

Unternehmenssicherheit: Schützen Sie die sensitiven Räume Einbruch, Zutritt und Spionage

Andreas Brönnimann

In den meisten Firmengebäuden gibt es sensitive Räume, die aufgrund ihrer Nutzung erhöhter Sicherheit bedürfen. Ein Beispiel dafür sind die Räumlichkeiten für Forschung und Entwicklung. Datendiebstähle oder Sachbeschädigung können hier verheerende Auswirkungen für das ganze Unternehmen haben. Es gilt daher, die nötigen Vorsichtsmassnahmen umzusetzen.

Die Sicherheit eines Unternehmens zu gewährleisten, ist eine komplexe Aufgabe für die Geschäftsleitung. Zahlreiche verschiedene Aspekte müssen berücksichtigt und aufeinander abgestimmt werden. Da die Sicherheitsbedürfnisse von Unternehmen zu Unternehmen meist unterschiedlich sind, bedarf es individueller Massnahmen.

Unbefugter Zutritt

Ein grundsätzliches Bedürfnis vieler Geschäftsleitungen ist es, dass das bzw. die Firmengebäude gegen unbefugten Zutritt abzusichern. Dafür braucht es primär mechanischen Einbruchschutz. Dieser sorgt dafür, dass Unbefugte nicht innert nützlicher Frist eindringen können. Dazu gehören insbesondere Tür- und Fenstericherungen sowie Sicherheitsglas oder Glas mit Sicherheitsfolien. Die mechanischen Einbruchschutz-Massnahmen können durch den Einsatz von elektronischen Meldesystemen sinnvoll ergänzt werden. So eignen sich beispielsweise Alarmanlagen und Videokameras zur

Prävention, Meldung und Aufklärung von unbefugten Zutritten.

Sensitive Räume

Beim Innenbereich von Firmengebäuden ist grundsätzlich zwischen allgemeinen und sensitiven Räumen zu differenzieren. Während allgemeine Räume (z.B. Putzraum, Pausenraum) grundsätzlich nicht sonderlich geschützt werden müssen, verlangen sensitive Räume aufgrund ihrer Nutzung erhöhte Sicherheit. Dies sind beispielsweise Räume für Server, Buchhaltung



oder Forschung und Entwicklung. Für jedes Unternehmen ist individuell festzulegen, welches die sensitiven Räume sind. Um diesbezügliche Entscheidungen zu treffen, können sich die Sicherheitsverantwortlichen beispielsweise verschiedene Szenarien vor Augen führen: Welche Folgen könnte es haben, wenn Forschungsergebnisse in die Hände von Unbefugten gelangen? Was hat es für Konsequenzen, wenn in unserem Betrieb der Server einen Tag lang ausfällt oder Daten verloren gehen? Be-

züglich Datenverlust ist zu erwähnen, dass gemäss Berechnungen des Multi-Technologiekonzerns 3M die Rekonstruktionskosten pro Gigabyte Daten ca. 2,5 Millionen Schweizer Franken betragen. Sind die sensitiven Räume einmal bestimmt, geht es darum, die Gefährdungssituation genau zu analysieren, die Sicherheitsanforderungen zu bestimmen und ein detailliertes Sicherheitskonzept zu erstellen. So ein Konzept sollte unbedingt durch Fachleute erstellt werden, um sicherzustellen, dass alle relevanten Aspekte bedacht und angemessen berücksichtigt werden.

Kontrollierter Zugang

Der Zugang zu einem Unternehmen, respektive dessen sensitive Räume und damit zu vertraulichen Unternehmensinformationen muss klar geregelt sein. Aus diesem Grund entscheiden sich viele Geschäftsleitungen für die Installation eines Zutrittskontrollsystems (ZUKO). Ein ZUKO alleine kann jedoch die Unternehmenssicherheit nicht garantieren. Neben technischen sind organisatorische Massnahmen unerlässlich! Denn was passiert beispielsweise, wenn ein Handwerker auftaucht und sagt, er sei bestellt worden, um die Spannung der Steckdosen im Raum für Forschung und Entwicklung zu überprüfen? Wer kontrolliert, ob er tatsächlich bestellt wurde und wenn ja, wer überprüft seine Identität? Wer kontrolliert ihn bei der Arbeit und wer übernimmt die Kontrollen, wenn der zuständige Mitarbeiter abwesend ist? Konkurrenzspionage geschieht oft nicht durch einen gewaltsamen Einbruchdiebstahl, sondern die Spione verschaffen sich mittels eines Vorwands Zugang zu sensitiven Räumen und kritischen Informationen. Für Unternehmen ist es daher sehr wichtig, die Zuständigkeiten für die Zutrittskontrolle externer Personen zu organisieren.

Der Ratgeber wird betreut von:



BST Sicherheitstechnik AG

Lagerhausweg 10, 3018 Bern

Tel. 031 997 10 10

Fax 031 997 55 50

info@bst-sicherheitstechnik.com

<http://www.bst-sicherheitstechnik.com>