La sécurité physique (SP) des baies de serveurs est essentielle

Quels sont les points à prendre en compte par l'administrateur IT ?

White Paper

Avril 2021

Auteur : Rashid Niamat

La demande de solutions offrant une sécurité renforcée ne cesse de croître. Cela découle principalement de la législation et de la réglementation mais aussi du fait qu'il faut pouvoir démontrer que l'on maîtrise cette question. Ces règles se chevauchent partiellement ou ne concernent au contraire que certains secteurs. Il existe de très nombreuses prescriptions dont les acheteurs, les installateurs et les administrateurs IT doivent tenir compte. Ce livre blanc de Rittal aborde les principaux aspects de la sécurité physique des baies de serveurs.
Face à la multitude de règles, l'administrateur IT a un peu trop souvent tendance à les négliger.

FRIEDHELM LOH GROUP

Sommaire

Introduction 2
- Présentation de la norme EN 50600 2
- Lien entre EN 50600 et ISO 27001 3
- ISO 27001 et NEN 7510 3
- Bâtiment neuf ou bâtiment existant 4
- Confusion en présence de différents profils de clients 4
- Zoom sur la sécurité physique 4
- L'accès aux baies de serveurs 5
- La qualité des baies de serveurs 5
- La climatisation est aussi une sécurité physique 5
- N'oubliez pas le RGPD 6

Introduction

La sécurité est un concept très vaste. En informatique, l'attention se porte davantage sur la sécurité numérique. En soi, c'est une évolution positive. Il convient en effet d'empêcher des personnes non autorisées d'accéder à des données et des applications numériques. L'augmentation exponentielle des rançongiciels ces dernières années nécessite également une plus grande vigilance et des mesures supplémentaires pour mieux protéger les environnements informatiques.

La vigilance vis-à-vis des données ne peut toutefois pas être considérée comme un domaine bien défini. Les données et les applications sont enregistrées sur des équipements matériels. Ces équipements matériels sont eux-mêmes installés dans une baie de serveurs. En se focalisant davantage sur les données, on risque d'accorder une moindre priorité au contrôle et à la gestion de la baie de serveurs abritant les contenus. Dans ce cas, rien ne dit que l'administrateur ***maîtrise*** tous les aspects.

Avec ce livre blanc, Rittal souhaite attirer l'attention spécifiquement sur la sécurité physique des baies de serveurs. Cette limitation de la portée du livre blanc est délibérée car même ce domaine partiel est déjà soumis à une pléthore de règles et d'exigences. L'objectif de ce document n'est pas d'aborder toutes les règles et prescriptions qui existent. Son but est de montrer au lecteur qu'un domaine numérique robuste n'est possible que si la base physique répond aux exigences de sécurité imposées.

Avant de pouvoir installer la première baie de serveurs, il faut déjà disposer d'une salle qui s'y prête parfaitement. Dans le cas d'une nouvelle construction, il faudra notamment se fier à la norme EN 50600 pour créer un projet tenant compte des multiples aspects de la sécurité physique.

Présentation de la norme EN 50600

Les 10 thèmes majeurs de la norme EN 50600 :

EN50600-1: Concepts généraux en matière de conception et de spécifications
EN 50600-2-1 : Construction des 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

EN 50600[I] est la première norme européenne à présenter des spécifications étendues pour la planification, la construction et l'exploitation d'un centre de données. Elle utilise à cette fin une approche holistique.
Elle définit les exigences pour les critères en termes de construction des bâtiments, de distribution d'énergie, de gestion climatique, de câblage et de systèmes de sécurité et elle spécifie des critères pour le fonctionnement des centres de données.

La norme EN 50600, rédigée par le CENELEC (Comité européen de normalisation en électronique et en électrotechnique), offre différentes possibilités et est dès lors structurée de façon modulaire jusqu'à un certain degré. EN 50600 est en premier lieu une norme qui s'applique aux nouveaux centres de données. Elle définit la nécessité de recourir à des conseils d'experts et des analyses professionnelles pendant la phase de conception et de construction.

Dès sa première version en 2012, la norme EN 50600 s'articule autour de 10 grands thèmes. Ceux-ci ont été repris dans le même ordre dans la nouvelle version v 2.0 du printemps 2020.

Lien entre EN 50600 et ISO 27001

Si la norme EN 50600 est encore relativement peu citée dans les publications, c'est notamment parce qu'elle a principalement un rôle de directive. En outre, c'est un règlement purement européen, qui a dès lors une portée plus limitée que la norme ISO 27001 valable dans le monde entier.

Les exigences et les meilleures pratiques formulées par EN 50600 portent sur la sécurité physique. De ce fait, la norme EN 50600 est à première vue strictement distincte de la norme ISO 27001. Cette norme porte sur le niveau de l'organisation et des processus pour sécuriser des données.

Par ailleurs, la stricte séparation entre EN 50600 et ISO 27001 est une séparation qui n'est pas perçue de la sorte dans la pratique. Pour pouvoir répondre aux exigences fixées par ISO 27001, il faudra en effet pouvoir démontrer le respect de certaines exigences dès la phase de construction. Il existe donc un lien entre les deux normes. Ce lien existe aussi entre EN 50600 et la norme NEN 7510 que nous citons ci-après.

Ce qui vaut pour l'ISO 27001 concerne aussi les organisations qui sont certifiées NEN 7510II. Cette certification, qui est obligatoire pour toute organisation aux Pays-Bas ayant accès à des données médicales, présente de nombreuses analogies avec l'ISO 27001. C'est pour ces raisons que les centres de données ainsi que les fournisseurs gérés disposeront souvent des deux certifications.

ISO 27001 et NEN 7510

Parmi les exigences de l'ISO 27001 et de NEN 7510, il faut aussi pouvoir démontrer de manière argumentée que des mesures ont été prises pour garantir la sécurité des données. Il est important d'assurer une bonne sécurité physique, par exemple la sécurité des accès et la protection contre les menaces de l'extérieur. Mais il faut aussi prévoir des mesures contre les intrusions, la poussière, les infiltrations d'eau ou les vapeurs toxiques. Autrement, on ne maîtrise pas la situation.

https://www.nen.nl/ict/datacenters/en-50600

[II] Pour plus d'informations sur NEN 7510, lisez cet article https://expert.rittal.nl/blog/nen-7510-informatiebeveiliging-gezondheidszorg/

On se renseigne également sur les mesures assurant un meilleur niveau de redondance pour savoir si les dispositions prises en vue de garantir la sécurité des données sont satisfaisantes.

Bâtiment neuf ou bâtiment existant

Pour des centres de données et des centres de calcul dans de nouveaux bâtiments, il est plus simple de démontrer à l'appui d'une norme EN 50600 existante que l'on a tenu compte de tous ces points. Cependant, la plupart des environnements de ce type aux Pays-Bas ne sont pas conçus et construits (modernisés) en utilisant cette norme relativement récente comme fil conducteur.

Dans ces cas-là, il est naturellement toujours possible d'être certifié selon ISO 27001 ou bien selon NEN 5710. Le processus d'audit est un peu différent et requiert probablement plus de temps.

Confusion en présence de différents profils de clients

Il sera encore peu question de confusion à ce stade. Il en ira tout autrement si le centre de données ou le centre de calcul dessert différents groupes de clients qui imposent chacun un catalogue d'exigences et de prescriptions spécifiques. Par conséquent, avec l'ISO 27001, on optera pour un champ d'application très étroit, ou l'on essaiera de le décrire de façon aussi générale que possible.

Ce qui arrive également, c'est que l'on fasse auditer l'environnement séparément pour chaque groupe de clients, en se basant chaque fois sur une norme distincte. Cette approche est parfois inévitable. La norme NEN7510 sert souvent d'exemple. Les salles qui répondent déjà à l'ISO 27001 ne peuvent pas être utilisés pour le stockage de données médicales. Cela nécessite un audit supplémentaire spécifique à NEN 7510. Les organisations qui traitent certaines données financières ou qui y ont accès n'échappent pas à un audit ISA3402 Type 2 et/ou PCI DSS. Il va de soi que de telles situations entraîneront des frais importants. De même, il est inévitable qu'un grand nombre de cadres réglementaires et de directives génère surtout des incertitudes et de la confusion dans le chef des utilisateurs et des administrateurs.

Zoom sur la sécurité physique

Le paragraphe qui précède décrit de façon générale les normes et directives les plus utilisées pour la protection des données. Dans de nombreux cas, il sera question d'un langage technique neutre lorsqu'il s'agit de sécurité physique. Le concept de « mesures appropriées » est une expression que l'on utilise facilement.

Ce que l'on entend précisément par ce terme doit être démontré à chaque fois à l'aide de questionnaires qui se penchent sur les détails de façon très précise. Il faut tenir compte de multiples aspects. Que l'on ait affaire à une salle de serveurs avec une baie de serveurs ou à un centre de données complet, les points suivants doivent être analysés minutieusement.

- Comment l'accès aux baies est-il organisé ?
- Comment le câblage depuis et vers les baies est-il agencé ?
- Comment veille-t-on au bon fonctionnement des équipements matériels dans les baies dans les conditions appropriées ?
- Quelles sont les procédures et les mesures en place pour documenter et consigner tous ces points ?

Accès aux baies de serveurs

Même si cela semble être des questions simples, toute personne concernée sait que les questions complémentaires sont de plus en plus complexes. Si l'on peut démontrer que l'accès à une baie de serveurs est limité par l'usage de verrous, la question complémentaire est de savoir si cela s'applique aussi à la salle où la baie est installée et si l'on a fait attention à la qualité des serrures.

Avec la limitation de l'accès à une baie de serveurs, on répond à une question importante lors de chaque audit. Mais ensuite, il faudra pouvoir démontrer comment cette mesure est contrôlée. C'est cette raison qu'on observe une demande croissante d'outils de surveillance au niveau des baies de serveurs. Ceci peut consister en un système vidéo qui surveille les baies ou toute la salle. La combinaison d'une serrure à cylindre et d'un code personnel pour accéder aux baies ou à la salle est également une pratique courante. Dans ce dernier cas, il faut consigner sous forme électronique à quelle heure un utilisateur a eu accès aux baies ou à la salle de serveurs.

Qualité des baies de serveurs

L'emplacement exact des baies impose des exigences à leur construction. Pour les centres de données, c'est peu souvent le cas mais ailleurs, certaines baies de serveurs doivent être installées dans des environnements humides ou poussiéreux. Leur mise en place dans un tel environnement ne doit pas être une entrave à leur pilotage, à condition de connaître les limitations de ces emplacements et d'avoir pris les mesures appropriées (voir aussi les conditions de NEN 7510). L'edge computing dans l'industrie de transformation, mais aussi les installations de télécommunications sont d'autres exemples de situations où il faut porter une réelle attention au type de baie.

Les environnements extérieurs nécessitent des baies à indice IP[III] élevé. Dans certaines conditions particulières, il peut même s'avérer nécessaire d'abriter la baie de serveurs dans un coffre.

> Le code **IP** *(International Protection Rating, également appelé Indice de Protection)* sur les matériels électriques indique le degré de protection de la construction d'appareils électriques ou électroniques contre un endommagement propre dû à une utilisation dans un « environnement hostile » et contre un éventuel danger pour l'utilisateur.
> Le code IP est normalisé à l'échelle internationale dans la norme CEI 60529. Le code IP comporte deux chiffres : le premier indique le degré de protection contre le contact et la pénétration de corps solides, le second indique le degré de protection contre les liquides.

La climatisation est aussi une sécurité physique

Lorsqu'on parle de la sécurité physique de baies et des données et applications qu'elles renferment, on pense en premier lieu à l'accès aux équipements matériels. Il est clair également que l'alimentation électrique et la connectique nécessitent une protection. La climatisation en revanche est moins souvent évoquée.

Pourtant, la climatisation est un facteur extrêmement important dans la protection des données et des matériels informatiques. La climatisation est d'ailleurs abordée dans la norme EN 50600 2-3. Cela n'a aucun lien direct avec la norme ISO 27001 ou NEN 7510.
C'est surtout qu'en cas de questions sur la robustesse et la redondance des solutions choisies, il faut pouvoir démontrer que des mesures appropriées ont été prises.

Rittal B.V. www.rittal.nl

[III] Cette définition est issue de https://nl.wikipedia.org/wiki/IP-code

Dans ce cadre, on examine l'ensemble des mesures en matière de HVAC. Pour déterminer les mesures sont suffisantes pour garantir la continuité de l'activité, on procède souvent aujourd'hui à une analyse détaillée des systèmes HVAC. C'est notamment pour cette raison que pour des petites installations, on choisit plus souvent des baies de serveurs intégrant d'origine un système HVAC.

N'oubliez pas le RGPD

Au plan technique, il n'y a guère d'obstacles pour aboutir au niveau approprié de sécurité physique. Les salles qui doivent être certifiées n'échappent donc pas non plus à la nécessité de faire des choix.

Mais cela ne dit pas pour autant que cet aspect figure suffisamment en tête de la liste des priorités. Qu'il s'agisse d'un nouveau bâtiment ou d'extensions à des salles de serveurs, il est toujours possible que la sécurité physique soit moins prioritaire. Cela se voit surtout dans les petites organisations. S'intéresser à la sécurité physique est une pratique encore trop peu répandue dans les entreprises qui, depuis des années, s'occupent davantage des données à caractère personnel – et cela représente un très grand groupe.

Toutes ces entreprises ont beaucoup plus affaire à la réglementation qui leur impose implicitement de réfléchir à la sécurité physique. Depuis la mise en place du RGPDIV en 2016, tout le monde doit pouvoir démontrer qu'il « a pris des mesures appropriées » ou qu'il lutte contre la perte et l'usage abusif de données à caractère personnel. Il s'agit en l'occurrence des données de clients et de fournisseurs mais aussi du personnel interne.

Par ce seul fait, chaque entrepreneur est confronté au RGPD. Pour beaucoup d'entrepreneurs, l'informatique est un instrument pour pouvoir mener leurs activités. Réfléchir à la protection de l'informatique est quelque chose de nouveau. Les exigences que le RGPD impose se révèlent larges et vagues. Cela accentue la confusion, surtout quand il s'agit de tenir compte de la notion de « mesures appropriées ».

Aujourd'hui, on réalise de plus en plus qu'il faut porter une grande attention à la sécurité physique de tout l'environnement de travail, y compris pour les matériels informatiques et les baies de serveurs. C'est en effet le fondement indispensable pour garantir une bonne protection des données à caractère personnel.

L'article 32 du RGPD (Règlement Général sur la Protection des Données) spécifie que les entreprises et les autorités doivent mettre en oeuvre les mesures techniques et organisationnelles appropriées pour garantir un traitement sécurisé des données à caractère personnel. L'Autorité de Protection des Données [aux Pays-Bas] précise à ce propos :

- *Les organisations doivent utiliser des techniques modernes pour protéger les données à caractère personnel.*
- *Du reste, elles doivent non seulement se pencher sur la technique mais aussi sur la façon d'assurer le traitement des données à caractère personnel en tant qu'organisation. Par exemple : qui a accès à quelles données ?*

Au travers de cet article, le RGPD impose donc des exigences sur la sécurité physique des environnements informatiques sur lesquels sont stockées des données à caractère personnel.

[iv] Le texte intégral de ce Règlement est disponible sur le site web du régulateur néerlandais https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/verordening_2016_-_679_definitief.pdf

Rittal B.V.
Hengelder 56 · Postbus 246 · 6900 AE ZEVENAAR
Tél. : (0316) 59 16 60 · Fax: (0316) 52 51 45
E-mail : sales@rittal.nl · www.rittal.nl

Pour plus d'informations sur ce thème :
Edgar Hoogakker · Product Manager Climatisation · Courriel : ehoogakker@rittal.nl