Cybersicherheitsagentur Baden-Württemberg
(CSBW)

Barrierefreie Version
CSBW-Factsheet: Cybersecurity-Wissen kompakt

Zum Thema: Informationssicherheitsvorfall erkennen

Helfen Sie mit, Informationssicherheitsvorfälle zu erkennen und effizient zu bearbeiten.

Jeder Verdacht auf ein **sicherheitsrelevantes Ereignis**[1] oder einen **Sicherheitsvorfall**[2] am Arbeitsplatz muss an die zuständige Stelle (z.B. IT-Helpdesk, Informationssicherheitsbeauftragter) gemeldet werden.
Nachfolgende Beispiele helfen Ihnen, mögliche Verdachtsmomente zu erkennen.

Beispiele für Verdachtsmomente:

1. Diebstahl oder Verlust mobiler Geräte, Datenträger oder Dokumente.
2. Anmeldung mit richtigen Zugangsdaten ist nicht mehr möglich.
3. Textdateien werden von allein Ordnern hinzugefügt.
4. Unerklärliche Fehlermeldungen und Warnhinweise erscheinen.
5. Meldungen über Virenfund.
6. Ohne Zutun werden Anwendungen gestartet oder Dateien geöffnet, verändert, gelöscht, der Zugriff auf diese gesperrt oder sie lassen sich plötzlich nicht mehr bearbeiten.
7. Kontrollleuchte der Webcam leuchtet, obwohl keine Videokonferenz läuft.
8. Ohne Zutun des Benutzenden werden E-Mails aus dessen Postfach versendet.
9. Erhalt einer Phishing-E-Mail.
10. Weiterleitung auf eine völlig andere Website nach korrekter Eingabe einer Internetadresse.
11. Fremde Personen erfragen vertrauliche Informationen per Telefon, E-Mail oder persönlich.
12. Geräte oder Gegenstände befinden sich unangekündigt in Ihren Räumlichkeiten, z.B. USB-Sticks, Kabel, Boxen.

Handlungsempfehlungen:

Bei **Verdacht eines Informationssicherheitsvorfalles**, melden Sie diesen an die Ihnen bekannte Meldestelle.

Folgende Inhalte sollte Ihre Meldung enthalten:

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

[1] **Sicherheitsrelevantes Ereignis:**

Ein sicherheitsrelevantes Ereignis liegt vor, wenn mindestens eines der Schutzziele der Informations-sicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) gefährdet erscheint.
Beispiel, bei dem die Vertraulichkeit verletzt ist:
Notizen über Passwörter liegen an leicht zugänglichen Orten.

[2] **Sicherheitsvorfall:**

Ein Sicherheitsvorfall liegt vor, wenn mindestens eines der Schutzziele der Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) verletzt ist.

Beispiel, bei dem die Vertraulichkeit und die Verfügbarkeit verletzt sind:
Bei einem Hacking-Angriff auf die Datenbank eines Fachverfahrens werden vertrauliche Datensätze kopiert, manipuliert oder gelöscht.

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

CSBW – Abteilung 1: Prävention – Stand 09.2023
Kontakt: schulungen@cybersicherheit.bwl.de