# 1. Allgemeine Gefährdungen

**Beginnen wir dieses Kapitel mit einem Beispiel:**

Es ist ein Tag wie jeder andere. Frau Susanne Müller beginnt ihre tägliche Arbeit in einem Anwaltsbüro in Basel. Noch weiß sie nicht, was sich heute anbahnen wird.

Susanne Müller will ihre Arbeit von gestern beenden, ein Vertrag für ein wichtiges Geschäft. Sie öffnet wie gewohnt den Aktenschrank und sucht die entsprechende Diskette. Auf einen Blick sieht sie, dass die Diskette weg ist und Unordnung herrscht. Sie denkt sofort: «Da stimmt doch was nicht» und informiert den Chef. Beide gehen von einer vorsätzlichen Handlung aus.

Nach langem Suchen finden sie die Diskette auf dem Pult ihrer Arbeitskollegin. Diese hatte gestern Abend die Diskette geholt, um einen Ausdruck des Vertrages zu machen. Es ist ein organisatorischer Mangel, dass die Diskette nicht mehr richtig versorgt wurde.

Beruhigt will sie die Diskette einlegen und die Datei laden, aber das Laufwerk rührt sich nicht. Ein technisches Versagen liegt am Diskettenlaufwerk vor.

Sie ruft den Servicetechniker an. Doch dieser kann mit dem Wagen nicht aus der Garage, da gerade das Fußball- Endspiel Basel–GC läuft und die Fußballfans ihre Fahrzeuge wild parkiert haben. Es liegt höhere Gewalt vor, dass der Schaden nicht sofort behoben werden kann.

Gefährdungen (Bedrohungen) können in folgende «Bedrohungsbilder» eingeteilt werden:

* Höhere Gewalt
* Menschliche Fehlhandlungen
* Technisches Versagen
* Vorsätzliche Handlungen
* Organisatorische Mängel

Diese Einteilung findet nicht nur im IT-Grundschutz Gebrauch, sondern in allen Bereichen, die sich mit Sicherheit und Schadensfällen befassen. Als Beispiel sind hier Versicherungen zu nennen. Es ist ein w eit verbreiteter Ansatz, Bedrohungsbilder zu standardisieren, um die Komplexität zu reduzieren. Sämtliche Gefährdungen bzw . Bedrohungen lassen sich in diese Kategorien einteilen. Nachfolgend ein Beispiel:

**Beispiel**

Heinz Knut arbeitet in einem Rechenzentrum. Er will wie jeden Morgen um 8 Uhr seine Arbeit beginnen.

Als er zu seiner Arbeit fährt, gerät er auf der Autobahn in ein Sommergewitter und innerhalb kurzer Zeit ist die Autobahn stellenweise unter Wasser, so dass er rund zwei Stunden festsitzt. Es handelt sich um höhere Gewalt, dass er nicht an seinem Arbeitsplatz erscheinen und somit seine Arbeit aufnehmen kann.

Ein wenig entnervt nimmt er seine Arbeit auf und verwechselt ein Tape zur Datensicherung, womit er aus Ver- sehen produktive Daten überschreibt. Es handelt sich um eine menschliche Fehlhandlung.

Nach dieser Aufregung holt er sich einen Kaffee und versucht von diesem Tag zu retten, was noch übrig ist.

Eine halbe Stunde später stürzt ein Server ab. Ursache: defekter Prozessor. Es handelt sich um ein technisches Versagen.

Er überlegt, was wohl passieren würde, wenn er vor lauter Wut den Server zum Fenster rauswerfen würde. Da es sich um eine vorsätzliche Handlung handeln würde, ist dies kein gangbarer Weg und so beginnt er den Server zu reparieren.

Der restliche Tag verläuft ruhig und er beginnt endlich seine E-Mails zu lesen. Rund 120 E-Mails sind angekommen. Die meisten beinhalten belanglose Informationen wie zum Beispiel Witze, Protokolle von Meetings, an denen er niemals teilgenommen hat, Umfragen, wer Weltmeister im Formel 1 wird, und so weiter. Er findet,

dass endlich jemand regeln sollte, dass solche Mails nicht verschickt werden, da er genügend andere Aufgaben hat. Er hat Recht, denn es handelt sich um einen organisatorischen Mangel.

Im Anhang finden Sie einen detaillierten Gefährdungskatalog für die einzelnen Bereiche. Dieser Anhang soll einen repräsentativen Querschnitt über die möglichen Bedrohungen aufzeigen, hat aber keinen Anspruch auf Vollständigkeit.

# 2.1 Gefährdungskatalog höhere Gewalt

➔ Siehe auch Anhang

Wie aus dem Anhang ersichtlich, umfasst höhere Gew alt alle Gefährdungen, die nicht oder nur bedingt beeinflusst w erden können. Im Vordergrund stehen Umw elteinflüsse w ie Naturkatastrophen. Um sich gegen höhere Gew alt zu schützen, müssen in den meisten Fällen M aßnahmen im Infrastrukturbereich gew ählt w erden.

**Zum Beispiel**

* Unterbrechungsfreie Stromversorgung
* Brandschutzeinrichtungen (inkl. Alarmierung)
* Aufgeräumte Rechenzentren
* Klimaeinrichtungen

Ergänzend dazu w erden Notfallkonzepte benötigt.

# 2.2 Gefährdungskatalog menschliche Fehlhandlungen

➔ Siehe auch Anhang (S. 92)

Bei der menschlichen Fehlhandlung stehen die Grenzen des menschlichen Denkvermögens im Mittelpunkt. Dabei wird davon ausgegangen, dass keine vorsätzliche Absicht hinter der Fehlhandlung steckt. Die Hauptursachen für menschliche Fehlhandlungen sind vor allem Unwissenheit, Unachtsamkeit und zu große Komplexität. Hierfür stehen folgende Gegenmaßnahmen im Vordergrund:

* Schulung (Sicherheit beginnt im Kopf)
* Sichere Applikationsfunktionen zur Verhinderung von Fehlmanipulationen
* Umfangreiche Testszenarien
* Restriktive Access Control
* Vertretungsregelungen

# 2.3 Gefährdungskatalog technisches Versagen

➔ Siehe auch Anhang (S. 92)

Unter technischem Versagen werden Gefährdungen zusammengefasst, die im Zusammenhang mit dem unerwarteten Ausfall eines gesamten Systems oder einzelner Systemkomponente stehen. Es beinhaltet auch die Grenzen der Zuverlässigkeit der eingesetzten Technologien. Mögliche Maßnahmen hierfür sind:

* Redundanzen
* Wartungsverträge
* Intensive Testszenarien (Burn-in) und Abnahmeverfahren
* Notfallkonzepte

# 2.4 Gefährdungskatalog vorsätzliche Handlungen

➔ Siehe auch Anhang

Die vorsätzlichen Handlungen beinhalten das bewusste Zuführen von Schaden an einem System. Unter System w ird hier nicht nur ein IT-System verstanden, sondern das Zusammenspiel von einzelnen Faktoren, die ein funktionierendes Ganzes ergeben. Die einzelnen Faktoren können Technologien, Mensch, Tier etc. sein. Mögliche Maßnahmen:

* Physische Zutrittskontrolle
* Zugangskontrolle (Passwörter, Benutzererkennung)
* Netzwerksicherheit (Firewall, Kryptologie)
* Systemsicherheit (Abschalten nicht benötigter Dienste)

# 2.5 Gefährdungskatalog organisatorische Mängel

➔ Siehe auch Anhang (S. 93)

Wenn Tätigkeiten oder Aufgaben in einem Unternehmen zu verrichten sind, diese aber kei- ner Organisation zugeordnet sind, spricht man von organisatorischen Mängeln. Ebenso, wenn Aufgaben und Tätigkeiten zw ar definiert sind, aber nicht wahrgenommen werden. Werden zum Beispiel Prozesse definiert, aber niemand kümmert sich um deren Kontrolle, so liegt in diesem Falle auch ein organisatorischer Mangel vor. Wichtig ist zu verstehen, dass hinter einem organisatorischen M angel immer ein menschliches Fehlverhalten (menschliche Fehlhandlung oder vorsätzliche Handlung) steht, denn eine Organisation ist in der Regel immer einer Person unterstellt, im höchsten Falle der Geschäftsleitung. Unw issenheit schützt hier nicht vor der Verantw ortung, die übernommen werden muss. Mögliche Maßnahmen hierfür sind:

* Konzepte
* Schaffen von neuen Stellen und Funktionen innerhalb einer Organisation
* Zuordnen von Aufgaben und Verantw ortlichkeiten
* Policy
* Weisungen

Im Rahmen von IT-Sicherheit gilt es die Bedrohungsbilder

* höhere Gewalt
* menschliche Fehlhandlungen
* technisches Versagen
* vorsätzliche Handlungen und organisatorische Mängel

auseinander halten zu können und auch zu wissen, was hinter den einzelnen Begriffen steckt. Es ist wichtig, Gefährdungen nach diesem Raster unterscheiden zu können, da dadurch bereits Hinweise auf die nötigen Gegenmaßnahmen gegeben werden.

# 3.1 Gefährdungs katalog höhere Gewalt

* Personalausfall (fehlende Stellvertreterregelung)
* Blitz
* Feuer
* Wasser
* Kabelbrand
* Staub, Verschmutzung
* Datenverlust durch starke Magnetfelder
* Ausfall eines Weitverkehrsnetzes (kein Einfluss von Seiten des Unternehmens möglich)
* Stromausfall Hauptversorgung (kein Einfluss von Seiten des Unternehmens möglich)
* Beeinträchtigung durch Großveranstaltungen
* Sturm

# 3.2 Gefährdungs katalog menschliche Fehlhandlungen

* Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
* Fahrlässige Zerstörung von Gerät oder Daten
* Nichtbeachtung von IT-Sicherheitsmaßnahmen
* Gefährdung durch Reinigungs- oder Fremdpersonal
* Fehlerhafte Administration des IT-Systems
* Verlust der Datenträger beim Versand
* Übertragung falscher oder nicht gewünschter Datensätze
* Fehlerhafte Administration von Zugangs- und Zugriffsrechten
* Freigabe von Verzeichnissen, Druckern oder der Ablagemappe
* Unbeabsichtigte Datenmanipulation
* Fahrlässiges Löschen von Objekten
* Server im laufenden Betrieb ausschalten
* Konfigurations- und Bedienungsfehler
* Ungeeigneter Umgang mit Passw örtern
* Sorglosigkeit im Umgang mit Informationen

# 3.3 Gefährdungs katalog technisches Versagen

* Ausfall der Stromversorgung
* Ausfall interner Versorgungsnetze
* Ausfall von Systemkomponenten
* Leitungsbeeinträchtigung durch Umfeldfaktoren
* Übersprechen von Leitungen
* Defekte Datenträger
* Bekanntwe rden von Software - Schwachstellen
* Verlust gespeicherter Daten
* Informationsverlust bei erschöpftem Speichermedium
* Software - Schwachstellen oder -Fehler
* Verlust der Datenbankintegrität/-konsistenz
* Ausfall oder Störung von Netzkomponenten
* Schlechte oder fehlende Authentifikation
* Ausfall von Komponenten eines Netz- und Systemmanagementsystems
* Software-Konzeptionsfehler
* Undokumentierte Funktionen

# 3.4 Gefährdungs katalog vorsätzliche Handlungen

* Manipulation/Zerstörung von IT-Geräten oder Zubehör
* Manipulation an Daten oder Software
* Unbefugtes Eindringen in ein Gebäude
* Diebstahl
* Vandalismus
* Anschlag
* Abhören von Leitungen
* Neugierige Mitarbeiter
* Gefährdung bei Wartungsarbeiten durch externes Personal
* Systematisches Ausprobieren von Passw örtern
* Erlangen und M issbrauch von Benutzerrechten
* Computer-Viren
* Wiedereinspielen von Nachrichten
* Maskerade (vortäuschen, jemand anderer zu sein)
* Analyse des Nachrichtenflusses
* Verhinderung von Diensten (DoS)
* Unberechtigtes Kopieren der Datenträger
* Umgehen der Systemrichtlinien
* Unberechtigter Anschluss von IT-Systemen an ein Netz
* Missbräuchliche E-Mail-Nutzung
* Vortäuschen eines falschen Absenders
* Überlastung durch eingehende E-M ails
* Gefälschte Zertifikate
* Hijacking von Netz-Verbindungen
* Abhören von Raumgesprächen über M obiltelefone
* Sabotage

# Wiederholungsfragen

Peter Meier möchte von seinem Unternehmen endlich ein neues Notebook. Er beschließt es «per Zufall» fallen zu lassen. Um welche Form der Bedrohung handelt es sich hierbei?

Sachbearbeiter Heinz Eberhard hat aus Versehen das Gruppenverzeichnis gelöscht. Um welche Form der Bedrohung handelt es sich hierbei?

Frau Hirt müsste dringend eine Präsentation ausdrucken, jedoch hat der Drucker immer Papierstau. Der herbeigerufene Servicetechniker reinigt das Gerät und macht darauf auf merksam, dass der Drucker seit zwei Jahren nicht mehr gereinigt wurde. Um welche Form der Bedrohung handelt es sich hierbei?

Herr Binder ist es leid, im Geschäft immer die lange Wartezeiten beim Internetzugang in Kauf zu nehmen. So beschließt er sein privates M odem mitzunehmen und an die hausin- terne Telefonanlage anzuschließen. Um w elche Form der Bedrohung handelt es sich hierbei?

Sandra Schwarz surft am Arbeitsplatz im Internet und besucht ab und zu eine Horoskop seite. Weiter interessiert sie sich auch sehr für den «Power-Chat» beim Provider «White-win». Der Vorgesetzte spricht sie darauf an und informiert sie, dass eine entsprechende Weisung mit dem Verbot der privaten Internetbenutzung bestehen würde. Frau Schwarz begründet ihr Verhalten damit, dass sie niemals darüber informiert wurde und auch keine entsprechende Vereinbarung unterschrieben hätte. Um welche Form der Bedrohung handelt es sich hierbei?