Mittelstand-Digital
Zentrum
Chemnitz

NACHGELESEN

# Was tun bei einem Sicherheits-vorfall?

ROLAND HALLAU


Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Mittelstand-
Digital

Die 10 Goldenen Regeln sollen Ihnen helfen, die Funktionsfähigkeit Ihrer IT-Systeme effizient zu schützen und im Schadensfall wiederherzustellen. Diese Tipps stammen aus der betrieblichen Praxis kleiner und mittlerer Unternehmen sowie dem Handwerk. Sie wurden in enger Zusammenarbeit mit Unternehmen erarbeitet. Wir erklären

In diesem Nachgelesen erfahren Sie:

- Wie Sie sich richtig vorbereiten,
- Wie Sie sich im Fall eines Falles richtig verhalten und
- was Sie abschließend unternehmen sollten.


## Impressum

**HERAUSGEBER**
Mittelstand-Digital Zentrum Chemnitz
c/o TU Chemnitz
Erfenschlager Str. 73, 09125 Chemnitz
Tel: 0371 531 19935 Fax: 0371 531 819935
info@digitalzentrum-chemnitz.de
www.digitalzentrum-chemnitz.de

**REDAKTION** Anikó Lessi

**GESTALTUNG UND PRODUKTION**
PUNKT191 – Marketing und Design
www.punkt191.de

**BILDNACHWEIS TITEL** MH Stock - Freepik.com
**VERÖFFENTLICHUNG** September 2025


© UveElena- Freepik.com

# Der Sicherheitsvorfall

Die Unternehmens-IT ist bei vielen Unternehmen die Basis der internen und externen Kommunikation, Organisation sowie der Steuerung von Prozessen. Im Zuge der Digitalisierung wird der Anteil der elektronischen Datenverarbeitung noch weiter zunehmen. Daher ist es sehr wichtig, dass die interne IT (sowohl im Büro als auch in der Produktion) reibungslos funktioniert. Durch eigen- aber auch fremdverursachte Fehler kann diese Funktionsfähigkeit beeinträchtigt werden.

## WANN WIRD VON EINEM SICHERHEITSVORFALL GESPROCHEN?

Als Sicherheitsvorfall wird in einem Unternehmen ein Ereignis bezeichnet, das die Vertraulichkeit, Verfügbarkeit und Integrität der Informationen, Geschäftsprozesse, IT-Dienste, IT-Systeme oder IT-Anwendungen mit hohem oder sehr hohem Schutzbedarf derart beeinträchtigt, dass ein großer Schaden für das Unternehmen / die Behörde / den Kunden / den Geschäftspartner entstehen kann. (BSI Grundschutz M 6.122)

## WIE KANN ICH DIE URSACHEN VON EINEM SICHERHEITSVORFALL ERMITTELN?

Sicherheitsvorfälle können sowohl zufällige Ereignisse z. B. Brände und Stromausfälle als auch bewusste oder unbewusste menschliche Eingriffe in die IT-Systeme als Ursache haben. Hierbei bietet eine Spezialdisziplin der Informatik, die IT-Forensik, eine geeignete Hilfestellung, die Sie durch Experten erhalten können. Typische Ziele der IT-Forensik (in Anlehnung an BSI Grundschutz M 6.126) sind: Methoden und Schwachstellen zu identifizieren, die zu einem Systemvorfall geführt haben, daraus entstandene Schäden zu erkennen, mögliche Angreifer zu identifizieren und Beweise für weitere juristische Aktionen zu sichern. Eine typische Folgekette einer IT-forensischen Analyse besteht aus der strategischen und operativen Vorbereitung, Datensammlung, Datenuntersuchung, Datenanalyse und der Dokumentation. Anhand dieses Prozesses sollten auch Sie Ihr Vorgehen bei einem Sicherheitsvorfall orientieren, um effektive Handlungsweisen umzusetzen. Die 10 goldenen Regeln unterstützen Sie hierbei.

## REGEL 1: SCHAFFEN SIE MASSNAHMEN ZUR UNTERSTÜTZUNG DER IT-FORENSIK

Um ein sicherheitsrelevantes Ereignis erkennen und im Anschluss analysieren zu können, ist es notwendig, geeignete Maßnahmen zu realisieren, die den IT-forensischen Prozess unterstützen. Hierzu können z. B. Systeme mit Inspektionsmöglichkeiten zur Datenpaketanalyse oder auch Überwachungs- und Monitoringsysteme zum Einsatz kommen. Wichtig ist auch, dass die Protokollierung von Ereignissen aktiviert wird, welche häufig in Betriebssystemen und Netzwerkgeräten Anwendung findet. Eine Sammlung der Log-Dateien kann auf einem zentralen Server erfolgen.

## REGEL 2: BEREITEN SIE IHRE ORGANISATION AUF EINEN VORFALL VOR

Eine Grundlage zur Bearbeitung von Sicherheitsvorfällen ist die Vorbereitung des Umgangs mit diesen. Neben der Definition von Vorfällen und Sicherheitszielen ist es wichtig, dass Ihre IT-Systeme bekannt sind (z. B. Netzwerkplan, eingesetzte Hard- und Software, Konfiguration). Bestimmen Sie verantwortliche und zu kontaktierende Personen im Unternehmen und identifizieren Sie geeignete Kontakte, die Sie bei einer Untersuchung des Vorfalls unterstützen (IT-Dienstleister bzw. -Forensiker). Das alles sollten Sie in einem sogenannten Notfallplan verfasst haben und beispielsweise mit Checklisten ergänzen, die beschreiben, wie mit Sicherheitsvorfällen proaktiv umzugehen ist.

### REGEL 3: LERNEN SIE SELBST, SICHERHEITS-RELEVANTE EREIGNISSE ZU ERKENNEN

Sicherheitsvorfälle zu erkennen, ist eine sehr komplexe Aufgabenstellung, da diese sich je nach Vorfall unterscheiden können. Zudem zeigen sich Auswirkungen häufig erst nach Tagen oder Wochen. Der Kernaspekt ist aber, dass alle Personen im Unternehmen aufmerksam sind und Unregelmäßigkeiten am IT-System melden. Dabei ist es wichtig, dass die Mitarbeiter auch wissen, ob es sich um einen Sicherheitsvorfall handelt (siehe Regel 2) und dementsprechend sensibilisiert sind. Weiterhin unterstützen Sie auch unter Umständen die aus Regel 1 bekannten technischen Hilfsmittel, da diese sicherheitsrelevante Vorfälle automatisch erkennen, teilweise selbständig verhindern oder Lösungsmöglichkeiten aufzeigen können.

# Wie sollten Sie sich beim Eintritt eines sicherheitsrelevanten Ereignisses verhalten?

### REGEL 4: RUHE BEWAHREN, ABER BESONNEN UND ZÜGIG HANDELN

Dies ist eine Grundregel und schützt die Anwendung der weiteren Regeln. Fehler durch hektisches oder panisches Handeln können zu einer Kettenreaktion führen und eine effiziente Wiederherstellung der Unternehmens-IT beeinträchtigen. Eine durchdachte, aber trotzdem schnelle Reaktion auf den Sicherheitsvorfall kann für Sie Kosten einsparen, Schaden für Ihre Kunden abwenden und u. U. eine notwendige forensische Analyse des Vorfalls vereinfachen. Orientieren Sie sich dafür an Ihren vorgeschriebenen Regeln des Notfallplans!

### REGEL 5: ÜBERBLICK VERSCHAFFEN

Versuchen Sie, in Ihren ersten Schritten zu ermitteln, was vorgefallen ist und welche wesentlichen Systeme betroffen sind. Hierzu sollten vom Mitarbeiter, welcher den Vorfall erkannt hat, folgende Fragen beantwortet oder in einer Checkliste abgearbeitet werden:

- Was ist vorgefallen?
- Wann und wo ist der Vorfall aufgetreten?
- Welche Systeme und Objekte sind betroffen (Netzwerkkomponenten, Software, Daten usw.)?
- Was sind aktuelle Auswirkungen?
- Gibt es eine Vermutung für die Ursache (infizierte E-Mail, Technikausfall etc.)?
- Sind bereits Maßnahmen durchgeführt worden (z. B. Herunterfahren des Rechners, Trennen der Netzwerkverbindung)?

### REGEL 6: VERHINDERN SIE EINE WEITERE AUSBREITUNG

Falls es sich um den Befall einiger Komponenten im Netzwerk mit Schadsoftware handelt, sollten Sie diese unter Quarantäne stellen, vom Netzwerk entkoppeln und alle Zugänge sperren. Eine weitere Möglichkeit ist das Herunterfahren der Systeme. Hierbei muss aber beachtet werden, dass Informationen zum Schädling bzw. Angriff, die noch im Hauptspeicher vorhanden sein können, verloren gehen. Ferner kann auch das Herunterfahren ein weiterer Auslöser zur Einnistung von weiteren Schadprogrammen sein!

### REGEL 7: UNTERSUCHEN UND ANALYSIEREN SIE DEN VORFALL

Häufig ist es zur Ableitung weiterer Maßnahmen notwendig, die Ursachen des Vorfalls zu analysieren. Möglicherweise ergeben sich dann auch einfachere Varianten zum Umgang. Jeder Angriff hinterlässt zudem Spuren, sei es durch eine eingesetzte Schadsoftware oder durch Kommunikation im Netzwerk. Erkenntnisse darüber könnten Aufschluss über den Vorfall liefern. Es ist beispielsweise in einigen Fällen möglich, durch forensische Datenanalysen im Hauptspeicher von Systemen, Schlüssel für Dateien auszulesen, die von sogenannter „Ransomware“ (Erpressungssoftware) kodiert und somit unlesbar gemacht wurden. Vermeiden Sie daher das Verändern von Daten (Spurenverwischung)!

### REGEL 8: LEITEN SIE GEEIGNETE MASSNAHMEN AB UND HANDELN SIE DANACH

In Abhängigkeit der Ergebnisse aus Regel 7 sollten Sie die Maßnahmen priorisieren, um eine zügige und korrekte Wiederherstellung der Systeme zu ermöglichen. Im Sinne der 80-20-Regel (Pareto-Effizienz) erzielen bereits 20 % (also die wichtigsten) Maßnahmen 80 % des gewünschten Effektes. In der Regel werden bei den betroffenen IT-Systemen kompromittierte Dateien gelöscht und durch Backups wieder eingespielt. Dabei ist darauf zu achten, dass die Backups selbst nicht von den Schadprogrammen betroffen sind. Dazu ist eine geeignete Analyse durchzuführen. Anschließend sollte die Funktionsfähigkeit der IT-Systeme überprüft und die bekannten Sicherheitslücken, die zum Vorfall geführt haben, geschlossen werden (z. B. durch Patches, Änderungen im

Netzwerkplan oder neue Handlungsanweisungen für die Mitarbeitenden).

Anschließend sollte die Funktionsfähigkeit der IT-Systeme überprüft und die bekannten Sicherheitslücken, die zum Vorfall geführt haben, geschlossen werden (z. B. durch Patches, Änderungen im Netzwerkplan oder neue Handlungsanweisungen für die Mitarbeitenden).

### REGEL 9: DOKUMENTIEREN SIE DEN SICHERHEITSVORFALL UND DIE MASSNAHMEN

Achten Sie darauf, dass die Vorfälle, auch im Ablauf, ausreichend dokumentiert werden. Dies kann mithilfe eines Protokolls erfolgen. Es bietet sich an, ein Standardprotokoll für einen IT-Sicherheitsvorfall anzulegen. Hierbei sollten sowohl der eigentliche Vorfall selbst als auch die Lösungsmaßnahmen dokumentiert werden. Hilfreich sind dabei auch Fotos, Screenshots und genaue Zeitangaben.

### REGEL 10: ZIEHEN SIE LEHREN AUS DEM SICHERHEITSVORFALL

Im Sinne eines ständigen Verbesserungsprozesses sollten Sie aus dem gesamten Vorfall lernen, um zukünftig die Schwachstellen zu vermeiden, durch die sich der Vorfall ereignen konnte. Denkbar wären Konfigurationsänderungen an den technischen Systemen, Systemerweiterungen, organisatorische Anpassungen und die laufende Schulung bzw. Sensibilisierung von Mitarbeitern. Passen Sie auch dementsprechend Ihre Dokumentationen an!

# Häufige Fehler beim Umgang mit IT-Sicherheitsvorfällen aus der Praxis

In der Praxis zeigt sich, dass Unternehmen bei einem Sicherheitsvorfall oft nach sehr ähnlichen Mustern reagieren und dabei immer wieder auf die gleichen Stolpersteine stoßen. Zu den häufigsten Fehlern gehören:

- Backups werden nicht gepflegt,
- Vorfälle nicht kommuniziert („Lessons learned“)
- keine ausreichende Sensibilisierung der Mitarbeitenden,
- kaum technische Hilfsmittel zur Erkennung,
- befallene Systeme sind zu lange online,
- Ressourcen zur Problembehandlung nicht ausreichend,
- Behinderung der Datenforensik und
- keine Dokumentation.

# Weiterführende Informationen


**1** BSI – Digitaler Ersthelfer: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Onlinekurs/Onlinekurs_node.html

**2** Daten- und Informationssicherheit. (o. D.). Industrie- und Handelskammer. https://www.ihk.de/themen/digitalisierung-und-innovation/daten-und-informationssicherheit-5420862

# Verfasst von

**ROLAND HALLAU** ist Projektmanager bei der tti Technologietransfer und Innovationsförderung Magdeburg GmbH. Im Mittelstand-Digital Zentrum Chemnitz ist er als Fachkoordinator im Bereich IT-Sicherheit tätig..
roland.hallau@digitalzentrum-chemnitz.de

# Weitere Informationen

Das Mittelstand-Digital Zentrum Chemnitz gehört zu Mittelstand-Digital. Mit dem Mittelstand-Digital Netzwerk unterstützt das Bundesministerium für Wirtschaft und Energie die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

**WAS IST MITTELSTAND-DIGITAL?**

Das Mittelstand-Digital Netzwerk bietet mit den Mittelstand-Digital Zentren und der Initiative IT-Sicherheit in der Wirtschaft umfassende Unterstützung bei der Digitalisierung. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenfreie Nutzung der Angebote von Mittelstand-Digital. Weitere Informationen finden Sie unter www.mittelstand-digital.de.

Mittelstand-Digital
Zentrum
Chemnitz

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

Mittelstand-
Digital

aufgrund eines Beschlusses
des Deutschen Bundestages