Physische Sicherheit

Einbrechen ist auch heute immer noch im Hoch. Eine Türe nicht richtig geschlossen, ein Fenster vergessen und schon bricht jemand ein und stiehlt etwas. Das Kapitel 11 beschäftigt sich daher mit den Themen «Physische und umgebungsbezogene Sicherheit». Das Ziel formuliert sich dementsprechend: «Unbefugter Zutritt, die Beschädigung und die Beeinträchtigung von Information und informationsverarbeitenden Einrichtungen der Organisation sind verhindert.»

In einem ersten Schritt gilt es ein Zonenkonzept zu erstellen. Welches sind öffentliche Bereiche? Wo haben nur interne Personen Zutritt? Wo sind besonders sensitive Räume? Ein solches dreistufiges Modell können wie folgt aussehen:

- Schutzzone 1
  Diese Zone umfasst Räumlichkeiten, die der Öffentlichkeit frei zugänglich sind (zum Beispiel Treppenhaus, WC usw.).
- Schutzzone 2
  Beinhaltet allgemeine Büroräumlichkeiten (zum Beispiel Empfang, Aufenthaltsraum, Büros allgemein).
- Schutzzone 3
  Räume, in denen die datenverarbeitenden Systeme oder archivierte Informationen lokalisiert sind (zum Beispiel Serverräume, Archive)

Weiter gilt es zu regeln, wer wo wann Zutritt hat. Jede Person sollte dabei über einen persönlichen Schlüssel (oder Batch) verfügen, der nicht weitergegeben werden darf. Die Zutrittsrechte werden oft über einen Schlüsselplan vergeben. Bei elektronisch gesicherten Schlüsseln oder Batches kann jede Türe einzeln programmiert und damit freigegeben werden. In diesem Zusammenhang gilt es auch zu definieren, was gemacht wird, wenn jemand seinen Schlüssel vergisst oder gar verloren hat. Wie werden Ersatzschlüssel ausgegeben (die Ausgabe und Rücknahme müssen schriftlich protokolliert werden)? Wie werden Schlüssel gesperrt (oder gar alle Schloss-Zylinder ersetzt)?

Werden Besucher empfangen, sollten sich diese am Empfang melden. Je nach Grösse und Sensitivität sollte dabei ein Besucherprotokoll geführt werden. Der Empfang notiert:

- Den vollständigen Namen des Besuchers
- Firmenname
- Kontaktperson
- Uhrzeit Besuchsbeginn
- Uhrzeit Besuchsende (wird erst beim Verlassen der Räumlichkeiten notiert)
- Unterschrift des Besuchers
- Allenfalls, ob ein Ausweis kontrolliert wurde

Für mich sind solche Listen zwiespältig. Ich als Besucher sehe auf einen Blick, wer bereits da war, zum Beispiel ein Mitbewerber und ich kann mich entsprechend einstellen. Daher bevorzuge ich eine elektronische Lösung, bei welcher keine anderen Firmen und Personen sichtbar sind. Besuchern sollte im Anschluss ein Besucher-Batch abgegeben werden, der sichtbar getragen werden muss. Gleichzeitig mit dem Schlüssel sollte die Hausordnung an Mitarbeitende und allenfalls Besucher abgegeben werden:

- Welche Türen sind immer abzuschliessen?
- Wo sind spezielle Türen (zum Beispiel Brandschutztüren, Brandabschnitte)?
- Regelung mit offenen Fenstern (zum Beispiel letzte Person kontrolliert, ob alle Fenster geschlossen sind)
- Wie funktioniert die Alarmanlage (zum Beispiel Zeiten, Verhalten bei einem Alarm)?
- Verhalten in sensitiven Räumen (zum Beispiel Serverraum mit Brandlöschanlage)?
- Wie ist das Verhalten bei einem Vorfall wie Brand?
- Wo befinden sich Feuerlöscher?
- Welches sind Notausgänge? Welche speziellen Regeln gelten hier?
- Wo befindet sich der Sammelplatz?

Häufig anwesende Externe, wie Supporter sollten regelmässig an die Hausordnung erinnert werden. In immer mehr Firmen gibt es keinen Empfang mehr, sondern es steht nur noch ein Telefon bei der Eingangstüre. Eine Liste mit allen Mitarbeitenden liegt auf und man wählt selbst die gewünschte Kontaktperson. Gerade die Telefonliste, die oft auch in Sitzungszimmern liegt, ist heikel. Je nach Ort kann diese unbemerkt abfotografiert werden und die fremde Person kennt alle Personen inkl. interner Telefonnummer. Ideal für die Vorbereitung eines Phishing-Angriffs. Überlegen Sie sich, ob es allenfalls alternative Möglichkeiten gibt.

Neben dem Zonen- und Zutrittskonzept ist es wichtig Massnahmen vor externen und umweltbedingten Schäden zu treffen. Je nach Region könnten dies Brände, Überschwemmungen, Erdbeben, Explosionen, Unruhen und anderen Formen von Naturkatastrophen und vom Menschen verursachten Katastrophen sein. Die Grundschutzkataloge des BSI bietet hier eine Vielzahl von Gefahren und passenden Massnahmen (www.bsi.de/gshb/).

Je nach Gebäude und Aufgaben kommen Anlieferungs- und Ladebereiche dazu. Auch diese gilt es ins Sicherheitskonzept aufzunehmen. Diese Bereiche werden erfahrungsgemäss nicht gleich geschützt und ein potenzieller Angreifer könnte über diese unbemerkt in ein Gebäude eindringen oder dort gelagertes Material stehlen.

Sicherheitsbereiche

In Sicherheitsbereichen gelten weitere Regeln, die es zu befolgen gilt. Diese Räume sollten von aussen nicht direkt sichtbar oder beschildert sein. Lieferanten und Handwerker sind in diesen Räumen immer zu begleiten und dürfen nicht allein gelassen werden (auch nicht für fünf Minuten). Das Mitführen von Foto-, Video-, Audio- und sonstigen Aufzeichnungsgeräte, dazu gehören auch Mobiltelefonen, sollte untersagt und nur nach ausdrücklicher Genehmigung gestattet werden. Für Serverräume sollten nachfolgende Themen ebenfalls geregelt sein:

- Ausstattung
  - Doppelboden
  - Wände
  - Leitungen im Raum
  - Beleuchtung
  - Brandabschottung
  - Grösse
- Umgang mit Zutritten
- Verwaltung von Schlüsseln
- Überwachungsmassnahmen
- Brandfrüherkennung
- Brandlöschung
- Klimatisierung
- Ordnung, inklusive Lagerverbot für leicht brennbare Materialien
- Verkabelung
- Rack-Aufteilung
- Reaktion bei Vorfällen
- Alarmierung

Geräte und Betriebsmittel

Das zweite Kapitel setzt sich mit der Sicherheit von Geräten und

Betriebsmitteln auseinander. Geräte und Betriebsmittel sollten so platziert und geschützt werden, dass Risiken durch umweltbedingte Bedrohungen und Gefahren sowie Möglichkeiten des unbefugten Zugangs verringert sind.

Während sich der erste Teil um das Gebäude und den Zutritt gekümmert hat, kommen nun Massnahmen zum Schutz der Geräte und Betriebsmittel dazu. Die Norm versteht darunter auch den Zugang zu diesen Systemen. So sollten alle Systeme mit einem Login versehen sein. Geräte mit sensitiven Daten dürfen nicht frei erreichbar sein, auch nicht im Gebäude.

Unterwegs sollten Informationen nicht von Fremden vom Display abgelesen werden können, zum Beispiel mit entsprechenden Filterfolien. Die Norm geht soweit, dass jegliche Massnahmen, die vor Diebstahl, Feuer, Sprengstoff, Rauch, Wasser, Staub, Vibrationen, chemische Auswirkungen, Störungen der Stromversorgung und Telekommunikationseinrichtungen, Blitzen, elektromagnetische Strahlung und Vandalismus schützen, ergriffen werden müssen. Aber auch Temperatur und Luftfeuchtigkeit können Geräte, und damit Daten, zerstören. Dies gilt es individuell zu prüfen.

Um einen störungsfreien Betrieb sicherzustellen, gehören auch Notstrom, Überwachungen, Alarmanlagen, Notbeleuchtung oder Notrufsysteme dazu. Je nach Kritikalität gilt es eine Redundanz über zwei unterschiedliche Wege sicherzustellen.

Ein weiterer wichtiger Punkt ist die Sicherheit der Verkabelung. Dies beginnt bereits mit der Hauseinführung und endet mit der Verteilung beim entsprechenden Arbeitsplatz. Oft geschieht es, dass Leitungen durch öffentliche Räume (zum Beispiel Garage) oder Steigzonen geführt werden. Eine Manipulation könnte dabei unbemerkt erfolgen. Nicht vergessen werden dürfen auch Patch-Schränke, die oft ungeschützt platziert werden. Mindestens abgeschlossen sollten diese sein, besser sogar in einem abgeschlossenen Raum untergebracht werden.

Die Instandhaltung von Geräten ist ein weiterer wichtiger Punkt. Die empfohlenen Service-Intervalle sind einzuhalten. Gerade für kritische Elemente wie eine Klima- oder Löschanlage ist dies sehr wichtig. Die Wartung darf aber nur durch befugte Beschäftigte oder externe Spezialisten durchgeführt werden, um (unabsichtliche) Beschädigungen zu vermeiden. Müssen Geräte eingeschickt werden, zum Beispiel PCs, Notebooks, Tablets oder andere mobile Geräte, gilt es alle Daten vorher zu löschen.

Die Norm erwähnt weiter das Entfernen von Werten. Auch hier gilt es Regeln zu definieren. Wann darf ein Gerät, aber auch Informationen oder Software mitgenommen werden? Welche Vorschriften und Sicherheitsbestimmungen sind einzuhalten? Dies gilt es in einer Weisung festzuhalten. Jede Mitnahme und Rückgabe sind auf geeignete Weise festzuhalten.

Folgende Vorschriften und Bestimmungen könnten bei mobilen Geräten definiert werden:

- Falls möglich ist ein Malware-Schutzprogramm zu verwenden
- Das Gerät muss verschlüsselt werden
- Das Gerät muss einen zuverlässigen Passwortschutz unterstützen
- Der Zugriff auf Firmendaten darf nur verschlüsselt
- Das Gerät darf niemals unbeaufsichtigt bleiben und sollte – falls möglich – bei Nichtbenutzung stets weggeschlossen werden
- Unberechtigte Personen dürfen keinen Zugriff auf enthaltene Daten haben
- Patches und Software-Aktualisierungen müssen regelmässig installiert werden
- Verboten ist die Speicherung illegaler Daten auf dem Gerät
- Verboten ist die Installation nicht-lizenzierter (illegaler) Software
- Endgeräte dürfen nicht mit «Jailbreak» und «Root»-Zugriff «geknackt» werden

Jedes Gerät kommt irgendwann an sein Lebensende. Auch für diesen Fall gilt es einige Überlegungen anzustellen. Wie werden Geräte entsorgt? Wird ein spezialisiertes Unternehmen beigezogen? Wie werden Daten von den Geräten entfernt? Oder wird gar der Datenträger sicher zerstört, zum Beispiel nach der DIN-Norm 66399? Sind die Daten nach einem aktuellen Verfahren verschlüsselt, kann nach erfolgter Risiko-Analyse ein defektes Gerät auch ohne Löschung entsorgt werden.

In einigen Firmen gibt es unbeaufsichtigte Geräte, zum Beispiel Empfangsmonitore, Self Service Portale oder ähnliches. Auch diese gilt es ins Sicherheitskonzept aufzunehmen. Mit diesen Geräten darf es nicht möglich sein, auf sensitive Daten zuzugreifen, da diese nicht unter ständiger Aufsicht sind. Idealerweise sind diese in einer eigenen, eingeschränkten Netzwerkzone untergebracht.

Die letzte Massnahme lautet «Richtlinien für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren». Damit ist schlicht und einfach ein aufgeräumter Arbeitsplatz und das Sperren des Computers gemeint. In vielen Audits und Kontrollen sehe ich immer wieder, dass der Arbeitsplatz verlassen wird, ohne den Computer zu sperren. Auch wenn nach einigen Minuten die automatische Sperre einsetzt, kann ein Fremder diese Zeit nutzen, und den Computer missbrauchen. Dabei wäre es so einfach: bei Windows: Win + L, beim Mac: Ctrl + Shift + Eject. Zum Glück besser sieht es bei der Ordnung am Arbeitsplatz aus. Hier wird abends alles korrekt verschlossen aufbewahrt. Nicht vergessen werden dürfen aber längere Abwesenheiten wie Kaffee-Pause, ein Meeting usw. Auch hier müssen sensitive Daten aufgeräumt, besser verschlossen, werden.

Werden die Punkte aus dem Kapitel A.11 korrekt umgesetzt, kann die physische Sicherheit des Gebäudes und von Geräten nachhaltig erhöht und ein sicherer Betrieb gewährleistet werden.

INFOS | KONTAKT

goSecurity GmbH
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch