

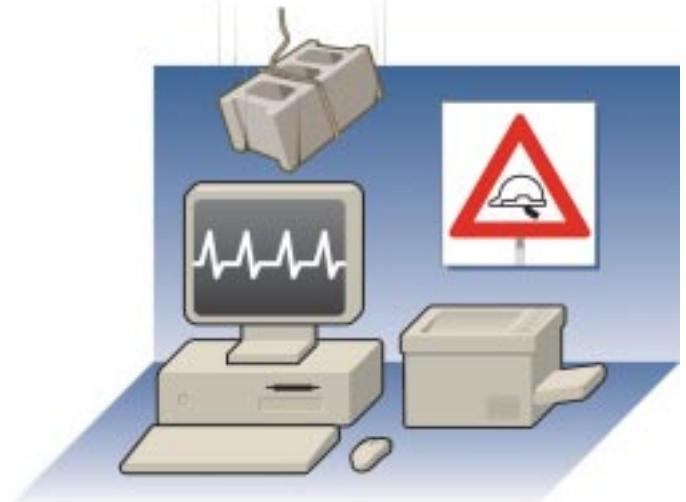
## Zusammenfassung

"Verwundbarkeit" bezeichnet alle Sicherheitslücken der EDV-Ressourcen, die von den Viren, Würmern etc. genutzt werden können, um die Ressourcen zu gefährden. Eine derartige Ausnutzung von Sicherheitslücken kann zu beträchtlichen Verlusten führen. Es werden täglich neue Verwundbarkeiten entdeckt. Diese können jegliche EDV-Ressourcen betreffen.

Die Verwundbarkeiten sind zu zahlreich, als dass sie vollständig aufgeführt werden können. Es ist jedoch möglich, diese Verwundbarkeiten je nach den verschiedenen Normen und Schulen wie etwa BS7799, EBIOS oder auch GMITS in drei Gruppen einzuteilen.

## Inhalt

- 1 Was ist eine Verwundbarkeit? →
- 2 Wer ist betroffen? →
- 3 Wie entstehen Verwundbarkeiten? →
- 4 Warum sollte man sich schützen? →
- 5 Vorbeugende Maßnahmen →



## 1 Was ist eine Verwundbarkeit?

**"Verwundbarkeit" bezeichnet alle Sicherheitslücken der EDV-Ressourcen, die von den Viren, Würmern etc. genutzt werden können, um die Ressourcen zu gefährden.**

Die Verwundbarkeiten lassen sich in drei Gruppen unterteilen:

### 1.1 Verwundbarkeiten auf organisatorischer Ebene (Management)

Eine fehlende korrekte Verwaltung eines EDV-Systems kann schnell zu dessen Gefährdung führen (unternehmensintern als kritische Ressourcen eingestuft).

Die Regeln für die Nutzung und die Implementierung dieser kritischen Ressourcen müssen auf der Ebene der Lösungsverwaltung definiert werden. Auf dieser Ebene müssen auch die Kontrollmaßnahmen eingeführt werden, die eine Überwachung der Einhaltung der Vorschriften ermöglichen. Die Entwicklung und die Verbreitung der Verfahren, die die ordnungsgemäße Funktionsweise der Lösung regeln, werden ebenfalls auf dieser Ebene verwaltet.

### 1.2 Verwundbarkeiten auf physikalischer Ebene

Diese Gruppe umfasst alle Verwundbarkeiten im Zusammenhang mit unvorhersehbaren Ereignissen wie etwa Ausfällen, Unfällen oder beabsichtigten Gefährdungen der Hardware.

Im Rahmen dieser Gruppe von Verwundbarkeiten werden alle physikalischen Eigenschaften der Rechenzentren und EDV-Ausrüstungen analysiert. Man spricht in diesem Zusammenhang auch von einem so genannten "Kontinuitätsplan".

### 1.3 Verwundbarkeiten auf technologischer Ebene

Diese Gruppe der Verwundbarkeiten ist mit Abstand die sich am schnellsten verändernde. Sie umfasst alle Verwundbarkeiten im Zusammenhang mit der Nutzung von Technologien oder Lösungen (Hardware, Software). Zahlreiche Menschen sind mit der Suche nach Verwundbarkeiten beschäftigt, und so werden täglich neue Sicherheitslücken offenbart. Zu dieser Familie der Verwundbarkeiten gehören auch alle Sicherheitslücken, die im Zusammenhang mit Interoperabilitätsproblemen, mit der Notwendigkeit einer Migration und mit der Einführung neuer Produkte stehen.

## 2 Wer ist betroffen?

Jede vernetzte Privatperson, jedes vernetzte kleine und mittelständische Unternehmen und vernetzte Verwaltungen, die die neuen Informations- und Kommunikationstechnologien und insbesondere das Internet nutzen.

## 3 Wie entstehen Verwundbarkeiten?

Es ist nicht möglich, die Entstehung aller Sicherheitslücken umfassend zu beschreiben. Sie sind einfach zu zahlreich.

Das Ziel dieses Abschnitts ist daher nicht die Erstellung einer vollständigen Liste, sondern die Beschreibung einiger Arten von Verwundbarkeiten, die ein beträchtliches Risiko für die EDV- und Kommunikationssysteme darstellen

### 3.1 Verwundbarkeiten auf organisatorischer Ebene (Management)

- ➔ Fehlende Verwaltung der Sicherheit von EDV- und Kommunikationssystemen: Spezielle Humanressourcen müssen der Überwachung der EDV- und Kommunikationssysteme zugewiesen werden. Diese Ressourcen müssen auch die Korrektur von Verstößen durchführen.
- ➔ Falsche Nutzung der implementierten Mittel: Selbst wenn auf der Ebene der Zugangskontrolle Vorschriften aufgestellt worden sind (Passwort), hat das Fehlen effektiver Kontrollen zur Folge, dass viele Benutzer dazu neigen, ihr Passwort nicht zu ändern oder bestimmte sicherheitsanfällige Passwörter zu verwenden.
- ➔ Fehlende Verfahren im Zusammenhang mit der Sicherheit von EDV- und Kommunikationssystemen: Die einzuhaltenden Regeln werden selten eindeutig aufgeführt.
- ➔ Fehlende Information der Anwender: Selbst wenn Verfahren bezüglich der Sicherheit der EDV- und Kommunikationssysteme vorhanden sind, so scheint es häufig der Fall zu sein, dass die Anwender und die Administratoren dieser Systeme davon keine Kenntnis haben.
- ➔ Eine in Bezug auf die Risiken unangemessene Sicherheitspolitik: Die tatsächliche Bewertung der Risiken, denen die Systeme ausgesetzt sind, wird nur selten ausgeführt, und folglich stehen die eingeführten Sicherheitsmaßnahmen häufig in keinem Verhältnis zu den Risiken.
- ➔ Interne Organisation: Die Vielfalt der EDV-Systeme und Anwendungen mit ihren speziellen und immer günstigeren Lösungen führt zu einer Komplexität bzw. der Unmöglichkeit, die Sicherheit der EDV- und Kommunikationssysteme zentral zu verwalten.

### 3.2 Die Verwundbarkeiten auf physikalischer Ebene

- ➔ Nicht-Redundanz: Ganz gleich, ob aus Gründen im Zusammenhang mit den EDV-Systemen, Softwareprogrammen oder aus physikalischen Gründen (Temperatur, Strom etc.), die Nichtverfügbarkeit eines Servers oder einer Datenbank kann zur Unterbrechung von Diensten führen.
- ➔ Fehlende Zugangskontrolle zu physikalischen Elementen: Der Zugang zu den Rechenzentren, zur den Anschlüssen oder sonstigen Komponenten muss so eingeschränkt sein, dass (un)beabsichtigte Manipulationen, die zu einem totalen Ausfall des Rechenzentrums oder eines Teils der Verbindungen zu den Anwendern führen können, vermieden werden.
- ➔ Falsche Lagerung von Sicherungs-Datenträgern: Die Sicherungs-Datenträger werden häufig im Rechenzentrum selbst aufbewahrt, wodurch sie bei einem Schadensfall unbrauchbar werden.
- ➔ Falsche Ressourcenverwaltung: Die Ressourcen müssen korrekt dimensioniert und sorgfältig überwacht werden.
- ➔ Fehlende Verwaltung der Verkabelung: Eine fehlende Dokumentation der Verkabelung kann zur ungewollten Trennung von Verbindungen und somit zur Nichtverfügbarkeit von Ressourcen in öffentlichen Netzwerken führen.

### 3.3 Die Verwundbarkeiten auf technologischer Ebene

- ➔ Interoperabilität der EDV- und Kommunikationssysteme: Um eine einfache Kommunikation zwischen verschiedenen Systemen zu gewährleisten, werden häufig zusätzliche Kommunikationsschichten eingerichtet, was zu neuen Verwundbarkeiten führen kann.
- ➔ Zuverlässigkeit der Aktualisierungen und Updates (Patches): Häufig erfolgt die Implementierung von Patches in Eile und ohne vorherige Abschätzung.
- ➔ Komplexität der Vorschriften bezüglich der Firewalls und Router: Die Implementierung von Filterungen und Zugangsregeln auf Anforderung macht einen Gesamtüberblick quasi unmöglich.

## 4

### Warum sollte man sich schützen?

Die Verwundbarkeiten sind die Ziele der Bedrohungen, denen alle Benutzer von EDV-Systemen ausgesetzt sind. Die Ausnutzung einer Verwundbarkeit durch eine Bedrohung kann zu beträchtlichen Verlusten führen:



#### Direkte finanzielle Verluste

- Zerstörung kritischer Daten,
- Außerbetriebsetzung Ihres gesamten EDV-Systems,
- ...



#### Ansehensverlust

- Infragestellung der Glaubwürdigkeit im Fall einer Verbreitung vertraulicher Informationen,
- ...



#### Zeitverlust

- Erkennung von Sicherheitslücken,
- Installation von Sicherheitspatches, oder/und schließen von "backdoors"
- Aufwand für die Wiederherstellung der zerstörten Daten,
- ...

## 5

### Vorbeugende Maßnahmen

#### Eine gute Adresse

In Hinblick auf technologische Verwundbarkeiten wird geraten, die Webseite

« [www.sans.org](http://www.sans.org) »,

zu besuchen, auf der permanent eine Liste der 20 häufigsten Verwundbarkeiten sowie eine Liste der 10 am häufigsten vom Betriebssystem (OS) verwendeten Verwundbarkeiten aktualisiert wird.

Sie finden diese Informationen unter folgender Adresse:

« [www.sans.org/top20](http://www.sans.org/top20) ».