Verschlüsselung heute

Christian Krause
Martin Rost
Kiel, 26.08.2014

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Gliederung

- Vertraulichkeitsschutz als normative Anforderung
- Sicherung der Vertraulichkeit als elementares operatives Schutzziel
- Einige systematische Überlegungen
- Angreifer, Motive, Möglichkeiten, Einschätzungen
- Konkretes

Zweck der Verschlüsselung

- Verschlüsselung ist eine Schutzmaßnahme zur Umsetzung des elementaren Schutzziels **Sicherung der Vertraulichkeit von Informationen**.
- Die Kenntnisnahme von Informationen soll nur dem vom Sender intendierten oder einem gesetzlich legitimierten Empfänger möglich sein. Alle anderen möglichen Empfänger gelten grundsätzlich als unbefugt.

Normative Regelung zur Sicherung der Vertraulichkeit im Grundgesetz

- Artikel 10 Grundgesetz
  - (1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.
  - (2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, daß sie dem Betroffenen nicht mitgeteilt wird und daß an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.

Normative Regelung

- Legaldefinition: § 88 Abs. 1 Telekommunikationsgesetz sowie § 206 Abs. 5 StGB.
- Operative Sicherung durch Datenschutzgesetze, die aus Artikel 1 und 2 GG abgeleitet sind.
- Einschränkungen:
  - Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses
  - § 100a, § 100b, § 100c, § 100g, § 100h und § 100i Strafprozessordnung.

Sicherung der Vertraulichkeit

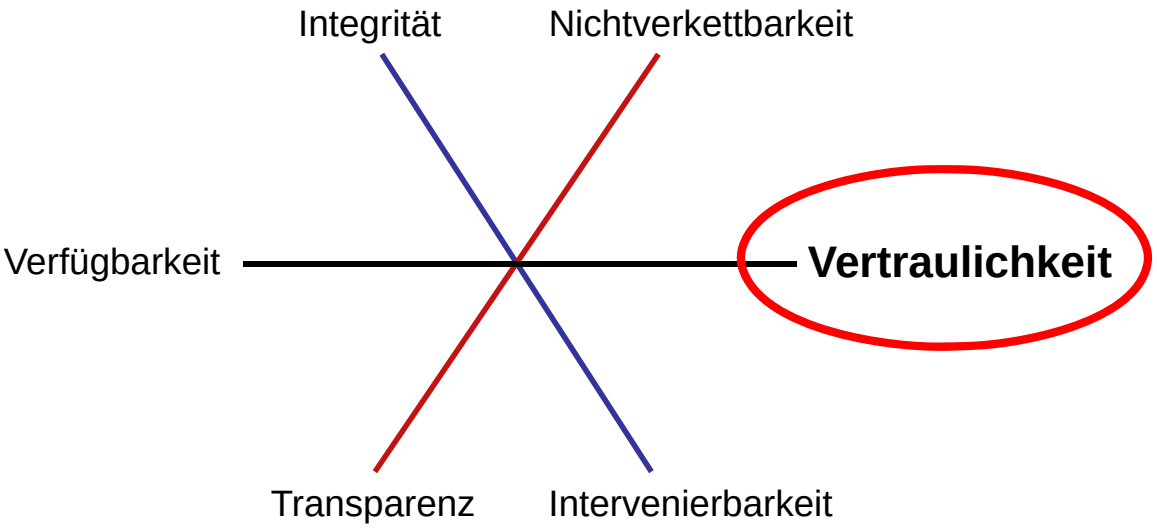
… muss erfolgen in Bezug auf

- **den Inhalt einer Information**
  (bspw. E-Mail, Dokument, Bild, Video, Audio)

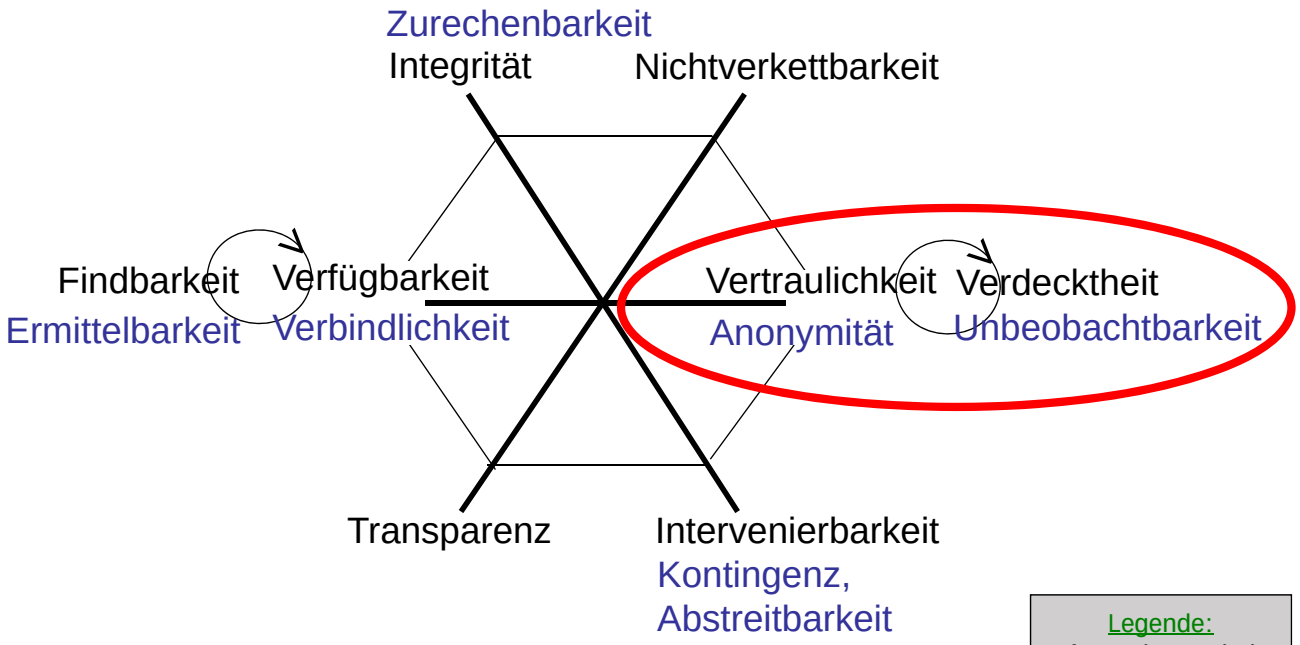
und

- **den Kontext einer Information**
  (beteiligte Personen einer Kommunikationsbeziehung).

Vertraulichkeit ist eines der sechs elementaren Schutzziele des modernen operativen Datenschutzes



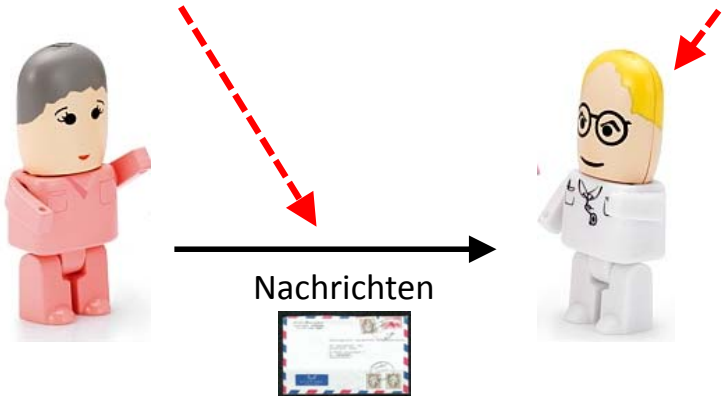
Schutzziele vollständiges Tableau



Zwei Angriffe auf Vertraulichkeit

Möglicher Angriff auf Vertraulichkeit der Beziehung Sender-Empfänger insbesondere durch IT und (IT-)Dienstleistungen

Möglicher Angriff auf den (gesetzlich garantierten) Zweckbindungsbedarf des Senders durch den Empfänger der Nachricht



Wer verschlüsselt, macht sich verdächtig

Deutschland: Ein Verschlüsselungsweltmeister?

News Newsticker 7-Tage-News Archiv Foren

Topthemen: Netzneutralität NSA TrueCrypt Windows 8.1 An

heise online > News > 2014 > KW 30 > Digitale Agenda der Bundesregierung: Deutschland

23.07.2014 08:21 « Vorige | Nächste »

Digitale Agenda der Bundesregierung: Deutschland als Verschlüsselungsweltmeister und Breitband-Land

vorlesen / MP3-Download

Die Bundesregierung will Deutschland zum "Verschlüsselungsstandort Nummer 1" machen und peilt eine "Datenordnungspolitik" an. Dies geht aus einem ins Netz entfleuchten Entwurf für die digitale Agenda hervor.

„Auch den Ausbau der Nutzung von Verfahren wie **De-Mail** nennt das Papier (…) in diesem Zusammenhang. Dabei kommt aber bislang keine durchgehende Verschlüsselung zum Tragen; Sicherheitsexperten warnen vor dem Einsatz der Technik."

„Das europäische Datenschutzrecht im digitalen Binnenmarkt möchte die Bundesregierung "rasch modernisieren und harmonisieren", um die Bürgerrechte zu stärken und der Bedeutung der **Privatsphäre als "entscheidendem wirtschaftlichen Standortfaktor"** gerecht zu werden. Wichtigster Schritt auf diesem Weg sei die Verabschiedung der umkämpften Datenschutz-Grundverordnung im nächsten Jahr.

Als Antwort auf die globale Vernetzung und die Enthüllungen über den Missbrauch personenbezogener Daten soll die Regierung führende Rolle auch bei der **Entwicklung darüber hinausgehender internationaler Datenschutzprinzipien** anstreben. Dazu ist etwa eine Arbeitsgruppe für den G7-Gipfel 2015 unter deutschem Vorsitz vorgesehen."

De-Mail bietet keine ernstzunehmende Verschlüsselung

Bremen Verwaltung online DIE LANDESBEAUFTRAGTE FÜR DATENSCHUTZ

AKTUELLES | WIR ÜBER UNS | DATENSCHUTZTIPPS | PUBLIKATIONEN

Orientierungshilfen und Handlungshilfen • Entschließungen und Beschlüsse • Jahresberichte

Weitere Veröffentlichungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Publikationen ▸ Entschließungen und Beschlüsse ▸ Konferenzentschließungen ▸

86. Konferenz: Enschließung: Sichere elektronische Kommunikation gewährleisten

ENTSCHLIESSUNG: SICHERE ELEKTRONISCHE KOMMUNIKATION GEWÄHRLEISTEN - ENDE-ZU-ENDE-VERSCHLÜSSELUNG EINSETZEN UND WEITERENTWICKELN

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 01. und 02. Oktober in Bremen

ZEIT ONLINE | DATENSCHUTZ

START POLITIK WIRTSCHAFT GESELLSCHAFT KULTUR WISSEN DIGITAL STUDIUM KARRIERE RI

Start › Digital › Datenschutz › De-Mail: Chaos Computer Club kritisiert Trickserei der Regierung

DE-MAIL

Chaos Computer Club kritisiert Trickserei der Regierung

Die Verschlüsselung der De-Mail sei unzureichend, sagen Kritiker. Statt der Technik will die Bundesregierung aber nur ihre Definition von "sicher" anpassen. VON PATRICK BEUTH

20. März 2013 12:46 Uhr 27 Kommentare

Die De-Mail, das Verfahren für die rechtsverbindliche elektronische Korrespondenz zwischen Bürgern und Behörden, ist so sicher wie eine Postkarte, sagen ihre Kritiker. Die Bundesregierung aber will dieses Problem nicht lösen, sie will es mit einem Gesetz für gelöst erklären.

Funktioniert Verschlüsselung technisch noch?


heise Security

heise Security Twitter heise Security Face

News Hintergrund Erste Hilfe

Security › News › 7-Tage-News › 2014 › KW 16 › Zugriff auf SMS-Nachrichten und Tor-Traffic dank

17.04.2014 15:55 « Vorige | Nächste »

Zugriff auf SMS-Nachrichten und Tor-Traffic dank Heartbleed

vorlesen / MP3-Download

Hackern ist es gelungen, die von SMS-Gateways verschickten Nachrichten auszulesen – Tokens zur Zwei-Faktor-Authentisierung inklusive. Und auch Tor-Exitnodes geben beliebige Speicherinhalte preis.


SPIEGEL ONLINE POLITIK

Login | Registrierung

Politik | Wirtschaft | Panorama | Sport | Kultur | Netzwelt | Wissenschaft | Gesundheit | einestages | Karriere | Uni | Schule | Reise | Auto

Nachrichten > Politik > Ausland > National Security Agency (NSA) > NSA und britischer Geheimdienst knacken systematisch Verschlüsselung

Neue Snowden-Enthüllungen: NSA knackt systematisch Verschlüsselung im Internet

Sicher ist nicht mehr sicher: Die US-amerikanischen und britischen Geheimdienste arbeiten mit Hochdruck an der Dechiffrierung von Daten, auf deren Verschlüsselung sich Millionen Internetnutzer verlassen. Das zeigen neue Geheimdokumente.

Freitag, 06.09.2013 – 00:41 Uhr

Teilen Empfehlen 3.346 Twittern 360 +1


THEMEN

Sicherheitsmaßnahmen (55)

IT-Strategie (51)

News & Trends (51)

Angriffsarten (36)

Cyberkriminalität (29)

mehr...

Schirmherrschaft: Bundesministerium des Innern


Neues aus der Kryptologie

RSA unsicher?

„RSA teilweise geknackt"; „Online Sicherheit im Web nicht mehr gewährleistet". Solche und andere Schlagzeilen sind seit Februar dieses Jahres in den Medien zu finden. Was ist passiert? Ist die Kommunikation im Internet wirklich nicht mehr sicher?

Die sichere Kommunikation im Internet, die Basis vieler Geschäftsmodelle, wird sehr oft durch Verschlüsselung mit dem RSA-Verfahren erreicht. RSA steht für die Namen der Erfinder dieses Verfahrens: Ron Rivest, Adi Shamir und Leonard


heise Security

News Hintergrund Erste Hilfe

Security › Hintergrund › Truecrypt ist unsicher - und jetzt?

KOMMENTAR: Truecrypt ist unsicher - und jetzt?

Jürgen Schmidt - 30.05.2014

Sollten wir jetzt wirklich alle auf Bitlocker umsteigen, wie es die Truecrypt-Entwickler vorschlagen? Einen echten Nachfolger wird es jedenfalls so bald nicht geben - und daran sind nicht zu letzt auch die Truecrypt-Entwickler schuld.

Wirksamkeit einer Verchlüsselung ist abhängig von

(1) der **wissenschaftlich anerkannten Begründung** eines Verfahrens für einen Algorithmus (Stichworte: „Primfaktorenzerlegung, Quantenverschränkung";

(2) der **Fehlerfreiheit der technischen Implementation** des wissenschaftlich anerkannten Algorithmus in Compiler und Applikation (Stichwort: RSA, aber auch: „Ritchie's back door", „schlechter Zufallsgenerator",);

(3) der **Fehlerfreiheit der Konfiguration und des Betriebs** der Programme auf einem angemessenen Sicherheitsniveau, insbesondere beim Erzeugen, Verwalten, Verbreiten und Zurückziehen von geheimen Schlüsseln (Stichwort: „PKI-Infrastruktur", „web-of-trust", „man-in-the-middle-attack").

Die Wirksamkeit des Schutzes ist auch abhängig von

(4) den **Motiven** eines Angreifers;

(5) der (angenommenen) **Stärke eines Angreifers** (know how, Rechen- und Speicherleistung, Geld, Zeit);

(6) der **Gelegenheit**, Zugriff auf Daten nehmen zu können;

(7) der **Fähigkeit des Rechtsstaats**, Verstöße zu ermitteln und ggfs. zu sanktionieren;

(8) der **Kompetenz der Anwender** im Umgang mit Software, Passworten und Sicherheitstoken.

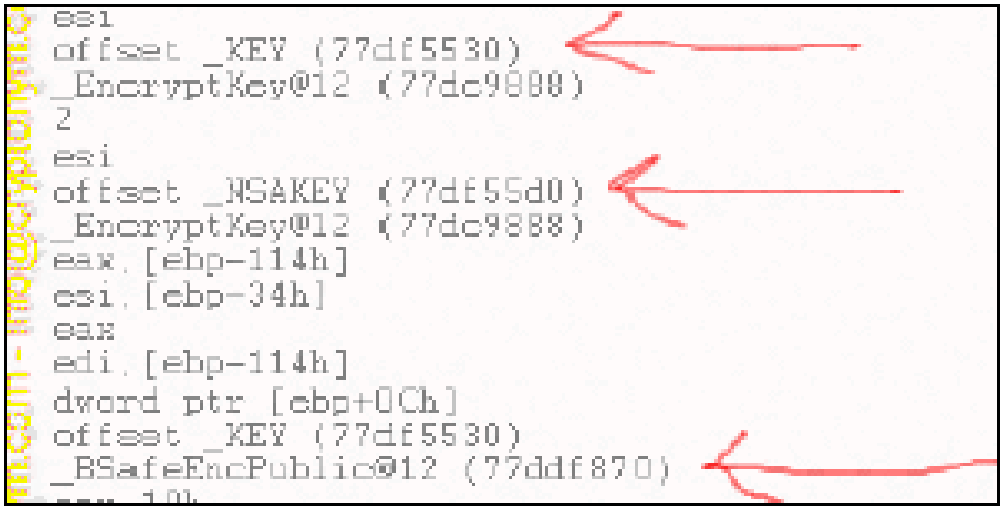
Bekannte Applikationen und Techniken der Vertraulichkeitssicherung

- **PGP/ GnuPG**:
  Verschlüsselung von E-Mail und einzelnen Dateien
- **Truecrypt** / Bitlocker
  Verschlüsselung von Festplatten oder Partitionen
- **WPA2 / VPN / SSL / TLS**:
  Verschlüsselung von Kommunikationsverbindungen zwischen Server und Client
- **TOR / JondoFox**: Sichern der Vertraulichkeit von Kommunikationsbeziehungen (Anonymisierung)
- **F5**: Verstecken einer Nachricht in einer Nachricht.

Dual_EC_DRBG: Ein eleganter Angriff

Dual Elliptic Curve Deterministic Random Bit Generator

- Algorithmen zur Verschlüsselung basieren auf der Verwendung von Zufallszahlen.
- Wenn diese Zahlen nicht zufällig sind, werden alle darauf basierenden Algorithmen angreifbar.
- Die Schwäche von Dual_EC_DRBG war seit 2007 bekannt.
- Für Entwickler und Nutzer einer API ist nicht ersichtlich, welcher Algorithmus im Hintergrund zum Einsatz kommt.



Das war 1999.
Bis heute ist nicht klar, was das *wirklich* ist.

Ist OpenSource die Lösung?

Fünf Typen von Angreifern auf Vertraulichkeit

1. Freunde, Verwandte, Nachbarn, Kollegen, Script-Kiddies, Kriminelle
2. Organisationen, die Informationen erheben und verarbeiten
   - Staatliche Exekutive
   - Arbeitgeber
   - Privatunternehmen, national und international
   - Wissenschaft und Forschung
   - Akademische Beratungsdienstleistungen (Ärzte, Rechtsanwälte)
3. Organisationen, die Informationen technisch vermitteln oder die Strukturen hierfür bereitstellen
   - IT-Dienstleister (Access- und Contentprovider, Cloudbetreiber)
   - Hardware und Software-Hersteller von zentralen IT-Komponenten
4. Organisationen, die unmittelbar personenbezogene Informationen nicht nur erheben und verarbeiten, sondern damit auch handeln
   - Nachrichtenbrooker, Scoring
5. Staatliche Nachrichtendienste (national, international)

Angreifer: Motive, Möglichkeiten, Schutz

Angreifer	Interesse an Daten	Technische Möglichkeiten	Prüfbarkeit / Sanktionierbarkeit	Welche Verschlüsselungsapplikation oder -technik schützt Betroffene?
Freunde, Nachbarn, Kollegen, ScriptKiddies	▬▬	▬	✓	PGP, 7Zip- & Office-Verschlüsselung, Jondos, F5, WPA, TLS, VPN
Im gewerblichen Umfeld: Firmen-Konkurrenz	▬▬	▬▬	✓ (im Inland)	PGP, 7Zip- & Office-Verschlüsselung, Jondos, F5, WPA, TLS, VPN
Arbeitgeber und dessen IT	▬▬	▬▬	✓	Keine, da IT nicht vom Nutzer kontrolliert wird
IT-Dienstleister, Provider, Cloud-Betreiber	▬	▬▬	schwierig	PGP, 7Zip- & Office-Verschlüsselung, F5
Social Web	▬▬	▬▬	schwierig	keine, wenn Verschlüsselung nicht auf eigenem PC
IT-Hersteller zentraler Komponenten (Compiler, Libraries, Betriebssystem)	▬	▬▬	✗	keine
Nachrichtendienste (ND)	▬▬	▬▬	✗	keine

Wesentliche Ergebnisse

- Angreifer haben
  - unterschiedliche Motive,
  - unterschiedliche Möglichkeiten für Angriffe und
  - unterliegen einer unterschiedlichen Kontrollier- und Sanktionierbarkeit.
- Schutz vor Nachrichtendiensten ist unmöglich, weil sie sich neben eigenen Angriffsmöglichkeiten Zugriff auch auf Daten aller anderen Organisationen verschaffen können (letztlich wg. Gewaltmonopol des Staates). Zudem können sich der Kontrolle durch Judikative und Legislative entziehen.
- Schutz vor den Herstellern von IT ist unmöglich.
- Der mögliche Schutz durch Technikapplikationen umfasst nur einen relativen kleinen Angreiferkreis

Pearl Index für Verschlüsselung

- **Kondom: 0.6! (theoretisch)**
  - **Oder 2?**
  - **Oder 8?**
  - **Maximal 15!**
    (real, durch Anwenderfehler)
- **Somit heißt es:**
  Trotz allem Verschlüsseln!

E-Mail-Verschlüsselung

- PGP / GPG bieten:
  - die Sicherung von Vertraulichkeit und Integrität
  - sind geeignet für regelmäßige verschlüsselte Kommunikation
  - Flexibilität bei sich ändernden Adressatenkreisen
- Was PGP / GPG **nicht** bietet:
  - Leichte Nutzbarkeit
    - (Schon gar nicht auf verschiedenen Endgeräten)
  - Perfect Forward Secrecy

E-Mail-Verschlüsselung

- **Mailvelope**
  - Probleme:
    - Implementierung
    - Schlüsselverwaltung
    - Privater Schlüssel auf mehreren Endgeräten

- **Smartphones und Tablets**
  - Intransparente Systeme
  - Geringe Konfigurationsmöglichkeiten
  - keine App, keine Verschlüsselung

Verzeichnis-Verschlüsselung
TrueCrypt or not TrueCrypt: *That is the question!*

- TrueCrypt wurde von seinen Entwicklern offiziell aufgegeben.
- Eben diese Entwickler raten vom Einsatz ab und raten zur Nutzung von Microsoft Bitlocker.

  - Bislang ist keine Sicherheitslücke in TrueCrypt bekannt.
  - Ein erstes Code-Review hat keine Schwachstellen aufgezeigt.
  - Bitlocker als Closed Source-Software kann bislang kein Code-Review vorweisen…

Cloud?

Verschlüsselung in der Cloud

- Bitte: Nur mit Containerverschlüsselung! (bspw. BoxCryptor oder TrueCrypt)
- Aber: Containerverschlüsselung torpediert sowohl Geschäftsmodell als auch Zusatzdienste von Cloud-Anbietern.

Verbindungsverschlüsselung

- Verbindungsverschlüsselung basiert auf Zertifikaten, also einer Vertrauensstruktur.
- Zertifikatsaussteller bzw. signierende Instanzen sind nicht per se vertrauenswürdig
- Lösungen?
  - Wenn irgend möglich, andere Zertifikate nutzen, als diejenigen, die standardmäßig dabei sind.
  - Künftige Entwicklungen, die Vertrauen in CAs obsolet machen, bspw. DANE

Passworte?

- Passworte schützen prinzipiell nie vor dem Betreiber oder Hersteller der IT

- Zwei Faktor-Authentifizierung WO IMMER ES GEHT!
  - GAuth
  - YubiKey

Vertraulichkeit der Kommunikationsbeziehung

- Anonymisierungsdienste wie JondoFox und TOR nutzen!

  „Man will trotz der sicherheitsrelevanten Bugs in Firefox aber trotzdem bei dem Browser bleiben, da es keine Alternative gebe, bei der sich die Privatsphäre-Funktionen des Tor-Bundles einfacher und sicherer umsetzen ließen.“

  (http://www.heise.de/newsticker/meldung/Haertung-des-Tor-Browsers-steht-und-faellt-mit-Firefox-Bugs-2299773.html (Meldung vom 21.08.2014))

Vertraulichkeit der Kommunikationsbeziehung

- Aber: Anonymisierungsdienste schützen in der Praxis nur vor dem Beobachten der Kommunikationsbeziehung an sich.
- Eine vollständige Anonymisierung gegenüber dem Webserver ist schwer zu realisieren:
  - Der vollständige Verzicht auf aktive Inhalte und sonstige Browsererweiterungem (Java, JavaScript, Silverlight, Flash sowie alle AddOns) macht viele Webseiten unbenutzbar.
  - Sinnvolle Alternative: Live-CDs

ULD www.datenschutzzentrum.de

Vielen Dank für Ihre Aufmerksamkeit

Martin Rost
ULD32@datenschutzzentrum.de
0431 9881391
Holstenstraße 98, 24103 Kiel

Christian Krause
ULD38@datenschutzzentrum.de
0431 9881247
Holstenstraße 98, 24103 Kiel