FH MÜNSTER
University of Applied Sciences

Cyber-Sicherheit und deutsche Hochschulen
Ein Ausblick

Workshop „Informationssicherheit
als strategische Aufgabe der Hochschulleitung“

Prof. Dr. Sebastian Schinzel

Email: schinzel@fh-muenster.de
Twitter: @seecurity

„Skript-Kiddies“

Angreifer-Ziele:

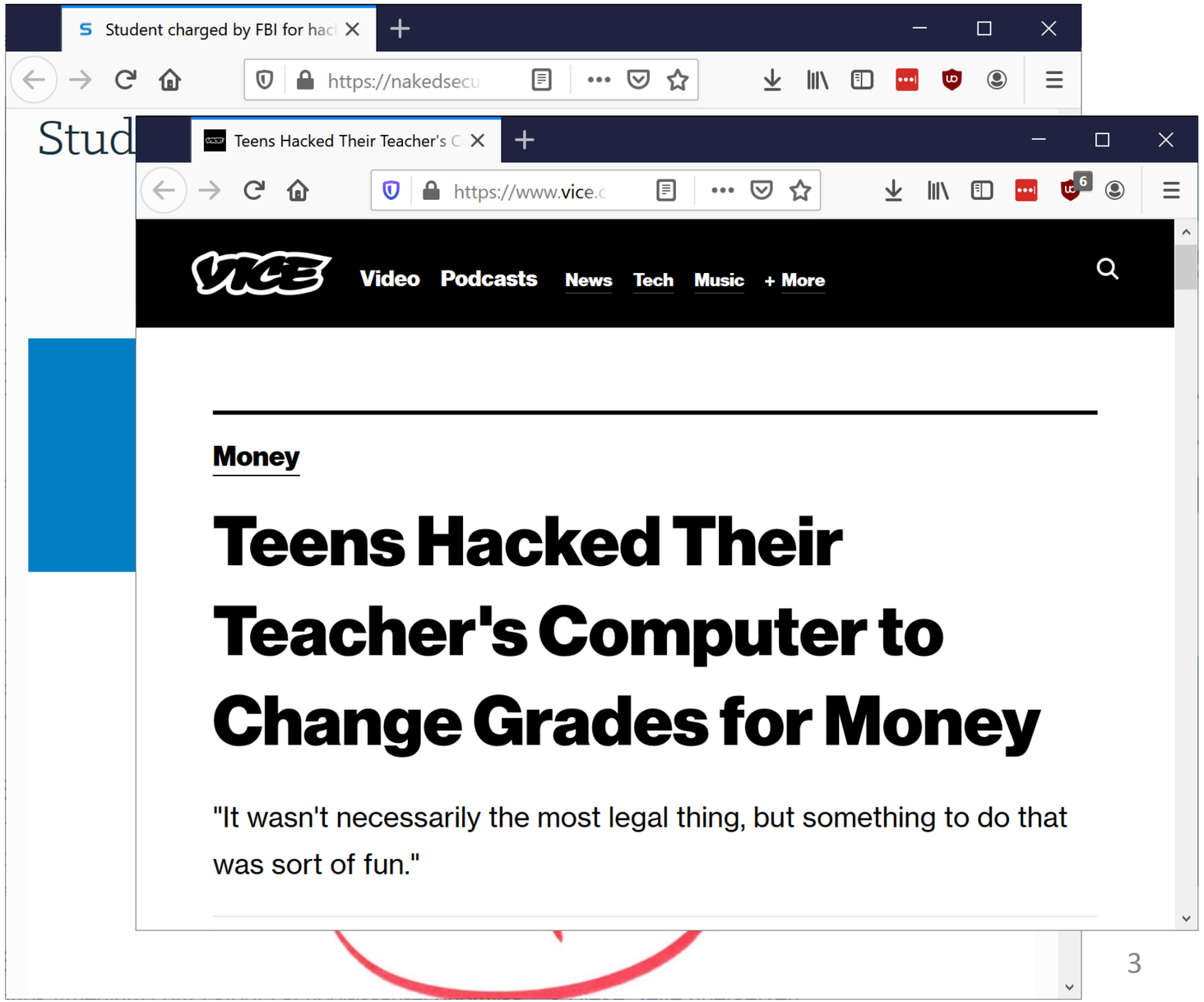
- Einfache Sabotage
- Sachbeschä-digung
- Rufschädigung

PDF: Criminal Complaint Against Student Charged With Making Harvard Bomb Threat

Angreifer-Ziele:

- Noten ändern
- Geld verdienen

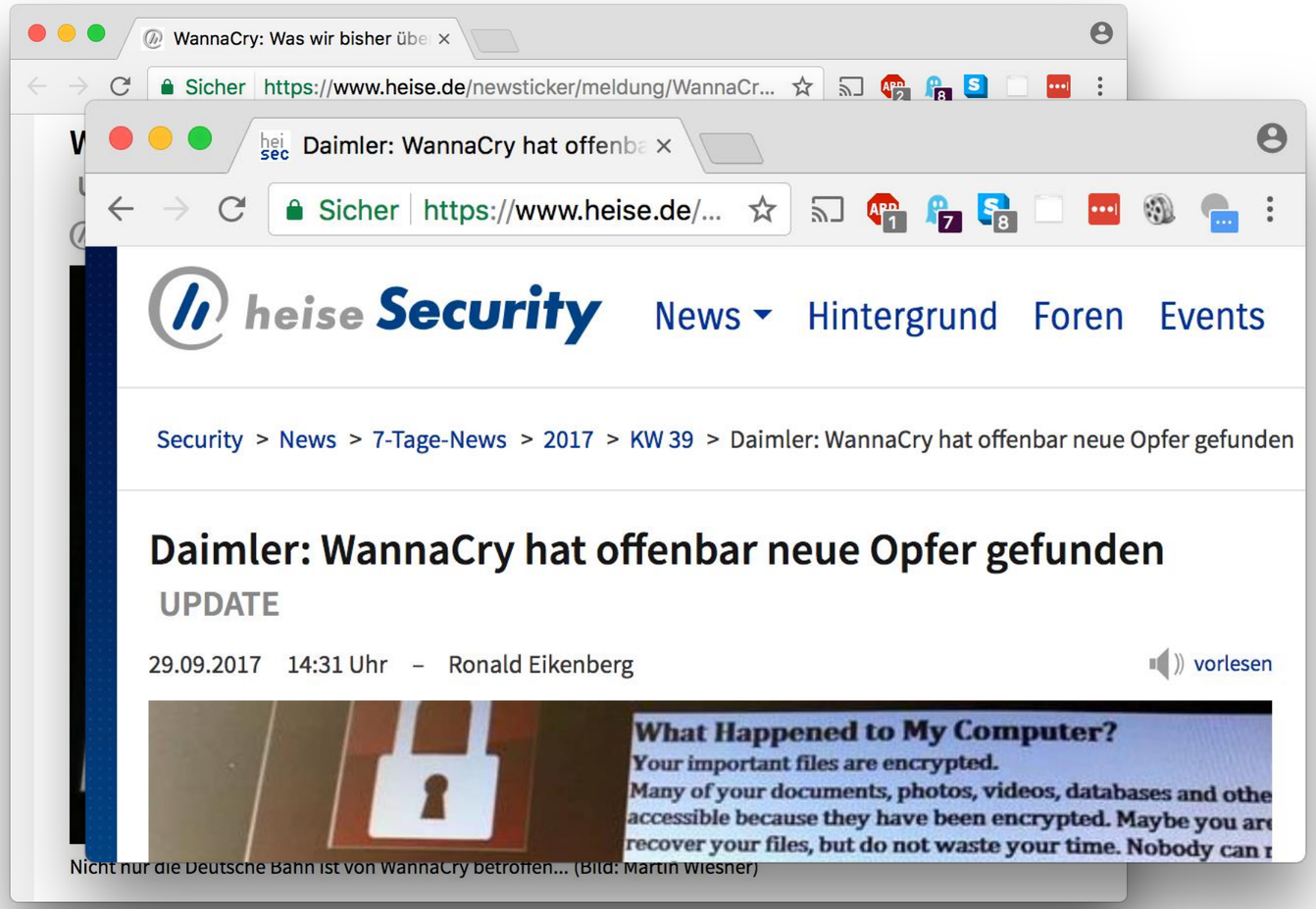
„Studierende“



„Schleppnetz-Angriffe“

Angreifer-Ziele

- Lösegeld fordern
- IT-Ressourcen missbrauchen
  - Spam, Phishing, DDoS, …



„Advanced Persistent Threats“

Angreifer-Ziele:

- Spionage
- Sehr gezielte Sabotage
- Langfristige Kontrolle über IT-Systeme

Informationssicherheit in Hochschulen

Informationssicherheit in Unternehmen	Informationssicherheit in Hochschulen
Eigene IT-Systeme	Eigene IT-Systeme + studentische Laptops, Tablets, Handys, → Eduroam + Separate Lehrstuhl-, Fachbereich-, Instituts-, private IT-Systeme
Eigene Mitarbeiter	Eigene Mitarbeiter + Studierende + Eduroam (der größere Teil aller Studierender, Mitarbeiter, Professoren weltweit) + selbstverantwortliche Mitarbeiter (Professoren, Forschergruppen, etc.)
→ Weisungshoheit im Unternehmen	→ „Freiheit in Forschung und Lehre“

Definition Informationssicherheit und Hochschulen

Rückschlüsse auf die Governance von Informationssicherheit:

1. Konkrete Arbeitsanweisungen an Hochschulverwaltung, Stab, etc. (wie in Unternehmen)
2. Schaffen von Anreizsystemen für Forschergruppen

Ein ***gutes*** Informationssicherheitskonzept...

- ...existiert und ist in Kraft gesetzt,
- dokumentiert gelebte sicherheitsrelevante Prozesse und gibt Anreize, bestehende Prozesse zu verbessern,
- wird ständig konsolidiert, angepasst, erweitert,
- ist bei betroffenen Personengruppen bekannt, akzeptiert und gelebte Praxis.

Ein ***schlechtes*** Informationssicherheitskonzept...

- ...ist unter dem Strich nur abgeheftet im Schrank,
- dokumentiert Soll-Zustände, die stark vom IST-Zustand divergieren,
- wurde nicht, oder nur unzureichend an die betroffenen Personengruppen kommuniziert,

Hochschulinformationssicherheitskonzept (Top-Down)

- ...wird von der Hochschulleitung verantwortet,
- von einem Sicherheitsverantwortlichen (>=50% Stelle) getrieben,
- dokumentiert bestehende sicherheitsrelevante Prozesse und kurz- und mittelfristig umsetzbare Änderungen,
- kommuniziert Richtlinien an betroffene Personengruppen (Security-Awareness)

Hochschulinformationssicherheitskonzept (Bottom-Up)

- ...identifiziert kritische Informationen und IT-Systeme,
- überprüft IT-Systeme und Prozesse auf kritische Schwachstellen (Scope: alles aus Eduroam Erreichbare),
- gibt kurzfristige Maßnahmen zur Behebung der Schwachstellen,
- stellt eine Incident-Response-Task-Force

Hochschulinformationssicherheitskonzept

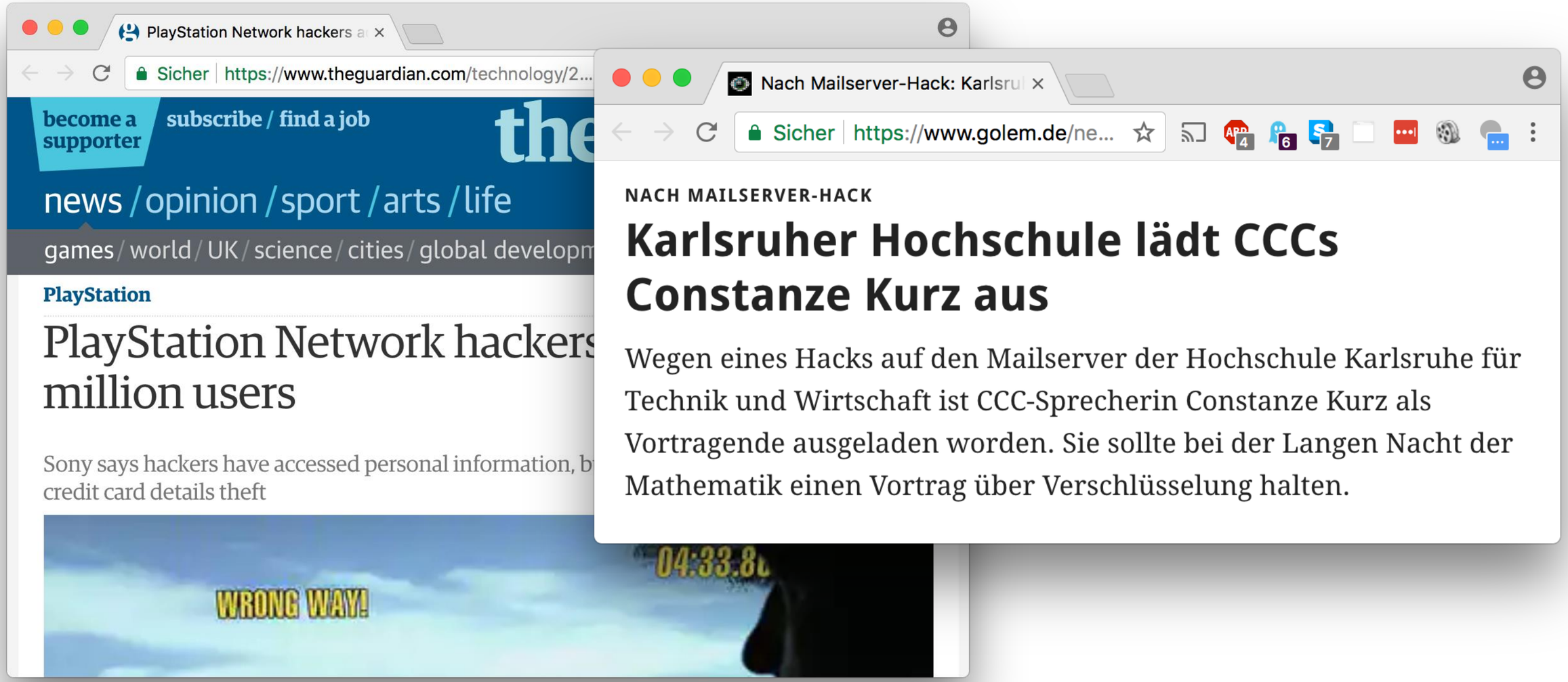
- Nicht top-down ***oder*** bottom-up
- Beide Vorgehen ergänzen sich sehr gut,
- sollten sich nach 2-3 Jahren „in der Mitte“ treffen.

Umgang mit Störfällen

Kommunikation sehr wichtig

- proaktives Informieren der betroffenen Personengruppen
- Pressestelle involvieren
- Externe Unterstützung meist hilfreich
- Kontakt zu DFN-CERT suchen

Umgang mit Störfällen



Studierende als Hacker-Experten?

Ihre IT-Infrastruktur ist (möglicherweise) bereits kompromittiert.

(Wie finden Sie es heraus? Und was machen Sie dann?)

Prof. Dr.-Ing. Sebastian Schinzel
Email: schinzel@fh-muenster.de
Twitter: @seecurity