

Physikalische Sicherheit in betriebskritischen Anlagen

Suzanne Niles

White Paper Nr. 82

APC[®]
Legendary Reliability[®]

Zusammenfassung

Physikalische Sicherheit, d. h. die Zugangskontrolle der Mitarbeiter zu Anlagen, ist von entscheidender Bedeutung für die Erreichbarkeit von Verfügbarkeitszielen im Datacenter. Durch die breitere Verfügbarkeit von neuen Technologien, wie die biometrische Identifikation und die Fernverwaltung von Sicherheitsdaten, wird die herkömmliche Karten- und Überwachungssicherheit zunehmend durch Sicherheitssysteme ersetzt, die eine zuverlässige Identifizierung und Verfolgung der menschlichen Aktivitäten in einem Datacenter und seiner Umgebung bieten können. Bevor IT-Manager jedoch in Geräte investieren, sollten die konkreten Sicherheitsanforderungen sorgfältig analysiert und die am besten geeigneten und kosteneffizientesten Sicherheitsmaßnahmen für ihre Anlage bestimmt werden. Dieses Dokument gibt einen Überblick über die Grundsätze der Mitarbeiteridentifikation und beschreibt die grundlegenden Elemente und Verfahren, die in Sicherheitssystemen verwendet werden.

Einführung

Der Faktor Mensch: Ein Risiko, das es zu steuern gilt

Wenn über Datacenter-Sicherheit gesprochen wird, kommt einem vermutlich zunächst der Schutz vor Sabotage, Spionage oder Datendiebstahl in den Sinn. Es liegt zwar auf der Hand, dass Schutzmaßnahmen gegen unbefugtes Eindringen und den vorsätzlichen Schaden, der dadurch verursacht werden kann, erforderlich sind. Jedoch stellen die normalen Aktivitäten der Mitarbeiter im Datacenter für die meisten Anlagen tagtäglich ein größeres Risiko dar.

Menschen sind für den Betrieb eines Datacenters wichtig. Untersuchungen zeigen jedoch durchgehend, dass sie für 60 Prozent der Ausfallzeiten im Datacenter direkt verantwortlich sind, und zwar durch Versehen und Fehler, wie z. B. falsche Vorgehensweisen, falsche Gerätekennzeichnungen, Fallenlassen von Gegenständen oder Verschütten von Flüssigkeiten, falsche Befehlseingaben und andere unvorhersehbare kleine und große Missgeschicke. Da menschliches Versagen bei der Anwesenheit von Menschen nicht vermieden werden kann, ist die Minimierung und Steuerung des Mitarbeiterzugangs zu Anlagen ein wesentliches Element des Risiko-Managements, selbst wenn es kaum Bedenken im Hinblick auf böswillige Aktivitäten gibt.

Die Identifikationstechnologie ändert sich mit der gleichen Geschwindigkeit wie die Anlagen, Informationen und Verbindungen, die sie schützen soll. Da ständig neue Systeme und Verfahren auf den Markt kommen, kann leicht vergessen werden, dass das alte Problem, das mithilfe dieser Technologien gelöst werden soll, weder technisch noch kompliziert ist: Das Fernhalten unbefugter oder böswilliger Personen von Orten, an denen sie nichts zu suchen haben. Zwar mag der erste Schritt, d. h. die Festlegung der sicheren Bereiche der Anlage und die Definition von Zugangsrichtlinien, einen komplexen Entwurf ergeben, doch der Instinkt lässt einen dabei nicht im Stich, denn IT-Manager wissen in der Regel, wer wozu Zugang haben sollte. Die Herausforderung liegt im zweiten Schritt: zu entscheiden, wie unvollkommene Technologien zur Umsetzung dieses Plans optimal genutzt werden können.

Physikalische Infrastruktur für hochverfügbare Netzwerke

Die physikalische Sicherheit ist Bestandteil der *physikalischen Infrastruktur für hochverfügbare Netzwerke* (NCPI), da sie eine direkte Rolle bei der Maximierung der Systemverfügbarkeit (der „verfügbaren Betriebszeit“) spielt. Dies geschieht durch die Reduzierung der Ausfallzeiten aufgrund von Unfällen oder Sabotage durch die Anwesenheit nicht erforderlicher oder böswilliger Personen.

Weitere NCPI-Elemente sind Stromversorgungs- und Kühlsysteme, Racks, Verkabelungen und Brandlöschsysteme.

Wer sind Sie, und warum sind Sie hier?

Neue Sicherheitstechnologien, wie Fingerabdruck- und Handscans, Augenscans, Smart Cards und Gesichtsgeometrie, mögen zwar exotisch und schwer verständlich erscheinen, das zugrunde liegende Sicherheitsziel jedoch, das unverändert geblieben ist, seit Menschen etwas besitzen, das sie schützen wollen, ist unkompliziert und jedem von uns vertraut: Wir möchten eine zuverlässige Antwort auf die Frage erhalten: „Wer sind Sie, und warum sind Sie hier?“

Die erste Frage, „Wer sind Sie?“, verursacht die meisten Probleme bei der Planung automatisierter Sicherheitssysteme. Aktuelle Technologien setzen unterschiedliche Mittel zur Identitätserkennung ein, mit einem unterschiedlichen Maß an Sicherheit und zu entsprechend unterschiedlichen Kosten. Eine Magnetstreifenkarte ist beispielsweise nicht teuer, bietet jedoch keine sichere Identitätserkennung (es ist nicht sicher, wer die Karte nutzt). Ein Irisscanner dagegen ist sehr teuer, bietet jedoch eine sehr sichere Identitätserkennung. Einen akzeptablen Kompromiss zwischen Erkennungssicherheit und Kosten zu finden, steht im Mittelpunkt der Planung von Sicherheitssystemen.

Die Antwort auf die zweite Frage, „Warum sind Sie hier?“ oder mit anderen Worten: „Was haben Sie an diesem Zugangspunkt zu suchen?“, ist vielleicht implizit, nachdem die Identität festgestellt wurde („Das ist Frau Alice Wilson, unsere Verkabelungsexpertin, sie arbeitet an der Verkabelung. Lassen Sie sie herein“), oder sie kann auf viele unterschiedliche Arten erfolgen: Das „Wer“ und „Warum“ einer Person kann kombiniert werden. Über die Informationen auf dem Magnetstreifen einer Magnetstreifenkarte könnte beispielsweise die Identität einer Person Informationen in einer Computerdatei mit einer Liste der Zugangsberechtigten abrufen, oder es könnten unterschiedliche Zugangsmethoden zu verschiedenen Teilen der Anlage vorgesehen werden, die den Zugang für unterschiedliche Zwecke ermöglichen. Manchmal ist nur die Frage „Warum sind Sie hier?“ relevant, und die Frage „Wer sind Sie?“ spielt keine Rolle, wie beispielsweise bei Reparatur- oder Reinigungskräften.

Kombination von Fachwissen für die Lösungsfindung

IT-Manager wissen über das „Wer und Warum“ in Verbindung mit der Sicherheit ihrer Einrichtung Bescheid. Sie sind jedoch mit den Einzelheiten der aktuellen Methoden oder Verfahren möglicherweise nicht vertraut genug, um sie anwenden zu können, und dies sollten sie auch nicht sein müssen. Sie wissen aber um ihre Budgetbeschränkungen und kennen die Risiken, die die verschiedenen Arten von Sicherheitsverletzungen in ihrer Anlage in sich bergen.

Ein Berater für Sicherheitssysteme wiederum ist zwar mit den Besonderheiten der Anlage nicht vertraut, er kennt jedoch die Funktionen, Nachteile und Kosten der aktuellen Methoden. Darüber hinaus verfügt er über Erfahrung durch die Planung von anderen Sicherheitssystemen und kann dazu beitragen, die auf dem „Wer und Warum“ basierenden Anforderungen zu klären, zu verbessern oder zu vereinfachen, indem er die richtigen Fragen stellt.

Mit diesem kombinierten Fachwissen kann ein System geplant werden, bei dem Zugriffsanforderungen, akzeptables Risiko, verfügbare Methoden und Budgetbeschränkungen in einem ausgewogenen Verhältnis zueinander stehen.

Definition des Problems

Sichere Bereiche: Was muss geschützt werden?

Der erste Schritt bei der Ausarbeitung eines Sicherheitsplans besteht darin, einen Lageplan der Anlage zu zeichnen und die Bereiche und Zugangspunkte zu bestimmen, für die unterschiedliche Zugangsrichtlinien oder **Sicherheitsstufen** erforderlich sind.

Folgende Bereiche können konzentrische Grenzen haben:

- Standort
- Gebäude
- Computerbereich
- Computerräume
- Geräteracks

Folgende Bereiche können nebeneinander liegende Grenzen haben:

- Besucherbereiche
- Büros
- Betriebsräume

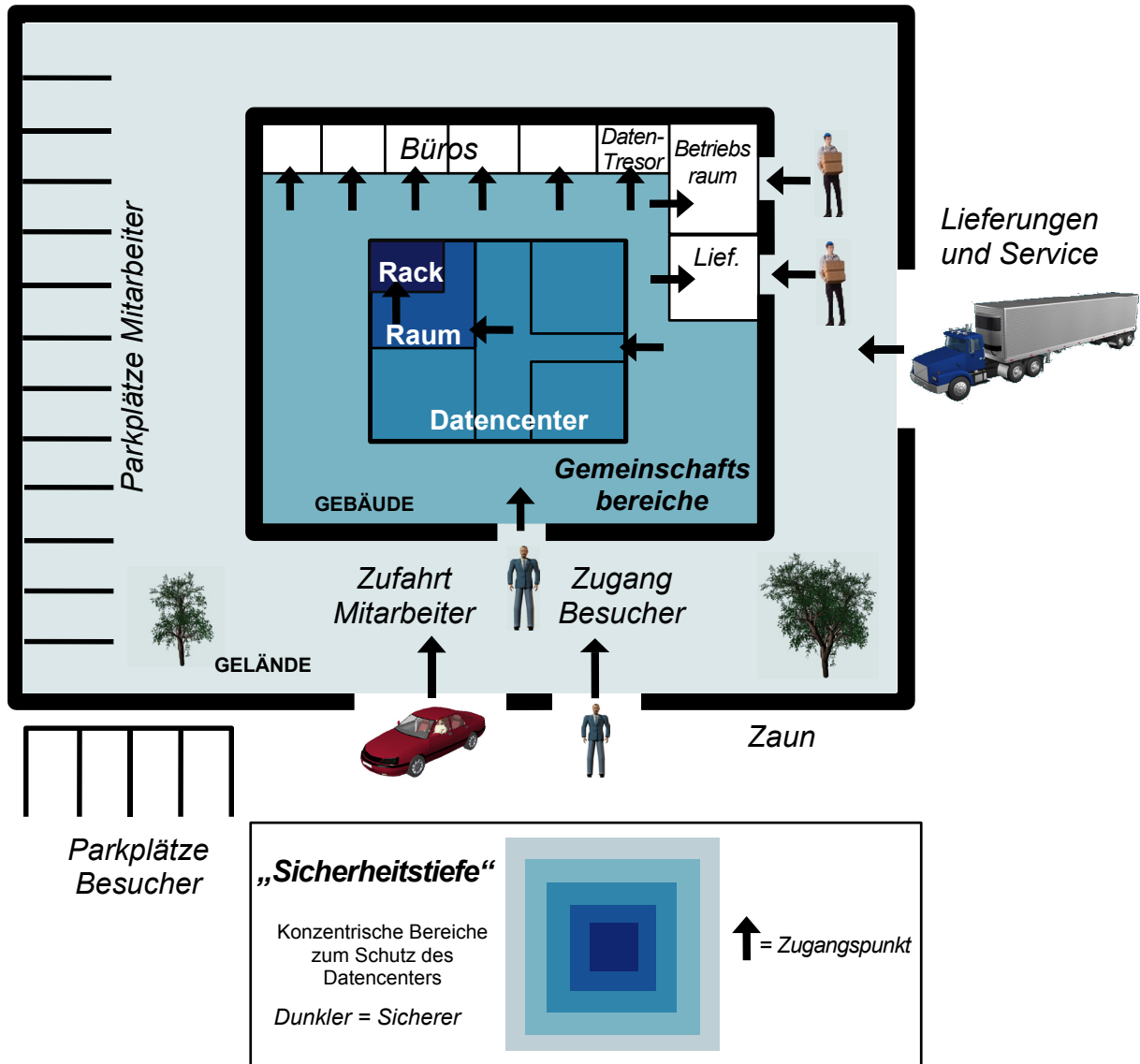
„Physikalische Sicherheit“ kann auch bedeuten...

Physikalische Sicherheit kann sich auch auf den Schutz vor Schäden durch Katastrophen (Feuer, Überschwemmung, Erdbeben, Bombenangriffe) oder Netzstörungen (Stromausfall, Ausfall des Klima- und Lüftungssystems) beziehen.

Hier bezieht sie sich nur auf den Schutz gegen unbefugtes Eindringen von Personen in eine Anlage.

Für Bereiche mit konzentrischen Grenzen können unterschiedliche oder immer strenger werdende Zugangsmethoden gelten, die zusätzlichen Schutz bieten, der auch als **Sicherheitstiefe** bezeichnet wird. Sicherheitstiefe bedeutet, dass ein innerer Bereich nicht nur durch seine eigenen Zugangsmethoden geschützt wird, sondern auch durch die Zugangsmethoden der ihn umschließenden Bereiche. Außerdem kann jeder Sicherheitsverletzung an einem der äußeren Bereiche durch eine strengere Zugangskontrolle an einem der weiter innen liegenden Bereiche entschärft werden.

Abbildung 1 – Lageplan mit Darstellung der „Sicherheitstiefe“



Sicherheit auf Rack-Ebene Das Rack stellt den innersten und sichersten Bereich dar. Rack-Schlösser werden (noch) nicht allgemein verwendet. Wenn sie jedoch verwendet werden, sind sie die letzte Bastion gegen unbefugten Zugang zu wichtigen Komponenten. Es wäre ungewöhnlich, dass jemand in einem Raum voller Racks Zugang zu jedem Rack haben muss. Durch Rack-Schlösser kann sichergestellt werden, dass Server-Verantwortliche nur Zugang zu Servern haben, Telekommunikationsexperten nur Zugang zu Telekommunikationsgeräten usw. „Verwaltbare“ Rack-Schlösser, die remote konfiguriert werden können, um bei Bedarf bestimmten Personen zu bestimmten Zeiten den Zugang zu ermöglichen, reduzieren das Risiko von Unfällen, Sabotage oder der nicht autorisierten Installation zusätzlicher Komponenten, die einen potenziell schädlichen Anstieg des Stromverbrauchs und der Rack-Temperatur verursachen können.

Sicherheit der Infrastruktur Es ist wichtig, in den Lageplan nicht nur die Bereiche aufzunehmen, die die funktionellen IT-Systeme der Anlage enthalten, sondern auch die Bereiche, die Elemente der physikalischen Infrastruktur enthalten, deren Gefährdung einen Ausfall bewirken könnte. Zum Beispiel könnten Klima- und Lüftungssysteme absichtlich abgeschaltet werden, die Generator-Startbatterien könnten gestohlen werden, oder Befehle zur Aktivierung der Sprinkleranlage könnten über eine Systemmanagementkonsole eingegeben werden.

Zugangskriterien: Wer hat wo Zugang?

Die Befugnis einer Person zum Zugang zu einem sicheren Bereich kann auf verschiedenen Kriterien basieren. Neben den üblichen, wie Identität und Zweck, die nachstehend als Erstes angeführt werden, kann es weitere Kategorien geben, die eine besondere Behandlung erfordern, wie beispielsweise ein „dringender Informationsbedarf“.

Persönliche Identität Bestimmte Personen, die in der Anlage bekannt sind, benötigen Zugang zu den für ihre Position relevanten Bereichen. Der Sicherheitsleiter beispielsweise benötigt Zugang zum größten Teil der Anlage, jedoch nicht zu den dort gespeicherten Kundendaten. Der Leiter des Bereichs IT-Betrieb kann über Zugang zu den Computerräumen und Betriebssystemen verfügen, jedoch nicht zu den Betriebsräumen, in denen die Stromversorgungs-, Klima- und Lüftungssysteme untergebracht sind. Der CEO des Unternehmens kann Zugang zu den Büros des Sicherheitsleiters und der IT-Mitarbeiter sowie zu den öffentlichen Bereichen haben, jedoch nicht zu den Computerräumen oder den Betriebsräumen.

Der Grund für die Anwesenheit Ein Installateur, gleichgültig ob es sich dabei um Herrn Smith oder Frau Jones handelt, kann Zugang zu Betriebsräumen und öffentlichen Bereichen erhalten. Die Reinigungskolonne, deren Namensliste sich täglich ändern kann, kann über Zugang zu den Gemeinschaftsbereichen verfügen, jedoch über keinen weiteren Zugang. Einem Netzwerk-Switch-Experten kann der Zugang zu Racks mit Switching-Komponenten gewährt werden, jedoch nicht zu Racks mit Servern oder Speicherkomponenten. In einer Webserveranlage können Systemwartungsmitarbeiter eines Kunden Zugang zu einem „Kundenraum“ erhalten und von dort aus Verbindungen zu ihrem persönlichen Server für administrative Zwecke herstellen.

Dringender Informationsbedarf Der Zugang zu hochsensiblen Bereichen kann bestimmten Personen für einen bestimmten Zweck gewährt werden, d. h. wenn diese Personen einen dringenden Informationsbedarf haben, und nur so lange dieser Bedarf besteht.

Probleme getrennt behandeln

Details von Identifizierungstechnologien sollten bei der ersten Aufstellung von Sicherheitsanforderungen völlig außer Acht gelassen werden. Zuerst müssen die Bereiche und die Zugangskriterien für die Anlage definiert werden, *dann* folgen nacheinander die Analyse der Kosten, Effektivität und Risiken, die Abwägung von Kompromissen und die Planung der optimalen Implementierung der Technologie.

Anwendung der Technologie

Identifikationsmethoden: Zuverlässigkeit und Kosten im Vergleich

Die Methoden zur Identifizierung von Personen fallen unter drei allgemeine Kategorien mit zunehmender Zuverlässigkeit – und zunehmenden Gerätekosten. Die Methoden sind:

- **objektbasiert**
- **wissensbasiert**
- **personenbasiert**

Objektbasiert

Am unzuverlässigsten (ein Objekt kann von anderen genutzt oder gestohlen werden)

Objektbasiert bezieht sich auf ein Objekt, das eine Person bei sich trägt, wie z. B. ein Schlüssel, eine Karte oder ein kleines Objekt (ein **Token**), das getragen oder an einem Schlüsselring befestigt werden kann. Es kann so „wenig intelligent“ wie ein altmodischer Metallschlüssel sein oder so „intelligent“ wie eine Karte mit einem Prozessor, die Informationen mit einem Kartenleser austauscht (eine **Smart Card**). Es kann sich um eine Magnetstreifenkarte handeln, die Informationen über den Karteneigentümer enthält (wie z. B. die bekannte Geldautomatenkarte), es kann eine Karte oder ein Token mit einem Sender und/oder Empfänger sein, die aus kurzer Entfernung mit dem Kartenleser kommunizieren (eine **Proximity-Karte** oder ein **Proximity-Token** — der Mobil Speedpass® ist ein Beispiel dafür).

Die *objektbasierte* Methode ist die unzuverlässigste Form der Identifizierung, denn es gibt keine Garantie dafür, dass ein Objekt von der richtigen Person verwendet wird – eine andere Person kann es nutzen, es kann gestohlen werden, verloren gehen oder von einer anderen Person gefunden werden.

Wissensbasiert

Zuverlässiger (eine Information kann nicht gestohlen, jedoch anderen mitgeteilt oder schriftlich festgehalten werden)

Die *wissensbasierte* Methode bezieht sich auf ein Passwort, einen Code oder ein Verfahren, wie z. B. das Öffnen eines Code-Schlusses, die Überprüfung an einem Kartenleser oder der Tastaturzugang zu einem Computer. Passwörter/Codes stellen ein Sicherheitsdilemma dar: Kann man sie sich gut merken, sind sie wahrscheinlich leicht zu erraten. Kann man sie sich nur schwer merken, sind sie zwar vermutlich auch schwer zu erraten, werden jedoch womöglich aufgeschrieben, was wiederum die Sicherheit reduziert.

Die *wissensbasierte* Methode ist zuverlässiger als die *objektbasierte* Methode, jedoch können Passwörter und Codes auch von anderen genutzt werden, und wenn sie schriftlich festgehalten werden, besteht das Risiko, dass sie von anderen gelesen werden.

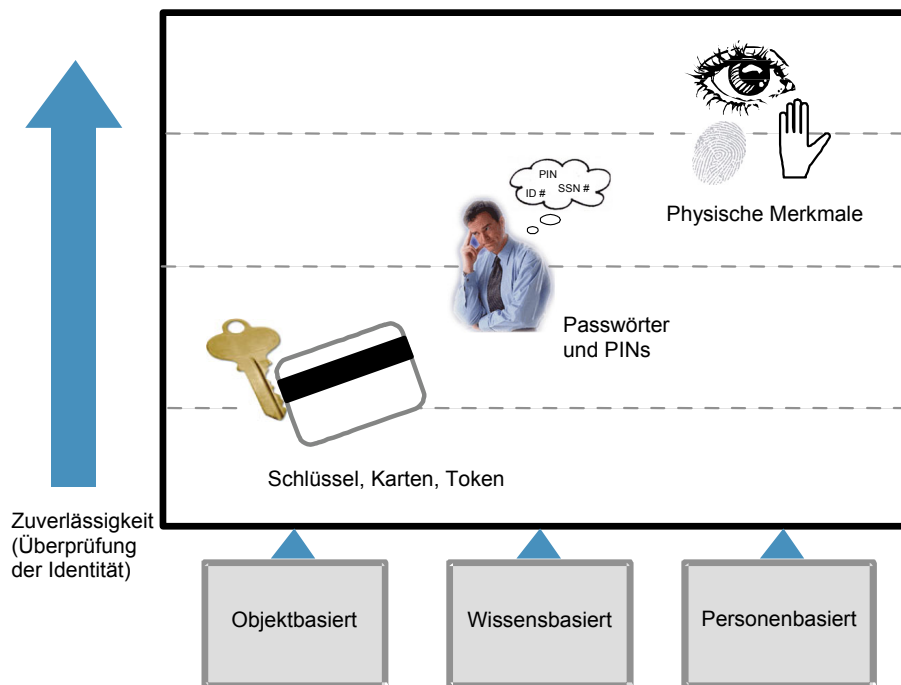
Personenbasiert

Am zuverlässigsten (basiert auf einem eindeutigen physischen Merkmal)

Die *personenbasierte* Methode bezieht sich auf die Identifizierung durch die Erkennung von eindeutigen physischen Merkmalen. Dies ist die natürliche Art und Weise, mit der Menschen einander mit nahezu hundertprozentiger Sicherheit erkennen. Dies mithilfe von technologischen Mitteln zu erreichen (oder zu versuchen), wird als **Biometrie** bezeichnet. Biometrische Scanverfahren wurden für eine Reihe von menschlichen Merkmalen entwickelt, die für die quantitative Untersuchung und Analyse geeignet sind:

- | | |
|----------------------------------|--|
| Fingerabdruck | Hand (Form der Finger und Dicke der Hand) |
| Iris (Farbenmuster) | Gesicht (relative Position von Augen, Nase und Mund) |
| Netzhaut (Muster der Blutgefäße) | Handschrift (Dynamik der Schreibbewegung) |
| Stimme | |

Abbildung 2 – Was jemand hat, Was jemand weiß, Was jemand ist



Biometrische Geräte sind in der Regel sehr zuverlässig, wenn eine Erkennung erreicht wird. Das heißt, wenn das Gerät meint, eine bestimmte Person zu erkennen, dann *ist* sie es mit fast hundertprozentiger Sicherheit auch. Die Hauptursache für Unzuverlässigkeiten bei der Biometrie ist nicht die falsche Erkennung oder die Täuschung durch Fälscher, sondern die Möglichkeit, dass ein legitimer Nutzer möglicherweise nicht erkannt wird („falsche Zurückweisung“).

Kombination von Methoden für höhere Zuverlässigkeit

Ein typischer Sicherheitsplan nutzt Methoden zunehmender Zuverlässigkeit (und Kosten), d.h. je weiter man vordringt, desto komplexer werden die Sicherheitsvorkehrungen. Zum Beispiel kann für den Zugang zu einem Gebäude eine Kombination aus Magnetstreifenkarte und PIN erforderlich sein, für den Zugang zum Computerraum ein Tastenfeldcode und ein biometrisches Merkmal. Durch die Kombination von Methoden an einem Zugangspunkt erhöht sich die Zuverlässigkeit an diesem Punkt. Durch die Verwendung unterschiedlicher Methoden für jede Stufe erhöht sich die Sicherheit der inneren Stufen erheblich, da auf diese Weise jede Stufe nicht nur durch ihre eigenen Methoden geschützt wird, sondern zusätzlich durch die Methoden der weiter außen liegenden Stufen, für die zuerst ein Zugang erreicht werden muss.

Warum ist es so kompliziert?

Die Planung von Sicherheitssystemen erscheint aus folgendem Grund so kompliziert: Es gibt keine Technologie, die es ermöglicht, schnell, einfach und kostengünstig die Identität einer Person zweifelsfrei zu bestimmen. Wir arbeiten mit verschiedenen Methoden, die jedoch unterschiedlich effektiv, benutzerfreundlich und kostenträchtig sind. Das erschwert die Analyse der Kosten/Effektivität/Risiken und führt dazu, dass Technologien kombiniert werden müssen oder zum weiteren Schutz konzentrische Sicherheitsgrenzen gezogen werden müssen.

Sicherheitssystemverwaltung

Einige Zugangskontrollgeräte, wie Kartenleser und biometrische Scanner, können die Daten von Zugangseignissen erfassen, wie z. B. die Identität der Personen, die Zutritt erhalten, und die Uhrzeit des Zutritts. Wenn diese Geräte netzwerkfähig sind, können sie die Informationen an ein Fernverwaltungssystem zur Überwachung und Protokollierung (wer kommt und geht), zur Gerätesteuerung (Konfiguration eines Schlosses für den Zugang bestimmter Personen zu bestimmten Zeiten) und für Alarmmeldungen (Benachrichtigung bei wiederholten, nicht erfolgreichen Versuchen oder bei Gerätefehler) weiterleiten.

Zugangskontrollgeräte

Karten und Token: Objektbasierte Methode

Gegenwärtig werden mehrere Karten- und Tokentypen für die Zugangskontrolle verwendet, von einfachen bis hin zu technisch fortgeschrittenen Arten, die einen vielfältigen Leistungsumfang bieten:

- Fähigkeit zur Neuprogrammierung
- Fälschungssicherheit
- Art der Interaktion mit dem Kartenleser: Durchziehen, Einstecken, an den Leser halten, kontaktbehaftet, kontaktlos („Proximity“)
- Benutzerfreundlichkeit: Physische Form und Tragekomfort
- Gespeicherte Datenmenge
- Rechenfähigkeit
- Kartenkosten
- Kartenleserkosten

Auch wenn sie aufgrund ihrer Technologie noch so sicher und zuverlässig sein mögen, wird die durch diese physikalischen „Objekte“ ermöglichte Sicherheit dadurch begrenzt, dass es keine Garantie dafür gibt, dass sie von der richtigen Person verwendet werden. Daher werden sie in der Regel mit einer oder mehreren weiteren Methoden zur Identifizierung der Identität kombiniert, z. B. einem Passwort oder sogar einem biometrischen Merkmal.

Die **Magnetstreifenkarte** mit einem einfachen Magnetstreifen, der die Identifikationsdaten enthält, ist der am häufigsten verwendete Kartentyp. Beim Ziehen der Karte durch einen Kartenleser werden die Informationen gelesen und in einer Datenbank überprüft. Dieses System ist kostengünstig und benutzerfreundlich, hat jedoch den Nachteil, dass es relativ leicht ist, die Karten zu duplizieren oder die auf ihnen gespeicherten Informationen zu lesen.

Die **Bariumferrit-Karte** (auch „Magnetpunktkarte“ genannt) entspricht der Magnetstreifenkarte, bietet jedoch mehr Sicherheit ohne große Mehrkosten. Sie enthält ein dünnes Plättchen aus magnetischem Material, um das ein Muster von runden Punkten angeordnet ist. Die Karte wird nicht gescannt oder durchgezogen, sondern einfach an den Kartenleser gehalten.

Die **Weigand-Karte** ist eine Variante der Magnetstreifenkarte. Sie enthält eine Reihe von speziell behandelten Drähten mit einer eindeutigen magnetischen Signatur. Beim Ziehen der Karte durch den Kartenleser wird die Signatur von einer Spule erkannt und in eine Bit-Folge umgewandelt. Der Vorteil dieser komplexen Kartenkonstruktion besteht darin, dass die Karten nicht dupliziert werden können, der Nachteil ist, dass sie nicht neu programmiert werden können. Bei dieser Technologie müssen die Karten nicht in direkten Kontakt mit dem Kartenleser kommen. Aus diesem Grund kann der Kopf des Kartenlesers in ein Gehäuse eingekapselt werden und ermöglicht daher eine Installation im Freien. Im Gegensatz zu den Kartenlesern für Proximity- und Magnetstreifenkarten werden Weigand-Kartenleser nicht durch Funkstörungen (RFI) oder elektromagnetische Felder (EMF) beeinflusst. Die Robustheit dieses Kartenlesers in Kombination mit der geringen Duplikationsmöglichkeit der Karte machen das Weigand-System extrem sicher (innerhalb der Grenzen der objektbasierten Methode), jedoch auch kostspieliger.

Die **Barcode-Karte** trägt einen Barcode, der beim Ziehen der Karte durch den Kartenleser gelesen wird. Dieses System ist sehr kostengünstig, jedoch leicht zu überlisten. Mit einem gewöhnlichen Kopierer kann ein Barcode gut genug dupliziert werden, um den Barcode-Leser zu täuschen. Barcode-Karten sind für minimale Sicherheitsanforderungen geeignet, insbesondere wenn diese eine große Anzahl von Lesegeräten in der gesamten Anlage erfordern oder an einem bestimmten Zugangspunkt ein hohes Verkehrsaufkommen anfällt. Es handelt sich dabei jedoch weniger um ein Sicherheitssystem, als vielmehr um eine kostengünstige Methode der *Zugangsüberwachung*. (Es wurde einmal gesagt, die Identifizierung durch Barcodes hätte nur den Zweck, „die ehrlichen Leute nicht hineinzulassen“.)

Die **Infrarotschatten-Karte** verbessert die geringe Sicherheit der Barcode-Karte, indem der Barcode zwischen PVC-Kunststofflagen eingeschlossen wird. Der Kartenleser sendet Infrarotlicht durch die Karte, und der Schatten des Barcodes wird von den Sensoren an der Außenseite gelesen.

Die **Proximity-Karte** (manchmal auch „Prox-Karte“ genannt) ist im Hinblick auf Benutzerfreundlichkeit einen Schritt weiter als die Karten, die durch den Kartenleser gezogen oder an den Leser gehalten werden müssen. Wie der Name schon sagt, muss die Karte nur in der Nähe (engl. „Proximity“) des Kartenlesers sein. Erreicht wird dies mithilfe der RFID (Radio Frequency Identification)-Technologie, wobei die Karte über das elektromagnetische Feld des Kartenlesers mit Strom versorgt wird. Diese überaus populäre Konstruktion funktioniert bei einer Entfernung von ca. 10 cm vom Kartenleser. Eine andere Konstruktion, die als **Vicinity-Karte** bezeichnet wird, funktioniert bei einer Entfernung von rund einem Meter vom Kartenleser.

Die **Smart Card**, die jüngste Entwicklung unter den Zugangskontrollkarten, ist im Begriff, die Methode der Wahl für neue Installationen zu werden. Diese Karte verfügt über einen integrierten Silizium-Chip für Onboard-Datenspeicherung und/oder -Berechnungen. Der Datenaustausch mit dem Kartenleser erfolgt entweder durch Kontakt des Chips mit dem Leser (*kontaktbehaftete* Smart Card) oder durch kontaktlose Interaktion mit dem Leser, wobei die gleiche Technologie wie bei den Proximity- und Vicinity-Karten verwendet wird (*kontaktlose oder berührungslose* Smart Card). Der Chip, der einen Durchmesser von ca. 1,3 cm hat, muss sich nicht unbedingt auf der Karte befinden, sondern kann an eine Foto-ID angehängt sein, sich an einer Schlüsselkette befinden oder als Knopf oder Schmuck getragen werden (wie z. B. das iButton®-Token). Die allgemeine Bezeichnung für Objekte, die einen solchen Chip tragen, lautet *smarte Medien*.

Smart Cards bieten ein hohes Maß an Flexibilität im Hinblick auf die Zugangskontrolle. Der Chip kann beispielsweise älteren Kartentypen hinzugefügt werden, um sie aufzurüsten und in bestehende Systeme zu integrieren. Es ist auch möglich, den Fingerabdruck oder Iris-Scan des Karteneigentümers für eine biometrische Überprüfung durch den Kartenleser auf dem Chip zu speichern und dadurch die Identifizierung von der objektbasierten Ebene auf die personenbasierte Ebene zu bringen. Kontaktlose Smart Cards, die über „Vicinity“-Reichweite verfügen, bieten eine nahezu optimale Benutzerfreundlichkeit: eine Transaktionszeit von einer halben Sekunde, ohne dass die Karte aus der Brieftasche genommen werden muss.

Tastenfelder und Code-Schlösser: Wissensbasierte Methode

Tastenfelder und **Code-Schlösser** sind weit verbreitete Methoden der Zugangskontrolle. Sie sind zuverlässig und sehr benutzerfreundlich, die von ihnen gebotene Sicherheit wird jedoch durch gemeinsam nutzbare und erratbare Passwörter begrenzt. Sie verfügen über eine telefonähnlich Tastatur für die Code-Eingabe. Wenn der Code für jeden Benutzer eindeutig ist, wird er als persönlicher Zugangscode oder persönliche Identifikationsnummer (PIN) bezeichnet. Ein *Tastefeld* impliziert in der Regel die Möglichkeit der Eingabe mehrerer Codes (einen Code für jeden Benutzer), während ein *Code-Schloss* sich gewöhnlich auf ein Gerät bezieht, für das ein einziger Code gilt, der von allen Zugangsberechtigten verwendet wird.

Die Sicherheitsstufe von Tastenfeldern und Code-Schlössern kann durch sich periodisch ändernde Codes erhöht werden. Dazu ist ein System für die Benutzerinformation und die Ausgabe von neuen Codes erforderlich. Bei Code-Schlössern, deren Code nicht geändert wird, muss das zugehörige Tastenfeld regelmäßig erneuert werden, wenn die Tasten erkennbare Abnutzungsspuren aufweisen. Wie bei Zugangskarten kann auch die Sicherheit durch Tastenfelder erhöht werden, wenn zur Bestätigung der Benutzeridentität ein biometrisches Merkmal hinzugezogen wird.

Biometrie: Personenbasierte Methode

Die biometrische Technologie ist in einer rasanten Entwicklung begriffen und wird zunehmend besser und kostengünstiger. Sehr zuverlässige und kostengünstige biometrische Überprüfungen, insbesondere die Fingerabdruckerkennung, finden derzeit Eingang in den größten Teil der Sicherheitslösungen. Das Lieferprogramm vieler Anbieter umfasst bereits eine breite Palette von biometrischen Geräten. In Kombination mit den herkömmlichen objektbasierten und wissensbasierten Methoden können bestehende Sicherheitsmaßnahmen mithilfe der Biometrie zur Best Practice der Zugangskontrolle werden.

Die biometrische Identifizierung wird in der Regel nicht verwendet, um eine Identität zu *erkennen*, indem in einer Datenbank nach einer Übereinstimmung gesucht wird, sondern um eine Identität zu *überprüfen*, die zuvor mithilfe der objektbasierten oder der wissensbasierten Methode festgestellt wurde. Wenn beispielsweise zuerst eine Karte/PIN verwendet wird, kann das Ergebnis mit einem Fingerabdruckscan überprüft werden. Mit zunehmender Leistungsstärke und Zuverlässigkeit kann die biometrische Technologie mit der Zeit eine eigenständige Methode zur *Erkennung* der Identität werden und es überflüssig machen, dass jemand eine Karte bei sich tragen oder sich an ein Passwort erinnern muss.

Bei der biometrischen Identifizierung können zwei Arten von Fehlern auftreten:

Falsche Zurückweisung: Ein legitimer Benutzer wird nicht erkannt. Man könnte zwar argumentieren, dass dadurch der geschützte Bereich besonders sicher wird. Es ist jedoch eine unzumutbare Frustration für legitime Benutzer, den Zugang verwehrt zu bekommen, weil der Scanner sie nicht erkennt.

Falsche Akzeptanz: Fehlerhafte Erkennung, entweder durch die Verwechslung eines Benutzers mit einer anderen Person oder durch die Akzeptanz eines Eindringlings als legitimen Benutzer.

Warum wird nicht *nur* biometrische Erkennung verwendet

F: Warum wird an einem Zugangspunkt, der Karte, PIN und biometrische Erkennung verwendet, nicht einfach nur die biometrische Erkennung verwendet, wenn die Biometrie so zuverlässig ist?

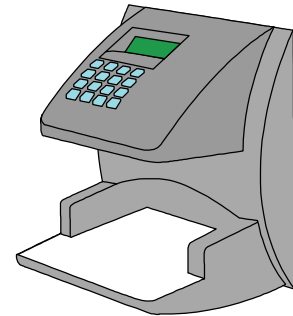
A: Der Grund dafür ist, dass (1) die biometrische Verarbeitungszeit möglicherweise nicht akzeptabel ist, wenn eine große Datenbank von Benutzerscans durchsucht werden muss und nicht nur ein Vergleich mit dem Scan eines einzelnen Benutzers vorgenommen wird, und dass (2) bei der biometrischen Erkennung das Risiko der falschen Zurückweisung bzw. der falschen Akzeptanz reduziert werden kann, wenn der Scan mit nur einem Benutzer in der Datenbank verglichen wird.

Es ist zwar fast unmöglich, biometrische Merkmale zu fälschen, dennoch bleibt das Risiko von Identifizierungsfehlern durch die Technologie.

Fehlerraten können durch Ändern der Schwelle („wie nahe ist nah genug“) zur Bestimmung der Übereinstimmung angepasst werden, jedoch wird durch das Senken einer Fehlerrate die andere erhöht.

Die Vorbehalte bei der Wahl einer biometrischen Funktion beziehen sich auf die Gerätekosten, die Fehlerraten (sowohl falsche Zurückweisung als auch falsche Akzeptanz) und die *Benutzerakzeptanz*, d. h. darauf, für wie aufdringlich, unangenehm oder sogar gefährlich ein Verfahren empfunden wird. Zum Beispiel gelten Netzhautscanner generell als Systeme mit geringer Benutzerakzeptanz, weil das Auge nur wenige Zentimeter vom Scanner entfernt sein muss und eine LED direkt in das Auge gerichtet wird.

Abbildung 3 – Handscanner



Weitere Elemente von Sicherheitssystemen

Im Mittelpunkt der Planung von Sicherheitssystemen stehen Geräte zur Identifizierung und Überprüfung von Personen an Zugangspunkten („Zugangskontrolle“). Dies wäre völlig ausreichend, *wenn* eine hundertprozentig zuverlässige Identifikation, uneingeschränktes Vertrauen in die Absichten von Personen, denen Zugang gewährt wurde, und die physikalische Vollkommenheit bruchsicherer Wände, Türen, Fenster, Schlösser und Decken möglich wäre. Um gegen unvermeidliche Fehlschläge aufgrund von Mängeln oder Sabotage gewappnet zu sein, umfassen Sicherheitssysteme in der Regel zusätzliche Schutz-, Überwachungs- und Wiederherstellungsmethoden.

Bauliche Planung

Beim Bau eines neuen oder der Renovierung eines alten Gebäudes können von Grund auf Maßnahmen für die physikalische Sicherheit getroffen werden, indem Architektur- und Konstruktionsmerkmale integriert werden, die ein unbefugtes Eindringen erschweren oder verhindern. Sicherheitsüberlegungen bei der Konstruktion und Planung eines Gebäudes beziehen sich in der Regel auf potenzielle Zugangs- und Fluchtwege, den Zugang zu wichtigen Elementen der Infrastruktur, wie z. B. Klima- und Lüftungssysteme sowie Verkabelungen, und potenzielle Versteckmöglichkeiten für Eindringlinge. Eine Auflistung einiger dieser Planungsüberlegungen ist im Anhang enthalten.

Eindringen im Huckepack und im Schlepptau: Türschleusen

Eine häufige und ärgerliche Lücke in einem sonst sicheren Zugangskontrollsystem kann die Möglichkeit sein, dass eine nicht autorisierte Person einer autorisierten Person durch eine Kontrollstelle folgen kann (dies wird als **Eindringen im Huckepack** bezeichnet, wenn die autorisierte Person dabei Hilfe leistet, also z. B. die Tür aufhält, oder als **Eindringen im Schlepptau**, wenn die nicht autorisierte Person unbemerkt durchschlüpfen kann). Die herkömmliche Lösung ist eine schleusenartige Vorrichtung, die so genannte **Türschleuse**. Diese verfügt über eine Zugangs- und Ausgangstür, wobei der Raum zwischen den beiden Türen nur Platz für eine Person bietet. Türschleusen können mit einer Zugangskontrolle am Zugang und am Ausgang oder nur am Ausgang konstruiert werden. In diesem Fall wird bei einem fehlgeschlagenen Versuch, die Schleuse zu verlassen, die Zugangstür versperrt und ein Alarm ausgegeben, dass ein Eindringling festgehalten wird. Ein Boden mit Trittsensoren kann zusätzlich gewährleisten, dass nur eine Person die Schleuse passiert.

Eine neue Technologie zur Lösung dieses Problems verwendet eine Overhead-Kamera zur optischen Verfolgung und Erfassung der durchgehenden Personen. Die Kamera gibt einen Alarm aus, wenn sie pro autorisiertem Zugang mehr als eine Person erkennt.

Kameraüberwachung

Festkameras können für Zwecke wie zur Aufzeichnung von Kfz-Nummernschildern an Zufahrten oder in Verbindung mit Trittsensoren zur Aufzeichnung von Personen an kritischen Standorten verwendet werden.

Verdeckt oder sichtbar angebrachte CCTV-Kameras ermöglichen Außen- oder Innenüberwachung, wirksame Abschreckung und die Auswertung von Aufnahmen nach einem Zwischenfall. Es können verschiedene Arten von Kameras verwendet werden: Festkameras, Drehkameras oder ferngesteuerte Kameras. Hier einige Überlegungen zur Positionierung von Kameras:

- Ist es wichtig, dass eine Person in Kamerareichweite leicht zu identifizieren ist?
- Soll nur festgestellt werden, ob sich jemand im Raum befindet?
- Soll durch die Überwachung festgestellt werden, ob Inventar entnommen wird?
- Soll die Kamera nur abschreckende Wirkung haben?

Bei der Aufzeichnung von CCTV-Signalen müssen die folgenden Fragen geklärt werden:

- Wie werden die Bänder indiziert und katalogisiert, um eine leichte Suche zu ermöglichen?
- Werden die Bänder vor Ort oder anderswo aufbewahrt?
- Wer soll Zugang zu den Bändern haben?
- Welches Verfahren soll für den Zugang zu den Bändern gelten?
- Wie lange werden die Bänder aufbewahrt, bevor sie vernichtet werden?

Eine neue Technologie ist in der Entwicklung begriffen, die die Automatisierung einer traditionell von Sicherheitskräften durchgeführten Aufgabe, das Überwachen der Monitore, durch softwaregestützte Erkennung von Änderungen (Bewegungen) auf dem Monitorbild ermöglichen soll.

Sicherheitskräfte

Trotz aller technologischen Fortschritte auf dem Gebiet der physikalischen Sicherheit stimmen Experten darin überein, dass ein qualifiziertes Team von Sicherheitskräften an oberster Stelle auf der Liste der Methoden zur Sicherung und Unterstützung der Zugangskontrolle steht. Sicherheitskräfte können bei der Überwachung alle menschlichen Sinne nutzen und darüber hinaus flexibel und intelligent auf verdächtige, ungewöhnliche oder bedrohliche Ereignisse reagieren.

Die IFPO (International Foundation for Protection Officers) ist eine gemeinnützige Organisation, die mit dem Ziel gegründet wurde, standardisierte Schulungen und Zertifizierungen für Sicherheitskräfte bereitzustellen. Das *Security Supervisor Training Manual* (Schulungshandbuch für Sicherheitskräfte) ist ein Referenzhandbuch für Sicherheitsbeauftragte und ihre Mitarbeiter.

Sensoren und Alarmmeldungen

Die traditionellen Alarmanlagen für Häuser und Gebäude und die verwendeten Sensoren, wie Bewegungssensoren, Wärmesensoren, Kontaktsensoren (Tür geschlossen) usw., sind allgemein bekannt. Bei Alarmanlagen für Datacenter empfiehlt sich darüber hinaus der Einsatz weiterer Arten von Sensoren, wie Laserschranken, Trittsensoren, Berührungssensoren, Vibrationssensoren. Außerdem gibt es in Datacentern möglicherweise auch Bereiche, für die sich ein stummer Alarm anstelle eines hörbaren empfiehlt, um Eindringlinge „auf frischer Tat“ zu ertappen.

Netzwerkfähige Sensoren können mit einem Fernverwaltungssystem überwacht und gesteuert werden, dies könnte auch Personalbewegungsdaten von Zugangskontrollgeräten einschließen (siehe den Abschnitt, **Sicherheitssystemverwaltung**) weiter oben.

Besucher

Der Umgang mit Besuchern muss bei jeder Planung eines Sicherheitssystems berücksichtigt werden. Typische Lösungen sind, temporäre Ausweise oder Karten für Bereiche mit geringer Sicherheit auszugeben und für Bereiche mit hoher Sicherheit eine Begleitung vorzuschreiben. Bei Türschleusen (die verhindern sollen, dass zwei Personen mit nur einer Berechtigung einen Zugangspunkt passieren) müssen Maßnahmen für eine zeitlich begrenzte Deaktivierung oder die Ausstellung von Besucherberechtigungen getroffen werden, um den Durchgang zu ermöglichen.

Der Faktor Mensch

Durch Technologie allein lässt sich nicht alles erreichen, insbesondere dann nicht, wenn es um die Durchführung einer ihrem Wesen nach sehr menschlichen Aufgabe geht: die Überprüfung der Identität und Absichten von Menschen. Menschen machen zwar einen erheblichen Teil des Sicherheitsproblems aus, sie sind jedoch auch Teil der Lösung. Mit ihren Fähigkeiten und Fehlern sind sie nicht nur das schwächste Glied, sondern auch die stärkste Stütze.

Der Faktor Mensch: Das schwächste Glied

Zusätzlich zu Fehlern und Unfällen birgt auch die natürliche menschliche Neigung zu Freundlichkeit und Vertrauen Risiken. Eine bekannte Person, die die Anlage betritt, könnte ein verärgertes oder ein abtrünniger Mitarbeiter sein. Die Versuchung, wegen eines bekannten Gesichts Regeln zu brechen oder Abläufe zu umgehen, kann verheerende Folgen haben. Eine signifikante Kategorie der Sicherheitsverletzungen sind „Insider-Jobs“. Selbst unbekannte Personen können bei der Umgehung von Sicherheitsmaßnahmen erstaunlich erfolgreich sein. Die Fähigkeit cleverer Unbekannter, Täuschungsmanöver durchzuführen, um Zugang zu erhalten, ist so gut dokumentiert, dass sie einen Namen hat: **Social Engineering**. Alle Personen, die in einem sensiblen Bereich arbeiten, müssen nicht nur im Hinblick auf Betriebs- und Sicherheitsabläufe geschult werden, sondern auch im Hinblick darauf, den kreativen Methoden des Social Engineering widerstehen zu können.

Der Faktor Mensch: Die stärkste Stütze

Beim Schutz gegen Sicherheitsverletzungen geht es häufig in erster Linie darum, unerwartete Faktoren zu erkennen und zu interpretieren – eine Fähigkeit, in der wachsame Menschen jeder Technologie überlegen sind. Wenn dann noch eine große Standfestigkeit gegenüber Manipulationsversuchen und Regelverstößen hinzukommt, können Menschen die Technologie auf unschätzbare Weise ergänzen.

Von wachsamem Mitarbeitern abgesehen, gibt es einen weiteren Personenkreis, der sich durch den hohen Wert des menschlichen Sehens und Hörens, durch sein Reaktionsvermögen und seine Flexibilität als ein besonderes Element in einem Sicherheitsplan empfiehlt: der altmodische Wachmann. Die Anwesenheit von Wachpersonal an Zugangspunkten sowie Streifengänge auf dem Gelände und im Gebäude sind zwar kostspielig, können jedoch überaus lohnend sein, wenn die technologische Sicherheit versagt oder sabotiert wird. Die schnelle Reaktion eines aufmerksamen Wachmanns, wenn „etwas nicht stimmt“ kann die letzte rettende Instanz bei einer potenziell verheerenden Sicherheitsverletzung sein.

Beim Schutz gegen versehentlichen oder absichtlichen Schaden ist der menschliche Beitrag der gleiche: ständige Wachsamkeit und strikte Befolgung von Vorgaben. Wenn alle, außer die für den Betrieb der Anlage wichtigen Personen, ausgeschlossen werden, bilden die übrigen Mitarbeiter, wenn sie entsprechend geschult sind und festgelegte Verfahrensweisen befolgen, die letztendliche Firewall eines effektiven Sicherheitssystems.

Die Wahl der richtigen Lösung: Risikotoleranz und Kosten im Vergleich

Das richtige Sicherheitssystem ist ein auf der bestmöglichen Einschätzung basierender Kompromiss, bei dem sich das Risiko und der potenzielle Schaden durch Personen, die sich am falschen Ort befinden, sowie die Kosten und Unannehmlichkeiten der Sicherheitsmaßnahmen zum Ausschluss dieser Personen in einem ausgewogenen Gleichgewicht befinden.

Potenzielle Kosten einer Sicherheitsverletzung

Jedes Datacenter hat zwar seine eigenen individuellen Merkmale und sein eigenes Verlustpotenzial, die folgenden allgemeinen Kategorien dürften jedoch für die meisten Datacenter relevant sein:

Physikalischer Verlust: Schäden an Räumen und Geräten durch Unfälle, Sabotage oder Diebstahl

IT-bezogener Produktivitätsverlust: Behinderung von Mitarbeitern an der Durchführung ihrer Hauptaufgaben während der Reparatur bzw. dem Austausch von Geräten, der Wiederherstellung von Daten oder der Fehlerbehebung von Systemen

Unternehmensbezogener Produktivitätsverlust: Unterbrechung der Geschäftsabläufe durch Ausfallzeiten

Datenverlust: Verlust, Beschädigung oder Diebstahl von Daten

Reputationseinbußen und Kundenverluste: Die Folgen schwerwiegender oder wiederholter Sicherheitsverletzungen: Geschäftsverluste, Rückgang des Börsenwerts, Rechtsstreitigkeiten.

Überlegungen bei der Planung von Sicherheitssystemen

Die Planung eines Sicherheitssystems kann eine komplizierte Gleichung mit vielen Variablen sein. Konkrete Strategien für die Planung von Sicherheitssystemen würden den Rahmen dieses Dokuments sprengen, jedoch sind bei jeder Planung mit großer Wahrscheinlichkeit die folgenden Punkte zu berücksichtigen:

Gerätekosten: Der umfassende Einsatz von hochzuverlässigen Identifikationsgeräten wird in der Regel durch Budgetvorgaben eingeschränkt. Der übliche Ansatz besteht darin, eine Reihe von Techniken zu implementieren, die verschiedenen Sicherheitsstufen entsprechen.

Kombination von Technologien: Die Zuverlässigkeit der Identifikation auf jeder Stufe kann durch die Kombination kostengünstigerer Technologien erhöht werden. Dabei wird der innerste Bereich durch den kombinierten Schutz aller ihn umgebenden konzentrischen Außengrenzen geschützt.

Benutzerakzeptanz: (Der „Unannehmlichkeitsfaktor“). Benutzerfreundlichkeit und zuverlässige Identifikation sind wichtig, um zu vermeiden, dass das System zu einer Quelle der Frustration wird und subversiven Aktivitäten Vorschub leistet.

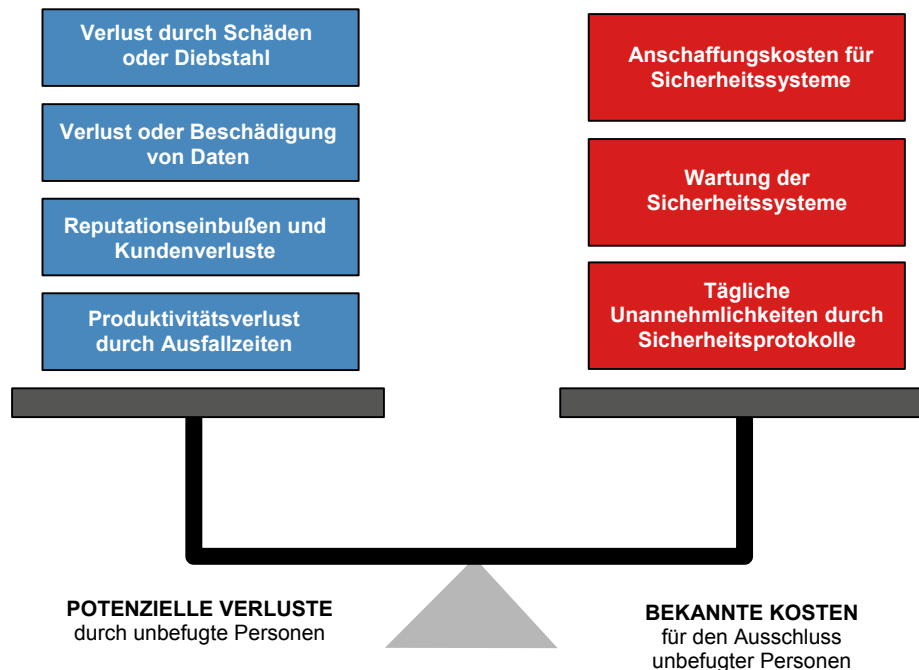
Skalierbarkeit: Kann der Plan Schritt für Schritt implementiert werden, wenn der Bedarf, das Budget und das Vertrauen in die Technologie steigen?

Rückwärtskompatibilität: Ist das neue Konzept mit Elementen eines bestehenden älteren Systems kompatibel? Die Weiterverwendung eines bestehenden Systems oder von Teilen davon kann die Implementierungskosten erheblich reduzieren.

Es geht nicht nur um Kosten

Selbst wenn die Kosten keine Rolle spielen würden, wäre es in den meisten Fällen auf nicht akzeptable Weise hinderlich und beschwerlich, eine Anlage mit den höchsten Sicherheitsmaßnahmen zu überziehen. Die Sicherheitsanforderungen für jeden zu schützenden Bereich müssen im Hinblick darauf, was der Bereich enthält und wer Zugang benötigt, realistisch analysiert werden.

Abbildung 4 – Abwägen potenzieller Verluste gegen bekannte Sicherheitskosten



Schlussfolgerung

Durch die schnell zunehmende Verbreitung von Datacentern und Webhosting-Sites ist der Bedarf an physikalischer Sicherheit in einer Anlage mindestens ebenso groß wie der Bedarf an Cybersicherheit bei Netzwerken. Eindringlinge, die ihre Identität fälschen und ihre Absichten verschleiern, können sehr großen Schaden verursachen, von der physikalischen Deaktivierung wichtiger Geräte bis hin zum Auslösen eines Software-Angriffs über eine nicht gesicherte Tastatur. Selbst die gewöhnlichen Fehler vertrauenswürdiger Mitarbeiter stellen eine signifikante tägliche Bedrohung für den Anlagenbetrieb dar, die dadurch minimiert werden kann, dass der Zugang nur auf die unbedingt erforderlichen Mitarbeiter beschränkt wird.

Die Technologien zur Implementierung umfassender Lösungen auf der Grundlage der Identifikationsprinzipien mittels der Methoden **objektbasiert**, **wissensbasiert**, und **personenbasiert** sind verfügbar und werden zunehmend kostengünstiger. Indem die Bewertung der Risikotoleranz mit einer Analyse der Zugangsanforderungen und verfügbaren Technologien kombiniert wird, kann ein effektives Sicherheitssystem konzipiert werden, bei dem Schutz und Kosten in einem realistischen und ausgewogenen Verhältnis zueinander stehen.

Über die Autorin:

Suzanne Niles ist Autorin für White Papers im APC Engineering Design Center in Billerica, Massachusetts. Sie studierte Mathematik am Wellesley College und erwarb anschließend am MIT (Massachusetts Institute of Technology) einen Bachelor in Informatik. Thema ihrer Abschlussarbeit war die Erkennung von handschriftlichen Zeichen. Suzanne Niles unterrichtet seit über 25 Jahren die unterschiedlichsten Zielgruppen und verwendet dabei eine Vielfalt von Medien, von Softwarehandbüchern, über Fotos bis hin zu Kinderliedern. Bevor Suzanne Niles 2004 zu APC kam, war sie Buchherausgeberin im Verlag The Village Group. Zu den von ihr herausgegebenen Büchern gehört auch das neue Buch von Wes Kussmaul, *Quiet Enjoyment*, dessen Thema die Sicherheit und Identität im Zeitalter des Internets ist.

Anhang

Sicherheitsüberlegungen bei der baulichen Planung

Beim Bau einer neuen oder der Renovierung einer alten Anlage können von Grund auf Maßnahmen für die physikalische Sicherheit getroffen werden, indem Architektur- und Konstruktionsmerkmale integriert werden, die ein unbefugtes Eindringen erschweren oder verhindern. Sicherheitsüberlegungen bei der Konstruktion und Planung eines Gebäudes beziehen sich in der Regel auf potenzielle Zugangs- und Fluchtwege, den Zugang zu wichtigen Elementen der Infrastruktur, wie Klima- und Lüftungssysteme und die Verkabelung, sowie potenzielle Versteckmöglichkeiten für Eindringlinge.

Informationen zu Sicherheitsüberlegungen bei der Standortwahl sind im APC White Paper Nr. 81, „Site Selection for Mission Critical Facilities“ (Wahl des Standorts von betriebskritischen Anlagen) enthalten.

- Die Lage des Eingangs zum Datacenter sollte so gewählt werden, dass in seiner unmittelbaren Umgebung nur der für das Datacenter bestimmte Verkehr anfällt.
- Es empfiehlt sich, massive Stahltüren und -rahmen zu verwenden, keine Hohltüren. Scharniere dürfen nicht von außen abmontiert werden können.
- Für die Wände von Datacentern sollten stärkere Materialien verwendet werden als die für Innenwände üblichen Gipsplatten. Zur Erkennung von Manipulationen können Sensoren in die Wände integriert werden.
- Der für das Datacenter verwendete Raum sollte keine direkten Außenwände aufweisen.
- Im Datacenter sind lange und ungehinderte Sichtlinien für Sicherheitsstationen oder Kameras vorzusehen.
- Die Sicht auf den Eingang und andere sensible Bereiche sollte durch Absperrvorrichtungen nach Außen verdeckt werden. Dadurch wird verhindert, dass Personen den Gebäudegrundriss oder die Sicherheitsmaßnahmen in Augenschein nehmen können.
- Besonders zu beachten ist die Lage von Lüftungskanälen, Wartungsluken, Lüftungsöffnungen, Wartungsaufzügen und anderen möglichen Öffnungen, die für einen unbefugten Zugang genutzt werden könnten. Alle derartigen Öffnungen, die breiter sind als 30 cm, sollten durch einbruchssichere Schutzgitter gesichert werden, um unbefugtes Eindringen zu verhindern.

- Hohlräume, die als Versteck für Personen oder Gegenstände dienen können, sind zu vermeiden. Beispielweise könnte der Hohlraum unter Hohlfußböden als Versteck genutzt werden. Potenzielle Verstecke sind unbedingt zu sichern und dürfen für Personen, die durch das Gebäude gehen, nicht leicht erkennbar sein.
- An allen Zugängen zum Dach sollten Schlösser und Türalarmanlagen installiert werden, damit bei einem Zugangsversuch eine sofortige Benachrichtigung der Sicherheitsverantwortlichen erfolgt. Zugangspunkte auf dem Dach sind möglichst zu vermeiden.
- Alle externen Rohrleitungen und Verkabelungen sowie Klima- und Lüftungssysteme sollten erfasst und entsprechend geschützt werden. Wenn sich diese Infrastrukturkomponenten irgendwo auf dem Standort befinden und nicht geschützt sind, können sie genutzt werden, um die Anlage zu sabotieren, ohne dass dazu Sicherheitsmaßnahmen deaktiviert werden müssen.
- Jeder Zugang zu internen Kabelsträngen sowie Rohr- und Lüftungskanälen, die in der Anlage verlaufen, muss verhindert werden. Die umfassendste Sicherheit eines Datacenters nützt nicht viel, wenn eine Person, die einen Gang entlang geht, Zugang zu Strom- oder Datenkabeln erhalten kann.
- Bei der Modernisierung einer bestehenden Anlage oder beim Aufbau eines neuen Datacenters in einem bestehenden Gebäude sollte die Lage des Datacenters innerhalb des Gebäudes betrachtet werden. Der Standort sollte weder unsicher sein noch vermeidbare Risiken bergen. Zum Beispiel sollten Datacenter nicht in unmittelbarer Nähe von Küchen, Produktionsbereichen mit großen Maschinen, Parkplätzen oder anderen Bereichen mit hohem Verkehrsaufkommen oder Zufahrten eingerichtet werden. Von Küchenbränden über Autobomben bis hin zu Verkehrsunfällen kann alles eine Gefährdung darstellen.
- Die zentrale Sicherheitsüberwachungsstation sollte durch ein Gehäuse aus kugelsicherem Glas geschützt werden.
- Wenn sich das Datacenter in einem separaten Gebäude befindet, muss die Außenseite dieses Gebäudes unauffällig gehalten werden. Es dürfen keine Kennzeichnungen, wie z. B. Firmennamen oder Logos, angebracht werden, die darauf hinweisen könnten, dass sich im Inneren ein Datacenter befindet.
- Mithilfe von Betonpollern oder anderen Hindernissen kann erreicht werden, dass unerwünschte Fahrzeuge einen genau festgelegten Abstand zum Gebäude einhalten müssen.

Glossar

Begriffe in Fettdruck werden in diesem Glossar definiert.

Barcode-Karte

Ein Kartentyp für die **Zugangskontrolle**, der einen Barcode zum Speichern von Informationen verwendet, die beim Ziehen der Karte durch einen Kartenleser gelesen werden.

Bariumferrit-Karte

Ein Kartentyp für die **Zugangskontrolle**, der ein Muster von magnetischen Punkten zum Speichern von Informationen verwendet, die gelesen werden, wenn die Karte flach auf einen Kartenleser gelegt wird. Wird auch als „Magnetpunktkarte“ bezeichnet.

Biometrisches Schloss

Ein Schloss, das durch einen biometrischen Scanner gesteuert wird.

Biometrie

Die Bestimmung der persönlichen Identität mithilfe einer Technologie zur Messung von physischen Merkmalen, wie z. B. ein Fingerabdruck, oder von Verhaltensmerkmalen.

Code-Schloss

Ein Schloss, das durch Eingabe eines Codes über ein Tastenfeld geöffnet wird.

Dringender Informationsbedarf

Eine sehr hohe Sicherheitsstufe, die den Zugang auf Personen beschränkt, für die eine besondere, dringliche Notwendigkeit für den Aufenthalt in dem gesicherten Bereich besteht (z. B. für den Zugriff auf bestimmte Daten). Der Zugang wird dabei nur für die Zeitspanne gewährt, während derer diese Notwendigkeit besteht.

Eindringen im Huckepack

Eine Sicherheitsverletzung, die auftritt, wenn eine autorisierte Person, die durch ordnungsgemäße Anmeldung Zugang erhalten hat, die Tür für eine nicht autorisierte Person offen hält und es dieser ermöglicht, die Kontrollstelle ohne Berechtigungsnachweis zu passieren. (Ein ähnlicher Verstoß ist das **Eindringen im Schlepptau**. Dabei schlüpft eine nicht autorisierte Person unbemerkt nach einem autorisierten Benutzer durch die Tür der Kontrollstelle.)

Eindringen im Schlepptau

Eine Sicherheitsverletzung, die auftritt, wenn eine nicht autorisierte Person unbemerkt durch eine Kontrollstelle schlüpft, indem sie einem autorisierten Benutzer durch eine offene Tür folgt. (Ein ähnlicher Verstoß ist das **Eindringen im Huckepack**. Dabei leistet der autorisierte Benutzer Hilfe und hält die Tür auf.)

Falsche Akzeptanz

Bei der biometrischen Identifikation: Das fehlerhafte Ergebnis der Identifizierung einer Person, die nicht in der Datenbank der bekannten Personen enthalten ist. Es handelt sich dabei um einen der beiden Fehler, die bei der biometrischen Identifikation auftreten können. Der andere Fehler ist die **falsche Zurückweisung**.

Falsche Zurückweisung

Bei der biometrischen Identifikation: Das fehlerhafte Ergebnis der Nicht-Erkennung einer bekannten Person. Es handelt sich dabei um einen der beiden Fehler, die bei der biometrischen Identifikation auftreten können. Der andere Fehler ist die **falsche Akzeptanz**.

FAR

Falsche Akzeptanzrate. Bei einem biometrischen Gerät der Prozentwert der Identifizierungen, bei denen es sich um **falsche Akzeptanz** handelt.

FRR

Falsche Rückweisungsrate. Bei einem biometrischen Gerät der Prozentwert der Identifizierungen, bei denen es sich um **falsche Zurückweisung** handelt.

Gesichtsgeometrie

Eines der physischen Merkmale, das mithilfe der biometrischen Technologie gemessen werden kann: die relative Position von Augen, Nase und Mund im Gesicht.

Handscan

Ein Verfahren zur biometrischen Identifikation, das die dreidimensionale Handgeometrie misst, d. h. die Form der Finger und die Dicke der Hand.

iButton®

Ein Mikrochip ähnlich wie bei **Smart Cards**, der jedoch in ein rundes Edelstahlgehäuse mit einem Durchmesser von ca. 17 mm eingekapselt ist und an einem Schlüsselanhänger oder als Schmuck getragen werden kann. iButtons sind extrem robust, jedoch nicht mit **RFID**-Technologie für die kontaktlose Nutzung erhältlich (Stand Mai 2004).

IFPO

International Foundation for Protection Officers. Eine gemeinnützige Organisation, die mit dem Ziel gegründet wurde, standardisierte Schulungen und Zertifizierungen für Sicherheitskräfte bereitzustellen. Das *Security Supervisor Training Manual* (Schulungshandbuch für Sicherheitskräfte) ist ein Referenzhandbuch für Sicherheitsbeauftragte und ihre Mitarbeiter.

Infrarotschatten-Karte

Ein Kartentyp für die **Zugangskontrolle**, bei dem der Barcode zwischen zwei Kunststofflagen eingeschlossen ist. Der Kartenleser sendet Infrarotlicht durch die Karte, und der Schatten des Barcodes wird von den Sensoren an der Außenseite gelesen.

Iris-Scan

Ein Verfahren zur biometrischen Identifikation, mit dem das Farbenmuster der Iris des Auges gemessen wird.

Kontaktbehaftete Smart Card

Eine **Smart Card**, die mit dem Kartenleser in Kontakt kommen muss. Vgl. **kontaktlose Smart Card**.

Kontaktlose Smart Card

Eine **Smart Card**, die **RFID**-Technologie nutzt, und daher verwendet werden kann, ohne den Kartenleser zu berühren. Die maximale Entfernung vom Kartenleser wird entweder durch den **Proximity**-Bereich (10 cm) oder den **Vicinity**-Bereich (1 m) bestimmt, je nachdem, welcher der beiden RFID-Standards verwendet wird.

Magnetstreifenkarte

Ein Kartentyp für die **Zugangskontrolle**, der einen Magnetstreifen zum Speichern von Informationen verwendet, die beim Ziehen der Karte durch einen Kartenleser gelesen werden.

Management

Automatisierte Kommunikation mit entfernten Geräten für die Überwachung, Steuerung und die Ausgabe von Alarmmeldungen. Traditionell „Gebäudeautomatisierung“ bzw. „Haushaltsautomatisierung“ genannt, bezieht sich der neue Begriff *Management* auf die netzwerkbasierende Kommunikation mit allen Elementen eines Datacenters, zu denen sowohl die IT-Komponenten (Server, Speicherkomponenten, Telekommunikations- und Netzwerkgeräte) als auch die physikalische Infrastruktur (Stromversorgung, Kühlung, Brandschutz und Sicherheit) gehören.

NCPI

Physikalische Infrastruktur für hochverfügbare Netzwerke (Network-Critical Physical Infrastructure). Elemente der *physikalischen* Infrastruktur eines Datacenters (im Gegensatz zur IT-Infrastruktur, wie z. B. Router und Speichermanager), die einen direkten Beitrag zur **Verfügbarkeit** leisten, indem sie den unterbrechungsfreien Betrieb sicherstellen. Die NCPI umfasst Stromversorgung, Kühlung, Brandschutz und die **physikalische Sicherheit**.

Netzhaut-Scan

Ein Verfahren zur biometrischen Identifikation, bei dem das Muster der Blutgefäße in der Netzhaut des Auges gemessen wird.

Objektbasierte Methode

Bei der **Zugangskontrolle** eine Methode zur Identifikation, die auf einem Objekt basiert, das sich im Besitz der betreffenden Person befindet, wie z. B. eine Karte oder ein **Token**. Es ist die unsicherste Kategorie der Identifikation, weil es keine Garantie dafür gibt, dass das Objekt von der richtigen Person verwendet wird.

Physikalische Infrastruktur für hochverfügbare Netzwerke – siehe NCPI

PAC

Persönlicher Zugangscodes (Personal Access Code). Eine andere Bezeichnung für PIN (Personal Identification Number). Dabei handelt es sich um einen Code oder ein Passwort zur Identifizierung eines Benutzers an einem **Zugangspunkt**.

Physikalische Sicherheit

Der Schutz physikalischer Anlagen vor Unfällen oder Sabotage durch die Anwesenheit nicht autorisierter oder böswilliger Personen. Ein physikalisches Sicherheitssystem umfasst grundsätzlich Geräte für die **Zugangskontrolle** zur automatisierten Überprüfung des Personenverkehrs an den Zugangspunkten sowie ein sensorbasiertes Alarmsystem. Zu den zusätzlichen Schutzmaßnahmen gehören Kameraüberwachung und die Überwachung durch Sicherheitskräfte. (Der Begriff der *physikalischen Sicherheit* wird manchmal in einer allgemeineren Bedeutung verwendet und bezieht sich dann auf den Schutz vor allen möglichen Arten von physikalischen Schäden, wie beispielsweise durch Wetter, Erdbeben und Bombenangriffe. In diesem Dokument bezieht sich der Begriff nur auf die Probleme, die durch die Anwesenheit nicht autorisierter *Personen* in der Anlage verursacht werden können.)

Personenbasierte Methode

Bei der **Zugangskontrolle** eine Methode zur Identifizierung, die auf einem für eine Person eindeutigen biologischen Merkmal oder einer Verhaltensweise basiert. Diese Methode ist die sicherste Kategorie zur Identifikation, weil es sehr schwierig ist, ein solches Merkmal zu fälschen. Sie ist jedoch durch das Risiko von Lese- oder Interpretationsfehlern nicht hundertprozentig zuverlässig. Eine andere Bezeichnung für diese Art der Identifizierung ist **Biometrie**.

Proximity-Karte

Eine Karte für die **Zugangskontrolle** mit einem integrierten **RFID**-Sender-Empfänger, der die Kommunikation mit einem Kartenleser über eine Entfernung von bis zu einem Meter ermöglicht.

Proximity-Smart Card

Eine **Smart Card**, die einen Chip mit **RFID**-Technologie besitzt, der die Kommunikation mit einem Kartenleser über eine Entfernung von bis zu 10 cm ermöglicht. Wird auch als **kontaktlose Smart Card** bezeichnet.

RFID

Funkfrequenzidentifizierung (Radio Frequency Identification). Kommunikation zwischen Karte und Kartenleser ohne physischen Kontakt. **Proximity-Karten**, **Vicinity-Karten** und **kontaktlose Smart Cards** funktionieren auf der Grundlage der RFID-Technologie. Der RFID-Chip wird durch ein elektromagnetisches Feld des Kartenlesers mit Strom versorgt und benötigt daher keine Batterie.

Schablone

In der **Biometrie** die computergestützte Umwandlung eines Scans, sodass dieser für eine Person noch immer eindeutig ist, jedoch wesentlich weniger Speicherplatz beansprucht. Diese Schablone, und nicht der Scan selbst, wird in einer Datenbank von Benutzern oder auf dem Chip einer **Smart Card** gespeichert und mit dem Live-Scan an einem **Zugangspunkt** verglichen

Schwelle

In der **Biometrie** der durch den Benutzer anpassbare Parameter, der zur Anpassung der beiden Fehlerraten (**falsche Akzeptanz** und **falsche Zurückweisung**) verwendet werden kann. Da dieser Parameter für „Wie nahe ist nah genug?“ steht, wird durch das Senken einer der Fehlerraten automatisch die andere erhöht.

Sicherheitstiefe

Konzentrische Sicherheitsgrenzen mit unterschiedlichen oder aufsteigend strengeren Zugangsmethoden. Ein innerer Bereich ist daher nicht nur durch seine eigenen Zugangsmethoden geschützt, sondern auch durch die Zugangsmethoden der ihn umschließenden Bereiche, für die zuerst der Zugang erreicht werden muss.

Sicherheitsstufen

Der Umfang der Sicherheitsmaßnahmen, von niedrig bis hoch, der an konzentrischen Grenzen vorgesehen wird. Dabei ist der Schutz an der äußersten Grenze (wie z. B. dem Gebäudeeingang) am niedrigsten und an der innersten Grenze (wie z. B. dem Zugang zu einem Rack) am höchsten.

Smart Card

Ein Kartentyp für die **Zugangskontrolle**, der einen Mikrochip zum Speichern von Informationen verwendet. Der Chip speichert nicht nur Daten, sondern kann auch Berechnungen durchführen und Daten mit dem Kartenleser austauschen. Die in dem Chip gespeicherten Informationen werden gelesen, wenn die Karte an den Kartenleser gehalten wird und die elektrischen Kontakte in Berührung miteinander kommen. Siehe auch **kontaktlose Smart Card**.

Smarte Medien

Kleine Objekte beliebiger Form, die die gleiche Art von Chip enthalten, wie er in einer **Smart Card** verwendet wird. Smarte Medien sind in der Regel kleine Objekte (**Token**), die an einem Schlüsselring befestigt oder als Schmuck getragen werden können.

Social Engineering

Das gezielte Einsetzen von Täuschungsmanövern, um eine nachlässigere Haltung gegenüber Sicherheitsmaßnahmen zu erreichen, wie z. B. das Mitteilen von Passwörtern, das Verleihen von Schlüsseln oder das Öffnen von Türen.

Stimmabdruck

In der **Biometrie** die digitale Darstellung der Stimme eines Benutzers, die zum Vergleich mit der Originalstimme des Benutzers an einem **Zugangspunkt** verwendet wird.

Token

Ein kleines Objekt mit einem Mikrochip, der die persönlichen Identifikationsdaten einer Person enthält. Das Token wird mit einem Kartenleser direkt in Berührung gebracht. Bei **RFID**-Fähigkeit genügt es, das Token in die Reichweite eines Kartenlesers zu bringen.

Türschleuse

Eine schleusenartige Vorrichtung mit gesicherter Zugangs- und Ausgangstür, wobei der Raum zwischen den beiden Türen nur Platz für eine Person bietet. Die Türschleuse ist eine Lösung für die Sicherheitslücke, die das **Eindringen im Huckepack** oder **im Schlepptau** ermöglicht. Dabei passiert eine nicht autorisierte Person ungehindert einen Kontrollpunkt, indem sie einer autorisierten Person durch eine offene Tür folgt.

Verwaltbar

Ermöglicht Fernüberwachung und -steuerung. Verwaltbare Geräte für die **Zugangskontrolle** ermöglichen die Kommunikation mit einem Fernverwaltungssystem zur **Überwachung** (wer wann kommt und geht), zur **Steuerung** (Konfiguration des Geräts für den Zugang bestimmter Personen zu bestimmten Zeiten) und für **Alarmmeldungen** (Benachrichtigung bei wiederholten, nicht erfolgreichen Zugangsversuchen oder bei Gerätefehler).

Verfügbarkeit

Eine berechnete Vorhersage der verfügbaren Betriebszeit eines Netzwerks. Bei unternehmenswichtigen Anlagen wird als Ziel „Fünfmal die Neun“ bzw. 99,999 % angestrebt, d. h. weniger als fünf Minuten Ausfallzeit pro Jahr.

Vicinity-Karte

Eine Karte für die **Zugangskontrolle** mit integriertem **RFID**-Sender-Empfänger, der die Kommunikation mit einem Kartenleser über eine Entfernung von bis zu einem Meter ermöglicht.

Weigand-Karte

Ein Kartentyp für die **Zugangskontrolle**, der speziell behandelte und magnetisierte integrierte Drähte zum Speichern von Informationen verwendet, die beim Ziehen der Karte durch einen Kartenleser gelesen werden.

Wissensbasierte Methode

Bei der **Zugangskontrolle** eine Methode zur Identifikation, die auf einer Information basiert, über die eine Person verfügt, wie z. B. ein numerischer Code oder ein Passwort. Diese Methode ist sicherer als die objektbasierte Methode. Die Information kann jedoch anderen mitgeteilt oder schriftlich festgehalten und von anderen gelesen werden.

Zifferschloss

Ein Schloss, das durch Drücken der Tasten in einer bestimmten Abfolge geöffnet wird. Im Unterschied zum **Code-Schloss** hat ein Zifferschloss in der Regel nur vier bis fünf Tasten, wobei jede Taste nur einmal gedrückt werden kann. Das Zifferschloss mit Metalltasten war der mechanische Vorläufer des heutigen Code-Schlusses, das über ein telefonähnliches Tastenfeld verfügt.

Zugangskontrolle

Die Steuerung des Zugangs von Personen zu Gebäuden, Räumen und Racks sowie die Steuerung der Verwendung von Tastaturen und Geräten durch automatisierte Geräte, die die auf einem Objekt, wie z. B. einer Karte, gespeicherten Informationen lesen (**objektbasiert**), die Eingabe eines Codes oder eines Passworts erfordern (**wissensbasiert**) oder ein physisches Merkmal durch biometrische Analyse erkennen (**personenbasiert**).

Zugangspunkt

Eine Stelle entlang der Grenze eines sicheren Bereichs, an der es eine Tür und eine bestimmte Methode der **Zugangskontrolle** gibt, mit der Benutzer kontrolliert werden, die in diesen Bereich gelangen möchten.