

DEN  
deutsches forschungsnetz





# Informationssicherheits-Dienste des DFN für Hochschulen

HRK-Workshop „Informationssicherheit als strategische Aufgabe der  
Hochschulleitung“

Dr. Ralf Gröper | 25. + 26.11.2019



# Der DFN-Verein: Übersicht

- ▶ Verein zur Förderung eines **D**eutschen **F**orschungs**N**etzes e.V.
- ▶ Gegründet **1984**
- ▶ **~345** Mitglieder (darunter sehr viele Hochschulen)
- ▶ DFN organisiert Forschungsnetz (X-WiN) und netznahe Dienste
  - ▷ für "öffentlich geförderte und die gemeinnützige **Forschung**"
  - ▷ viele Dienste mit Bezug zu **Informationssicherheit**
  - ▷ Zusatzdienste größtenteils im Entgelt für Anschluss enthalten

# Der DFN-Verein: Übersicht

- ▶ Der DFN versorgt Wissenschaftseinrichtungen
  - ▷ an über **800** Standorten
  - ▷ mehr als **2,5 Millionen** versorgte Mitarbeitende und Studierende
- ▶ **~40M€** Jahresbudget, aus Entgelten der Teilnehmer
- ▶ Standorte in Berlin und Stuttgart
  - ▷ **~60 Mitarbeiter\*innen**
  - ▷ zzgl. DFN-CERT

# Hochschulen im Fokus der Angreifer?

Hacker-Angriffe auf Hochschulen

## Wenn die Praktikantin aus China in Verdacht gerät

Quelle: Deutschlandfunk, 14.11.2019

„Emotet“ in Berlin

09.11.2019, 23:42 Uhr

## Computervirus befällt auch Humboldt-Uni

Quelle: Der Tagesspiegel

## Antwerp University hit by cyberattack

Monday, 28 October 2019

Quelle: The Brusseles Times



DFN-CERT @DFNCERT · 13. Nov.

⚠ Achtung: Aktuell Phishing gegen die @UniLeipzig! Bitte keine Daten eingeben und keine Links anklicken! ⚠

URL: [hxxps://notranjamodrost\[.\]si/wpincludes/error/nil/all/unileipzig/unileipzig.htm](https://notranjamodrost[.]si/wpincludes/error/nil/all/unileipzig/unileipzig.htm) (@Hetzner\_Online)

SSL-Zertifikat von @SectigoHQ



DFN-CERT @DFNCERT · 12. Nov.

⚠ Achtung: Aktuell Phishing gegen die @tuBraunschweig! Bitte keine Daten eingeben und keine Links anklicken! ⚠

URL: [hxxps://sostanj\[.\]tv/statistika/images/clean/all/tubraunschweig/tubraunschweig.htm](https://sostanj[.]tv/statistika/images/clean/all/tubraunschweig/tubraunschweig.htm)

# DFN-Dienste mit Sicherheitsbezug

- ▶ DFN-Dienste sind **Bausteine**
- ▶ Bausteine müssen in Prozesse des **Informationssicherheits-  
Managementsystems** der Einrichtungen eingebunden sein
  - ▶ DFN-CERT berät bei **Konzeption** und **Einführung** eines ISMS
- ▶ Welche Bausteine gibt es vom DFN?

# Dienst DFN-CERT + DoS-Schutz

## ▶ **DFN-CERT** (CERT = **C**omputer **E**mergency **R**esponse **T**eam)

### ▶ Incident Response

- ▶ Zertifiziert nach Trusted Introducer

### ▶ CERT-Portal

- ▶ Schwachstellenmeldungen
- ▶ Automatische Warnmeldungen bei erkannten Auffälligkeiten
- ▶ Verwundbarkeits-Scanner

## ▶ **DoS**-Erkennung, Analyse & Mitigation

- ▶ Schutz des DFN-Backbones
- ▶ DoS-Basisschutz für teilnehmende Einrichtungen
- ▶ erweiterter DoS-Schutz für teilnehmende Einrichtungen

- ▶ **DFN-AAI**: Föderierter Login bei externen Anbietern (z.B. Fachverlage)
- ▶  : Internationaler Zugang zu WLAN-Netzen
- ▶ **DFN-PKI**: Vertrauensdiensteanbieter gemäß eIDAS-VO
  - ▶ Zertifiziert nach europäischer Norm ETSI EN 319 411-1

# Weitere Dienste mit Sicherheitsbezug



- ▶ **DFN-MailSupport** (E-Mail SPAM & Virus-Erkennung)

- ▶ Zertifiziert nach ISO27001/BSI IT-Grundschutz und Datenschutz

# Veranstaltungen, Konferenzen, Veröffentlichungen des DFN



- ▶ Veranstaltungen und Konferenzen
  - ▷ Konferenz **Sicherheit in vernetzten Systemen**
  - ▷ Konferenz **Datenschutz**
  - ▷ **DFN-Betriebstagung**
  - ▷ **Forum Hochschulkanzler**
  - ▷ ...und viele weitere...
  
- ▶ Veröffentlichungen
  - ▷ **DFN-Mitteilungen**
  - ▷ **Infobrief Recht**

# Ausblick: Security Operations

- ▶ Ziel: Proaktive **Angriffserkennung** und –**Abwehr**
  - ▶ Ergänzung der bestehenden Dienste
- ▶ Angriffserkennung und Abwehr durch **Security Operations Center** (SOC)
  - ▶ Ständige Auswertung vor Ort vorhandener Daten
- ▶ Ein Anwendungsfall (unter vielen): Früherkennung von **Phishing-Kampagnen**
  - ▶ Bereitstellung von *Threat Intelligence* zur zeitnahen Abwehr an Hochschulen
- ▶ **Sukzessive Einführung** in den kommenden Jahren
  - ▶ **Mehrere Ausbaustufen**, Ressourcen müssen aufgebaut werden
  - ▶ Ggf. gestaffeltes zusätzliches Entgelt



## **Dr. Ralf Gröper**

Bereichsleiter „Security, Trust & Identity Services“

DFN-Verein  
Alexanderplatz 1  
10178 Berlin

Tel. +49 (0)30 884299-337  
e-mail: [groeper@dfn.de](mailto:groeper@dfn.de)

