Bauhaus-Universität Weimar

IT-Grundschutz

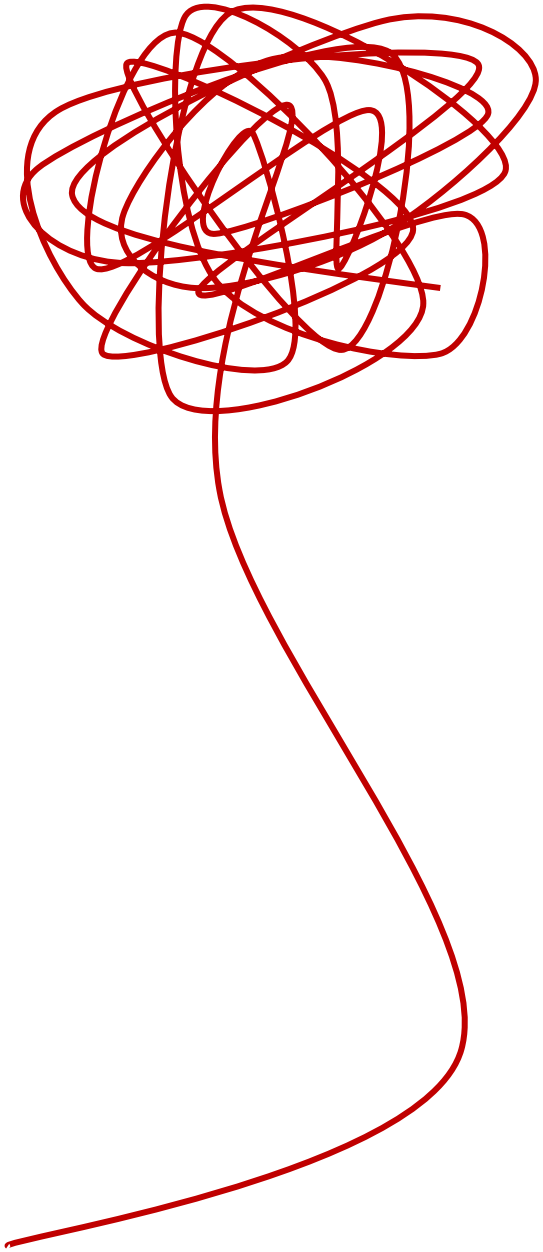
Dr. Markus von der Heyde
Leiter SCC

10. Tagung der DFN-Nutzergruppe Hochschulverwaltung 2011

DFN
Deutsches Forschungsnetz

www.uni-weimar.de

Einleitung



- Mein Handy
- Die Frage
- Die Ampel
- Eine Bedrohung?
- IT-Grundschutz in Weimar
- So nie
- Fazit
- Wie Hunde

Oje - mein Handy ist weg!

- Wie groß ist der Schaden?

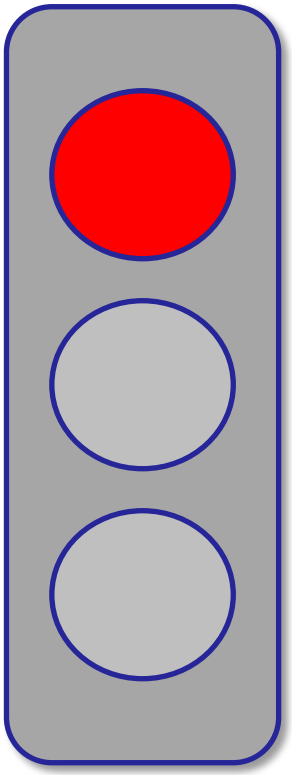
Das Verlieren des Handys ist schlimmer als das meiner Schlüssel. Meine Daumen sind dann so gelangweilt!
(EDUCause, Dan Adinolfi)

Die Frage

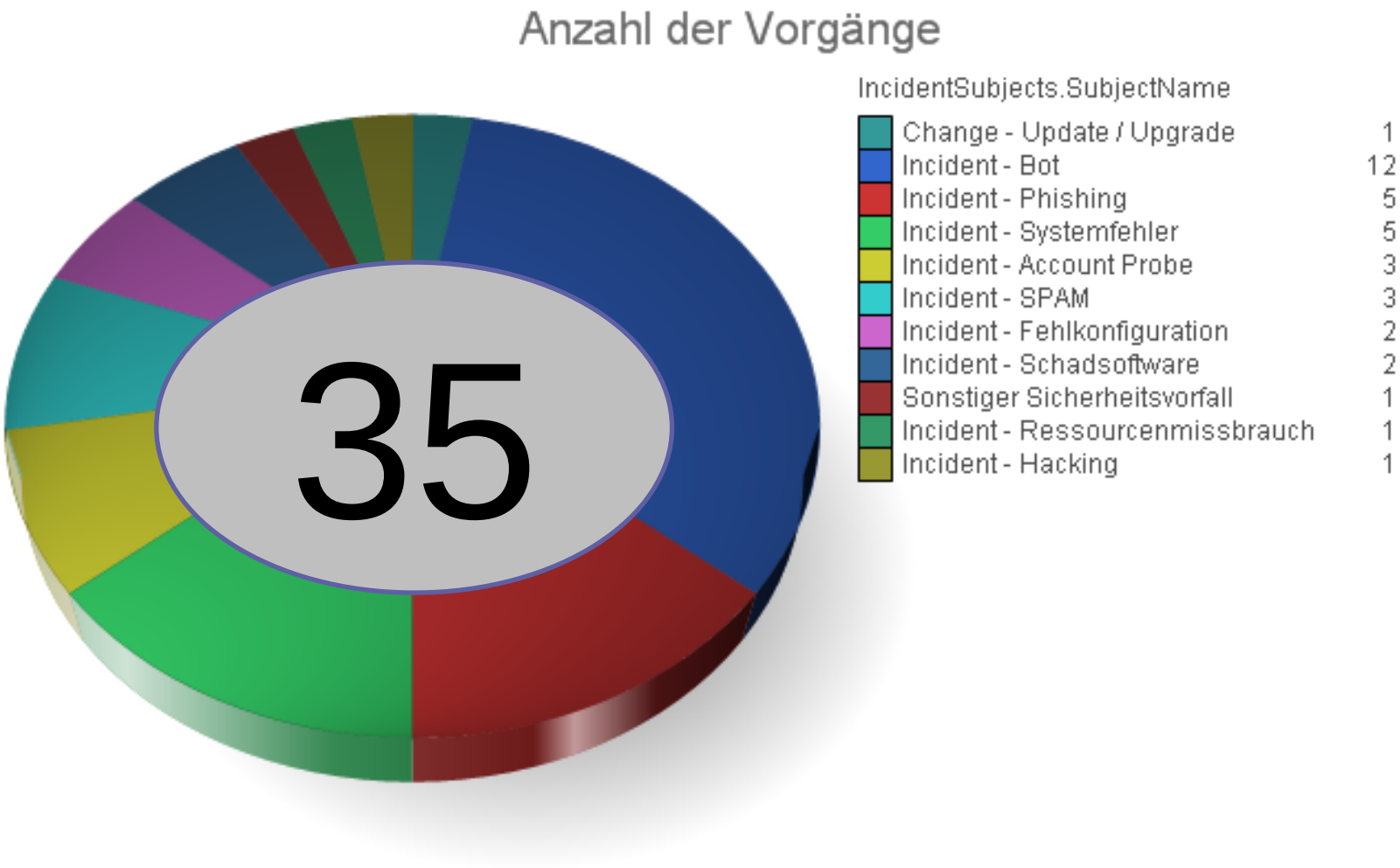
Straßenverkehrsordnung = IT-Grundschutz

Die Ampel

- Na dann gehen wir mal…



Wie groß ist die "Bedrohung"?



Statistik: Jan-Apr. 2011 – Bauhaus-Uni

Wie groß ist die "Bedrohung"?

?

?

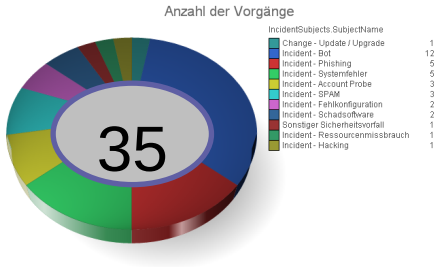
?

?

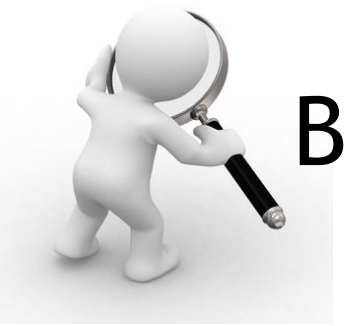
?

?

?



Statistik: Jan-Apr. 2011 – Bauhaus-Uni

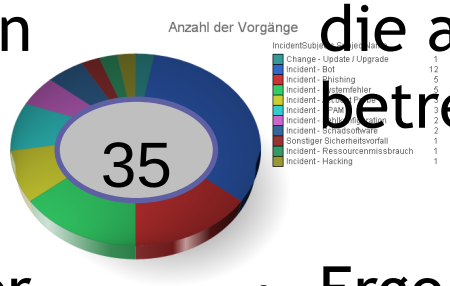


Bin ich persönlich „betroffen“?

optimistisch

- 35 Fälle in 4 Monaten, d.h. bei 6000 Nutzern nur alle 57 Jahre ein Vorfall pro Nutzer.

- Ergo: Wir haben hier doch kein Problem



pessimistisch

- 35 Fälle in 4 Monaten, d.h. 105 Fälle im Jahr, die alle 6000 Nutzer betreffen könnten.

- Ergo: Wir müssen dringend etwas tun

Was ist die richtige Frage?

- ~~Sind dies viele oder wenige Fälle?~~
- ~~Wären die Fälle vermeidbar?~~
- Warum stehen die Fälle überhaupt hier an der Wand?

IT-Grundschutz in Weimar

- **Zwei** Hochschulen in Weimar: Bauhaus-Universität und Hochschule für Musik FRANZ LISZT
- **Zwei** Perspektiven: Anwender und Administratoren
- **Zwei** Rollen: Verantwortlich für Initiierung und Verantwortlich für Umsetzung

Gültig für alle

Link zur Webquelle

Struktur - Umfang

GS Weimar

20 Maßnahmen des IT-Grundschutzes für **IT-Anwender**

50 Maßnahmen des IT-Grundschutzes für **IT-Personal**

- 2. 1 Allgemeines - 3
- 2. 2 Sicherung der Infrastruktur - 4
- 2. 3 Hard- und Softwareeinsatz -3
- 2. 4 Zugriffsschutz - 4
- 2. 5 Kommunikationssicherheit - 2
- 2. 6 Umgang mit schützenswerten Daten und Datenträgern - 2
- 2. 7 Umgang mit Datenträgern - 2

- 3. 1. Allgemeines - 2
- 3. 2. Organisation von IT-Sicherheit - 9
- 3. 3. Personelle Maßnahmen - 4
- 3. 4. Sicherung der Infrastruktur - 9
- 3. 5. Hard- und Softwareeinsatz - 10
- 3. 6. Zugriffsschutz - 6
- 3. 7. System- und Netzwerkmanagement - 2
- 3. 8. Kommunikationssicherheit - 4
- 3. 9. Datensicherung - 4

Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates (M 2.32)

Verantwortlich für Initiierung: IT-Verantwortliche

Verantwortlich für Umsetzung: IT-Personal

Um entdeckte Schwachstellen in Software-Produkten und bestimmten Hardware-Komponenten schnellst möglich zu beheben, damit sie nicht durch potentielle Angreifer ausgenutzt werden können ist es unabdingbar, dass Patches und Updates der Hersteller zeitnah eingespielt werden. Neben dem Betriebssystem sind auch die eingesetzten Applikationen (einschließlich ihrer Erweiterungen) und Treiber stets aktuell zu halten. Die Software sollte durch automatische Update-Services oder den regelmäßigen Besuch der Hersteller-Webseiten immer auf dem aktuellen Stand gehalten werden.

Systemadministratoren sollten sich daher regelmäßig über bekannt gewordene Software-Schwachstellen informieren.

Die Integrität und Authentizität der einzuspielenden Sicherheitsupdates und Patches ist sicherzustellen (Nutzung vertrauenswürdigen Quellen), außerdem sind sie immer mit Hilfe eines Malwareschutzprogramms zu prüfen.

so nie

Mit einem wirksamen Patch-Management wäre dieser Datenklau so nicht passiert.

Straßenverkehrsordnung ? = IT-Grundschutz

Wahr

- generelle Schutzfunktion
- mangelnde Sensibilität
- subjektive Einschränkung
- Überschreitung hat Ruf eines Kavaliersdelikts
- gilt nicht für mich
- …

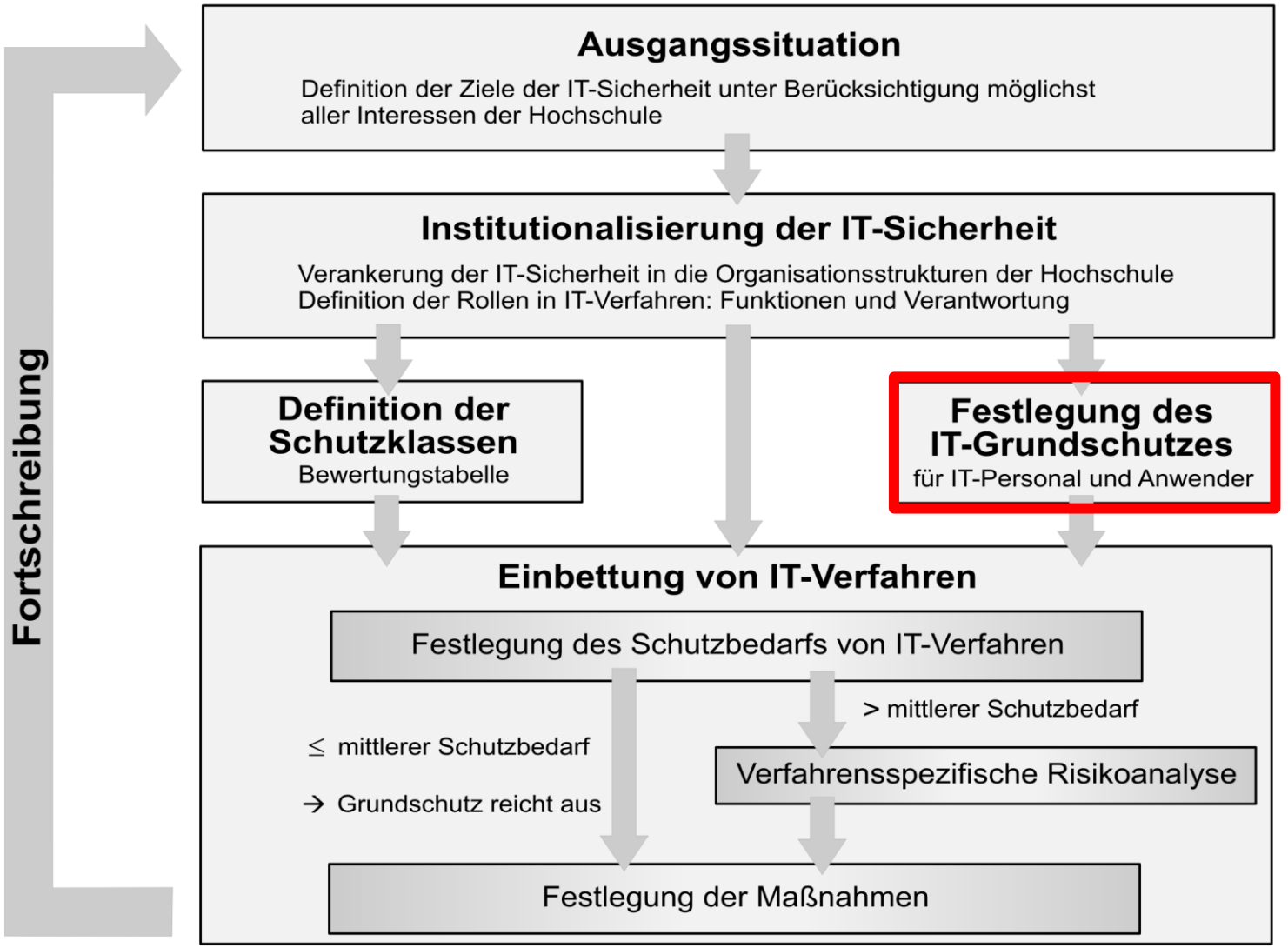
Falsch

- Institution hat Spielraum zur Interpretation

→ Daher müssen wir diesen aktiv nutzen:

Es bedarf eines Beschlusses zur Gültigkeit

Prozessmodell nach BSI – erprobt in Hochschulen



Auf den Hund gekommen ?

"We are less dog, and more the tail.“
(Mike Richichi)