Handlungsempfehlung der Goethe-Universität Frankfurt zur Nutzung von E-Mail-Diensten

Diese Handlungsempfehlung gilt für alle Angehörigen der Goethe-Universität Frankfurt. Sie regelt die dienstliche Nutzung von E-Mail-Diensten. Ordnungen und Satzungen der Goethe-Universität, insbesondere die IT-Sicherheitsordnung, IT-Sicherheitsrichtlinie und die IuK-Nutzungsordnung[1], werden durch diese Handlungsempfehlung nicht berührt.

Sowohl beruflich als auch privat ist der E-Mail-Dienst ein viel genutztes Kommunikationsmittel. E-Mails beinhalten oft nicht nur Text, sondern auch Links zu Webseiten und Downloads sowie Anhänge wie Bilder und Dokumente. Dadurch entstehen aber auch Risiken bei der E-Mail-Kommunikation. Angreifer und Kriminelle nutzen die Neugier der Menschen aus, um Schadsoftware per E-Mail zu verbreiten und an vertrauliche Daten wie Passwörter, Zugangsdaten oder Kreditkartennummern heranzukommen.

Bei der Nutzung von E-Mail-Diensten sind folgende Regeln des Sicherheits-Management-Teams (SMT) der Goethe-Universität zu beachten:

1) Für **dienstliche Belange** muss die dienstliche E-Mail-Adresse der Goethe-Universität Frankfurt zur elektronischen Kommunikation genutzt werden, sowohl als Empfangs- als auch als Absender-Adresse.

2) Die **automatische Weiterleitung** von dienstlichen E-Mails an E-Mail-Adressen externer Mail-Systeme, die nicht von der Goethe-Universität Frankfurt betrieben werden, ist **nicht zulässig**. Dienstliche Nutzung **externer E-Mail-Adressen** muss vom behördlichen **Datenschutzbeauftragten** der Goethe-Universität genehmigt werden (dsb@uni-frankfurt.de).

3) **Dienstliche E-Mail-Adressen** sollten **nicht** zur Nutzung **privater externer Dienstleistungen** (z. B. soziale Netzwerke, Online Shopping usw.) verwendet werden.

4) **Studierenden** wird aus Sicherheitsgründen empfohlen, die **Uni-Mail-Accounts** zur elektronischen Kommunikation mit Angehörigen der Universität zu verwenden.

5) Alle Beschäftigten der Goethe-Universität Frankfurt sollen – soweit möglich – Studierende nur per Uni-Mail-Adressen (**@xxx.uni-frankfurt.de-Adressen**) kontaktieren (mit Ausnahme von Antworten auf ihre E-Mails).

[1] Allgemeine Nutzungsordnung für die Informationsverarbeitungs- und Kommunikationsinfrastruktur der Goethe-Universität Frankfurt

6) Verseuchte **E-Mail-Anhänge** und **Links** sind einer der häufigsten Wege, Schadsoftware in Computer einzuschleusen. Deshalb gilt stets erhöhte Aufmerksamkeit vor dem Klicken auf einen Link bzw. vor dem Öffnen eines Anhangs. Absender, Betreff und E-Mail-Text sollten stimmig und plausibel sein.

7) **Bewerbungen** bzw. **Bewerbungsunterlagen** dürfen ausschließlich im **PDF-Format** eingereicht werden. Im Falle von Zip-Dateien oder Word-Dokumenten können Sie die Bewerber/innen dazu auffordern, Bewerbungen im PDF-Format noch einmal einzureichen.

8) **Digitale Zertifikate** bescheinigen die Vertrauenswürdigkeit von Kommunikationspartnern. Achten Sie auf Gültigkeit und Vertrauenswürdigkeit des Zertifikats, wenn Sie eine signierte E-Mail erhalten.

9) Bei Fragen können Sie sich an Ihren zuständigen IT-Support bzw. an Ihre/n IT-Sicherheitsbeauftragte/n wenden.

Informationsquellen

- Bundesamt für Sicherheit in der Informationstechnik (BSI)
  https://www.bsi-fuer-buerger.de

- DFN Computer Emergency Response Team (DFN-CERT)
  https://www.dfn-cert.de

- IT-Sicherheitsmanagement-Team (SMT) der Goethe-Universität
  https://www.uni-frankfurt.de/smt

- Goethe-Universität Computer Emergency Response Team (GU-CERT)
  https://www.rz.uni-frankfurt.de/gu-cert

- Hochschulrechenzentrum (HRZ) der Goethe-Universität
  https://www.uni-frankfurt.de/hrz/it-sicherheit