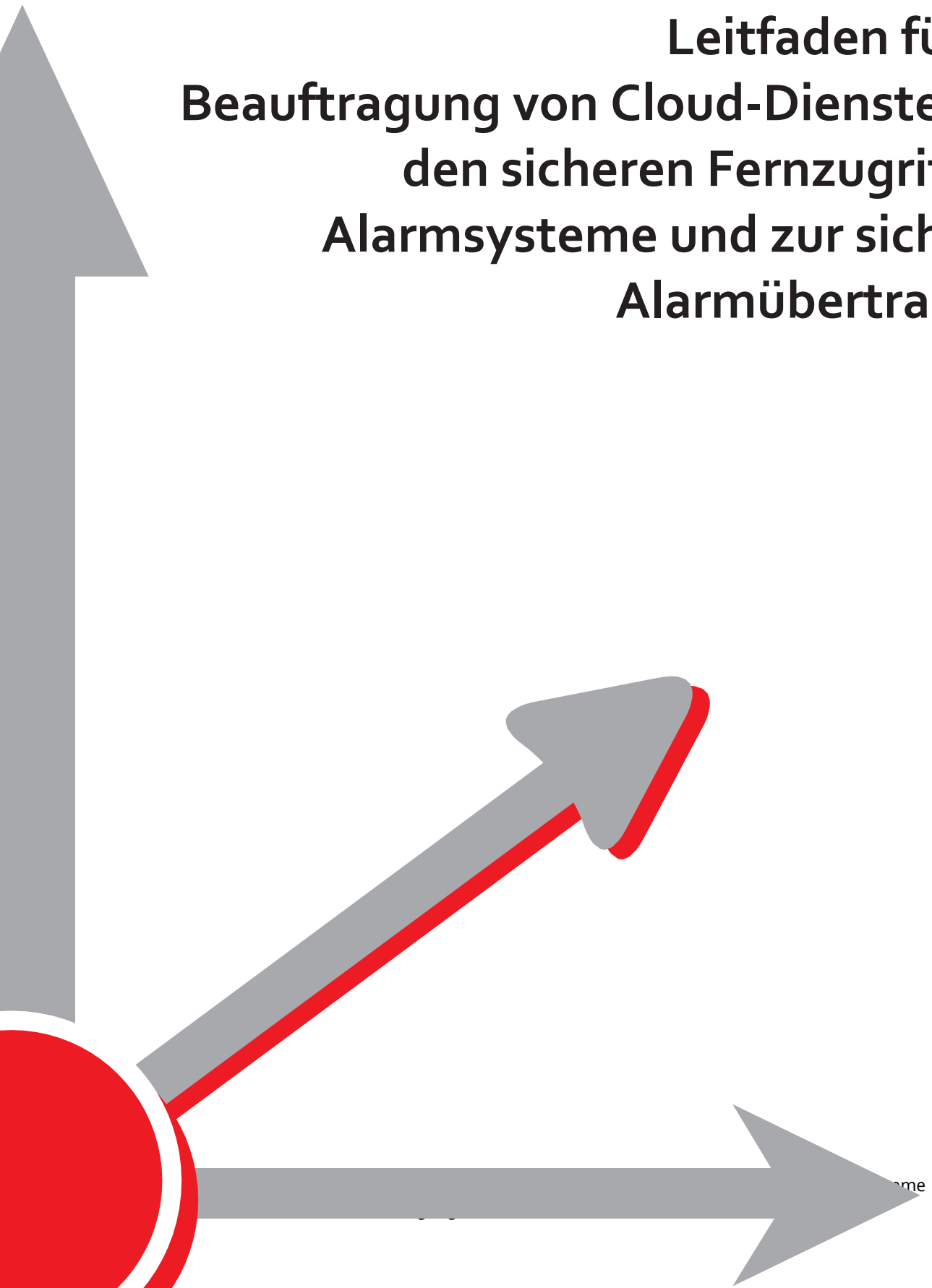
Leitfaden für die Beauftragung von Cloud-Diensten für den sicheren Fernzugriff auf Alarmsysteme und zur sicheren Alarmübertragung



Liste der Änderungen

Datum	Änderungsnummer	Absatz /Seite	Änderung
Februar 2025	1.0		Erste Veröffentlichung

VORWORT

Dieses Dokument dient als allgemeiner Leitfaden und ist kein Ersatz für eine ausführliche Beratung spezifischer Umgebungen. Obwohl bei der Zusammenstellung und Vorbereitung dieser Publikation mit großer Sorgfalt vorgegangen wurde, um die Richtigkeit zu gewährleisten, kann Euralarm unter keinen Umständen die Verantwortung für Fehler, Auslassungen oder erteilte Ratschläge oder für Verluste übernehmen, die durch eine Nutzung der in dieser Publikation enthaltenen Informationen entstehen.

HAFTUNGSAUSSCHLUSS

Dieses Dokument dient ausschließlich der Orientierung der Euralarm-Mitglieder und ggf. ihrer Mitglieder über den Stand der Dinge in Bezug auf den betreffenden Gegenstand. Obwohl alle Anstrengungen unternommen wurden, um die Richtigkeit dieser Informationen zu gewährleisten, sollten sich die Leser nicht auf deren Vollständigkeit oder Richtigkeit verlassen und sie auch nicht als Rechtsauslegung verwenden. Euralarm haftet nicht für die Bereitstellung falscher oder unvollständiger Informationen.

Anmerkung: Die englische Version dieses Dokuments ist das genehmigte Euralarm-Referenzdokument.

Euralarm • Gubelstrasse 11 • CH-6300 Zug • Schweiz

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

Inhaltsverzeichnis

1. Einleitung

Es wird immer üblicher, die neueste Technologie zu nutzen, um eine IP-basierte Alarmübertragung und einen Fernzugriff auf Brandschutz- und/oder Sicherheitssysteme (FSSS) zu ermöglichen und somit einen Teil der Ausrüstung außerhalb der Räumlichkeiten des FSSS-Dienstleisters zu platzieren. Dieses Dokument soll FSSS-Dienstleistern (z. B. Installateuren) bei der Nutzung der Dienste eines Rechenzentrums zur Unterbringung eines Teils der Ausrüstung helfen.

Es werden zwei verschiedene Anwendungsfälle mit ihren spezifischen Anforderungen und Zielgruppen betrachtet.

- Ein Anwendungsfall ist die Alarmübertragung über ein Alarmübertragungssystem (ATS), das von einem Alarmübertragungsdienstleister (ATSP) betrieben und verwaltet wird, für den Verfügbarkeit, Übertragungszeit, Fehlerberichterstattung und Schutz vor Substitution wesentliche Merkmale sind. Die Norm für Alarmübertragungssysteme (ATS) EN 50136-1 erlaubt gehostete Konfigurationen, bei denen das Cloud-Element an einem sicheren Ort, z. B. in einem Rechenzentrum, untergebracht werden muss. Die höchsten Kategorien von ATS beinhalten Sicherheitsanforderungen, die im gesamten System erfüllt werden müssen. Die Anleitung für diesen Anwendungsfall richtet sich an alle Stellen, die die Rolle des ATSP übernehmen.
- Ein weiterer Anwendungsfall ist der Fernzugriff auf das FSSS über eine Fernzugriffsinfrastruktur (RAI), die von einem Fernzugriffsinfrastruktur-Dienstanbieter (RAISP) betrieben und verwaltet wird, für den der sichere Zugriff auf das FSSS und die Daten im Vordergrund steht, während die Verfügbarkeit nur der Bequemlichkeit dient. Die technischen Spezifikationen für die Remote Access Infrastructure (RAI) CLC/TS 50136-10 verlangen, dass sich der Remote Access Server (RAS) an einem sicheren Ort befindet, und enthalten Anforderungen an die Sicherheit der übertragenen Daten. Die Anleitung für diesen Anwendungsfall richtet sich an alle Stellen, die die Rolle des RAISP übernehmen, insbesondere an kleine und mittlere FSSS-Dienstleister, die die Rolle des RAISP übernehmen möchten, mit Cloud-Diensten nicht vertraut sind und Remote-Dienste gemäß EN 50710 bereitstellen möchten.

Es gibt zwar eine Reihe guter Gründe, Cloud-Lösungen in Betracht zu ziehen, doch sollten FSSS-Dienstleister die Auswirkungen auf ihr Unternehmen verstehen, einschließlich Verfügbarkeit, Service-Level-Vereinbarungen, Datensicherheit, Compliance sowie rechtliche und vertragliche Anforderungen. FSSS-Dienstleister müssen weiterhin die Einhaltung bestehender Standards nachweisen, z. B. in Bezug auf Leistung und Verfügbarkeit, Backups, Zugriffskontrolle usw. Die Verantwortlichkeiten für die Wartung sollten von allen Beteiligten klar verstanden und akzeptiert werden. Dazu gehört das Lebenszyklusmanagement für Betriebssysteme, Plattformen (z. B. Datenbanken, Virtualisierung usw.) und Anwendungen. Der FSSS-Dienstleister sollte bestätigen können, dass diese Aktivitäten gemäß den Erwartungen und Dienstleistungsverträgen des FSSS-Dienstleisters durchgeführt wurden.

Die Speicherung, Weitergabe und Sicherheit von Daten ist von entscheidender Bedeutung und erfordert rechtliche Überlegungen, die über die in diesem Dokument gemachten Aussagen hinausgehen. Daher wird in diesem Dokument nicht versucht, diese rechtlichen Anforderungen zu interpretieren oder diesbezügliche Leitlinien bereitzustellen.

Wesentliche Teile der vorliegenden Richtlinie wurden mit Zustimmung der BSIA aus der BSIA-Richtlinie „ARC-Überlegungen bei der Nutzung von Rechenzentrums- oder Cloud-Diensten" übernommen. EURALARM dankt seinem Mitglied, der British Security Industry Association, für diesen Beitrag.

Diese Richtlinie enthält eine Beschreibung wichtiger Konzepte im Zusammenhang mit Cloud-Diensten, berücksichtigt relevante Standards und gibt einen Überblick über die rechtlichen Kriterien für die Wahl des CSP. Die Richtlinie erhebt jedoch nicht den Anspruch, alle gesetzlichen Anforderungen der einzelnen Länder in Europa zu berücksichtigen. Es sollte darauf geachtet werden, die Richtlinie im Kontext etwaiger örtlicher gesetzlicher Anforderungen zu betrachten, die Vorrang haben.

2. Abkürzungen

AICPA: Amerikanisches Institut für Wirtschaftsprüfer (American Institute of Certified Public Accountants)
AMS: Alarm Management System
ANSI: Amerikanisches Institut für Normung
ARC: Alarm-Empfangszentrale
AS: Alarmanlage
ATS: Alarmübertragungssystem
BSIA: Britischer Verband der Sicherheitsindustrie
CLC: CENELEC
CSP: Cloud-Dienstanbieter
EN: Europäischer Standard (Norm)
FaaS: Funktion als Dienstleistung
FSSS: Brandsicherheitssysteme und/oder Sicherheitssysteme
IaaS: Infrastruktur als Dienstleistung
IEC: Internationales Elektrotechnisches Komitee
ISO: Internationale Organisation für Normung
IT: Informationstechnologie
MARC: Überwachungs- und Alarmempfangszentrale
PaaS: Plattform als Dienstleistung
PSTN: Öffentliches Telefonvermittlungsnetz
RAC: Fernzugriffs-Client
RAE: Fernzugriffsendpunkt
RAI: Infrastruktur für Fernzugriff
RAS: Server für Fernzugriff
RCT: Empfangszentrum Sendeempfänger
RCT-A: RCT bei der ARC
RCT-H: Gehostete RCT
SaaS: Software als Dienstleistung
SLA: Service Level Agreement
SOC: System- und Organisationskontrollen
SPT: Transceiver für überwachte Standorte
TIA: Verband der Telekommunikationsindustrie
TS: Technische Spezifikation

3. Thematik

Dieses Dokument behandelt das Cloud-Element einer Fernzugriffsinfrastruktur (RAI, die für den Fernzugriff auf

Funktionen des FSSS verwendet wird) und eines Alarmübertragungssystems (ATS, das zur Übertragung von Alarmen vom FSSS an die Alarmempfangsstelle verwendet wird).

3.1. Fernzugriff auf FSSS

Im Falle einer RAI wird dieses Cloud-Element in Abbildung 1 als RAS bezeichnet.

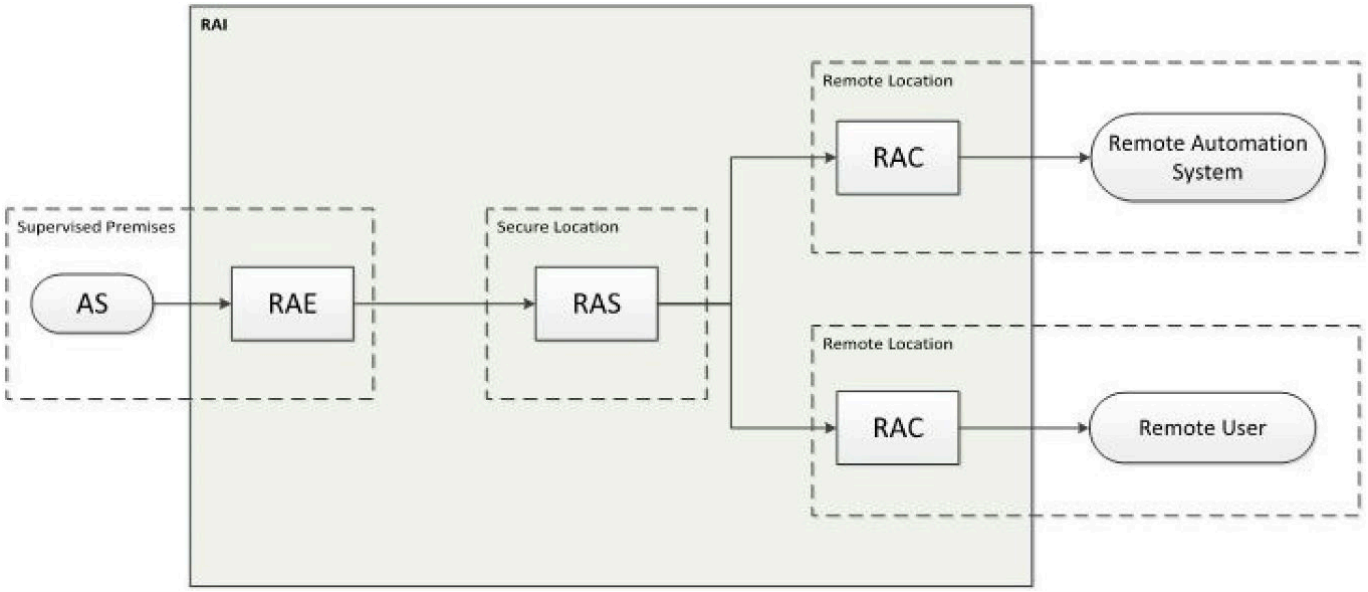


Abbildung 1. Logisches Diagramm der Fernzugriffsinfrastruktur (entnommen aus CLC/TS 50136-10:2022)

3.2. Alarmübertragung

Im Falle eines ATS erlaubt der europäische Standard eine nicht gehostete Konfiguration, die in Abbildung 2a dargestellt ist. Bei dieser Konfiguration wird eine direkte Verbindung zwischen dem Alarmsystem (AS) und der ARC (MARC) hergestellt. Der Standard erlaubt auch eine gehostete Konfiguration, die in Abbildung 2b dargestellt ist. In dieser Konfiguration laufen die Alarmmeldungen von zahlreichen Alarmsystemen bei einem Empfänger zusammen, der in einem Rechenzentrum untergebracht ist und als RCT-H identifiziert wird. Dort werden sie verarbeitet, bestätigt und gespeichert, und das ARC erhält über einen gesicherten Kommunikationspfad Zugang zu ihnen. Überlegungen zum Wechsel von der PSTN-Kommunikation zur IP-Alarmübertragung wurden in einem Whitepaper von Euralarm im Jahr 2019 angestellt: "Netzwerke der neuen Generation für Alarmkommunikation"[1]. Der FSSS-Diensteanbieter sollte sicherstellen, dass der ATS mit EN 50136-1, der SPT mit EN 50136-2 und die RCT, RCT-H und RCT-A mit EN 50136-3 übereinstimmen (siehe A2.2 in Anhang 2 zur Erläuterung dieser Normen). Dadurch wird sichergestellt, dass das gesamte ATS die Alarmmeldungen rechtzeitig übermittelt und auf Fehler bei der Übermittlung der Alarme überwacht wird.

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

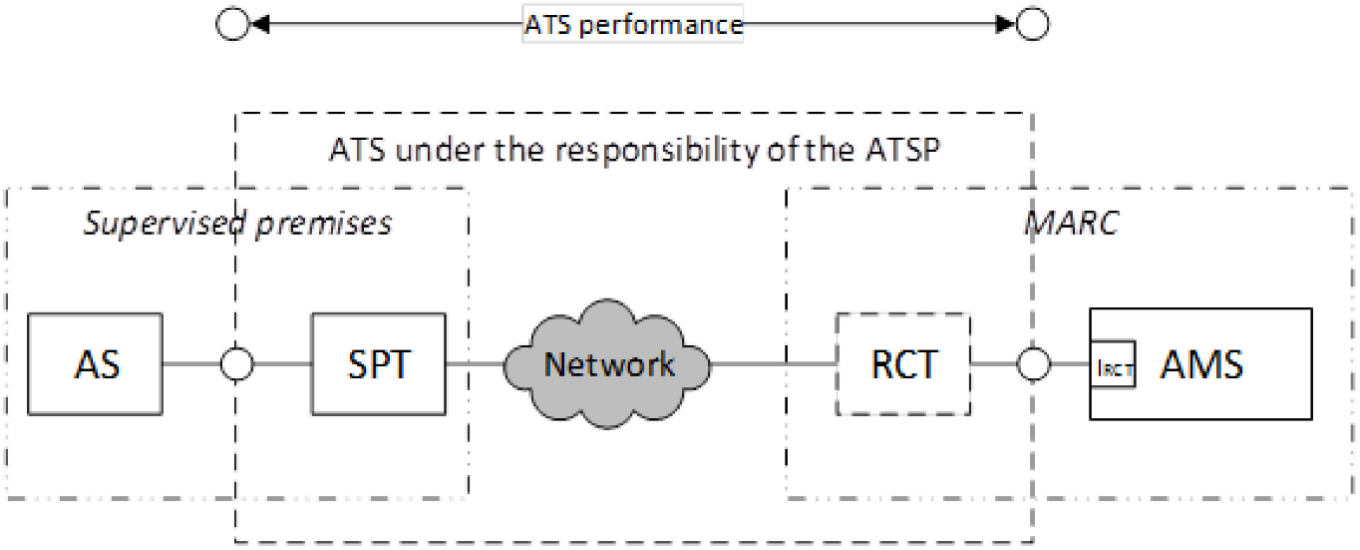


Abbildung 2a. Beispiel für ein **nicht gehostetes** Alarmübertragungssystem (aus EN 50136-1/A1:2018)

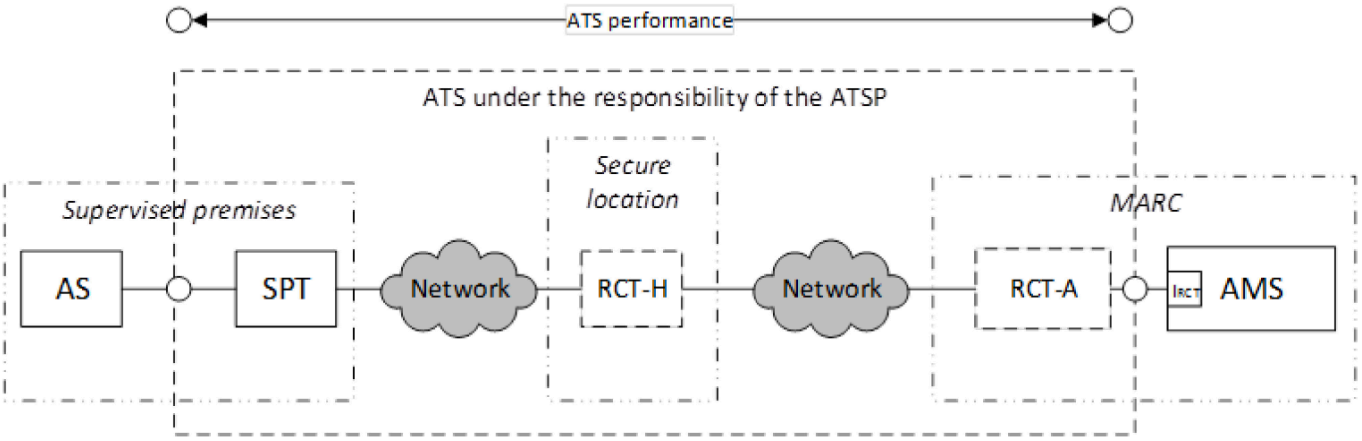


Abbildung 2b. Beispiel eines **gehosteten** Alarmübertragungssystems (entnommen aus EN 50136-1/A1:2018)

3.3. Allgemein

Der vorliegende Leitfaden umreißt die Überlegungen, die FSSS-Dienstleister anstellen sollten, wenn sie sich für die Nutzung der Dienste eines Rechenzentrums oder von Cloud-Diensten entscheiden. Dies sollte bei der Entscheidung helfen, wie viel des FSSS-Dienstleisters sicher und geschützt in einer Cloud-Umgebung gehostet werden sollte/könnte (oder teilweise gehostet wird).

Ein FSSS-Dienstleister schützt ständig Leben und Eigentum, und in dieser Hinsicht sind die Anforderungen kritischer als bei den meisten anderen Organisationen.

4. Cloud-Umgebungen

4.1. Einleitung

Die Durchführung einer Due Diligence zur Bewertung und Auswahl von Cloud-Service-Anbietern ist entscheidend. Die Due Diligence bezieht sich auf die gründliche Recherche und Bewertung potenzieller Anbieter oder Dienstleister, bevor eine Geschäftsbeziehung mit ihnen eingegangen wird. Dieser Prozess wird helfen, die Fähigkeiten, die Zuverlässigkeit, die Sicherheitsmaßnahmen und die allgemeine Eignung des Anbieters für Ihre speziellen Bedürfnisse besser zu verstehen.

Drei Umgebungen sind klassischerweise definiert als: Private Business Cloud-Lösung, Data Centre Hosted (im Folgenden „Data Centre") oder Native Cloud (im Folgenden „Cloud"). Der FSSS-Dienstleister kann entweder eine oder mehrere dieser Umgebungen nutzen, in denen er die technische Ausrüstung für den Fernzugriff oder die Alarmübertragung betreibt, oder die vom Hersteller des FSSS angebotene Lösung verwenden.

Dieses Dokument impliziert nicht, dass Private-Business-Cloud-Lösungen oder Cloud-Umgebungen die einzigen Betriebsmodi für alle Anwendungen sind, sondern es ist zulässig, dass der FSSS-Dienstanbieter Anwendungen in mehreren Umgebungsmodellen betreiben kann und wird. Mit anderen Worten: Sie können alle drei Betriebsumgebungen in mehr oder weniger starkem Maße nutzen, je nach den Anforderungen an die Dienste.

FSSS-Dienstleister sollten bei der Wahl einer eigenen Lösung oder eines Rechenzentrums oder einer Cloud-Lösung auch die Anforderungen an die Zertifizierung durch Dritte berücksichtigen.

Die Nutzung von Rechenzentren/Cloud-Diensten schließt die Verantwortlichkeiten von FSSS-Dienstleistern, wie sie in EN 16763, EN 50710 oder EN 50136-1 beschrieben sind, nicht aus (siehe A2.2 in Anhang 2 zur Erläuterung dieser Normen). Ein Euralarm Leitfaden[2] zur Implementierung von Remote Services wurde veröffentlicht und ist auf der Website zu finden. Es hilft dem FSSS-Dienstleister bei der Vorabkontrolle, ob die Anforderungen dieser Standards erfüllt werden.

4.2. Private Cloud-Lösung für Unternehmen

Private Unternehmenslösungen werden vom FSSS-Dienstleister verwaltet. Die Server sind entweder in demselben Gebäude oder auf demselben Gelände installiert, auf dem sich der FSSS-Dienstanbieter befindet, oder in einem anderen Gebäude unter der Verantwortung des FSSS-Dienstanbieters. Ein Anwendungsanbieter liefert dem Dienstleistungsunternehmen die Software, die auf den Servern läuft. Die Server werden entweder vom FSSS-Dienstleister beschafft oder als Teil der Dienstleistung des Anwendungsanbieters erworben.

Upgrades von Serverbetriebssystemen, Datenbanken und der Anwendungssoftware werden zwischen dem FSSS-Dienstleister und dem Anwendungsanbieter koordiniert. Sicherheit (Verschlüsselung im Ruhezustand usw.) und Zuverlässigkeit (z. B. Datenbankreplikation mit geografischer Vielfalt) sind Lösungen, die in der Regel vom Anwendungsanbieter entwickelt werden.

4.3. Rechenzentrum

Bei den Lösungen für Rechenzentren handelt es sich um Server, die in einem Gebäude installiert sind, das von einem Drittunternehmen betrieben wird, welches für die physische Sicherheit, die Stromversorgung und den Platz für die Server sorgt. Diese Server können einem bestimmten FSSS-Dienstanbieter vorbehalten sein oder in einer mandantenfähigen Umgebung betrieben werden. Diese Server werden entweder vom FSSS-Dienstanbieter oder vom Anwendungsanbieter als verwalteter Dienst gewartet.

4.4. Cloud

4.4.1. Beschreibung

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

Cloud-Lösungen umfassen alle Funktionen der Rechenzentrumslösung, aber die Server und andere damit verbundene Technologien (Datenbanken usw.) werden vom Cloud-Service-Anbieter bereitgestellt und gewartet (z. B. AWS - Amazon Web Services, Microsoft Azure, Google Cloud, IBM). Das Cloud Shared Responsibility Model (SRM) ist ein Rahmenwerk, das die Verantwortlichkeiten zwischen einem Cloud-Service-Anbieter und dem Anwendungsanbieter für die Sicherung der Cloud-Umgebung abgrenzt.

Der Cloud-Service-Anbieter schützt die Werte der Umgebung des Anwendungsentwicklers. Sie sorgen zum Beispiel für die physische Sicherheit und sichern die Virtualisierungsdienste. Der Anwendungsanbieter sichert die Assets in seiner Cloud-Instanz, d.h. der Anwendungsanbieter sichert das Betriebssystem, das er auf den Servern installiert und verwaltet, wer Zugang zu Ihrer Cloud-Umgebung hat.

Cloud Computing umfasst mehrere Modelle, die auf unterschiedliche Bedürfnisse und Anwendungsfälle zugeschnitten sind. Es ist wichtig zu beachten, dass sich diese Modelle nicht gegenseitig ausschließen. Cloud-Service-Anbieter bieten oft eine Kombination dieser Modelle an, um unterschiedlichen Anforderungen und Präferenzen zu erfüllen. In den folgenden Abschnitten werden 4 verschiedene Cloud-Modelle beschrieben.

4.4.2. Infrastruktur als Dienstleistung (IaaS)

Dieses Modell bietet virtualisierte Computerressourcen über das Internet. Es bietet virtuelle Maschinen, Speicher und Netzwerke, die Benutzer bereitstellen und verwalten können. Die Benutzer haben mehr Kontrolle über die Infrastruktur, einschließlich der Betriebssysteme und Anwendungen.

4.4.3. Plattform als Dienstleistung (PaaS)

PaaS bietet Entwicklern eine Plattform für die Erstellung, Bereitstellung und Verwaltung von Anwendungen, ohne sich um die zugrunde liegende Infrastruktur kümmern zu müssen. Es bietet eine vorkonfigurierte Umgebung mit Tools, Frameworks und einer Laufzeitumgebung für die Anwendungsentwicklung. Die Benutzer können sich auf die Programmierung und die Anwendungslogik konzentrieren, während die Plattform für Skalierbarkeit, Lastausgleich und Bereitstellung sorgt.

4.4.4. Serverloses Rechnen

Serverloses Computing ist ein Modell, bei dem Entwickler Code als einzelne Funktionen oder Codeeinheiten schreiben und bereitstellen. Der Cloud Service Provider verwaltet die Infrastruktur, weiterhin skaliert und stellt er die Ressourcen automatisch bedarfsgesteuert bereit. Die Entwickler müssen sich nicht um Server oder die Verwaltung der Infrastruktur kümmern und können sich ganz auf das Schreiben des Codes konzentrieren.

4.4.5. Software als Dienstleistung (SaaS)

SaaS ist eine vollständige Softwareanwendung, die über das Internet bereitgestellt wird. Endbenutzer des FSSS oder FSSS-Dienstleister können auf die Software zugreifen und sie nutzen, ohne dass eine Installation oder Verwaltung erforderlich ist. Anbieter von SaaS-Lösungen betreiben ihre Server in IaaS-, PaaS- oder Serverless-Computing-Modellen.

4.4.6. Überlegungen für native Cloud-Modelle

Bei der Wahl zwischen den verschiedenen Umgebungen ist es wichtig, die spezifischen Anforderungen und Einschränkungen einer unternehmenskritischen Anwendung sorgfältig zu berücksichtigen. Faktoren wie Leistungsanforderungen, Skalierbarkeitsanforderungen, Verwaltungsoptionen und Kostenüberlegungen sollten abgewogen werden, um die beste Lösung für die Ziele der Anwendung zu finden.

Weitere Informationen finden Sie in Anhang 1.

4.5. Herstellerlösung

Die Hersteller von FSSS haben ihre Lösungen entwickelt und bieten sie den FSSS-Dienstleistern an, die ihre Systeme nutzen. Eine solche Lösung kann auf einer der 3 oben beschriebenen Umgebungen basieren. Der FSSS-Dienstleister muss sich nicht um die Wartung der Server, Software und Anwendungen kümmern. Er muss eine vertragliche Vereinbarung treffen, die seinen Bedürfnissen und Erwartungen entspricht.

In der Regel hat der FSSS-Dienstleister keinen Vertrag mit dem Hersteller über die Nutzung seiner Lösung, sondern er akzeptiert die Bedingungen, indem er sich bei der Anwendung in der Cloud anmeldet. Daher ist es ratsam, dass der Hersteller ein Dokument für den Installateur erstellt, in dem der Rahmen seiner Cloud-Anwendung deutlich dargestellt wird:

- Welcher Cloud-Service-Anbieter,
- wo sich die Daten befinden werden,
- wie diese – einschließlich der Sicherheitsmaßnahmen – zugänglich sind,
- Servicelevel wie Wiederherstellungszeit und Wartung,
- auf welche Zertifizierung sich der Hersteller beziehen kann,
- wie der FSSS-Dienstanbieter den FSSS ordnungsgemäß anbinden sollte,
- ...

4.6. Überlegungen zu Betriebsumgebungen

Private Cloud-Lösungen für Unternehmen und Lösungen für Rechenzentren erfordern Investitionen in Hardware, Software und Infrastruktur sowie das Fachwissen, um diese einzurichten und zu warten. Cloud-basierte Lösungen erfordern nach wie vor, dass der Anwendungsanbieter über die nötigen Fähigkeiten verfügt, um die erforderlichen Funktionen zu verstehen, zu überwachen und zu skalieren. Der Cloud-Service-Anbieter bündelt kompetente IT-Services für die Bereitstellung und Wartung der Hardware, Betriebssysteme und Datenbanksoftware.

Es sollten Schritte unternommen werden, um die Sicherheit von Daten zu berücksichtigen, die über Online- oder Cloud-basierte Verbindungen zugänglich sind.

5. Rechtliche Kriterien für den Standort von Servern

5.1. Einleitung

Die Vorschriften für Datenserver in den europäischen Ländern werden durch eine Kombination aus nationalen Gesetzen und Verordnungen der Europäischen Union geregelt. Nachfolgend finden Sie einen Überblick über die wichtigsten Vorschriften in verschiedenen europäischen Ländern sowie den übergreifenden EU-Rahmen.

5.2. Allgemeine Datenschutzgrundverordnung der Europäischen Union (DSGVO)

Die GDPR, die seit Mai 2018 in Kraft ist, ist die wichtigste Verordnung zum Schutz von Daten und Privatsphäre in der EU. Sie gilt für alle Mitgliedsstaaten und umfasst:

- Grundsätze der Datenverarbeitung: Rechtmäßigkeit, Fairness, Transparenz, Zweckbindung, Datenminimierung, Genauigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit;
- Rechte der betroffenen Person: Recht auf Auskunft, Berichtigung, Löschung (Recht auf Vergessenwerden), Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch;
- Datenübermittlung: Beschränkungen für die Übermittlung personenbezogener Daten außerhalb der EU/des EWR, um ein angemessenes Schutzniveau zu gewährleisten;
- Benachrichtigung über Datenschutzverletzungen: Verpflichtung zur Benachrichtigung von Behörden und betroffenen Personen über Datenschutzverletzungen innerhalb von 72 Stunden.

5.3. Beispiele für länderspezifische Vorschriften

Deutschland

Bundesdatenschutzgesetz (BDSG): Ergänzt die DSGVO um zusätzliche Anforderungen, einschließlich strengerer Regeln für die Datenverarbeitung zu Beschäftigungszwecken und spezifischer Pflichten für Datenschutzbeauftragte.

Frankreich

Datenschutzgesetz (Loi Informatique et Libertés): Setzt die Bestimmungen der DSGVO durch und fügt nationale Besonderheiten hinzu, wie z.B. Regeln für die Verarbeitung von Gesundheitsdaten und zusätzliche Befugnisse für die nationale Datenschutzbehörde (CNIL).

Vereinigtes Königreich

Datenschutzgesetz 2018: Setzt die Datenschutz-Grundverordnung um und enthält besondere Bestimmungen für die Datenverarbeitung durch Behörden und Strafverfolgungsbehörden. Nach dem Brexit hat das Vereinigte Königreich die britische Datenschutz-Grundverordnung (UK GDPR) verabschiedet, die die EU-DSGVO widerspiegelt, aber unabhängig funktioniert.

Italien

Datenschutzkodex (Codice in materia di protezione dei dati personali): Entspricht der Datenschutz-Grundverordnung (GDPR), mit zusätzlichen nationalen Vorschriften für die Datenverarbeitung zu wissenschaftlichen und historischen Forschungszwecken sowie für journalistische Zwecke.

Spanien

Organisches Gesetz über Datenschutz und digitale Rechte (LOPDGDD): Ergänzt die DSGVO durch spezifische Regeln für digitale Rechte und zusätzliche Schutzmaßnahmen für Minderjährige und schutzbedürftige Personen.

Niederlande

Niederländisches Umsetzungsgesetz (Uitvoeringswet AVG): Ergänzt die DSGVO durch nationale Bestimmungen, insbesondere in Bezug auf die Verarbeitung von Strafregister- und Arbeitnehmerdaten.

Belgien

Belgisches Umsetzungsgesetz (Gegevensbeschermingsautoriteit GBA) Rahmengesetz vom 30. Juli 2018

Die gemeinsamen Themen der Länder sind:

- Datenlokalisierung: In einigen Ländern gelten besondere Anforderungen für die Datenlokalisierung, insbesondere für sensible Daten wie Gesundheitsdaten;
- sektorspezifische Vorschriften: Viele Länder erlassen zusätzliche Vorschriften für bestimmte Sektoren, wie Finanzen, Gesundheit und Telekommunikation;

- Datenschutzbehörden: Jedes Land hat eine nationale Datenschutzbehörde, die für die Durchsetzung der Datenschutzgesetze und die Bearbeitung von Beschwerden zuständig ist. Beispiele sind CNIL in Frankreich, ICO in Großbritannien und BfDI in Deutschland;
- grenzüberschreitende Datenübertragungen: Die EU-Länder folgen im Allgemeinen dem Rahmen der DSGVO für internationale Datenübertragungen, der Mechanismen wie Standardvertragsklauseln (SCCs), verbindliche Unternehmensregeln (BCRs) und Angemessenheitsentscheidungen umfasst.

Diese Liste der länderspezifischen Gesetzgebungen ist nicht erschöpfend. Für genauere Bestimmungen und die neuesten Aktualisierungen empfiehlt es sich, die jeweiligen nationalen Datenschutzbestimmungen und Gesetzestexte der einzelnen Länder zu konsultieren.

5.4. Nützliche Referenzen

- Europäische Kommission - Datenschutz[3]
- DSGVO Text[4]
- CNIL (Frankreich)[5]
- ICO (UK)[6]
- BfDI (Deutschland)

6. Verteilung von Rollen und Verantwortlichkeiten

6.1. Auswirkungen von Wartungsaktivitäten (geplant/ungeplant)

Die Verfügbarkeit der Infrastruktur kann je nach den damit erbrachten Diensten von unterschiedlicher Bedeutung sein. Alarmübertragungsdienste erfordern eine hohe Verfügbarkeit, die durch die entsprechende Kategorie in EN 50136-1 definiert ist. Die Verfügbarkeit wird im Allgemeinen als weniger kritisch für Fernzugriffsdienste angesehen.

Der FSSS-Dienstleister (bzw. der Hersteller in der Herstellerlösungsumgebung) sollte über Prozesse verfügen, die regeln, wie die Wartungsaktivitäten verwaltet und ggf. entschärft werden, z. B. sekundäre Systemverfügbarkeit oder duplizierte Infrastruktur usw.

Anbieter von FSSS-Diensten, die eine gehostete Lösung in Erwägung ziehen, sollten sicherstellen, dass mit den Anbietern von Cloud-Diensten Vereinbarungen (SLAs) getroffen werden, die gewährleisten, dass der Anbieter von FSSS-Diensten im Voraus über die Dauer von Offline-Zeiten während geplanter Wartungsarbeiten informiert wird. Diese Vereinbarungen sollten auch beinhalten, wie ungeplante Wartung gehandhabt und kommuniziert wird.

Wenn FSSS-Dienstleister für IT-Dienste auf 3. Parteien angewiesen sind, sollte der FSSS-Dienstleister berücksichtigen, wie sich Vorfälle auf die Fähigkeit des IT-Dienstleisters Support zu leisten auswirken können.

6.2. IT-Kompetenz

[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

Der FSSS-Dienstleister ist letztlich für seine eigenen Geräte und Systeme verantwortlich und benötigt ein gewisses Maß an lokaler IT-Kompetenz, um die routinemäßige Überwachung und Wartung der Lösung des FSSS-Dienstleisters zu gewährleisten.

6.3. Sicherheit

Anbieter von FSSS-Dienstleistungen sollten sich überlegen, wer Zugang zu ihren Systemen und Daten hat, und die Anforderungen an das Personal überprüfen. Es gibt mehrere Optionen, um die Sicherheitsprobleme zu lösen, darunter:

- Identitäts- und Zugriffsmanagement (IAM)
- Verschlüsselung
- Sicherheitsüberwachung und Protokollierung
- Compliance und Zertifizierungen
- Netzwerksicherheit.

Rechenzentrumslösungen erfordern Personal vor Ort und/oder Fernzugriff für die Verwaltung und Wartung der Infrastruktur, einschließlich Hardware-Wartung, Software-Upgrades und Sicherheits-Patches. Im Gegensatz dazu werden Cloud-Lösungen vom Cloud-Service-Provider verwaltet, der sich um die Wartung der Infrastruktur, Software-Upgrades und Sicherheits-Patches kümmert, so dass sich die internen IT-Mitarbeiter auf ihre Kernaufgaben konzentrieren können.

In jeder Cloud-Umgebung gibt es eine gemeinsame Verantwortung zwischen dem Cloud Service Provider (CSP) und dem Nutzer (FSSS Service Provider oder Hersteller). Sicherheit für Dinge wie Datenklassifizierung, Netzwerkkontrollen und physische Sicherheit brauchen klare Eigentümer. Die Aufteilung dieser Verantwortlichkeiten ist als Modell der geteilten Verantwortung (SRM) für die Cloud-Sicherheit bekannt. Schauen Sie sich dieses Diagramm an, um zu sehen, wo die Verantwortlichkeiten in verschiedenen Cloud-Umgebungen liegen.

Private Cloud-Lösung für Unternehmen	**Infrastruktur als Dienstleistung *IaaS***	**Plattform als Dienstleistung *PaaS***	**Software als Dienstleistung *SaaS***
Daten & Konfigurationen	Daten & Konfigurationen	Daten & Konfigurationen	Daten & Konfigurationen
Anwendungscode	Anwendungscode	Anwendungscode	Anwendungscode
Skalierung	Skalierung	Skalierung	Skalierung
Laufzeit	Laufzeit	Laufzeit	Laufzeit
Betriebssystem	Betriebssystem	Betriebssystem	Betriebssystem
Virtualisierung	Virtualisierung	Virtualisierung	Virtualisierung
Hardware	Hardware	Hardware	Hardware
Verwaltet vom FSSS-Dienstleister oder Hersteller			
Vom Cloud-Service-Anbieter verwaltet			

Weitere Informationen und Hinweise zu SRM finden Sie auf der Website des Center for Internet Security (CIS)[7].

[7] https://www.cisecurity.org/insights/blog/shared-responsibility-cloud-security-what-you-need-to-know

7. Vertragsabschluss für Cloud-Dienste

Die Europäische Kommission schrieb bereits 2012 in ihrer Mitteilung mit dem Titel "Das Potenzial des Cloud Computing in Europa freisetzen"[8]:

> *"Traditionelle IT-Outsourcing-Vereinbarungen wurden in der Regel im Voraus ausgehandelt und bezogen sich auf Datenspeicherung, Verarbeitungseinrichtungen und Dienstleistungen, die im Detail und im Voraus definiert und beschrieben wurden. Cloud Computing-Verträge hingegen schaffen im Wesentlichen einen Rahmen, in dem der Nutzer je nach Bedarf Zugang zu unbegrenzt skalierbaren und flexiblen IT-Funktionen hat. Die größere Flexibilität des Cloud Computing im Vergleich zum traditionellen Outsourcing wird derzeit jedoch häufig durch eine geringere Sicherheit für den Kunden aufgrund von nicht ausreichend spezifischen und ausgewogenen Verträgen mit Cloud-Anbietern ausgeglichen.*
>
> *Die Komplexität und Unsicherheit des rechtlichen Rahmens für Anbieter von Cloud-Diensten führt dazu, dass sie häufig komplexe Verträge oder Service Level Agreements mit umfangreichen Haftungsausschlüssen verwenden. Die Verwendung von Standardverträgen nach dem Motto "nimm es oder lass es" mag für den Anbieter kostensparend sein, ist aber für den Nutzer, einschließlich des Endverbrauchers, oft unerwünscht. Solche Verträge können auch die Wahl des anwendbaren Rechts vorschreiben oder die Datenwiederherstellung verhindern. Selbst größere Unternehmen haben wenig Verhandlungsmacht, und die Verträge sehen oft keine Haftung für Datenintegrität, Vertraulichkeit oder Servicekontinuität vor."*

Um diese Komplexität und Ungewissheit in den Griff zu bekommen, finden Sie in den "Leitlinien zum Outsourcing an Cloud-Service-Anbieter"[9] , die von der Europäischen Wertpapier- und Marktaufsichtsbehörde (esma) im Jahr 2021 in zahlreichen europäischen Sprachen herausgegeben wurden, detaillierte Anleitungen zu den wichtigsten Vertragselementen. Insbesondere die folgenden Abschnitte des Dokuments können von Bedeutung sein:

- Leitlinie 3 - Wichtige Vertragselemente
- Leitlinie 4 - Informationssicherheit
- Leitlinie 5 - Ausstiegsstrategien
- Leitlinie 6 - Zugriffs- und Prüfungsrechte.

HINWEIS: Ähnliche Leitlinien finden Sie auch auf der Website der Europäischen Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung (eiopa)[10].

Darüber hinaus bereitet die Europäische Kommission im Rahmen des Datenschutzgesetzes ((EU) 2023/2854) Standardvertragsklauseln vor, die den Beteiligten bei der Umsetzung der Bestimmungen über den Wechsel des Cloud-Anbieters und die Weitergabe von Daten helfen sollen. Dieser Leitfaden wird voraussichtlich im Laufe des Jahres 2025 veröffentlicht werden.

Anhang 2 dieses Euralarm-Leitfadens verweist schließlich auf Standards und Zertifizierungssysteme, deren Einhaltung im Vertrag mit dem Cloud-Service-Anbieter verlangt werden kann.

Weitere Informationen zu Cloud Computing-Verträgen finden Sie auf der EC-Website:

[8] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF
[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

- "Cloud Computing Verträge"[11]
- "Vergleichende Studie über Cloud Computing-Verträge"[12]

8. Fazit

Da es weder ein eindeutiges noch ein einheitliches Zertifizierungssystem für Rechenzentren und Cloud-Dienste gibt, sollte der FSSS-Dienstanbieter sicher sein, dass der CSP dafür sorgt, dass das Rechenzentrum die erforderlichen Zuverlässigkeits- und Sicherheitsanforderungen für den jeweiligen Anwendungsfall erfüllt. Jede Konformitätserklärung, die der CSP oder der Hersteller zum Nachweis der Zuverlässigkeit und Sicherheit des Cloud-Dienstes vorlegt, sollte zumindest die folgenden Punkte enthalten:

- bezüglich des verwendeten Rechenzentrums:
    - seinen Namen und Standort(e);
    - Grad der Gewährleistung der Geschäftskontinuität von keiner Kontinuität bis zur vollständigen Kontinuität im Falle eines Ausfalls des Rechenzentrums (entscheidend für die Alarmübertragung und den Komfort beim Fernzugriff);
    - Mittel zur Minimierung des Ausfallrisikos, wie z.B. Auswahl eines oder mehrerer Standorte, Gebäudestruktur, Stromversorgungssysteme, Kühlsysteme, mechanische Systeme, Architektur, physische Sicherheit, Cybersicherheit, Verkabelungsinfrastruktur, Telekommunikationssysteme, Backup-Strategie, Brandschutz und Sicherheit (entscheidend für die Alarmübertragung und den Komfort beim Fernzugriff);
- in Bezug auf den Cloud-Service:
    - genutzten Cloud-Umgebung;
    - eine klare und verständliche Verteilung der Rollen und Verantwortlichkeiten, die in einem SLA festgelegt ist;
    - Disaster Recovery Plan (DRP) vorhanden (wichtig für die Alarmübermittlung und die Bequemlichkeit beim Fernzugriff);
    - Testplan nach einem Software-Update;
    - Benachrichtigung des FSSS-Dienstleisters im Falle von System- oder Software-Updates oder eines Anbieterwechsels;
- in Bezug auf die Cybersicherheit und den Datenschutz von Rechenzentren und Cloud-Diensten:
    - die Einhaltung von ISO/IEC 27001;
    - Zertifikat im Rahmen des EUCS-Zertifizierungssystems (sofern verfügbar, siehe A2.6);
    - sichere Zugriffskontrollmechanismen mit Authentifizierung für den Zugriff auf gespeicherte Daten und Funktionen;
    - Verschlüsselung von Daten bei der Übertragung;
    - Abschwächung der Auswirkungen von (D)DOS-Angriffen;
    - Prozess zur Behandlung von Schwachstellen;
    - Überprüfung durch Penetrationstests;
- für die Alarmübertragung:
    - Übereinstimmung des ATS mit der Norm EN 50136-1 in einer erklärten Kategorie, die dem geschützten Risiko angemessen ist (Übertragungszeit, Verfügbarkeit, Meldezeit bei Übertragungsfehlern, Verschlüsselungserfordernis, Substitutionssicherheit, Bestätigungsmodus usw.);
    - Dual Path (DP) Kategorie, wo hohe Risiken abgedeckt werden oder für lebenswichtige (lebensbedrohliche) Systeme;
- für den Fernzugriff auf FSSS:
    - die Übereinstimmung der RAI mit CLC/TS 50136-10.

[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

9. Literaturverzeichnis

"GWB-Überlegungen bei der Nutzung von Rechenzentren oder Cloud-Diensten", BSIA (British Security Industry Association), Ausgabe 1, Oktober 2023.

Anhang 1 - Rechenzentrum/IaaS und Serverless

Für eine unternehmenskritische Anwendung haben sowohl IaaS (Infrastructure as a Service) als auch serverlose Umgebungen ihre Vor- und Nachteile. Hier sind einige Vergleiche zwischen den beiden:

- Management-Komplexität: In einer IaaS-Umgebung haben die Benutzer die volle Kontrolle über die Infrastruktur. Das bedeutet, dass sie sich um Aufgaben wie die Bereitstellung und Verwaltung von Servern, die Konfiguration von Netzwerken und die Sicherstellung hoher Verfügbarkeit kümmern müssen. Dies erfordert mehr Fachwissen, Zeit und Ressourcen im Vergleich zu einer Serverless-Umgebung, in der die Verwaltung der Infrastruktur nach außen abstrahiert wird. Mit Serverless können sich Anwendungsanbieter ausschließlich auf die Bereitstellung von Softwarediensten fokusieren. Sie haben jedoch weniger Verständnis für die zugrunde liegende Infrastruktur, was bei bestimmten geschäftskritischen Anwendungen eine Einschränkung darstellen kann.

- Skalierbarkeit: In einer IaaS-Umgebung erfordert die Skalierung der Infrastruktur zur Bewältigung eines erhöhten Datenverkehrs oder Bedarfs manuelle Eingriffe und Konfigurationen. Andererseits skalieren serverlose Umgebungen die Ressourcen automatisch auf der Grundlage der Anzahl der ausgelösten Anfragen oder Ereignisse, was eine dynamischere Skalierbarkeit ermöglicht. Serverless kann jedoch bestimmte Einschränkungen in Bezug auf die Skalierbarkeit haben, z. B. die maximale Anzahl gleichzeitiger Ausführungen oder die Ausführungsdauer, was sich auf sehr anspruchsvolle Anwendungen auswirken kann.

- Kaltstart und Leistung: In serverlosen Umgebungen gibt es oft ein Konzept namens "Kaltstart", bei dem die erste Ausführung einer Funktion eine zusätzliche Latenzzeit verursacht, da die Laufzeitumgebung initialisiert werden muss. Diese Latenzzeit kann sich auf Echtzeit- oder Low-Latency-Anwendungen auswirken. In einer IaaS-Umgebung werden Anwendungen auf dedizierten Servern oder virtuellen Maschinen ausgeführt, die in der Regel eine konstante Leistung ohne Kaltstartverzögerungen bieten. Darüber hinaus kann es in serverlosen Umgebungen Einschränkungen bei den Ressourcen geben, die einzelnen Funktionen zugewiesen werden, was die Leistung ressourcenintensiver Anwendungen beeinträchtigen kann.

- Vendor Lock-In: Während sowohl IaaS- als auch Serverless-Umgebungen ein gewisses Maß an Anbieterbindung mit sich bringen, verfügen Serverless-Umgebungen häufig über enger integrierte Dienste und ereignisgesteuerte Architekturen, was die Migration von Anwendungen zwischen verschiedenen Cloud-Service-Anbietern oder auf eine lokale Infrastruktur erschweren kann. In einer IaaS-Umgebung haben die Benutzer mehr Flexibilität, um ihre Anwendungen zwischen verschiedenen Anbietern zu verschieben oder sie sogar intern zu nutzen.

- Kosten und Vorhersehbarkeit: Serverlose Umgebungen folgen einem nutzungsabhängigen Preismodell, das für Anwendungen mit sporadischen oder variablen Arbeitslasten kosteneffizient sein kann. Die Preisstruktur kann jedoch manchmal komplex und unvorhersehbar sein, insbesondere bei zusätzlichen Gebühren für API-Aufrufe, Datenübertragung und Ressourcennutzung. In einer IaaS-Umgebung haben die Benutzer mehr Kontrolle über die Ressourcenzuweisung und die Preisgestaltung, was eine bessere Kostenvorhersagbarkeit, aber potenziell höhere Fixkosten ermöglicht.

Anhang 2 - Standards und Zertifizierungssysteme

A2.1. Einleitung

Nachfolgend finden Sie die wichtigsten Standards für Alarmübermittlung, Fernzugriff und Rechenzentren, die bei der Bestimmung der Leistung eines Systems oder Dienstes in Bezug auf seine Widerstandsfähigkeit, Robustheit und Zuverlässigkeit hilfreich sein können.

A2.2. Standards für Alarmübertragung, Fernzugriff auf Alarmsysteme und Ferndienste

EN 50136-1 Allgemeine Anforderungen an Alarmübertragungssysteme

Diese Europäische Norm legt die Anforderungen an die Leistungs-, Zuverlässigkeits- und Sicherheitsmerkmale von Alarmübertragungssystemen fest. Sie spezifiziert die Anforderungen an Alarmübertragungssysteme, die eine Alarmübertragung zwischen einem Alarmsystem in einem überwachten Gebäude und einer Meldeeinrichtung in einer Alarmempfangszentrale ermöglichen.

Diese Europäische Norm gilt für Übertragungssysteme für alle Arten von Alarmmeldungen wie Feuer, Einbruch, Zugangskontrolle, Sozialalarm usw.

Ein FSSS-Dienstanbieter, der die Rolle des ATSP (Alarmübermittlungsdienstanbieter) übernimmt, sollte die Bestimmungen dieses Standards einhalten.

CLC/TS 50136-10 Alarmanlagen - Anforderungen für den Fernzugriff

Dieses Dokument spezifiziert die Mindestanforderungen für eine sichere Verbindung und Sitzung für den Fernzugriff auf ein oder mehrere Alarmsysteme, z.B. Brandschutzsysteme, Einbruch- und Überfallmeldeanlagen, elektronische Zugangskontrollsysteme, Systeme zur Sicherung des Außengeländes, Videoüberwachungssysteme und soziale Alarmsysteme.

Dieses Dokument spezifiziert die Anforderungen an die Leistungs-, Zuverlässigkeits-, Integritäts- und Sicherheitsmerkmale einer Fernzugriffsinfrastruktur.

Dieses Dokument spezifiziert die Anforderungen an eine Fernzugriffsinfrastruktur zwischen einem Fernzugriffs-Client und einem Alarmsystem in den überwachten Räumlichkeiten und kann entweder als Teil des ATS oder als separate Infrastruktur integriert werden.

Ein FSSS-Dienstanbieter, der die Rolle des RAISP (Remote Access Infrastructure Service Provider) übernimmt, sollte die Bestimmungen dieser technischen Spezifikation einhalten.

EN 50710 Anforderungen an die Bereitstellung von sicheren Ferndiensten für Brandschutz- und Sicherheitssysteme

Dieses Dokument spezifiziert die Mindestanforderungen für die Bereitstellung von sicheren Remote-Diensten über eine Remote Zugangsinfrastruktur (RAI), die entweder vor Ort oder extern (z.B. über IP-Verbindungen) zu den folgenden Systemen durchgeführt wird:

a) Brandschutzsysteme, einschließlich, aber nicht beschränkt auf Feuermelde- und Feueralarmsysteme, fest installierte Feuerlöschsysteme, Rauch- und Hitzeschutzsysteme;
b) Sicherheitssysteme, einschließlich, aber nicht beschränkt auf Einbruch- und Überfallmeldeanlagen, elektronische Zugangskontrollsysteme, Systeme zur Sicherung der Außenbereiche und Videoüberwachungssysteme;
c) soziale Alarmsysteme;
d) Notfall-Soundsysteme;
e) eine Kombination aus solchen Systemen;
f) Verwaltungssysteme, die mit den Systemen a) - e) verbunden sind.

Diese Norm ist als Ergänzung zur EN 16763 *Dienstleistungen für Brandschutzsysteme und Sicherheitssysteme.*gedacht.

A2.3. Standard für Cloud-Dienste

CEN/TS 18026 Dreistufiger Ansatz für eine Reihe von Cybersicherheitsanforderungen für Cloud-Dienste

Diese Technische Spezifikation (TS) enthält eine Reihe von Cybersicherheitsanforderungen für Cloud-Dienste. Dieser TS gilt für Organisationen, die Cloud-Dienste anbieten, und für deren Unterdienstorganisationen.

Hinweis: Diese neue TS wurde im Jahr 2024 veröffentlicht.

A2.4. Standard für Informationssicherheits-Managementsysteme

ISO/IEC 27001 Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Managementsysteme für Informationssicherheit - Anforderungen

ISO/IEC 27001 ist ein weithin anerkannter internationaler Standard, der die besten Praktiken für die Implementierung und Pflege eines Informationssicherheitsmanagementsystems (ISMS) beschreibt. Dieser Standard bietet einen Rahmen für das Management von Informationssicherheitsrisiken, einschließlich Menschen, Prozesse und Technologie.

ISO/IEC 27001 deckt alle Aspekte der Informationssicherheit ab, einschließlich Vertraulichkeit, Integrität und Verfügbarkeit, und verlangt von Organisationen, dass sie Kontrollen einführen, um die Vertraulichkeit, Integrität und Verfügbarkeit ihrer Informationsbestände sicherzustellen.

Der Standard verlangt außerdem, dass Organisationen einen risikobasierten Ansatz für das Informationssicherheitsmanagement verfolgen, der die Identifizierung und Bewertung von Risiken, die Implementierung geeigneter Kontrollen zur Minderung dieser Risiken sowie die kontinuierliche Überwachung und Überprüfung der Wirksamkeit der Kontrollen umfasst.

Durch die Implementierung von ISO/IEC 27001 können Organisationen ihr Engagement für die Informationssicherheit unter Beweis stellen und den Interessengruppen die Gewissheit geben, dass ihre Informationen auf sichere und effektive Weise verwaltet werden. Der Standard ist für Unternehmen aller Größen und Branchen anwendbar und wird weithin als Maßstab für das Management der Informationssicherheit anerkannt.

A2.5. Standards für Rechenzentren

ISO/IEC 22237 (und EN 50600) Informationstechnologie - Einrichtungen und Infrastrukturen von Rechenzentren

ISO 22237 ist die ISO-Normenreihe, die den Aufbau, die Struktur, den Betrieb, die physische Sicherheit und die Informationssicherheit von Rechenzentren regelt. Die Absicht der Norm ist es, die notwendigen Bedingungen zu definieren, damit die Ziele der ISO 27001 in einer Rechenzentrumsumgebung erreicht werden können.

Die EN 50600 ist die EN-Normenreihe, die die Planung, den Entwurf, die Beschaffung, die Integration, die Installation, den Betrieb und die Wartung von Einrichtungen und Infrastrukturen in Rechenzentren regelt. Die EN 50600-Serie enthält zwar ähnliche Bestimmungen wie die ISO 22237-Normen, aber sie sind nicht vollständig aufeinander abgestimmt.

EN 50600 ist eine wachsende Familie von Normen, die derzeit aus den folgenden Teilen besteht:

- EN 50600-1, Allgemeine Konzepte
- EN 50600-2-1, Bauwesen
- EN 50600-2-2, Energieversorgung und -verteilung
- EN 50600-2-3. Umweltkontrolle
- EN 50600-2-4, Telekommunikationsverkabelungsinfrastruktur
- EN 50600-2-5, Sicherheitssysteme
- EN 50600-3-1, Management- und Betriebsinformationen
- EN 50600-4-1, Überblick über und allgemeine Anforderungen an Leistungsindikatoren
- EN 50600-4-2, Effektivität der Energienutzung
- EN 50600-4-3, Faktor für erneuerbare Energie

EN 50600 sieht ein Klassifizierungssystem vor, das auf den Schlüsselkriterien Verfügbarkeit, Sicherheit und Energieeffizienz basiert:

1. Verfügbarkeit Klasse. Die AC-Klassifizierung wird in den Bereichen Stromversorgung, Lüftungs- und Klimasysteme und Verkabelung definiert;
2. Schutzklasse. PC ist für den Einbruchschutz, den Brandschutz, den Rauchschutz sowie den Schutz vor Umweltgefahren definiert. Es sollen mindestens drei Schutzklassen gebildet werden;
3. Granularitätsstufe (GL). Die Fähigkeit zum energieeffizienten Betrieb wird anhand von Messqualitäten und Messumfang für die Lüftungs- und Klimaanlagen definiert. Der Standard unterscheidet zwischen drei verschiedenen Granularitätsstufen;

Damit das Design eines Rechenzentrums diesem Standard entspricht:

a. Es wird eine Analyse der Geschäftsrisiken durchgeführt;
b. Eine geeignete AC-Klasse wird anhand der Geschäftsrisikoanalyse ausgewählt;
c. Ein geeigneter PC für die Wege und Räume des Rechenzentrums;
d. Ein angemessener Grad der Befähigung zur Energieeffizienz, GL;
e. Der Designprozess und die Prinzipien werden angewendet.

Anmerkung: Derzeit berücksichtigen Rechenzentren in der Regel weder die EN 50600 noch die ISO 22237. Rechenzentren (AWS, ...) sind in der Regel durch das private Uptime Institute (Tier Certification) und/oder nach ANSI/TIA-942 zertifiziert. Diese 2 Zertifizierungssysteme werden als komplementär betrachtet.

Uptime Institute Tier Zertifizierung

Diese private Zertifizierungsstelle wendet ihre eigenen Tier Standards für die Verfügbarkeit und die Gesamtleistung von Rechenzentren an. Es ermöglicht verschiedene Leistungsstufen, die sowohl die bauliche

Umgebung als auch die Vorgehensweise und Leistung des Betriebsteams berücksichtigen. Es sind 4 Stufen definiert:

- Stufe I: Grundlegende Kapazität: Standortweite Abschaltungen sind für Wartungs- oder Reparaturarbeiten erforderlich. Kapazitäts- oder Verteilungsausfälle haben Auswirkungen auf die Website.
- Stufe II: Redundante Kapazitätskomponenten: Standortweite Abschaltungen für Wartungsarbeiten sind weiterhin erforderlich. Kapazitätsausfälle können die Website beeinträchtigen. Ausfälle bei der Verteilung haben Auswirkungen auf die Website.
- Stufe III: Gleichzeitige Wartung möglich: Jede einzelne Kapazitätskomponente und jeder Verteilungspfad an einem Standort kann zu Wartungszwecken oder zum Austausch planmäßig entfernt werden, ohne dass der Betrieb beeinträchtigt wird. Der Standort ist immer noch dem Risiko eines Geräteausfalls oder eines Bedienungsfehlers ausgesetzt.
- Stufe IV: Fehlertolerant: Ein einzelner Geräteausfall oder eine Unterbrechung des Verteilungsweges wird den Betrieb nicht beeinträchtigen. Eine fehlertolerante Website ist auch gleichzeitig wartbar.

ANSI/TIA-942 Telekommunikationsinfrastruktur-Standard für Rechenzentren

ANSI/TIA-942 ist ein von der Telecommunications Industry Association (TIA) veröffentlichter Standard, der Richtlinien für das Design und den Bau von Rechenzentren enthält, einschließlich Stromversorgungssysteme, mechanische Systeme, Architektur, Sicherheit, Telekommunikationssysteme, Brandschutz und Sicherheit. Der Standard soll sicherstellen, dass Rechenzentren zuverlässig, sicher und skalierbar sind, um den sich entwickelnden Anforderungen der IT-Branche gerecht zu werden.

ANSI/TIA-942 bietet ein umfassendes Rahmenwerk für das Design von Rechenzentren, einschließlich Empfehlungen für die Standortwahl, die Gebäudestruktur, die Verkabelungsinfrastruktur, Kühl- und Stromversorgungssysteme, die Sicherheit und das Management.

ANSI/TIA-942 wird von Entwicklern, Betreibern und Prüfern von Rechenzentren verwendet, um sicherzustellen, dass Rechenzentren nach den besten Praktiken und Standards der Branche entworfen und gebaut werden. Der Standard wird auch häufig von Aufsichtsbehörden und Kunden herangezogen, um die Zuverlässigkeit und Sicherheit von Rechenzentren zu bewerten.

System- und Organisationskontrollen (SOC) 2

SOC 2 ist eine Reihe von Standards, die vom American Institute of Certified Public Accountants (AICPA) entwickelt wurden, um die Sicherheit, Verfügbarkeit, Verarbeitungsintegrität, Vertraulichkeit und den Datenschutz der Systeme und Daten eines Dienstleistungsunternehmens zu bewerten und zu prüfen.

Anmerkung: Während ISO/IEC 27001 allgemein gehalten ist, ist SOC 2 auf Rechenzentren zugeschnitten.

SOC 2-Berichte werden von Dienstleistungsunternehmen (wie z.B. Rechenzentren) verwendet, um ihren Kunden und Stakeholdern zu zeigen, dass sie wirksame interne Kontrollen zum Schutz ihrer sensiblen Daten eingerichtet haben.

SOC 2-Berichte basieren auf den Trust Services Criteria (TSC), einer Reihe von Grundsätzen und Kriterien, die zur Bewertung der Wirksamkeit der Kontrollen einer Dienstleistungsorganisation über ihre Systeme und Daten verwendet werden.

Es gibt zwei Arten von SOC 2-Berichten: Typ I und Typ II. In Berichten des Typs I wird die Gestaltung der Kontrollen einer Dienstleistungsorganisation bewertet, während in Berichten des Typs II die Wirksamkeit dieser Kontrollen über einen bestimmten Zeitraum hinweg beurteilt wird.

SOC 2-Audits werden von unabhängigen, von der AICPA zertifizierten Prüfern durchgeführt.

SOC 2-Audits sind freiwillig, aber sie werden für Dienstleistungsunternehmen, die ihr Engagement für Sicherheit und Datenschutz nachweisen wollen, immer wichtiger.

Um sich auf ein SOC 2-Audit vorzubereiten, müssen Dienstleistungsunternehmen eine Risikobewertung durchführen und eine umfassende Reihe von Kontrollen implementieren, um die Trust Services Criteria zu erfüllen.

SOC 2-Audits umfassen in der Regel eine Kombination aus Befragungen, Dokumentationsprüfungen und Systemtests, um die Wirksamkeit der Kontrollen eines Dienstleistungsunternehmens zu bewerten.

SOC 2-Berichte enthalten eine Stellungnahme des Wirtschaftsprüfers zur Effektivität der Kontrollen einer Dienstleistungsorganisation sowie eine Beschreibung der getesteten Kontrollen und der festgestellten Schwachstellen.

SOC 2-Berichte können an Kunden, Interessengruppen und Aufsichtsbehörden weitergegeben werden, um zu gewährleisten, dass ein Dienstleistungsunternehmen wirksame Kontrollen zum Schutz sensibler Daten implementiert hat.

Ist der SOC 2-Bericht Typ II DIE Empfehlung für Cybersicherheitsaspekte?

SOC 3

SOC iii ist eine Art von Prüfbericht, der einen Überblick über die Kontrollen einer Organisation in Bezug auf Sicherheit, Verfügbarkeit, Verarbeitungsintegrität, Vertraulichkeit und Datenschutz gibt.

Im Gegensatz zu den SOC 1- und SOC 2-Berichten, die für ein bestimmtes Publikum bestimmt sind und detailliertere Informationen über die Kontrollen einer Organisation liefern, sind die SOC 3-Berichte für ein allgemeines Publikum bestimmt und liefern eine Zusammenfassung der Kontrollen der Organisation, die öffentlich zugänglich ist.

Die SOC 3-Berichte basieren auf denselben Kontrollen und Kriterien wie die SOC 2-Berichte, sind jedoch nicht so detailliert wie diese. Stattdessen enthalten die SOC 3-Berichte eine kurze Beschreibung des Systems und der Kontrollen der Organisation sowie eine Erklärung eines unabhängigen Wirtschaftsprüfers, der die Einhaltung der SOC 2-Kriterien durch die Organisation bestätigt.

SOC 3-Berichte werden häufig von Unternehmen verwendet, um ihr Engagement für Sicherheit und Compliance gegenüber Kunden, Partnern und anderen Interessengruppen zu demonstrieren. Da sie öffentlich zugänglich sind, können sie auch von potenziellen Kunden oder Investoren verwendet werden, um die Sicherheitslage eines Unternehmens zu bewerten, bevor sie mit ihm Geschäfte machen.

A2.6. Zertifizierungssysteme

Das Cybersicherheitsgesetz (CSA, (EU) 2019/881) bietet einen europäischen Rahmen für die Cybersicherheitszertifizierung von Produkten, Prozessen und Dienstleistungen. Die ENISA, die Agentur der Europäischen Union für Cybersicherheit, ist berechtigt, Zertifizierungssysteme für Cybersicherheit zu entwickeln, die auf freiwilliger Basis verwendet werden und in der gesamten Europäischen Union gültig sind. Die zweite Regelung soll Cloud-Dienste (EUCS) abdecken. Zum Zeitpunkt der Erstellung dieses Leitfadens ist er noch in Vorbereitung. Es wird erwartet, dass dieses System die oben vorgestellte CEN/TS 18026 nutzt. Wenn es verfügbar ist, könnte es ein nützliches Instrument für den CSP werden, um die Sicherheit seiner Lösung zu demonstrieren und für den FSSS-Dienstanbieter, um dem CSP zu vertrauen.

Datum der Veröffentlichung: 18-02-2025

Euralarm
Gubelstraße 22
CH-6301 Zug (Schweiz)

Swiss Commercial Registrierung Nein: CHE-222.522.503

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