

# Erste-Hilfe-Maßnahmen

Wurden Sie Opfer eines Cyber-Angriffs? Die folgenden Hinweise können Ihnen helfen, den Schaden zu begrenzen.

## Bewahren Sie Ruhe

Überlegen Sie sorgfältig, bevor Sie Systeme abschalten oder Netzwerkverbindungen unterbrechen. Auch wenn diese Maßnahmen oft sinnvoll oder notwendig sind, so können sie schwerwiegende Auswirkungen auf Ihr Geschäftsmodell haben, Spuren und Beweise vernichten oder die Angreifer warnen.

## Bestimmen Sie eine Einsatzleitung

Sie benötigen eine Einsatzleitung, die technischen und organisatorischen Sachverstand über Ihr Unternehmen vereint, und welche befugt ist, weitreichende Entscheidungen zu treffen. Dazu gehören idealerweise die Geschäftsführung und die IT-Verantwortlichen.

## Versuchen Sie, ein erstes Bild der Lage zu gewinnen

Für eine schnelle Aufklärung ist eine Offenheit aller Beteiligten hilfreich. Motivieren Sie Ihre Mitarbeitenden, Versäumnisse und Fehler einzugestehen. Wenn Mitarbeitende offen reden können, ohne mit schwerwiegenden Konsequenzen rechnen zu müssen, kann ein Angriff früher abgewehrt und schlimmere Schäden vermieden werden.

## Protokollieren Sie alle Aktivitäten an Ihren IT-Systemen

Dokumentieren Sie, welche Maßnahmen Sie bereits selbst ergriffen haben. Machen Sie Fotos von auffälligen Bildschirminhalten. Erstellen Sie Snapshots von virtuellen Infrastrukturen.

## Erwägen Sie, die Polizei einzuschalten

Die Polizei verfügt technisch und rechtlich über Ermittlungsinstrumente, die Ihnen selbst oder privatrechtlichen Dienstleistern nicht zur Verfügung stehen.

## Vorsicht bei Erpressung

Auch wenn es verlockend klingt, einer Erpressung nachzugeben, so besteht keine Garantie, dass Ihre Zahlung Ihr Problem auch wirklich löst. Außerdem befeuern Sie damit das kriminelle Geschäftsmodell.

## Bereiten Sie eine Stellungnahme vor

Je nach Situation können gut informierte Mitarbeitende und Kunden durch ihr Verhalten (Tun und Unterlassen) dazu beitragen, den weiteren Schaden zu begrenzen. Informieren Sie sich über etwaige Meldepflichten nach der EU-Datenschutz-Grundverordnung.

## Vorsicht bei der Kommunikation über Ihre IT-Systeme

Je nach Art des Angriffs kann es passieren, dass ein Angreifer Ihre E-Mail-Kommunikation mitlesen kann. Eventuell kann dies auch Ihre Festnetztelefone oder Faxgeräte betreffen. Ziehen Sie in Erwägung, vertrauliche Gespräche über private Mobiltelefone zu führen.

**0800-CYBERWEHR 0800-292379347**

**Kontakt**  
Max Bechler  
T +49 721 9654-637  
E [team@cyberwehr-bw.de](mailto:team@cyberwehr-bw.de)  
W [www.cyberwehr-bw.de](http://www.cyberwehr-bw.de)