

# Verhaltensregeln

## 10 Schritte im IT-Sicherheitsnotfall



**Gehen Sie koordiniert und Schritt für Schritt vor. Betrachten Sie die ggf. betroffenen IT-Systeme als einen Tatort. Unkoordinierte Handlungen führen schnell dazu, dass Spuren verändert und hierdurch wichtige Beweismittel vernichtet werden. Bedenken Sie: Bei einem Mord würden Sie das Mordwerkzeug auch nicht anfassen. Lassen Sie das System daher unverändert.**

### 1. Verändern Sie das System nicht

Schalten Sie z.B. das System auf keinen Fall aus und führen Sie keinen Neustart des Rechners oder dergleichen durch. Flüchtige Spuren (z.B. im Arbeitsspeicher) könnten hierdurch vernichtet werden.

### 2. Sichern Sie mögliche Beweismittel

Schränken Sie den Zugang zu möglichen Beweismitteln (z.B. Desktoprechner, Smartphones, USB-Sticks etc.) ein, bis diese forensisch gesichert wurden.

### 3. Protokollieren Sie Ihre Schritte

Protokollieren Sie durchgängig jeden einzelnen Schritt! Dokumentieren Sie beispielsweise unbedingt wer wann wo Zugriffsmöglichkeiten auf die Beweismittel hatte. Fotografieren Sie beispielsweise die lokalen Gegebenheiten.

### 4. Informieren Sie die relevanten internen Stellen

Informieren Sie das Management, die Rechtsabteilung, den IT-Sicherheitsbeauftragten sowie den betrieblichen Datenschutzbeauftragten über den Sicherheitsvorfall. Legen Sie anschließend gemeinsam fest, welche weiteren internen Stellen ggf. informiert werden müssen (z.B. Personalabteilung, Compliance- oder Revisionsabteilung, Presseabteilung oder Betriebsrat). Denken Sie aber daran, der Täter wurde noch nicht gefasst. Soweit daher auch interne Stellen zum potentiellen Täterkreis gehören, weiten Sie den Kreis der informierten Personen nicht unnötig aus.

### 5. Benennen Sie eine verantwortliche Leitungsperson

Benennen Sie eine Person, welche die Aufklärung und Bearbeitung des Sicherheitsvorfalls intern koordiniert und beispielsweise Schnittstellen zu externen Dienstleistern (z.B. IT-Forensiker) bildet.

### 6. Ermitteln Sie den Sachverhalt

Ermitteln Sie, was genau (Art, Umfang, Datum) passiert ist bzw. zu sein scheint. Handelt es sich z.B. um einen Abfluss von Betriebs- oder Geschäftsgeheimnissen, wer kommt als Täter in Frage, wie und wann ist dies konkret vorgefallen, welche Umstände lassen auf eine fahrlässige oder vorsätzliche Begehung schließen und welche Systeme sind relevant? Oder handelt es sich um eine Hackerattacke? Welche Systeme sind in diesem Fall potentiell davon betroffen und welche Anhaltspunkte gibt es hierfür?

### 7. Schalten Sie IT-Forensik-Experten ein

Sofern Sie keine IT-Forensiker beschäftigen, holen Sie sich externe Hilfe, um den Sachverhalt so aufzuklären und aufzuarbeiten, dass dieser auch die Voraussetzungen für ein potentielles späteres Gerichtsverfahren erfüllt. IT-Forensiker sind darauf spezialisiert, vorhandene digitale Spuren gerichtsfest forensisch zu sichern, zu analysieren und anschließend zu präsentieren.

### 8. Informieren Sie externe Stellen

Klären Sie mit der Unternehmensführung, der Rechtsabteilung und dem betrieblichen Datenschutzbeauftragten ab, ob ggf. externe Stellen (z.B. Aufsichtsbehörden oder von einem Datendiebstahl betroffene Personengruppen) über den Sicherheitsvorfall informiert werden müssen. Einige Gesetze (z.B. BDSG, TMG oder IT-Sicherheitsgesetz) verlangen u.U. entsprechende Informationsweitergaben und es drohen bei Nicht-Einhaltung Bußgelder.

### 9. Beseitigung

Beseitigen Sie schließlich die von den IT-Forensik-Experten identifizierten Bedrohungen. Blocken Sie beispielsweise bösartige IP-Adressen, ändern Sie die unternehmensweiten Passwörter und verifizieren Sie die Neugestaltung. WICHTIG: Stellen Sie unbedingt sicher, dass zuvor alle kompromittierten Systeme identifiziert wurden! Ansonsten warnen Sie ggf. die Angreifer, was dazu führt, dass weitere Hintertüren in Ihre Systeme implementiert oder Daten exfiltriert oder beschädigt werden.

### 10. Wiederherstellung und Lesson Learned

Nachdem Sie die akute Bedrohung beseitigt haben, verbessern oder implementieren Sie anschließend Lösungen zum Langzeitschutz. Redesignen Sie beispielsweise Ihr Netzwerk (Stichwort Netzsegmentierung), zentralisieren Sie das Logging (SIEM) oder optimieren Sie Ihr Security Awareness Training.

Nutzen Sie den Sicherheitsvorfall sodann als Lerneffekt für die Zukunft. Halten Sie beispielsweise nach neuen Bedrohungen Ausschau und führen Sie regelmäßige Pentests sowie IT-Sicherheitsaudits durch.

**Gern beantworten wir Ihre Fragen oder erstellen Ihnen ein individuelles Angebot.**

#### Hamburg

intersoft consulting services AG  
Beim Strohhause 17, 20097 Hamburg  
Telefon: 040 / 790 235 0

#### Frankfurt

intersoft consulting services AG  
Niederan 13 - 19, 60325 Frankfurt  
Telefon: 069 / 153 477 16

#### München

intersoft consulting services AG  
Marsstraße 37, 80335 München  
Telefon: 089 / 599 467 24

#### Berlin

intersoft consulting services AG  
Fischerinsel 16, 10179 Berlin  
Telefon: 030 / 804 923 00

#### Stuttgart

intersoft consulting services AG  
Friedrichstraße 15, 70174 Stuttgart  
Telefon: 0711 / 490 396 28

#### Kiel

intersoft consulting services AG  
Caprivistraße 29, 24105 Kiel  
Telefon: 0431 / 640 886 23

#### Düsseldorf

intersoft consulting services AG  
Pempelforter Straße 47,  
40221 Düsseldorf  
Telefon: 0211 / 917 382 90