Cybersicherheitsagentur Baden-Württemberg
(CSBW)

CSBW CYBER SICHERHEITS AGENTUR BADEN-WÜRTTEMBERG

Barrierefreie Version
CSBW-Factsheet: Cybersecurity-Wissen kompakt

Zum Thema: Erste Hilfe bei einem Cybernotfall

Richtig reagieren! Schäden vermeiden mit unseren Erste-Hilfe-Maßnahmen bei einem Cyberangriff!

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.

Sofortmaßnahmen

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

Weiterführende Maßnahmen (nach Meldung und Absprache)

1. 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.
2. Identifizieren aller betroffenen Geräte/Systeme
3. Forensische Sicherung
   Sichern Sie alle System-Protokolle, Log-Dateien, Notizen, Datenträger und andere digitale Informationen.

Cyberangriff melden

Diese Informationen sollten Sie unbedingt entsprechend Ihrer Alarmplanung weitergeben:

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

Weitere Aspekte

Zusätzlich sollten Sie folgende Aspekte abklären:

1. Muss Ihre eigene Institution alarmiert werden?
2. Müssen relevante Behörden, die Polizei oder Fachexperten hinzugezogen werden?
3. Besteht eine Melde- oder Informationspflicht gegenüber Dritten? Wer muss noch informiert werden?
4. Wurde der Vorfall bereits bewertet und als Cyberangriff eingestuft? Oder handelt es sich um einen technischen Defekt?
5. Haben Sie alle bisher durchgeführten Maßnahmen kontinuierlich abgestimmt und dokumentiert?
6. Wurde besonderer Fokus auf die vorrangig zu schützenden Prozesse gelegt?
7. Wurden vor dem Vorfall Backups erstellt? Sind die Backups vor weiteren Einwirkungen geschützt?
8. Sind die ausgenutzten Schwachstellen der Systeme bekannt und wurden bereits entsprechende Maßnahmen zu deren Behebung veranlasst?
9. 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 Seite orientiert sich an den TOP 12 Maßnahmen bei einem Cyber-Angriff der Allianz für Cybersicherheit (ACS) und der IT-Notfallkarte der ACS.

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

CSBW – Abteilung 1: Prävention – Stand 05.2023
Kontakt: schulungen@cybersicherheit.bwl.de