IT-Infrastrukturen und Datenschutz – brüchiges Fundament & dürftige Statik?

Marit Hansen
Landesbeauftragte für Datenschutz
Schleswig-Holstein

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Überblick

1. IT-Infrastrukturen und ihre Bedeutung als Fundament
2. Zustand der IT-Infrastrukturen: wie vertrauenswürdig?
3. Umgang mit Risiken
4. Datenschutz-Infrastrukturen
5. Fazit

Fundament

Ein **Fundament** (von lat. *fundus* ‚Bodengrund') ist im Bauwesen Teil der allgemeinen Gründung. Es besteht aus Elementen wie Platten, Pfählen (siehe Pfahlgründung), Träger, Steinen und so weiter. Heutzutage besteht das Fundament hauptsächlich aus Stahlbeton.

WIKIPEDIA

Baustatik

Baustatik oder die Statik der Baukonstruktionen ist die Lehre von der Sicherheit und Zuverlässigkeit von Tragwerken im Bauwesen. In der Baustatik werden die Kräfte und deren gegenseitige Auswirkungen in einem Bauwerk sowie in jedem dazugehörigen Bauteil berechnet. Die Berechnungsverfahren der Baustatik sind Hilfsmittel der Tragwerksplanung und mit der Lehre der Modellbildung und der Konstruktionslehre Teil der Tragwerkslehre.

ULD www.datenschutzzentrum.de

Fundament & Statik

- Im Bauwesen wichtig – sonst Einsturzgefahr
- Analogie: IT-Infrastrukturen: Fundament & Statik für die Informationsgesellschaft

vertrauenswürdige

Ohne IT-Infrastrukturen keine Informationsgesellschaft

vertrauenswürdige

IT-Infrastrukturen und DS – brüchiges Fundament, dürftige Statik

Bei Pfusch am Bau: Schuldfrage + Verjährung?

Kieler Nachrichten
Das Portal der KN und Segeberger Zeitung

EINGESTÜRZTE HALLE

Die Schuldfrage bleibt offen

Fünfeinhalb Jahre nach dem Einsturz einer ehemaligen Tennishalle in Plön unter Schneelast bleibt die Frage nach menschlicher Verantwortung unbeantwortet: Wie das Landgericht Kiel am Freitag bestätigte, platzte die Fünf-Millionen-Euro-Schadensersatzklage gegen einen Gutachter.

„... als Gutachter dürfe man sich hierzulande gewöhnlich auf eine behördlich geprüfte und genehmigte Statik verlassen“

Im schneereichen Winter 2009/2010 war die ehemalige Plöner Tennishalle Anfang Februar eingestürzt. Sie begrub die Störzucht unter sich, Hunderte von Fischen verendeten. Nach der Schneeschmelze wurde das Ausmaß der Zerstörung der Halle sichtbar.

Quelle: Dirk Schneider

Von Thomas Geyer

Artikel veröffentlicht: Freitag, 28.08.2015 20:22 Uhr

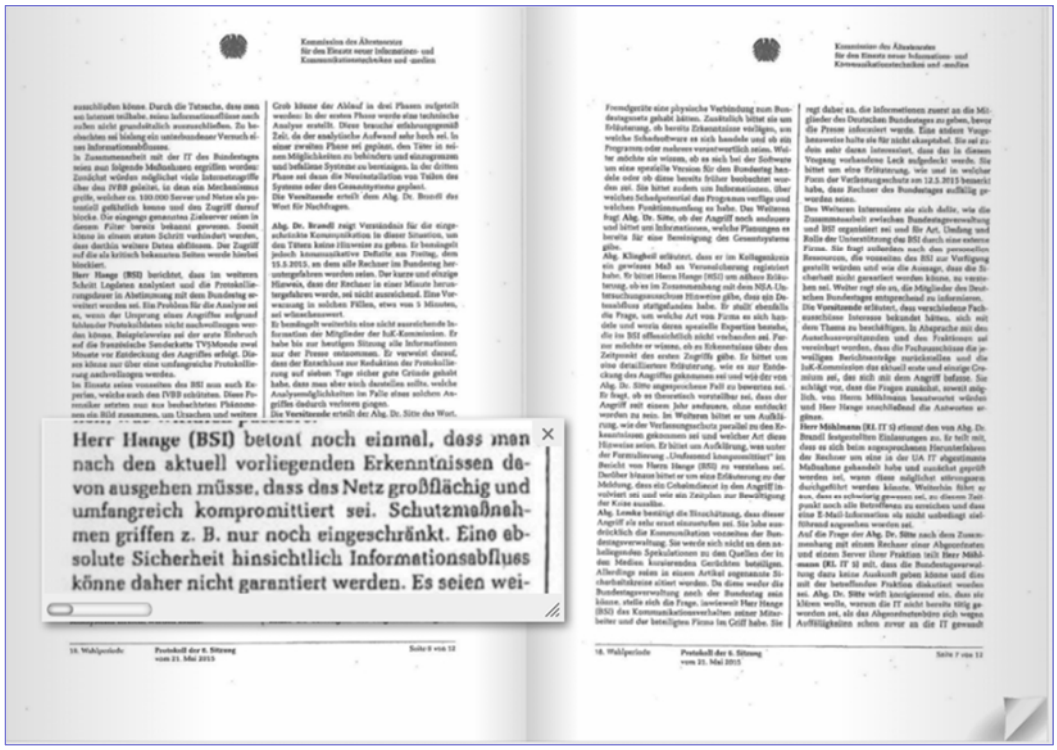
Artikel aktualisiert: Freitag, 28.08.2015 21:22 Uhr

Quelle: http://www.kn-online.de/News/Aktuelle-Nachrichten-Ploen/News-Aktuelle-Nachrichten-Ploen/Eingestuerzte-Halle-Die-Schuldfrage-bleibt-offen

Überblick

1. IT-Infrastrukturen und ihre Bedeutung als Fundament
2. Zustand der IT-Infrastrukturen: wie vertrauenswürdig?
3. Umgang mit Risiken
4. Datenschutz-Infrastrukturen
5. Fazit

Brüchiges Fundament?



Herr Hange (BSI) betont noch einmal, dass man nach den aktuell vorliegenden Erkenntnissen davon ausgehen müsse, dass das Netz großflächig und umfangreich kompromittiert sei. Schutzmaßnahmen griffen z. B. nur noch eingeschränkt. Eine absolute Sicherheit hinsichtlich Informationsabfluss könne daher nicht garantiert werden. Es seien wei-

Beispiel: „Bundestags-Hack“

Kommission des Ältestenrates für den Einsatz neuer Informations- und Kommunikationstechniken und –medien, Protokoll vom 21.05.2015

Gefährdungslage (BSI 2014)

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf

Bedrohungen	2013	2014	Prognose
Schwachstellen	↑	→	→
Spam	↓	↑	→
Schadprogramme	↑	↑	↑
Drive-by-Exploits und Exploit-Kits	↑	→	→
Botnetze	→	→	→
Social Engineering	→	↑	→
Identitätsdiebstahl	↑	↑	↑
Denial of Service (DoS; DDoS)	→	→	→
Advanced Persistent Threats (APT)	↑	→	↑

↑ Steigend → Gleichbleibend ↓ Sinkend

Tabelle 2: Zusammenfassung der Gefährdungslage der Angriffsmethoden und -mittel

Ursachenforschung I

Informatik-Baumeister

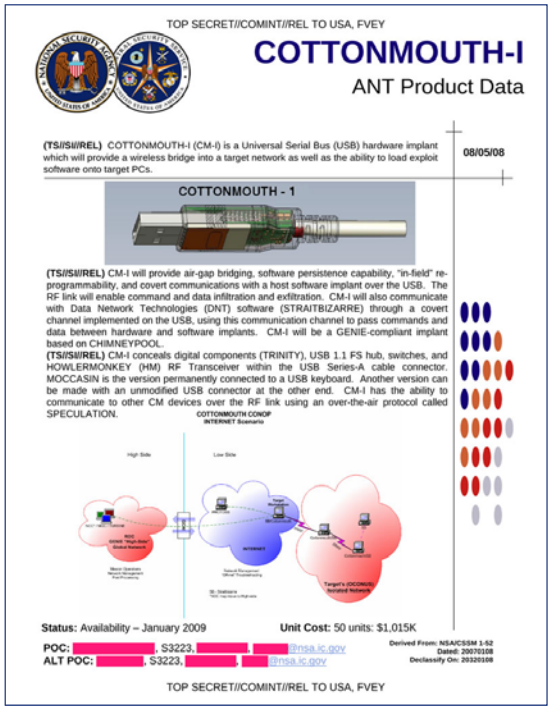
„Unter hoher Wachstumsgeschwindigkeit hat die Informatik kein professionelles Selbstverständnis entwickelt, das *per se* zuverlässige und bedachte Konstruktionen zum beruflichen Normalfall werden läßt.“

Wolfgang Coy (1992)

Ursachenforschung II

- Konzeptionelle Unmöglichkeit, Vertrauenswürdigkeit zu garantieren bei fremdbestimmten Komponenten
  - Erstellung
  - Betrieb
- Komplexität & Wechselwirkungen zwischen Komponenten
- Reale Welt mit IT-Landschaft, die „quick & dirty“ statt mit solider Planung entstanden ist
- Informatik-Beispiel:
  Datenabflüsse über verdeckte Kanäle („covert channels“)

Beispiele für genutzte verdeckte Kanäle



TOP SECRET//COMINT//REL TO USA, FVEY

COTTONMOUTH-I

ANT Product Data

(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

08/05/08

COTTONMOUTH - 1

(TS//SI//REL) CM-I will provide air-gap bridging, software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. The RF link will enable command and data infiltration and exfiltration. CM-I will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-I will be a GENIE-compliant implant based on CHIMNEYPOOL.

(TS//SI//REL) CM-I conceals digital components (TRINITY), USB 1.1 FS hub, switches, and HOWLERMONKEY (HM) RF Transceiver within the USB Series-A cable connector. MOCCASIN is the version permanently connected to a USB keyboard. Another version can be made with an unmodified USB connector at the other end. CM-I has the ability to communicate to other CM devices over the RF link using an over-the-air protocol called SPECULATION.

COTTONMOUTH CONOP
INTERNET Scenario

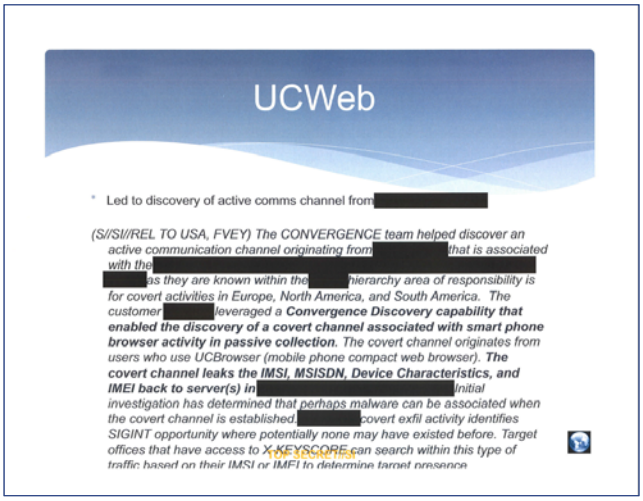
Status: Availability – January 2009 **Unit Cost:** 50 units: $1,015K

POC: [redacted], S3223, [redacted]@nsa.ic.gov

ALT POC: [redacted], S3223, [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY



UCWeb

- Led to discovery of active comms channel from [redacted]

*(S//SI//REL TO USA, FVEY) The CONVERGENCE team helped discover an active communication channel originating from [redacted] that is associated with the [redacted] as they are known within the [redacted] hierarchy area of responsibility is for covert activities in Europe, North America, and South America. The customer [redacted] leveraged a **Convergence Discovery capability that enabled the discovery of a covert channel associated with smart phone browser activity in passive collection**. The covert channel originates from users who use UCBrowser (mobile phone compact web browser). **The covert channel leaks the IMSI, MSISDN, Device Characteristics, and IMEI back to server(s) in** [redacted] Initial investigation has determined that perhaps malware can be associated when the covert channel is established [redacted] covert exfil activity identifies SIGINT opportunity where potentially none may have existed before. Target offices that have access to X-KEYSCORE can search within this type of traffic based on their IMSI or IMEI to determine target presence*

Quelle: Snowden-Dokumente (NSA)

ULD www.datenschutzzentrum.de

Ursachenforschung III

- Keine Stunde Null für den Aufbau von IT-Infrastrukturen
- Sondern Vermächtnis und Erblast der bisherigen Entwicklungen
  - Technisch
  - Politisch

- Wer beherrscht heute die Komponenten?
  - Hardware?
  - Internet-Verwaltung?
  - Router?
  - Zentrale Dienstleistungen im Netz?

Ursachenforschung IV

- Wer hat Interesse an Sicherheit?
- Wer hat Interesse an Unsicherheit?

- Lukrativer Markt
  für Zero-Day-Exploits
  (Angriffsmöglichkeit, bevor es eine Gegenmaßnahme gibt; Entwickler haben 0 Tage Zeit zum Reagieren)

http://tegenlicht.vpro.nl/backlight/zerodays.html
https://www.youtube.com/watch?v=4BTTiWkdT8Q

Überblick

1. IT-Infrastrukturen und ihre Bedeutung als Fundament
2. Zustand der IT-Infrastrukturen: wie vertrauenswürdig?
3. Umgang mit Risiken
4. Datenschutz-Infrastrukturen
5. Fazit

Vertrauenswürdigkeit – wirklich nötig?

- Psychologischer Rat:
  - Kontrollillusion aufgeben
  - Nicht blind Experten folgen
- Risikobewusstsein & Risikokompetenz schaffen ...
- ...auf der Basis von Wissen und Aufklärung
- Aber: Risikobequemlichkeit, gerade wenn negative Folgen nicht unmittelbar bemerkbar

Wie geht Vertrauenswürdigkeit?

- Prüfbarkeit herstellen
- Zugesicherte Funktionalität nachweisen
  - Durch Fremd-Attestierung
- Offenlegen
  - Open Source bei Software und Hardware
  - Komplexität reduzieren
  - Umfassende Transparenz über Konzepte, Änderungen, Umgang mit Fehlern
- Singuläre und unkontrollierbare Abhängigkeiten vermeiden

Überblick

1. IT-Infrastrukturen und ihre Bedeutung als Fundament
2. Zustand der IT-Infrastrukturen: wie vertrauenswürdig?
3. Umgang mit Risiken
4. Datenschutz-Infrastrukturen
5. Fazit

Datenschutz-Infrastrukturen

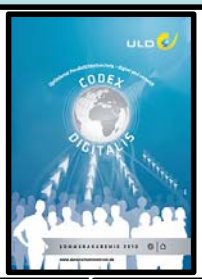
- Ende-zu-Ende-Verschlüsselung
  - Mit vertrauenswürdigem Schlüsselaustausch
- Signatur-Infrastrukturen
  - Mit pseudonymen Signaturen, Gruppensignaturen, ...
- Anonymisierungs-Infrastrukturen
  - Mit hintereinandergeschalteten Mix-Knoten im Internet
  - Whistleblower-Systeme
- Datenschutz-Service für jede und jeden

Überblick

1. IT-Infrastrukturen und ihre Bedeutung als Fundament
2. Zustand der IT-Infrastrukturen: wie vertrauenswürdig?
3. Umgang mit Risiken
4. Datenschutz-Infrastrukturen
5. Fazit

Verfeinerung: Fundament & Statik

- Eigentliches Fundament: Grund- und Menschenrechte
- IT-Infrastrukturen:



Fundament & Statik für die Informationsgesellschaft

vertrauenswürdige

Ohne IT-Infrastrukturen keine Informationsgesellschaft

vertrauenswürdige

Fazit

- Vertrauenswürdigkeit von IT-Infrastrukturen?
  - Zustand: nicht zufriedenstellend ☹
  - Trend: kein Selbstgänger ☹
- Verbesserungen sind nötig und möglich
- Nicht nur IT-Sicherheit erhöhen, sondern
  - (Eingebauten) Datenschutz
  - Transparenz: Information der Betroffenen über Risiken
- Nicht-Verbessern der Vertrauenswürdigkeit als ~~Investition~~ für die Informationsgesellschaft erhebliche Gefahr