

## Zusammenfassung

Ein Dieb ergattert sich anderer Leute Güter ohne deren Einwilligung oder Wissen. Ein solcher Diebstahl kann ebenfalls alle Bereiche einer EDV-Infrastruktur betreffen.

Dieser Diebstahl kann innerhalb eines Firmengebäudes oder während dem Transport von EDV-Material ausgeführt werden. Wie der Diebstahl, kann auch der Verlust von EDV-Material grosse Auswirkungen auf die betreffende Person haben.

## Inhalt

- 1 Was versteht man unter physikalischer Sicherheit? →
- 2 Was versteht man unter vorbeugenden Maßnahmen und Schutzmaßnahmen? →
- 3 Das Rechenzentrum - gibt es Unterscheidungsmerkmale? →
- 4 Wie kann man sich vor Vorfällen schützen? →



### 1 Was versteht man unter physikalischer Sicherheit?

Die physikalische Sicherheit hat zum Ziel, den Betrieb der EDV-Geräte unter optimalen Betriebsbedingungen zu ermöglichen, um die maximale Leistung über einen größtmöglichen Zeitraum zu gewährleisten.

### 2 Was versteht man unter vorbeugenden Maßnahmen und Schutzmaßnahmen?

Wenn man von Maßnahmen spricht, muss man zwischen vorbeugenden Maßnahmen und Schutzmaßnahmen unterscheiden.

- Die vorbeugenden Maßnahmen haben zum Ziel, das Eintreten eines Schadensfalls zu verhindern.
- Die Schutzmaßnahmen haben zum Ziel, das Eigentum bei Eintreten eines Schadensfalls zu schützen.

Es ist illusorisch, anzunehmen, dass die vorbeugenden Maßnahmen jegliche Schadensfälle unmöglich machen. Selbst bei der Durchführung dieser Art von Maßnahmen empfiehlt es sich, zusätzliche Schutzmaßnahmen zu ergreifen.

Das Ausmaß der erforderlichen Schutzmaßnahmen ist umgekehrt proportional zu den ergriffenen vorbeugenden Maßnahmen.

### 3 Das Rechenzentrum - gibt es Unterscheidungsmerkmale?

Aus den verschiedensten Gründen, die mit dem Gerätetyp, den Betriebsbedingungen, ihrer Kritikalität, den ausgesendeten Störungen oder der abgestrahlten Wärme etc. zusammenhängen, ist es vernünftig, spezielle Rechenräume einzurichten, die von den Arbeitsflächen, die von den Arbeitnehmern genutzt werden, getrennt sind.

Es lassen sich verschiedene Rechenraum-Typen unterscheiden:

## 3.1 Rechenraum des Typs

In diesem Raum sind normalerweise alle speziellen Geräte untergebracht, die für die Bereitstellung von EDV-Ressourcen erforderlich sind. Hier befinden sich die Server, Großrechner, die Lösungen zur Datensicherung und -wiederherstellung, Speicherracks etc.

In den meisten mittelständischen Unternehmen enthält dieser Raum auch die für den Netzbetrieb kritischen Komponenten (Switches, Router etc.) sowie die Zugangspunkte und Geräte, die zur Verbindung des Unternehmens mit der Außenwelt dienen (Telefonzentrale, Internet-Zugang etc.).

Bei größeren Infrastrukturen sind diese Ausrüstungen auf verschiedene Räume wie beispielsweise den Netzwerkraum, den Fernmelderaum und den Anschlussraum aufgeteilt.

In sehr großen Rechenzentren wird sogar zwischen dem «Totraum», in dem sich die Ausrüstungen befinden, die nur selten einen Eingriff durch den Menschen erfordern (Prozessoren, Speichereinrichtungen etc.), und dem «Lebendraum», in dem sich alle Ausrüstungen befinden, die häufig eines Eingriffs durch den Menschen bedürfen (Backup-Automat etc.), unterschieden.

## 3.2 Etagen-Anschlussraum

Auf Etagenebene befinden sich üblicherweise Räume, in denen die auf der jeweiligen Etage befindlichen Geräte über einen gemeinsamen Kabelbaum mit dem EDV-Raum verbunden werden. Diese Räume enthalten üblicherweise Stecktafeln sowie Etagen-Switches.

Diese Räume und die Verbindungstechnik werden normalerweise mit einer maximalen Redundanz eingerichtet, um mögliche Unterbrechungen so weit wie möglich einzuschränken.

## 4

# Wie kann man sich vor Vorfällen schützen?

Die in diesem Dokument beschriebenen vorbeugenden Maßnahmen und Schutzmaßnahmen erheben weder den Anspruch auf Vollständigkeit, noch sind sie in allen Fällen unbedingt erforderlich. Die Auswahl der zu ergreifenden vorbeugenden Maßnahmen und Schutzmaßnahmen muss abhängig von einer Untersuchung erfolgen, die eine Risikoanalyse beinhaltet und eine Einschätzung der Kosten der zu ergreifenden Maßnahmen berücksichtigt.

Um die Effizienz aller vorbeugenden Maßnahmen und Schutzmaßnahmen zu gewährleisten, ist es erforderlich, sie im Rahmen eines organisationellen und verfahrensorientierten Konzepts zu integrieren.

Die folgenden Aspekte werden in diesem Kapitel behandelt:

- ➔ Wasserschäden.
- ➔ Brandschäden.
- ➔ Stromschäden.
- ➔ Schäden aufgrund falscher Klimatisierung.
- ➔ Vorfälle im Zusammenhang mit der Telekommunikation.
- ➔ Physikalisches Eindringen.
- ➔ Elektrostatische Phänomene.
- ➔ Unzugänglichkeit des Rechenzentrums.

## 4.1 Wasserschäden

### 4.1.1. VORFÄLLE

Diese Art von Vorfällen können verschiedenste Ursachen wie beispielsweise die nachfolgend aufgeführten haben:

- ➔ Bruch einer Haushaltswasserleitung.
- ➔ Bruch einer Kühlleitung.
- ➔ undichte Fassade oder undichtes Dach.
- ➔ Auslösung von Sprinkleranlagen.
- ➔ Verstopfung der Abwasserleitungen.

### ➔ HINWEIS:

Dieser Punkt ist umso kritischer, da die meisten EDV-Räume mit Zwischendecken ausgestattet sind, die keine einfache Schadenserkenkung ermöglichen. Außerdem sind die Ummantelungen der Kabel zwischen den Etagen ideale Abflüsse für das Wasser, das sich so in alle Anschlussräume ausbreiten kann.

## 4.1.2. FOLGEN

Die Folgen hängen natürlich vom Ausmaß des Schadens ab, aber man kann davon ausgehen, dass folgende Bereiche betroffen sind:

- ➔ verschiedene Kurzschlüsse, die zu einem Ausfall der Geräte führen,
- ➔ Gefahr eines tödlichen Unfalls durch elektrischen Strom.
- ➔ Funktionsstörung gewisser Alarmer und sonstiger Sicherheitseinrichtungen, dysfonctionnement
- ➔ Beschädigung von Geräten.
- ➔ Korrosion von Kabeln und Steckverbindern.

## 4.1.3. GEGENMAßNAHMEN

### Prévention

- ➔ Wählen Sie den Standort der EDV-Räume sorgfältig aus und vermeiden Sie dabei das Risiko einer Überschwemmung (vermeiden Sie Untergeschosse, das oberste Stockwerk etc.).
- ➔ Schränken Sie den Wasserumlauf im EDV-Raum ein (bringen Sie das Klimatisierungsaggregat außerhalb des EDV-Raums an etc.).
- ➔ Verlegen Sie das Rohrleitungsnetz so, dass der EDV-Raum nicht durchquert wird oder die Leitungen in den Raum hineinragen.

### Schutzmaßnahmen:

- ➔ Bringen Sie Systeme zur Erkennung von Undichtheiten an.
- ➔ Stellen Sie die EDV-Geräte an einer höherliegenden Position auf (nicht auf dem Boden).
- ➔ Verwenden Sie hermetische Rohre für die Netzkabel (220 V) sowie für die Netzkabel.
- ➔ Unterteilen Sie die Geschosdecke so, dass das Wasser zu Ableitungssystemen geführt wird.

## 4.2 Brandschäden

### 4.2.1. VORFÄLLE

Diese Art von Schäden können unabhängig davon, ob es sich um einen Unfall oder um Brandstiftung handelt, zur teilweisen Zerstörung des Unternehmens und insbesondere der EDV-Ausstattungen führen.

### 4.2.2. FOLGEN

Die Folgen dieser Schadensart können nicht nur auf der Ebene der elektronischen Datenverarbeitung sondern in allen Unternehmensbereichen ein beträchtliches Ausmaß erreichen. In Bezug auf das EDV-System kann ein Brandschaden über einen längeren Zeitraum zur vollständigen oder teilweisen

Nichtverfügbarkeit der Architektur führen. Die Schäden sind häufig mit Wasserschäden durch das Löschwasser und durch von den Rauchgasen verursachte Schäden verbunden.

### Die üblicherweise festgestellten Schäden sind ganz unterschiedlicher Art:

- ➔ vollständige oder teilweise Zerstörung des Rechenzentrums.
- ➔ vollständige oder teilweise Zerstörung der Kupfer- und LWL-Verkabelung.
- ➔ Schäden, die durch die Rauchgase und die Löschmittel verursacht werden,
- ➔ physikalische Beschädigungen an den EDV-Geräten.

## 4.2.3. GEGENMAßNAHMEN

### Vorbeugende Maßnahmen

- ➔ Berücksichtigen Sie die Umgebung der Gebäude.
- ➔ Vermeiden Sie eine Lagerung von feuergefährlichen Produkten in oder in der Nähe von EDV-Räumen.
- ➔ Überprüfen Sie regelmäßig die elektrischen Schaltkreise.
- ➔ Vermeiden Sie die Aneinanderreihung von Mehrfachsteckdosen.
- ➔ Bringen Sie Rauchmelder an.
- ➔ Ermitteln Sie mögliche Brandausbreitungswege und planen Sie Abschottungen ein (Luftscheunen, Brandschutzmauern etc.).

### Schutzmaßnahmen:

- ➔ Installieren Sie Löscheinrichtungen an, die zu keiner Beschädigung der EDV-Geräte und zu keinem Personenschaden führen können (erkundigen Sie sich bei der Feuerwehr vor Ort).
- ➔ Wählen Sie die Notausgänge sorgfältig aus.
- ➔ Achten Sie auf die Einhaltung des Rauchverbots.
- ➔ Erstellen und proben Sie einen Katastrophenplan, der eine Auslagerung der Informationen an ein spezielles Datenzentrum beinhaltet.
- ➔ Verwenden Sie feuerfeste Schränke für die Lagerung der Datenträger (achten Sie darauf, dass diese Schränke immer verschlossen sind).

## 4.3 Stromschäden

### 4.3.1. VORFÄLLE

Stromschäden können infolge von Störungen der Stromversorgung auftreten, die sich in Form von Überspannungen, Spannungsabfällen bzw. Stromausfällen äußern können. Diese Art des Ausfalls kann das gesamte Unternehmen oder einen Teil hiervon betreffen und interne oder externe Ursachen haben.

Leider sind das Auftreten und die Dauer dieser Phänomene mit Ausnahme der vom Versorgungsunternehmen oder dem Gebäudetechnikdienst angekündigten Abschaltungen der Stromversorgung nicht vorhersehbar. Ein Stromausfall kann mit bösen Absichten erfolgen oder durch eine Fehlhandlung bedingt sein, jedoch auch durch Naturereignisse wie etwa Gewitter, Stürme etc. hervorgerufen werden.

#### 4.3.2. FOLGEN

Die Gefahr einer Beschädigung hängt von der Stärke des Stromausfalls ab, denn bestimmte Geräte sind in der Lage, diesen Phänomenen entgegenzuwirken, indem Sie die laufenden Transaktionen vor dem Ausfall noch ordnungsgemäß beenden.

##### Folgen :

- ➔ Datenverlust.
- ➔ Geräteausfall.
- ➔ Brandgefahr.
- ➔ Gefahr eines tödlichen Unfalls durch elektrischen Strom.

##### HINWEIS :

Es sei darauf hingewiesen, dass die auf die Etagen verteilten Anschlussgeräte sowie die Personal Computer und Peripheriegeräte auch kritische Geräte sind, die häufig anfällig gegenüber Stromausfällen sind.

#### 4.3.3. SCHUTZMAßNAHMEN

##### Vorbeugende Maßnahmen

- ➔ Achten Sie bei der elektrischen Verkabelung auf eine redundante Ausführung der Speisestromkreise.
- ➔ Achten Sie auf eine angemessene Auslegung der Stromversorgung (Tabellen, Stärke etc.)
- ➔ Statten Sie kritische Elemente des EDV-Systems mit einer doppelten Stromversorgung aus.
- ➔ Vermeiden Sie eine Aneinanderreihung von Mehrfachsteckdosen.
- ➔ Statten Sie das Gebäude mit einem Mechanismus aus, der den Aufbau von «Blitzen» verhindert.
- ➔ Installieren Sie Blitzschutzanlagen.

##### Schutzmaßnahmen:

- ➔ Installieren Sie Sicherheitskreise für den Fall eines Stromausfalls (Notstromaggregat).
- ➔ Installieren Sie so genannte «no break»-Schaltkreise im gesamten Gebäude, um dort anfällige Hardwareausrüstungen und Peripheriegeräte anzuschließen.

- ➔ Verwenden Sie UPS-Lösungen (Uninterruptible Power Supply) mit Alarmsoftware in den Räumen, die nicht über ein Notstromaggregat versorgt werden können.

##### HINWEIS :

Es lässt sich häufig feststellen, dass sich das Stromausfallproblem bei Wiederherstellung der Stromversorgung fortsetzt. Es ist tatsächlich so, dass der gleichzeitige Neustart aller Geräte zu einer Überlastung und letztendlich zum Durchbrennen der Sicherungen führt. Daher wird ein schrittweiser Neustart der Geräte empfohlen.

#### 4.4

### Schäden aufgrund falscher Klimatisierung

#### 4.4.1. VORFÄLLE

EDV-Geräte sind für den Betrieb unter ganz bestimmten Umgebungsbedingungen konzipiert. Diese Umgebungsbedingungen müssen berücksichtigt und eingehalten werden, um folgende Schäden zu vermeiden:

- ➔ Funktionsstörung der Wasser- oder Stromversorgung.
- ➔ Ausfall oder Funktionsstörung des Kühlsystems.
- ➔ Effets du rayonnement solaire direct.

#### 4.4.2. FOLGEN

Die Einhaltung der normalen Betriebsbedingungen ist zu beachten, da ansonsten die verschiedensten und nur schwer zu diagnostizierenden zufälligen Funktionsstörungen auftreten können. Die üblichen Folgen einer fehlerhaften Klimatisierung sind jedoch:

- ➔ die Notwendigkeit, die Geräte in regelmäßigen Abständen ausschalten und neu starten zu müssen.
- ➔ eine vorzeitige Alterung und damit eine verkürzte Gesamtnutzungsdauer der EDV-Geräte.
- ➔ eine Beeinträchtigung der Leistung der Pufferbatterien der unterbrechungsfreien Stromversorgung

#### 4.4.3. SCHUTZMAßNAHMEN

##### Vorbeugende Maßnahmen

- ➔ Installieren Sie Vorrichtungen zur Einschränkung der direkten Sonneneinstrahlung.
- ➔ Installieren Sie ein redundantes Belüftungssystem, das ausreichend dimensioniert ist, um den aktuellen und zukünftigen Anforderungen zu entsprechen.
- ➔ Installieren Sie eine Lösung zur Temperaturüberwachung, die mit einer Alarmvorrichtung ausgestattet ist.

## 4.5 Vorfälle im Zusammenhang mit der Telekommunikation

### 4.5.1. VORFÄLLE

Zu dieser Art von Vorfällen zählen unter anderem:

- ➔ Sabotage.
- ➔ Geräteausfall oder -verlust.
- ➔ Signalstörungen.
- ➔ Trennung von Verbindungskanälen.
- ➔ Ausfall des Dienstes eines Anbieters.
- ➔ Ausfall einer Vermittlungsstelle.

In diese Kategorie werden üblicherweise andere Vorfälle als die, welche einen direkten Einfluss auf die physikalischen Elemente haben, eingestuft. Hierzu zählt beispielsweise das Eindringen in EDV-Systeme. Diese Vorfälle werden im vorliegenden Dokument jedoch nicht behandelt.

### 4.5.2. VORFÄLLE

Die Auswirkungen hängen logischerweise von der Nutzung der in den kritischen Produktionsketten betroffenen Dienste ab.

**Es können sich folgende Konsequenzen ergeben:**

- ➔ Ausfall bestimmter Softwareprogramme.
- ➔ Isolation des Unternehmens gegenüber der Außenwelt.
- ➔ Mögliche Beschädigung der Daten.
- ➔ Trennung von Verbindungskanälen.
- ➔ Deaktivierung bestimmter Überwachungseinrichtungen (Video, Alarm etc.).

### 4.5.3. SCHUTZMAßNAHMEN

**Vorbeugende Maßnahmen**

- ➔ Schützen Sie sorgfältig die Telekommunikationsräume.
- ➔ Verwenden Sie geschirmte, ummantelte Kabel für die externen Verbindungen (Schirmung, Warnung, Klemmen etc.).
- ➔ Trennen Sie die Ummantelungen von Starkstrom-, Schwachstrom und Klimatisierungsleitungen.
- ➔ Schützen Sie Kommunikationseinrichtungen (Antennen etc.) gegen Blitzschlag.

**Schutzmaßnahmen:**

- ➔ Richten Sie doppelte und über verschiedene Vermittlungsstellen laufende Verbindungen mit getrennten Zugriffspfaden ein.
- ➔ Installieren Sie kritische Komponenten doppelt und richten Sie ein System zur Lastverteilung ein.
- ➔ Richten Sie, sofern dies möglich ist, Ersatzverbindungen ein.
- ➔ Schulen Sie mehrere Bediener für die Gewährleistung des Übergangs bei einem Ausfall des Dienstes.

## 4.6 Physikalisches Eindringen

### 4.6.1. VORFÄLLE UND AUSWIRKUNGEN

Der Aufenthalt von unbefugten Personen in den EDV-Räumen (und in den Räumlichkeiten des Unternehmens) kann verschiedene unerwünschte Vorfälle wie beispielsweise die nachfolgend aufgeführten zur Folge haben:

- ➔ Diebstahl von Geräten.
- ➔ Aufhebung der Geheimhaltung.
- ➔ Sabotage.

### 4.6.2. FOLGEN

**Es können sich folgende Konsequenzen ergeben:**

- ➔ Ansehensverlust (Infragestellung der Glaubwürdigkeit im Fall einer Verbreitung streng vertraulicher Informationen etc.).
- ➔ unmittelbare finanzielle Verluste (Zerstörung entscheidender Daten, Außerbetriebsetzung des gesamten EDV-Systems etc.).
- ➔ Zeitverlust (Aufwand für die Wiederherstellung der zerstörten Daten etc.).

### 4.6.3. SCHUTZMAßNAHMEN

Gerade in diesem Bereich ist es unerlässlich, alle Maßnahmen in einen organisations- und verfahrenstechnischen Audit-Plan zu integrieren.

**Vorbeugende Maßnahmen**

- ➔ Richten Sie einen allgemeinen Gebäudeschutz (Abschirmung, «Bunker» etc.) mit einer begrenzten Anzahl an Zugängen (Fenster, Türen etc.) ein.
- ➔ Nutzen Sie ein System zur Bewegungs- und Eindringungserkennung, das mit einer rund um die Uhr besetzten Überwachungszentrale verbunden ist.
- ➔ Installieren Sie ein Zugangskontrollsystem (Badge, Biometrie etc.), das die Überwachung und Rückverfolgung des Zugangs zu kritischen Räumen ermöglicht.
- ➔ Entwickeln Sie eine Politik zur Identifikation von Besuchern.

## Schutzmaßnahmen:

- Verwenden Sie Diebstahlschutzvorrichtungen für die Peripheriegeräte und PCs oder tragbaren Computer.
- Achten Sie auf die Einhaltung einer so genannten «Clean Desk-Politik, die ein Mittel zur maximalen Einschränkung des Risikos eines Daten- oder Gerätediebstahls darstellt.
- Installieren Sie ein Video-Überwachungssystem.

### HINWEIS :

Holen Sie sich vor der Einführung dieser Überwachungsmaßnahmen die Genehmigung bei der Nationalen Kommission für den Datenschutz ein.  
(Art. 11 des Gesetzes vom 2 August 2002)

## 4.7 Elektrostatische Phänomene

### 4.7.1. VORFÄLLE

Unter diesem Begriff sind alle elektromagnetischen und elektrostatischen Phänomene zusammengefasst.

Diese Störungen können im Fall von meteorologischen Phänomenen von einer unternehmensexternen Quelle stammen oder auf Emissionen von Funkgeräten oder anderen elektrischen Geräten beruhen. Die Quelle kann jedoch auch mit dem Gebäude in Verbindung stehen.

### 4.7.2. FOLGEN

Es können sich folgende Konsequenzen ergeben:

- zufällige Funktionsstörungen.
- Beschädigung der auf magnetischen Datenträgern gespeicherten Daten.

### HINWEIS :

Ein anderes Phänomen ist die Nutzung der vom EDV-System gesendeten Strahlungen zum Abfangen von Daten. Dies ist beispielsweise bei «drahtlosen» Netzwerken der Fall.

### 4.7.3. SCHUTZMAßNAHMEN

#### Maßnahmen

- Richten Sie die EDV-Räume (Verarbeitung und Anschluss) in ausreichender Entfernung von Elektroinstallationen, Aufzügen und anderen Störquellen ein.

- Verwenden Sie LWL für vertikale Verbindungen (z.B. zwischen den verschiedenen Etagen), um so die Risiken einzuschränken,
- Erden Sie alle Geräte und nicht nur die Komponenten des EDV-Systems,
- Wählen Sie die Bodenbeläge mit Bedacht aus.

## Schutzmaßnahmen:

- Tragen Sie bei allen Eingriffen an der EDV-Architektur Erdungsarmbänder.

## 4.8 Unzugänglichkeit des Rechenzentrums

### 4.8.1. VORFÄLLE

Der Zugang zum Rechenzentrum kann aus den verschiedensten Gründen wie beispielsweise den nachfolgend aufgeführten unmöglich sein:

- Naturkatastrophen und Attentate.
- Richterliche Entscheidung infolge eines Schadensfalls.
- Demonstrationen, Unruhen und gesellschaftliche Bewegungen.

### 4.8.2. FOLGEN

Die Folgen eines gesperrten Zugangs zum EDV-System können verschiedenster Art sein:

- Unterbrechung des Betriebs des Rechenzentrums.
- Einschränkung der ordnungsgemäßen Funktionsweise des Systems und insbesondere der sensiblen Geräte.

### 4.8.3. SCHUTZMAßNAHMEN

#### Vorbeugende Maßnahmen:

- Wählen Sie Ihre Standorte dort, wo die Gefahr von Naturkatastrophen gering ist.
- Richten Sie Schutzmaßnahmen gegen Eindringlinge ein.

#### Schutzmaßnahmen:

- Installieren Sie eine sichere Lösung zur Übernahme der Kontrolle per Fernzugriff.
- Planen Sie die Möglichkeit der Umschaltung zu einem Ausweichstandort ein.