INSTITUT FÜR RECHTSINFORMATIK
UNIVERSITÄT DES SAARLANDES

CISPA
HELMHOLTZ-ZENTRUM i. G.

RECHTSWISSENSCHAFTLICHE FAKULTÄT
UNIVERSITÄT DES SAARLANDES

Technische Sicherheitsmaßnahmen im Licht der DS-GVO

Prof. Dr. Christoph Sorge
juris-Stiftungsprofessur
für Rechtsinformatik

Institut für Rechtsinformatik und CISPA an der Universität des Saarlandes

Institut für Rechtsinformatik

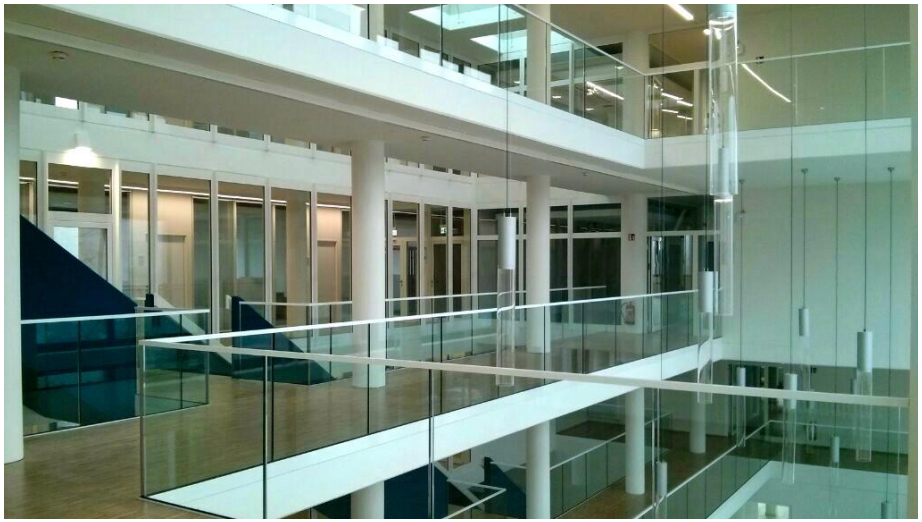
- Forschung an der Schnittstelle von Recht und IT
- Teil der rechtswissenschaftlichen Fakultät
- Fünf Lehrstühle und ein Emeritus

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



Vorbemerkung

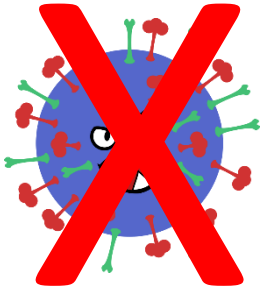
- IT-Sicherheitsthemen mehrfach in der DS-GVO erwähnt (Art. 6 Abs. 4 lit. e, 24, 25, 32 – weitere Normen bei weiter Fassung des Begriffs)
- Auch „Privacy by Design“ greift auf Methoden der IT-Sicherheit zurück
- Hier aber Fokus auf IT-Sicherheit im engeren Sinn und Einordnung des Art. 32

Sicherheit?

Einführung von

- Firewalls
  - Ohne/mit Deep Packet Inspection

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

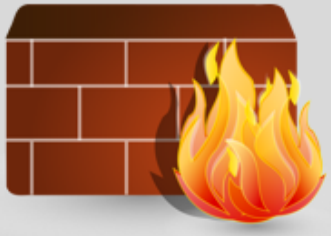


Bilder: Openclipart, User juanjo (Firewall), User qubodup (Virus)

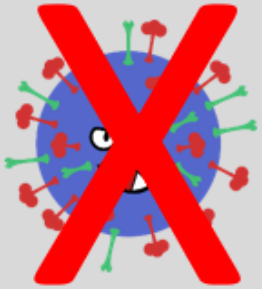
Sicherheit?

Einführung von

- Firewalls
  - Ohne/mit Deep Packet Inspection



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



IT-Sicherheit in der DS-GVO

- Art. 32 DS-GVO

„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter *geeignete technische und organisatorische Maßnahmen*, um ein dem Risiko *angemessenes Schutzniveau* zu gewährleisten […]“

Einzelne Maßnahmen nach Art. 32 DS-GVO

- Im Folgenden einige Kommentare zu einzelnen Maßnahmen nach Art. 32 Abs. 1 DS-GVO durch die „Informatiker-Brille“

- Dabei aber: Kontext berücksichtigen
  - Art. 32 fordert nicht Umsetzung einer bestimmten Einzelmaßnahme – diese sind nur „unter anderem“ eingeschlossen

Einzelne Maßnahmen nach Art. 32 DS-GVO

- Im Folgenden einige Kommentare zu einzelnen Maßnahmen nach Art. 32 Abs. 1 DS-GVO durch die „Informatiker-Brille“

- Dabei aber: Kontext berücksichtigen
  - Art. 32 fordert nicht Umsetzung einer bestimmten Einzelmaßnahme – diese sind nur „unter anderem“ eingeschlossen

- Sprachliche Eigenheiten („Fähigkeit“ als Maßnahme) werden im Folgenden ignoriert

Einzelne Maßnahmen nach Art. 32 DS-GVO

- (a) „die *Pseudonymisierung* und *Verschlüsselung* personenbezogener Daten“
  - Völlig unterschiedliche Themen, aber beide unter Buchstabe (a) gefordert
- Pseudonymisierung: Erst in jüngerer Zeit in einigen Lehrbüchern als Schutzziel der IT-Sicherheit aufgeführt
  - Verhältnismäßig schwacher Schutz – Gefahr nachträglicher Zusammenführung von Pseudonymen mit zugehörigen Daten
- Verschlüsselung
  - Standard-Maßnahme der IT-Sicherheit zum Schutz der Vertraulichkeit
  - Hier (natürlich) unterspezifiziert

Bild: Openclipart, User Dustwin

Einzelne Maßnahmen nach Art. 32 DS-GVO

- (b) „die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen“
- (bis auf Belastbarkeit) klassische Schutzziele der IT-Sicherheit
- Vermischung der Ziele bzgl. Systemen und Daten

Einzelne Maßnahmen nach Art. 32 DS-GVO

- (c) „die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen“
- Bedeutung des Notfallmanagements tatsächlich oft unterschätzt
- Backups, Löschanlagen, …
- Festlegung von Verantwortlichkeiten, Meldeketten, …

Einzelne Maßnahmen nach Art. 32 DS-GVO

- (d) „ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.“

- „Meta-Maßnahme“

- IT-Sicherheit als Prozess, nicht als statischer Zustand

Zwischenfazit

- Artikel 32 Abs. 1 beschreibt eher Ziele als Maßnahmen
- Zunächst unbefriedigende, weil vage Norm
- Aber: Tatsächlich erscheinen allgemeine Zielvorgaben als sachgerecht
  - Kein „one size fits all“ an Sicherheitsmaßnahmen verfügbar

→ Anforderungen der DS-GVO als Ausgangspunkt

Risikobetrachtung

- Art. 32 Abs. 2:
  „Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung […] verbunden sind.“

→ Wiederum: Vorschrift entspricht Standard-Vorgehensweise der IT-Sicherheit

- Berücksichtigung von Eintrittswahrscheinlichkeit und Schwere der möglichen Schutzgutsverletzung

- Beispiel: Bewertung mit Scorecards

Regulierung von IT-Sicherheit

- Art. 32 Abs. 3: Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens als Indiz für Erfüllung der Anforderungen an die IT-Sicherheit

- Lässt sich IT-Sicherheit regulieren, zertifizieren, auditieren?

- Ja
  - Vorgabe von Sicherheitsstandards, Zertifizierungen, Meldepflichten, …

  → Hilfreich

- , aber…
  - Praktische Beispiele zeigen auch Versagen der Regulierungsmechanismen

Bruce Schneier: „Security mindset“

Uncle Milton Industries has been selling ant farms to children since 1956. Some years ago, I remember opening one up with a friend. There were no actual ants included in the box. Instead, there was a card that you filled in with your address, and the company would mail you some ants. My friend expressed surprise that you could get ants sent to you in the mail.

I replied: "What's really interesting is that these people will send a tube of live ants to anyone you tell them to."

Security requires a particular mindset. Security professionals—at least the good ones—see the world differently. They can't walk into a store without noticing how they might shoplift. They can't use a computer without wondering about the security vulnerabilities. They can't vote without trying to figure out how to vote twice. They just can't help it. https://www.schneier.com/blog/archives/2008/03/the_security_mi_1.html

Foto: Nutzer Rama, Wikimedia Commons, Cc-by-sa-2.0-fr
https://commons.wikimedia.org/wiki/File:Bruce_Schneier_at_CoPS2013-IMG_9058.jpg

Konflikt IT-Sicherheit vs. Datenschutz

- Zum Teil (scheinbarer oder echter) Konflikt zwischen Zielen der IT-Sicherheit und des Datenschutzes

- Beispiele
  - Logging (von Zugriffen auf schützenswerte Daten)
  - Intrusion Detection Systems
  - Aufbrechen verschlüsselter Verbindungen durch Arbeitgeber

Beispiel IDS

- Standard-Maßnahme der IT-Sicherheit, bezogen auf Netze und teils auch Endsysteme
- Erkennung von Angriffen (anhand vordefinierter Muster) bzw. Anomalien (anhand gelernten Normalverhaltens)
- Problem: IDS verarbeiten in der Regel personenbezogene Daten (z.B. IP-Adressen und zugehörige Aktivitäten)
  - Welches System startet einen Angriff auf Dritte?
  - Wer lädt wann welche Datenmengen herunter?
  - Wie viele Verbindungen baut ein bestimmter Rechner auf?

Rechtmäßigkeit des IDS-Einsatzes?

- Verpflichtung zum Einsatz von IDS durch Art. 32?
  - Unter Umständen: Ja

- Rechtfertigung des IDS-Einsatzes?

Erwägungsgrund 49: Zumindest für Betreiber von elektronischen Kommunikationsnetzen und –diensten überwiegendes berechtigtes Interesse (Art. 6 Abs. 1 lit. f) in dem Maße, wie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist

→ Abwägung!

→ Wie fällt diese aus beim Aufbrechen verschlüsselter Verbindungen?

Fazit

- Sprachlich nicht durchgehend geglückte, aber inhaltlich nachvollziehbare Regelung der IT-Sicherheitsanforderungen in Art. 32 DS-GVO
- Problem der Unbestimmtheit der Norm in der Praxis wohl lösbar
- Rückgriff auf Standards und Zertifizierungen trotz deren Grenzen

Kontakt

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

Christoph Sorge
Campus E9.1
66123 Saarbrücken