IT-Sicherheit. Aktuelle Fragen.

Prof. Dr. Michael Meier

Arbeitsgruppe IT-Sicherheit
Institut für Informatik

UNIVERSITÄT BONN

Abteilung Cyber Security
Fraunhofer FKIE

Fraunhofer
FKIE

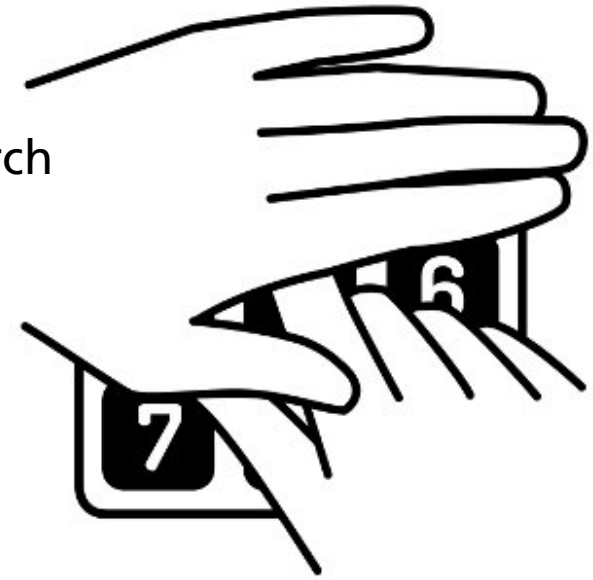
Überblick

- IT-Sicherheit
  - Ziele, Verfahren und Annahmen
- Herausforderungen
  - Zielkonflikte
  - Programmierfehler
  - Hardware-“Macken“
  - Faktor Mensch
- Aktuelle Fragen (und Antworten)
  - Internet-Routing-Manipulation
  - IT-Security-Awareness messen
  - Digitaler Identitätsdiebstahl

Schutzziele der IT-Sicherheit

- Grundlegende Schutzziele und Sicherheitsinteressen
  - **Vertraulichkeit** von Informationen und Aktivitäten
    - Keine unautorisierte Kenntnisnahme
  - **Integrität** von Daten und Computersystemen
    - Keine unautorisierte unbemerkte Manipulation
  - **Verfügbarkeit** von Daten und Funktionen/Diensten
    - Keine unautorisierte Einschränkung der Nutzung

Verfahren
Authentifikation



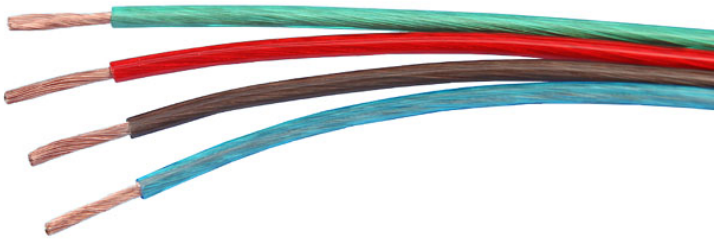
- Nachweis der vorgegebenen Identität der Beteiligten durch
  - geheimes Wissen
    - Passwort, PIN, TAN
  - persönlicher Besitz
    - Smartcard, Token
  - biometrische Eigenschaften
    - Fingerabdruck, Iris, Schreibdynamik
- Kombination von Merkmalen erhöht die Sicherheit

Verfahren

Basisansätze für Sicherheitsmechanismen

- **Redundanz** erlaubt
  - die Ableitung erforderlicher Information
  - zur Erkennung von Fehlern und Angriffen sowie
  - zur Wiederherstellung nach unerwünschten Ereignissen.

- **Isolation** verhindert
  - unerwünschte Informationsflüsse.



- **Ununterscheidbarkeit**
  - lässt böswillige Beobachtungen zufällig oder standardisiert erscheinen und macht sie damit nutzlos.

Annahmen
In der Realen Welt

- Hinsichtlich der Absicherung eines Wohnhauses
  - Die Tür ist die einzige Zutrittsmöglichkeit.
    Es kann bspw. nicht durch die Fenster betreten werden.
  - Hersteller, Lieferanten und Verkäufer der Türen, Schlösser und Schlüssel agieren regelkonform und missbrauchen nicht das in sie gesetzte Vertrauen; keiner behält Duplikate der Schlüssel.
  - Die Hausbewohner verlieren keine Schlüssel.
  - Einbrecher werden durch Schutzmaßnahmen abgeschreckt oder scheitern daran, die Tür aufzubrechen.
- In der Praxis schwer zu erfüllen
  - Das Versagen der Schutzmaßnahmen muss in Betracht gezogen werden.
  - ⇨ Ergänzende reaktive Maßnahmen: Alarmanlage, Wachdienst

Annahmen
In der digitalen Welt

- Hard- und Software funktionieren fehlerfrei und enthalten keine Hintertüren.
- Intel, Microsoft, Apple und Co. agieren regelkonform und missbrauchen nicht das in sie gesetzte Vertrauen.
- Geheimnisse werden geeignet aufbewahrt.
- Biometrische Merkmale sind nicht kopierbar/simulierbar.
- Es gibt kein effizientes Faktorisierungsverfahren.
  (Bzw. es gibt keine Quantencomputer).

Unterschiede zwischen realer und digitaler Welt

- Risiko für Täter zur Verantwortung gezogen zu werden, ist in der digitalen Welt ein vielfaches geringer als in der realen Welt.
- Erforderliche Kenntnisse und Fähigkeiten zur Durchführung von Einbrüchen und Angriffen sind in der digitalen Welt einfach **kopierbar** und **vervielfältigbar**. Insbesondere können Abläufe und Vorgehensweisen von Angreifern mit Softwareprogrammen **automatisiert** werden
- Ein einzelner Angreifer kann gleichzeitig mehrere Opfer angreifen.

⇨ Zusätzliche Maßnahmen erforderlich um in der digitalen Welt ein vergleichbares Niveau zur erreichen.

Präventive und Reaktive Verfahren

- Sicherheitsmechanismen zielen darauf ab
  - Sicherheitsverletzungen zu verhindern
  - durch Sicherheitsverletzungen verursachten Schaden zu begrenzen
  - die Konsequenzen von Sicherheitsverletzungen zu kompensieren.

- Das Versagen von (einzelnen) Sicherheitsmaßnahmen muss antizipiert werden.

Ziele
Spezifische Sicherheitsziele

- **Forward Secrecy** von kryptographischen Verschlüsselungsprotokollen
  - **Folgenlosigkeit** bei Kompromittierung von **Langzeitgeheimnissen**
- Beispielszenario
  - Wenn die NSA heute Ihre verschlüsselte Kommunikation aufzeichnet und morgen Ihr Langzeitgeheimnis (Passwort, privaten Schlüssel) bricht/ermittelt, dann kann die NSA immer noch nicht die heute aufgezeichnete Kommunikation entschlüsseln.
- Ansatz
  - **Langzeitgeheimnisse** werden zur Vereinbarung eines sicheren Kanals verwendet.
  - Zur Sicherung des Kanals wird ein **Kurzzeitgeheimnis** verwendet, das nicht aus dem Langzeitgeheimnis ermittelbar ist.

Löwe und Gazelle

Um zu überleben,
muss ein Löwe schneller sein als die langsamste Gazelle
muss eine Gazelle schneller sein als der schnellste Löwe

Bildquelle: http://quoteinvestigator.com/category/dan-montano/

Löwe und Gazelle

Um zu überleben,
muss ein Löwe schneller sein als die langsamste Gazelle
muss eine Gazelle schneller sein als ~~der schnellste Löwe~~
die langsamste Gazelle

Aufwands- / Nutzenbetrachtungen

Wie hoch ist der Aufwand eines Angreifers und welchen Nutzen kann er aus einem Angriff ziehen?

Rechtfertigt das erkannte Risiko die Ausgaben/den Aufwand für die gewählten Sicherheitsmechanismen?

Überblick

- IT-Sicherheit
  - Ziele, Verfahren und Annahmen
- Herausforderungen
  - Zielkonflikte
  - Programmierfehler
  - Hardware-“Macken“
  - Faktor Mensch
- Aktuelle Fragen (und Antworten)
  - Internet-Routing-Manipulation
  - IT-Security-Awareness messen
  - Digitaler Identitätsdiebstahl

Schutzziele der IT-Sicherheit

- Grundlegende Schutzziele und Sicherheitsinteressen
  - **Vertraulichkeit** von Informationen und Aktivitäten
    - Keine unautorisierte Kenntnisnahme
  - **Integrität** von Daten und Computersystemen
    - Keine unautorisierte unbemerkte Manipulation
  - **Verfügbarkeit** von Daten und Funktionen/Diensten
    - Keine unautorisierte Einschränkung der Nutzung

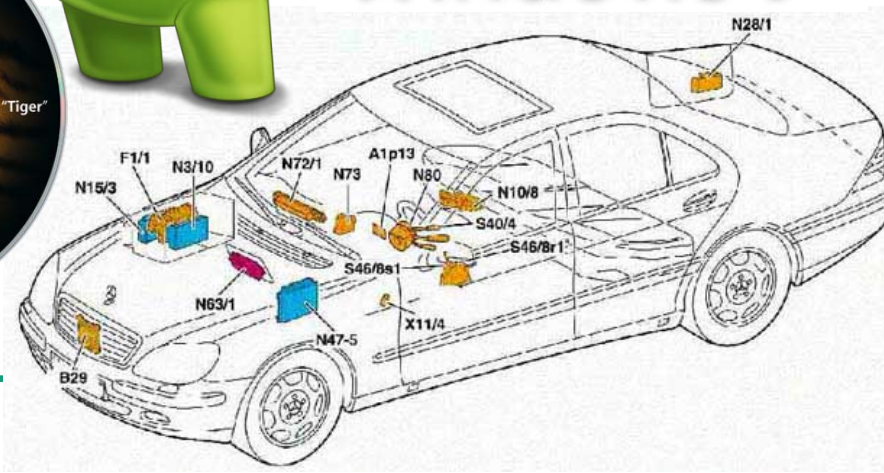
IT-Sicherheit: Inhärente Zielkonflikte
Beispiel 1: Vertraulichkeit versus Verfügbarkeit

- Um die Vertraulichkeit einer Information zu erhalten kann die Löschung der Information (Selbstzerstörung) sinnvoll sein.
  - ⇨ Verlust der Verfügbarkeit

- Um die Verfügbarkeit zu gewährleisten können Sicherheitskopien von vertraulichen Informationen (z.B. Passwörtern) sinnvoll sein.
  - ⇨ Erhöhtes Risiko eines Vertraulichkeitsverlustes

Fehlerhafte Programme (Software oder Hardware)

- Ursache: Komplexität
- Auswirkung: professionell entwickelte Programme enthalten pro 1000 Zeilen Programmcode (LoC - Lines of Code) 1 bis 3 Fehler;
  eine Teilmenge davon ist sicherheitskritisch.
- Wie groß sind typische Programme? [1]
  - Android: 12 Mio LoC
  - Windows 7: 40 Mio LoC
  - MAC OS X : 85 Mio LoC
  - Software im Auto: 100 Mio LoC



[1] http://www.informationisbeautiful.net/visualizations/million-lines-of-code/

IT-Sicherheit: Inhärente Zielkonflikte
Beispiel 2: Software(-Aktualisierung) versus „feste“ Hardware

- Bei Veränderbarkeit der Programme können entdeckte Fehler nachträglich durch Software-Updates korrigiert werden.
  - bei Unveränderbarkeit (z.B. purer Hardware) nicht

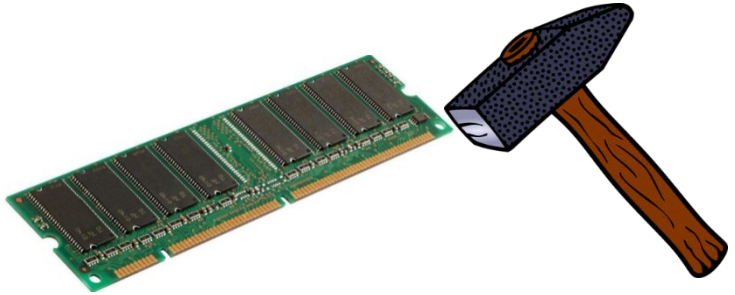
- Die Veränderbarkeit von Programmen ist notwendige Voraussetzung für Infektionen mit Schadsoftware.
  - Bei Unveränderbarkeit können Infektionen ausgeschlossen werden.

In einer Welt ohne Programmierfehler
Mögliche künftige Angriffstechniken

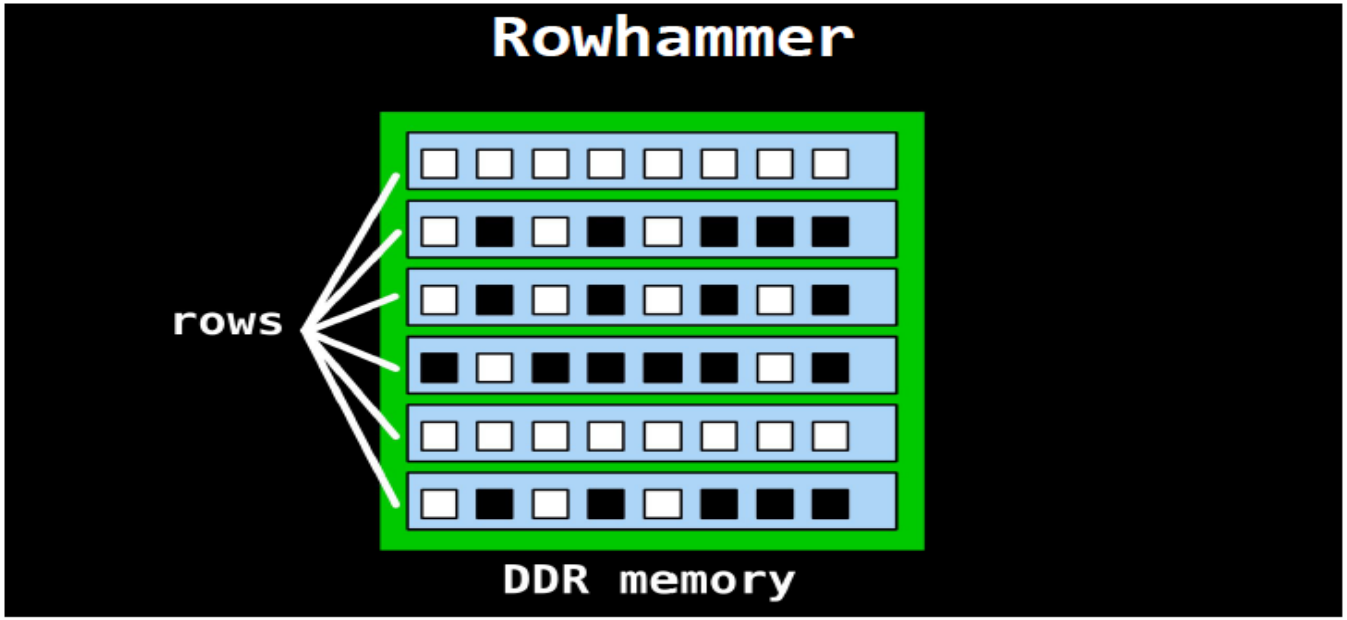
- Wie kann ein Angreifer unautorisiert den Programmspeicher **lesen** und **schreiben**?
  - Ausnutzung der Eigenschaften von moderner Software und Hardware

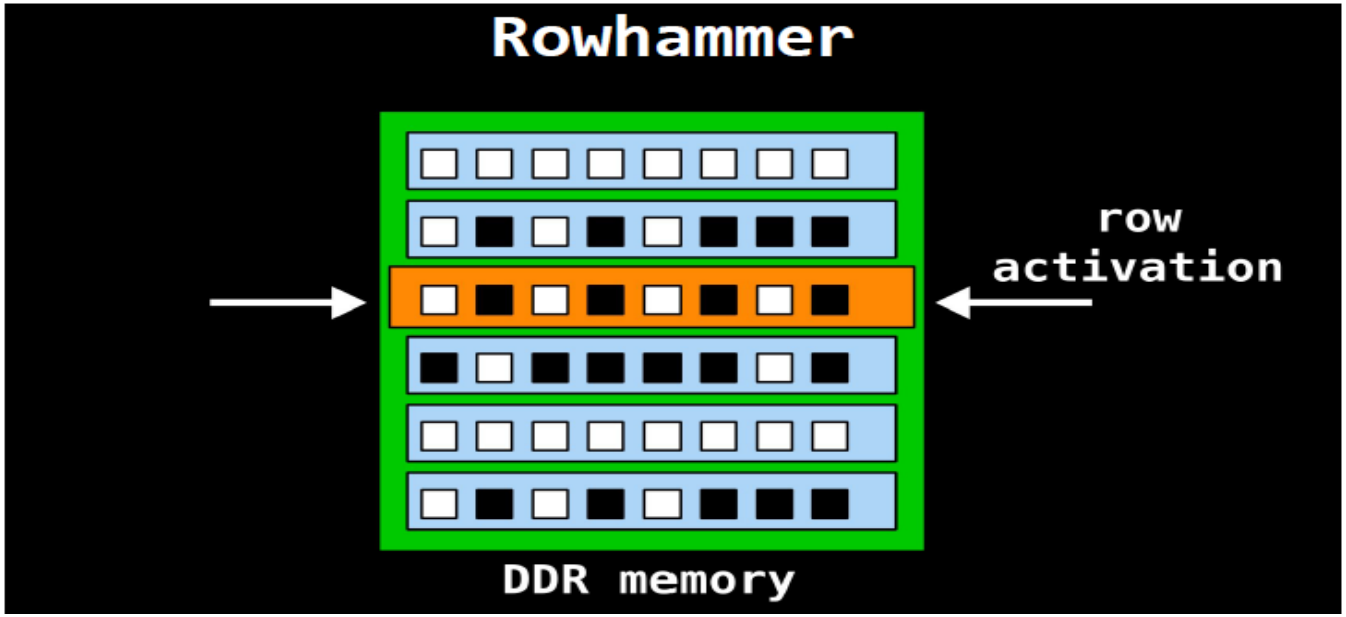
- Seitenkanäle (z.B. zeit-basierte) ermöglichen **Lese-Zugriffe**
  - Verwendung von Caching resultiert in unterschiedlichem Zeitverhalten abhängig davon, ob angefragte Daten zuvor genutzt wurden

- Hardware-„Macken“ wie **Rowhammer** erlauben **Schreib-Zugriffe**

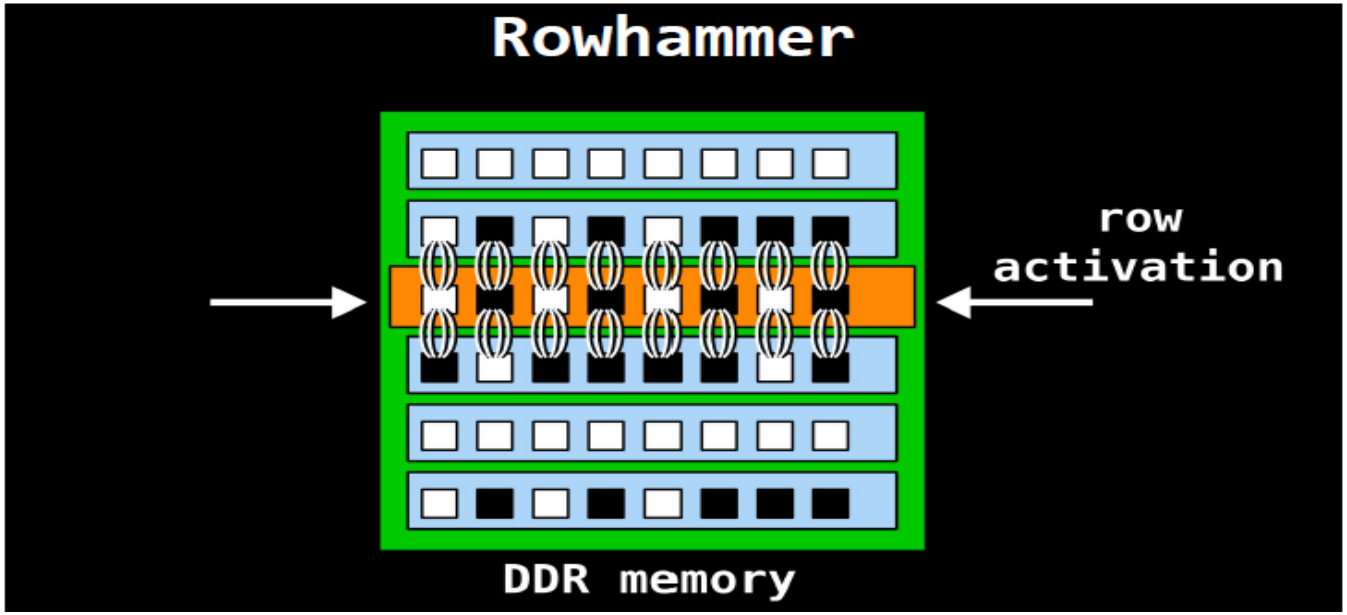


- Speicherzellen sind in Zeilen (Rows) organisiert

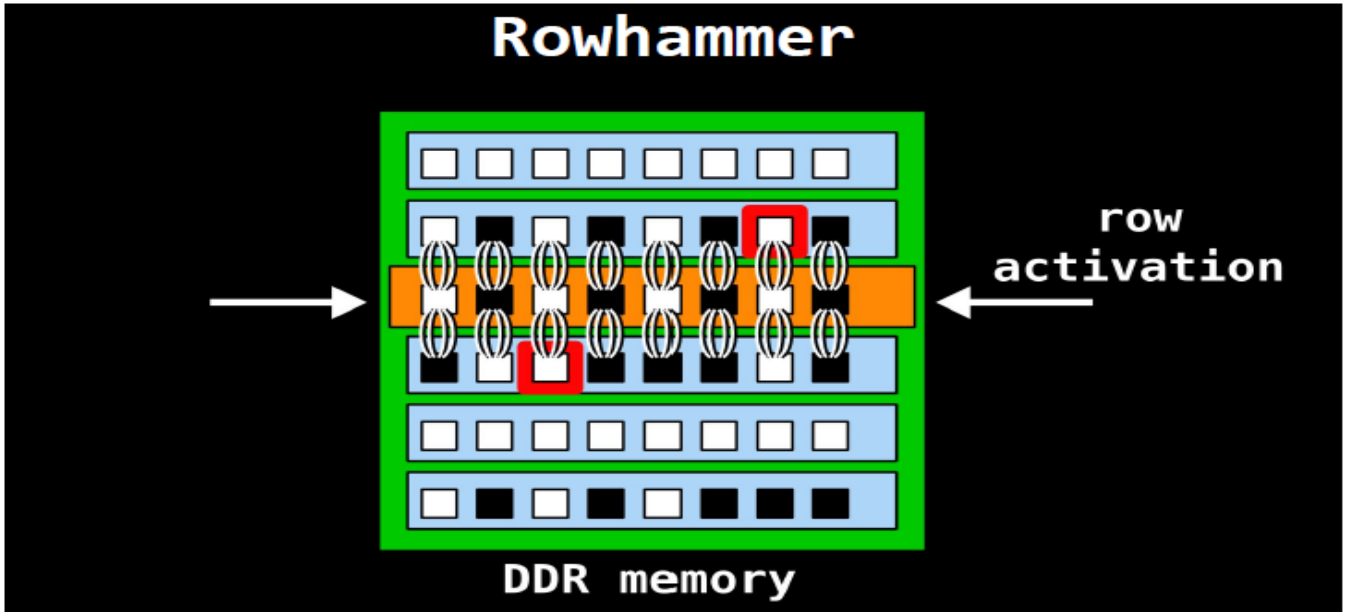



Rowhammer
row
activation
DDR memory

- Elektromagnetische Interaktion zwischen benachbarten Speicherzellen



- Stör-Fehler manifestieren sich als zufällige Wertänderungen von Bits
- Ausgelöst durch maßgeschneiderte Speicher-Zugriffsmuster, die schnell mehrfach dieselbe Speicherzeile aktivieren



IT-Sicherheit: Inhärente Zielkonflikte
Beispiel 3: Zusätzliche Schutz-Software versus größere „Angriffsfläche“

- Zusätzliche Schutz-Software erhöht den Schutz gegenüber spezifischen Bedrohungen
  - Anti-Viren-Scanner
  - Personal Firewall
  - …
- Zusätzliche Schutz-Software erhöht die Komplexität
  - Noch mehr fehlerhafte Software
  - Mehr „Angriffsfläche“

IT-Sicher
Beispiel 3: ffsfläche“

- Zusätzlich chen Bedrohu
  - Anti-V
  - Person
  - …
- Zusätzlich
  - Noch r
  - Mehr „

Alert!

Lücke in Symantec Endpoint Protection kann Angreifern höhere Rechte verschaffen

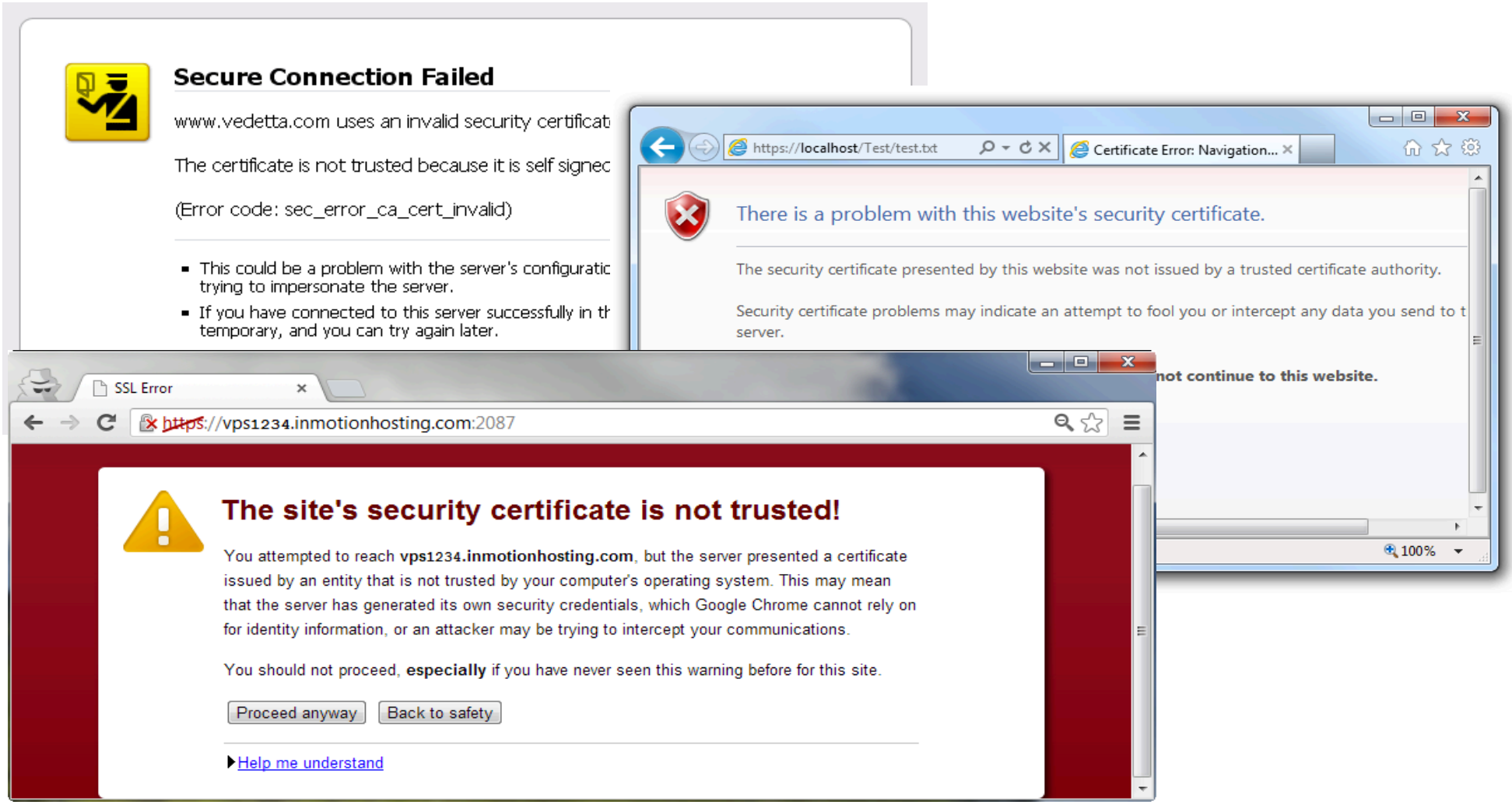
09.11.2017 14:59 Uhr – Dennis Schirrmacher vorlesen

Symantec schließt drei Lücken in Endpoint Protection für Windows.

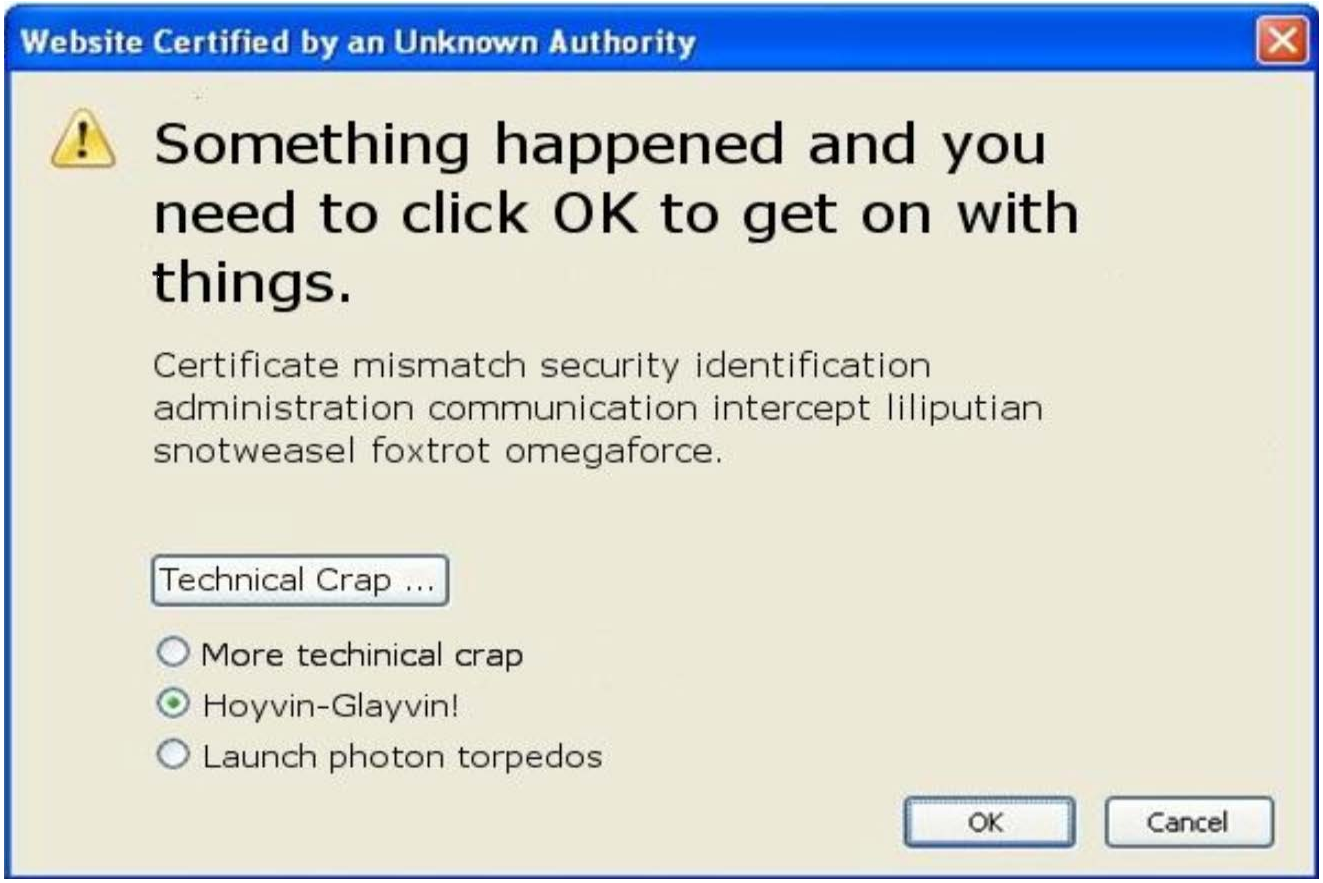
Die Sicherheitslösung Symantec Endpoint Protection (SEP) ist unter Windows in verschiedenen Versionen verwundbar. Der Software-Hersteller stuft das durch die drei Sicherheitslücken ausgelöste Angriffsrisiko jeweils mit "hoch", "mittel" und "niedrig" ein. Das Notfallteam des BSI CERT Bund sieht das Risiko insgesamt als "hoch" an.

Setzen Angreifer an der in diesem Fall bedrohlichsten Lücke (CVE-2017-13681) an, sollen sie sich lokal und einfach authentisiert höhere Rechte aneignen können. Über die zweite Schwachstelle (CVE-2017-13680) könnten Angreifer Dateien löschen. Die

Faktor Mensch
Sicherheitswarnungen von Web-Browsern



Was die meisten Nutzer verstehen:



Sicherheit, Komplexität und der Mensch

- Komplexität ist der größte Feind von Sicherheit
- Systeme werden immer komplexer.

- Wir haben die Technologie um (fast) alle Systeme sicher zu gestalten.
- Es fehlen uns die Menschen die diese korrekt einsetzen wollen und können.

- Wir haben zwei Optionen:
  - Den Menschen an die Technologie anzupassen
  - Die Technologie an den Menschen anzupassen

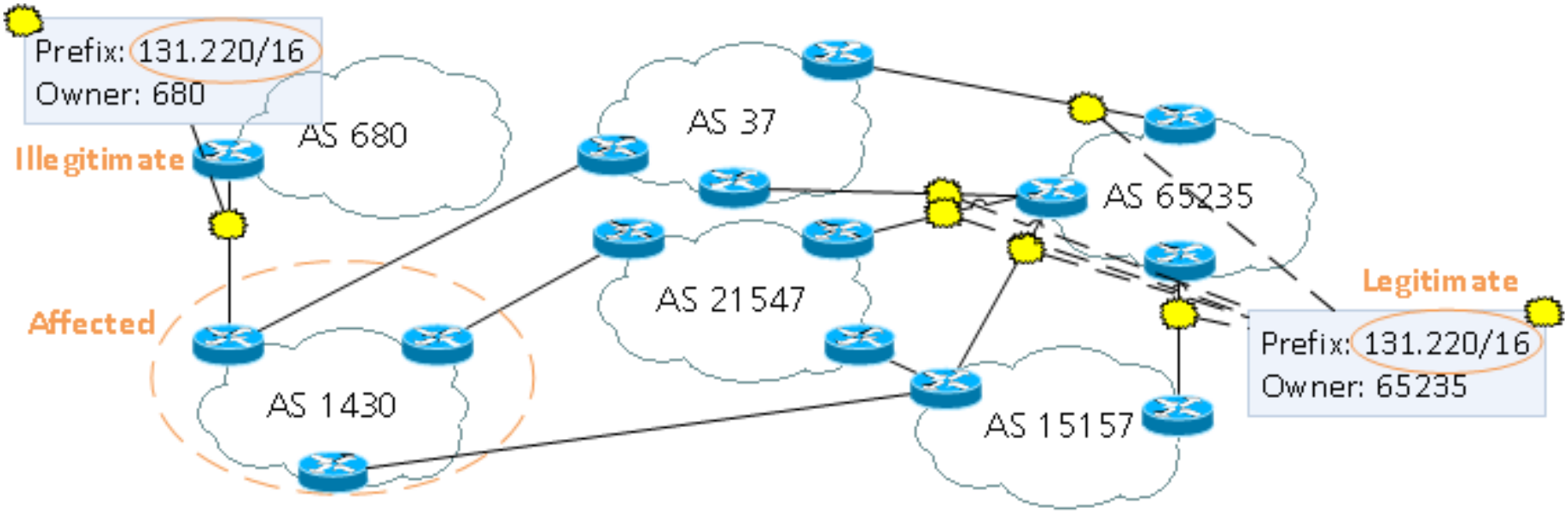
Zwischenfazit

- Verteidigung in der Tiefe erforderlich
  - Mehrere Verteidigungslinien
  - Versagen einzelner Schutzmechanismen muss antizipiert werden
  - Präventive **und** reaktive Sicherheitsmechanismen erforderlich
    - Kontinuierliche Überwachung und Kontrolle
    - Vorbereitung auf Vorfälle und Notfälle
- IT-Sicherheit ist ein Prozess.

Überblick

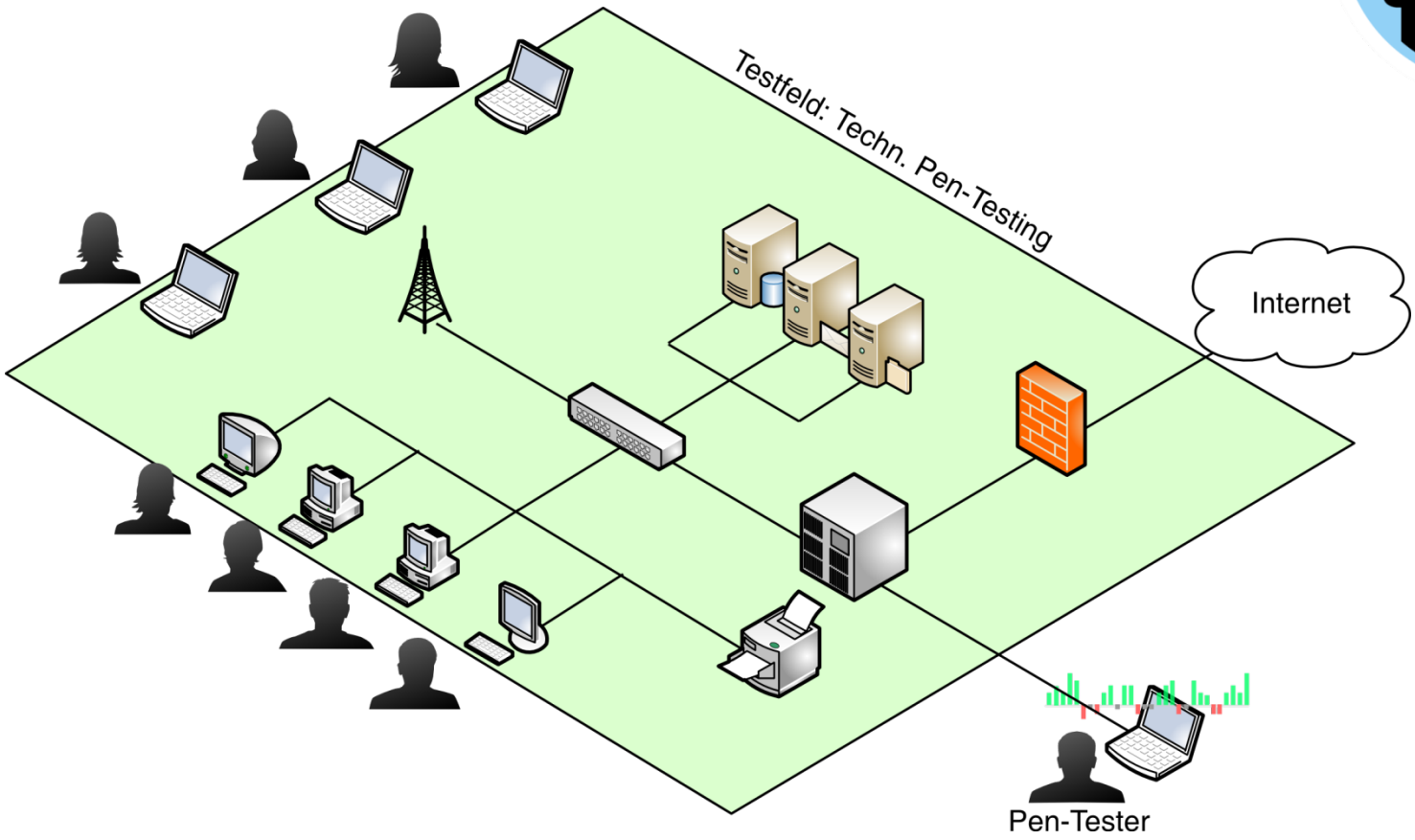
- IT-Sicherheit
  - Ziele, Verfahren und Annahmen
- Herausforderungen
  - Zielkonflikte
  - Programmierfehler
  - Hardware-“Macken“
  - Faktor Mensch
- Aktuelle Fragen (und Antworten)
  - Internet-Routing-Manipulation
  - IT-Security-Awareness messen
  - Digitaler Identitätsdiebstahl

Erkennung und Behandlung von Internet-Routing-Anomalien insbesondere IP-Prefix-Hijacking

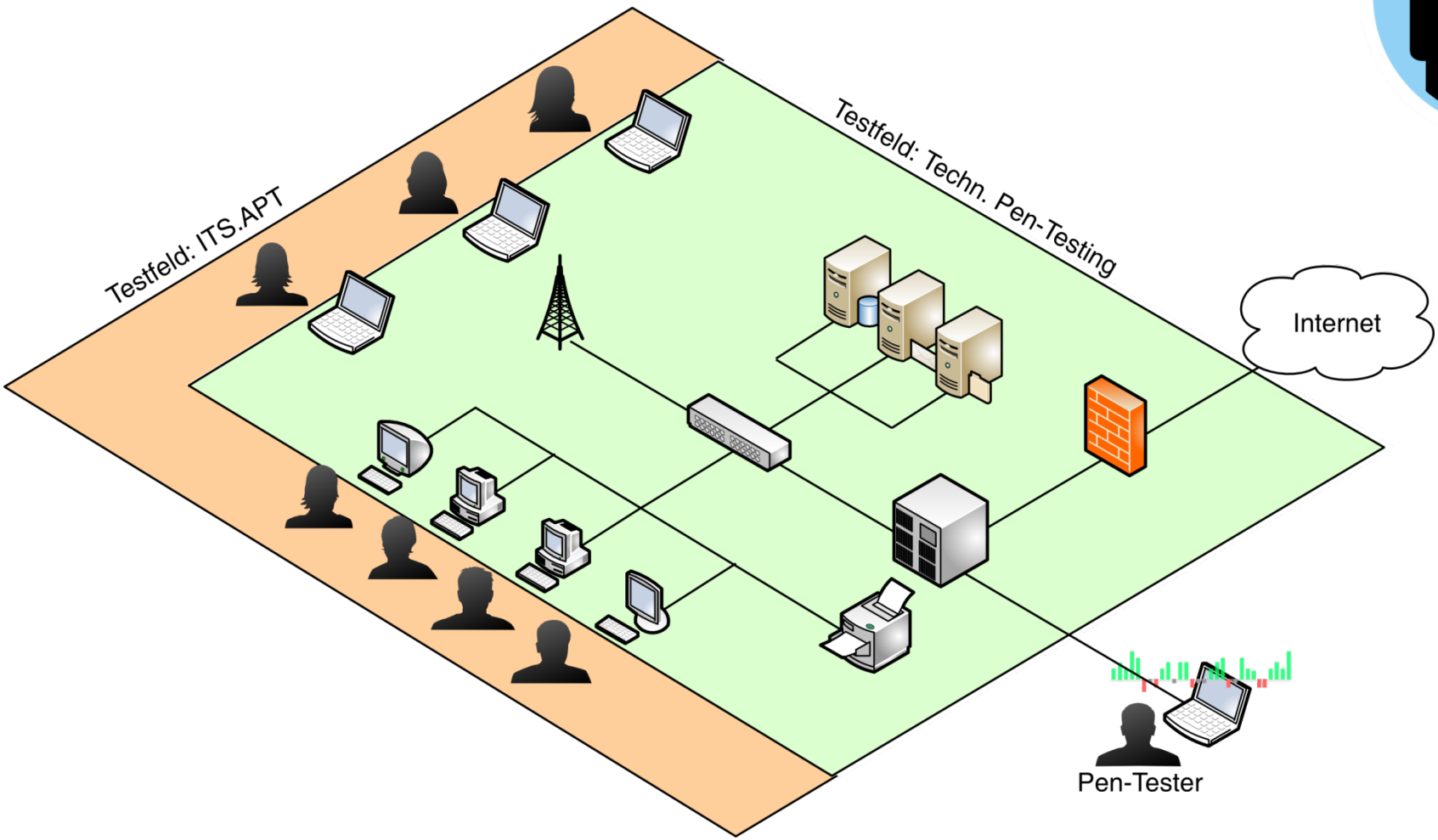


- Einzelnen Wegweisern (BGP Announcements) kann man nicht trauen
- Zusätzliche Informationen einbeziehen
- Transparenz von Wegewahlentscheidungen und Widersprüchen

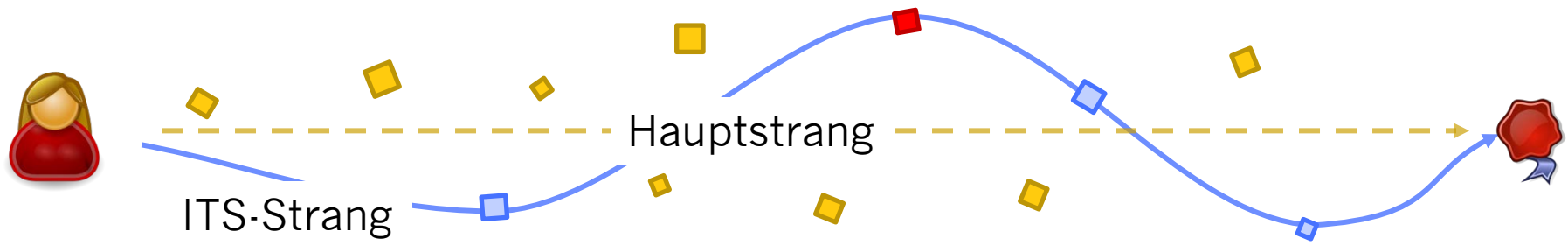
IT-Sicherheits Awareness Penetration Testing - ITS.APT



IT-Sicherheits Awareness Penetration Testing - ITS.APT

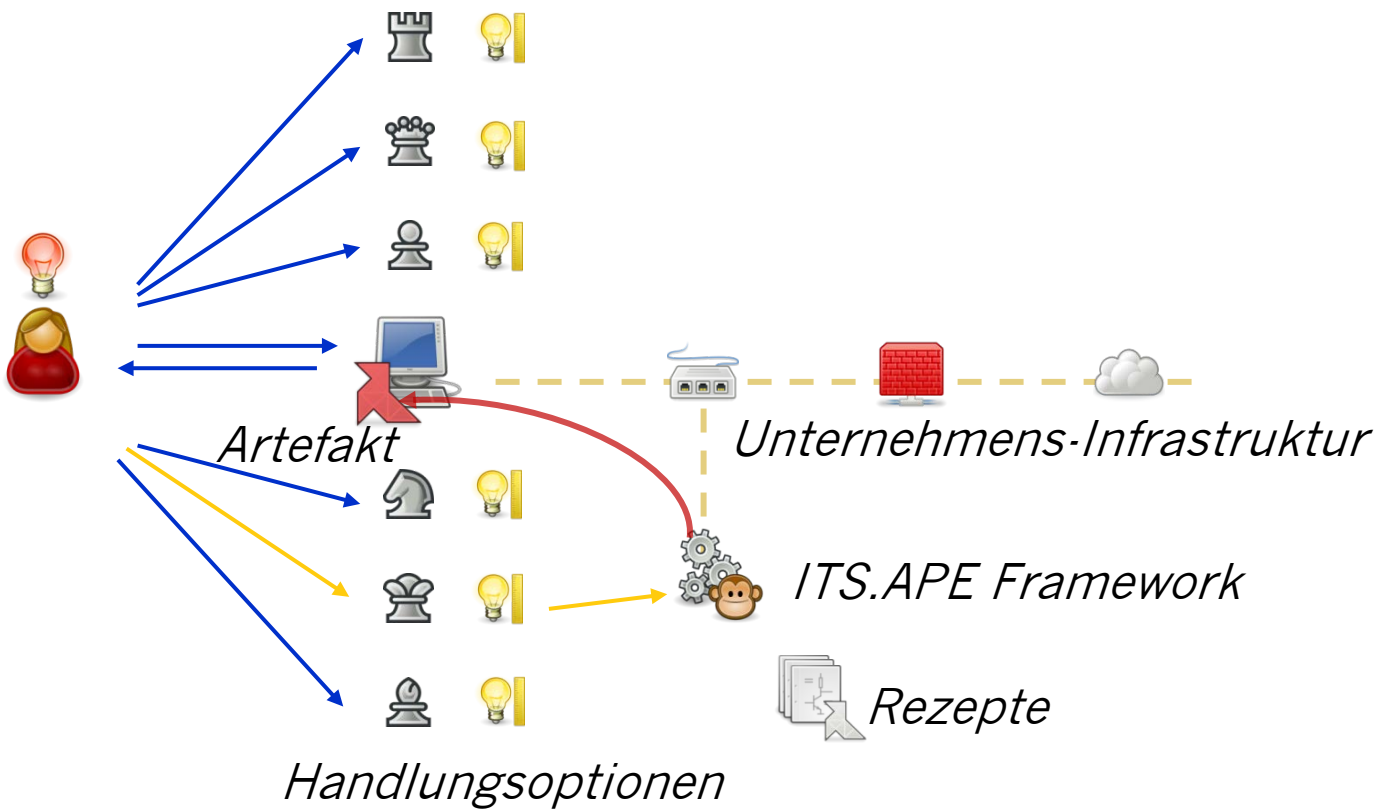


Artefakte



- Elemente in der Situation
- Elemente mit Sicherheitsbezug
- Artefakte

IT-Security Awareness Messen



Das Konsortium

6 Partner:

- Psychologen
- Juristen
- Datenschützer
- IT-Sicherheitsdienstleister
- **IT-Sicherheitsforscher**
- Betreiber einer kritischen Infrastruktur

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

UNIVERSITÄT DUISBURG ESSEN

Westfälische Wilhelms-Universität Münster

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

ERNW
providing security.

UNIVERSITÄT BONN

UKSH
UNIVERSITÄTSKLINIKUM
Schleswig-Holstein

EIDI – Effektive Warnung nach Digitalem Identitätsdiebstahl
Ausgangspunkt

EIDI

- Identitätsdaten, Konto- und Kreditkarteninformationen, Email-Adressen, Account-Namen und Passwörter werden gestohlen oder „gesammelt“

- Bemerken Betroffene einen Identitätsdiebstahl?
  - ⇨ In der Regel nicht oder erst bei Feststellung eines Schadens.

EIDI – Effektive Warnung nach Digitalem Identitätsdiebstahl
Ausgangspunkt

- **Identitätsdatensammlungen** werden
  - bei der Aufklärung von IT-Sicherheitsvorfällen durch Strafverfolgungsbehörden oder IT-Sicherheitsforscher aufgefunden oder
  - im Internet gehandelt / getauscht oder
  - anonym z.B. auf Pastebin veröffentlicht

PASTEBIN

- Was machen wir damit?

- **Wer** informiert **wann** und **wie** (proaktiv) die Betroffenen?

EIDI – Effektive Warnung nach Digitalem Identitätsdiebstahl
Idee: EIDI-Warndienst

- **proaktiv**,

  im Unterschied zu

  - have i been pwned
  - HPI-Leakchecker
  - BSI Sicherheitstest

  - Was ist mit Oma Erna?
  - ⇨ proaktiv

- **Teilprobleme**

  - Sammeln
  - Analysieren
  - Validieren
  - Dienstidentifikation
  - Warnen
  - …

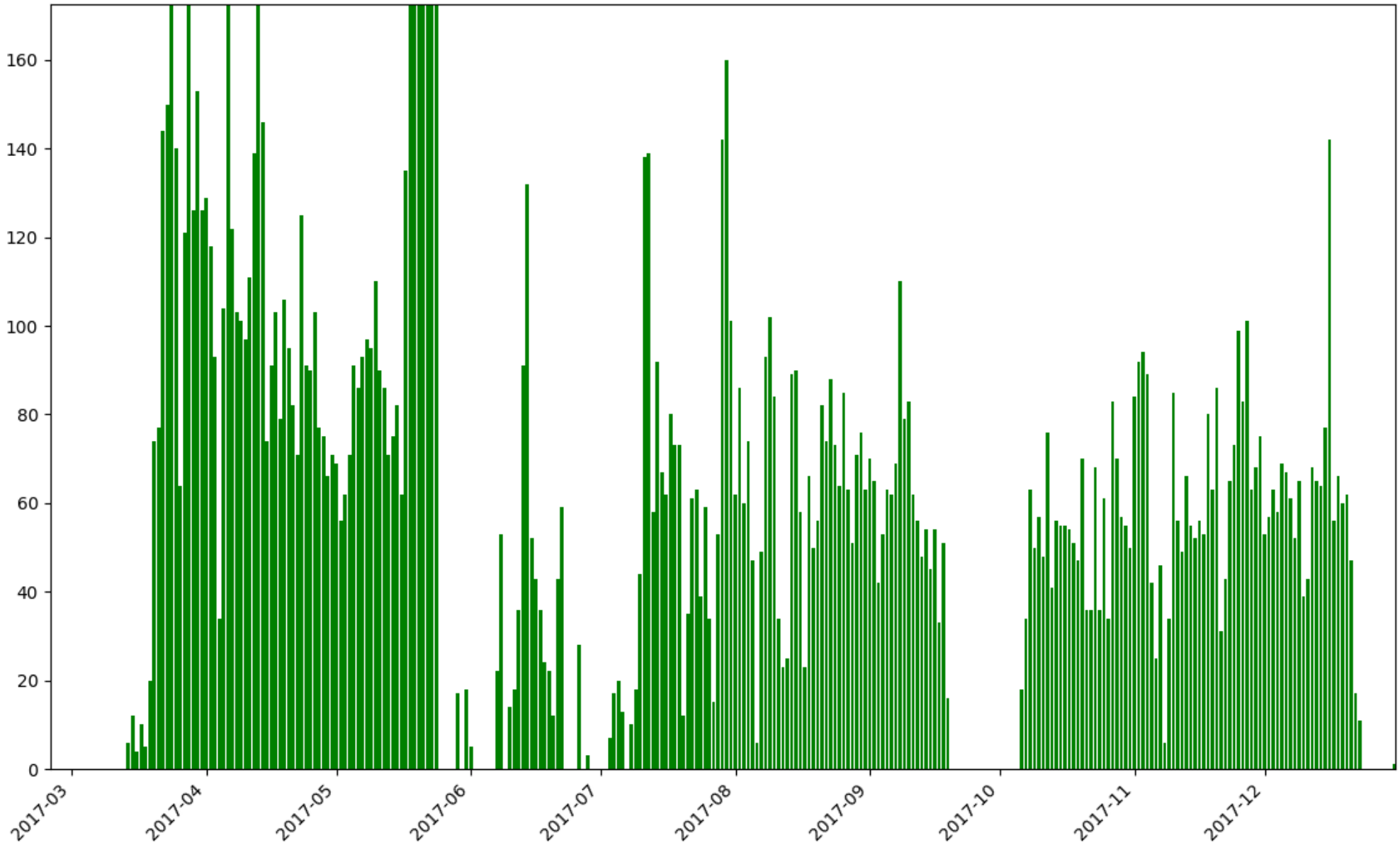
Sammlung von Identitätsdaten

- Aktuell ≥ **5 127 243 813** E-Mail-Adressen

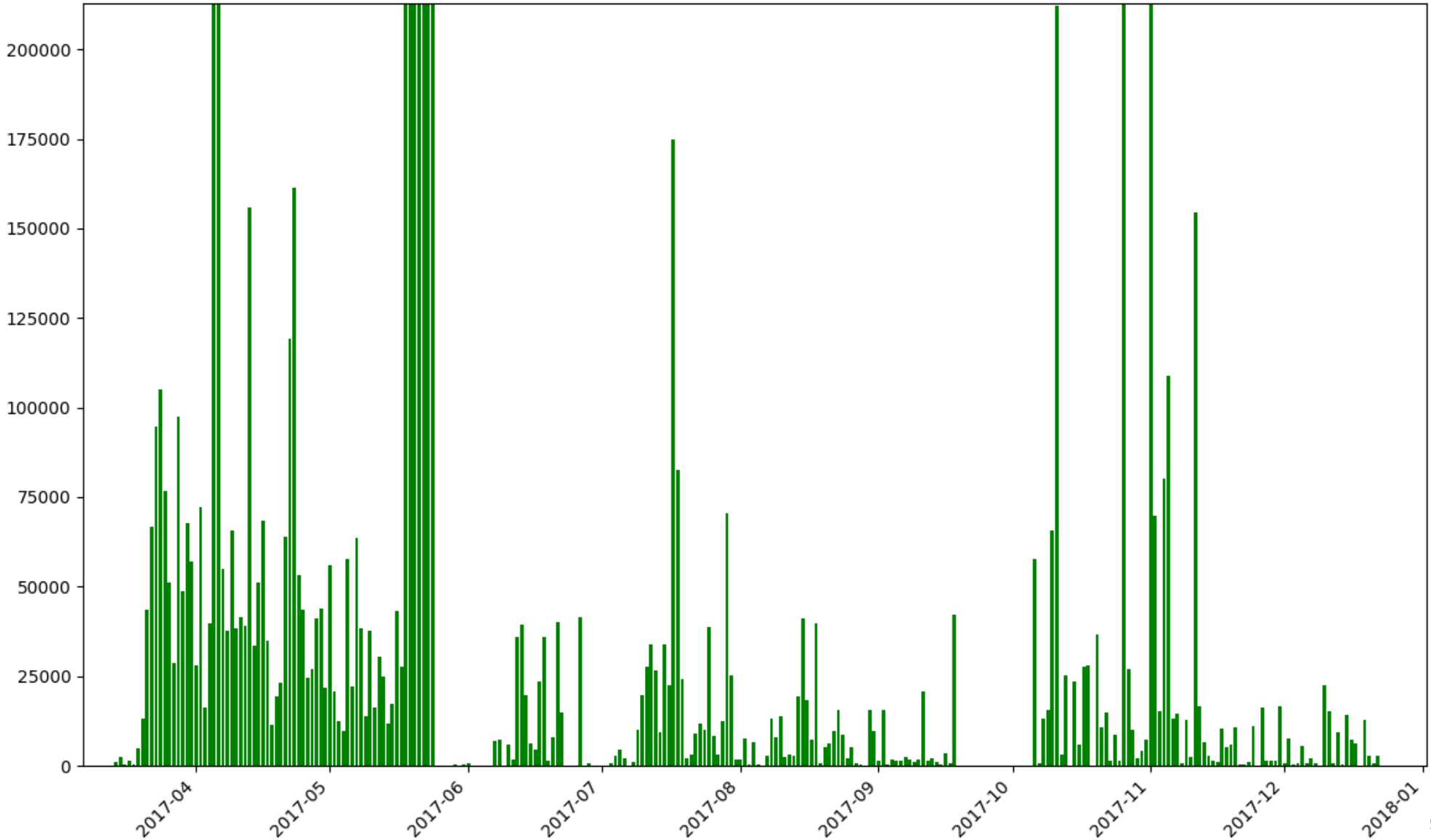
- **Automatisiert**
  - auswertbare Leak-Announcement-Pages
  - auffindbare Datensenken
    - pastebin.com
    - slexy.org
    - micropaste.com
    - siph0n.net
    - pastelink.net
    - …

PASTEBIN

Sammlung von Identitätsdaten – „Pastes/Leaks“ pro Tag



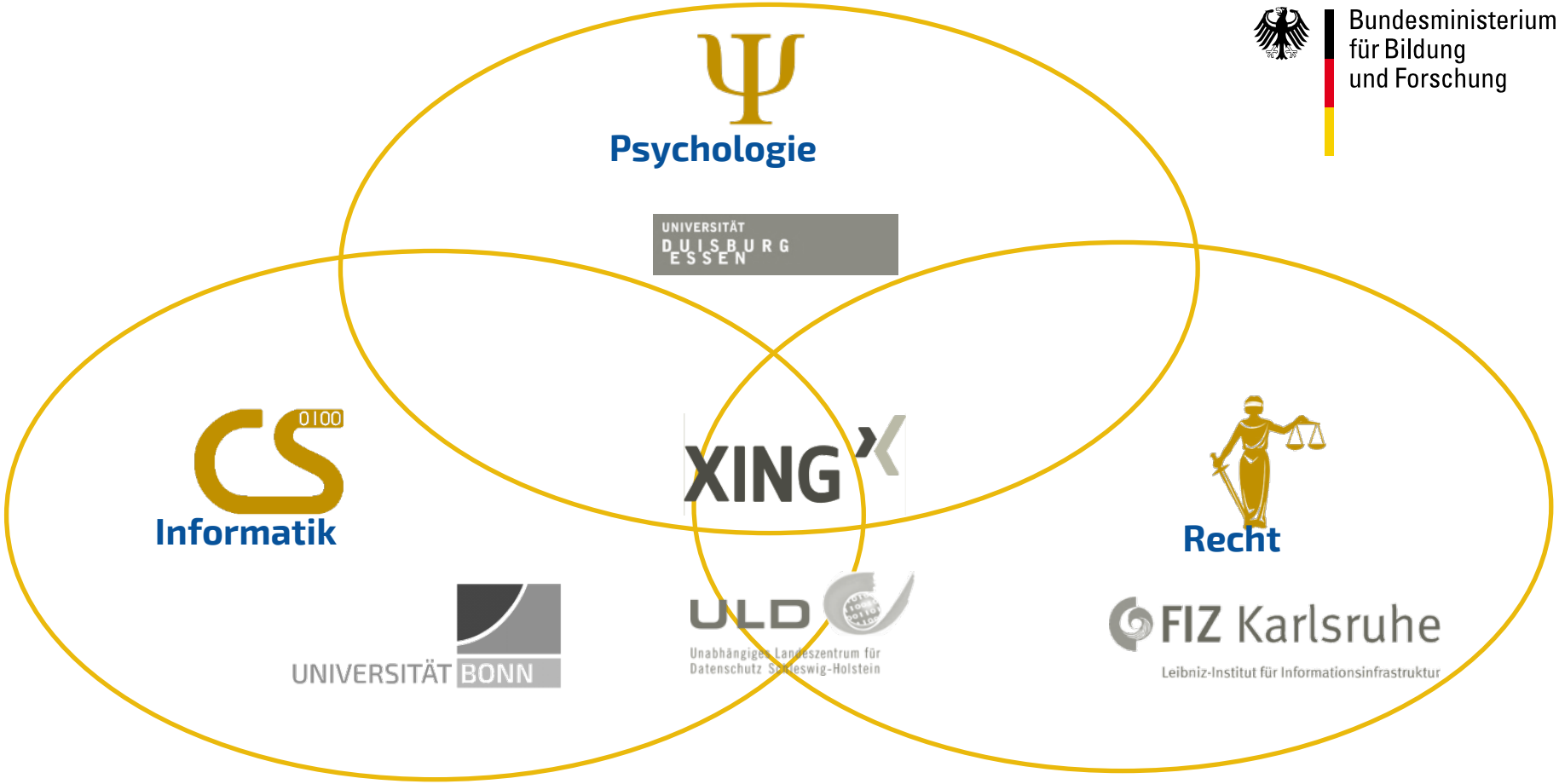
Sammlung von Identitätsdaten – E-Mail-Adressen pro Tag



Konsortium

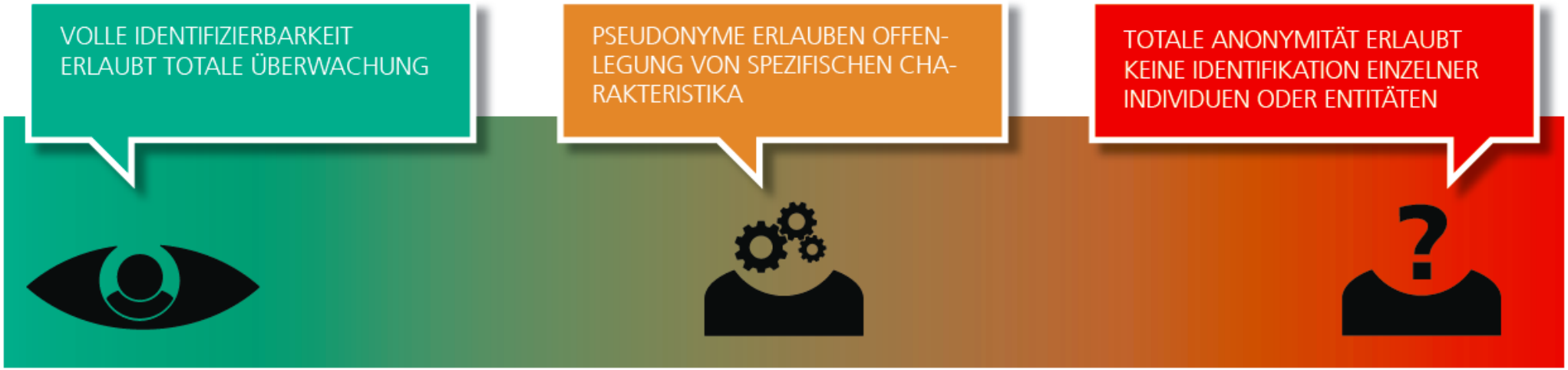
GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung



Pseudonyme -
Enabler für Kooperatives Verteiltes IT-Sicherheits-Monitoring

- Austausch sicherheitsrelevanter Informationen unterliegt sowohl Verfügbarkeits- als auch Vertraulichkeitsanforderungen
  - Beide können in Einklang gebracht werden
  - Maßgeschneiderte Pseudonyme erlauben geeignete Balance



Überblick

- IT-Sicherheit
  - Ziele, Verfahren und Annahmen
- Herausforderungen
  - Zielkonflikte
  - Programmierfehler
  - Hardware-“Macken“
  - Faktor Mensch
- Aktuelle Fragen (und Antworten)
  - Internet-Routing-Manipulation
  - IT-Security-Awareness messen
  - Digitaler Identitätsdiebstahl

Bachelor-Studiengang Cyber Security
geplant ab Wintersemester 2019/2020

Vielen Dank für Ihre Aufmerksamkeit

Prof. Dr. Michael Meier

Universität Bonn
Informatik 4
Endenicher Allee 19A
53115 Bonn
EMail: mm@cs.uni-bonn.de

Fraunhofer FKIE
Fraunhofer Str. 20
53343 Wachtberg
EMail: michael.meier@fkie.fraunhofer.de