Aufgaben und Ziele der Informationssicherheit am Beispiel der Goethe-Universität Frankfurt

Prof. Dr. Udo Kebschull

Adham Zeidan

Goethe-Universität Frankfurt

kebschull@hrz.uni-frankfurt.de

Agenda

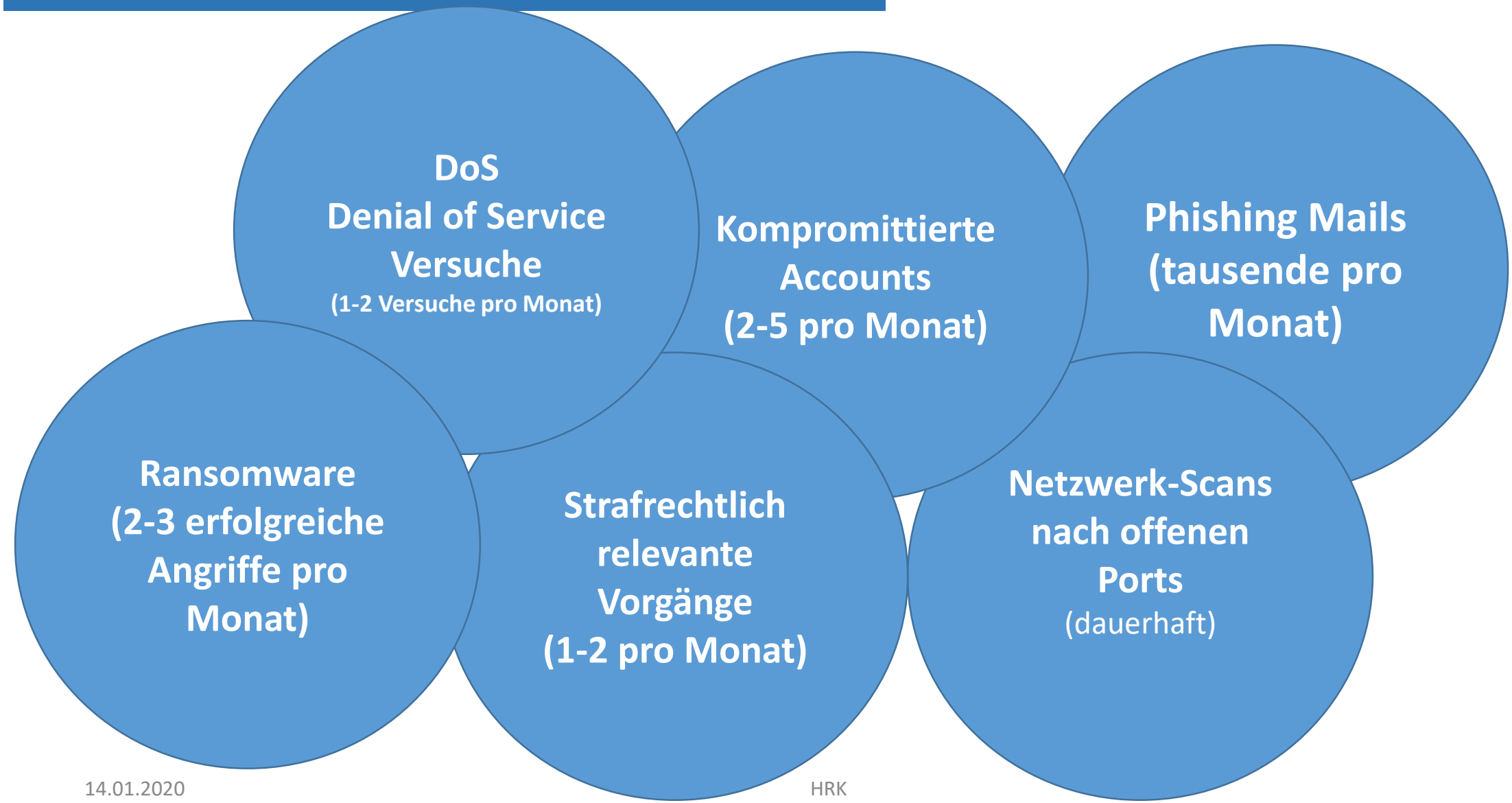
- **Typische Angriffe auf die Hochschul-IT**
- **Der Begriff Informationssicherheit**
- **Das Sicherheitskonzept der Goethe-Universität Frankfurt**
- **Wo stehen wir?**
- **Erkenntnisse**

Komplexe Infrastruktur

IT-Systeme am Universitätsnetz der Goethe-Universität

- **Mehr als**
  - **25 Mailserver**
  - **50 Webserver**
  - **60.000 aktive Universitäts-Accounts**
  - **700 Netzwerkdrucker**
  - **10.000 dienstliche Endgeräte**
- **Eine unbekannte Anzahl privater Geräte**
  - **Notebook**
  - **Tablets**
  - **Mobiltelefon**

Typische Angriffe auf die Hochschul-IT

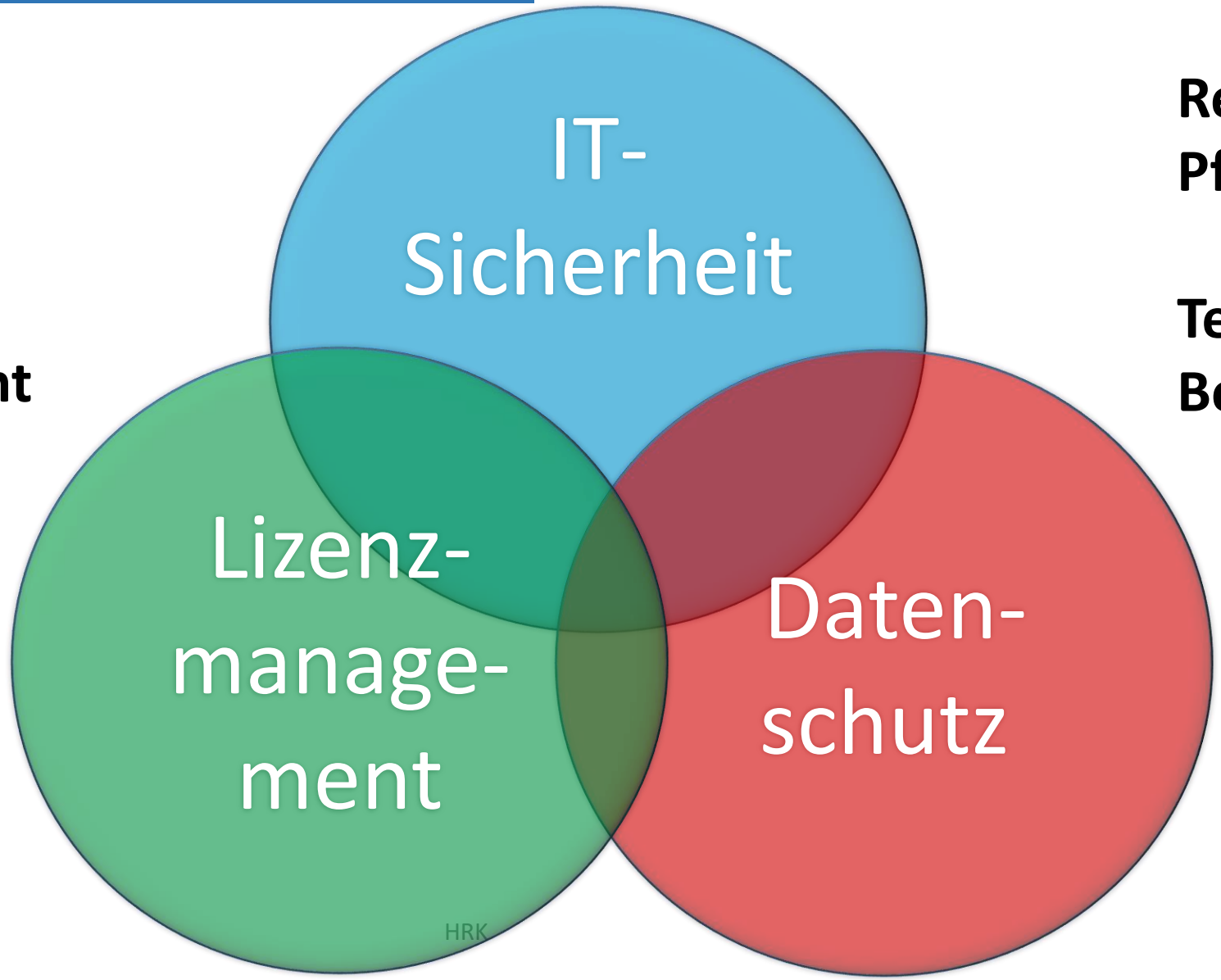


Was ist eigentlich Informationssicherheit?

- **Informationssicherheit = Datensicherheit**
  - **Informationssicherheit oder Datensicherheit ist der Schutz von Daten hinsichtlich gegebener Anforderungen an deren Vertraulichkeit, Verfügbarkeit und Integrität**
- **Datenschutz**
  - **Schutz personenbezogener Daten vor Missbrauch durch Dritte**
- **IT-Sicherheit**
  - **Teilmenge der Informationssicherheit, die sich auf den Schutz elektronisch gespeicherter Informationen und deren Verarbeitung konzentriert**
  - **Ziel: Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit von elektronisch gespeicherten Daten, IT-Diensten und -Systemen**
- **Datensicherung (engl. Backup/Restore)**
  - **Erstellung von Sicherungskopien zum Schutz vor Datenverlust**

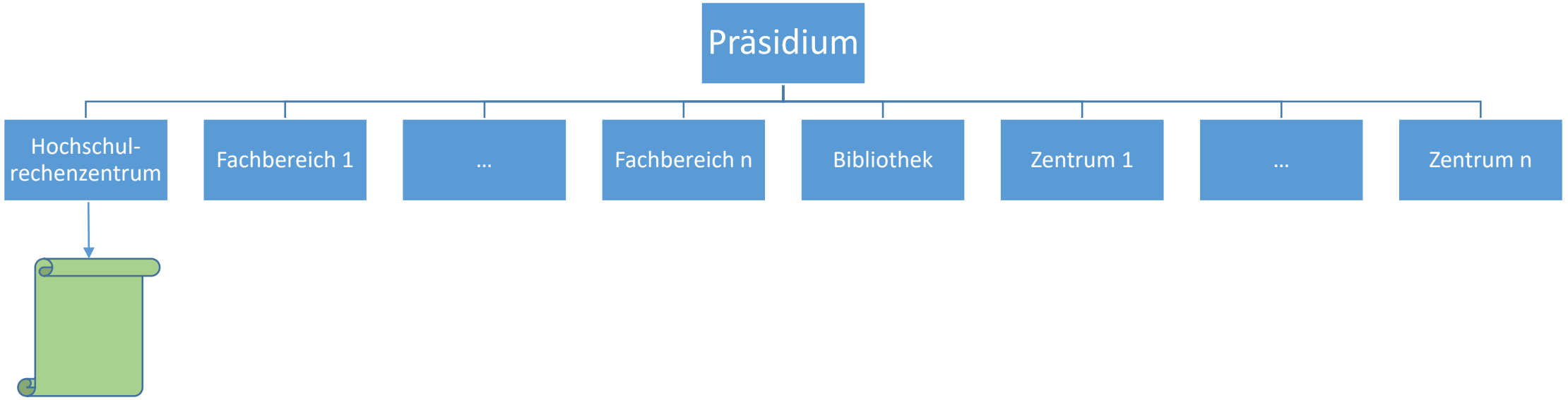
Aufgaben eines IT-Betreibers

Datenschutz
≠
IT-Sicherheit
≠
Rechtssicherheit
im Lizenzmanagement



Rechtliche
Pflichten
&
Technischer
Betrieb

Das Sicherheitskonzept der Goethe-Universität



Das Sicherheitskonzept der Goethe-Universität


14. Mai 2013

UniReport

Goethe-Universität Frankfurt am Main

Satzungen und Ordnungen

IT-Sicherheitsordnung der Goethe-Universität Frankfurt am Main

Beschluss des Präsidiums vom 7. Mai 2013 gemäß § 37 Abs. 8 Hessisches Hochschulgesetz vom 14. September 2009 in der geltenden Fassung (HHG, GVBL I S.666ff.)

Präambel

Der Betrieb einer Hochschule hängt in hohem Maße von der Qualität ihrer IT-Dienstleistungen ab. Das Vertrauen der Benutzerinnen und Benutzer in die Informationstechnik bildet die Grundlage für ihren erfolgreichen Einsatz. Integrität, Vertraulichkeit und Verfügbarkeit der IT-Dienste und Daten sind nachhaltig sicherzustellen. Um dieser Verpflichtung angesichts einer wachsenden Bedrohung der sich rasch weiterentwickelnden Technik bei gleichzeitig begrenzter personeller und finanzieller Ausstattung der Hochschule nachzukommen, müssen sämtliche Einrichtungen der Hochschule den Schutz der Informationstechnik als gemeinsame Herausforderung begreifen, die auf der Basis einer einheitlichen Rahmenrichtlinie der IT-Sicherheit der Hochschule in einem kontinuierlichen IT-Sicherheitsprozess angegangen wird. Unerlässliche Grundvoraussetzung für den Erfolg ist dabei ein Ausgleich zwischen den Anforderungen akademischer Freiheit und IT-Sicherheit.

§ 1 Gegenstand der Ordnung

Die IT-Sicherheitsordnung bestimmt die für den IT-Sicherheitsprozess der Goethe-Universität erforderliche Organisationsstruktur und definiert Aufgaben und Verantwortlichkeiten.

§ 2 Geltungsbereich

Die IT-Sicherheitsordnung erstreckt sich auf die gesamte Informationstechnik der Goethe-Universität in ihren wissenschaftlichen und nicht wissenschaftlichen Einrichtungen und gilt für sämtliche Benutzerinnen und Benutzer, die diese einsetzen oder bereitstellen. Sie ist verbindlich für die Fachbereiche und wissenschaftlichen, zentralen oder sonstigen Einrichtungen der Hochschule sowie von diesen mit der Wahrnehmung von IT-Dienstleistungen und sonstigen mit der IT-Sicherheit zusammenhängenden Tätigkeiten beauftragten Firmen oder Personen. Für den Bereich des Klinikums, speziell der Krankenversorgung, sollen gesonderte Regelungen gelten. Bis zu ihrem Erlass gilt diese Ordnung entsprechend.

§ 3 Beteiligte des IT-Sicherheitsprozess

Am IT-Sicherheitsprozess sind beteiligt:
(1) Präsidium der Universität
(2) zentrale IT-Sicherheitsbeauftragte
(3) IT-Sicherheits-Management-Team (SMT)
(4) dezentrale IT-Sicherheitsbeauftragte
(5) Personalrat der Hochschule
(6) behördliche Datenschutzbeauftragte der Universität
(7) Einrichtungen der Hochschule
(8) Hochschulrechenzentrum

§ 4 Einsetzung des zentralen IT-Sicherheitsbeauftragten

(1) Das Präsidium setzt eine zentrale IT-Sicherheitsbeauftragte oder einen zentralen IT-Sicherheitsbeauftragten ein, die oder der ihm unmittelbar berichtet.

(2) Jeder Fachbereich, wissenschaftliche, zentrale und sonstige Einrichtung der Hochschule benennt eine dezentrale IT-Sicherheitsbeauftragte oder einen dezentralen IT-Sicherheitsbeauftragten.

(3) Eine dezentrale IT-Sicherheitsbeauftragte oder ein

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

IT-Sicherheitsrichtlinie für die Goethe-Universität Frankfurt

Version 1.0.12

Steckbrief

Zielsetzung	Einheitliche Sicherheitsstandards zur Gewährleistung eines ordnungsgemäßen IT-Betriebs
Regelungsinhalte	Regelungen zur Informationssicherheit und Datenschutz
Zielgruppe	Alle Mitglieder der Goethe-Universität Frankfurt und Nutzer deren IT-Ressourcen
Geltungsbereich	Alle Einrichtungen der Goethe-Universität Frankfurt
Gültigkeitsdauer	Unbegrenzt

Präsidium

SMT

GU-CERT

Hochschul-rechenzentrum

Fac

n

Bibliothek

entrum n

Die Sicherheitsordnung der Goethe-Universität

14. Mai 2013

UniReport

Goethe-Universität I Frankfurt am Main — Satzungen und Ordnungen

IT-Sicherheitsordnung der Goethe-Universität Frankfurt am Main

Beschluss des Präsidiums vom 7. Mai 2013 gemäß § 37 Abs. 8 Hessisches Hochschulgesetz vom 14. September 2009 in der geltenden Fassung (HHG, GVBL I S.666ff.)

Präambel

Der Betrieb einer Hochschule hängt in hohem Maße von der Qualität ihrer IT-Dienstleistungen ab. Das Vertrauen der Benutzerinnen und Benutzer in die Informationstechnik bildet die Grundlage für ihren erfolgreichen Einsatz. Integrität, Vertraulichkeit und Verfügbarkeit der IT-Dienste und Daten sind nachhaltig sicherzustellen. Um dieser Verpflichtung angesichts einer wachsenden Bedrohung der sich rasch weiterentwickelnden Technik bei gleichzeitig begrenzter personeller und finanzieller Ausstattung der Hochschule nachzukommen, müssen sämtliche Einrichtungen der Hochschule den Schutz der Informationstechnik als gemeinsame Herausforderung begreifen, die auf der Basis einer einheitlichen Rahmenrichtlinie der IT-Sicherheit der Hochschule in einem kontinuierlichen IT-Sicherheitsprozess angegangen wird. Unerlässliche Grundvoraussetzung für den Erfolg ist dabei ein Ausgleich zwischen den Anforderungen akademischer Freiheit und IT-Sicherheit.

§ 1 Gegenstand der Ordnung

Die IT-Sicherheitsordnung bestimmt die für den IT-Sicherheitsprozess der Goethe-Universität erforderliche Organisationsstruktur und definiert Aufgaben und Verantwortlichkeiten.

§ 2 Geltungsbereich

Die IT-Sicherheitsordnung erstreckt sich auf die gesamte Informationstechnik der Goethe-Universität in ihren wissenschaftlichen und nicht wissenschaftlichen Einrichtungen und gilt für sämtliche Benutzerinnen und Benutzer, die diese einsetzen oder bereitstellen. Sie ist verbindlich für die Fachbereiche und wissenschaftlichen, zentralen oder sonstigen Einrichtungen der Hochschule sowie von diesen mit der Wahrnehmung von IT-Dienstleistungen und sonstigen mit der IT-Sicherheit zusammenhängenden Tätigkeiten beauftragten Firmen oder Personen. Für den Bereich des Klinikums, speziell der Krankenversorgung, sollen gesonderte Regelungen gelten. Bis zu ihrem Erlass gilt diese Ordnung entsprechend.

§ 3 Beteiligte des IT-Sicherheitsprozess

Am IT-Sicherheitsprozess sind beteiligt:
(1) Präsidium der Universität
(2) zentrale IT-Sicherheitsbeauftragte
(3) IT-Sicherheits-Management-Team (SMT)
(4) dezentrale IT-Sicherheitsbeauftragte
(5) Personalrat der Hochschule
(6) behördliche Datenschutzbeauftragte der Universität
(7) Einrichtungen der Hochschule
(8) Hochschulrechenzentrum

§ 4 Einsetzung des zentralen IT-Sicherheitsbeauftragten

(1) Das Präsidium setzt eine zentrale IT-Sicherheitsbeauftragte oder einen zentralen IT-Sicherheitsbeauftragten ein, die oder der ihm unmittelbar berichtet.

(2) Jeder Fachbereich, wissenschaftliche, zentrale und sonstige Einrichtung der Hochschule benennt eine dezentrale IT-Sicherheitsbeauftragte oder einen dezentralen IT-Sicherheitsbeauftragten.

(3) Eine dezentrale IT-Sicherheitsbeauftragte oder ein

IT-Sicherheitsordnung der Goethe-Universität Frankfurt am Main 1
UniReport Satzungen und Ordnungen vom 14. Mai 2013

regelt

- **Zusammensetzung des Sicherheitsmanagementteams (SMT)**
- **Auftrag des SMT**
- **Umsetzung des IT-Sicherheitsprozesses**

Das SMT der Goethe-Universität

- **Sicherheitsmanagement-Team (SMT)**
  - **Organisation und Management des Sicherheitsprozesses**
  - **Bestellung der dezentralen IT-Sicherheitsbeauftragten**
  - **Organisation der Schutzbedarfsanalyse und Risikoabschätzung**
  - **Schnittstelle zur Universitätsleitung**
- **Zusammensetzung (feste Mitglieder)**
  - **Vorsitz VP**
  - **Behördlicher Datenschutzbeauftragte(r)**
  - **Leiter(in) des HRZ**
  - **Leiter(in) Referat Arbeitsschutz**
  - **Vertretung der dezentralen IT-Sicherheitsbeauftragten**
  - **Geschäftsstelle**

Die Sicherheitsrichtlinie der Goethe-Universität

IT-Sicherheitsrichtlinie

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

IT-Sicherheitsrichtlinie für

die

Goethe-Universität Frankfurt

Version 1.0.12

Steckbrief

Zielsetzung	Einheitliche Sicherheitsstandards zur Gewährleistung eines ordnungsgemäßen IT-Betriebs
Regelungsinhalte	Regelungen zur Informationssicherheit und Datenschutz
Zielgruppe	Alle Mitglieder der Goethe-Universität Frankfurt und Nutzer deren IT-Ressourcen
Geltungsbereich	Alle Einrichtungen der Goethe-Universität Frankfurt
Gültigkeitsdauer	Unbegrenzt

Version 1.0.12 – 2016 1 von 71

regelt

- **Geltungsbereich**
- **Definition von Rollen und Aufgaben**
- **Verantwortlichkeiten und Organisation der IT-Sicherheit**
- **Umsetzung des IT-Grundschutzes an der Goethe-Universität**
- **Feststellung des Schutzbedarfs und Risikobewertung**

Das IT-Sicherheitskonzept der Goethe Universität

14. Mai 2013

UniReport

Goethe-Universität | Frankfurt am Main — Satzungen und Ordnungen

IT-Sicherheitsordnung der Goethe-Universität Frankfurt am Main

Beschluss des Präsidiums vom 7. Mai 2013 gemäß § 37 Abs. 8 Hessisches Hochschulgesetz vom 14. September 2009 in der geltenden Fassung (HHG, GVBL I S.666ff.)

Präambel

Der Betrieb einer Hochschule hängt in hohem Maße von der Qualität ihrer IT-Dienstleistungen ab. Das Vertrauen der Benutzerinnen und Benutzer in die Informationstechnik bildet die Grundlage für ihren erfolgreichen Einsatz. Integrität, Vertraulichkeit und Verfügbarkeit der IT-Dienste und Daten sind nachhaltig sicherzustellen. Um dieser Verpflichtung angesichts einer wachsenden Bedrohung der sich rasch weiterentwickelnden Technik bei gleichzeitig begrenzter personeller und finanzieller Ausstattung der Hochschule nachzukommen, müssen sämtliche Einrichtungen der Hochschule den Schutz der Informationstechnik als gemeinsame Herausforderung begreifen, die auf der Basis einer einheitlichen Rahmenrichtlinie der IT-Sicherheit der Hochschule in einem kontinuierlichen IT-Sicherheitsprozess angegangen wird. Unerlässliche Grundvoraussetzung für den Erfolg ist dabei ein Ausgleich zwischen den Anforderungen akademischer Freiheit und IT-Sicherheit.

§ 1 Gegenstand der Ordnung

Die IT-Sicherheitsordnung bestimmt die für den IT-Sicherheitsprozess der Goethe-Universität erforderliche Organisationsstruktur und definiert Aufgaben und Verantwortlichkeiten.

§ 2 Geltungsbereich

Die IT-Sicherheitsordnung erstreckt sich auf die gesamte Informationstechnik der Goethe-Universität in ihren wissenschaftlichen und nicht wissenschaftlichen Einrichtungen und gilt für sämtliche Benutzerinnen und Benutzer, die diese einsetzen oder bereitstellen. Sie ist verbindlich für die Fachbereiche und wissenschaftlichen, zentralen oder sonstigen Einrichtungen der Hochschule sowie von diesen mit der Wahrnehmung von IT-Dienstleistungen und sonstigen mit der IT-Sicherheit zusammenhängenden Tätigkeiten beauftragten Firmen oder Personen. Für den Bereich des Klinikums, speziell der Krankenversorgung, sollen gesonderte Regelungen gelten. Bis zu ihrem Erlass gilt diese Ordnung entsprechend.

§ 3 Beteiligte des IT-Sicherheitsprozess

Am IT-Sicherheitsprozess sind beteiligt:
(1) Präsidium der Universität
(2) zentrale IT-Sicherheitsbeauftragte
(3) IT-Sicherheits-Management-Team (SMT)
(4) dezentrale IT-Sicherheitsbeauftragte
(5) Personalrat der Hochschule
(6) behördliche Datenschutzbeauftragte der Universität
(7) Einrichtungen der Hochschule
(8) Hochschulrechenzentrum

§ 4 Einsetzung des zentralen IT-Sicherheitsbeauftragten

(1) Das Präsidium setzt eine zentrale IT-Sicherheitsbeauftragte oder einen zentralen IT-Sicherheitsbeauftragten ein, die oder der ihm unmittelbar berichtet.

(2) Jeder Fachbereich, wissenschaftliche, zentrale und sonstige Einrichtung der Hochschule benennt eine dezentrale IT-Sicherheitsbeauftragte oder einen dezentralen IT-Sicherheitsbeauftragten.

(3) Eine dezentrale IT-Sicherheitsbeauftragte oder ein

IT-Sicherheitsordnung der Goethe-Universität Frankfurt am Main 1
UniReport Satzungen und Ordnungen vom 14. Mai 2013

IT-Sicherheitsrichtlinie

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

IT-Sicherheitsrichtlinie für die Goethe-Universität Frankfurt

Version 1.0.12

Steckbrief

Zielsetzung	Einheitliche Sicherheitsstandards zur Gewährleistung eines ordnungsgemäßen IT-Betriebs
Regelungsinhalte	Regelungen zur Informationssicherheit und Datenschutz
Zielgruppe	Alle Mitglieder der Goethe-Universität Frankfurt und Nutzer deren IT-Ressourcen
Geltungsbereich	Alle Einrichtungen der Goethe-Universität Frankfurt
Gültigkeitsdauer	Unbegrenzt

Version 1.0.12 – 2016 — 1 von 71

Schulungen

Handlungsempfehlungen

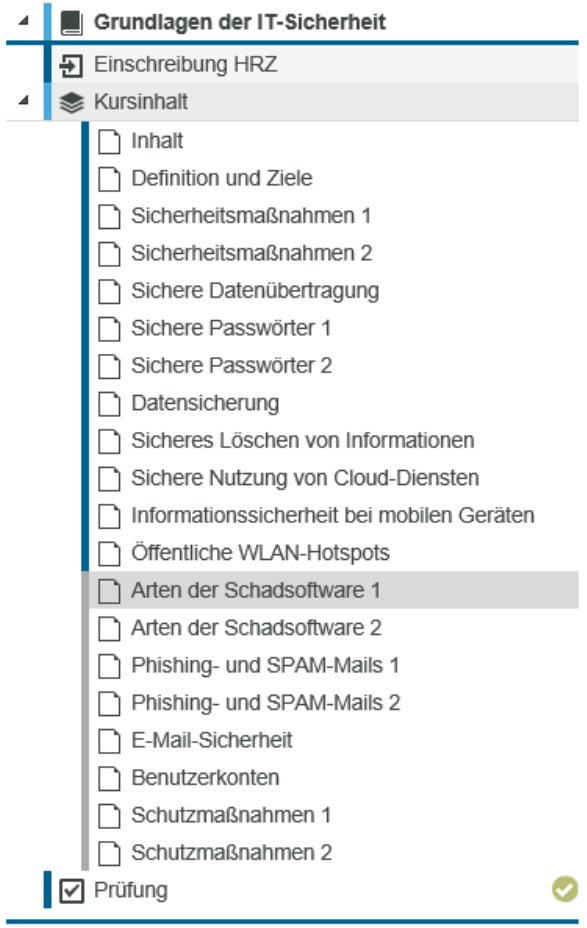
Handlungsanweisungen

Online Schulung für IT-Nutzer(innen)

- **Schulung mit anschließender e-Prüfung**

Quelle: © TAlex / Fotolia.com

- Arten der Schadsoftware (Malware)
  - Virus
    - Löschen oder Beschädigung von Informationen, Daten und Systemen
  - Trojaner
    - Erpressung (Verschlüsselungs-Trojaner)
    - Spionage und Aufzeichnen (Tastureingaben, Mikrofon, Webcam und Anmeldeinformation)
    - Missbrauch von Systemen und Geräten für illegale Aktivitäten
  - Wurm
    - Verbreitet sich extrem schnell im Netzwerk
    - Ziel: Sicherheitslücken öffnen bzw. schaffen für andere Malwaresorten (Viren, Trojaner)
  - Verbreitung der Schadsoftware folgt durch:
    - Verdächtige Mail-Anhänge
    - Spam- und Phishing-Mails mit verdächtigen Links
    - Durch Besuchen von kompromittierten Webseiten
    - Durch Ausführung von infizierten Dateien/Downloads



Handlungsempfehlungen für Nutzer(innen)

- **Nutzung von Internetdiensten**
- **Umgang mit Passwörtern**
- **Nutzung von mobilen Geräten**
- **Auslagerung von Daten in die Cloud**
- **Nutzung von E-Maildiensten**

SMT
SICHERHEITSMANAGEMENT-TEAM

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Handlungsempfehlung der Goethe-Universität Frankfurt zur Nutzung von E-Maildiensten

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 heran zu kommen.

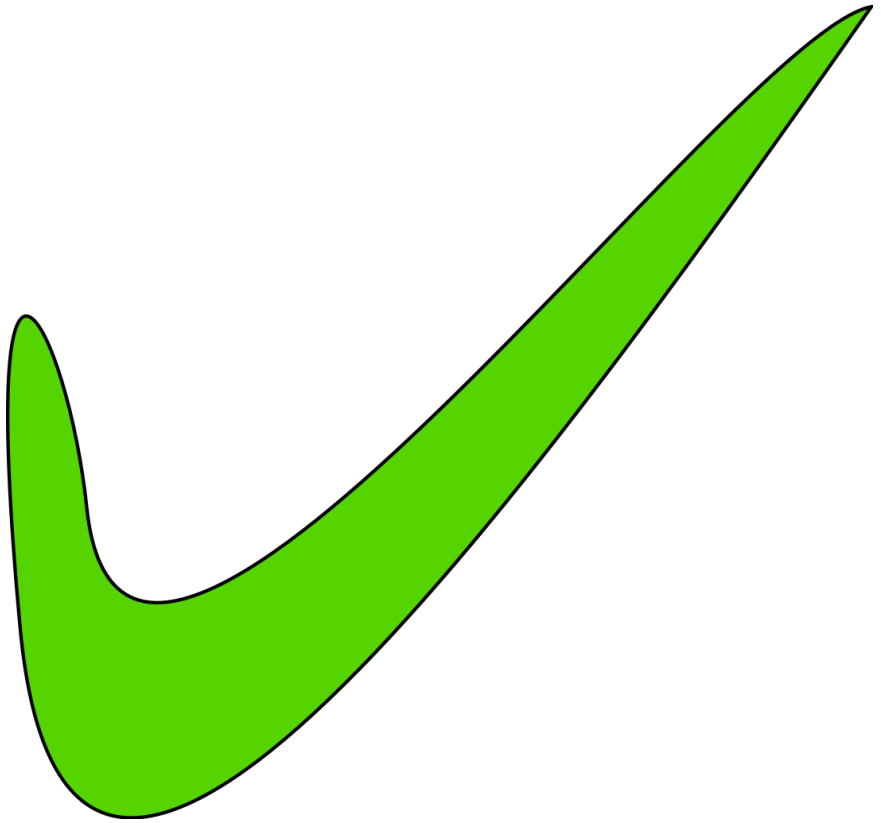
Bei der Nutzung von E-Maildiensten sind folgende Regeln des Sicherheits-Management-Teams (SMT) der Goethe-Universität zu beachten:

Das CERT an der Goethe-Universität

- **Computer Emergency Response Team (CERT)**
- **<u>Operative</u> Abwehr von Angriffen**
- **Testen von IT-Infrastrukturen auf Sicherheitslücken**
- **Beobachten von SPAM-Wellen**
- **Hilfe bei festgestellten Angriffen**
  - **Phishing**
  - **Ransomware**
- **Zusammensetzung:**
  - **Ein Festangestellter (50%) und eine einstellige Zahl an Freiwilligen**

Wo stehen wir jetzt?

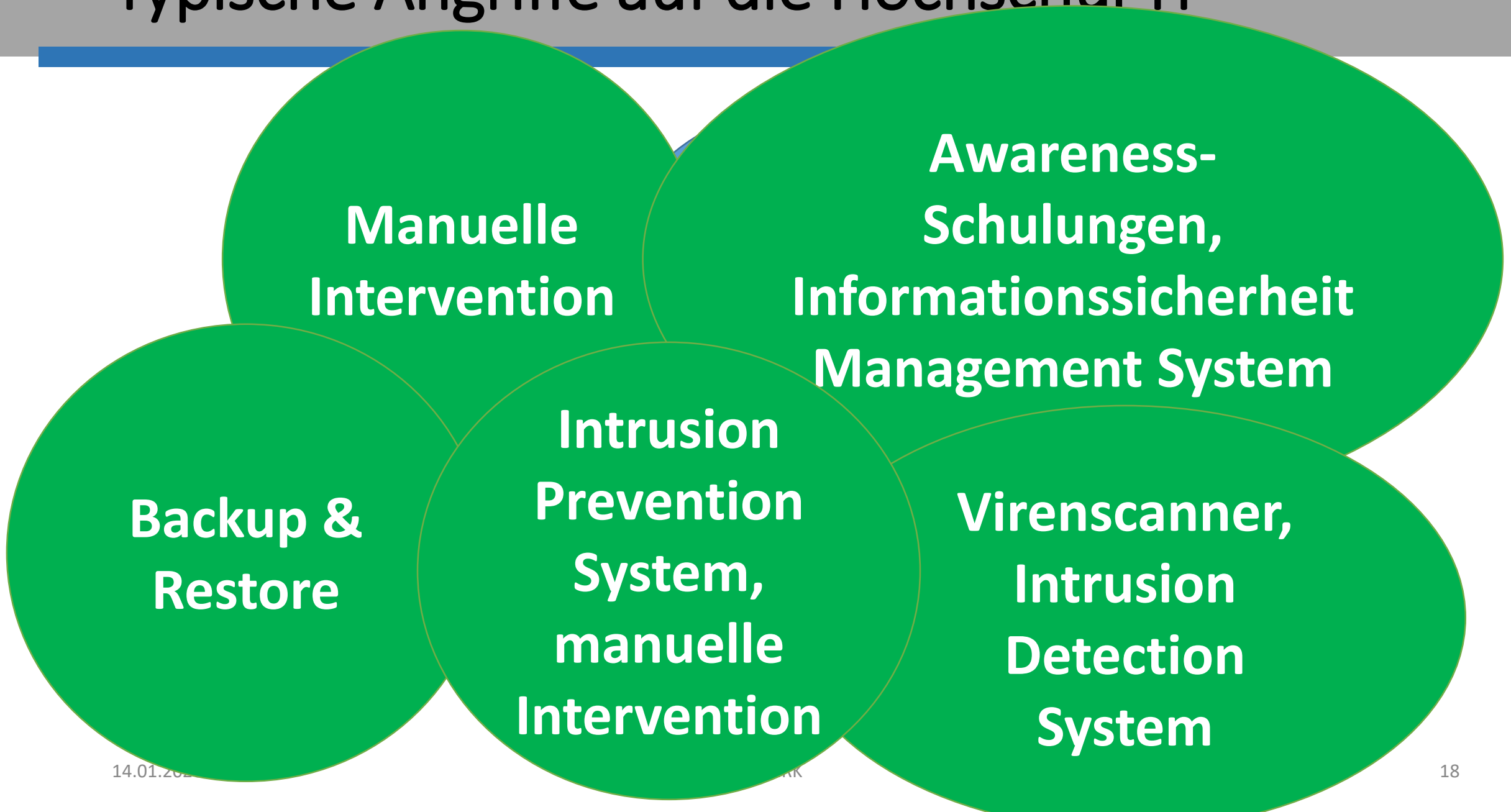
- **Erreichte Meilensteine / Ziele**
  - **Die IT-Sicherheitsordnung**
  - **Die IT Sicherheitsrichtlinie**
  - **Online Schulung für die Nutzer**
  - **Benennung der IT-Sicherheitsbeauftragten**
  - **Schulung der IT Sicherheitsbeauftragten**
  - **Die ersten Handlungsempfehlungen für Nutzende**
  - **Anmeldung von IT-Verfahren bzw. –Dienste**
  - **Strukturanalyse**
  - **Aufbau des Incident Response Teams (GU-CERT)**



Nächste Schritte

- **Veröffentlichung der ersten Handlungsanweisungen für Administrator(inn)en**
- **Erweiterung der Handlungsempfehlungen**
- **IT-Dokumentation und Abbildung von IT-Verfahren**
- **Weitere Schulungsangebote für die IT-Sicherheitsbeauftragten**
- **Erweiterung der Sensibilisierungsmaßnahmen**
- **Durchführung von Schutzbedarfsanalysen**
- **Durchführung von Risikobewertungen**

Typische Angriffe auf die Hochschul-IT



Erkenntnisse über die IT der Goethe-Universität

- **Über 50 dezentrale IT-Sicherheitsbeauftragte wurden benannt**
  - **Zentrale Einrichtungen (HRZ, UB, SD, IKH, ABL, usw.)**
  - **Verwaltungsbereichen (IMM, BAM, SSC, Justitiariat, Finanzen und Controlling, usw.)**
  - **Fachbereichen (FB01 – FB16)**
  - **Institute und Zentren**

Vielen Dank!

Prof. Dr. Udo Kebschull

Adham Zeidan

Goethe-Universität Frankfurt

kebschull@hrz.uni-frankfurt.de