southco®

Les technologies d'accès au niveau du rack améliorent la sécurité du centre de données

LIVRE BLANC

southco.com

AUTEUR :

Sonny Van Ngo, responsable du développement commercial, Solutions d'accès électronique, Southco, Inc

Les centres de données sont en pleine expansion, en raison de facteurs tels que la demande de bande passante nécessaire pour travailler à domicile, l'essor important des applications de cloud computing et la croissance massive des plateformes de visioconférence. À mesure que le secteur investit dans l'expansion de ses capacités — l'ajout d'étages aux sites existants et la construction de nouvelles installations — les investissements dans la sécurité des données et la sécurisation physique de ces nouvelles installations doivent être une priorité absolue.

Mais ce ne sont pas seulement les centres de données qui connaissent une croissance rapide. Les coûts liés aux violations de données de toutes sortes augmentent aussi rapidement. Le coût moyen d'une violation aux États-Unis s'élève à 9,4M $, selon le rapport « Le coût d'une violation des données » d'IBM Security.[1]

Les acteurs du secteur des centres de données sont fortement incités à investir de manière significative dans la protection de leurs installations contre toutes sortes de risques. La sécurité au niveau du rack reste une vulnérabilité dans certains endroits et constitue l'un des domaines que les principaux centres de données étudient. Il existe désormais des gammes de dispositifs de verrouillage électronique , de dispositifs de contrôle d'accès et de systèmes conçus pour garantir que chaque armoire de serveur et chaque rack devant être sécurisé contre tout accès non autorisé puisse être facilement et entièrement protégé.

Les centres de données d'aujourd'hui contiennent l'infrastructure physique qui alimente notre monde numérique. La protection de ces ressources nécessite plusieurs couches de contrôle d'accès. L'investissement dans des solutions de fermeture et de verrouillage électroniques intelligentes au niveau du rack est de plus en plus important, afin de minimiser les risques et de protéger les données contre le vol grâce à une gamme de loquets électroniques spécialisés qui fournissent un contrôle d'accès basé sur le temps uniquement aux utilisateurs autorisés.

[1] « 4,35 millions USD — le coût moyen global d'une violation de données », 17 octobre 2022, Security (https://www.securitymagazine.com/articles/98486-435-million-the-average-cost-of-a-data-breach#:~:text=The%20global%20average%20cost%20of,of%20a%20Data%20Breach%20Report.%E2%80%9D).

La série de poignées escamotables électroniques H3-EM de Southco offre la flexibilité nécessaire pour s'adapter à toute technologie de lecteur choisie par le propriétaire du rack, dont les lecteurs RFID, PIN et biométriques comme composant intégral du loquet électronique.

Adopter une approche de la sécurité à plusieurs niveaux

Pratiquement tous les centres de données disposent de systèmes et de processus de sécurité bien établis pour gérer et suivre l'accès des techniciens, qu'il s'agissent des équipes qui installent de nouveaux équipements ou effectuent diverses tâches de maintenance. Il existe plusieurs niveaux de sécurité et de contrôle d'accès : à la porte d'entrée du bâtiment, un sas avant le hall d'entrée, puis un contrôle d'accès pour entrer dans chaque salle de centre de données, et enfin une cage en fonction de la structure du centre de données. Tout cela est généralement soutenu par une surveillance vidéo 24/7 sous plusieurs angles.

Cependant, c'est au niveau du rack que la sécurité des données et le contrôle d'accès risquent de ne pas être à la hauteur. Si les serveurs se trouvent derrière des portes, il se peut qu'il n'y ait pas de loquets physiques qui sécurisent ces portes. Et dans les batteries de serveurs plus anciennes, les racks de serveurs sont largement ouverts à tous ceux qui ont pu accéder à la cage qui les entoure.

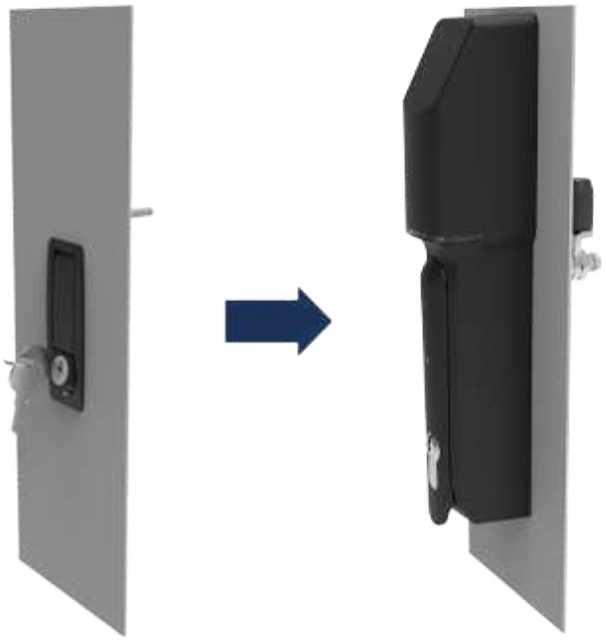
L'impact de telles violations de données peut s'avérer élevé, et n'implique pas seulement les coûts réels mentionnés ci-dessus : les données à caractère personnel sont protégées par de multiples réglementations et normes qui s'appliquent aux opérations du centre de données. La loi HIPPA (Health Insurance Portability and Accountability Act) énonce trois règles de protection des renseignements sur la santé des patients, qui couvrent la confidentialité, la sécurité et la notification des infractions. Le non-respect de ces trois règles, de l'obligation de conformité et des politiques de sécurité, ou toute violation de sécurité des systèmes d'information électroniques, l'accès non autorisé aux dossiers de santé électroniques ou aux informations de santé protégées électroniquement, peuvent entraîner des sanctions civiles et pénales sévères, ainsi qu'une perte de réputation professionnelle.

La norme PCI-DSS (Payment Card Industry Data Security Standard) spécifie que tout accès physique aux données, ou aux systèmes qui hébergent les données des titulaires de carte, ou qui permettent à d'accéder aux données, périphériques, systèmes ou copies papier, et éventuellement de les supprimer, doit être restreint de manière appropriée. De plus, la loi FISMA (Federal information Security Management Act) précise que les entreprises doivent limiter l'accès physique aux systèmes d'information, aux équipements et aux environnements d'exploitation respectifs uniquement aux personnes autorisées.

Gamme d'approches de la sécurité en rack

La responsabilité de la sécurité au niveau du rack peut varier en fonction du type de centre de données. Certains sont entièrement détenus et exploités par une société ou une entité, c'est pourquoi il incombe à une seule organisation de sécuriser les racks et les armoires de serveurs. Dans les centres de données co-localisés, où plusieurs utilisateurs possèdent et exploitent un ou plusieurs racks ou armoires avec de nombreux autres propriétaires/opérateurs, c'est généralement le propriétaire du serveur qui définit la manière de sécuriser ces racks et la sophistication de cette solution de verrouillage et de gestion des accès.

Dans ces conditions, il est important que tous les utilisateurs de centres de données apprécient la



Pour mettre à niveau de manière économique des milliers d'armoires de serveurs en passant du verrouillage mécanique aux loquets électroniques, les kits de rétromontage d'armoire d'équipementiers d'origine de Southco permettent de mettre facilement à niveau les systèmes de verrouillage mécanique existants vers des solutions de verrouillage électroniques en fournissant du matériel conçu pour s'adapter aux configurations de panneaux des principaux fabricants.

gamme d'options disponibles pour assurer la sécurité au niveau du rack. Les fabricants d'armoires passent des mécanismes de verrouillage et de clé traditionnels à des solutions intégrées combinant des fonctions de verrouillage et de surveillance électroniques permettant une sécurité optimale.

Les loquets électroniques sont actionnés par des dispositifs de contrôle d'accès externes qui valident les informations d'identification de l'utilisateur et produisent un signal qui déclenche le cycle de déverrouillage. Les principaux fournisseurs proposent désormais des loquets électroniques modulaires qui peuvent être combinées à n'importe quel dispositif de contrôle d'accès, y compris les pavés tactiles, les cartes d'identification par radiofréquence (RFID), les lecteurs biométriques ou les systèmes Bluetooth® sans fil.

Ces loquets électroniques modulaires ont l'avantage majeur de permettre une mise à niveau relativement facile de la technologie de lecteur au fil du temps. Les systèmes sont conçus pour protéger les investissements des clients dès le départ. Ces systèmes sont conçus pour offrir une installation et des performances efficaces ; ils sont généralement équipés de moteurs à engrenages commandés par microprocesseur qui garantissent une consommation d'énergie minimale et fournissent des capacités de verrouillage et de surveillance intelligentes.

Ces loquets électroniques modulaires peuvent être l'élément clé de la sécurité au niveau du rack. Ils peuvent être modifiés ou adaptés en fonction des exigences uniques de chaque serveur et propriétaire de l'armoire, offrant ainsi une plus grande flexibilité pour s'adapter aux processus de sécurité et de contrôle d'accès d'une entreprise. Les principaux fournisseurs de kits de rétromontage de verrouillage électronique ont également développé plusieurs variantes pour faciliter l'installation de loquets électroniques sur une large gamme de formats et de configurations de portes d'armoire.

En outre, certains propriétaires de centres de données et de serveurs cherchent à augmenter les procédures de sécurité d'accès standard en instaurant une authentification multifactorielle n'accordant pas l'accès avec une seule information. Un loquet électronique peut être conçu pour exiger de l'utilisateur qu'il présente une carte RFID, puis qu'il saisisse un code PIN sur un pavé tactile. Les capacités modulaires de la dernière génération de loquets électroniques peuvent prendre en charge cette capacité.

Avantages des plateformes EAS complètes

Les plateformes EAS permettent aux gestionnaires de centres de données et aux propriétaires de racks d'intégrer facilement un verrouillage intelligent dans l'ensemble de l'installation, de son périmètre à ses serveurs. Pour ce faire, il suffit d'exploiter le système de gestion des bâtiments (BMS) existant du centre de données et de l'intégrer aux nouveaux systèmes électroniques, ou d'utiliser un système distinct entièrement en réseau.

Une solution d'accès électronique est composée de trois composants principaux : un lecteur de contrôle d'accès ou un dispositif de saisie d'information, un loquet électromécanique et un contrôleur de système pour restreinte l'accès, le surveiller et enregistrer son état. Lors de la conception d'une solution d'accès électronique, il est important de choisir le loquet électronique spécifique convenant à l'armoire pour fournir l'intelligence, la flexibilité et la sécurité nécessaires au niveau du rack.

Les plateformes de SAE permettent un contrôle d'accès très spécifique. Par exemple, un technicien reçoit une clé électronique par le biais d'une application sur son smartphone ou sa tablette d'entreprise Bluetooth®. Cette clé n'activera qu'une seule porte d'armoire et seulement pendant une période définie pour lui permettre d'effectuer une tâche d'entretien spécifique.

Chaque fois qu'un loquet électronique est actionné, une « signature » électronique est créée et enregistrée pour surveiller l'accès, soit localement avec des indicateurs visuels ou des alarmes sonores, soit à distance sur un réseau informatique. Ces signatures peuvent être stockées pour créer des pistes d'audit qui affichables à tout moment afin de reconstruire une série d'événements d'accès, en conservant le suivi de l'emplacement, de la date, de l'heure, de la durée d'accès et des informations d'identification spécifiques de l'utilisateur.

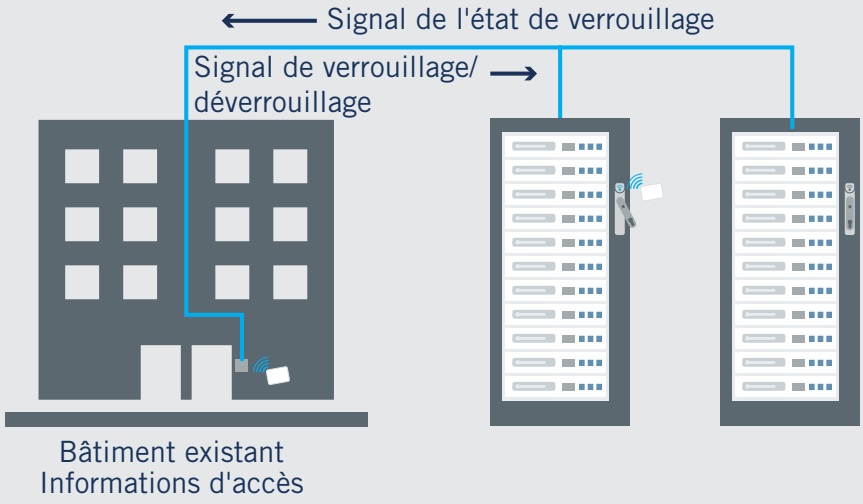
Ces pistes d'audit fournissent aux gestionnaires de centres de données une capacité supplémentaire : elles peuvent suivre l'ouverture d'une porte de rack de serveur afin de surveiller l'activité de maintenance et de service. Si une activité prévue pendant une demi-heure est programmée pour un rack de serveur, mais que la piste d'audit indique que la porte a été ouverte pendant plusieurs heures, la direction peut chercher à savoir pourquoi le retard s'est produit et améliorer la gestion du personnel de service et des coûts de service.

Cette piste d'audit peut également permettre de démontrer la conformité aux réglementations de protection des données, d'identifier et de répondre rapidement aux violations de sécurité ou reconstruire les événements menant à une violation. La gestion à distance et la surveillance en temps réel éliminent le besoin de personnel sur site et réduisent les coûts associés à la gestion de la sécurité du centre des données.

Choisir la solution de sécurité appropriée au niveau du rack

À mesure que l'utilisation et la construction des centres de données augmentent de manière spectaculaire, il existe d'importantes raisons de s'assurer que la protection des données et des applications contenues dans ces centres soit entièrement prise en charge, ce qui implique de prendre des décisions intelligentes quant à la mise en œuvre de la sécurité au niveau du rack.

Il s'agit là d'un défi pour les nouvelles installations et, dans de nombreux cas, pour les centres de données existants qui n'ont pas entièrement investi dans des loquets électroniques et un contrôle d'accès au niveau du rack. Les principaux fournisseurs de systèmes de sécurité ont développé une gamme de plateformes de verrouillage électronique pour les nouvelles installations et les applications de mise à niveau afin de répondre aux exigences et aux processus uniques de chaque utilisateur final. Un partenariat avec ces fournisseurs et leur expertise peuvent aider à trouver la solution de sécurité et d'accès adaptée pour fournir une protection adéquate de l'infrastructure numérique critique au niveau du rack.



La sécurité du centre de données depuis l'entrée de l'installation jusqu'au rack du serveur est assurée par la poignée de verrouillage électronique H3-EM de Southco avec lecteur modulaire et le kit d'intégration du système de sécurité (SSI) à interface Wiegand, offrant des options pour tout niveau d'intégration entre les dispositifs de verrouillage électronique Southco et les systèmes d'accès existants au bâtiment.

À propos de Southco

Southco, Inc. est le concepteur et fabricant leader mondial de solutions d'accès technologiques. De la qualité à la performance en passant par l'esthétique et l'ergonomie, nous comprenons que les premières impressions sont durables en matière de conception de produit. Southco aide depuis plus de 70 ans les plus grandes marques du monde à créer de la valeur pour leur clients grâce à des solutions d'accès innovantes conçues pour améliorer les points de contact avec leurs produits dans des applications de transport et industrielles, ainsi que dans l'équipement médical, les centres de données et bien plus.

Loquets

Fixations

Supports d'écran

Poignées

Charnières

Siège mondial Amérique
Concordville, PA, USA
Tél. : (1) 610 459 4000

Siège Europe
Worcester, RU
Tél. : (44) (0) 1905 346722

Siège Asie-Pacifique
Hong Kong, Chine
Tél. : (852) 3127 1503