In die Digitale Zukunft – aber sicher:

Strategien und Werkzeuge zum Einsatz von Verschlüsselung

Prof. Dr. Michael Waidner
Fraunhofer-Institut für Sichere Informationstechnologie SIT, Darmstadt und
Technische Universität Darmstadt

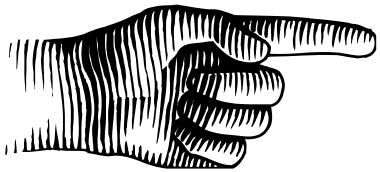
(c) www.neoclipart.com

CASED

Future Internet Kongress
Frankfurt, 17. September 2015

Fraunhofer SIT

Überblick



- Fraunhofer SIT: Führendes Forschungsinstitut für Cybersicherheit
- Digitalisierung und Cybersicherheit
- Verschlüsselung
  - Strategien
  - Volksverschlüsselung
  - Omnicloud & Panbox
- Zusammenfassung

Fraunhofer-Institut für Sichere Informationstechnologie

Führendes Institut f. angewandte Cybersicherheitsforschung in Deutschland

Fraunhofer SIT

- **Sicherheit großer, integrierter IT-basierter Systeme**
  - Entwurf ("by design"), Analyse, Tests, Experimente und Messungen
  - Cybersecurity, Forensics, Privacy, Cloud, Embedded, Internet, Infrastruktur, Software, Business/Industrial IT
- **In Zahlen und Fakten**
  - Gründung **1961,** Fokus auf Cybersicherheit seit **1996,** Teil der Fraunhofer-Gesellschaft seit **2001**
  - 170 Angestellte in 9 Abteilungen in Darmstadt (HQ) und Birlinghoven
  - 1/3 Grundfinanzierung, 2/3 Auftragsforschung für Industrie & Staat
  - Forschungspartnerschaften mit TU Darmstadt und Hochschule Darmstadt: **CASED & EC SPRIDE**

Forschungspartner in Darmstadt

Center for Advanced Security Research Darmstadt (LOEWE)
European Center for Security and Privacy by Design (BMBF)

Gemeinsames »Dach« für Darmstädter Cybersicherheitsforschung

Mehr als 400 wiss. MA aus 47 Ländern + mehr als 2000 Studierende

TU Darmstadt

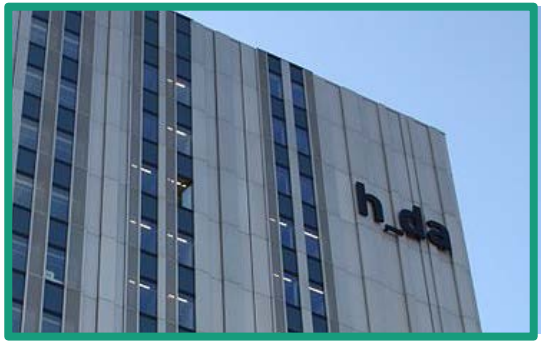
32 Profs in
10 Fachbereichen

Fraunhofer SIT

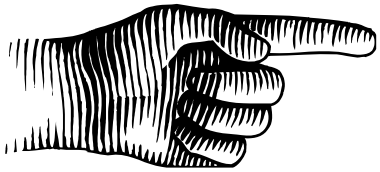
170 Mitarbeiter/innen
in 9 Abteilungen

Hochschule Darmstadt

13 Profs



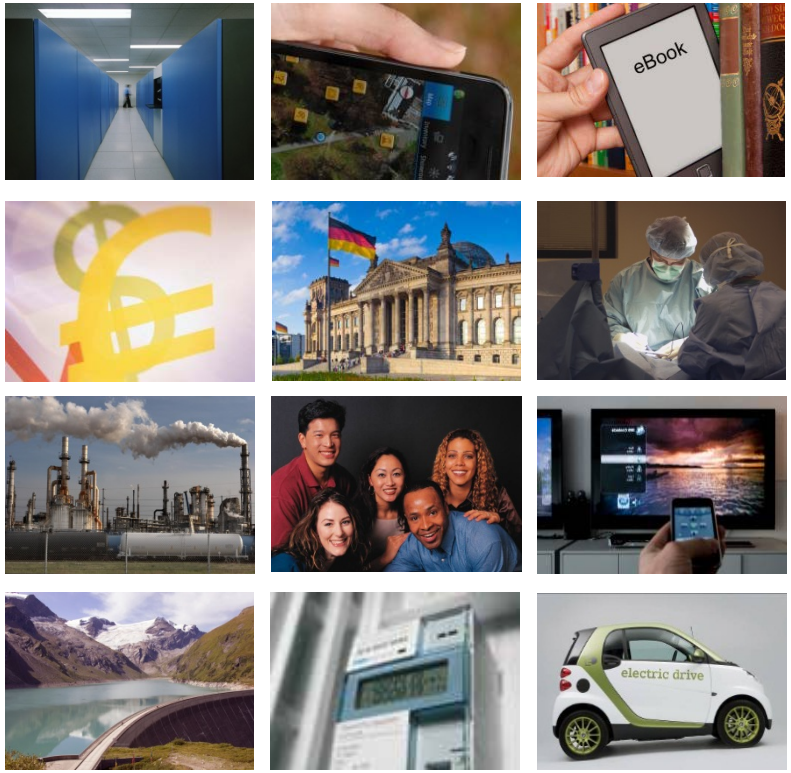
Überblick

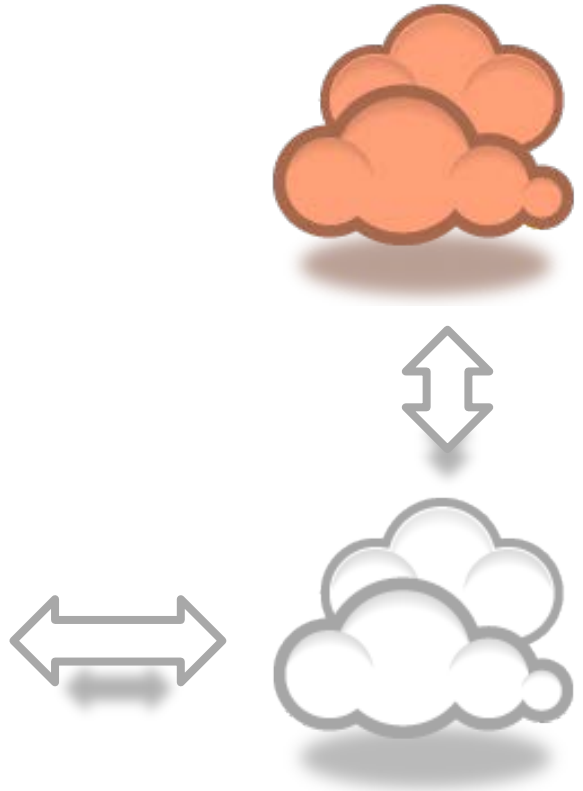


- Fraunhofer SIT: Führendes Forschungsinstitut für Cybersicherheit
- Digitalisierung und Cybersicherheit
- Verschlüsselung
  - Strategien
  - Volksverschlüsselung
  - Omnicloud & Panbox
- Zusammenfassung

»Digitale Welt« ist überall

Verbunden, programmierbar, offen und gemeinsam genutzt. Es fallen großen Mengen an Daten an, oft sensitive, meist unstrukturierte.

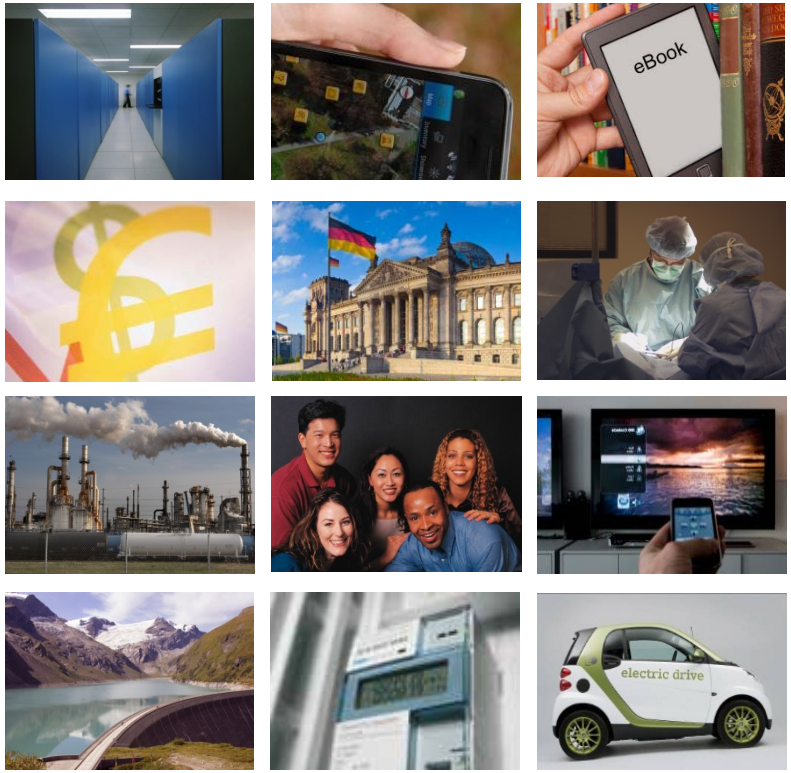




Alle neuen Technologien, Dienste, Erbringungs- und Geschäftsmodelle erzeugen zusätzliche Herausforderungen für Sicherheit und Privatsphäre

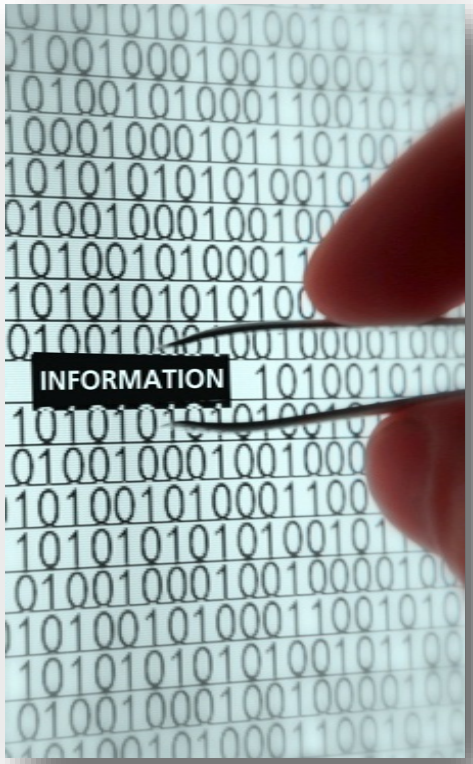
»Digitale Welt« ist überall

Zentrale Sicherheitsanforderung: Schutz von Daten vor unerlaubtem Zugriff, unerlaubter Verwendung, unerlaubter Veränderung



- **Unternehmenssicht**
  - Information ist die kritische Ressource für eine erfolgreiche Transformation
- **Bürgersicht**
  - Jede Handlung erzeugt eine Fülle von Informationen

Digitale Transformation – Vertraulichkeit im Fokus



Wirtschaftsspionage gefährdet Unternehmens-Know-how:

- 51% der Unternehmen sind betroffen mit einem jährlichen Schaden von 51 Mrd. Euro[1].
- Der Mittelstand steht verstärkt im Fokus[2].

Vertraulichkeitsverletzungen bei personenbezogenen Daten verletzen Datenschutzgesetze und schädigen **Reputation**

Personalprofile und **Scores** gefährden Privatheit und entscheiden über Ansehen und Kreditwürdigkeit

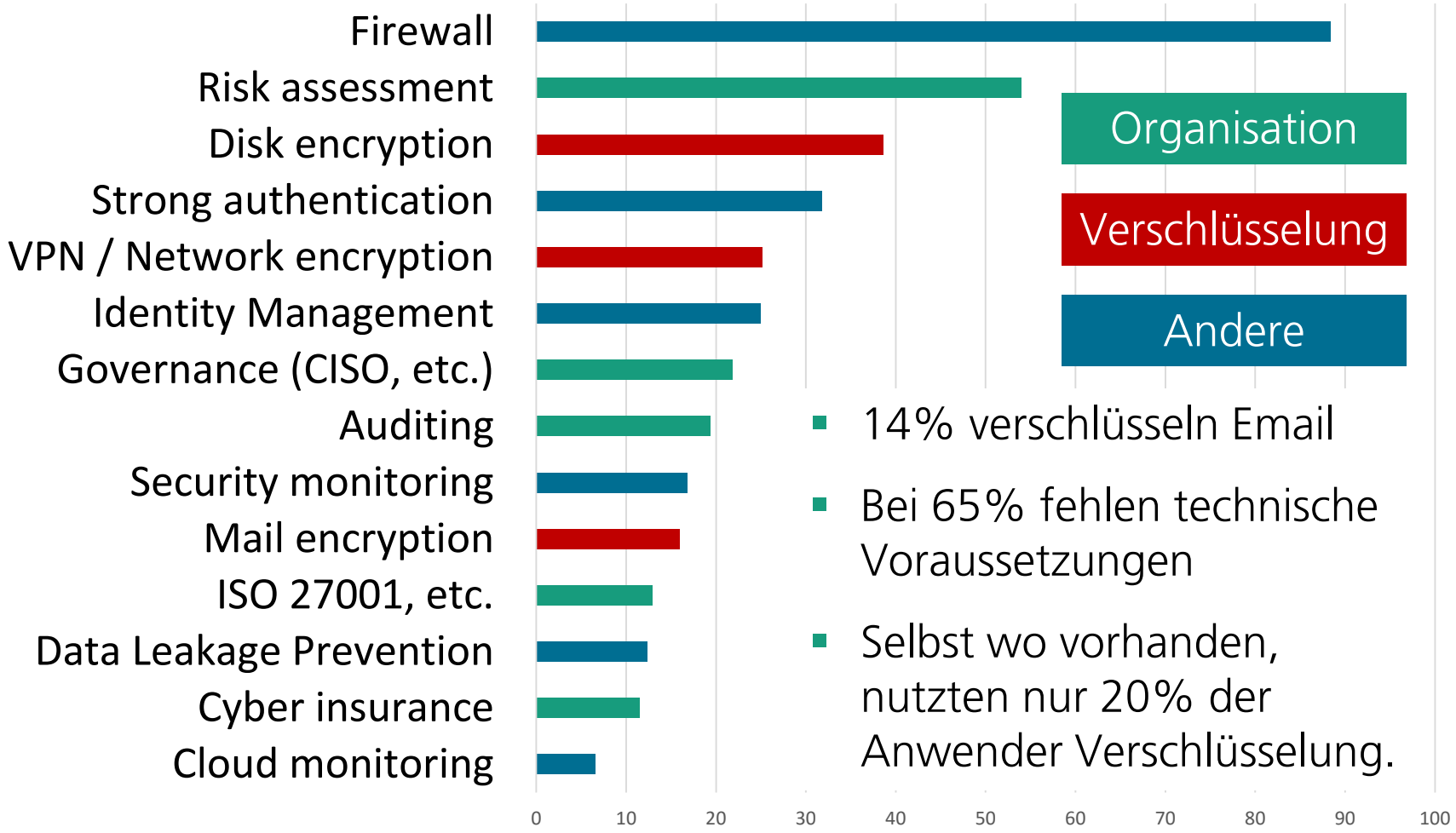
Identitätsmissbrauch befördert Cyber-Mobbing und Betrug

- 21% aller Nutzer wurden bereits durch Identitätsdiebstahl geschädigt[3].

[1] Studie bitkom 7/2015
[2] Corporate Trust 2014
[3] SCHUFA 9/2013

Sicherheitslösungen werden zu wenig genutzt

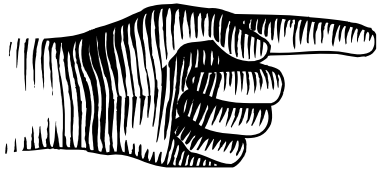
Verschlüsselung mangelhaft



Source: Studie Industriespionage 2014; Corporate Trust, 30. Juli 2014 (Grafiken 24, 27, 29)

Überblick

- Fraunhofer SIT: Führendes Forschungsinstitut für Cybersicherheit
- Digitalisierung und Cybersicherheit
- Verschlüsselung
  - Strategien
  - Volksverschlüsselung
  - Omnicloud & Panbox
- Zusammenfassung

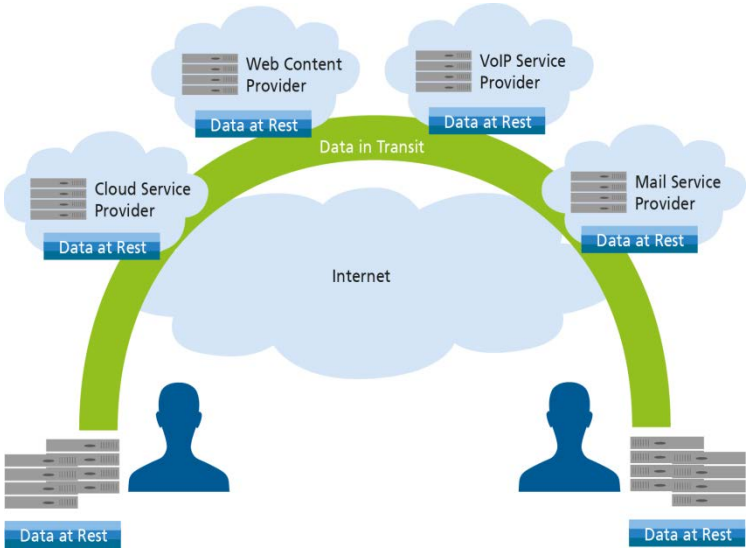


Ratgeber zur Planung und Implementierung von Verschlüsselungslösungen für kleine und mittlere Unternehmen mit vielen Referenzlösungen für unterschiedliche Typen von KMU

`https://www.sit.fraunhofer.de/reports`

Investition in Ihre Zukunft
HESSEN
Investitionen für diese Entwicklung wurden von der Europäischen Union aus dem Europäischen Fonds für regionale Entwicklung und vom Land Hessen kofinanziert.
Dieser Report wurde aus dem Projekt Enterprise Encryption finanziert.

Ansatzpunkte für Verschlüsselung



Verschlüsselung für Data in Transit:

- E-Mail-Kommunikation
- Instant Messaging
- Sprachkommunikation
- Kollaborationsanwendungen
- Externe und ggf. interne Netzwerkzugriffe

Verschlüsselung für Data at Rest auf der Ebene

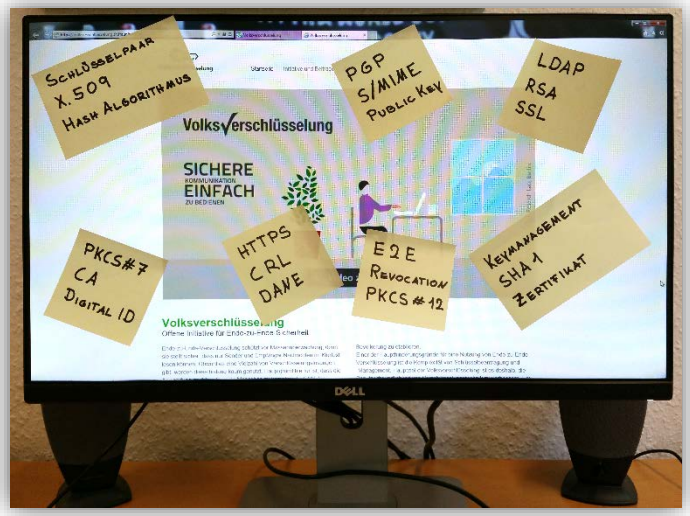
- der Datenträger
- von Containern, Verzeichnissen
- der Dateien

Problemfeld: unkoordinierter Einsatz von Verschlüsselung

- Vielzahl an Schlüsseln erschwert die Verwaltung
- Mangelnde vertrauenswürdige Kommunikationswege für die Verbreitung von Schlüsseln
- Keine Kontrolle über Schlüsselverteilung
- Keine Einschätzung über die Güte von Schlüsselmaterial
- Keine Verwaltungsunterstützung bei Kompromitierung von Schlüsseln
- Langfristige Sicherung von Schlüsselmaterial

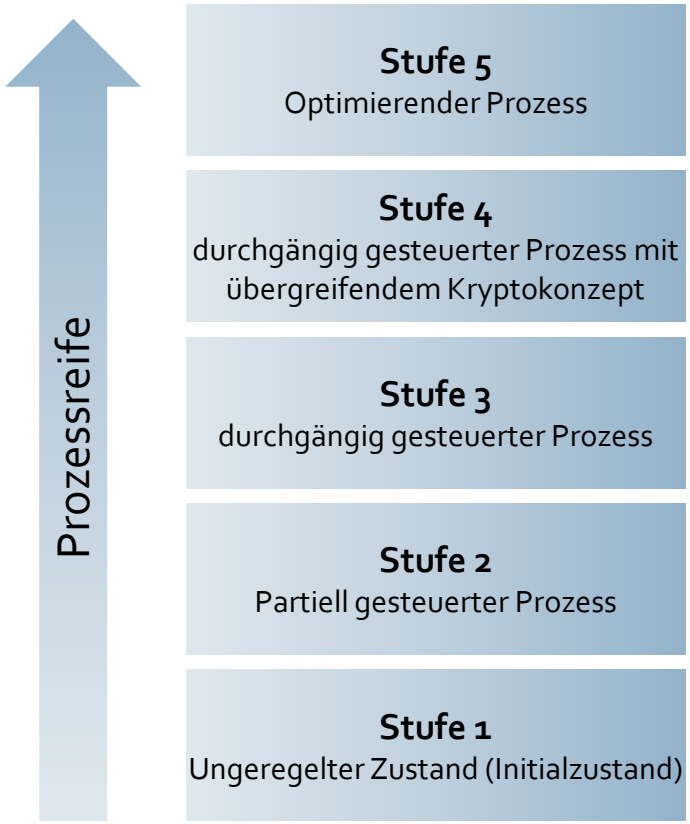
Lösungsansatz: Asymmetrische Verschlüsselung

Hindernisse für die Nutzung von asymmetrischer Verschlüsselung



- Das Konzept asymmetrischer Verschlüsselung ist komplex und nicht intuitiv nachvollziehbar.
- Anwender nutzen eine Vielzahl von Systemen und Programmen. Sie haben keine ausreichende Expertise, um Verschlüsselung richtig und sicher zu konfigurieren.
- Es gibt keine für KMU und private Nutzer praktikable Lösung für ein übergreifendes Schlüsselmanagement.
- Die Usability existierenden Lösungen ist schlecht.
- Schlüssel und Zertifikate sind nicht breit verfügbar. Es fehlt eine Infrastruktur, um Schlüssel zu verteilen.

Herausforderung: konsistente, prozessübergreifende Lösung



- Stufe 1:
  keine organisatorischen und systematisch eingeführten technischen Vorkehrungen für Verschlüsselung
- Stufe 2
  Es existieren vereinzelt Vorkehrungen und Regelungen.
- Stufe 3
  Es gibt ein Gesamtkonzept für Vertraulichkeitsschutz.
- Stufe 4
  Das Konzept wird um ein Kryptokonzept mit durchgängigem Schlüsselmanagement ergänzt.
- Stufe 5
  Nutzung von Kennzahlen und regelmäßigen Audits als Instrumente zur Optimierung

Strategien für kleine und mittlere Unternehmen

- KMU sind mit der eigenständigen Verwaltung kryptographischer Instrumente überfordert.
- Sie sollten einem bewährten Vorgehensmodell folgen, das dem Reifegrad Stufe 2 entspricht.
- Beispiel: Handwerksbetrieb mit wenigen Angestellten und kleinem Netzwerk mit drei PCs und einem Server

Vorgehensmodell für KMU (1/3)
Beispiel Handwerksbetrieb

1. Bestimmung des Schutzbedarfs der Informationen

Informationsbestände.	Bewertung
Personaldaten mit Gehaltsinformationen, Fehlzeiten etc.	Dies sind sehr sensible Informationen mit sehr hohen Vertraulichkeitsanforderungen.
Kundendaten (Adressen, Angebote, erbrachte Leistungen und Umsätze)	Dies sind sensible Informationen mit hohen Vertraulichkeitsanforderungen.
Leistungsverzeichnisse,	Diese Informationen haben geringe Vertraulichkeitsanforderungen, da sie z. T. öffentlich verfügbar sind. Dort, wo sie unternehmensspezifisch sind, würde bei unberechtigten Zugriffen kein Schaden entstehen.
Lagerinformationen	Dies sind für das Unternehmen sensible Informationen. Die Vertraulichkeitsanforderungen sind hoch, da diese Informationen das Know-how der Firma repräsentieren und einen Konkurrenzvorteil bieten können.
Kalkulationen	Dies sind sehr sensible Informationen. Die Vertraulichkeitsanforderungen sind sehr hoch.

Vorgehensmodell für KMU (2/3)
Beispiel Handwerksbetrieb

2. Bestimmung der Gefährdungen und Kritikalität der Übertragungswege und Speicherorte

- Vertraulichkeitsverletzungen beim Verlust von mobilen Datenträger und Laptops
- Unautorisierter Zugriff auf sensible Daten im Unternehmen, z. B. durch unzufriedene Mitarbeiter, die Informationen zu neuen Arbeitgebern mitnehmen
- Datenschutzverletzung durch unberechtigten Zugriff auf personenbezogene Daten
- Unberechtigter Zugriff auf E-Mails z.B. zum Steuerberater mit vertraulichem Inhalt

Vorgehensmodell für KMU (3/3)
Beispiel Handwerksbetrieb

3. Skizze einer Verschlüsselungslösung

Data in Transit

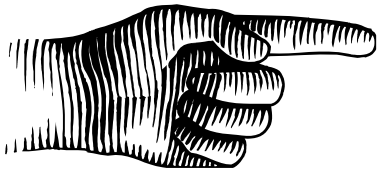
- E-Mails zum Steuerberater (Personaldaten, Kosten- und Ertragsinformationen) werden verschlüsselt übertragen, z.B. mit Hilfe der Volksverschlüsselung
- Angebote an Kunden per E-Mail werden verschlüsselt, z.B. mit Hilfe der Volksverschlüsselung

Data at Rest

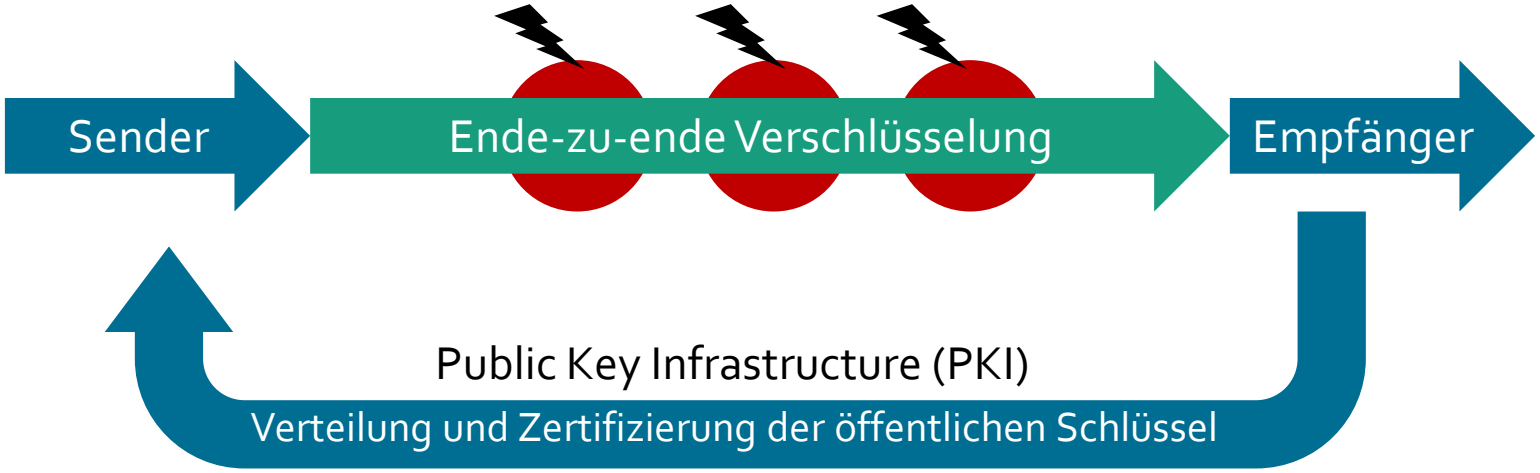
- Festplattenverschlüsselung für Laptops
- USB-Sticks mit hardwarebasierter Verschlüsselung
- Sensible Daten auf den Firmen-PCs (Personaldaten, Lagerverwaltung, Angebote, Kosten, Erträge) sind in verschlüsselten Containern abzulegen.

Überblick

- Fraunhofer SIT: Führendes Forschungsinstitut für Cybersicherheit
- Digitalisierung und Cybersicherheit
- Verschlüsselung
  - Strategien
  - Volksverschlüsselung
  - Omnicloud & Panbox
- Zusammenfassung



Ende-zu-ende Verschlüsselung ist Mittel der Wahl gegen Massenüberwachung



Herausforderungen: Sichere Standards/Code, Laientauglichkeit, Skalierbarkeit

Volksverschlüsselung

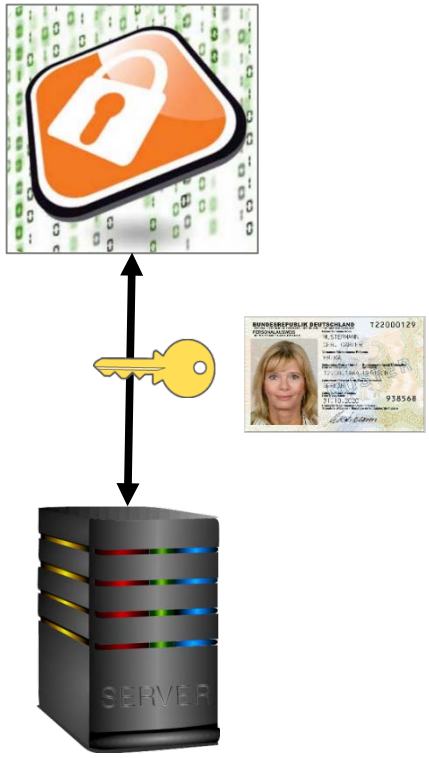
- Ende-zu-Ende-Verschlüsselung ist strategisches Ziel für Deutschland und ein wirksames Mittel gegen die anlasslose Massenausspähung.
- Problem:
  - Wie erhalten Menschen kryptografische Schlüssel?
  - Wie erreicht man „Laientauglichkeit“?
- Lösungsansatz:
  - Die **VV-Software** steuert den ganzen Prozess
  - Fraunhofer SIT betreibt Online-Zertifizierungsstelle

Die **VV-Software** wird für alle großen Betriebssysteme bereitgestellt.

- Microsoft Windows®
- Mac OS X®
- Linux®
- Android®
- iOS®

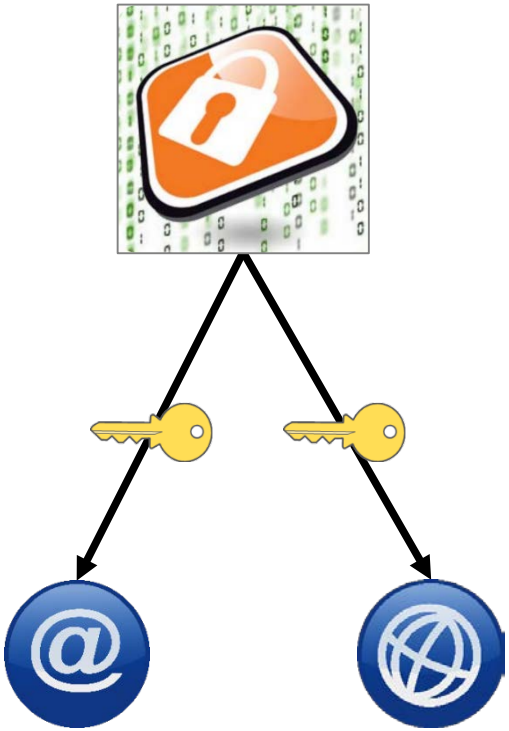
Volksverschlüsselung

1. VV-Software erzeugt Schlüssel und lässt sie zertifizieren

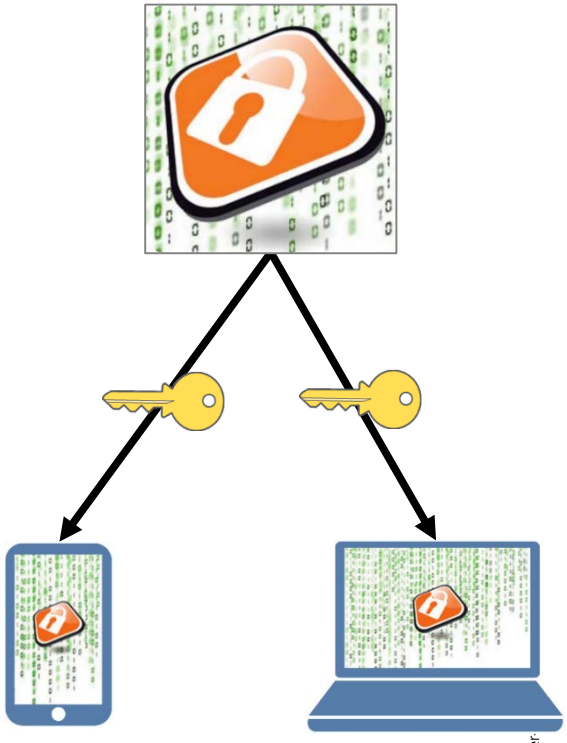


Zertifizierung

2. VV-Software verteilt Schlüssel an lokale Anwendungen



3. VV-Software verteilt Schlüssel an weitere Geräte



Volksverschlüsselung

VV-Software (Client-Anwendung)

- Erzeugung/Verwaltung kryptografischer Schlüssel
- Beantragung von Zertifikaten über die VV-PKI
- Installation der Schlüssel/Zertifikate in lokalen Anwendungen (z.B. Browser, E-Mail-Programm)
- Backup + Sperranträge für Zertifikate

Volksverschlüsselung

Status: Beta-Version

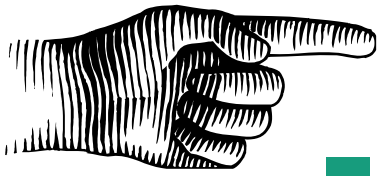
Unterstützte Plattformen: Windows (Linux, Mac OS X, mobile OS geplant)

Release: Öffentliche Beta-Version für Mitte November geplant, VV-Software wird zur privaten Nutzung kostenlos sein (Quellcode offen)

Informationen unter: https://volksverschluesselung.de/

Überblick

- Fraunhofer SIT: Führendes Forschungsinstitut für Cybersicherheit
- Digitalisierung und Cybersicherheit
- Verschlüsselung
  - Strategien
  - Volksverschlüsselung
  - Omnicloud & Panbox
- Zusammenfassung



Sichere Nutzung von Cloud-Speicherdiensten

Hintergrund

- Steigende Beliebtheit von Cloud-Speicherdiensten
- Nutzer teilen immer mehr Daten mit anderen Nutzern
- Risiko: Kein Schutz der Daten in der Cloud

Ziele

- Cloud-Speicher sicherer machen
- Bindung an Cloud-Anbieter verhindern

Lösungen

- **OmniCloud** (Zielgruppe: KMUs)
- **PanBox** (Zielgruppe: Private Nutzer, Unternehmen)

OmniCloud

Zielgruppe

- KMUs ohne Budget für private Clouds
- Fokus auf Backups, Netzwerklaufwerke, Datenaustausch

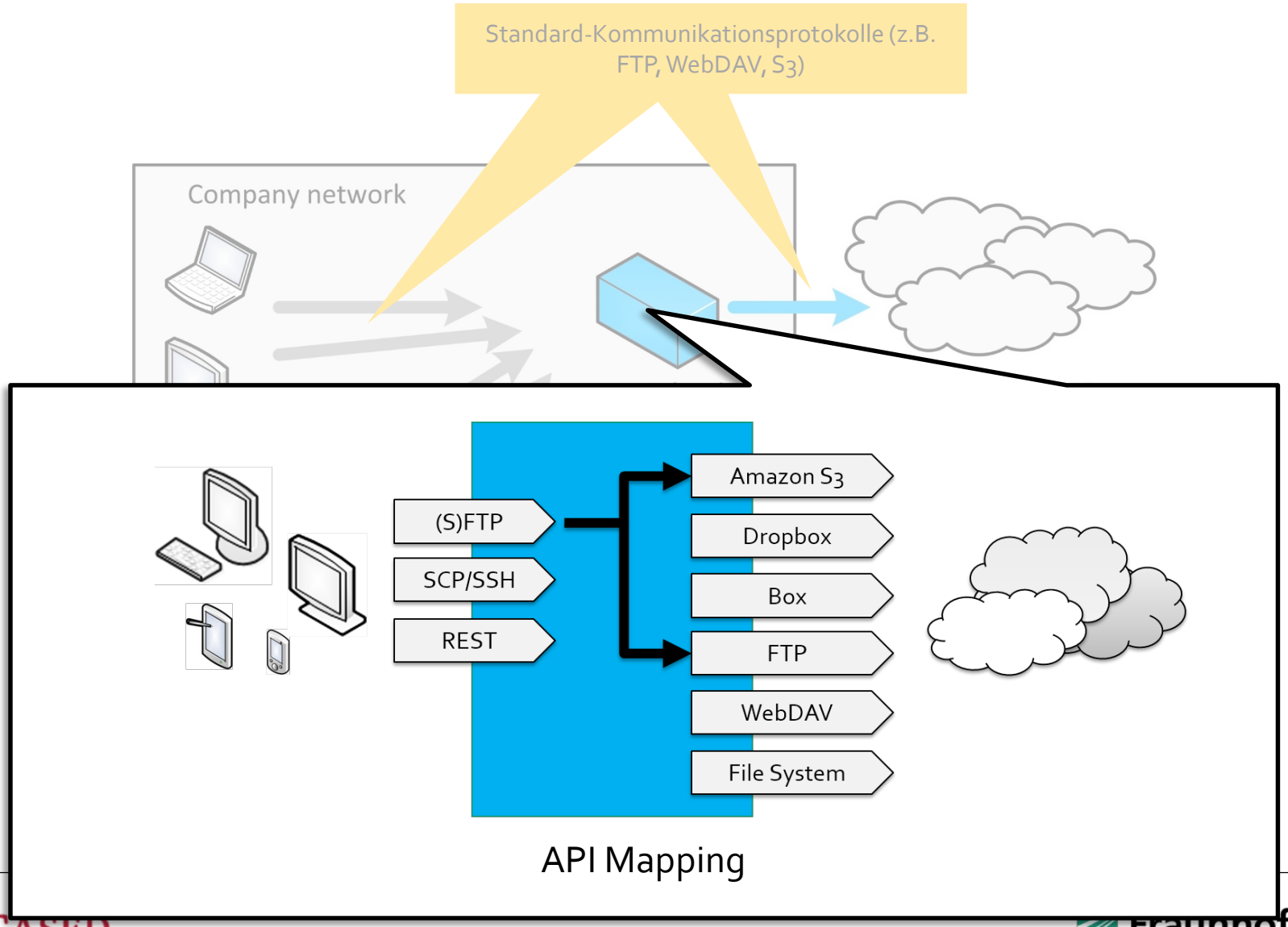
Konzept

- Zentrales Enterprise-Gateway im Unternehmensnetzwerk
- Keine Installationen auf den Endgeräten notwendig

"Investment in your Future"
Investments for this work were co-funded by the European Union with European regional development funds and by the state government of Hessen

HESSEN

Einfache Integration: OmniCloud Enterprise Gateway



OmniCloud – Sicherheit

Lokale Datenverschlüsselung

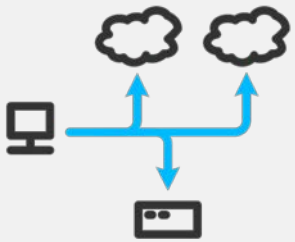
- Vor dem Verlassen des Unternehmensnetzwerks
- Separate Schlüssel für jede Datei
- Schlüssel bleiben im Unternehmensnetzwerk

Rollenbasierte Zugriffskontrolle

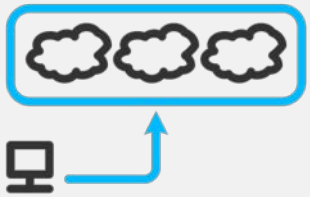
Verschleierung von Dateinamen und Verzeichnisstrukturen

Name	Size	Modified
Parent directory		
zrmeungj9ohckefczeq9egd9x9otgvmngiusvfghc	8.2 MB	2012-10-02 09:20
97aun4k9bojvcdf79q4uirfcfdp7ueqjcqckbogsxb	861 KB	2012-09-05 16:32
zdecjtdrtncizyyuywrzy7ip7ezueukhfoj4vtdisepx	18.2 MB	2012-08-02 11:37

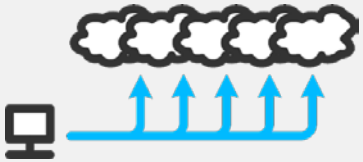
OmniCloud – Weitere Merkmale



Mirroring



Striping



RAID

Speicherstrategien

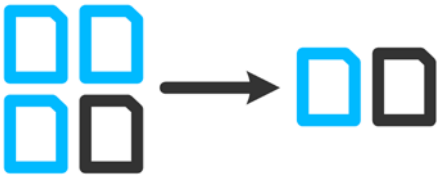
- Geben an, wie Dateien über die Cloud-Speicher verteilt werden
- Berücksichtigen spezifische Eigenschaften der Cloud-Speicher

Daten-Deduplikation

Erkennung doppelter Dateien

Dateien werden nur einmal in der Cloud abgelegt

Reduzierung der Kosten für Cloud-Speicher



OmniCloud – Status

Status: Produkt (Version 1.0)

Unterstützte Plattformen: Windows, Linux, Mac OS X

Release: Ende 2015 (geplant), Vertriebspartnerschaften sind erwünscht, Testversionen auf Anfrage erhältlich

Informationen unter: http://www.omnicloud.sit.fraunhofer.de

PanBox

Zielgruppe

- Privatanwender und Unternehmen

Konzept

- Installation auf den Endgeräten der Nutzer
- Client-Anwendungen der Cloud-Speicherdienste können weiterverwendet werden
- Kein zentraler PanBox-Server notwendig

Gefördert durch:

Bundesministerium der Justiz und für Verbraucherschutz

aufgrund eines Beschlusses des Deutschen Bundestages

PanBox – Status

Status: Open-Source Software

Gemeinschaftsentwicklung Fraunhofer SIT / Sirrix AG

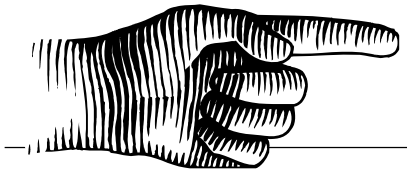
Unterstützte Plattformen: Windows, Linux, Android

Vertrieb: Sirrix AG (kostenloser Download)

Informationen unter: https://www.sit.fraunhofer.de/panbox/

Überblick

- Fraunhofer SIT: Führendes Forschungsinstitut für Cybersicherheit
- Digitalisierung und Cybersicherheit
- Verschlüsselung
  - Strategien
  - Volksverschlüsselung
  - Omnicloud & Panbox
- Zusammenfassung



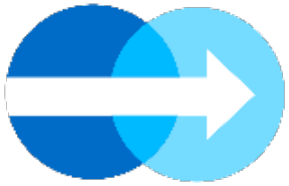
Zusammenfassung: Verschlüsselung für alle(s)

- **Verschlüsselung schützt Daten vor unerlaubter Einsicht**
- **Ziel: Konsequente, flächendeckende Ende-zu-Ende Verschlüsselung**
- **Herausforderungen**
  - Skalierbarkeit: Föderation von PKIs
  - Laientauglichkeit: Automatisierung
  - Kosten: Grundversorgung

Automatisierung:

Volksverschlüsselung

Sichere Cloud-Speicher:



PanBox

Prof. Dr. Michael Waidner

Fraunhofer-Institut für
Sichere Informationstechnologie SIT

Institutsleiter

www.sit.fraunhofer.de

Technische Universität Darmstadt

Fachbereich Informatik, Lehrstuhl SIT
CASED & EC SPRIDE, Direktor

www.sit.tu-darmstadt.de

Institut	Rheinstraße 75, 64295 Darmstadt
E-Mail	michael.waidner@sit.fraunhofer.de
Telefon	+49 6151 869 250 (Büro)
	+49 170 929 8243 (Mobil)