Partagé avec
TLP (Traffic Light Protocol) –
VERT

Approuvé

Norme en matière de sécurité physique des centres de données

ID du document : **SEC-08**

À l'attention de: Fédération de l'Alliance

Approuvé le 2024-04-03

Approuvé par le Conseil national de la sécurité (CNS)

1. Introduction

La présente norme définit les exigences de sécurité physique pour les centres de données qui hébergent les Systèmes et services de la Fédération de l'Alliance. Le respect des exigences stipulées dans ce document est essentiel pour protéger les Systèmes et services de la Fédération de l'Alliance contre les menaces de sécurité physique.

2. Définitions

Reportez-vous à SEC-00 Glossaire de la sécurité de l'information.

3. Applicabilité

La présente norme s'applique aux centres de données qui hébergent les Systèmes et services de la Fédération de l'Alliance.

4. Exigences en matière de sécurité physique

4.1 Structure / Enceinte

4.1.1. L'accès du public au périmètre du centre de données devrait être restreint. La signalisation devrait délimiter clairement l'espace accessible au public des zones réservées au personnel autorisé. Un périmètre de sécurité extérieur avec contrôles de l'accès devrait être établi pour empêcher l'accès direct du public.

4.1.2. Le centre de données doit être situé dans une pièce entièrement fermée. Les murs doivent s'étendre du sol à la dalle du plafond et être construits d'un matériau solide

et résistant tels que le béton ou la brique. S'ils ne le sont pas (par exemple, des cloisons sèches), ils doivent être renforcés par un treillis métallique.

4.1.3. Les portes doivent être fermées et verrouillées à tout moment lorsqu'elles ne sont pas utilisées et comporter un mécanisme de sécurité qui permet au personnel de sortir du centre de données en cas de défaillance du système d'accès.

4.1.4. Les portes doivent se fermer automatiquement, à l'exception des portes des quais de chargement.

4.1.5. Du matériel de fixation de qualité sécurité doit être utilisé pour les portes et être construit en métal, y compris le cadre.

4.1.6. Toutes les fenêtres des murs ou des portes du périmètre du centre de données doivent être renforcées. L'installation d'un film de sécurité de haute qualité (Profilon AXA1-15Mil ou supérieur) devrait être envisagée.

4.1.7. Pour les nouvelles constructions, la plomberie (par exemple, pour l'eau potable et le drainage) ne doit pas traverser le plafond du centre de données, autrement des mesures d'atténuation doivent être mises en place (par exemple, déflexion, drains, etc.). Ceci ne s'applique pas aux systèmes de refroidissement spécialement conçus pour l'équipement du centre de données.

4.1.8. Il est considéré comme étant une bonne pratique d'empêcher les interférences électroniques (par exemple, en utilisant des plaques de blindage, des armoires métalliques fermées et mises à la terre, etc.).

4.2 Visibilité et accès à l’équipement

4.2.1. Les racks et armoires du centre de données devraient être verrouillées pour isoler l'équipement à l'intérieur (y compris en restreignant l'accès aux ports USB et autres ports), à moins que le centre de données ne soit dédié exclusivement aux Systèmes et services de la Fédération de l'Alliance.

4.2.2. Des stores ou des revêtements devraient être installés aux fenêtres si nécessaire pour réduire les lignes de visibilité depuis l’extérieur du centre de données pour l’équipement, les écrans et les objets de valeur.

4.3 Câblage électrique et réseau

4.2.3. Tous les câbles réseau pour la transmission des données entre les périphériques du centre de données devraient être physiquement situés à l'intérieur du périmètre du centre de données. Le câblage réseau transportant ces données ou prenant en charge les services d'information qui doivent fonctionner physiquement à l'extérieur

du périmètre du centre de données d'une zone accessible au public doit être protégé de toute interception ou tout dommage.

4.2.4. Les systèmes indispensables devraient être connectés par un système d'alimentation sans interruption (UPS) afin de continuer à fonctionner en cas de coupure de courant de courte durée. Les nouvelles constructions devraient être conçues pour séparer physiquement l'alimentation principale, y compris l'UPS, et l'équipement de données afin d'éviter tout risque de dommage à l'équipement en cas de panne catastrophique des batteries du système d'alimentation.

4.3.1. Il est considéré comme étant une bonne pratique d'installer une alimentation redondante dans le centre de données et d'envisager d'installer des systèmes d'alimentation de secours supplémentaires (par exemple, des générateurs) pour les pannes de plus longue durée, en fonction de la criticité du système.

4.4 Gestion des accès

4.4.1. Les mécanismes d'accès suivants sont privilégiés et devraient être installés : carte/porte-clé électronique d'accès de proximité, serrure d'entrée à clavier et serrure biométrique qui identifient la personne de manière unique.

4.4.2. L'accès au centre de données doit être enregistré électroniquement ou entré dans un journal dans les cas où le mécanisme d'accès n'identifie pas la personne de manière unique.

4.4.3. Les personnes désignées doivent être autorisées à accorder l'accès au centre de données. Un processus de gestion formel doit être établi pour gérer l'accès physique au centre de données, y compris la révocation de l'accès par porte-clé, carte ou clavier.

4.4.4. Les entrepreneurs qui auront accès au centre de données doivent être préautorisés conformément à la section 4.4.3.

4.4.5. Toute personne, y compris les entrepreneurs, qui n'a pas été autorisée à accéder au centre de données doit être accompagné à tout moment par une personne autorisée.

4.4.6. La prise de photos et d'enregistrements vidéo dans un centre de données doivent être préautorisés.

4.5 Contrôle de l'environnement

4.5.1. Des systèmes de chauffage, de ventilation et de climatisation suffisants doivent être en place pour maintenir efficacement tous les systèmes à l'intérieur des plages de température et d'humidité requises par les fabricants.

4.5.2. La température et l'humidité doivent être surveillées, et une alarme déclenchée en cas de dépassement des seuils préétablis.

4.6 Extinction des incendies

4.6.1. Des dispositifs de détection et d'extinction d'incendie doivent être en place, tels que des détecteurs et des extincteurs.
4.6.2. Les systèmes automatisés d'extinction d'incendie doivent tenir compte de la sécurité du personnel du centre de données.

4.7 Surveillance et temps de réponse

4.7.1. Des alarmes de sécurité doivent être mises en place aux points d'accès au périmètre du centre de données (portes, fenêtres) et doivent comprendre des systèmes de détection de mouvement, dans la mesure du possible, pour identifier et alerter en cas d'accès non autorisé.
4.7.2. Les alarmes de sécurité et les alarmes environnementales doivent être surveillées 24 heures sur 24, 7 jours sur 7.
4.7.3. Le temps de réponse pour la sécurité physique (pendant et en dehors des heures ouvrables) doit être inférieur à 60 minutes en cas d'accès physique non autorisé et/ou de danger environnemental.
4.7.4. La surveillance vidéo doit être installée dans le centre de données pour assurer la couverture des actifs et des espaces, et des précautions doivent être prises pour éviter d'enregistrer des informations sensibles ou personnelles. Les enregistrements vidéo doivent être conservés pendant au moins 30 jours et l'accès aux enregistrements doit être restreint conformément à une procédure documentée.

4.8 Équipement et inventaire

4.8.1. Un registre devrait être tenu pour tout équipement entrant et sortant du centre de données.
4.8.2. Un inventaire devrait être tenu pour l’équipement de rechange et pour l’équipement en service.

5. Information connexe

SEC-00 Glossaire de la sécurité de l’information