

Richtlinie

Sicherheitsrelevante Ereignisse: Meldepflicht & Sofortmaßnahmen

I Geltungsbereich

Diese Richtlinie ist verbindlich für alle Mitglieder und Angehörigen der Universität sowie für externe IT-Dienstleister und weitere Dritte, die Informationen oder IT-Systeme der Universität nutzen oder verarbeiten.

II Meldepflicht und Meldewege

Alle Mitglieder und Angehörigen der Universität sowie die vorgenannten IT-Dienstleister und weiteren Dritten sind aufgefordert, mögliche **sicherheitsrelevante Ereignisse** unverzüglich und auch bei Verdacht an den IT Service Desk zu melden, um Schäden zu minimieren und weitere Gefährdungen zu vermeiden:

- Telefonisch über den **Hausanschluss 1818**
oder
- per E-Mail an **informationssicherheit@tu-freiberg.de**.

Sofern möglich, halten Sie bitte die folgenden Informationen bereit:

- Wer meldet (Name, E-Mail-Adresse, Telefonnummer)?
- Welches IT-System ist betroffen (Art und Kennung des Systems, Gebäude, Raum)?
- Wie haben Sie mit dem IT-System gearbeitet? Was haben Sie beobachtet?
- Wann ist das Ereignis eingetreten (Datum, Uhrzeit)?

Weiterhin sind ggf. die für die dezentrale Administration zuständigen Personen zu informieren.

III Sofortmaßnahmen und Verhaltenshinweise

Falls Sie einen (erfolgreichen) Angriff auf Ihren Arbeitsplatz-PC oder ein anderes IT-System befürchten, sind die folgenden Sofortmaßnahmen zu beachten:

1. Bewahren Sie Ruhe.
2. Lassen Sie das Gerät eingeschaltet und trennen Sie dieses unverzüglich vom Datennetz, indem Sie das Netzkabel ziehen sowie Funk-Verbindungen (z. B. WLAN, Mobilfunk) deaktivieren.
3. Stellen Sie die weitere Arbeit am betroffenen Gerät oder IT-System ein.

4. Informieren Sie unverzüglich den IT Service Desk (s. o.) über den Vorfall.

Grundsätzlich gelten während der Reaktion auf sicherheitsrelevante Ereignisse die folgenden Hinweise:

- a) Dokumentieren Sie nach Möglichkeit Ihre Beobachtungen, z. B. durch Fotoaufnahmen oder Screenshots.
- b) Passwörter müssen gewechselt werden, wenn sie Dritten bekannt geworden sind oder der Verdacht dazu besteht (<https://password.tu-freiberg.de>).
- c) Leiten Sie weitere Maßnahmen nur nach Anweisung durch das URZ, den Beauftragten für Informationssicherheit oder die für die dezentrale Administration verantwortlichen Personen ein.

IV Erkennen sicherheitsrelevanter Ereignisse

Als **sicherheitsrelevantes Ereignis** wird eine Beobachtung oder Abweichung bezeichnet, die auf eine mögliche Beeinträchtigung der Informationssicherheit hinweist und die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder IT-Systemen gefährden kann. Typische Folgen dieser Ereignisse sind ausgespähte, manipulierte oder zerstörte Informationen.

Die nachfolgenden Beispiele sollen dabei unterstützen, einen potenziellen Informationssicherheitsvorfall als solchen zu erkennen:

- Offene Fenster und Türen in sicherheitsrelevanten Bereichen,
- bei Abwesenheit nicht gesperrte PCs,
- unbekannte Personen in nicht öffentlich zugänglichen Bereichen,
- verdächtige E-Mails mit Anhängen oder Links,
- ungewöhnliche Telefonanrufe,
- unerwartete Fehler- oder Warnmeldungen auf einem IT-System,
- IT-Systeme reagieren stark verlangsamt oder sind gar nicht erreichbar,
- Verlust oder Diebstahl von Geräten oder Datenträgern,
- Datenlecks (versehentliche oder absichtliche Freigabe vertraulicher Daten an Dritte),
- Malware-Infektionen (Viren, Trojaner, andere Schadsoftware).

Weitere Hinweise zu sicherheitsrelevanten Ereignissen und zur Informationssicherheit an unserer Universität finden Sie auf der Webseite der Stabsstelle Informationssicherheit (<https://tu-freiberg.de/informationssicherheit>).