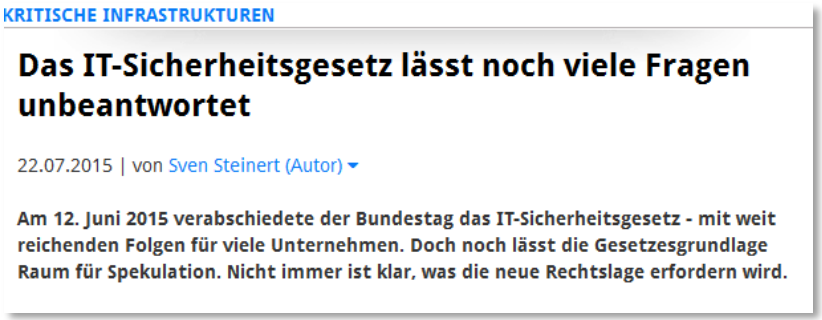
ALLES KRITIS(CH) ODER WAS?

OFFENE FRAGEN UND PRAKTISCHE HERAUSFORDERUNGEN VOR UND NEBEN DEM ITSIG

Dr. Guido Brinkel
Head of Public Affairs
1&1 Internet SE
twitter.com/guidobrinkel

| Das ITSiG ist da – und jetzt…?


KRITISCHE INFRASTRUKTUREN

Das IT-Sicherheitsgesetz lässt noch viele Fragen unbeantwortet

22.07.2015 | von Sven Steinert (Autor)

Am 12. Juni 2015 verabschiedete der Bundestag das IT-Sicherheitsgesetz - mit weit reichenden Folgen für viele Unternehmen. Doch noch lässt die Gesetzesgrundlage Raum für Spekulation. Nicht immer ist klar, was die neue Rechtslage erfordern wird.


DVZ Logistik & Verlader

Rubriken Themen Die Zeitung Abos Veranstaltungen Karriere Shop

Startseite > Rubriken > Logistik & Verlader > IT-Sicherheitsgesetz verunsichert Logistiker

IT-Sicherheitsgesetz verunsichert Logistiker


News Newsticker 7-Tage-News Archiv Foren

Topthemen: Windows 10 IDF Android iPhone 6s Apple IFA 2015

heise online > News > 2015 > KW 17 > Geplantes IT-Sicherheitsgesetz lässt Fragen offen

« Vorige | Nächste »

Geplantes IT-Sicherheitsgesetz lässt Fragen offen

heise online 20.04.2015 19:35 Uhr – Stefan Krempl vorlesen


eco Datacenter Expert Group

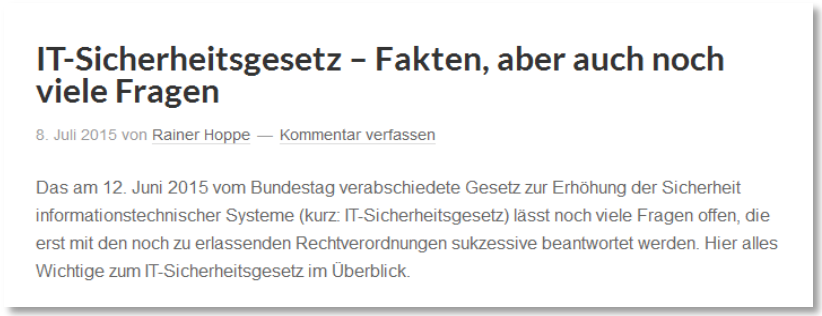
Aktuell Rückblicke Köpfe Termine Ziele Kontakt

Köln | 10.09.2015

Sind wir eine Kritische Infrastruktur?

Housing, Hosting und IT-Sicherheitsgesetz

Am 12. Juni 2015 hat der Deutsche Bundestag das sogenannte „IT-Sicherheitsgesetz" beschlossen. Mit der Veröffentlichung des Gesetzestextes trat das IT-Sicherheitsgesetz am Samstag, den 25. Juli 2015 in Kraft.


IT-Sicherheitsgesetz – Fakten, aber auch noch viele Fragen

8. Juli 2015 von Rainer Hoppe — Kommentar verfassen

Das am 12. Juni 2015 vom Bundestag verabschiedete Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (kurz: IT-Sicherheitsgesetz) lässt noch viele Fragen offen, die erst mit den noch zu erlassenden Rechtverordnungen sukzessive beantwortet werden. Hier alles Wichtige zum IT-Sicherheitsgesetz im Überblick.


Start > Online > Web

Freitag, 28. August 2015

Gesetzliche Pflicht zum Schutz von personenbezogenen Daten

IT-Sicherheitsgesetz: Das müssen Webseitenbetreiber wissen

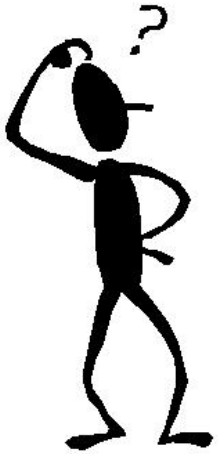
Andreas Dölker, 2 Wochen online Kommentare

Baustellen aus Praxissicht – der Anwendungsbereich

Der Anwendungsbereich nach dem Gesetzestext:

➔ Einrichtungen, Anlagen oder Teile davon
➔ IKT: Sprach- und Datenkommunikation & Speicherung von Daten
➔ Hohe Bedeutung für das **Funktionieren des Gemeinwesens**

- bei Ausfall oder Beeinträchtigung…
  - …erhebliche **Versorgungsengpässe**
  - …oder Gefährdungen der **öffentl. Sicherheit**
- ab bestimmten **Versorgungsgrad** (branchenspezifisch)



Hä?

Die Gretchenfrage:
Wer ist KRITIS(CH)?

Baustellen aus Praxissicht – der Anwendungsbereich

Die KRITIS-VO | Was wissen wir (nicht)?

Sprach- und Datenübertragung

Datenspeicherung und –verarbeitung

- IKT nimmt gewisse Sonderstellung ein, aufgrund der **Interpendenzen zu anderen KRITIS-Sektoren**.
- Versorgungsgrad-Bezug bedeutet praktisch, dass v.a. **(End-)Kundenzahlen** als Kriterium relevant werden.
- Für Transportdienstleistungen wird hohe Bedeutung für Gemeinwesen faktisch unterstellt – gleichzeitig Folgefragen aufgrund **Bereichsausnahmen für Telekommunikationsdienste**

- **Fokus auf physische Infrastrukturen**, z.B. Zugangs- und Backbone-Netzbetrieb, Vermittlung (PoP, IXS), Rootserver, Signalisierung, Domain Name System
- „Datenübertragung“ wird offenbar generisch als **Transportleistung** verstanden, gemeint ist mithin nicht jeder Dienst, der auch Daten überträgt.
- **„Sprachübertragung“** daher wohl auf alte PSTN-Welt bezogen.
- Somit faktisch: Alle Komponenten technischen Netzbetriebs, jedoch **nicht Dienste-Ebene?**
- **Verhältnis zum TKG** bzw. Reichweite der Bereichsausnahmen im ITSiG?

- Ebenfalls Fokus auf physische Infrastrukturen | Anwendungsbereich: **RZ-Betrieb (Housing) & Hosting**?
- Hosting: Generelle Kritikalitätsannahme oder in **Abhängigkeit von gehosteten Diensten**?
- Woran bemisst sich **Kritikalität** – woran sollen „Schwellenwerte“ ansetzen?
- Differenzierung nach ***Eigenbetrieb oder Service für Dritte?***

Baustellen aus Praxissicht – der Anwendungsbereich

Die KRITIS-VO | Was wissen wir (nicht)?

Sprach- und Datenübertragung

Datenspeicherung und –verarbeitung

E-Mail?

VoIP?

Cloudbasierte Services?

Freie WLAN-Netze?

Social Media?

TK-Resale?

Messaging

Baustellen aus Praxissicht – der Anwendungsbereich

Die KRITIS-VO | Was wissen wir (nicht)?

Sprach- und Datenübertragung

Datenspeicherung und –verarbeitung

- Perspektive: Ausgehend von Infrastruktur oder vom Dienst?
- Generell: Unklare Rolle der Dienste-Ebene.
- Maßstab für Bestimmung des Versorgungsgrades.

| Baustellen aus Praxissicht – Telemedien & das ITSiG

„(7) **Diensteanbieter** haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für **geschäftsmäßig angebotene Telemedien** durch technische und organisatorische Vorkehrungen sicherzustellen, dass…

….**kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und**

diese a) **gegen Verletzungen des Schutzes personenbezogener Daten** und b) **gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind**, gesichert sind.

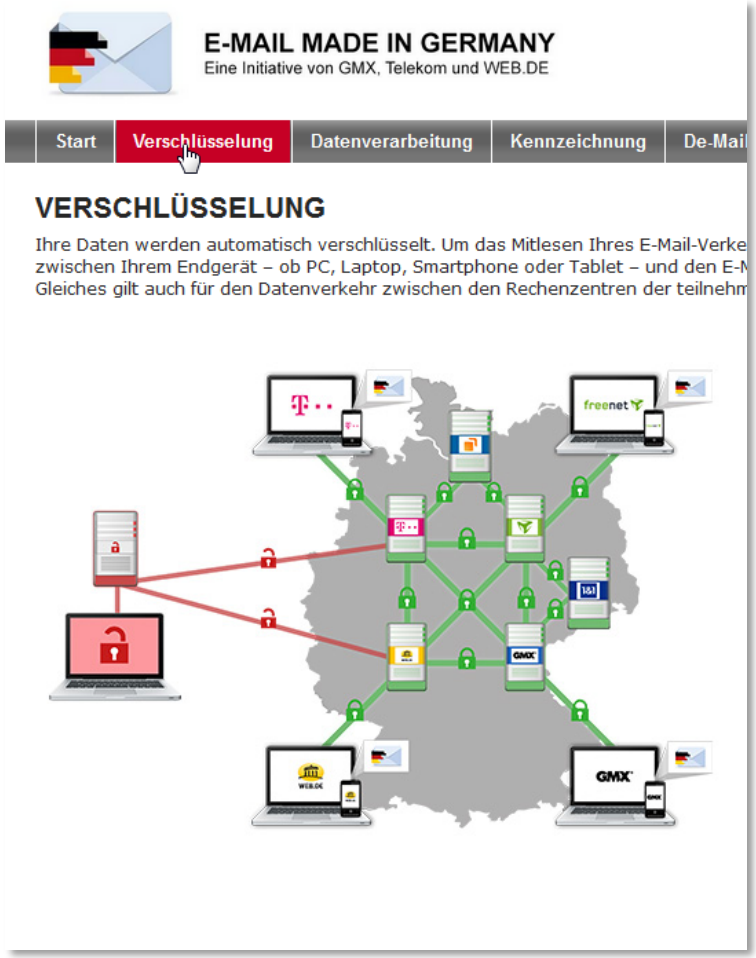
Maßstab: Stand der Technik
„Verschlüsselung“ als Regelbeispiel
Kein Konnex zu kritischen Infrastrukturen

| Baustellen aus Praxissicht – Telemedien & das ITSiG

Zielsetzung der Regelung	mögliche Maßnahmen
➔Hauptverbreitungswege von Schadsoftware eindämmen. ➔Insbesondere drive by downloads	➔Einspielen von Sicherheitspatches ➔Vertragliche Absicherungen im Verhältnis zu Werbedienstleistern ➔Verschlüsselungs- und Authentifizierungsmethoden (bei personalisierten Telemedien)

- Drive by downloads nur auf eigenen Diensten verhindern?
- Was ist ein „personalisierter Telemediendienst“ ?
- Verschlüsselung – was ist gemeint? https:// ? PGP/S-MIME? Verschlüsselung der Datensätze auf dem Server?
- Mindeststandards, Updatepflicht oder flexibles System?
- Enforcement / abmahnfähige Pflichten (Marktverhaltensregeln)?

| Baustellen aus Praxissicht – Telemedien & das ITSiG



| Das ITSiG ist da – und sonst so?

IT-Sicherheit im Consumer-Bereich am Beispiel WEB.de & GMX Ende-zu-Ende Verschlüsselung

| where we come from…

…letztes Jahr im NSA-Ausschuss….

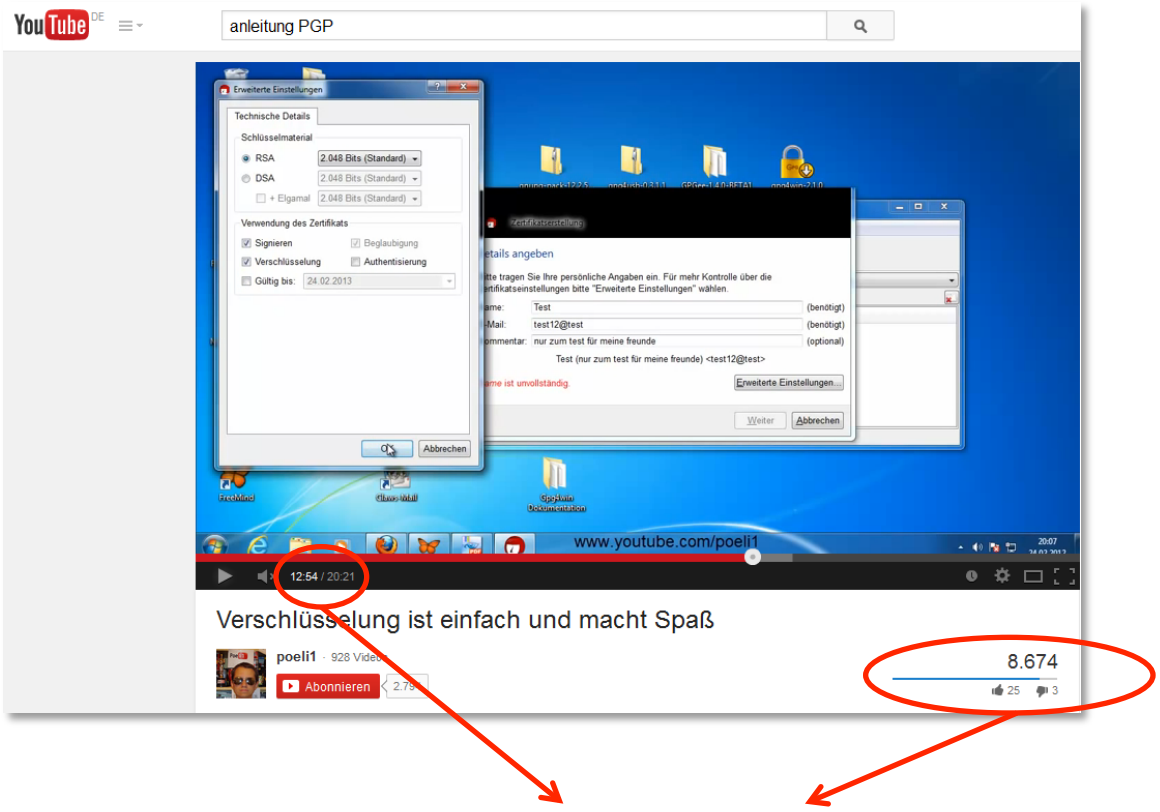
Michael Waidner, Chair Fraunhofer SIT

Sandro Gaycken Institute of Computer Science der FU-Berlin

„Derzeit ist Verschlüsselungstechnik für den normalen Nutzer furchtbar kompliziert und die Anwendung für den Laien kaum zu durchschauen“

„Flächendeckende Ende-zu-Ende-Verschlüsselung ist ein ebenso wichtiger Aspekt der Grundversorgung einer digitalen Gesellschaft wie der Breitbandausbau".

reality check…



20 Minuten 8000 Abrufe

„Derzeit ist Verschlüsselungstechnik für den normalen Nutzer furchtbar kompliziert und die Anwendung für den Laien kaum zu durchschauen“

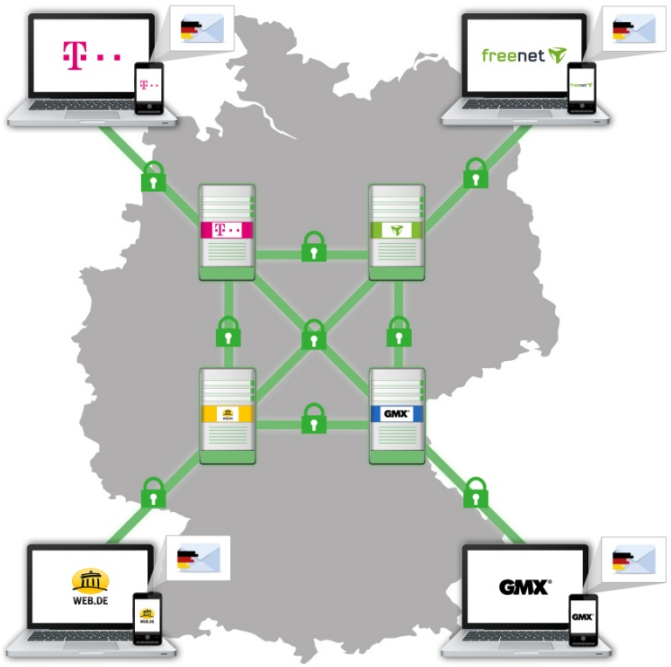
Sandro Gaycken
Institute of Computer Science der FU-Berlin

Das Problem heißt

Massenkompatibilität!

Zwei Schritte für mehr Akzeptanz von Verschlüsselung…

2013: Transportverschlüsselung via EmiG



2015: Integrierte Ende-zu-Ende-Verschlüsselung

20 Aug

So geht's: Verschlüsselte E-Mails versenden

Veröffentlicht am 20. August 2015

GMX Nutzer richten PGP ab sofort mit nur wenigen Klicks ein (Bild: Larry Washburn/fstop/Corbis)

Startschuss für Ende-zu-Ende Verschlüsselung aller Mail-Angebote: WEB.DE und GMX haben heute ihr neues, stark vereinfachtes Verschlüsselungsverfahren auf Basis des weltweit anerkannten Standards „Pretty Good Privacy" (PGP) für alle ihre Mail-Angebote live geschaltet. Damit ist es für Nutzer möglich, ganz einfach ohne Vorkenntnisse vertrauliche Nachrichten und Dokumente durchgängig vor Zugriffen Dritter zu schützen.

PGP nutzt das sogenannte Public-Key-Verfahren. Dabei gibt es für jeden Nutzer ein eindeutig zugeordnetes Schlüsselpaar: Den …lichen und den privaten Schlüssel. E-Mails …hlüssel codiert und können dann mithilfe …ost entschlüsselt werden, wenn er den …ng erfordert nur einige Mausklicks und ist

WEB.DE Newsroom

Newsroom | Mail | Cloud | Mobile | Sicherheit | De-Mail | Pre

WEB.DE > Newsroom > Verschlüsselung voranbringen

Verschlüsselung voranbringen

WEB.DE und GMX haben PGP in ihre E-Mail-Produkte integriert. Damit können die über 30 Millionen Nutzer der beiden Dienste ihre Mails mit einer Profi-Technologie durchgängig verschlüsseln – auch mobil. Jan Oetjen, Geschäftsführer von GMX und WEB.DE, spricht im Interview über die Hintergründe.

21. August 2015 von Martin Wilhelm

WEB.DE und GMX Geschäftsführer Jan Oetjen im Interview: "Unsere Lösung ist PGP in seiner ursprünglichen Form, ohne Verwässerung der Sicherheit, aber mit maximalem Komfort." © WEB.DE

Warum Ende-zu-Ende-Verschlüsselung?

- Global zunehmende Überwachung
- Gesteigerte Sensibilität für Privatsphäre
- Wunsch nach Vertraulichkeit
- Ergänzung zu E-Mail made in Germany
- Ergänzung zu De-Mail

Ende-zu-Ende Verschlüsselung bei WEB.DE & GMX

PGP & E-Mail made in Germany

E-Mail ohne EmiG

Vertraulichkeit der Inhalte nicht sichergestellt:

„Inhalte sind bei Missbrauch wie auf einer Postkarte für jeden einsehbar“

- Verschlüsselte Verbindungswege zwischen den Anbietern können nicht garantiert werden
- Datenschutzbestimmung des Anbieters/ im Ausland?
- Unautorisierter Zugriff staatlicher Behörden?
- Filterung von E-Mails z.B. zu Werbezwecken durch den Anbieter?

E-Mail mit EmiG

Sicherheitsversprechen für die Übermittlung von Nachrichten und Schutz der Daten:

„Brief mit geschützter Transport-verbindung ab und bis zum Postfach – jedoch ohne E2E“

- Sicherheit für die Kommunikation im E-Mail made in Germany-Verbund für ca. 70% der E-Mail-Postfächer in Deutschland
- TLS-Verschlüsselung der Verbindungswege
- Serverstandorte und Speicherung ausschließlich in Deutschland
- Anwendung des strengen deutschen Datenschutzgesetzes

E-Mail mit PGP (mit/ohne EmiG)

Sicherheitsversprechen für die ausschließliche Lesbarkeit für Absender und Empfänger:

„Verschlüsselte Nachricht mit individuellem Zugangscode nur für Sender und Empfänger“

- Höchster Schutz für die E-Mail-Kommunikation durch E2E
- Signatur stellt sicher, dass Mail von erwartetem Absender stammt
- Schutz vertraulicher Inhalte bei:
  - Falschem Empfänger
  - Ungewollter Weiterleitung
  - Unbefugtem Zugang ins Postfach
  - Unklaren Datenschutz-bestimmungen und nicht garantierter Transport-verschlüsselung von Nicht-EmiG-Empfängern

Anforderung an die Lösung

- Einfach in der Verwendung
  - Einrichtungsassistent, Einladungsprozess, Erkennen von PGP Mails
  - Sicheres Public-Key-Verzeichnis, Backup-Lösung für Private und Public Keys, Synchronisation aller verwendeten Geräte
  - Verschlüsselung von Attachments
- Kompatibilität mit E-Mail
- Offener Standard außerhalb WEB.DE / GMX
  - Kompatibel zu anderen E-Mail-Anbietern, Verwendung vorhandener Schlüssel
  - Verwendung von OpenPGP
- Multi-Device-Fähigkeit
  - Anbindung weiterer Geräte (Desktop, Mobile) per QR-Code oder Freischaltcode
- Transparentes System
  - Mailvelope für Webmail, Sicherheitsmodul für Apps, Security Audits durch externe Sicherheitsspezialisten
  - Keine serverseitige Verschlüsselung, sondern echte Ende-zu-Ende-Verschlüsselung