INSTITUT FÜR RECHTSINFORMATIK
UNIVERSITÄT DES SAARLANDES

CISPA Center for IT-Security, Privacy and Accountability

Nichts ist unmöglich: Konzepte zur Cybersicherheit in Unternehmen

Christoph Sorge, Universität des Saarlandes

juris-Stiftungsprofessur für Rechtsinformatik
Fakultät R

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
- Eines von drei BMBF-geförderten Kompetenzzentren für IT-Sicherheit sowie designiertes Helmholtz-Zentrum
- ca. 200 (bald: > 500) Forscher arbeiten an unterschiedlichsten technischen Aspekten der IT-Sicherheit

www.cispa.saarland

Grundfrage

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

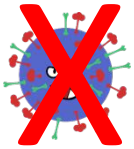
Max im Film „Strange Days" (1995)

Folgerung

Einführung von

- Firewalls
  – Ohne/mit Deep Packet Inspection

- Intrusion Detection / Intrusion Prevention
- verschlüsselter Kommunikation (E-Mail, Aufruf von Websites etc.)
- Antivirus-Software



Bilder: Openclipart, User juanjo (Firewall), User qubodup (Virus)

Folgerung

Einführung von

- Firewalls
  – Ohne/mit Deep Packet Inspection

- Intrusion Detection / Intrusion Prevention
- verschlüsselter Kommunikation (E-Mail, Aufruf von Websites etc.)
- Antivirus-Software

Beispiele für Angriffe

Low Tech

- Diebstahl aller Arten von Datenträgern (einschließlich Papier)
- Dumpster diving

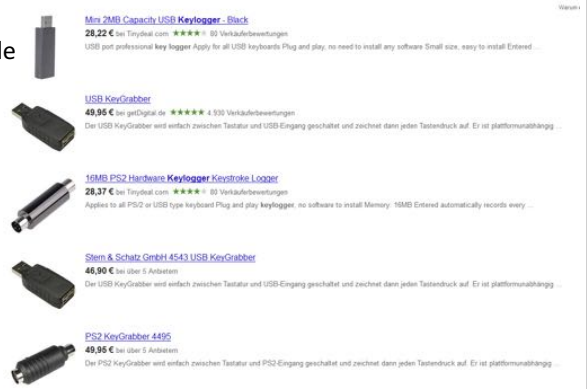
Bildquelle: Ethan Lofton über Flickr, CC BY-NC-SA 2.0
https://www.flickr.com/photos/elofton/5202726514/

Maßnahmen:

- Verschlüsselung aller digitalen Datenträger (ggf. Ausnahme für physisch gesicherte, z.B. im Panzerschrank aufbewahrte Datenträger)
- Zuverlässige Vernichtung nicht mehr benötigter Datenträger

Direkter Zugriff auf IT-Systeme

- Hardware-Keylogger
  - Mitlesen aller eingegebenen Zeichen
  - Speichern und Mitnahme durch Angreifer zu späterem Zeitpunkt; alternativ drahtlose Übermittlung der Tastendrücke möglich
  - Bild: Suche nach „Keylogger“ bei Google Shopping



Maßnahmen:
- Zutrittskontrolle
- Sensibilisierung der Mitarbeiter
- Ggf. regelmäßige Überprüfung der Anschlüsse

7

UNIVERSITÄT DES SAARLANDES | INSTITUT FÜR RECHTSINFORMATIK UNIVERSITÄT DES SAARLANDES | CISPA | juris-Stiftungsprofessur für Rechtsinformatik Fakultät R

Beispiele für Angriffe

Shoulder Surfing
- Direkte Beobachtung eines Nutzers bei Interaktion mit einem IT-System

Maßnahmen:
- Sitzplatzwahl
- Privacy-Filter (Schutzfolien)
- Beschränkung der Bearbeitung vertraulicher Dokumente außerhalb der Büroräume

8

Beispiele für Angriffe

- Duplizieren von Schlüsseln durch „optisches Auslesen“ (Laxton/Wang/Savage 2008)

Lesen vertraulicher Dokumente in Reflexionen (Backes/Durmuth/Unruh 2008)

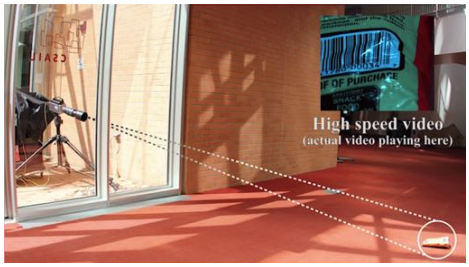
- Bild: Spiegelung eines Monitorbildes in einer Teekanne, aufgenommen aus 40 m Entfernung
- Prinzip auch auf Spiegelungen im Auge anwendbar

Maßnahmen:
- Sensibilisierung der Mitarbeiter
- Ggf. Schließen von Jalousien o.ä.

UNIVERSITÄT DES SAARLANDES | INSTITUT FÜR RECHTSINFORMATIK UNIVERSITÄT DES SAARLANDES | CISPA | juris-Stiftungsprofessur für Rechtsinformatik Fakultät R

Beispiele für Angriffe

- Akustische Signale erzeugen Schwingungen von Objekten
  - Beispiel: Fensterscheiben → Erfassen dieser Schwingungen mit Lasern
  - Neuere Forschungsergebnisse: Erfassen der Schwingungen von Objekten innerhalb eines Raums per Videokamera



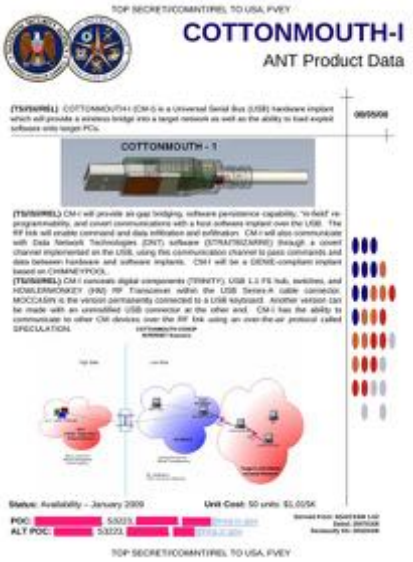
Maßnahmen:
- Sensibilisierung der Mitarbeiter
- Ggf. Schließen von Jalousien o.ä.

Bildquelle: Ausschnitt aus https://www.youtube.com/watch?v=FKXOucXB4a8

Direkter Zugriff auf IT-Systeme

- NSA: Cottonmouth-Projekt
  - Ziel: Überwachung nicht vernetzter Geräte
  - Mittel: Per USB angeschlossener Radiosender
  - Mögliche Unterbringung in normal großem USB-Stecker
- Auch: Abfangen online bestellter Hardware in der Post

Maßnahmen hier wohl nicht alltagstauglich



Praxis-Beispiel (nach Presseberichten): Bundestag

- Eingehende E-Mail mit Betreff *„Ukraine conflict with Russia leaves economy in ruins“,* Absenderadresse …@un.org
- Enthaltener Link führt zu Website mit Schadsoftware (vermutlich: Ausnutzung einer Sicherheitslücke im Browser)
- Anschließend weitere Verbreitung im internen Netz des
- Kein Zugriff auf Dokumente des Vertrauensgremiums, die per Boten auf Papier überbracht werden

Maßnahmen:
- Sensibilisierung der Mitarbeiter
- Patch-Management → schnelle Updates
- Rückkehr zu Papier und Schreibmaschine?

Sicherheitskonzepte

- Sicherheitskonzepte enthalten Maßnahmen aus allen Kategorien (administrativ, personell, physische Sicherheit, Netzsicherheit …)
  - Basierend auf Strukturanalyse und Risikoanalyse (je nach Schutzziel: Vertraulichkeit, Verfügbarkeit, Integrität, …)
- Kern: Sicherheits-Leitlinie mit Vorgaben zu Sicherheitsmanagement
- Einbeziehung der Mitarbeiter
  - Vorgaben an Mitarbeiter, z.B. Auswahl und Aufbewahrung von Passwörtern
  - Ermutigung, Sicherheitsbedrohungen rasch zu melden

13

UNIVERSITÄT DES SAARLANDES | INSTITUT FÜR RECHTSINFORMATIK UNIVERSITÄT DES SAARLANDES | CISPA | juris-Stiftungsprofessur für Rechtsinformatik Fakultät R

Sicherheitskonzepte: Elemente

- Strategie zur Datenspeicherung, insbesondere
  - Auf mobilen Datenträgern
  - In der Cloud
- Sollen Daten verschlüsselt werden? (Ja!)
  - Wie? (Basierend auf Passwort, Smartcards, …)
  - Sichere Verschlüsselung im Prinzip gelöst
- Strategie für Backups

14

Sicherheitskonzepte: Elemente

- Wichtig für Medienunternehmen auch: Sichere Kommunikationswege / Erreichbarkeit von außen
  - Verschlüsselte E-Mail (S/MIME und GPG) als Muss – Ende-zu-Ende-Verschlüsselung, nicht nur Transportverschlüsselung
  - Ggf. gesicherte Kommunikationsplattformen im Web
  - Unterstützung von Anonymität, z.B. Tor Hidden Services
- Problem eher der Nutzbarkeit als der Sicherheit der Verschlüsselung
  - Recht neuer Ansatz: Ende-zu-Ende-verschlüsselte Kommunikation über Web-Plattformen

15

UNIVERSITÄT DES SAARLANDES | INSTITUT FÜR RECHTSINFORMATIK UNIVERSITÄT DES SAARLANDES | CISPA | juris-Stiftungsprofessur für Rechtsinformatik Fakultät R

Sicherheitskonzepte: Elemente

- Schutz vor Schadsoftware
  - Bislang ungelöstes Problem
  - Eher „symptomatische Behandlung“ – Erkennung der Verbreitungswege, ungewöhnlichen Verhaltens etc.
  - Updates helfen gegen Ausnutzung bekannter Sicherheitslücken
  - Firewalls und IDS/IPS helfen, Ausbreitungswege einzuschränken
- Antivirussoftware
  - Erkennungsraten für bekannte und verbreitete Schadsoftware sehr hoch
  - Erkennung maßgeschneiderter oder sehr neuer Schadsoftware aber mangelhaft

→ Ziel: Folgen von Schadsoftware gering halten

16

Abstufungen der Sicherheit

- Basics
  - Maßnahmen, die nichts kosten (Türen abschließen etc.)
  - Maßnahmen gegen Angriffe, die den Angreifer nichts oder sehr wenig kosten (z.B. Ausnutzung bereits bekannter Sicherheitslücken)
- Zusätzliche Maßnahmen entsprechend Schutzbedarf
  - Maßgabe: Schutzbedarf nicht unterschätzen!
- Bis hin zu nicht vernetzten PCs (ohne WLAN und Bluetooth) in fensterlosen, stets verschlossenen, bewachten Räumen und ohne Verwendung mobiler Datenträger

17

Fazit

- „Nichts ist unmöglich“ – gilt insbesondere für die Angreifer
- Strukturanalyse und Schutzbedarfsfeststellung als erste Schritte
- IT bietet zahlreiche Maßnahmen
- Aber: Kein umfassender Schutz alleine durch IT
- Sicherheitsbewusstsein jedes einzelnen Mitarbeiters notwendig

→ IT-Sicherheit im Unternehmen als übergreifendes Problemfeld

18

UNIVERSITÄT DES SAARLANDES | INSTITUT FÜR RECHTSINFORMATIK UNIVERSITÄT DES SAARLANDES | CISPA | juris-Stiftungsprofessur für Rechtsinformatik Fakultät R

Kontakt

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

Christoph Sorge
Campus E9.1
66123 Saarbrücken