Sichere Kommunikation und Datenhaltung für Unternehmer

René 'Lynx' Pfeiffer

DeepSec GmbH
https://deepsec.net/, rpfeiffer@deepsec.net

Security Eye 2015
Dienstag, 22. September 2015
Grand Hotel Wien, Kärntner Ring 9, 1010 Wien.

DEEPSEC

Kommunikation und Daten

Vereinfachung

- Verzicht auf Diskussion aller *Cloud* Varianten
- Verzicht auf Wort *Cyber* (es heißt eigentlich *Technik*)
- Verzicht auf Produktpräsentationen – keine Happy Ends
- Fokus auf Internet
  - wenige Firmen können noch offline arbeiten
  - Löwenanteil der Kommunikation verwendet Internet

Schöne neue Digitale Welt

Reale Digitale Welt

Risikoanalyse

Why We Spy on Our Allies

The European Parliament's recent report on Echelon, written by British journalist Duncan Campbell, has sparked angry accusations from continental Europe that U.S. intelligence is stealing advanced technology from European companies so that we can – get this – give it to American companies and help them compete. My European friends, get real. True, in a handful of areas European technology surpasses American, but, to say this as gently as I can, the number of such areas is very, very, very small. Most European technology just isn't worth our stealing.
Why, then, have we spied on you? The answer is quite apparent from the Campbell report – in the discussion of the only two cases in which European companies have allegedly been targets of American secret intelligence collection. Of Thomson-CSF, the report says: „The company was alleged to have bribed members of the Brazilian government selection panel." Of Airbus, it says that we found that „Airbus agents were offering bribes to a Saudi official." These facts are inevitably left out of European press reports.

That's right, my continental friends, we have spied on you because you bribe. Your companies' products are often more costly, less technically advanced or both, than your American competitors'. As a result you bribe a lot. So complicit are your governments that in several European countries bribes still are tax-deductible.

R. James Woolsey, a Washington lawyer and a former Director of Central Intelligence

Publiziert: **The Wall Street Journal**, March 17, **2000**.

Why We Spy on Our Allies

The European Parliament's recent report on Echelon, written by British journalist Duncan Campbell, has sparked angry accusations from continental Europe that U.S. intelligence is stealing advanced technology from European companies so that we can – get this – give it to American companies and help them compete. My European friends, get real. True, in a handful of areas European technology surpasses American, but, to say this as gently as I can, the number of such areas is very, very, very small. Most European technology just isn't worth our stealing.

Why, then, have we spied on you? The answer is quite apparent from the Campbell report – in the discussion of the only two cases in which European companies have allegedly been targets of American secret intelligence collection. Of Thomson-CSF, the report says: „The company was alleged to have bribed members of the Brazilian government selection panel." Of Airbus, it says that we found that „Airbus agents were offering bribes to a Saudi official." These facts are inevitably left out of European press reports.

That's right, my continental friends, we have spied on you because you bribe. Your companies' products are often more costly, less technically advanced or both, than your American competitors'. As a result you bribe a lot. So complicit are your governments that in several European countries bribes still are tax-deductible.

R. James Woolsey, a Washington lawyer and a former Director of Central Intelligence

Publiziert: **The Wall Street Journal**, March 17, **2000**.

International Safe Harbor Privacy Principles

- EU Direktive 95/46/EC für Datenschutz (1995)

  Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
- Diskrepanz Datenschutz USA $\longleftrightarrow$ EU
- Safe-Harbor-Abkommen deklariert USA konform (2000)

  Entscheidung der EU Kommission, *kein Vertrag (!)*
- USA PATRIOT Act (2001)
- PRISM Programm der NSA (2005, seit 2013 bekannt)
- Safe-Harbor-Abkommen ist Waschzettel ohne Bedeutung

Anforderungen

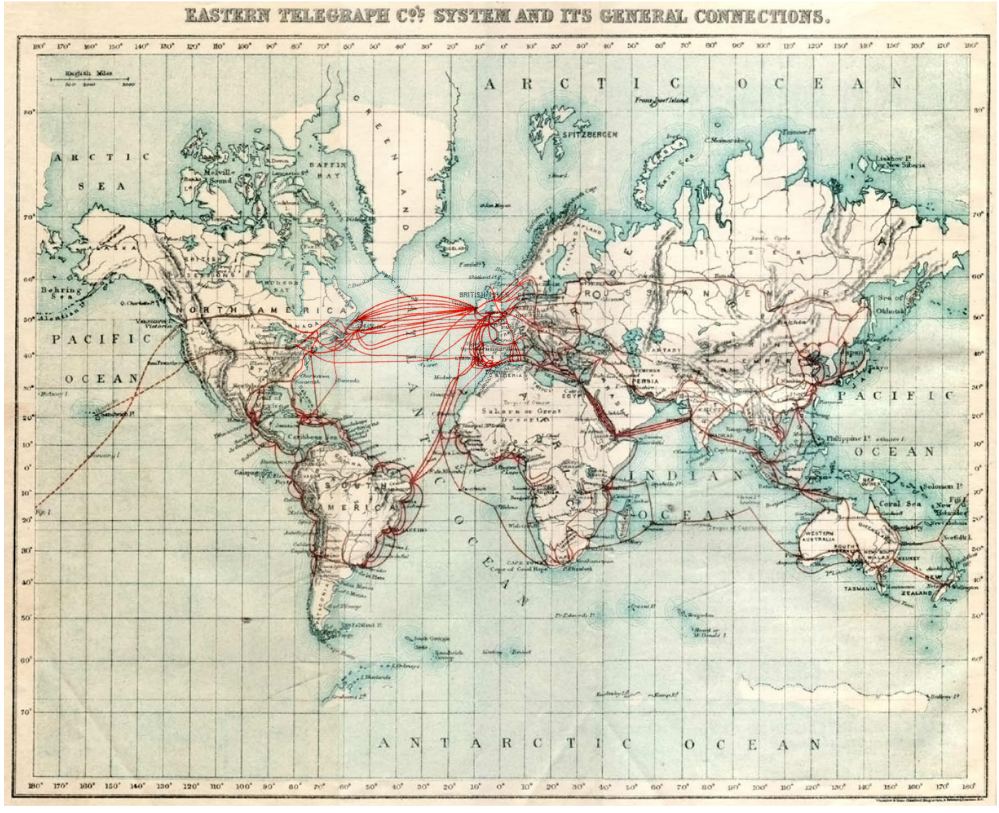
Klassische Ziele - C.I.A.

- *Vertraulichkeit / confidentiality*
- *Integrität / integrity*
- *Verfügbarkeit / availability*
- *Authentizität / authenticity*
- *Verbindlichkeit/Nichtabstreitbarkeit / non repudiation*
- *Zurechenbarkeit / accountability*
- *Anonymität / anonymity*
- *glaubhafte Abstreitbarkeit / plausible deniability*

Alltägliche Kommunikationsmittel

- Telefonie (*Festnetz*)
- Telefonie (*Festnetz*) $\longrightarrow$ POTS, Internet
- Mobilfunk (*Festnetz*, Mobilfunknetz)
- Mobilfunk (*Festnetz*, Mobilfunknetz) $\longrightarrow$ POTS, Internet
- E-Mail
- E-Mail $\longrightarrow$ Internet
- Messenger Apps
- Messenger Apps $\longrightarrow$ Internet

Typische Kommunikationswege



Typische Kommunikationswege

- kabelgebundene Übertragungen (Glasfaser, Land & See)
- Satelliten & Richtfunkstrecken
  - spielen untergeordnete Rolle
  - niedrigere Bandbreite
  - primär verwendet für schlecht erschlossene Gebiete
- Backbone des Internet ist kabelgebunden

Exkurs: Athen Affäre

- Ericsson entdeckt am 4. März 2005 trojanische Pferde im Lawful Interception Subsystem von Vodafone Greece.
- Kostas Tsalikidis, Leiter Network Design bei Vodafone Greece, erhängt sich am 9. März 2005.
- Vodafone deaktiviert Subsystem und löscht versehentlich alle Logs und Spuren.
- Software im Subsystem hörte Telefonate von über 100 Regierungsmitgliedern ab.
- Täter sind unbekannt.
- Lektüre: *The Athens Affair (IEEE Spectrum, Juli 2007)*

Exkurs: Belgacom

- Techniker entdecken Anomalien im Belgacom Netzwerk (Sommer 2012).
- Schadsoftware *Regin* auf Systemen wird entdeckt (Juni 2013).
- Attacke war hochspezialisiert auf Datendiebstahl.
- Spuren führen zum britischen GCHQ.
- Infektion begann 2010.
- GCHQ hat seit 2008 einen *Freibrief für illegale Operationen*.
- Lektüre: Operation Socialist, The Intercept

Crypto 101: Ende-zu-Ende Verschlüsselung

- Sender kennen Schlüssel der Empfänger
- Nur Empfänger können Nachrichten entschlüsseln
- Transportsystem kann nicht in Nachricht hineinschauen
- *Schlüsselmanagement notwendig!*
- *Identitätsprüfung notwendig!*
- PGP, GnuPG, S/MIME, bestimmte Messenger

Crypto Exkurs: De-Mail

- De-Mail - sicher, vertraulich und nachweisbar (?)
- Daten sind sogar *abschnittsweise verschlüsselt*!
- Ende-zu-Ende Verschlüsselung nicht implementiert
  - Empfehlung Nachrichten zusätzlich zu verschlüsseln
  - Ende-zu-Ende Verschlüsselung als Browser Add-Ons geplant
- gute Idee mit Fehlern im Design
- derzeit eigentlich keine Verbesserung

EFF Secure Messenger Scorecard

	Encrypted in transit?	Encrypted so the provider can't read it?	Can you verify contacts' identities?	Are past comms secure if your keys are stolen?	Is the code open to independent review?	Is security design properly documented?	Has there been any recent code audit?
Skype	✓	✗	✗	✗	✗	✗	✗
TextSecure	✓	✓	✓	✓	✓	✓	✓
Threema	✓	✓	✓	✓	✗	✓	✗
Viber	✓	✗	✗	✗	✗	✗	✗

Empfehlungen

Checkliste

- eigene Daten vollständig klassifizieren
- Transportwege für Datenklassen festlegen
- Verschlüsselung hinterfragen (lassen)
  - keine proprietären Lösungen
  - Algorithmen müssen offengelegt sein
  - Schlüssel muß/müssen bei Ihnen liegen - und nur dort!
- keine Hintertüren akzeptieren
- gewählte Lösungen periodisch Sicherheitstest unterziehen

Fragen?

Über die DeepSec

Die DeepSec GmbH veranstaltet seit 2007 jährlich im November die *DeepSec In-Depth Security Conference* in Wien. Die DeepSec bringt als neutrale Plattform die Sicherheitsexperten aus allen Bereichen zum Gedanken- und Erfahrungsaustausch zusammen. Dort erhalten IT- und Security-Unternehmen, Anwender, Behördenvertreter, Forscher und die Hacker-Community in über 42 Vorträgen und Workshops die Chance, sich über die aktuellen und zukünftigen Sicherheitsthemen auszutauschen. Die Konferenz möchte insbesondere dem verbreiteten Vorurteil entgegen wirken, dass Hacker zwangsläufig Kriminelle sind.

Über den Autor

René Pfeiffer ist selbstständiger Systemadministrator und Vortragender an der Fachhochschule Technikum Wien im Bereich Computer- und Datensicherheit. Mit über 15 Jahren Berufs- und 30 Jahren Computererfahrung sowie einem akademischen Hintergrund in theoretischer Physik verbindet er in Schulungen und Projekten erfolgreich Theorie und Praxis.

Seine Themenschwerpunkte liegen im Bereich IT Administration, Aufbau sicherer Infrastrukturen (Host-/Netzwerkbereich), sichere Kommunikation in Organisationen und Infrastruktur (VPN Technologien, Nachrichtensysteme), Wireless Security, technische Dokumentation, Betreuung von Forschungsarbeiten in der IT Security, technischem Auditing und Evaluierung von Software.

Herr Pfeiffer hält seit 2000 jährlich Fachvorträge und Schulungen auf Tagungen und Seminaren (Institute for International Research (I.I.R.), Business Circle, Confare, Linuxwochen Österreich, SAE Institute Wien, DeepSec In-Depth Security Conference, Bundesverband Sicherheitspolitik an Hochschulen, Kundenveranstaltungen).

Kontakt

- ℹ *https://deepsec.net/*
- ℹ *https://deepintel.net/*
- 🗲 *rpfeiffer@deepsec.net*
- 🗲 *deepsec@deepsec.net*
- +43.676.5626390 (Threema, TextSecure & RedPhone)
- Videos *http://www.vimeo.net/deepsec*
- *https://twitter.com/deepsec*

Quellenverzeichnis

- Bild (Cover) des Flottendienstboots A52 *Oste*, aufgenommen von KleeBuchemer.
- Wikipedia, Scrub Island Resort (British Virgin Islands).
- Wikipedia, USMC 1st Lt. Daniel Barbeau und Cpl. Vincent O'Brian.
- Wald in den schottischen Highlands, © 2013 René Pfeiffer.
- Wikipedia, historische Karte der Seekabel.
- Screenshot EFF Secure Messaging Scorecard
- Wikipedia, alte Telefonzelle in der Portobello Road, London.
- Wikipedia, Serie *Get Smart*, Schauspieler Don Adams.