Aktuelle Situation IT-Sicherheit im Digitalisierungszeitalter

Simmons & Simmons Digital Day 2018

26.04.2018, München

Agenda

„Aktuelle Situation IT-Sicherheit und Technologietrends im Digitalisierungszeitalter“

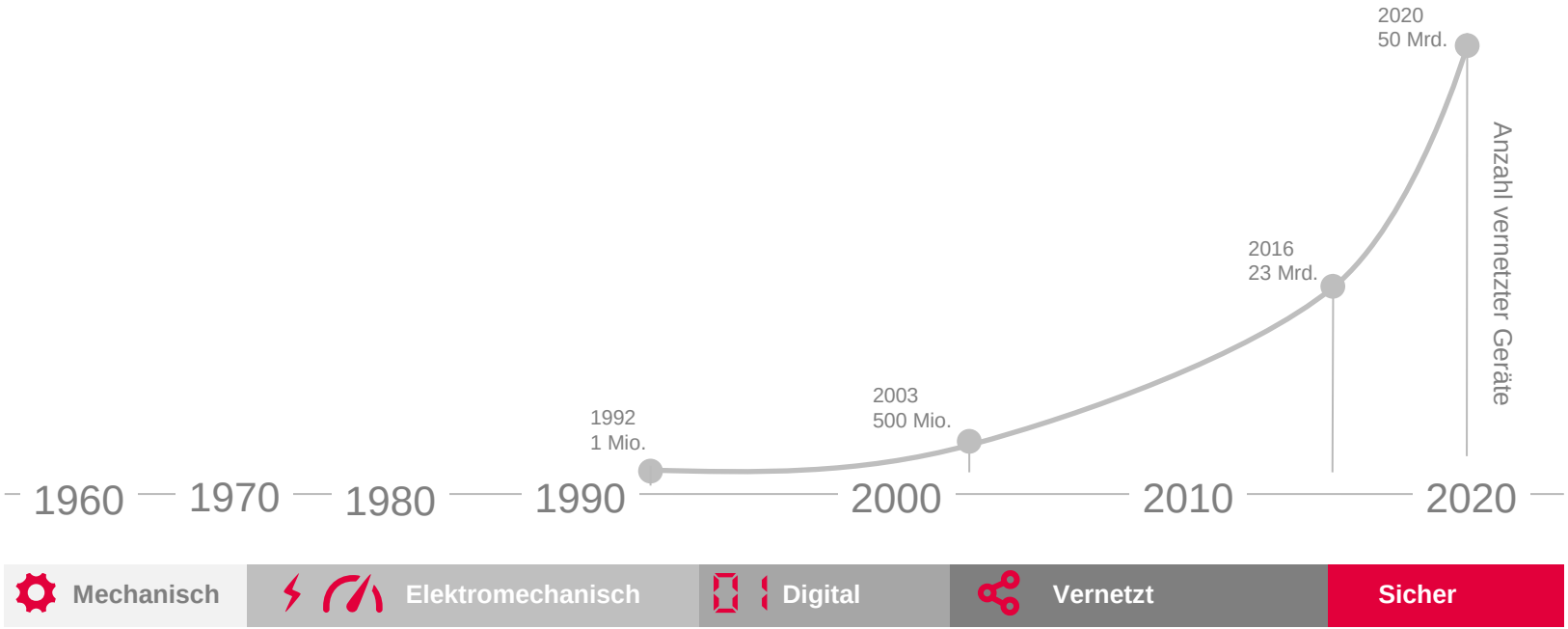
Aktuelle Produkte, Konzepte und Vorgehensweisen zum Schutz von Industrieunternehmen

Live-Demo „Wir alle sind Opfer“

Aktuelle Situation IT-Sicherheit und Technologietrends im Digitalisierungszeitalter

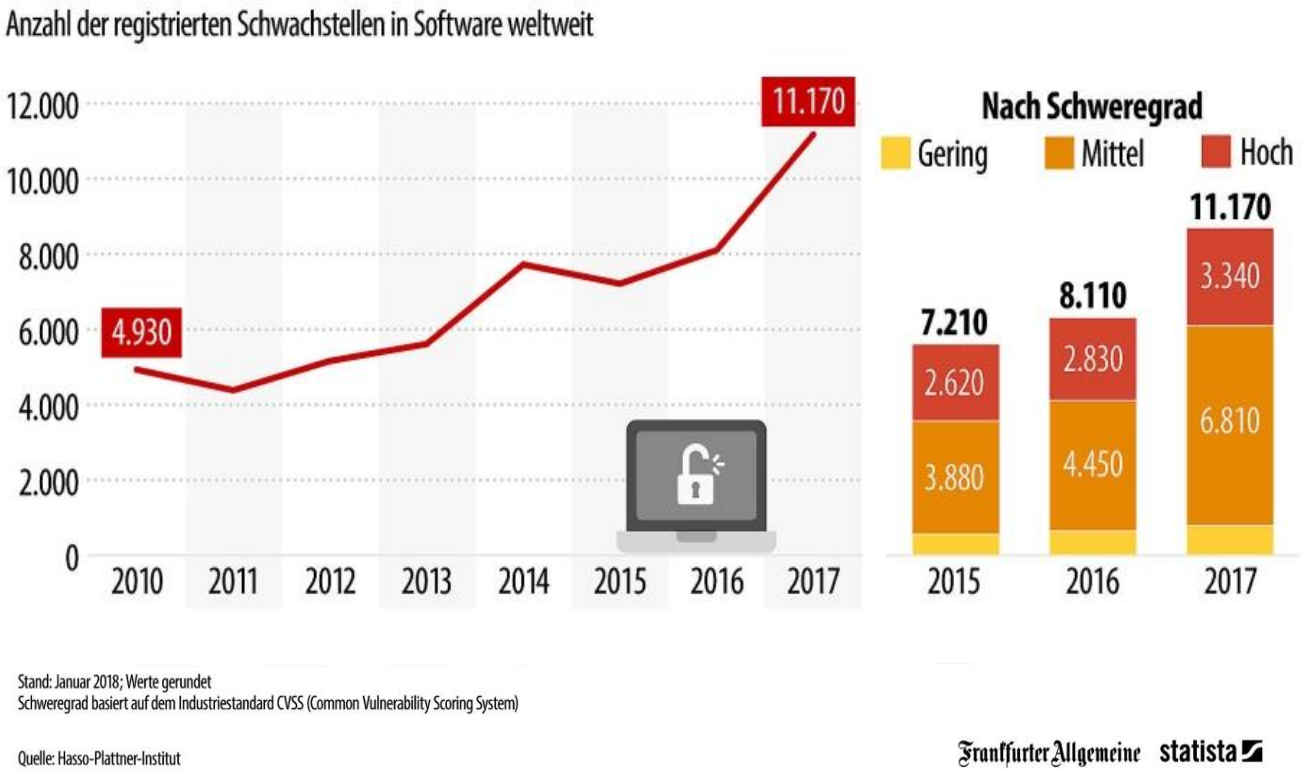
secunet

Digitalisierung bedeutet Vernetzung



secunet

Sicherheitslücken auf Rekordhoch



secunet

Wanna Cry

Auslöser:

→ E-Mails und Wurmfunktionalität

Auswirkung:

→ Verschlüsseln aller Daten
Wirkfunktion: Erpressung

Ziele:

→ Weltweit, britisches Gesundheitssystem, Renault, Telefonica, FedEx, Deutsche Bahn

Vermutungen:

→ Ob konkretes Ziel avisiert war ist unklar

Quellen: Threat Intellegence in KRITIS – Prof. Dr. Christian Dietrich; Wikipedia

secunet

NotPetya

Auslöser:

→ Update der ukrainischen Steuersoftware MeDoc

Auswirkung:

→ Verschlüsseln aller Daten, Tatsächliche Wirkfunktion: Sabotage/Zerstörung (Wiper)

Ziele:

→ In Ukraine, the central bank, a state telecom, municipal metro, and Kiev's Boryspil Airport, Chernobyl nuclear site – Maersk (300Mio. Verlust)

Vermutungen:

→ Gezielter Angriff auf die Ukraine

Quellen: Threat Intellegence in KRITIS – Prof. Dr. Christian Dietrich; Wikipedia

secunet

Spectre & Meltdown – Globale Sicherheitslücke

Situation:

→Designfehler in Hard- und Software

Auswirkung:

→ Grundsätzliche Angreifbarkeit von Systemen, Unlauterer Zugriff auf Informationen

Auslöser: E-Mail, Webseite, USB, …

Probleme:

→ Globalisierung und Monopolstellungen, Offensichtlicher Hinweis auf den Verlust Digitaler Souveränität

Quellen: https://www.windowscentral.com/intel-says-its-patches-will-make-pcs-immune-meltdown-and-spectre-exploits

secunet

Wie ist die aktuelle Situation zur IT-Sicherheit einzuschätzen

Cybercrime betrifft alle Bereiche – Thesen

- **IoT(2017)**: Kriminelle bieten Mirai-Botnetz mit 400.000 IoT-Geräten zur Miete an
- **IoT(2017)**: Fehler in Geschirrspüler ermöglicht Zugriff auf Webserver
- **Cloud**
- **Wahlen**
- **EU ist angreifbar** → Digitale Souveränität ist eingeschränkt?
- Ziel: **Deutschlands Mittelstand**

secunet

Wie ist die aktuelle Situation zur IT-Sicherheit einzuschätzen

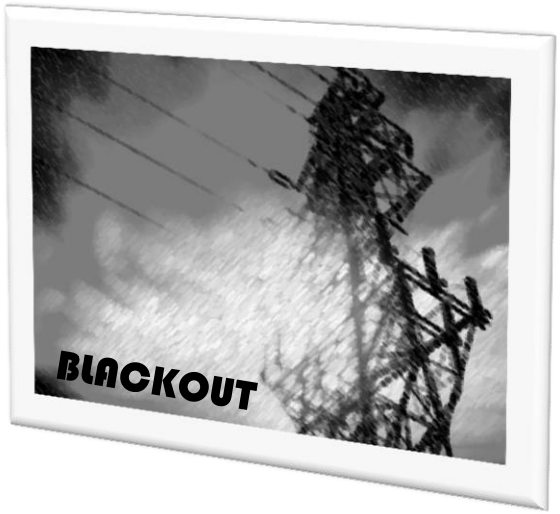
Cybercrime betrifft alle Bereiche - Thesen

- **IoT**: Kriminelle bieten Mirai-Botnetz [illegible] äten zur Miete an
- **IoT**: Fehler in [illegible] erver
- **Clou** [illegible]
- **Wahle** [illegible]
- **EU ist** [illegible] Souveränität ist eingeschränkt?
- Ziel: **Deutschlands Mittelstand**

Die Brisanz wurde durchaus auch erkannt
Bsp. IT Sicherheitsgesetz, EU-Vorbereitung Cybersecurity Act

secunet

Fazit: …vom kleinen Klick zum großen Blackout…



secunet

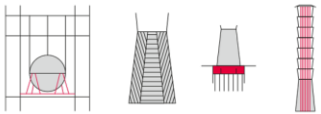
Fazit: …vom kleinen Klick zum großen Blackout…

secunet

Jede Architektur benötigt Stabilitätsanker

Resilience

Sicherheit



secunet

Technologietrends...

Trends

- Mobilität / Data Center / Cloud
  - Smartphones / Tablets / App‘isierung
  - 5G Netzwerke / Netzwerk-Virtualisierung
  - Multi-Tenancy / „Mandantentrennung“
  - Software Defined Everything (SDx)
  - Edge Cloud / „Smart Dust“
  - Automatisierung (CD/CI)
- Wachsende Bandbreiten
- Algorithmen / „Künstliche Intelligenz“

secunet Antworten

- SDN / Cloud Forschungsprojekte
- Open Stack Security
- „100 G auf L1…L3“ inkl. Managebarkeit
- Neue Mobile Devices

- Mikro-Hypervisor / Introspection
- Anti Tamper Technologien
- Post Quantum Kryptographie
- Separation Kernel / KBA

… und Sicherheit (?)

- „Software eats the world“
  - Hardware Standardisierung
  - Produktion in Asien
  - → **(sehr) punktuell eigene Hardware-Lösungen**
  - → **Enge Kooperationen mit Marktführern (Mellanox, Lenovo, Samsung…)**

- Funktionale Komplexität
  - siehe Trends – steigt „gefühlt“ exponentiell
  - → **Architektur + Defense-in-Depth + Detektion + Secure Product Lifecycle**

- Vertrauenswürdigkeit
  - Vollständige Evaluierbarkeit zunehmend schwierig (technische Expertise, Zeit)
  - → **Optimierung des Evaluationsprozesses**
  - → **Vertrauenswürdigkeit von Herstellern und Prozessen**

secunet

Auf einen Blick

- Kundenorientierte Unternehmensstruktur
- Mehr als 500 Mitarbeiter an elf deutschen Standorten
- Gegründet 1997
- Im Prime Standard der Deutschen Börse gelistet
- Größter Anteilseigner (79%): Giesecke & Devrient GmbH
- Umsatz 2017: € 158,3 Mio.
  EBIT 2017: € 23,5 Mio.

Wir sprechen Ihre Sprache

Unsere gemeinsamen Projekte werden aus einer von fünf Divisionen heraus durchgeführt.
Jede Division bietet marktspezifische Produkte und Leistungen aus der Angebotspalette.

Öffentliche Auftraggeber	Innere Sicherheit	Verteidigung	KRITIS	Automotive
Auswärtiges Amt	Bundeskriminalamt	Bundesministerium der Verteidigung	Berliner Wasserbetriebe	BMW
ELW	EUROPOL	Bundeswehr	T-Systems	Continental
Bundesagentur für Arbeit	BUNDESPOLIZEI	NATO OTAN	VORWEG GEHEN	Audi
			Lufthansa	

secunet

Aktuelle Produkte, Konzepte und Vorgehensweisen zum Schutz von Industrieunternehmen

secunet

Von der Analyse zur Maßnahme – aktiv und reaktiv

Sicherheitskultur und -architektur

- Klare Sicherheitsorganisation (ISMS, DSMS, …)
- Klare Sicherheitsarchitektur (Separieren, Separieren, Separieren)
- Sensibilisierte Mitarbeiter und Führungskräfte
- Penetrationstests, Notfallübungen, …

„Incident Response“

- Monitoring
- Notfallmanagement
- Forensik

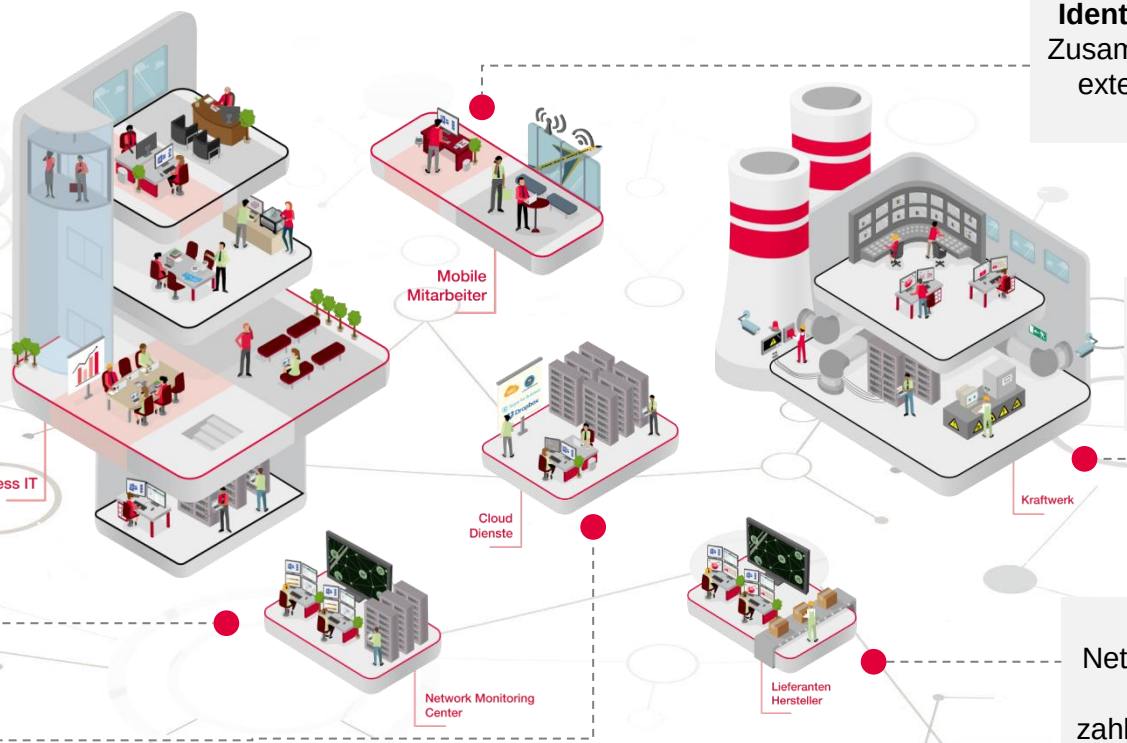
secunet

Herausforderungen für die Industrie in der Digitalisierung

Verteilte **Daten**sammlung, zentrale Datenhaltung – sicherer **Transport** und sichere **Speicherung**

Datenumfang und **Datenströme** kontrollieren (Sensor-Überfluss)

Auslagerung von **IT-Komplexität**



Identitätsmanagement im Zusammenspiel interner und externer Mitarbeiter und Fachkräfte

Sicherheitszonen zur Risikosteuerung aufrechterhalten oder einrichten

Leistungsfähige Netzwerkinfrastruktur und **Schnittstellen** zu zahlreichen **Stakeholdern**

secunet

Sichere Vernetzung durch die secunet security infrastructure (ssi)

Sicherheitszonen
(durchgehende Isolation unterschiedlicher Schutzbereiche)

Endgerätesicherheit
(Sicher in getrennten Netzen arbeiten)

Datenflusskontrolle
(hochsichere Gateways)

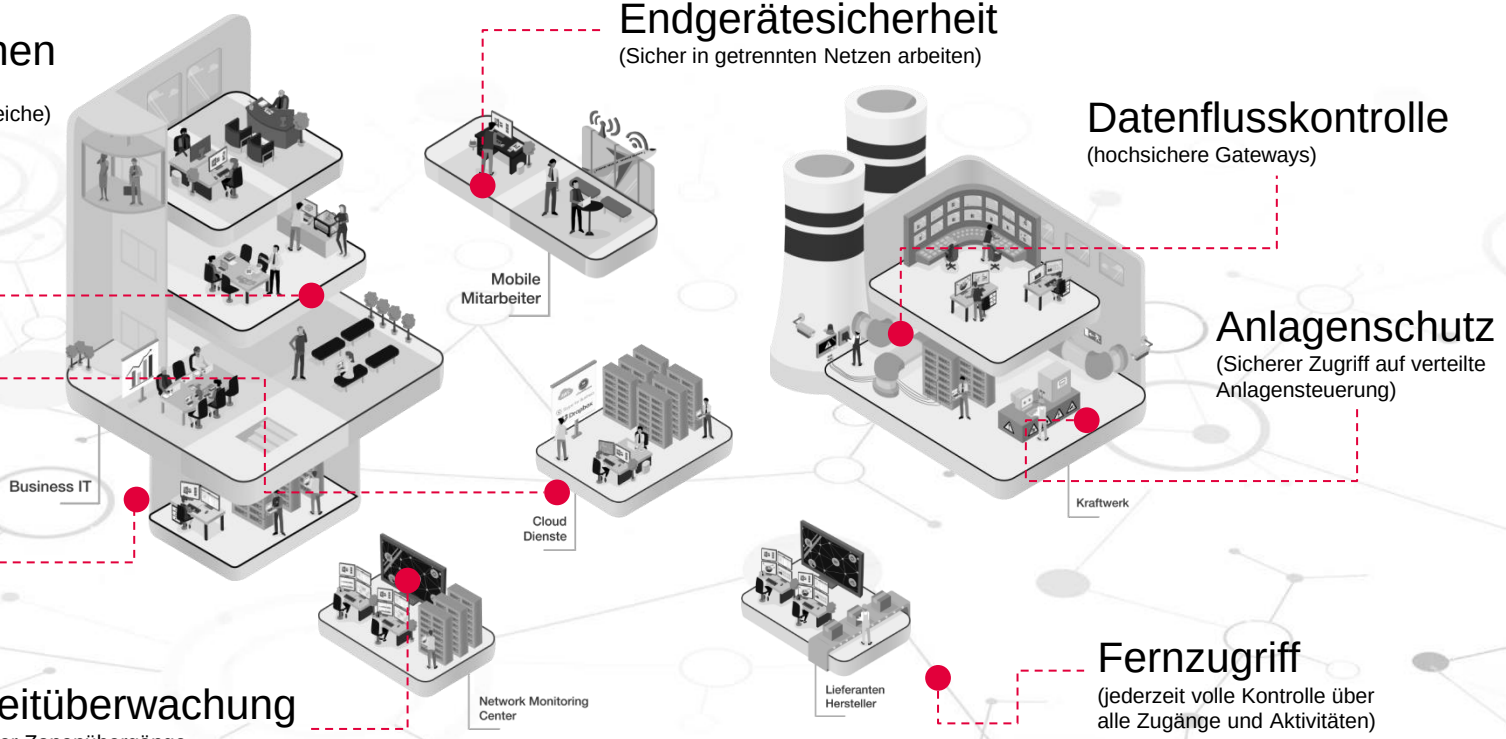
Cloudanbindung
(geschützte Datenablage und Nutzung externer Dienste)

Anlagenschutz
(Sicherer Zugriff auf verteilte Anlagensteuerung)

Standortvernetzung
(geschützter Datentransfer zwischen Standortnetzen)

Echtzeitüberwachung
(Kontrolle der Zonenübergänge und Erkennung von Angriffen)

Fernzugriff
(jederzeit volle Kontrolle über alle Zugänge und Aktivitäten)



secunet

Schutz und Absicherung IT-gestützter Geschäftsprozesse

Security Infrastructures

+ IT-Sicherheitsarchitekturen
+ IT-Sicherheitskonzepte
+ IT-Sicherheitslösungen
+ SINA Produktfamilie
+ secunet safe surfer
+ Netzwerküberwachung in Echtzeit
+ Industrie Konnektor

Pentest & Consulting

+ Penetrationtests
+ Sicherheitsmanagement (ISMS)
+ Audit & Revision
+ Datenschutzmanagement
+ Sicherheitsanalysen
+ Sensibilisierung

KEYs & IDENTITIES

+ eHealth Konnektor
+ secunet PKI Suite
+ eIDAS-Lösungen

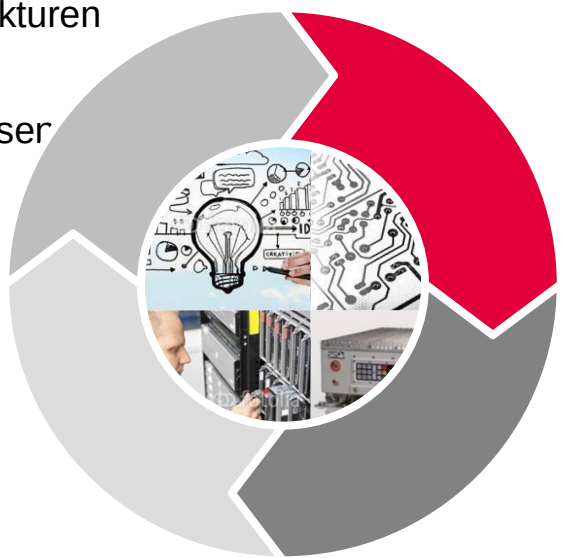
Was wir für Sie leisten

Beratung und Konzeption

- Sicherheitsdesign und -architekturen
- Sicherheitskonzepte
- Sicherheit in kritischen Prozessen
- IT-Grundschutz / ISMS
- Penetrationstests

Service

- Support, Wartung und Betrieb
- Schulung und Training
- Managed Security Services und Monitoring



Entwicklung

- Zugelassene Kryptolösungen
- PKI (eID PKI Suite)
- Biometrische Identifikations-systeme
- Kundenspezifische Soft- und Hardwareprodukte
- Sicherheit für Webanwendungen

Integration

- Sichere Netzinfrastrukturen und Arbeitsplätze
- SINA Produktportfolio
- Elektronische VS-Bearbeitung
- secunet safe surfer

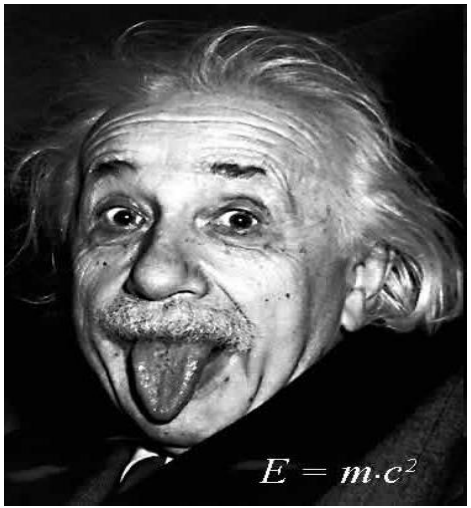
Live-Demo „Wir alle sind Opfer“

secunet

Das Problem

Die Welt wird nicht bedroht von den Menschen, die böse sind,

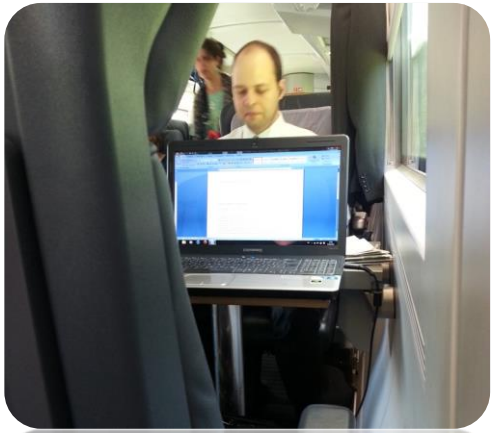
sondern von denen, die das Böse zulassen.



Albert Einstein
14.03.1879 - 18.04.1955
deutscher Physiker und Nobelpreisträger

Live Demo

Unachtsamkeit mit Folgen



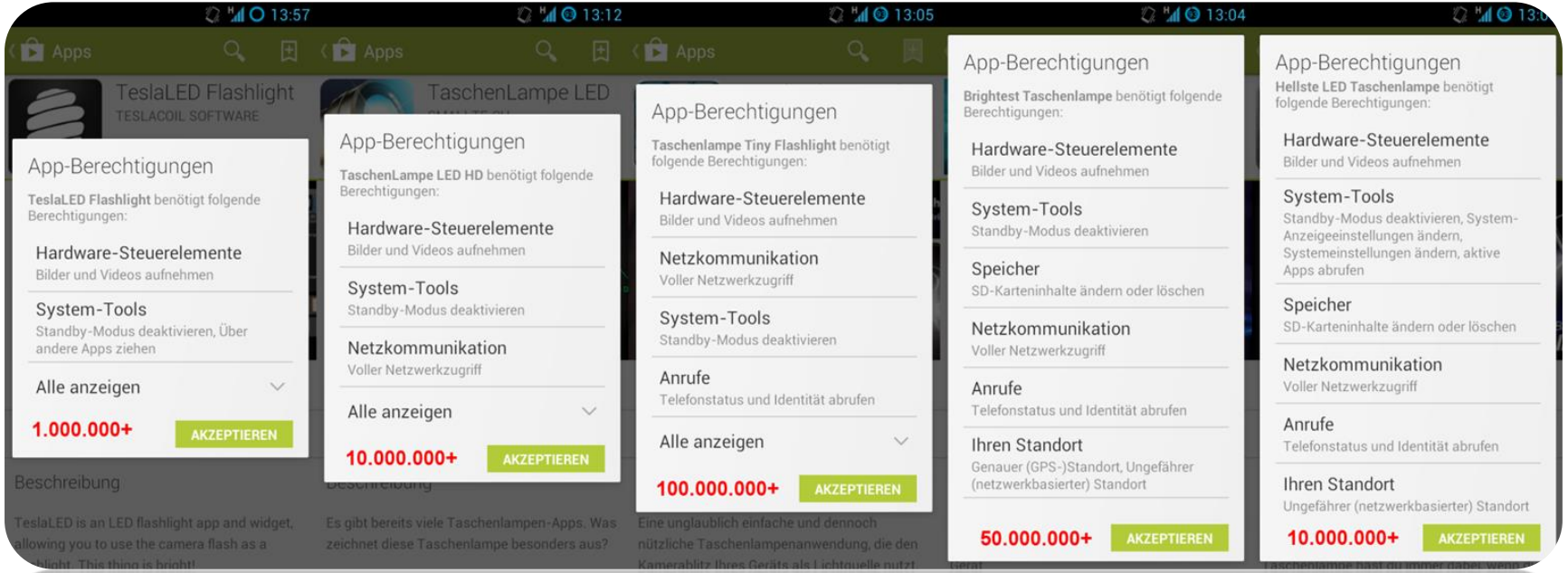
Quelle: Linnemann, secunet

secunet

Hacken ist (k)ein Kinderspiel

Quelle:
http://www.huffingtonpost.com/2013/09/11/iphone-fingerprint-child_n_3907107.html

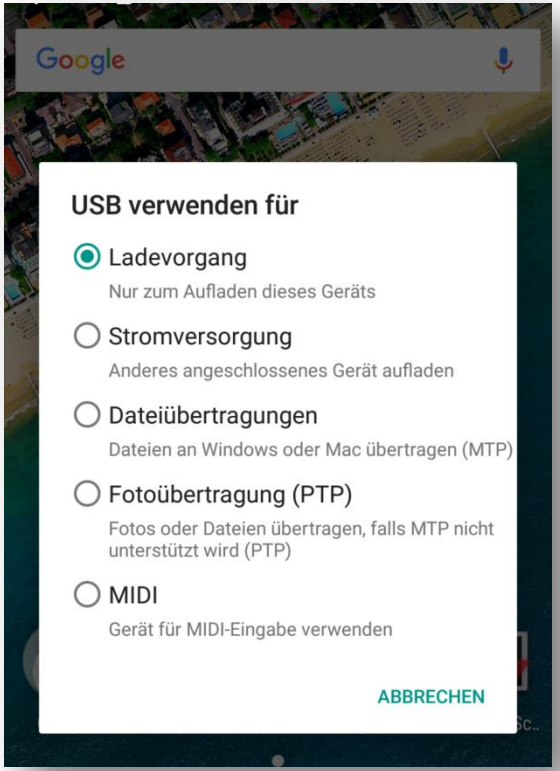
Warum Ihre Taschenlampe surfen kann …



Quelle: Jungbauer, secunet

secunet

„Vertrauen“ ist gut, „nicht vertrauen“ ist besser…



Quelle: Jungbauer, secunet

Erkenntnis

Quelle: Internet

secunet

secunet Security Networks AG

Wir schützen vernetzte Infrastrukturen.

info@secunet.com