

An aerial photograph of the NSA Headquarters at Fort Meade. The main building is a large, dark, rectangular structure with a white roof section. It is surrounded by a large parking lot filled with many cars. In the background, there are other buildings and a forested hill.

Datenspuren und Internet

Quelle: Wikipedia, NSA Headquarter Fort Meade

Agenda

- Historie - Technik
 - Hardwarebeispiel „Switch“
 - Softwarebeispiel „IPv4 / IPv6“
- Kommunikation
 - Beispiel E-Mail
 - Beispiel Fahrzeugkommunikation
 - Beispiel Cookie
 - Beispiel „tägliches Leben“
 - Beispiel Anonym im Netz
- Auswirkungen
 - Passwortgenerator
 - Verschlüsselung
 - Fazit

Historie

- 1957 RAND Corp. entwickelt zusammen mit Advanced Research Projects Agency (ARPA) im Auftrag des DoD (Department of Defense) eine „paketorientierte“ dezentrale Datenübertragung über ein „Netzwerk“
- Verschieden werden kleine nummerierte Pakete, die den Weg selber suchen. Jeder Computer bildet einen Netzknoten, jedes Paket hat Absender und Empfänger
- 1969 ARPANET bis 1971: 30 dezentrale Teilnehmer / Knoten, Ende 1969 steigen UCLA (Los Angeles), UCSB (Santa Barbara), Stanford (SRI), Uni Utah ein
- Alle Computer, die sich an (gemeinsame) Protokolle halten, sind kompatibel
- 1990 Tim Berners Lee entwickelt am CERN (das Kommerzielle) WWW
- 1995 vBNS (very high speed Backbone Network) als schnellstes Netz verbindet fünf amerikanische Zentren für Supercomputerforschung mit 622 Mbit/s
- Europäische Backbones (Ebone, betrieben von KPNQuest) gibt es seit 2002 nicht mehr, alles wird über das Backbone in den USA geroutet
- ...

Technik

■ Hardwarebeispiel „Switch“

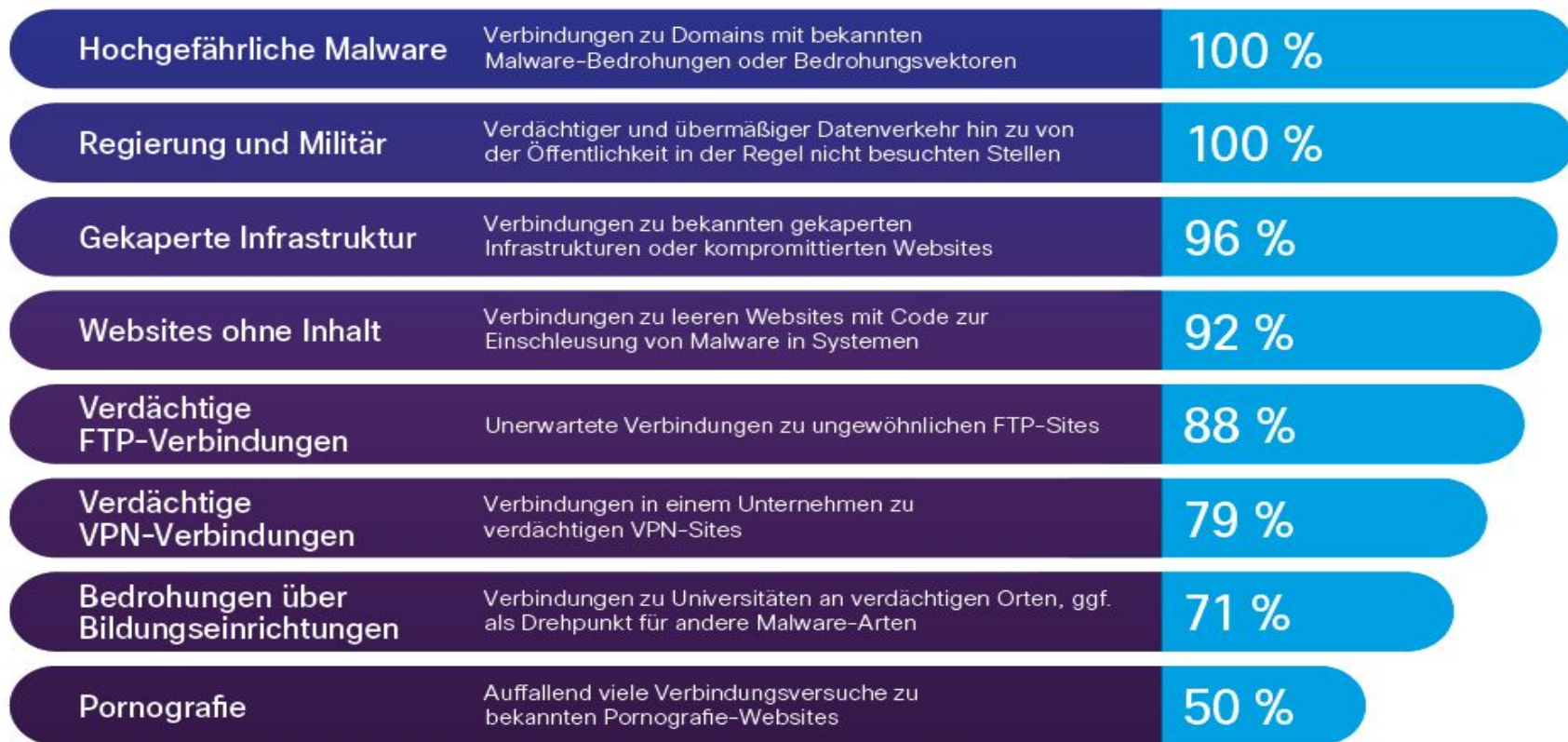
- 1:1 Datenleitungs-Umschalter, Aussen: Stern, Intern: Bus
- „Kleine“ Switch arbeiten auf der OSI Schicht 2 (nur Vermittlung)
- „Managbare“ Switch arbeiten auf der OSI Schicht 3 (Routingtabellen, Fragmentierung, Routing zwischen Netzen.. und können VLAN
- Softwareupdate erfolgt automatisch (i.d.R.), administrierbar über HTML
- Qualität:
 - Anschluss IP (Quelle und Ziel) muss „gemerkt“ werden (MAC-Adresse und Port #)
 - Datenpakete können zwischengespeichert werden, Latenzzeit speichernd
 - Datenpriorisierung
 - Schreiben Sie private E-Mails im Unternehmen?
 - Geschwindigkeitsbeispiel: Knoten in FFM DE-CIX 1,4 Tbit/s Datenvolumen im Jahr 2008.. arbeitet nicht analysierend..

Technik

■ Hardwarebeispiel „Switch“ (Cisco)

ABBILDUNG 27

Die Verbreitung von schädlichem Datenverkehr



Quelle: Cisco 2014 Annual Security Report

Technik

- Softwarebeispiel „IPv4 / IPv6“
- Protokoll des Paketversandes bzw. der Adressverwaltung
- Datenschutz bei „IPvx“ (Leitfaden) BSI (www.bsi.bund.de)
- IPv4
 - 4 294 967 296 Adressen, kein Sicherheitsprotokoll
- IPv6
 - $3,4 \cdot 10^{38}$ Adressen, Ipsec
- IPv6 Header

Version	Traffic Class	Flow Label		
Payload Length			Next Header	Hop Limit
Source Address				
Destination Address				

Quelle: Eigene Darstellung

Kommunikation

■ Vorratsdatenspeicherung

- EU Richtlinie 2006/24/EG verlangt die Speicherung aller Verbindungsdaten für mindestens sechs Monate und höchstens zwei Jahre
- Provider müssen speichern
- Speicherung aller Verkehrs- und Verbindungsdaten zur Identifizierung
- Speicherung des kompletten Umfeldes, wer, wann, mit wem, was, wo...
- Datenverwendung ohne Informationspflicht für die Benutzer
- ...

- EuGH kippt Vorratsdatenspeicherung, da nicht mit EU-Recht vereinbar
- Grundsatz der Verhältnismäßigkeit ist überschritten
- Datenspeicherung nicht im Unionsgebiet
- ...

Kommunikation

- **Beispiel „E-Mail“**

- E-Mail = Postkarte
- Klarnamen / Pseudonym in der Mail
- Mailgruppierungen zuordnen
- Private Inhalte in der Mail
- ...

- **Lösungsansätze**

- Nicht im lokalen Computer speichern
- Nach dem Versand löschen / schreddern
- Internetcafe ohne Videoaufzeichnung
- WLAN-Hotspot ohne Authentifizierung
- Einmal-Adressen (10minutemail.com, anonbox.net, privatdemail.net, trash-mail.com)
- Aber, Kommunikation – ja?

Kommunikation

- **Beispiel „Fahrzeugkommunikation“**
- Fest verbaute / aktivierte SIM-Karte im Fahrzeug
- Sporadisch
 - Km-Leistung, Serviceintervall, Serviceanforderung (Verschleisssteile), Daten des Fahrzeugs, Batteriespannung..
- Probleme
 - Fahrzeugdaten (Check-Control), Setup, Fehlerspeicher..
- Unfall
 - Standort (Lokalisierung), Fahrgeschwindigkeit, Unfallschwere, Fahrgestellnummer, Farbe, Modell..
- Heimanwendung: Passwortgeschützter Router eines grossen Providers...

Kommunikation

- Beispiel „Cookie“

- Zweck

- Textdatei die Daten der besuchten Site enthält, „Besuchsinfo“, zeitlich beschränkt archiviert inkl. Selbstlöschfunktion, keine direkte Zustimmung erforderlich

- Nutzen

- Kein erneutes Anmelden, Wiedererkennungseffekt..

- Aber..

- Protokolliertes Internetverhalten, Websites, Eingaben, Tastatur ...



Quelle: Wikipedia

Kommunikation

- **Beispiel „tägliches Leben“**
- **Einkaufen..**
 - Zahlen Sie mit der EC-Karte? Nutzen Sie Paypal? Verwenden Sie Payback?
- **Telefon**
 - Löschen Sie Anruflisten? – auch beim Provider?
- **RFID**
 - Warensortimente, Einkaufen...
- **Reisen**
 - Haben Sie eine Bahncard? Nehmen Sie den Accu aus dem Smartphone?
- **Nachrichten**
 - Twittern Sie? Nutzen Sie n-tv? Haben Sie einen Facebook-Account?

Kommunikation

- Beispiel „Anonym im Netz“
- Facebook-Account? Nutzen Sie Online-Banking?
- Welche IP-Adresse haben Sie? (who is..)
- Nutzen Sie Newsletter, auch HTML? Löschen Sie alle Log-Daten?
- Geben Sie Ihre Steuererklärung elektronisch ab / Elster? – erledigt dies Ihr Steuerberater?
- Googeln Sie?

Webprotokoll für unverschluselt@mandalka.name

Gesamtes Protokoll

[Web](#)
[Bilder](#)
[News](#)
[Produkte](#)
[Anzeigen](#)
[Video](#)
[Karten](#)
[Blogs](#)
[Bücher](#)

[Pausieren](#)
[Elemente entfernen](#)

Trends

Interessante Artikel

Lesezeichen

Heute

02:13 Gesucht nach ["wolfgang schäuble" cdu koffer mit schwarzgeld von waffenhändler](#) - 1 Ergebnis angezeigt
 ☆ [Lügen, fest verinnerlicht - Artikel - SPIEGEL WISSEN...](#) - [spiegel.de](#)
 02:12 Gesucht nach ["wolfgang schäuble" cdu koffer mit schwarzgeld von waffenhändler](#) - 1 Ergebnis angezeigt
 ☆ [CDU-AFFÄRE: Spender verzweifelt gesucht - Deutschland...](#) - [focus.de](#)
 02:11 Gesucht nach [verbotenes](#) - 2 Ergebnisse angezeigt
 ☆ [TP: Verbotenes in deutschen Netzen](#) - [heise.de](#)
 ☆ [Verbotenes oder indiziertes Medium – Wikipedia](#) - [wikipedia.org](#)
 02:10 Gesucht nach [verdächtiges](#) - 2 Ergebnisse angezeigt
 ☆ [Ist hier was verdächtiges zu sehen? - Trojaner-Board](#) - [trojaner-board.de](#)
 ☆ [Verdächtiges Verhalten und verdächtige Dateien – Sophos ...](#) - [sophos.de](#)
 02:09 Gesucht nach [wie kriege ich Hämorrhiden weg?](#) - 1 Ergebnis angezeigt
 ☆ [http://www.wer-weiss-was.de/theme49/article4127278.html](#)
 02:08 Gesucht nach [Sexualpraktik X oder Y](#) - 1 Ergebnis angezeigt
 ☆ [EROTIKWÄSCHE 2 x String Mieder Bauch weg sex y Po NEU...](#) - [ebay.de](#)
 02:07 Gesucht nach [Erziehungsberatung in Musterstadt](#) - 1 Ergebnis angezeigt
 ☆ [Musterantrag zur Kostenübernahme beim Jugendamt](#) - [kind-vater.de](#)
 02:06 Gesucht nach [vielleicht mein neuer Arbeitgeber](#) - 1 Ergebnis angezeigt
 ☆ [Kriegt mein neuer Chef mit, das ich früher oft krank machte?](#) - [talkteria.de](#)

Quelle: Google

Auswirkungen

■ Reaktionen..

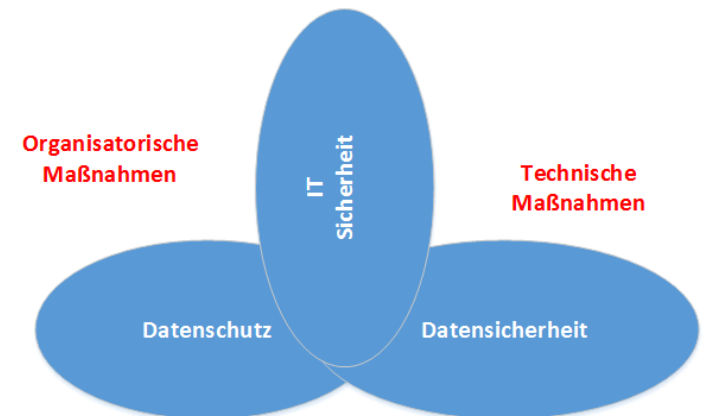
- Cloud Computing
- Dokumentaufbewahrung
- Fernsteuersoftware

■ Lösungen (?)

- BSI – Erstellung von Kryptokonzepten (Leitfaden) (www.bsi.bund.de)
- BSI – Sicheres Löschen magnetischer Datenträger (vgl. oben)
- Datenschutz (persönlich) und Datensicherheit (Daten)



Quelle: Intel



Quelle: Datenschutz in Österreich

Auswirkungen

- Beispiel „Passwortgenerator“
- KeyPassPasswort Safe
- Open Source Produkt (OSI Certified)
- Verschlüsselung komplett (SHA-256) mit 256 Bits
- Verschlüsselt auch das eigene Passwort und komplett alle Inhalte der Einträge
- Programm kann als Datei kopiert werden (PC, Smartphone, Tablet..)



Auswirkungen

- **Beispiel „Verschlüsselung, PGP“**
- Pretty Good Privacy
- Quelltext offen / nicht offen.. (McAfee)
- Privater Schlüssel & öffentlicher Schlüssel = Asymmetrisches Verfahren
- Signiert
 - Keine Manipulationen (Integrität), Absender-Sicher (Authentizität), es wird ein Hash-Wert erzeugt, der einem Fingerprint der Nachricht entspricht (SHA-256), hiervon wird mit dem Privaten Schlüssel eine Signatur erzeugt
- Verschlüsselt
 - Zusammenfassung des Klartextes und der Signatur, Komprimierung, verschlüsselung mit (einmal) Session-Key (dieser muss mit dem öffentlichen Schlüssel des Empfängers verschlüsselt ihm mitgeteilt werden), Wandlung des Textes in druckbare ASCII Zeichen.. Versand..

Auswirkungen

- **Fazit**
- **Wesentlich**
 - Alle Informationen seit 1969... sind offen, transparent, zugänglich
 - Anpassungen sind erfolgt, aber im Wesentlichen?
- **Können Sie „ohne?“**
 - Ohne Facebook? Ohne Google?
 - Ohne Werbung? Ohne Spam?
 - Ohne NSA?
- **Danke für Ihre Aufmerksamkeit ;-)**

