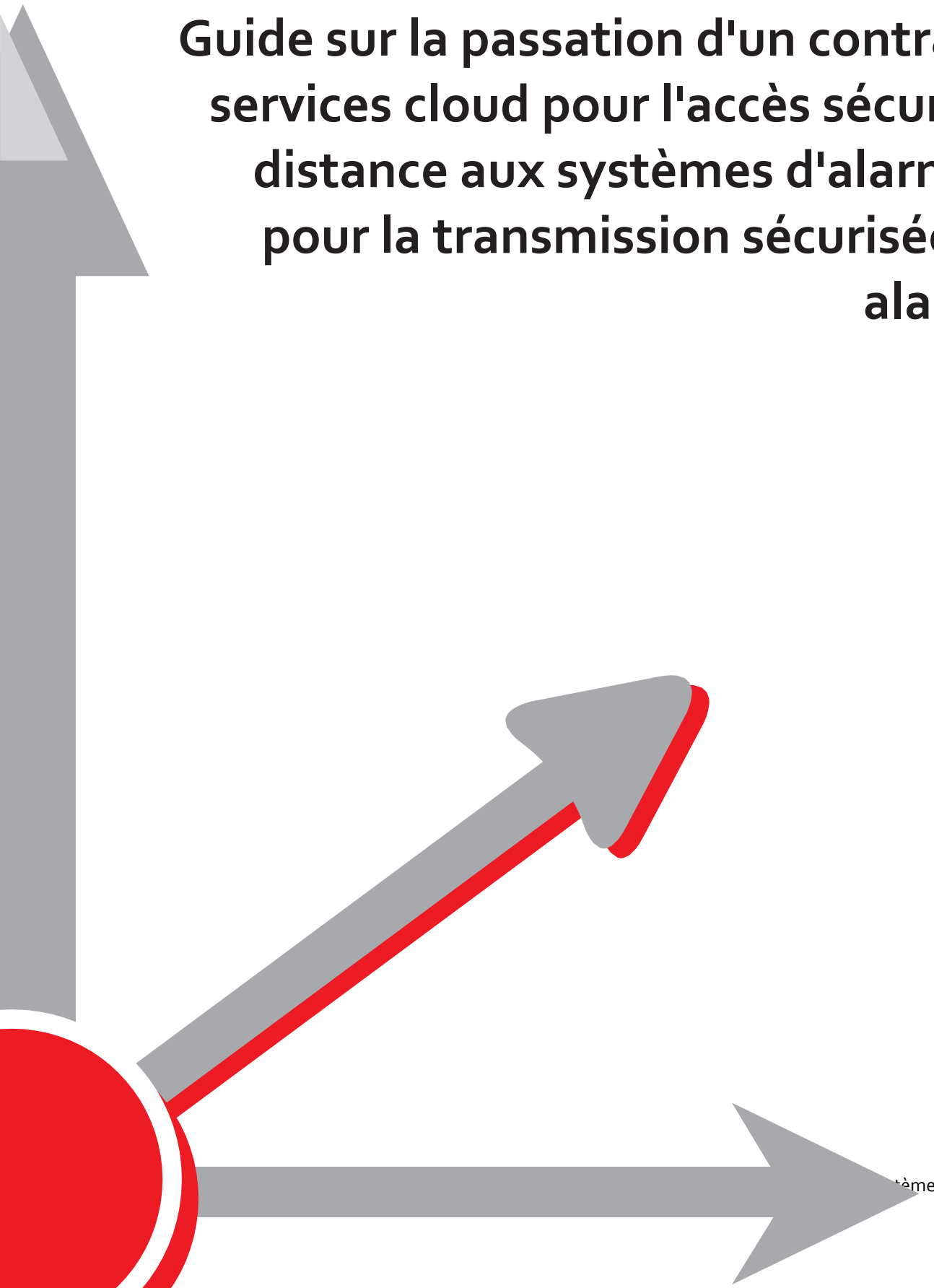
Guide sur la passation d'un contrat de services cloud pour l'accès sécurisé à distance aux systèmes d'alarme et pour la transmission sécurisée des alarmes



tèmes d'alarme et

Tableau de révision des modifications

Date	Rev #	Paragraphe /Page	Changements
Février 2025	1.0		Première version

AVANT-PROPOS

Ce document est destiné à servir d'orientation générale et ne remplace pas des conseils détaillés dans des circonstances spécifiques. Bien que le plus grand soin ait été apporté à la compilation et à la préparation de cette publication pour en garantir l'exactitude, Euralarm ne peut en aucun cas accepter la responsabilité d'erreurs, d'omissions ou de conseils donnés ou de toute perte résultant de la confiance accordée aux informations contenues dans cette publication.

CLAUSE DE NON-RESPONSABILITÉ

Le présent document a pour seul but d'informer les membres d'Euralarm et, le cas échéant, leurs membres, sur l'état des affaires concernant le sujet traité. Bien que tout ait été mis en œuvre pour garantir son exactitude, les lecteurs ne doivent pas se fier à son exhaustivité ou à son exactitude, ni s'en servir comme d'une interprétation juridique. Euralarm n'est pas responsable de la fourniture d'informations incorrectes ou incomplètes.

Note : La version anglaise de ce document est le document de référence approuvé par Euralarm.

Euralarm – Gubelstrasse 11 – CH-6300 Zug – Suisse

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

Table des matières

1. Introduction

Il est de plus en plus courant d'utiliser les technologies les plus récentes pour assurer la transmission d'alarmes par IP et l'accès à distance aux Systèmes de Protection Incendie et/ou aux Systèmes de Sûreté (SPIS) et, par conséquent, de localiser une partie de l'équipement en dehors des locaux du fournisseur de services SPIS. Le présent document aidera les fournisseurs de services SPIS (par exemple les installateurs) à utiliser les services d'un centre de données pour héberger une partie de l'équipement.

Deux cas d'utilisation différents sont examinés ici, avec leurs exigences spécifiques et leur public cible.

- L'un des cas d'utilisation est la transmission d'alarmes via un système de transmission d'alarmes (ATS) exploité et géré par un fournisseur de services de transmission d'alarme (ATSP), pour lequel la disponibilité, le temps de transmission, le signalement des défaillances et la protection contre la substitution sont des caractéristiques essentielles. La norme EN 50136-1 relative aux systèmes de transmission d'alarme (ATS) prévoit des configurations hébergées dans lesquelles l'élément cloud doit se trouver dans un lieu sécurisé, qui peut être un centre de données. Les catégories les plus élevées d'ATS comprennent des exigences de sécurité qui doivent être respectées dans l'ensemble du système. Les orientations relatives à ce cas d'utilisation s'adressent à toute entité jouant le rôle d'ATSP.
- Un autre cas d'utilisation est l'accès à distance au SPIS via une infrastructure d'accès à distance (RAI) exploitée et gérée par un fournisseur de services d'infrastructure d'accès à distance (RAISP), pour lequel l'accès sécurisé au SPIS et aux données est une caractéristique essentielle, tandis que la disponibilité n'est qu'une question de commodité. La spécification technique de l'infrastructure d'accès à distance (RAI) CLC/TS 50136-10 exige que le serveur d'accès à distance (RAS) se trouve dans un endroit sûr et comprend des exigences relatives à la sécurité des données transférées. Les conseils pour ce cas d'utilisation s'adressent à toute entité jouant le rôle de RAISP, plus particulièrement aux petits et moyens fournisseurs de services SPIS qui ont l'intention de jouer le rôle de RAISP, qui ne sont pas familiers avec les services cloud et qui souhaitent fournir des services à distance conformément à la norme EN 50710.

Bien qu'il y ait un certain nombre de bonnes raisons d'envisager des solutions cloud, les fournisseurs de services SPIS doivent comprendre l'impact sur leur activité, y compris la disponibilité, les accords de niveau de service, la sécurité des données, la conformité, les exigences légales et contractuelles. Les fournisseurs de services SPIS devront toujours démontrer qu'ils respectent les normes existantes, par exemple en matière de performance et de disponibilité, de sauvegardes, de contrôle d'accès, etc. Les responsabilités en matière de maintenance doivent être clairement comprises et acceptées par toutes les parties prenantes. Elles comprendront la gestion du cycle de vie des systèmes d'exploitation, des plates-formes (par exemple base de données, virtualisation, etc.) et des applications. Le fournisseur de services SPIS doit être en mesure de confirmer que ces activités ont été menées conformément aux attentes et aux accords de service du fournisseur de services SPIS.

Le stockage, le partage et la sécurité des données sont d'une importance vitale et devront faire l'objet d'un examen juridique au-delà de ce qui est indiqué dans le présent document.

Des sections importantes du présent guide ont été reprises de celui du BSIA intitulé "ARC considerations when using data centre or cloud services", avec l'accord du BSIA. EURALARM remercie son membre, la British Security Industry Association, pour cette contribution.

Ce guide décrit les concepts importants liés aux services cloud, examine les normes pertinentes et donne un

aperçu des critères juridiques pour le choix du fournisseur de services cloud (CSP). Toutefois, le guide ne prétend pas répondre à toutes les exigences légales des différents pays d'Europe. Il convient de prendre soin d'examiner les lignes directrices dans le contexte des exigences légales locales qui prévalent.

2. Abréviations

AICPA : American Institute of Certified Public Accountants (Institut américain des experts-comptables)
AMS : Alarm Management System (Système de gestion des alarmes)
ANSI : American National Standards Institute (Institut national américain de normalisation)
ARC : Alarm Receiving Centre (Centre de réception des alarmes)
AS : Alarm System (Système d'alarme)
ATS : Alarm Transmission System (Système de transmission d'alarme)
BSIA : British Security Industry Association (Association britannique de l'industrie de la sécurité)
CLC : CENELEC
CSP : Cloud Service Provider (fournisseur de services cloud)
EN : norme européenne
FaaS : Function as a Service (Fonction en tant que service)
IaaS : Infrastructure as a Service (Infrastructure en tant que service)
IEC : International Electrotechnical Committee (Comité électrotechnique international)
ISO : International Standardisation Organisation (Organisation internationale de normalisation)
IT : Information Technology (Technologies de l'information)
MARC : Monitoring and Alarm Receiving Centre (Centre de surveillance et de réception des alarmes)
PaaS : Platform as a Service (Plate-forme en tant que service)
PSTN : Public Switched Telephone Network (Réseau téléphonique public commuté)
RAC : Remote Access Client (Client d'accès à distance)
RAE : Remote Access Endpoin (point d'accès à distance)
RAI : Remote Access Infrastructure (Infrastructure d'accès à distance)
RAS : Remote Access Server (Serveur d'accès à distance)
RCT : Receiving Centre Transceiver (émetteur-récepteur du centre de réception d'alarme)
RCT-A : RCT à l'ARC
RCT-H : RCT hébergé
SaaS : Software as a Service (logiciel en tant que service)
SLA : Service Level Agreement (accord de niveau de service)
SOC : System and Organization Controls (Contrôles des systèmes et de l'organisation)
SPIS : Systèmes de sécurité incendie et/ou systèmes de sûreté
SPT : Supervised Premises Transceiver (Émetteur-récepteur dans les locaux surveillés)
TIA : Telecommunications Industry Association (Association de l'industrie des télécommunications)
TS : Technical Specification (Spécification technique)

3. Sujet

Ce document couvre l'élément cloud d'une infrastructure d'accès à distance (RAI, utilisée pour accéder à distance aux fonctionnalités du SPIS) et d'un système de transmission d'alarme (ATS, utilisé pour transmettre les alarmes du SPIS au centre de réception d'alarme).

3.1 Accès à distance au SPIS

Dans le cas d'une RAI, cet élément cloud est identifié comme le RAS dans la figure 1.

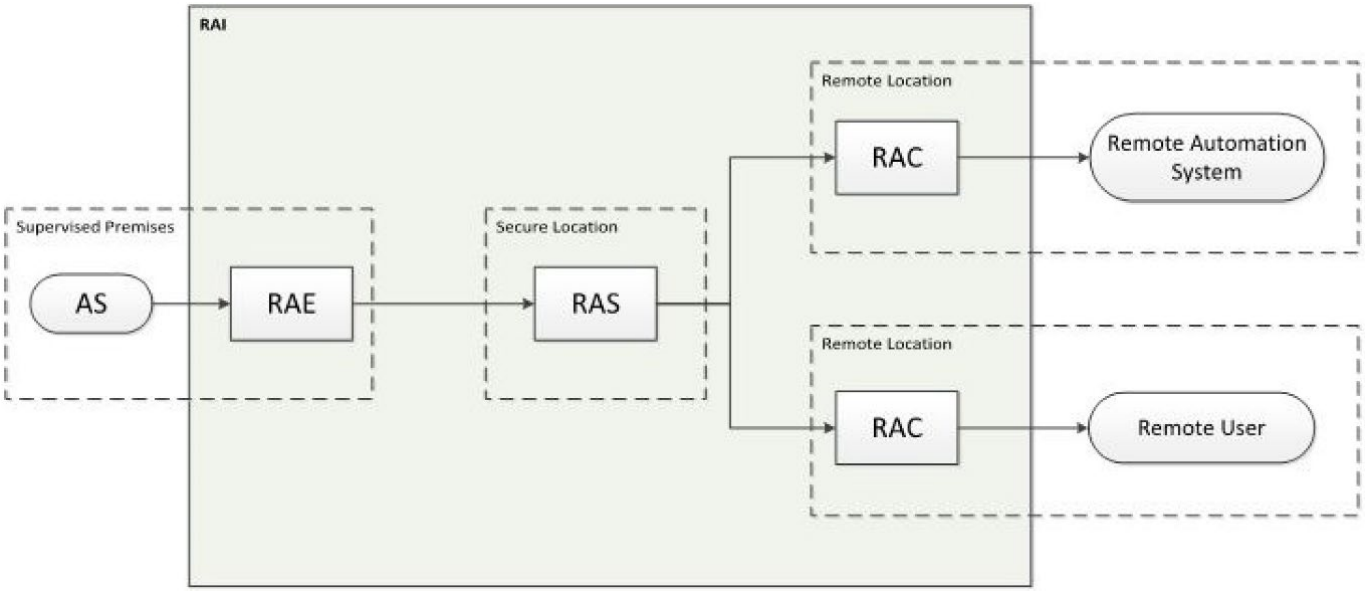


Figure 1. Schéma logique de l'infrastructure d'accès à distance (extrait de CLC/TS 50136-10:2022)

3.2 Transmission d'alarme

Dans le cas d'un ATS, la norme européenne prévoit une configuration non hébergée, décrite à la figure 2a. Dans cette configuration, un lien direct est établi entre le système d'alarme (AS) et l'ARC (MARC). La norme prévoit également une configuration hébergée, décrite à la figure 2b. Dans cette configuration, les messages d'alarme provenant de nombreux systèmes d'alarme convergent vers un récepteur hébergé dans un centre de données et identifié comme RCT-H, où ils sont traités, acquittés et stockés, et où l'ARC y a accès via une voie de communication sécurisée. Les considérations relatives au passage des communications PSTN à la transmission d'alarme IP ont été présentées dans un livre blanc d'Euralarm datant de 2019 : "New Generation Networks for alarm communications"[1] . Le fournisseur de services SPIS doit s'assurer que l'ATS est conforme à la norme EN 50136-1, que le SPT est conforme à la norme EN 50136-2 et que les RCT, RCT-H et RCT-A sont conformes à la norme EN 50136-3 (voir A2.2 à l'annexe 2 pour l'explication de ces normes). Cela garantit que l'ensemble du système ATS transmet les messages d'alarme en temps voulu et qu'il est surveillé en cas de défaillance dans la transmission des alarmes.

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

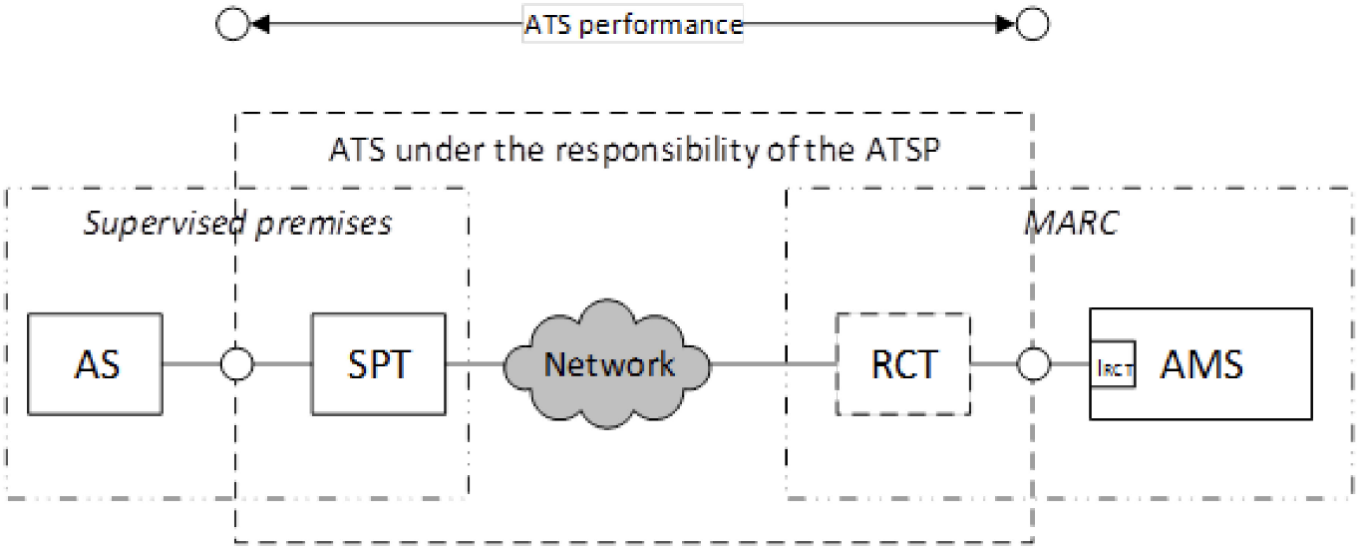


Figure 2a. Exemple de système de transmission d'alarme **non hébergé** (extrait de la norme EN 50136-1/A1:2018)

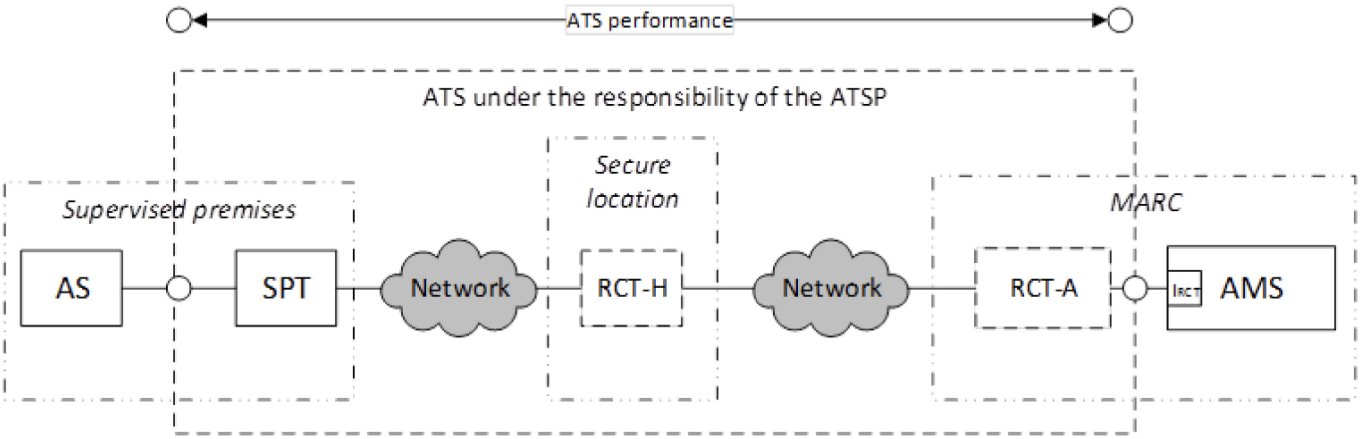


Figure 2b. Exemple de système de transmission d'alarme **hébergé** (extrait de la norme EN 50136-1/A1:2018)

3.3 Général

Les présentes lignes directrices décrivent les éléments à prendre en compte par le fournisseur de services SPIS lorsqu'il choisit d'utiliser les services d'un centre de données ou des services cloud. Cela devrait aider à décider dans quelle mesure le fournisseur de services SPIS devrait/pourrait être hébergé de manière sûre et sécurisée (ou partiellement hébergé) dans un environnement cloud.

Un fournisseur de services SPIS protège constamment des vies et des biens et, à cet égard, les exigences sont plus critiques que pour la plupart des autres organisations.

4. Environnements cloud

4.1 Introduction

Un contrôle préalable est crucial lors de l'évaluation et de la sélection des fournisseurs de services cloud. Ce contrôle préalable consiste à effectuer des recherches approfondies et à évaluer les vendeurs ou les prestataires de services potentiels avant de nouer une relation d'affaires avec eux. Ce processus permet de mieux comprendre les capacités, la fiabilité, les mesures de sécurité et l'adéquation globale du fournisseur aux besoins spécifiques.

Trois environnements sont classiquement définis : private business cloud solution, data centre hosted (ci-après Centre de données) ou native cloud (ci-après Cloud). Le fournisseur de services SPIS peut soit utiliser un ou plusieurs de ces environnements pour faire fonctionner l'équipement technique qui compose l'accès à distance ou la transmission d'alarme, soit utiliser la solution offerte par le fabricant du SPIS.

Le présent document n'implique pas que les environnements private business cloud solution ou native cloud constituent le mode d'exploitation unique pour toutes les applications mais il reconnaît que le fournisseur de services SPIS peut exploiter et exploitera des applications dans des modèles d'environnement multiples. En d'autres termes, il peut utiliser les trois environnements d'exploitation à des degrés divers, en fonction des exigences du service.

Les fournisseurs de services SPIS doivent également prendre en compte les exigences de certification de leur tierce partie lorsqu'ils choisissent leur propre solution, des solutions de centre de données ou des solutions cloud.

L'utilisation de centres de données/services cloud n'exclut pas les responsabilités du fournisseur de services SPIS telles que détaillées dans les normes EN 16763, EN 50710 ou EN 50136-1 (voir A2.2 de l'annexe 2 pour l'explication de ces normes). Un guide Euralarm[2] consacré à la mise en œuvre des services à distance a été publié et peut être consulté sur le site web. Il aide le fournisseur de services SPIS à vérifier au préalable sa conformité avec les exigences de ces normes.

4.2 Private business cloud solution

Les solutions privées sont gérées par le fournisseur de services SPIS. Les serveurs sont installés soit dans le même bâtiment ou dans les mêmes locaux que le fournisseur de services de SPIS, soit dans un autre bâtiment sous la responsabilité du fournisseur de services de SPIS. Un fournisseur d'applications fournira à la société de services le logiciel à exécuter sur les serveurs. Les serveurs sont soit achetés par le fournisseur de services SPIS, soit achetés dans le cadre du service du fournisseur d'applications.

Les mises à jour des systèmes d'exploitation des serveurs, des bases de données et du logiciel d'application seront coordonnées entre le fournisseur de services SPIS et le fournisseur d'applications. La sécurité (encryption des données stockées, etc.) et la fiabilité (comme la réplication de la base de données avec une diversité géographique) sont des solutions qui sont généralement mises en place par le fournisseur d'applications.

4.3 Centre de données

Les solutions de centre de données sont des serveurs installés dans des locaux exploités par une société tierce qui assure la sécurité physique, l'alimentation électrique et l'espace de stockage des serveurs. Ces serveurs peuvent être dédiés à un fournisseur de services SPIS spécifique ou fonctionner dans un environnement multi-locataires. Ces serveurs sont maintenus par le fournisseur de services SPIS ou par le fournisseur d'applications en tant que service géré.

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

4.4 Cloud

4.4.1 Description

Les solutions cloud comprennent toutes les caractéristiques de la solution du centre de données mais les serveurs et autres technologies connexes (bases de données, etc.) sont fournis et entretenus par le fournisseur de services cloud (par exemple, AWS - Amazon Web Services, Microsoft Azure, Google Cloud, IBM). Le modèle de responsabilité partagée pour le cloud (SRM) est un cadre qui délimite les responsabilités entre un fournisseur de services cloud et le fournisseur d'applications pour la sécurisation de l'environnement cloud.

Le fournisseur de services cloud protège les actifs de l'environnement du développeur d'applications. Par exemple, il assure la sécurité physique et sécurise les services de virtualisation. Le fournisseur d'applications sécurise les actifs de son instance cloud, c'est-à-dire qu'il sécurise le système d'exploitation qu'il installe sur les serveurs et qu'il détermine qui a accès à votre environnement cloud.

L'environnement cloud englobe plusieurs modèles qui répondent à différents besoins et cas d'utilisation. Il est important de noter que ces modèles ne s'excluent pas mutuellement et que les fournisseurs de services cloud proposent souvent une combinaison de ces modèles afin de répondre aux différentes exigences et préférences. Les sections suivantes décrivent quatre modèles différents d'environnement cloud.

4.4.2 Infrastructure en tant que service (IaaS)

Ce modèle fournit des ressources informatiques virtualisées sur l'internet. Il offre des machines virtuelles, du stockage et des réseaux que les utilisateurs peuvent approvisionner et gérer. Les utilisateurs ont davantage de contrôle sur l'infrastructure, y compris sur les systèmes d'exploitation et les applications.

4.4.3 Plate-forme en tant que service (PaaS)

Le PaaS offre aux développeurs une plateforme qui leur permet de créer, de déployer et de gérer des applications sans se soucier de l'infrastructure sous-jacente. Il fournit un environnement préconfiguré avec des outils, des cadres et un moteur d'exécution pour le développement d'applications. Les utilisateurs peuvent se concentrer sur le codage et la logique de l'application, tandis que la plateforme gère l'évolutivité, l'équilibrage de la charge et le déploiement.

4.4.4 Serverless computing

Serverless computing est un modèle dans lequel les développeurs écrivent et déploient du code sous forme de fonctions individuelles ou d'unités de code. Le fournisseur de services cloud gère l'infrastructure et dimensionne automatiquement les ressources en fonction de la demande. Les développeurs n'ont pas à se préoccuper des serveurs ou de la gestion de l'infrastructure et se concentrent uniquement sur l'écriture du code.

4.4.5 Logiciel en tant que service (SaaS)

Le SaaS est une application logicielle complète fournie sur l'internet. Les utilisateurs finaux des SPIS ou les

fournisseurs de services SPIS peuvent accéder au logiciel et l'utiliser sans qu'il soit nécessaire de l'installer ou de le gérer. Les fournisseurs de solutions SaaS exploitent leurs serveurs dans des modèles informatiques IaaS, PaaS ou serverless.

4.4.6 Considérations relatives aux modèles native cloud

Il est important d'examiner attentivement les exigences et les contraintes spécifiques d'une application critique lors du choix d'un environnement. Des facteurs tels que les besoins de performance, les exigences d'évolutivité, les options de gestion et les considérations de coût doivent être pris en compte pour déterminer la solution la mieux adaptée aux objectifs de l'application.

Voir l'annexe 1 pour plus d'informations.

4.5 Solution du fabricant

Les fabricants de SPIS ont développé leurs solutions et les proposent aux fournisseurs de services SPIS qui utilisent leurs systèmes. Une telle solution peut être basée sur l'un des trois environnements décrits ci-dessus. Le fournisseur de services SPIS ne doit pas se préoccuper de la maintenance des serveurs, des logiciels et des applications. Il doit veiller à ce que l'accord contractuel corresponde à ses besoins et à ses attentes.

En général, le fournisseur de services SPIS n'a pas de contrat avec le fabricant pour l'utilisation de sa solution, mais il accepte les conditions en se connectant à l'application cloud. Par conséquent, il est conseillé au fabricant d'élaborer un document pour l'installateur dans lequel il précise clairement son application cloud :

- quel fournisseur de services cloud,
- l'endroit où se trouvent les données,
- les modalités d'accès, y compris les mesures de sécurité,
- le niveau de service, comme le temps de récupération et la maintenance,
- la certification à laquelle le fabricant peut se référer,
- la manière dont le fournisseur de services SPIS doit connecter correctement le SPIS,
- ...

4.6 Considérations relatives aux environnements d'exploitation

Les solutions private business cloud et les solutions de centre de données nécessitent des investissements dans le matériel, les logiciels et l'infrastructure, ainsi que l'expertise nécessaire à leur mise en place et à leur maintenance. Les solutions basées sur le cloud exigent toujours du fournisseur d'applications qu'il possède les compétences nécessaires pour comprendre, contrôler et faire évoluer les fonctionnalités requises. Le fournisseur de services cloud regroupe des services informatiques spécialisés pour le déploiement et la maintenance du matériel, des systèmes d'exploitation et des logiciels de base de données.

Des mesures doivent être prises pour assurer la sécurité des données accessibles via des connexions en ligne ou dans le cloud.

5. Critères légaux pour la localisation des serveurs

5.1 Introduction

Les réglementations relatives aux serveurs de données dans les pays européens sont régies par une combinaison de lois nationales et de réglementations de l'Union européenne. Voici un aperçu des principales règles en vigueur dans les différents pays européens, ainsi que du cadre général de l'UE.

5.2 Règlement général sur la protection des données (RGPD) de l'Union européenne

Le RGPD, en vigueur depuis mai 2018, est le principal règlement régissant la protection des données et la vie privée dans l'UE. Il s'applique à tous les États membres et comprend :

- les principes de traitement des données : légalité, loyauté, transparence, limitation des finalités, minimisation des données, exactitude, limitation du stockage, intégrité et confidentialité ;
- les droits des personnes concernées : droit d'accès, de rectification, d'effacement (droit à l'oubli), de limitation du traitement, de portabilité des données et d'opposition ;
- transfert de données : restrictions au transfert de données à caractère personnel en dehors de l'UE/EEE, garantissant des niveaux de protection adéquats ;
- notifications des violations de données : obligation de notifier aux autorités et aux personnes concernées les violations de données dans un délai de 72 heures.

5.3 Exemples de réglementations nationales

Allemagne

Loi fédérale sur la protection des données (Bundesdatenschutzgesetz, BDSG) : Complète le RGPD avec des exigences supplémentaires, y compris des règles plus strictes sur le traitement des données à des fins d'emploi et des obligations spécifiques pour les responsables de la protection des données.

France

Loi Informatique et Libertés : Met en œuvre les dispositions du RGPD et ajoute des spécificités nationales, telles que des règles sur le traitement des données de santé et des pouvoirs supplémentaires pour l'autorité nationale de protection des données (CNIL).

Royaume-Uni

Loi sur la protection des données 2018 : Met en œuvre le RGPD et comprend des dispositions spécifiques pour le traitement des données par les autorités publiques et les organismes d'application de la loi. À la suite du Brexit, le Royaume-Uni a adopté le UK GDPR, qui reflète le RGPD de l'UE mais fonctionne de manière indépendante.

Italie

Code de protection des données (Codice in materia di protezione dei dati personali) : S'aligne sur le RGPD, avec des règles nationales supplémentaires sur le traitement des données pour la recherche scientifique et historique, et à des fins journalistiques.

Espagne

Loi organique sur la protection des données et des droits numériques (LOPDGDD) : Complète le RGPD avec des règles spécifiques sur les droits numériques et des protections supplémentaires pour les mineurs et les personnes vulnérables.

Pays-Bas

Loi néerlandaise de mise en œuvre (Uitvoeringswet AVG) : Complète le RGPD par des dispositions nationales, notamment en ce qui concerne le traitement des casiers judiciaires et des données des employés.

Belgique

Loi d'application belge (Autorité de Protection des Données) loi cadre du 30 juillet 2018

Les thèmes communs à tous les pays sont les suivants :

- localisation des données : certains pays ont des exigences spécifiques en matière de localisation des données, en particulier pour les données sensibles telles que les dossiers médicaux ;
- les réglementations sectorielles : de nombreux pays imposent des réglementations supplémentaires pour certains secteurs tels que la finance, la santé et les télécommunications ;
- Autorités de protection des données (APD) : chaque pays dispose d'une APD nationale chargée de faire appliquer les lois sur la protection des données et de traiter les plaintes. Il s'agit par exemple de la CNIL en France, de l'ICO au Royaume-Uni et du BfDI en Allemagne ;
- les transferts de données transfrontaliers : Les pays de l'UE suivent généralement le cadre du RGPD pour les transferts internationaux de données, qui comprend des mécanismes tels que les Clauses Contractuelles Types (SCC), les Règles Contraignantes d'Entreprise (BCR) et les décisions d'adéquation.

Cette liste de législations nationales n'est pas exhaustive. Pour des réglementations plus spécifiques et les dernières mises à jour, il est conseillé de consulter les autorités nationales de protection des données et les textes juridiques de chaque pays.

5.4 Références utiles

- Commission européenne - Protection des données[3]
- Texte du RGPD[4]
- CNIL (France)[5]
- ICO (ROYAUME-UNI)[6]
- BfDI (Allemagne)

6. Répartition des rôles et des responsabilités

6.1 Impact des activités de maintenance (planifiées/non planifiées)

La disponibilité de l'infrastructure peut être plus ou moins critique selon les services qu'elle fournit. Les services de transmission d'alarmes nécessitent une disponibilité élevée définie par la catégorie applicable de la norme EN 50136-1. La disponibilité est généralement considérée comme moins critique pour les services d'accès à distance.

Le fournisseur de services SPIS (ou le fabricant dans l'environnement de la solution fabricant) doit avoir mis en place des processus pour gérer les activités de maintenance et, le cas échéant, les atténuer, par exemple en assurant la disponibilité d'un système secondaire ou en dupliquant l'infrastructure, etc.

Les fournisseurs de services de SPIS qui envisagent une solution hébergée doivent s'assurer que des accords (SLA) sont en place avec les fournisseurs de services cloud pour garantir que le fournisseur de services SPIS est informé à l'avance de la durée des périodes de mise hors ligne pendant la maintenance planifiée. Ces accords doivent également prévoir les modalités de gestion et de communication de la maintenance non planifiée.

[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

Lorsque les fournisseurs de services SPIS font appel à des tiers pour les services IT, le fournisseur de services SPIS doit examiner comment les incidents peuvent influer sur la capacité des prestataires de services informatiques à fournir une assistance.

6.2 Compétence IT

Le fournisseur de services SPIS est en fin de compte responsable de son propre équipement et de ses propres systèmes et aura besoin d'un certain niveau de compétence informatique locale pour garantir la gestion des activités de contrôle et de maintenance de routine sur la solution du fournisseur de services SPIS.

6.3 Sécurité

Les fournisseurs de services SPIS doivent déterminer qui a accès à leurs systèmes et à leurs données et tenir compte des exigences en matière de contrôle du personnel. Il existe plusieurs options pour résoudre les problèmes de sécurité, notamment

- Gestion des identités et des accès (IAM)
- Cryptage
- Surveillance de la sécurité et enregistrement des événements (log)
- Conformité et certifications
- Sécurité des réseaux.

Les solutions de centre de données nécessitent du personnel sur place et/ou un accès à distance pour gérer et entretenir l'infrastructure, y compris la maintenance du matériel, les mises à jour logicielles et les correctifs de sécurité. En revanche, les solutions cloud sont gérées par le fournisseur de services cloud, qui s'occupe de toute la maintenance de l'infrastructure, des mises à jour logicielles et des correctifs de sécurité, libérant ainsi le personnel IT interne pour qu'il se concentre sur les fonctions essentielles de l'entreprise.

Dans tout environnement cloud, il y a une responsabilité partagée entre le fournisseur de services cloud (CSP) et l'utilisateur (fournisseur de services SPIS ou fabricant). La sécurité des éléments tels que la classification des données, les contrôles du réseau et la sécurité physique doit être clairement définie. La répartition de ces responsabilités est connue sous le nom de modèle de responsabilité partagée (SRM) pour la sécurité du cloud. Consultez le tableau ci-dessous pour savoir où se situent les responsabilités dans les différents environnements cloud.

Solution d'informatique dématérialisée pour les entreprises	Infrastructure en tant que service *IaaS*	Plate-forme en tant que service *PaaS*	Logiciel en tant que service *SaaS*
Données et configurations	Données et configurations	Données et configurations	Données et configurations
Code d'application	Code d'application	Code d'application	Code d'application
Mise à l'échelle	Mise à l'échelle	Mise à l'échelle	Mise à l'échelle
Temps d'exécution	Temps d'exécution	Temps d'exécution	Temps d'exécution
Système d'exploitation	Système d'exploitation	Système d'exploitation	Système d'exploitation
Virtualisation	Virtualisation	Virtualisation	Virtualisation
Matériel	Matériel	Matériel	Matériel
Sous la responsabilité du fournisseur de services SPIS ou le fabricant			
Sous la responsabilité du fournisseur de services cloud			

De plus amples informations et conseils sur les SRM sont disponibles sur le site web du Center for Internet Security (CIS) .[7]

7. Passation de contrats de services cloud

La Commission européenne a écrit en 2012 dans sa communication intitulée " Exploiter le potentiel de l'informatique en nuage en Europe " :[8]

> *" Traditionnellement, dans le domaine de l'informatique, les accords d'externalisation faisaient l'objet d'une négociation et concernaient le stockage de données, les installations de traitement et des services définis et décrits en détail dès le départ. En revanche, les contrats relatifs aux services informatiques en nuage constituent essentiellement un cadre dans lequel l'utilisateur a accès à des capacités informatiques infiniment modulables et souples, selon ses besoins. Toutefois, si l'informatique en nuage offre actuellement davantage de souplesse qu'une externalisation traditionnelle, le client doit, en contrepartie, faire face à davantage d'incertitudes car les contrats avec les prestataires de services en nuage ne sont ni suffisamment précis ni suffisamment équilibrés.*
>
> *La complexité et le flou du cadre juridique applicable aux prestataires de services en nuage font que ces derniers ont souvent recours à des contrats compliqués ou à des accords sur le niveau de service assortis de clauses de non-responsabilité détaillées. Le recours à des contrats standard «à prendre ou à laisser» pourrait permettre au prestataire de faire des économies mais, souvent, l'utilisateur, et notamment l'utilisateur final, n'en veut pas. Les contrats de ce type peuvent aussi imposer un choix en matière de droit applicable ou interdire la récupération de données. Même les grandes entreprises n'ont qu'un faible pouvoir de négociation, et les contrats contiennent rarement de clause de responsabilité concernant l'intégrité des données, la confidentialité ou la continuité du service. »*

Afin d'aider à résoudre cette complexité et cette incertitude, des conseils détaillés sur les éléments contractuels clés peuvent être trouvés dans les "Guidelines on outsourcing to cloud service providers"[9] publiées par l'Autorité européenne des marchés financiers (esma) en 2021 dans de nombreuses langues européennes. En particulier, les sections suivantes du document peuvent être pertinentes :

- Orientation 3 - Éléments contractuels clés
- Orientation 4 - Sécurité de l'information
- Orientation 5 - Stratégies de retrait
- Orientation 6 - Droits d'accès et d'audit.

REMARQUE : Des orientations similaires sont également disponibles sur le site web de l'Autorité européenne des assurances et des pensions professionnelles (eiopa)[10] .

En outre, dans le cadre du Data Act ((UE) 2023/2854), la Commission européenne prépare des clauses contractuelles types pour guider les parties prenantes dans la mise en œuvre des dispositions concernant le changement de fournisseur de services cloud et le partage des données. Ces orientations devraient être publiées dans le courant de l'année 2025.

[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
[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

Enfin, l'annexe 2 de la présente ligne directrice Euralarm fait référence à des normes et à des systèmes de certification dont le respect peut être exigé dans le contrat conclu avec le fournisseur de services cloud.

De plus amples informations sur les contrats cloud sont disponibles sur le site web de la Commission européenne:

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

8. Conclusion

Étant donné qu'il n'existe pas de système de certification unique ou unifié pour les centres de données et les services cloud, le fournisseur de services SPIS doit avoir l'assurance que le CSP veille à ce que le centre de données réponde aux exigences de fiabilité et de sécurité requises pour le cas d'utilisation considéré. Toute déclaration de conformité revendiquée par le CSP ou le fabricant pour démontrer la fiabilité et la sécurité du service cloud doit au moins englober les considérations suivantes :

- concernant le centre de données utilisé :
  - son nom et son (ses) emplacement(s) ;
  - niveau d'assurance de la continuité des activités de l'absence de continuité à la continuité totale en cas de défaillance du centre de données (essentiel pour la transmission des alarmes et commode pour l'accès à distance) ;
  - les moyens de minimiser le risque de défaillance comme le choix d'un ou de plusieurs sites, la structure du bâtiment, les systèmes d'alimentation électrique, les systèmes de refroidissement, les systèmes mécaniques, l'architecture, la sécurité physique, la cybersécurité, l'infrastructure de câblage, les systèmes de télécommunications, la politique de sauvegarde, la protection contre l'incendie et la sûreté (essentielle pour la transmission des alarmes et commode pour l'accès à distance) ;
- concernant le service cloud :
  - l'environnement cloud utilisé ;
  - une répartition claire et comprise des rôles et des responsabilités dûment définie dans un accord de niveau de service ;
  - plan de reprise après sinistre (DRP) en place (essentiel pour la transmission des alarmes et commode pour l'accès à distance) ;
  - plan de test après une mise à jour du logiciel ;
  - la notification du fournisseur de services SPIS en cas de mise à jour du système, de mise à jour du logiciel ou de changement de prestataire ;
- concernant la cybersécurité et la confidentialité des centres de données et des services cloud :
  - la conformité à la norme ISO/IEC 27001 ;
  - certificat dans le cadre du système de certification EUCS (le cas échéant, voir A2.6) ;
  - des mécanismes de contrôle d'accès sécurisés avec authentification pour accéder aux données et fonctions stockées ;
  - le cryptage des données en transit ;
  - l'atténuation des effets des attaques (D)DOS ;
  - le processus de traitement des vulnérabilités ;
  - vérification par des tests de pénétration ;
- pour la transmission des alarmes :
  - la conformité de l'ATS à la norme EN 50136-1 dans une catégorie déclarée appropriée au risque

[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

protégé (délai de transmission, disponibilité, délai de signalement en cas d'échec de la transmission, exigence de cryptage, sécurité contre la substitution, mode d'accusé de réception, etc.) ;
    - la catégorie à double chemin de transmission (DP) là où des risques élevés sont couverts ou pour des systèmes vitaux (mettant la vie en danger) ;
- pour l'accès à distance au SPIS :
    - la conformité de la RAI à la spécification technique CLC/TS 50136-10.

9. Bibliographie

"ARC considerations when utilizing data centre or cloud services", BSIA (British Security Industry Association), Issue 1, October 2023.

Annexe 1 - Centre de données/IaaS et serverless

Pour une application critique, les environnements IaaS (Infrastructure as a Service) et serverless ont tous deux leurs avantages et leurs inconvénients. Voici quelques comparaisons entre les deux :

- Complexité de la gestion : dans un environnement IaaS, les utilisateurs ont le contrôle total de l'infrastructure, ce qui signifie qu'ils doivent s'occuper de tâches telles que le provisionnement et la gestion des serveurs, la configuration du réseau et la garantie de la haute disponibilité. Cela nécessite plus d'expertise, de temps et de ressources par rapport à un environnement serverless où la gestion de l'infrastructure est abstraite. Avec le serverless, les fournisseurs d'applications peuvent se concentrer uniquement sur la fourniture de services logiciels, mais ils ont moins de compréhension de l'infrastructure sous-jacente, ce qui peut être une limitation pour certaines applications critiques.

- Évolutivité : Dans un environnement IaaS, la mise à l'échelle de l'infrastructure pour gérer l'augmentation du trafic ou de la demande nécessite une intervention et une configuration manuelles. En revanche, les environnements serverless mettent automatiquement à l'échelle les ressources en fonction du nombre de demandes ou d'événements déclenchés, ce qui permet une évolutivité plus dynamique. Cependant, le serverless peut avoir certaines limitations sur l'évolutivité, telles que les exécutions simultanées maximales ou la durée d'exécution, ce qui peut avoir un impact sur les applications très exigeantes.

- Démarrage à froid et performances : Les environnements serverless ont souvent un concept appelé "démarrage à froid", où la première exécution d'une fonction subit une latence supplémentaire en raison de la nécessité d'initialiser l'environnement d'exécution. Cette latence peut avoir un impact sur les applications en temps réel ou à faible latence. Dans un environnement IaaS, les applications s'exécutent sur des serveurs dédiés ou des machines virtuelles, qui offrent généralement des performances constantes sans délai de démarrage à froid. En outre, les environnements serverless peuvent avoir des limitations sur les ressources allouées aux fonctions individuelles, ce qui peut affecter les performances des applications gourmandes en ressources.

- Verrouillage des fournisseurs : Si les environnements IaaS et serverless impliquent tous deux un certain niveau de verrouillage des fournisseurs, les environnements serverless ont souvent des services plus étroitement intégrés et des architectures pilotées par les événements, ce qui peut rendre plus difficile la migration des applications entre différents fournisseurs de services cloud ou vers une infrastructure sur site. Dans un environnement IaaS, les utilisateurs ont plus de flexibilité pour déplacer leurs applications entre différents fournisseurs ou même les amener en interne.

- Coût et prévisibilité : Les environnements serverless suivent un modèle de tarification à l'utilisation, qui peut être rentable pour les applications dont la charge de travail est sporadique ou variable. Cependant, la structure tarifaire peut parfois être complexe et imprévisible, notamment avec des frais supplémentaires pour les appels API, le transfert de données et l'utilisation des ressources. Dans un environnement IaaS, les utilisateurs ont davantage de contrôle sur l'allocation des ressources et la tarification, ce qui permet une meilleure prévisibilité des coûts, mais des coûts fixes potentiellement plus élevés.

Annexe 2 - Normes et schémas de certification

A2.1. Introduction

Les normes fondamentales suivantes relatives à la transmission des alarmes, à l'accès à distance et aux centres de données peuvent être utiles pour déterminer les performances d'un système ou d'un service en termes de résilience, de robustesse et de fiabilité.

A2.2. Normes relatives à la transmission d'alarmes, à l'accès à distance aux systèmes d'alarme et aux services à distance

EN 50136-1 Exigences générales pour les systèmes de transmission d'alarme

Cette norme européenne spécifie les exigences relatives aux caractéristiques de performance, de fiabilité et de sécurité des systèmes de transmission d'alarme. Elle spécifie les exigences relatives aux systèmes de transmission d'alarme assurant la transmission des alarmes entre un système d'alarme situé dans un local surveillé et un équipement d'annonce situé dans un centre de réception des alarmes.

Cette norme européenne s'applique aux systèmes de transmission de tous les types de messages d'alarme tels que l'incendie, l'intrusion, le contrôle d'accès, l'alarme sociale, etc.

Un fournisseur de services SPIS jouant le rôle d'ATSP (Alarm Transmission Service Provider) doit se conformer aux dispositions de celle-ci.

CLC/TS 50136-10 Systèmes d'alarme - Exigences relatives à l'accès à distance

Ce document spécifie les exigences minimales en matière de connexion et de session sécurisées pour l'accès à distance à un ou plusieurs systèmes d'alarme, par exemple les systèmes de sécurité incendie, les systèmes d'alarme contre les intrusions et les hold-up, les systèmes de contrôle d'accès électronique, les systèmes de sécurité du périmètre extérieur, les systèmes de vidéosurveillance et les systèmes d'alarme sociale.

Il spécifie les exigences relatives aux caractéristiques de performance, de fiabilité, d'intégrité et de sécurité d'une infrastructure d'accès à distance.

Il spécifie les exigences relatives à une infrastructure d'accès à distance entre un client d'accès à distance et un système d'alarme situé dans les locaux surveillés ; cette infrastructure peut être intégrée à l'ATS ou constituer une infrastructure distincte.

Un fournisseur de services SPIS jouant le rôle de RAISP (Remote Access Infrastructure Service Provider) doit se conformer aux dispositions de cette spécification technique.

EN 50710 Lignes directrices et exigences relatives aux services à distance sécurisés pour les systèmes de protection incendie et les systèmes de sûreté

Ce document spécifie les exigences minimales pour la fourniture de services à distance sécurisés par l'intermédiaire d'une infrastructure d'accès à distance (RAI) effectuée soit sur le site soit hors site (par exemple

via des connexions IP) aux systèmes suivants :

a) les systèmes de sécurité incendie, y compris mais sans s'y limiter, les systèmes de détection et d'alarme incendie, les systèmes fixes de lutte contre l'incendie, les systèmes de contrôle des fumées et de la chaleur ;
b) les systèmes de sûreté, y compris mais sans s'y limiter, les systèmes d'alarme en cas d'intrusion ou de hold-up, les systèmes de contrôle d'accès électronique, les systèmes de sécurité du périmètre extérieur et les systèmes de vidéosurveillance ;
c) les systèmes d'alarme sociale ;
d) les systèmes de sonorisation d'urgence ;
e) une combinaison de ces systèmes ;
f) les systèmes de gestion connectés aux systèmes a) à e).

Cette norme est destinée à compléter la norme EN 16763 *Prestations de services pour les systèmes de sécurité incendie et les systèmes de sûreté.*

A2.3. Norme pour les services cloud

CEN/TS 18026 Three-level approach for a set of cybersecurity requirements for cloud services

Cette spécification technique (TS) fournit un ensemble d'exigences de cybersécurité pour les services cloud. Elle s'applique aux organismes fournissant des services cloud et à leurs organismes de sous-services.

A2.4. Norme pour les systèmes de gestion de la sécurité de l'information

ISO/IEC 27001 Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

ISO/IEC 27001 est une norme internationale largement reconnue qui décrit les meilleures pratiques pour la mise en œuvre et le maintien d'un système de gestion de la sécurité de l'information (SGSI). Cette norme fournit un cadre pour la gestion des risques liés à la sécurité de l'information, y compris les personnes, les processus et la technologie.

La norme ISO/IEC 27001 couvre tous les aspects de la sécurité de l'information, y compris la confidentialité, l'intégrité et la disponibilité, et exige des organisations qu'elles mettent en œuvre des contrôles pour garantir la confidentialité, l'intégrité et la disponibilité de leurs actifs informationnels.

La norme exige également que les organisations adoptent une approche de la gestion de la sécurité de l'information fondée sur les risques, ce qui implique l'identification et l'évaluation des risques, la mise en œuvre de contrôles appropriés pour atténuer ces risques ainsi que la surveillance et l'examen continus de l'efficacité des contrôles.

En mettant en œuvre la norme ISO/IEC 27001, les organismes peuvent démontrer leur engagement en matière de sécurité de l'information et donner aux parties prenantes l'assurance que leurs actifs informationnels sont gérés de manière sûre et efficace. La norme s'applique aux organisations de toutes tailles et de tous secteurs, et elle est largement reconnue comme une référence en matière de gestion de la sécurité de l'information.

A2.5. Normes pour les centres de données

ISO/IEC 22237 (et EN 50600) Technologie de l'information — Installation et infrastructures de centres de traitement de données

ISO 22237 est la série de normes ISO qui régit la conception, la structure, l'exploitation et la sécurité physique et informatique des centres de données. L'objectif de la norme est de définir les conditions nécessaires à la réalisation des objectifs de la norme ISO 27001 dans un environnement de centre de données.

La norme EN 50600 est la série de normes EN qui régit la planification, la conception, l'approvisionnement, l'intégration, l'installation, l'exploitation et la maintenance des installations et des infrastructures dans les centres de données. Bien que la série EN 50600 contienne des dispositions similaires aux normes ISO 22237, elles ne sont pas totalement alignées.

La norme EN 50600 est une famille de normes en pleine expansion qui se compose actuellement des éléments suivants :

- EN 50600-1, Concepts généraux
- EN 50600-2-1, Construction de bâtiments
- EN 50600-2-2, Alimentation en énergie et distribution de l'énergie
- EN 50600-2-3. Contrôle environnemental
- EN 50600-2-4, Infrastructure du câblage dédié télécommunications
- EN 50600-2-5, Systèmes de sécurité
- EN 50600-3-1, Informations de gestion et de fonctionnement
- EN 50600-4-1, Vue d'ensemble et exigences générales relatives aux indicateurs-clés de performance
- EN 50600-4-2, Efficacité de l'utilisation de l'énergie
- EN 50600-4-3, Coefficient d'énergie renouvelable

La norme EN 50600 prévoit un système de classification basé sur les critères clés que sont la disponibilité, la sécurité et l'efficacité énergétique :

1. Classe de disponibilité. La classification AC est définie dans les domaines de l'alimentation électrique, des systèmes de ventilation et de climatisation et du câblage ;
2. Classe de protection. La PC est définie pour la prévention des intrusions, la protection contre l'incendie, la protection contre la fumée ainsi que la protection contre les risques environnementaux. Au moins trois classes de protection doivent être constituées ;
3. Niveau de granularité (GL). La capacité de fonctionnement économe en énergie est définie au moyen des qualités et de l'étendue des mesures pour les systèmes de ventilation et de climatisation. La norme distingue trois niveaux de granularité différents ;

Pour que la conception d'un centre de données soit conforme à cette norme :

a. Une analyse des risques pour l'entreprise doit être réalisée ;
b. Une classe AC appropriée est sélectionnée sur la base de l'analyse des risques de l'entreprise ;
c. Un PC approprié pour les chemins et les espaces du centre de données ;
d. Un niveau d'habilitation approprié en matière d'efficacité énergétique (GL) ;
e. Le processus et les principes de conception sont appliqués.

Remarque : actuellement, les centres de données ne tiennent généralement compte ni de la norme EN 50600 ni de la norme ISO 22237. Les centres de données (AWS, ...) sont généralement certifiés par l'institut privé Uptime Institute (Tier Certification) et/ou selon ANSI/TIA-942. Ces deux systèmes de certification sont considérés comme complémentaires.

Certification de niveau de l'Uptime Institute

Cet organisme de certification privé applique ses propres normes de niveau pour la disponibilité et les performances globales des centres de données. Il prévoit différents niveaux de performance qui tiennent compte à la fois de l'environnement bâti ainsi que de l'approche et de la performance de l'équipe d'exploitation. 4 niveaux sont définis :

- Niveau I : Capacité de base : Des arrêts à l'échelle du site sont nécessaires pour des travaux de maintenance ou de réparation. Les pannes de capacité ou de distribution auront un impact sur le site.
- Niveau II : Composants à capacité redondante : Les arrêts de maintenance à l'échelle du site sont toujours nécessaires. Les pannes de capacité peuvent avoir un impact sur le site. Les pannes de distribution auront un impact sur le site.
- Niveau III : Maintenance simultanée : Chaque composant de capacité et chaque chemin de distribution d'un site peuvent être retirés de manière planifiée à des fins de maintenance ou de remplacement sans que cela ait une incidence sur les opérations. Le site reste exposé à une panne d'équipement ou à une erreur de l'opérateur.
- Niveau IV : Tolérance aux pannes : Une défaillance d'un équipement individuel ou une interruption du chemin de distribution n'aura pas d'impact sur les opérations. Un site tolérant aux pannes est également maintenable simultanément.

ANSI/TIA-942 Telecommunications Infrastructure Standard for Data Centers

ANSI/TIA-942 est une norme publiée par la Telecommunications Industry Association (TIA) qui fournit des lignes directrices pour la conception et la construction de centres de données, y compris les systèmes d'alimentation électrique, les systèmes mécaniques, l'architecture, la sécurité, les systèmes de télécommunications, la protection contre les incendies et la sécurité. Cette norme vise à garantir que les centres de données sont fiables, sécurisés et évolutifs pour répondre aux besoins changeants de l'industrie des technologies de l'information.

La norme ANSI/TIA-942 fournit un cadre complet pour la conception des centres de données, y compris des recommandations pour le choix du site, la structure du bâtiment, l'infrastructure de câblage, les systèmes de refroidissement et d'alimentation, la sécurité et la gestion.

Cette norme est utilisée par les concepteurs, les opérateurs et les auditeurs de centres de données pour s'assurer que ces derniers sont conçus et construits conformément aux meilleures pratiques et normes du secteur. La norme est également fréquemment citée en référence par les organismes de réglementation et les clients pour évaluer la fiabilité et la sécurité des centres de données.

System and Organization Controls (SOC) 2

SOC 2 est un ensemble de normes élaborées par l'American Institute of Certified Public Accountants (AICPA) pour évaluer et contrôler la sécurité, la disponibilité, l'intégrité du traitement, la confidentialité et la protection de la vie privée des systèmes et des données d'un organisme de services.

Remarque : alors que la norme ISO/IEC 27001 est générique, la norme SOC 2 est contextualisée pour les centres de données.

Les rapports SOC 2 sont utilisés par les organisations de services (telles que les centres de données) pour démontrer à leurs clients et parties prenantes qu'elles ont mis en place des contrôles internes efficaces pour protéger leurs données sensibles.

Les rapports SOC 2 sont basés sur les Trust Services Criteria (TSC), qui sont un ensemble de principes et de critères utilisés pour évaluer l'efficacité des contrôles d'une organisation de services sur ses systèmes et ses données.

Il existe deux types de rapports SOC 2 : Le type I et le type II. Les rapports de type I évaluent la conception des contrôles d'un organisme de services, tandis que les rapports de type II évaluent l'efficacité de ces contrôles sur une période donnée.

Les audits SOC 2 sont réalisés par des auditeurs tiers indépendants certifiés par l'AICPA.

Les audits SOC 2 sont volontaires, mais ils deviennent de plus en plus importants pour les organismes de services qui souhaitent démontrer leur engagement en matière de sécurité et de protection de la vie privée.

Pour se préparer à un audit SOC 2, les organismes de services doivent procéder à une évaluation des risques et mettre en place un ensemble complet de contrôles pour répondre aux critères des services fiduciaires.

Les audits SOC 2 impliquent généralement une combinaison d'entretiens, d'examens de la documentation et de tests des systèmes afin d'évaluer l'efficacité des contrôles d'un organisme de services.

Les rapports SOC 2 comprennent un avis de l'auditeur sur l'efficacité des contrôles d'un organisme de services ainsi qu'une description des contrôles qui ont été testés et des déficiences identifiées.

Les rapports SOC 2 peuvent être communiqués aux clients, aux parties prenantes et aux organismes de réglementation afin de garantir qu'un organisme de services a mis en œuvre des contrôles efficaces pour protéger les données sensibles.

SOC 3

SOC iii est un type de rapport d'attestation qui fournit une vue d'ensemble des contrôles d'une organisation en matière de sécurité, de disponibilité, d'intégrité du traitement, de confidentialité et de respect de la vie privée.

Contrairement aux rapports SOC 1 et SOC 2, qui sont destinés à un public spécifique et fournissent des informations plus détaillées sur les contrôles d'une organisation, les rapports SOC 3 sont destinés à un public général et fournissent un résumé des contrôles de l'organisation qui peut être partagé publiquement.

Les rapports SOC 3 sont basés sur les mêmes contrôles et critères que les rapports SOC 2 mais ils ne fournissent pas le même niveau de détail. Au lieu de cela, les rapports SOC 3 comprennent une brève description du système et des contrôles de l'organisation ainsi qu'une déclaration d'un auditeur indépendant attestant de la conformité de l'organisation aux critères SOC 2.

Les rapports SOC 3 sont souvent utilisés par les organisations pour démontrer leur engagement en matière de sécurité et de conformité à leurs clients, partenaires et autres parties prenantes. Parce qu'ils sont accessibles au public, ils peuvent également être utilisés par des clients ou des investisseurs potentiels pour évaluer la posture de sécurité d'une organisation avant de faire affaire avec elle.

A2.6. Systèmes de certification

Le Règlement sur la cybersécurité (CSA, (UE) 2019/881) fournit un cadre européen pour la certification de la cybersécurité des produits, des processus et des services. ENISA, l'agence de l'Union européenne pour la cybersécurité, est habilitée à élaborer des schémas de certification de la cybersécurité destinés à être utilisés sur une base volontaire et valables dans l'ensemble de l'Union européenne. Le deuxième schéma concerne les services cloud (EUCS). Il est encore en cours de préparation à la date de rédaction de ce guide. Il devrait utiliser la specification technique CEN/TS 18026 présentée ci-dessus. Lorsqu'il sera disponible, il pourrait devenir un outil utile pour le CSP afin de démontrer la sécurité de sa solution et pour le fournisseur de services SPIS de faire confiance au CSP.

Date de publication : 17 février 2025

Euralarm
Gubelstrasse 22
CH-6301 Zug (Suisse)

Numéro d'enregistrement commercial suisse CHE-222.522.503

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