

CSBW

CYBER  
SICHERHEITS  
AGENTUR  
BADEN-WÜRTTEMBERG

## Informationssicherheitsvorfall erkennen

Jeder Verdacht auf ein **sicherheitsrelevantes Ereignis**<sup>1</sup> oder einen **Sicherheitsvorfall**<sup>2</sup> am Arbeitsplatz muss an die zuständige Stelle (z.B. IT-Helpdesk, Informationssicherheitsbeauftragte) gemeldet werden.

Nachfolgende Beispiele helfen Ihnen, mögliche Verdachtsmomente zu erkennen.

Helfen Sie mit,  
Informationssicherheitsvorfälle  
zu erkennen



### Beispiele für Verdachtsmomente:

- ▶ **Diebstahl** oder **Verlust** mobiler Geräte, Datenträger oder Dokumente.
- ▶ Anmeldung mit richtigen **Zugangsdaten** ist nicht mehr möglich.
- ▶ Textdateien werden **ohne Ihr Zutun in Ordner verschoben**.
- ▶ **Unerklärliche Fehlermeldungen** und **Warnhinweise** erscheinen.
- ▶ Meldungen über **Virenfunde**.
- ▶ **Ohne Zutun** werden **Anwendungen** gestartet oder **Dateien** geöffnet, verändert, gelöscht, der Zugriff auf diese gesperrt oder sie lassen sich plötzlich nicht mehr bearbeiten.
- ▶ **Kontrollleuchte der Webcam leuchtet**, obwohl keine Videokonferenz läuft.
- ▶ Ohne Zutun des Benutzenden werden **E-Mails** aus dessen Postfach versendet.
- ▶ Erhalt einer **Phishing-E-Mail**.
- ▶ **Weiterleitung auf eine völlig andere Website** nach korrekter Eingabe einer Internetadresse.
- ▶ **Fremde Personen erfragen vertrauliche Informationen** per Telefon, E-Mail oder persönlich.
- ▶ **Geräte oder Gegenstände** befinden sich unangekündigt in Ihren Räumlichkeiten z.B. Kabel oder Datenträger wie USB-Sticks und externe Festplatten.

## Handlungsempfehlungen:

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

## Folgende Inhalte sollte Ihre Meldung enthalten:

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

## <sup>1</sup> Sicherheitsrelevantes Ereignis:

Ein sicherheitsrelevantes Ereignis liegt vor, wenn mindestens eines der Schutzziele der Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) gefährdet erscheint.

*Beispiel, bei dem die Vertraulichkeit verletzt ist: Zettel mit Passwörtern liegen an leicht zugänglichen Orten.*

## <sup>2</sup> 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 und gelöscht.*