

## Zusammenfassung

Menschliche Fehler als Bedrohung zu betrachten, mag etwas taktlos erscheinen; dennoch sind sie, wie aus Statistiken unterschiedlicher Organisationen hervorgeht, nach wie vor eine sehr häufige Ursache von EDV-Schadensfällen.

Als "menschlicher Fehler" gilt jedes menschliche Verhalten, das einer sachgemäßen Benutzung zuwiderläuft und ungewollte Schäden unterschiedlicher Art verursacht.

## Inhalt

- 1 Was ist ein menschlicher Fehler? →
- 2 Wer ist betroffen? →
- 3 Wie funktioniert das? →
- 4 Warum sollte man sich schützen? →
- 5 Wie sollte man sich schützen? →
- 6 Statistiken →



## 1 Was ist ein menschlicher Fehler?

Als "menschlicher Fehler" gilt jedes menschliche Verhalten, das einer sachgemäßen Benutzung zuwiderläuft und ungewollte Schäden unterschiedlicher Art verursacht. Absichtliche Handlungen zu unlauteren Zwecken gelten nicht als Fehler.

Es ist unmöglich, eine Liste sämtlicher menschlichen Fehler zu erstellen. Obwohl es unzählige Möglichkeiten im Bereich der menschlichen Fehler gibt, lassen sich einige Unterscheidungskriterien aufstellen, anhand derer menschliche Fehler unterteilt werden können.

### 1.1 Fehler des Types «Nachlässigkeit»

Unter diese Kategorie fallen alle Handlungen von Personen, die zwar umfassend informiert sind, sich aber nicht an die Vorschriften halten. Daher könnte man Fahrlässigkeit mit einer absichtlichen Handlung gleichsetzen. Allerdings ist Fahrlässigkeit im Allgemeinen nicht mit betrügerischen Absichten verbunden.

#### Beispiele:

- ➔ Nichtbeachtung der vorgesehenen Verfahren für die Speicherung von Daten
- ➔ Abbruch der Aktualisierung des Anti-Viren-Programms beim Start des Rechners
- ➔ Weitergabe des Passworts an einen Arbeitskollegen
- ➔ Nutzung der EDV-Architektur des Unternehmens zu privaten Zwecken

- ➔ Installation eines "nicht der Norm entsprechende" Softwareprogramms auf einem Gerät, insbesondere auf einem Computer oder einem Server

### 1.2 Fehler des Types «Unfähigkeit»

Unter diesen Begriff fallen alle unwissentlich begangenen Fehler. Tatsächlich können viele Fehler "in gutem Glauben" begangen werden, ohne dass der Benutzer sich einer unsachgemäßen oder regelwidrigen Benutzung und der Tragweite seiner Handlungen bewusst ist.

#### Beispiele:

- ➔ "Social Engineering" (siehe den Abschnitt zu diesem Thema)
- ➔ falsche Verwendung eines EDV-Tools
- ➔ Löschen von Daten.

## 2 Wer ist betroffen?

**Jeder Benutzer eines EDV-Geräts oder -Systems kann menschliche Fehler begehen.**

## 3 Wie funktioniert das ?

Menschliche Fehler sind unbeabsichtigt herbeigeführte Bedrohungen, die auf verschiedenen Sicherheitslücken beruhen, insbesondere:

### 3.1 Faulheit und mangelnde Gewissenhaftigkeit

Unter diese Kategorie fallen alle fahrlässigen Handlungen, denen ohne Rechenschaftspflichten und Sanktionsmechanismen kaum abzuhelfen ist.

### 3.2 Mangelnde Sensibilisierung und Schulung in der Sicherheit

Eine Person ohne entsprechende Bewusstseinsbildung stellt eine durchaus bedeutende Sicherheitslücke dar, deren Kehrseite darin besteht, dass der begangene Fehler nicht wahrgenommen und somit auch nicht vom Betroffenen selbst erkannt und korrigiert wird.

Mangelnde Ausbildung und Sensibilisierung einer Person in Sicherheitsfragen ist eine Sicherheitslücke, die das hochgefährliche so genannte "Social Engineering" ermöglicht.

#### «SOCIAL ENGINEERING»

Dabei handelt es sich um eine Technik, Personen sensible Informationen abzunötigen. Im Gegensatz zu anderen Angriffen ist hier keine Software erforderlich.

Allein die Überzeugungskraft des "Crackers" und die Habgier oder Unwissenheit seines Opfers sind der Schlüssel zum Erfolg eines solchen Angriffs. Es gibt vier grundlegende Techniken des Social Engineering.

#### 1. Per Telefon

Der Cracker nimmt telefonisch Kontakt zu seinem Opfer auf. Das ist die einfachste Methode. Sein Ziel ist es, so schnell wie möglich an die gewünschten Informationen zu kommen.

#### 2. Per Post

Der Cracker schreibt seinem Opfer einen äußerst seriös wirkenden Brief. Er verwendet oft eine Postfachadresse auf den Namen eines fiktiven Unternehmens.

#### 3. Per Internet

Diese Methode ähnelt der Telefonmethode. Der Cracker gibt sich einfach als Systemoperator, EDV-Verantwortlicher oder Systemingenieur aus.

#### 4. Über persönlichen Kontakt

Diese Art des Social Engineering wird am seltensten angewandt, weil sie für den Cracker mit Schwierigkeiten und Risiken verbunden ist. Allerdings dürften die meisten EDV-Dienstleister, wenn sie Social Engineering praktizieren wollten, die gewünschten Informationen wahrscheinlich ohne große Schwierigkeiten erhalten.

## 4 Warum sollte man sich schützen?

⚠ Menschliche Fehler stellen eine erhebliche Bedrohung für alle Benutzer von EDV-Systemen und Kommunikationssystemen dar und können zu erheblichen finanziellen Schäden und einem bedeutenden Ansehensverlust führen.

## 5 Wie sollte man sich schützen ?

Das von dem amerikanischen Mathematiker Gibbs aufgestellte Gesetz der "Unzuverlässigkeit" besagt: "Jedes System, das von der Zuverlässigkeit des Menschen abhängt, ist unzuverlässig."

Es gibt mehrere Möglichkeiten, menschlichen Fehlern vorzubeugen. Dennoch sollte man viel Energie auf die Begrenzung der Auswirkungen menschlicher Fehler verwenden und nicht grundsätzlich davon ausgehen, dass man in der Lage sei, alle menschlichen Fehler zu vermeiden. Die wichtigsten Gegenmaßnahmen sind:

### 5.1 Die Sensibilisierung

In diesem Bereich lässt sich das Risiko auf einfache Weise erheblich senken. Die meisten Menschen sind im Grunde genommen guten Willens. Achten, diese fürsorglich zu behandeln.

Wenn man sie über die Tragweite ihrer täglichen Handlungen und den Wert der verarbeiteten Daten informiert, werden sie genau darauf

### 5.2 Die Schulung

Das beste Mittel, den falschen Umgang mit Daten und Softwareprogrammen zu vermeiden, ist die Ausbildung der Benutzer in der Bedienung der Software und der Behandlung der Datenträger.

## 5.3 Die Erstellung und die Kontrolle von Prozeduren

Es ist äußerst wichtig, Verfahren einzurichten, die alle sicherheitsrelevanten Aspekte (Zugang, Datensicherung usw.) abdecken. Diese Verfahren müssen in regelmäßigen Abständen kontrolliert und Verstöße mit Strafen belegt werden.

## 5.4 Das Vier-Augen-Prinzip

**Doppelte Überprüfung**  
Um Eingabefehler bei kritischen Softwareprogrammen (Online-Banking usw.) zu vermeiden, empfiehlt es sich, eine doppelte Eingabe der Daten oder eine doppelte Überprüfung vorzusehen.

## 5.5 Das Fehler-Management

Fehler lassen sich nicht immer ganz ausschließen. Daher müssen aus Fehlern Konsequenzen gezogen werden, damit sie sich nicht wiederholen. Nur durch eine gezielte Analyse der begangenen Fehler und ihrer Ursachen können Fehler in der Zukunft vermieden werden.

## 5.6 Das zentralisierte Management

**Zentralisierte Verwaltung**  
Um menschliche Fehler weitestgehend auszuschließen, wird empfohlen, nur denjenigen Personen den Zugang zu den Softwareprogrammen und Daten zu gestatten, die diese auch wirklich benötigen.

## 6

## Statistiken

2002 wurden in Frankreich 24% der EDV-Schadensfälle durch einen Unfall, 14% durch menschliche Fehler und 62% durch böswillige Handlungen verursacht (Quelle: CLUSIF - Club de Sécurité Informatique Français).

Nachstehend finden Sie eine Aufstellung der Häufigkeit menschlicher Fehler im Vergleich zu anderen Bedrohungen.

