JUSTUS-LIEBIG-UNIVERSITÄT GIESSEN

Die Präsidentin

Mitteilungen der Justus-Liebig-Universität Gießen

Ausgabe vom **08.04.2026**

2.26.30 Nr. 3b
Handlungsempfehlungen für Erstmaßnahmen bei Informationssicherheitsvorfällen

Handlungsempfehlungen für Erstmaßnahmen bei Informationssicherheitsvorfällen

Vom 24.02.2026

Bisherige Fassungen:

	Präsidium	Verkündung
Urfassung	24.02.2026#	08.04.2026

Verhaltensregeln und Erstmaßnahmen

Bei einem potenziellen **Informationssicherheitsvorfall** sind die folgenden Verhaltensregeln und Erstmaßnahmen zu beachten:

1. Bewahren Sie Ruhe.
2. Melden Sie sich unverzüglich beim HRZ-Helpdesk:
   a. telefonisch über **0641 / 99 - 13100** (während der Arbeitszeiten)

      oder

   b. über das Formular auf **https://uni-giessen.de/isb/meldung**.
3. Wenn im Informationssicherheitsvorfall ein **vernetztes Gerät oder System** involviert ist, dann **trennen Sie es vom Netzwerk**, indem Sie das Netzwerkkabel ziehen sowie Funk-Verbindungen (z.B. WLAN, Mobilfunk, Bluetooth) deaktivieren, um eine mögliche Ausbreitung des Vorfalls zu verhindern. Der Helpdesk unterstützt Sie dabei.
4. Stoppen Sie alle Arbeiten am betroffenen Gerät oder System, bis eine Fortsetzung der Arbeiten nach der Meldung freigegeben wurde.

Während der Reaktion auf Informationssicherheitsvorfälle gelten folgende Empfehlungen:

a) Verzichten Sie darauf, eigenständige Maßnahmen zur Problemlösung zu ergreifen, um mögliche Spuren nicht zu verwischen.

b) Dokumentieren Sie nach Möglichkeit die ungewöhnlichen Aktivitäten durch Fotoaufnahmen oder Screenshots, um später bei der Analyse wertvolle Informationen bereitstellen zu können.

c) Geben Sie in keinem Fall persönliche oder vertrauliche Informationen an Dritte weiter, auch nicht in Reaktion auf mögliche Warnmeldungen.

Erkennen von potenziellen Informationssicherheitsvorfällen

Die nachfolgenden Beispiele bzw. Indikatoren sollen dabei unterstützen, einen potenziellen Informationssicherheitsvorfall als solchen erkennen zu können und in der Folge unverzüglich die in Kapitel 1 beschriebenen Schritte einzuleiten.

- Verlust oder Diebstahl: Geräte oder Datenträger sind verloren gegangen oder gestohlen worden, wodurch Unbefugte nun Zugriff auf die darauf gespeicherten Daten haben könnten.
- Offenliegende Dokumente: Papierdokumente lagen offen an einem Ort, an dem sich auch Personen aufhielten, die nicht befugt waren, sie einzusehen.
- Unbefugter Zugriff: Unbefugte Personen haben auf Dateien oder Daten zugegriffen, zum Beispiel aufgrund von Sicherheitslücken im System, falschen Berechtigungen oder versehentlichem Senden von Dateien an die falsche Empfängeradresse.
- Unbekannte Dateien oder Programme: Auf einem Computer oder Server wurden unbekannte Dateien oder Programme entdeckt.
- Ungewöhnlicher Zustand von Dateien: Dateien wurden aus unerklärlichen Gründen verändert, sind nicht mehr lesbar, lassen sich nicht öffnen oder sind verschwunden.
- Änderungen an Einstellungen: Es wurden unerwartete Änderungen an Konfigurationen oder Einstellungen festgestellt, die nicht selbst vorgenommen wurden.
- Unbekannte E-Mail im Postfach: Im Ordner „Gesendet“ befinden sich E-Mails, die nicht selbst verfasst oder verschickt wurden. Dies kann auf eine unautorisierte Nutzung oder Manipulation der eigenen E-Mail-Adresse durch Dritte hinweisen, oft im Zusammenhang mit Spam-Versand oder anderen betrügerischen Aktivitäten.
- Systeme sind langsam oder gar nicht erreichbar: Dienste, Systeme, Server oder Computer reagieren stark verlangsamt oder sind gar nicht erreichbar.
- Login-Probleme: Die Anmeldung bei Diensten, Systemen oder Apps ist nicht mehr möglich.
- Ungewöhnliche Warnhinweise: Unerwartete Warnmeldungen oder Pop-ups, die auf Sicherheitsprobleme hindeuten, sind aufgetaucht.
- Verdächtige Weiterleitungen: Interaktionen mit Anwendungen und Diensten, wie zum Beispiel Suchanfragen im Internet, werden auf unerwartete Websites umgeleitet, was auf Schadsoftware oder unerwünschte Browser-Erweiterungen hindeutet.
- Anwendungen installieren sich von selbst: Unerwünschte Anwendungen sind ohne Zustimmung des Nutzenden auf dem System installiert worden. Dies kann durch automatisch startende Downloads auf Webseiten, manipulierte E-Mail-Anhänge, Nutzung unbekannter USB-Sticks oder Installation von als legitim anmutender Software ausgelöst werden.
- Phishing: Kriminelle haben durch gefälschte E-Mails, Nachrichten oder Websites Zugang zu vertraulichen Informationen wie Passwörtern, Kreditkartendaten oder persönlichen Identifikationsdaten erlangt.

Gießen, den 24.02.2026
Prof. Dr. Katharina Lorenz
Präsidentin der Justus-Liebig-Universität Gießen