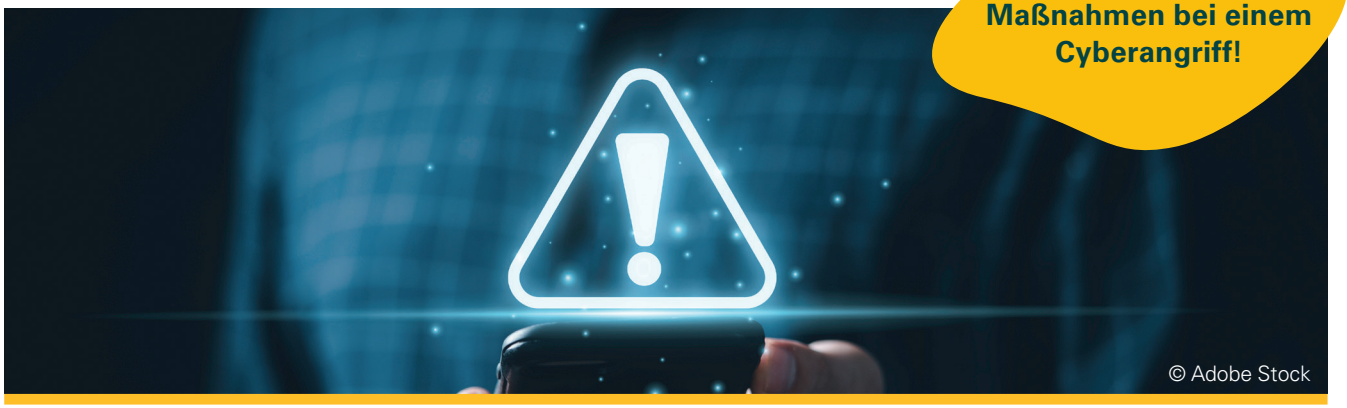
CSBW
CYBER
SICHERHEITS
AGENTUR
BADEN-WÜRTTEMBERG

Erste Hilfe bei einem Cybernotfall

Bei der Bewältigung eines Cyberangriffs spielen viele Faktoren eine Rolle. Je nach Gegebenheiten der betroffenen IT-Infrastruktur und der Art des Angriffs müssen unterschiedliche zeitkritische Maßnahmen ergriffen werden. Um frühzeitig Schäden zu begrenzen, sollten die hier genannten Sofortmaßnahmen im Falle eines Cyberangriffs umgesetzt werden.



© Adobe Stock

Sofortmaßnahmen

- **Ruhe bewahren!**
  Sie sollten keine übereilten Entscheidungen treffen.
- **Weitere Arbeit am betroffenen Gerät/System einstellen!**
  Vermeiden Sie unnötige Mehrbelastungen des Systems. Dokumentieren Sie den Vorfall möglichst genau.
- **Cyberangriff melden!**
  Meldung an ISB, IT-Abteilung oder Führungskraft, gemäß Ihrer IT-Notfallplanung.

Weiterführende Maßnahmen (nach Meldung und Absprache)

- **Betroffenes Gerät/System bei Bedarf vom Netzwerk und vom Internet trennen!**
  Verhindern Sie, dass evtl. weitere Geräte befallen werden oder weiterer Schadcode aus dem Internet nachgeladen werden kann.
- **Identifizieren aller betroffenen Geräte/Systeme**
- **Forensische Sicherung**
  Sichern Sie alle System-Protokolle, Log-Dateien, Notizen, Datenträger und andere digitale Informationen.

Erste Hilfe bei einem Cybernotfall

Cyberangriff melden

Diese Informationen sollten Sie unbedingt entsprechend Ihrer Notfallplanung weitergeben:

- **Wer** meldet? (Name, Stelle etc.)
- **Welches** IT-System ist betroffen?
- **Wie** und in welchem Umfang haben Sie vor dem Vorfall am betroffenen System gearbeitet?
- Ist Ihnen am System etwas aufgefallen? **Was** haben Sie beobachtet?
- **Wann** ist das Ereignis eingetreten?
- **Wo** befindet sich das betroffene Gerät/ System? (Gebäude, Etage, Raum, Arbeitsplatz)

Zusätzlich sollten Sie folgende Aspekte abklären:

- Muss Ihre eigene Institution alarmiert werden?
- Müssen relevante Behörden, die Polizei oder Fachexperten hinzugezogen werden?
- Besteht eine Melde- oder Informationspflicht gegenüber Dritten? Wer muss noch informiert werden?
- Wurde der Vorfall bereits bewertet und als Cyberangriff eingestuft oder handelt es sich um einen technischen Defekt?
- Haben Sie alle bisher durchgeführten Maßnahmen kontinuierlich abgestimmt und dokumentiert?
- Wurde besonderer Fokus auf die vorrangig zu schützenden Prozesse gelegt?
- Wurden vor dem Vorfall Backups erstellt? Sind die Backups vor weiteren Einwirkungen geschützt?
- Sind die ausgenutzten Schwachstellen der Systeme bekannt und wurden bereits entsprechende Maßnahmen zu deren Behebung veranlasst?
- Sind alle relevanten Zugangsberechtigungen zu Accounts überprüft worden?

Weitere Informationen und Hilfestellungen finden Sie auf folgenden Seiten:
www.bsi.bund.de
www.allianz-fuer-cybersicherheit.de

Diese Seiten orientieren sich an den TOP 12 Maßnahmen bei einem Cyber-Angriff der Allianz für Cybersicherheit (ACS) und der IT-Notfallkarte der ACS

CSBW
CYBER SICHERHEITS AGENTUR
BADEN-WÜRTTEMBERG

Weitere Factsheets und Informationen unter:
www.cybersicherheit-bw.de

CSBW Prävention
Kontakt: schulungen@cybersicherheit.bwl.de
Stand: 05.2023