INSTITUT FÜR RECHTSINFORMATIK
UNIVERSITÄT DES SAARLANDES

CISPA HELMHOLTZ-ZENTRUM i. G.

RECHTSWISSENSCHAFTLICHE FAKULTÄT
UNIVERSITÄT DES SAARLANDES

Sicherheits- und Risikomanagement im ERV

Prof. Dr. Christoph Sorge
juris-Stiftungsprofessur
für Rechtsinformatik

Institut für Rechtsinformatik und CISPA an der Universität des Saarlandes

Institut für Rechtsinformatik
- Forschung an der Schnittstelle von Recht und IT
- Teil der rechtswissenschaftlichen Fakultät
- Fünf Lehrstühle und ein Emeritus

www.rechtsinformatik.saarland

Center for IT Security, Privacy and Accountability
- Helmholtz-Zentrum i.Gr.
- ca. 200 (bald: > 500) Forscher arbeiten an unterschiedlichsten technischen Aspekten der IT-Sicherheit

www.cispa.saarland

Universität des Saarlandes
Prof. Dr. Christoph Sorge

IT-Sicherheitsforscher und Sicherheitsbeauftragte

- Denken an den „Worst Case“
- Hauptberuf: „Bedenkenträger“

Grundfrage

„The issue's not whether you're paranoid, Lenny, I mean look at this shit, the issue is whether you're paranoid enough."

Max im Film „Strange Days" (1995)

→ Idealvorstellung: Systeme und Verfahren, die kein Vertrauen benötigen, sondern nachvollziehbar und nachweisbar sicher sind

Bevor wir fortfahren…

- Wesentliche Information fehlt bisher: Was verstehen wir eigentlich unter „sicher"?
  - Sicherheit als „Funktionssicherheit" (engl. „safety") eines IT-Systems: System tut, was es soll – auch unter zufällig eintretenden, widrigen Bedingungen
  - Sicherheit als „Informationssicherheit" (engl. „security") eines IT-Systems: System widersteht auch intelligenten Angreifern – und gibt insbesondere keine Informationen preis, die es nicht preisgeben sollte

Fokus im Folgenden auf „Security"

Grundbaustein: Kryptographie

- Kryptographie liefert beweisbare Sicherheit
  - unter bestimmten mathematischen Annahmen
  - bezüglich einzelner, konkreter Schutzziele (z.B. Vertraulichkeit)
  - in einem konkreten Umfeld und nur gegenüber Entitäten, die bestimmte Informationen (z.B. private Schlüssel) nicht haben

Folgerung

Problem verschlüsselter Kommunikation mit Kryptographie zunächst einfach lösbar

Weitere Maßnahmen der Kommunikationssicherheit

- Firewalls
  - Ohne/mit Deep Packet Inspection
- Intrusion Detection / Intrusion Prevention

Bilder: Openclipart, User juanjo (Firewall)

Weitergehend

Problem verschlüsselter Kommunikation mit Kryptographie zunächst einfach lösbar

Weitere Maßnahmen der Kommunikationssicherheit

- Firewalls
  - Ohne/mit Deep Packet Inspection
- Intrusion Detection / Intrusion Prevention

Zwischenfazit

- Kryptographie bietet „echte“ Sicherheit
→ Wunsch, Probleme möglichst mit Kryptographie zu lösen
- Deutlich weniger Formalisierung und damit Möglichkeiten für Sicherheitsbeweise bei Entwicklung von Software und erst recht komplexen IT-Systemen
- „Hundertprozentig“ sicheres IT-System daher praktisch nicht möglich
→ Sicherheitsmanagement braucht Reaktionsmöglichkeiten auf neue Entwicklungen (Update-/Patch-Management) und falls Sicherheitsziele verletzt werden (Notfallmanagement)
- IT-Sicherheit (auch) als Prozess denken

Wie sicher ist „sicher“?

- Ist Sicherheit erreicht, wenn…
  - … Kosten für den Angreifer so hoch werden, dass der Angriff sich nicht lohnt?

Woher kennen Sie die Kosten für den Angreifer?
Wieso sollte der Angreifer sich rational verhalten?

  - … der erwartete Schaden (berechnet aus Schadenhöhe und Eintrittswahrscheinlichkeit) niedrig genug ist?

Woher kennen Sie die Eintrittswahrscheinlichkeit?

Folge

- IT-Sicherheitsmanagement ist keine exakte Wissenschaft
- Orientierung an Erfahrungen und Standards
  - Beispiel: IT-Grundschutz des BSI
- Erste Aufgaben: Verstehen,
  - welche Systeme vorhanden sind
  - welche Schutzziele bezogen auf diese Systeme erreicht werden sollen
  - mit welcher Art von Angreifern zu rechnen ist
  - welches Schadenspotential in Abhängigkeit von betroffenen Systemen und Schutzzielen besteht

Sicherheitsmanagement: BSI

- Bestandteile eines Managementsystems für Informationssicherheit nach BSI-Standard 100-1

BSI-Standard 100-1, Seite 13

Kernbotschaften (subjektiv interpretiert):

- Erarbeitung einer Sicherheits-Leitlinie in Abhängigkeit von den gegebenen Rahmenbedingungen
- Umsetzung der Leitlinie

Sicherheitsmanagement: BSI

- Bestandteile eines Managementsystems für Informationssicherheit nach BSI-Standard 100-1

BSI-Standard 100-1, Seite 13

Kernbotschaften (subjektiv interpretiert):

- Jeder einzelne Mitarbeiter bzw. Beteiligte muss sich mit IT-Sicherheit befassen

Sicherheitsmanagement: BSI

- Bestandteile eines Managementsystems für Informationssicherheit nach BSI-Standard 100-1

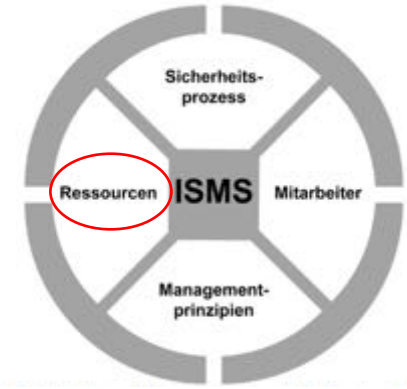
BSI-Standard 100-1, Seite 13

Kernbotschaften (subjektiv interpretiert):

- Leitungsebene übernimmt Verantwortung und setzt (nach Kosten/Nutzen-Abwägung) Ziele für IT-Sicherheit
- Leitungsebene hält sich an Richtlinien

Sicherheitsmanagement: BSI

- Bestandteile eines Managementsystems für Informationssicherheit nach BSI-Standard 100-1



BSI-Standard 100-1, Seite 13

Kernbotschaften (subjektiv interpretiert):

- IT-Sicherheit kostet Geld

Sicherheitsmanagement im ERV

- Sicherheitsmanagement für den ERV als Ganzes existiert folglich nur rudimentär
  - Keine einheitliche Verantwortlichkeit für den Gesamtprozess, sondern nur für Teilsysteme
  - Beispiel: Übermittlung von Dokumenten zwischen Rechtsanwalt und Gericht betrifft zumindest deren Systeme sowie das beA bzw. EGVP
  - Per se kein Problem – sofern Beteiligte sich ihrer jeweiligen Verantwortlichkeit bewusst sind

Sicherheitsmanagement im ERV

Offene Fragen:

- Wer führt die Abwägung zwischen Kosten und Nutzen von IT-Sicherheitsmaßnahmen durch?
- Wie detailliert sollte Sicherheitsmanagement durch Gesetz- und Verordnungsgeber geregelt werden?
  - Diverse Vorgaben für das beA in der RAVPV
  - Zu viel? Zu wenig?
  - Sind die bestehenden Regelungen „richtig“?
  - Wie erfolgt die Rückkopplung?
- Vorbildcharakter der eIDAS-Verordnung?

Offenheit und Kerckhoffs-Prinzip

- „La Cryptographie militaire“ (Auguste Kerckhoffs)
  - Forderung nach Verwendung von Schlüsseln
  - Forderung, dass Verschlüsselung nicht durch Bekanntwerden des Verfahrens unsicher werden darf
  - Forderung nach Untersuchung der Sicherheit kryptographischer Verfahren durch Experten

- Verallgemeinerung auf IT-Sicherheit?
  - Vorteile der Offenheit?
  - Rechts-Kompatibilität der Offenheit?

Folgerungen für das beA+

- Vertrauen in IT-Sicherheit benötigt Offenheit
  - in Bezug auf Sicherheitsarchitekturen und -protokolle (!)
  - in Bezug auf Details der Umsetzung und Quellcode (?)
  - ~~in Bezug auf kryptographische Schlüssel, Log-Dateien, …~~
  - in Bezug auf entdeckte Sicherheitslücken (wann?)
- Kryptographie (→ Ende-zu-Ende-Verschlüsselung) als Königsweg, aber nicht einziger Weg
- Einbettung in eine übergreifende ERV-Architektur und in die Kanzleiorganisation

Kontakt

christoph.sorge@uni-saarland.de
www.legalinf.de
Twitter: @legalinf

Christoph Sorge
Campus E9.1
66123 Saarbrücken