

# IT-Sicherheit

Die IT-Sicherheitsinfrastruktur an der UHH ist aufgrund der Größe der Universität, der über die Stadt verteilten Campusbereiche und den zu beachtenden Verantwortungsbereichen komplex strukturiert. Die universitätsübergreifenden Sicherheitsmaßnahmen werden vom RRZ koordiniert und größtenteils auch erbracht. Ergänzt werden diese Sicherheitsmaßnahmen durch dezentrale Dienstleistungen in den verschiedenen Fachbereichen der UHH.

Zu den technischen Sicherheitsaspekten zählen die nach Stand der Technik üblichen Mechanismen. An der UHH werden diverse Sicherheitsdienstleistungen vom RRZ erbracht. Hierzu zählen insbesondere:

- Betrieb von Firewalls
- Betrieb von IDS
- Vorfallsbehandlung (Incident-Management)
- Patchverteilung
- Virenprüfung
- Sicherheitsberatung

Zu den organisatorischen Sicherheitsaspekten gehört die Schaffung von verbindlichen Richtlinien für den Netzbetrieb und der Netzbenutzung ( Net-Policy und deren untergeordneten Richtlinien), sowie die hierarchische Strukturierung des Fehler- und Störungsmanagements durch Delegation von (Teil-)Verantwortlichkeiten an geschulte Mitarbeiter und Mitarbeiterinnen vor Ort in den dezentralen Einrichtungen der UHH.

Hierzu zählt auch die zentral im RRZ koordinierte und dezentral umgesetzte Vorfallsbearbeitung bei Bekanntwerden von Sicherheitsvorfällen durch interne IDS-Mechanismen (Sperrlisten-Management) oder externe Meldung an entsprechende eMail-Adressen der UHH ([abuse\(at\)uni-hamburg.de](mailto:abuse@uni-hamburg.de)).

Über eine zentrale Service-Stelle (RRZ-Serviceline) können Benutzer bei Sicherheitsproblemen Hilfe anfordern. Sie werden in komplizierten Fällen, gestützt durch ein Trouble-Ticket-System, an Spezialisten des RRZ weitervermittelt.

Über eMail-Verteiler und WWW-basierte Informationssysteme werden darüber hinaus Sicherheitsmeldungen (WIN-SEC, WIN-SEC-SSC Meldungen) des DFN-CERT an dezentrale DV-Verantwortliche weitergeleitet bzw. universitätsintern verteilt.