SICHERHEITSTECHNIK

Zugangsschutz und physikalische Sicherheit von Serverräumen

Viel zu oft vernachlässigen Unternehmen die physikalische Sicherheit ihrer IT-Anlagen. Sind Brandschutzüberlegungen meist noch abgedeckt, werden auf den Schutz des Rechenzentrums zugeschnittene Massnahmen oft vernachlässigt. Gravierend ist es, wenn Teile der IT durch unzureichende Zutrittskontrollen gestohlen oder beschädigt werden. Wie IT-Verantwortliche systematisch physikalische Sicherheit in Verbindung mit Zugangskontrollmassnahmen etablieren, zeigt dieser Beitrag.

Text: Thomas Gronenwald, Bilder: Redaktion

Eines der komplexesten Themengebiete im Bereich der IT-Sicherheit ist der physische Schutz. Gleichwohl ist dies eine der unterschätztesten Sicherheitsaufgaben. Sehr viele Unternehmen ergreifen konkrete technische Massnahmen zur Absicherung vor Viren und sonstigem Schadcode oder dem Hacker-Angriff von aussen. Vernachlässigt wird dabei immer wieder, das eigene Rechenzentrum gegen einschlägige Gefahren zu wappnen. Besonders schwierig kann es bei einem Einbruch oder Schadenfall werden, wenn die Daten nicht zusätzlich extern gesichert sind. Je nach Grösse und Bedeutsamkeit des Rechenzentrums gilt es die verschiedenen Gefahrenpotenziale zu beurteilen und entsprechend zu behandeln. In diesem Artikel behandeln wir die wichtigsten Aspekte: >

Einbruchhemmende Türen und Fenster mit entsprechenden Widerstandsklassen bieten eine hohe physikalische Sicherheit, vorausgesetzt, sie sind geschlossen und verriegelt.
Les portes et fenêtres anti-effraction présentant des classes de résistance adéquates offrent une sécurité physique élevée, à condition qu'elles soient fermées et verrouillées.

Das Fachregelwerk Metallbauerhandwerk – Konstruktionstechnik enthält im Kap. 2.3.1 wichtige Informationen zum Thema «Metalltüren».

TECHNIQUE DE SÉCURITÉ

Protection des accès et sécurité physique des salles de serveurs

Les entreprises négligent beaucoup trop souvent la sécurité physique de leurs installations informatiques. Si elles tiennent généralement compte de la protection incendie, elles négligent souvent de prendre des mesures appropriées pour protéger leur centre informatique. Les conséquences peuvent être graves si des parties de l'infrastructure IT sont volées ou endommagées en raison de contrôles d'accès insuffisants. Cet article explique comment les responsables IT peuvent mettre en place de manière systématique une sécurité physique associée à des mesures de contrôle d'accès.

La protection physique est l'un des aspects les plus complexes de la sécurité informatique. Pourtant, c'est aussi l'un des plus sous-estimés. De très nombreuses entreprises prennent des mesures techniques concrètes pour se protéger des virus et autres codes malveillants ou pour se prémunir contre les attaques de pirates. Mais elles négligent très souvent d'armer leur propre centre informatique contre les dangers qui le menacent. Un cambriolage ou un sinistre peut s'avérer particulièrement nocif si les données n'ont pas été sécurisées par une sauvegarde externe. Il convient d'évaluer les différents potentiels de risques et d'agir en fonction de la taille et de l'importance du centre informatique. >

Was die physikalische Sicherheit von Serverräumen betrifft, sollten Sie nach dem Motto «Vertrauen ist gut, Kontrolle ist notwendig» verfahren.
En matière de sécurisation physique de salles de serveurs, appliquez toujours le principe suivant : « La confiance, c'est bien ; le contrôle, c'est nécessaire. ».

>

Verwendung von Sicherheitstüren und -fenstern

Die Kombination verschiedener Massnahmen stellt einen effektiven Schutz gegen Einbruch in das Unternehmen (und damit das Rechenzentrum) dar. Beispielsweise sind dies einbruchhemmende Türen und Fenster (mit entsprechenden Widerstandsklassen), Rollladensicherungen bei einstiegsgefährdeten Türen oder Fenstern, besondere Schliesszylinder, Zusatzschlösser und Riegel, Sicherung von Kellerlichtschächten, Verschluss von nicht benutzten Nebeneingängen oder einbruchgesicherte Notausgänge. Auch den Einsatz eines Zugangskontrollsystems sollten Sie prüfen.

Die Normen SN EN 1627 und SN EN 356 legen die jeweiligen Widerstandsklassen von RC 1 bis RC 6 – auch in Kombination mit Glas – fest. Generell sollten Sie in einem Serverraum oder Rechenzentrum den Einsatz entsprechender – nach Möglichkeit geprüfter - Türen und Fenster nicht nur erwägen, sondern zwingend in die Realität umsetzen. Obwohl es als Selbstverständlichkeit erscheint, sollten Sie zudem eine konkrete Regelung dazu finden, Fenster und Türen stets geschlossen zu halten.

Gefahrenmeldeanlage

Eine Gefahrenmeldeanlage ist ein komplexes Gesamtsystem bestehend aus zahlreichen Komponenten. Eine solche Anlage sollte jede Form der Gefahr melden können (Wasser, Feuer,

> Cet article aborde les aspects les plus importants.

Utilisation de portes et de fenêtres de sécurité

Combiner différentes mesures représente une protection efficace contre le cambriolage de l'entreprise (et, par conséquent, celui du centre informatique). Parmi ces mesures, on retrouve p. ex. l'ajout de portes et fenêtres anti-effraction (avec les classes de résistance adéquates), de volets roulants pour assurer la protection des portes ou fenêtres fracturables, de cylindres de serrure particuliers, de serrures additionnelles et de verrous, de protections de soupiraux, d'obturations d'entrées annexes inutilisées ou de sorties de secours protégées contre l'effraction. Vous devriez aussi envisager l'utilisation d'un système de contrôle d'accès.

Les normes SN EN 1627 et SN EN 356 déterminent les différentes classes de résistance de RC 1 à RC 6, y compris en combinaison avec du verre. De manière générale, le placement de portes et fenêtres certifiées dans une salle de serveurs ou un centre informatique ne doit pas rester une idée vague. Vous devez impérativement la concrétiser. Cela semble aller de soi, mais vous devriez aussi trouver une règle concrète pour maintenir les portes et fenêtres fermées en permanence.

Système avertisseur de danger

Un système avertisseur de danger est une installation complexe qui compte de nombreux composants. Une telle installation doit pouvoir signaler toute forme de danger (eau, feu, fumée, température, effraction). De nombreuses solutions techniques existent. Mais le principal défi, c'est d'alerter et de réagir de manière appropriée face à de tels incidents. Il convient de prendre des mesures organisationnelles et, éventuellement, de planifier le travail des équipes en fonction.

Comparaison des méthodes de contrôle d'accès

Un centre informatique représente en général une unité fonctionnelle clé pour l'entreprise avec des exigences de protection particulières. Mais le bâtiment, les bureaux et les autres parties de bâtiments qui font partie des équipements doivent aussi être protégés contre l'accès non autorisé. Pour mettre en œuvre des mesures de protection appropriées, il convient de définir en amont des règles appro-

Rauch, Temperatur, Einbruch). Technisch existieren viele Lösungen dafür. Jedoch ist die Hauptherausforderung die entsprechende Meldung und Reaktion auf solche Vorfälle. Diesen Ablauf sollten Sie organisatorisch regeln und eventuell entsprechende Schichtpläne erstellen.

Zutrittskontrollverfahren im Vergleich

Ein Rechenzentrum stellt in der Regel für das Unternehmen eine wichtige und zentrale Funktionseinheit mit besonderen Schutzanforderungen dar. Aber auch das Gebäude, die Büros und sonstige zur Einrichtungen gehörende Gebäudeteile sollten vor unbefugtem Zutritt geschützt werden. Um geeignete Schutzmassnahmen umsetzen zu können, sollten Sie >

priées sur l'octroi des droits d'accès, la réglementation des accès ainsi que le contrôle de ceux-ci. Sur la base de ces réglementations, vous devriez ensuite mettre en place une protection d'accès efficace avec des mesures appropriées.

Mais avant d'envisager des mesures techniques, analysez rigoureusement l'environnement dans le but de recenser et d'évaluer tous les accès à prendre en compte (portes, portails, ascenseurs, etc.). Par un contrôle d'accès, vous vous assurez que seul le personnel autorisé par vous peut accéder aux zones de sécurité définies par vos soins. Il s'agit d'enregistrer au moins la date et l'heure d'accès ainsi que l'heure à laquelle un collaborateur quitte la zone de sécurité.

La plupart des contrôles d'accès dans les zones de bâtiments où le besoin de protection est faible peuvent être assurés sur la base du critère de « possession » ou de « connaissance », ce qui se fait généralement au moyen de cartes à puce ou de codes PIN. Pour les accès aux zones de sécurité sensibles telles que le centre informatique ou la salle de serveurs, vous devez recourir à >

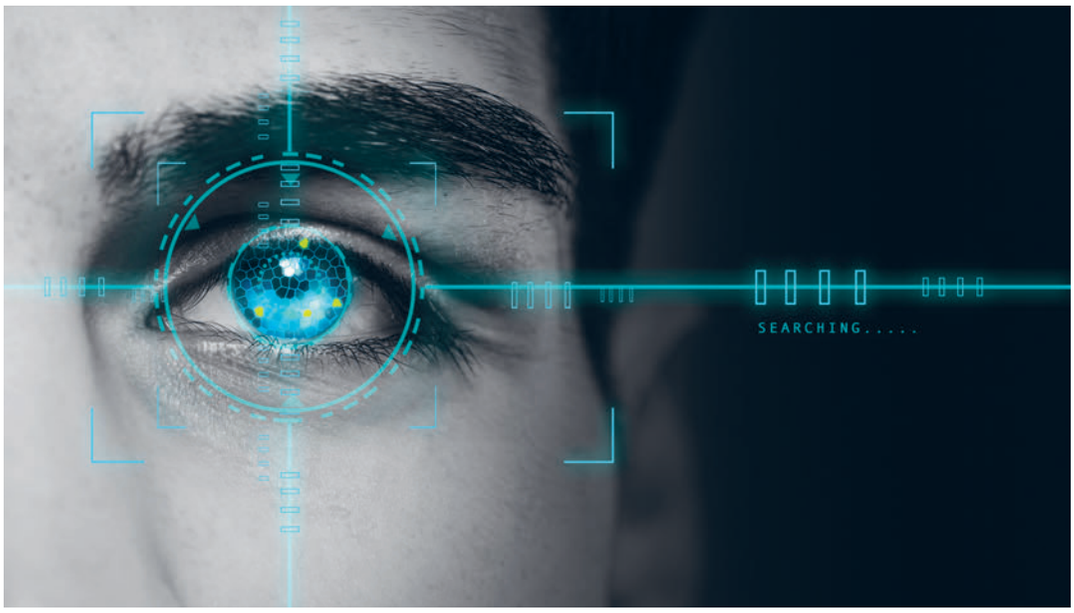
> im Vorfeld geeignete Regelungen über die Vergabe von Zutrittsberechtigungen und der Zutrittsregelung sowie der Kontrolle dieser treffen. Basierend auf diesen Regelungen sollten Sie dann mit entsprechenden Massnahmen einen geeigneten Zugriffsschutz etablieren. Bevor Sie jedoch über technische Massnahmen nachdenken, führen Sie eine geeignete und grundsolide Umfeldanalyse durch. Ziel hierbei ist es, alle zu betrachtenden Zugänge (Türen, Tore, Aufzüge ect.) zu erfassen und zu bewerten. Durch eine Zutrittskontrolle stellen Sie sicher, dass nur das von Ihnen autorisierte Personal Zutritt zu den von Ihnen definierten Sicherheitsbereichen erhalten. Dafür sollten Sie mindestens das Datum und die Uhrzeit des Zutritts sowie des Verlassens eines Sicherheitsbereiches durch einen Mitarbeiter dokumentieren. Die Zutrittskontrolle in Gebäudebereichen mit niedrigerem Schutzbedarf können Sie zumeist mit einem der beiden Kriterien «Besitz» oder «Wissen» sicherstellen. Hierbei kommen in der Regel entsprechende Smartcards oder PIN-Codes zum Einsatz. Für Zutritte in sensible Sicherheitsbereiche wie etwa das Rechenzentrum oder den Serverraum sollten Sie auf zusätzliche Authentifizierungsmechanismen zurückgreifen.

Zugangsschutz und physikalische Sicherheit von Serverräumen

Heutige Schliesssysteme werden in mechanische und mechatronische Systeme unterteilt. Bei einem mechanischen Schliesssystem ist nicht nur der Zylinder, sondern auch die eigentliche Schliessbewegung mechanisch. Anders verhält es sich bei mechatronischen Schliesssystemen. Hierbei werden die Vorzüge von mechanischen Schliessanlagen mit einer elektrischen Zutrittskontrolle gepaart. Die eigentliche mechanische Zylinderbewegung wird durch elektrische Impulse und ein elektronisches Schloss betätigt. Mechanische Schliessanlagen bilden nach wie vor die Grundlage für ein wirkungsvolles Sicherungskonzept. Gute Schliessanlagen bieten aufgrund der immer weiterentwickelten eingesetzten Materialien und Mechanismen einen hohen Widerstand gegen unbefugten Zutritt. Entscheidendes Merkmal bei Schliessanlagen ist, dass nicht alle Schlüssel alle Schlösser schliessen. Diese Schliessberechtigungen beziehungsweise Schliesskombinationen werden bei der Erstellung des sogenannten Schlüssel- und Schliessplans festgelegt. Ein wesentlicher Nachteil ist jedoch, dass der Verlust eines Schlüssels ein erhöhtes Sicherheitsrisiko birgt. Schlimmstenfalls muss beim Verlust eines Schlüssels die komplette Schliessanlage erneuert werden. Wer den Schlüssel besitzt, ob befugt oder unbefugt, erhält Zugriff zu sämtlichen derart gesicherten Räumlichkeiten. Mechatronische Schliessverfahren (oder auch: intelligente Schliesstechnik) stellen eine Symbiose aus bewährter Technik und moderner Elektronik dar. Mechatronische Systeme verwenden anstatt eines herkömmlichen Schlüssels elektronische Komponenten wie beispielsweise ein Zahlenschloss oder eine Magnetstreifenkarte. Sie bieten aufgrund ihrer Programmierbarkeit eine wesentlich höhere Flexibilität als herkömmliche Schliesssysteme.

Biometrie bietet hohe Sicherheit

Zutrittskontrollsysteme auf Basis biometrischer Merkmale erfassen als Identifikationsmerkmal individuelle körperliche Merkmale. Dies bietet den Vorteil, dass das Identifikationsmittel



Verschiedene Systeme eignen sich für die Regelung der Zutrittsberechtigung. Eines der Iriserkennung ist die präziseste, berührungslose und komfortable Biometrielösung für die schnelle Authentifizierung und positive Identifizierung.
Différents systèmes conviennent pour réglementer les droits d'accès. La reconnaissance de l'iris est la solution biométrique sans contact et confortable la plus précise pour l'authentification rapide et l'identification positive.

> des mécanismes d'authentification supplémentaires.

Protection des accès et sécurité physique des salles de serveurs

Les systèmes de fermeture actuels sont des systèmes mécaniques ou mécatroniques. Dans le cas d'un système de fermeture mécanique, le cylindre est mécanique, mais aussi le mouvement de fermeture proprement dit. Il en va différemment des systèmes de fermeture mécatroniques, qui associent les avantages des systèmes de fermeture mécaniques à un contrôle d'accès électrique. Le mouvement du cylindre purement mécanique est actionné par des impulsions électriques et une serrure électronique. Les systèmes de fermeture mécaniques restent à la base d'un concept de protection efficace. En raison des matériaux et mécanismes en constante évolution, les bons systèmes de fermeture offrent une résistance élevée contre l'accès non autorisé. Une caractéristique déterminante des systèmes de fermeture est que toutes les clés ne peuvent pas fermer toutes les serrures. Ces autorisations de fermeture ou combinaisons de fermeture sont décidées lors de la création du plan de clés et de fermeture. Cependant, il reste un inconvénient majeur : la perte d'une clé suscite un risque plus élevé pour la sécurité. Dans le pire des cas, la perte d'une clé demande de remplacer l'ensemble du système de fermeture. La personne en possession de la clé, qu'elle en ait le droit ou non, a accès à l'ensemble des locaux sécurisés de la sorte. Les procédés de fermeture mécatroniques (ou système de fermeture intelligent) associent technique éprouvée et électronique moderne. Les systèmes mécatroniques font appel à des composants électroniques comme p. ex. une serrure à combinaison ou une carte à piste magnétique à la place d'une clé traditionnelle. Programmables, ils sont nettement plus flexibles que les systèmes de fermeture traditionnels.

La biométrie, une sécurité élevée

Les systèmes d'accès basés sur des caractéristiques biométriques identifient les individus sur la base de caractéristiques corporelles propres à

nicht verloren oder gestohlen oder wie eine PIN vergessen werden kann. Dabei lassen sich verschiedene Merkmale des Menschen für eine Identifizierung nutzen: Fingerabdruck, Handgeometrie, Gesichtserkennung, Stimmerkennung, Iriserkennung und Retinaerkennung. Bei der Identifikation eines der oben genannten Merkmale werden folgenden Anforderungen gestellt:

Um Personen anhand eines biometrischen Merkmals identifizieren zu können, ist eine initiale Vermessung des Merkmals notwendig. Hierzu wird ein sogenanntes Template oder ein Referenzdatensatz erstellt, anhand dessen das Merkmal zukünftig verglichen wird. Wichtig hierbei ist natürlich, dass dieser Datensatz sorgfältig gesichert und vor Missbrauch geschützt werden muss. Eine Änderung eines biometrischen Merkmals ist, anders als bei einem herkömmlichen Passwort, nicht möglich. Typische Anwendungsbereiche für biometrische Identifikationsverfahren sind Autorisierungen am Endgerät per Fingerabdruck oder Gesichts- und Iriserkennung zur Zutrittssicherung von Sicherheitsbereichen wie beispielsweise Rechenzentren.

Quelle: it-administrator.de ■

Mechatronische Systeme lassen sich auf einfache Weise ansteuern und verwalten.

Les systèmes mécatroniques se pilotent et se gèrent aisément.

chacun. Ils ont l'avantage d'éliminer tout risque de perte ou de vol du moyen d'identification. Et plus de risque d'oublier un code comme c'est le cas avec un code PIN. Diverses caractéristiques corporelles peuvent être utilisées pour l'identification : empreinte digitale, géométrie de la main, reconnaissance faciale, vocale, de l'iris et rétinienne. L'identification d'une personne à l'aide de l'une des caractéristiques ci-dessus exige l'enregistrement préalable de cette caractéristique ainsi que la création d'un modèle ou d'un jeu de données de référence afin de pouvoir effectuer une comparaison. Il convient évidemment de protéger soigneusement ce jeu de données contre les abus. Contrairement à un mot de passe traditionnel, il n'est pas possible de modifier une caractéristique biométrique. Les procédures d'identification biométriques sont typiquement utilisées pour les autorisations au terminal par empreinte digitale ou reconnaissance faciale et de l'iris afin de protéger l'accès à des zones de sécurité telles que des centres informatiques. ■