IT-Sicherheitsvorfall melden

1. Was ist ein IT-Sicherheitsvorfall?

1. Sie haben versehentlich einen verdächtigen Anhang in einer *E-Mail* geöffnet.
2. Sie haben versehentlich auf eine verdächtige Web-Adresse (*Link*) in einer *E-Mail* geklickt.
3. Sie erhalten eine *Erpresser-E-Mail*.
4. Sie erhalten eine *E-Mail*, in der Sie aufgefordert werden, persönliche Daten (Benutzername, Passwort, Kontonummer, ...) über eine Web-Seite einzugeben oder jemandem mitzuteilen.
5. Sie erhalten sehr viele unerwünschte Nachrichten in Ihr Postfach (*Spam-Mail*).
6. Ihr Benutzerkonto wird zum Senden von *Spam-Mail* missbraucht.
7. Ihr Rechner verhält sich merkwürdig (Festplatte läuft im Dauerbetrieb, Rechner reagiert nicht auf Eingaben, ...), da er ggf. mit Schad-Software verseucht ist.
8. Sie werden angerufen (i. A. geben sich die Personen als Beschäftigte einer *Hotline* einer bestimmten Firma aus), da Ihr Rechner angeblich Probleme hat, die mit Ihrer Hilfe gelöst werden können, wenn Sie bestimmte Einstellungen vornehmen, die Ihnen jetzt telefonisch durchgegeben werden.
9. Sie werden angerufen und nach Ihrer Arbeitsumgebung gefragt (eingesetzte Produkte, Kolleginnen und Kollegen, Vorgesetzte, *E-Mail*-Adressen, ...), damit diese Informationen später ggf. für einen Angriff auf die Rechner und/oder das Netz der Hochschule benutzt werden können (Informationsbeschaffung über *Social Engineering*).
10. Sie haben eine regelwidrige Benutzung laut Kapitel 6 der IT-Sicherheitsrichtlinie der Hochschule festgestellt.
11. Wenn Ihnen generell etwas merkwürdig oder verdächtig vorkommt, kann es sich ebenfalls um einen IT-Sicherheitsvorfall handeln.

Melden Sie den Vorfall zeitnah! Alle Hochschulangehörigen sind verpflichtet, IT-Sicherheitsvorfälle zu melden.

Seitenanfang

2. Was ist ein IT-Sicherheitsnotfall?

1. Ihr Endgerät wurde gestohlen oder Sie haben es verloren.
2. Ihre Dateien werden automatisch gelöscht, verändert oder verschlüsselt. **Versuchen Sie, den Schaden laut Kapitel 5 im Grundschutzdokument zu begrenzen.** Verwenden Sie Ihr Endgerät erst dann wieder, wenn Sie dazu vom Rechenzentrum aufgefordert werden.

3. Ihre Zugangsdaten (Benutzername/Passwort, Chipkarte, ...) wurden gestohlen. **Ändern Sie sofort Ihr Passwort und/oder lassen Sie ggf. Ihr Benutzerkonto sperren.**
4. Sie werden akut erpresst oder bedroht, um die IT-Infrastruktur der Hochschule zu kompromittieren. **Melden Sie den Notfall sofort einer Person des Präsidiums oder des Justitiariats der Hochschule.**

Melden Sie alle Notfälle zeitnah!

Seitenanfang

3. Wem melde ich was?

Wenden Sie sich bitte an die Ansprechperson Ihrer Organisationseinheit bzw. des Rechenzentrums, wenn Sie einen IT-Sicherheitsvorfall oder -notfall erkennen, einen Verstoß gegen die IT-Sicherheitsrichtlinie bemerken oder selbst Opfer eines Angriffs auf elektronischem Wege geworden sind bzw. Sie Vorgänge mit strafrechtlichen Konsequenzen bemerkt haben. Alle IT-Sicherheitsvor- und -notfälle (mit Ausnahme von Erpressungen und Bedrohungen) müssen zusätzlich an den betroffenen Systemadministrator bzw. die betroffene Systemadministratorin gemeldet werden, der bzw. die für das Endgerät, den Laborrechner, den *Server* oder die spezielle Software zuständig ist.

Ihre Meldung sollte folgende Angaben enthalten:

1. Wer meldet (Name, *E-Mail*-Adresse, Telefonnummer)?
2. Wann hat sich der Vorfall ereignet (Datum, Uhrzeit)?
3. Wo hat sich der Vorfall ereignet (Gebäude, Raum)?
4. Art des Vorfalls (Schad-Software-Befall, Einbruch ins System, ...)?
5. Welches System ist betroffen (Name, IP-Adresse)?

Seitenanfang

Letzte Änderung: 02. November 2021 | PDF-Version