Cybercrime vs. Selbstdatenschutz

Angriffsvektoren und Schutzmaßnahmen, Live ...

Prof. Dr. Thomas Städter

Gefahren für das informationelle Selbstbestimmungsrecht

„Daten sind das Öl des 21. Jahrhunderts“

[Gross-Selbeck, 2015]

- Werbung als Geschäftsgrundlage, Weiterverkauf von Daten und Analysen
- Daten(schutz) im Wandel der Mobilität

„If you're not paying for something, you're not the customer, you're the product being sold.“

[Andrew Lewis]

Paradigmenwechsel in der IKT

- „data-driven economy“: Geschäftsmodelle beruhen auf der Sammlung von Daten
- Konzentration und Monopolbildung, immer weniger „Big Player“
- Rechtsordnungen sind grundsätzlich national ausgerichtet, Datenverarbeitung ist aber global

Cybercrime ...

Cybercrime Bundeslagebild

Ransomware / Verschlüsselungstrojaner

- Digitale Erpressung

DDoS (Distributed Denial of Service)

- Fehlerhafte Heimvernetzungen
- Angriffe auf digitale Infrastrukturen

Cybercrime-as-a-Service

- Bereitstellung von Botnetzen für verschiedenste kriminelle Aktivitäten
- DDoS-Attacken
- Malware-Herstellung und Verteilung
- Datendiebstahl

Doxing

- Veröffentlichung privater Daten zum Schaden einer Person

[vgl. Bitkom, 2018, 2019; BSI, 2018; Symantec, 2017]

Weitere Entwicklungen

Interview Markus Hartmann, Oberstaatsanwalt:

Wie schätzen Sie die weiteren Entwicklungen auf dem Gebiet Cybercrime ein?

„Es wird nicht weniger. Und leider auch nicht einfacher. Wir sehen zunehmend zielgerichtete, hochkomplexe Kompromittierungen und Angriffe aus dem Graubereich zwischen organisierter und drittstaatlich induzierter Cyberkriminalität. Für die Strafverfolger ist es eine Herausforderung, ihre Handlungsfähigkeit in diesem Umfeld zu bewahren...

Ich wünsche mir aus den Erfahrungen unserer Ermittlungsverfahren, dass die Unternehmen mehr in qualifizierte Sicherheitsmaßnahmen investieren und verstehen, dass Cybersicherheit nicht schon mit dem Kauf von Produkt X oder der Anschaffung von Appliance Y gewährleistet ist. Cybersicherheit ist eine Dauerbaustelle.“

[iX 9/2018]

Awareness

„Die Frage ist nicht, ob man Sie angreifen wird, sondern wann ...“

[Cal Leeming]

Schadensursachen

- Erfolgreiche, kriminelle Geschäftsmodelle einerseits,
- Mangelndes Cybersicherheitstraining andererseits.

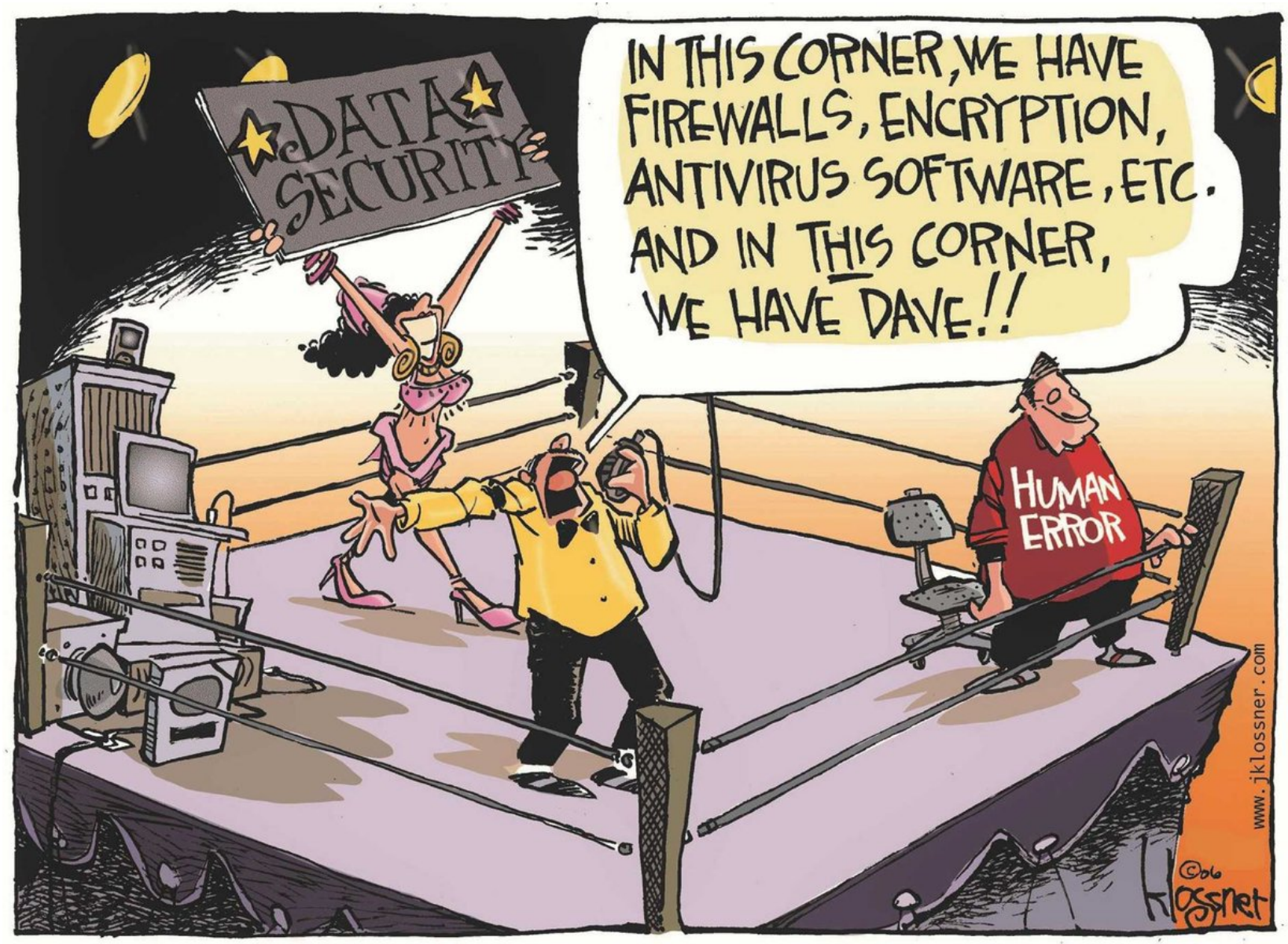
Maßnahmen

- Aufklärung, Aufklärung, ...
- Schulen
- Cybersicherheit-Events mit unabhängigen Experten
- Red Team Assessments
- Haftung von IT-Dienstleistern

Selbstdatenschutz

- Wie können wir uns selbst schützen?
- WIE kommuniziere ich WAS und auf WELCHEM Kanal?

Generalprobe für die Bedrohungen des 21. Jahrhunderts



Schwachstelle

- Verwundbarer (vulnerable) Punkt eines IT-System, durch den Sicherheitsziele umgangen werden können

Bedrohung

- liegt vor, wenn darauf abgezielt wird, eine oder mehrere Schwachstellen eines IT-Systems zu nutzen, die zu einem Verlust der Authentizität, der Verfügbarkeit, der Vertraulichkeit oder der Integrität führen

Risikoszenario (nach ISO 27001/27005) oder Gefährdung (nach BSI Grundschutz)

- liegt vor, wenn eine Schwachstelle auf eine Bedrohung trifft

Angriff

Unautorisierter Zugriff oder Zugriffsversuch auf ein IT-System und die darin gespeicherten und verarbeiteten Objekte

Arten von Angriffen

Passiv - unautorisierte Informationsgewinnung

Aktiv - unautorisierter Eingriff in Daten(objekte)

Angriffsmethoden

Maskieren

Subjekt täuscht die Identität eines anderen Subjekts vor

Abhören

Ein Subjekt erfasst unautorisiert Informationen

Autorisierungsverletzung

Ein Subjekt nutzt unautorisiert Dienste oder Ressourcen

Informationsverlust und -modifikation

Objekte werden modifiziert oder unbrauchbar gemacht

Informationsfälschung

Modifikation von Informationen unter falscher Identität

Abstreitbarkeit

Beteiligung an einer Transaktion wird abgestritten

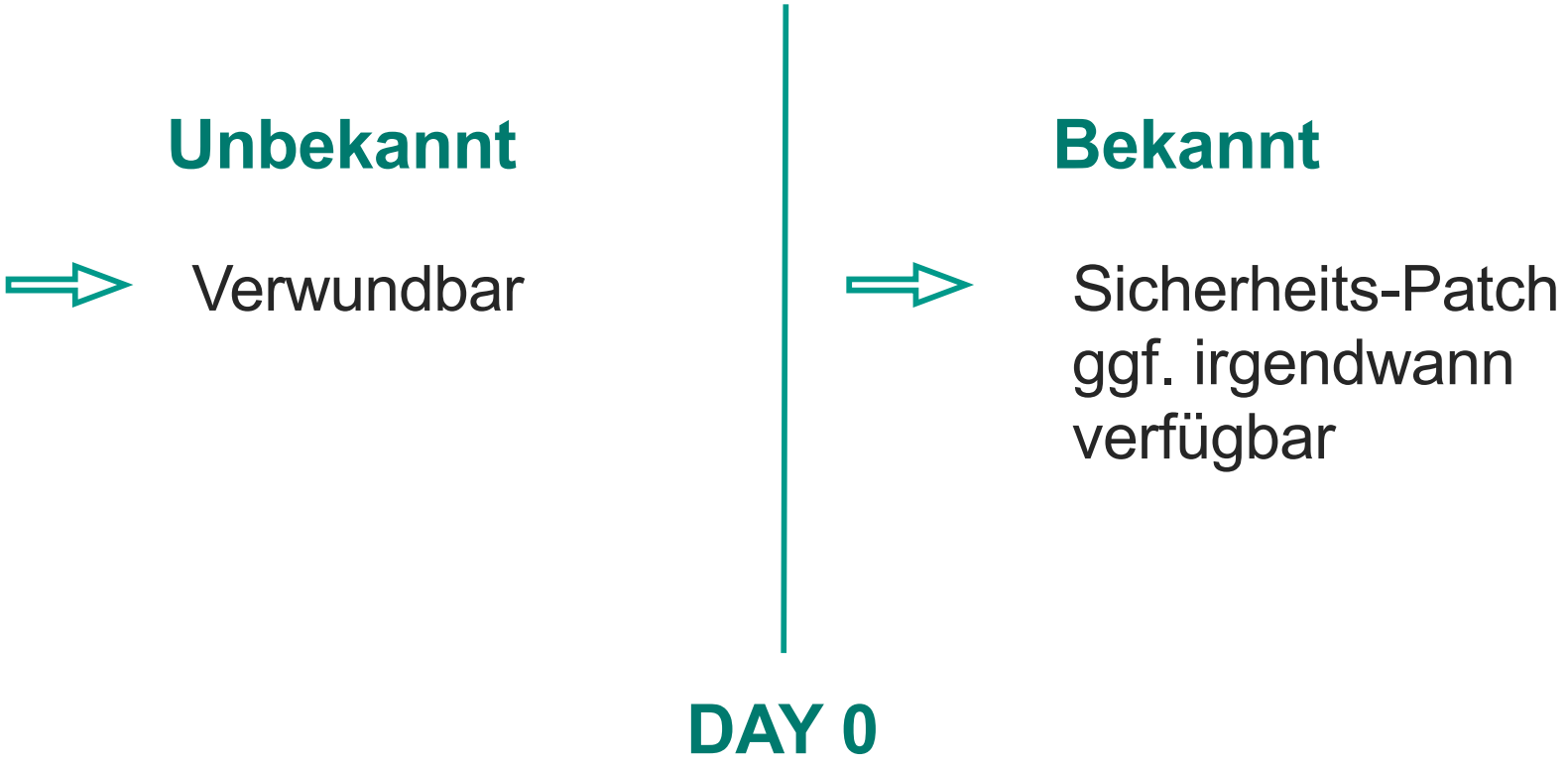
Sabotage

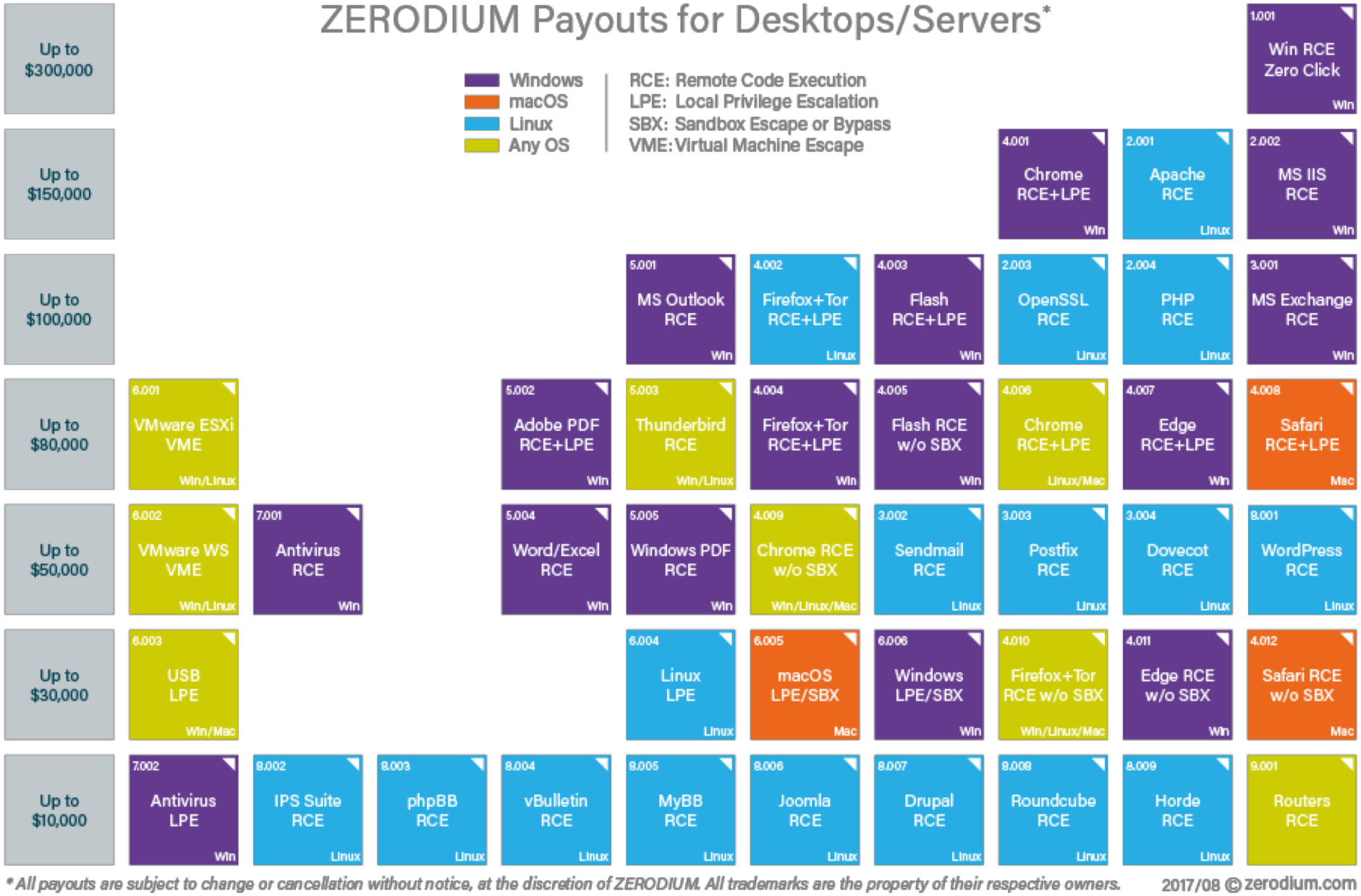
Manipulation der Verfügbarkeit / Funktionsfähigkeit des Systems

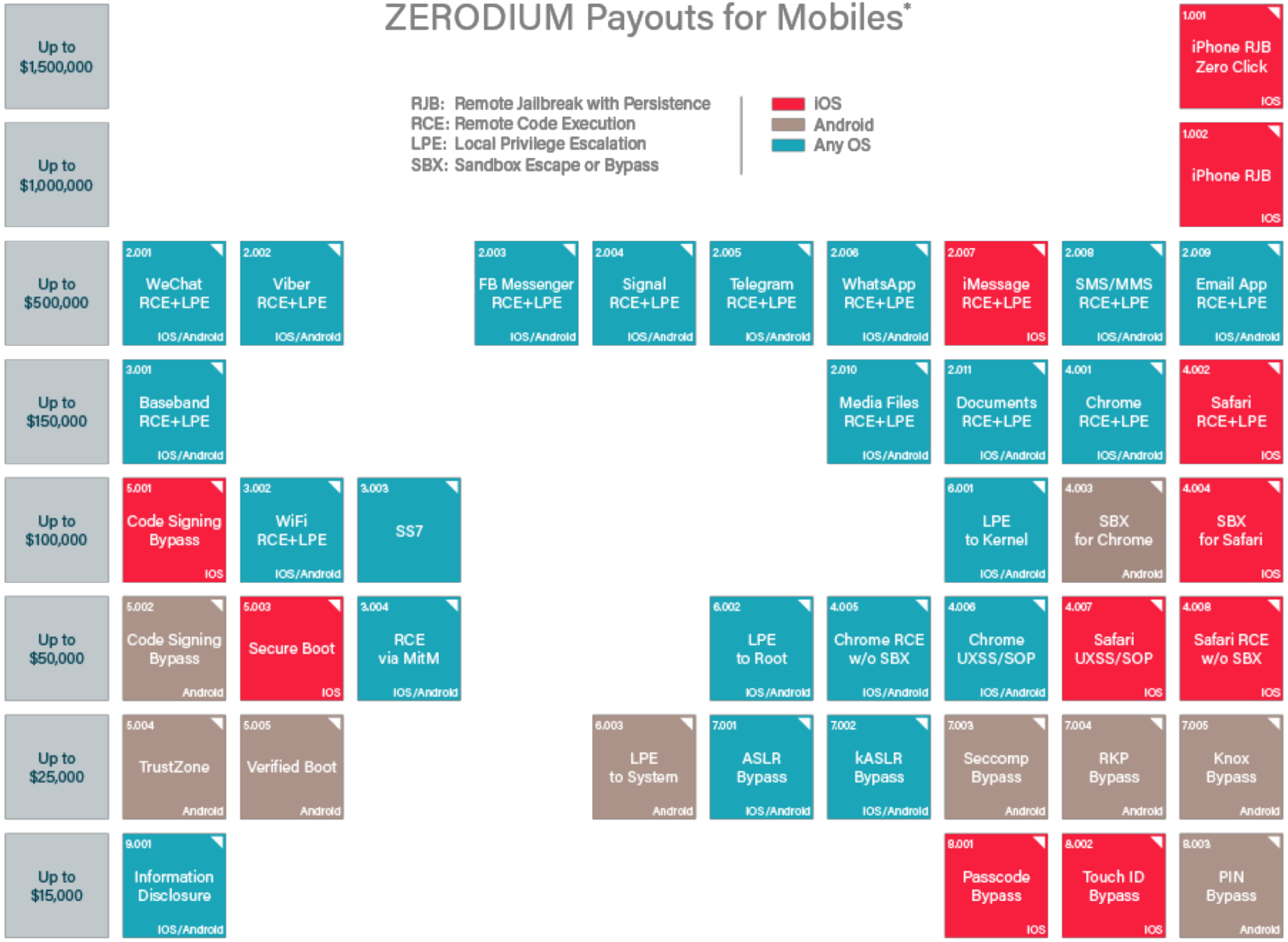
Doxing

Veröffentlichung privater Daten zum Schaden einer Person

Sicherheitslücken




ZERODIUM Payouts for Desktops/Servers*
Windows
macOS
Linux
Any OS
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
VME: Virtual Machine Escape
Up to $300,000
1.001 Win RCE Zero Click Win
Up to $150,000
4.001 Chrome RCE+LPE Win
2.001 Apache RCE Linux
2.002 MS IIS RCE Win
Up to $100,000
5.001 MS Outlook RCE Win
4.002 Firefox+Tor RCE+LPE Linux
4.003 Flash RCE+LPE Win
2.003 OpenSSL RCE Linux
2.004 PHP RCE Linux
3.001 MS Exchange RCE Win
Up to $80,000
6.001 VMware ESXi VME Win/Linux
5.002 Adobe PDF RCE+LPE Win
5.003 Thunderbird RCE Win/Linux
4.004 Firefox+Tor RCE+LPE Win
4.005 Flash RCE w/o SBX Win
4.006 Chrome RCE+LPE Linux/Mac
4.007 Edge RCE+LPE Win
4.008 Safari RCE+LPE Mac
Up to $50,000
6.002 VMware WS VME Win/Linux
7.001 Antivirus RCE Win
5.004 Word/Excel RCE Win
5.005 Windows PDF RCE Win
4.009 Chrome RCE w/o SBX Win/Linux/Mac
3.002 Sendmail RCE Linux
3.003 Postfix RCE Linux
3.004 Dovecot RCE Linux
8.001 WordPress RCE Linux
Up to $30,000
6.003 USB LPE Win/Mac
6.004 Linux LPE Linux
6.005 macOS LPE/SBX Mac
6.006 Windows LPE/SBX Win
4.010 Firefox+Tor RCE w/o SBX Win/Linux/Mac
4.011 Edge RCE w/o SBX Win
4.012 Safari RCE w/o SBX Mac
Up to $10,000
7.002 Antivirus LPE Win
8.002 IPS Suite RCE Linux
8.003 phpBB RCE Linux
8.004 vBulletin RCE Linux
8.005 MyBB RCE Linux
8.006 Joomla RCE Linux
8.007 Drupal RCE Linux
8.008 Roundcube RCE Linux
8.009 Horde RCE Linux
9.001 Routers RCE
*All payouts are subject to change or cancellation without notice, at the discretion of ZERODIUM. All trademarks are the property of their respective owners.
2017/08 © zerodium.com


ZERODIUM Payouts for Mobiles*
RJB: Remote Jailbreak with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
iOS
Android
Any OS
Up to $1,500,000
1.001 iPhone RJB Zero Click iOS
Up to $1,000,000
1.002 iPhone RJB iOS
Up to $500,000
2.001 WeChat RCE+LPE iOS/Android
2.002 Viber RCE+LPE iOS/Android
2.003 FB Messenger RCE+LPE iOS/Android
2.004 Signal RCE+LPE iOS/Android
2.005 Telegram RCE+LPE iOS/Android
2.006 WhatsApp RCE+LPE iOS/Android
2.007 iMessage RCE+LPE iOS
2.008 SMS/MMS RCE+LPE iOS/Android
2.009 Email App RCE+LPE iOS/Android
Up to $150,000
3.001 Baseband RCE+LPE iOS/Android
2.010 Media Files RCE+LPE iOS/Android
2.011 Documents RCE+LPE iOS/Android
4.001 Chrome RCE+LPE iOS/Android
4.002 Safari RCE+LPE iOS
Up to $100,000
5.001 Code Signing Bypass iOS
3.002 WiFi RCE+LPE iOS/Android
3.003 SS7
6.001 LPE to Kernel iOS/Android
4.003 SBX for Chrome Android
4.004 SBX for Safari iOS
Up to $50,000
5.002 Code Signing Bypass Android
5.003 Secure Boot iOS
3.004 RCE via MitM iOS/Android
6.002 LPE to Root iOS/Android
4.005 Chrome RCE w/o SBX iOS/Android
4.006 Chrome UXSS/SOP iOS/Android
4.007 Safari UXSS/SOP iOS
4.008 Safari RCE w/o SBX iOS
Up to $25,000
5.004 TrustZone Android
5.005 Verified Boot Android
6.003 LPE to System Android
7.001 ASLR Bypass iOS/Android
7.002 kASLR Bypass iOS/Android
7.003 Seccomp Bypass Android
7.004 RKP Bypass Android
7.005 Knox Bypass Android
Up to $15,000
9.001 Information Disclosure iOS/Android
8.001 Passcode Bypass iOS
8.002 Touch ID Bypass iOS
8.003 PIN Bypass Android
* All payouts are subject to change or cancellation without notice, at the discretion of ZERODIUM. All trademarks are the property of their respective owners.
2017/08 © zerodium.com

Ursachen, Auswirkungen und Maßnahmen

Anwender

- Anwenderfehler, z.B. bei:
  - Phishing-E-Mails
  - USB-Sticks dubioser Herkunft
- Böswilliges Verhalten

Maßnahmen

- Aufklärung
- Identitätsmanagement
- Zugriffskontrollen
- Prinzipien für die Gewährleistung der Integrität
  - Need-to-Know-Prinzip
  - Separation-of-Duties-Prinzip
  - Rotation-of-Duties-Prinzip

Computer und IT

- Den größten Schaden verursacht i.d.R. nicht der Angriff, sondern die Ausfallzeit
- Imageschäden und Bußgelder (Art. 83 DSGVO)

Maßnahmen

- Anti-Viren-Lösungen reichen nicht
- TOMs gemäß Art. 32 DSGVO
- Business- Continuity-Lösung
- Disaster-Recovery-Plan
- Backup

Selbstdatenschutz

Endanwender haben meist wenig Einblick in das Thema IT-Sicherheit und interessieren sich auch kaum dafür.

Dabei kommt es nicht nur auf technische Faktoren an, auch der menschliche Faktor spielt eine wichtige Rolle.

Wie können wir uns selbst schützen?

WIE kommuniziere ich WAS und auf WELCHEM Kanal?

Demonstration zu IT-Sicherheit und aktivem Datenschutz

„PPP“ als generische Maßnahme

Passwörter

- Starke und individuelle Passwörter für unterschiedliche Dienste
- 2-Faktor-Authentifizierung

Patching

- Alter Grundsatz „never change a running system“ gilt nicht mehr
- Software-Updates sind unvermeidbar

Prävention

- Aufklärung und Schulung
- Technische und organisatorische Maßnahmen
- Notfallplan

Passwörter

Angriffsvektoren

- Informationsverlust bei IT-Dienstleistern
- Sniffing (Abhören) eines unverschlüsselten WLANs *
- Spear-Phishing in Kombination mit Social-Engineering *
- USB-Sticks fremder Herkunft *

Maßnahmen

- Prüfen der eigenen e-Mail-Adresse: www.HavelbeenPwned.com *
- Prüfen des Passworts *
- Passwort-Routine / Individuelles Schema entwickeln
  Stamm
  Plattform
  Zähler
- 2-Faktor-Authentifizierung aktivieren
- Nutzung eines VPN *

* Live Demo

Hackerparagraph - §202 StGB

Neben Computersabotage wird auch die Anwendung von Hackertools unter Strafe gestellt

Absatz C: Bereits der Besitz solcher Tools wird potentiell unter Strafe gestellt:

§202c StGB: Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach §202a oder §202b vorbereitet, indem er Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§202a, Abs. 2) ermöglichen, oder Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

Es liegt keine explizite Ausnahme für Sicherheitsprüfungen vor, deswegen ...

Bemerkung zur Rechtslage in Deutschland

WLAN-Sniffer: Das absichtliche Abhören oder Protokollieren von fremden Funkverbindungen ist verboten, sofern es vom Netzbetreiber nicht explizit erlaubt wurde.

Ungewolltes Abhören scheint nach dem deutschen Telekommunikationsgesetz erlaubt zu sein, jedoch ist eine Speicherung, Weitergabe oder Verwendung der so erlangten Daten ebenfalls nicht zulässig.

Entscheidung des BverfG vom 18.05.2009:

Im Rahmen von reinen Sicherheitstests ist nicht nur die Verwendung von „Dual use“-Software gestattet, es dürfen sogar Hacking-Tools verwendet werden.

Sicherheitstests: Vermeidung juristischer Probleme (1/2)

Empfehlungen des Bitkom:

Eindeutige Autorisierung von festgelegten Personen zur Testdurchführung durch das Management.

Die Durchführung solcher Tests ist in der Aufgabenbeschreibung dieser Personen enthalten.

Der Einsatz der Programme außerhalb dienstlicher Tätigkeit ist untersagt.

Das Einverständnis des Systemeigentümers muss vorliegen und der Test mitsamt Ablauf muss mit ihm abgesprochen sein.

Tests für interne oder externe Kunden benötigen einen schriftlichen Auftrag. Dieser Auftrag muss Art, Umfang und die zu testenden Systeme benennen, sowie die beauftragten Mitarbeiter namentlich enthalten.

Während der Testdurchführung sind aussagekräftige Protokolle zu führen.

Die Testergebnisse und Informationen sind sicher zu verwahren und unterliegen der Geheimhaltung.

Sicherheitstests: Vermeidung juristischer Probleme (2/2)

Werden Tests außerhalb der internen Räumlichkeiten durchgeführt, sollte eine Kopie des schriftlichen Auftrags als Nachweis für strafrechtliche Ermittlungen vor Ort mitgeführt werden.

Die zutreffenden gesetzlichen Regelungen (BDSG, Fernmeldegeheimnis nach dem TKG) sind zu beachten.

Bei versehentlichen Schädigung Dritter ist der Test unverzüglich abzubrechen und der Geschädigte ist zu informieren. Die Ursache ist zu ermitteln und zu dokumentieren, besonders warum nicht von einer Schädigung Dritter ausgegangen wurde.

Ergeben sich in einem Test Zugriffsmöglichkeiten auf Daten außerhalb der Autorisierung, darf auf diese Daten nicht zugegriffen werden.

VPN (Virtual Private Network)

Datenverkehr zwischen zwei Teilnehmern im VPN wird verschlüsselt

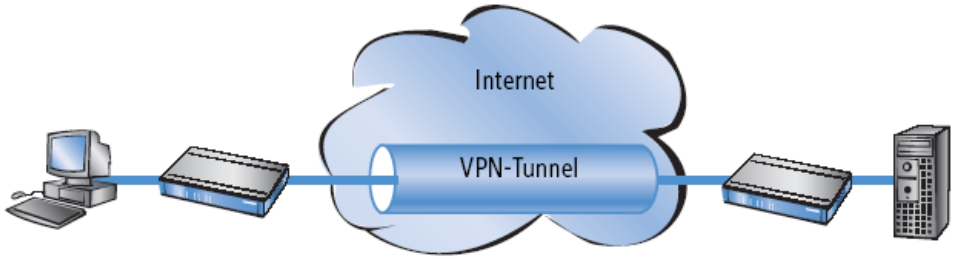
Während der Übermittlung sind die Daten für Dritte unlesbar

Tunnel

- Sichere Verbindungen innerhalb eines öffentlichen IP-Netzes
- Offen nur am Anfang und am Ende, dazwischen perfekt abgeschirmt
- VPN-Tunnel über Festverbindung, Wählverbindung und IP-Netzwerk
- Authentifizierung der Teilnehmer
- Erkennen und Ablehnen „nachgespielter“ Pakete (Antireplay)

Gängige Protokolle und Implementierungen

- IPSec
- TLS (OpenVPN)



[Lancom]

Angriffsvektoren

- Beobachtung, Aufdeckung, Identifizierung, Verknüpfung, Profiling
- Phishing
- USB-Stick fremder Herkunft
- Diebstahl von unverschlüsselten Datenträgern
- Datendiebstahl bei IT-Dienstleistern
- Verschlüsselung von Daten (z.B. WannaCry, Emotet u.a.)

Maßnahmen

- Spurenarmes Surfen *
- Nutzung von Mix-Servern / Tor *
- Datenträgerverschlüsselung *
- „Vertrauen ist gut, Kontrolle ist besser“ [Lenin]
- Sicherer Cloud-Speicher *
- Backups

Spurenarmes Surfen, Unterbinden von Tracking

Datensparsame Suchmaschinen:

https://startpage.com
https://duckduckgo.com

Deaktivierung von Google Analytics

https://tools.google.com/dlpage/gaoptout?hl=de

Google: Suchanfragen im Webprotokoll entfernen

https://history.google.com/

Browser-Addons, z.B.:

- AdBlock Plus
- Disconnect
- NoScript
- uMatrix
- Ghostery
- Privacy Badger
- Click to Play
- HTTPS Everywhere
- Mailvelope

Anonymisierungsdienst

- Anonymität und Abhörsicherheit
- Hidden Service im Darknet
- Für normale Anwender könnte sich de facto das Risiko erhöhen, tatsächlich überwacht und ausspioniert zu werden!

Das Darknet als Einkaufsmeile

- Schwarzmarkt-Plattformen mit funktionierenden Treuhändler-Modellen
- Links zu den großen und kleinen Kryptomärkten in "Branchen"- Blogs wie Deepdotweb.com oder in Listen auf der Diskussionsplattform Reddit
- Dark Web Map: https://www.hyperiongray.com/dark-web-map/

Darknet

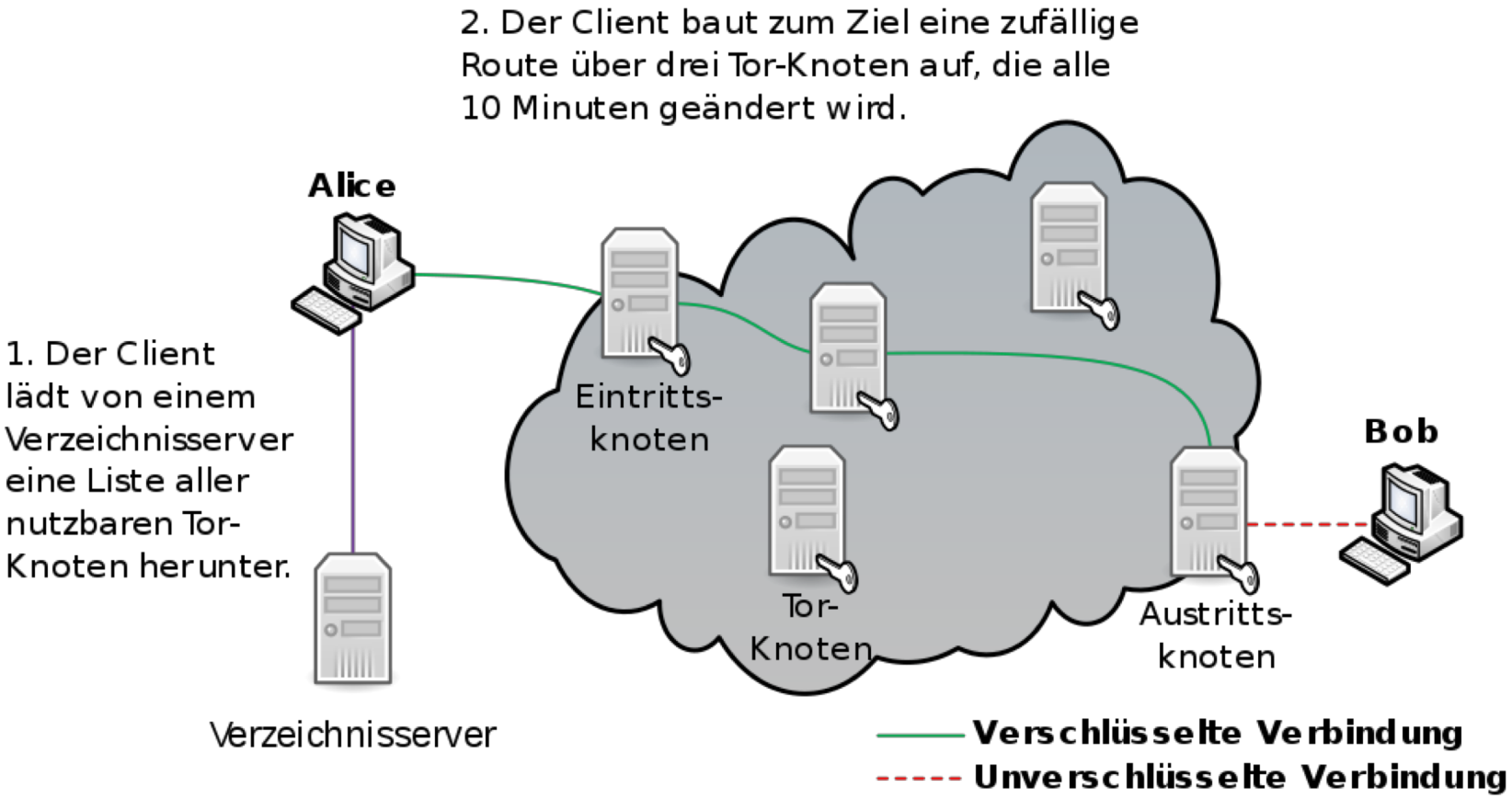
Einerseits

- Oberbegriff für Overlay-Netze, die das Internet lediglich als Transport-Medium nutzen und darauf eine eigene, auf Anonymität der Teilnehmer abzielende Infrastruktur aufbauen.
- „Das Darknet ist das Internet, wie man es sich eigentlich wünschen würde. Ein Netz ohne Zensur und Überwachung, mit all seinen Vor- und Nachteilen“. [Linus Neumann]

Andererseits

- Illegale Inhalte und Angebote
- werden auch von Google nicht erfasst.

Tor - Arbeitsweise



[Saman Vosoghi, Wikimedia Commons; Copyrighted free use]

Hidden Services im Tor-Netz *

Facebook via Hidden Service

- https://www.facebookcorewwwi.onion

Hidden Services / The Hidden Wiki

Suchmaschine für Tor Hidden Services / not Evil

Suchmaschine für Tor Hidden Services / Torch

Sicherer Briefkasten von heise Investigativ

- http://sq4lecqyx4izcpkp.onion/

Verschlüsselung von Datenträgern

Betriebssystem-spezifische Verfahren:

- BitLocker für MS-Windows
- FileVault für Mac OSX

Plattform-übergreifende, offene Verschlüsselungslösung mit VeraCrypt

- Derzeit eines der wenigen Krypto-Projekte, die nach wie vor großes Vertrauen genießen
- Professioneller Code-Review hat bislang keine Schwächen offenbart
- Umsetzung einer „Glaubhaften Abstreitbarkeit“

Sicherheit für Notebooks, Tablets und SmartPhones (1/2)

Basisschutz

- Geräte nie unbeaufsichtigt liegen lassen
- Zugriffsschutz aktivieren
- Sicherheitsupdates (aktuelles System)
- Virenscanner
- Personal Firewall
- Datenträger verschlüsseln (z.B. BitLocker bei MS-Windows, FileVault bei MacOSX)

Sicherungskopien

- Regelmäßige Sicherungskopien der Daten anfertigen
- Betriebssystem-spezifische Anwendungen (z.B. Time Machine bei Mac OSX) für Backups auf externen Datenträgern
- Sicheres, verschlüsseltes Backup in der Cloud (z.B. mit BoxCryptor)

Sicherheit für Notebooks, Tablets und SmartPhones (2/2)

Sicherer Umgang mit Wechseldatenträgern

- Verschlüsseln sensibler Informationen (z.B. mit VeraCrypt)
- Richtige Lagerung der Speichermedien
- Richtiges Löschen/Sicheres Löschen mit Daten-Shreddern

„Freigaben“ auf Ordner/Dateien

- Nur bei Bedarf aktivieren
- Zugriffe kontrollieren

Nutzung von Apps

- Sensibler und bedachter Umgang mit Apps
- Kostenlose, werbefinanzierte Apps teils unbekannter Herkunft vs. Apps von vertrauenswürdigen Anbietern
- Einkauf nur in einem verifizierten Store
- Auf Datenschutzbestimmungen achten

„Sicherer“ Cloud-Speicher

Risiken:

- Datenschutz, Verlust, Datenintegrität, Compliance, ...
- Wo werden Daten Wie lange gespeichert und von Wo wird auf diese Daten zugegriffen?
- Wann und Wie wird unerlaubtes Eindringen und unerlaubter Zugriff auf Systeme und Daten gemeldet?

Maßnahmen

- Sicherheitsbedingungen und -vorkehrungen der Anbieter prüfen
- Kostenlose Angebote kritisch hinterfragen
- Kennwortrichtlinien für das Internet beachten
- Regelmäßige lokale Sicherungskopien erstellen
- Auf Datenschutzbestimmungen achten!
- Verantwortungsbewusster Umgang mit sensiblen Daten

„Sichere“ Cloud-Lösungen

Tokenization oder Obfuscation

- Secure Hashing
- Erzeugung von Ersatzwerten für sensitive Daten
- In einer Mapping-Tabelle bei einer „Trusted 3rd Party“ wird gespeichert, welcher zu sichernde Wert welchem Ersatzwert zugeordnet ist.
- Im Unternehmen können alle Stellen auf diese Mapping-Tabelle zugreifen, die Zugriff auf die Daten haben müssen.

CASB (Cloud Access Security Broker)

- Einhaltung der Datenschutzgesetze und der Compliance-Vorgaben zum Speicherort von Daten

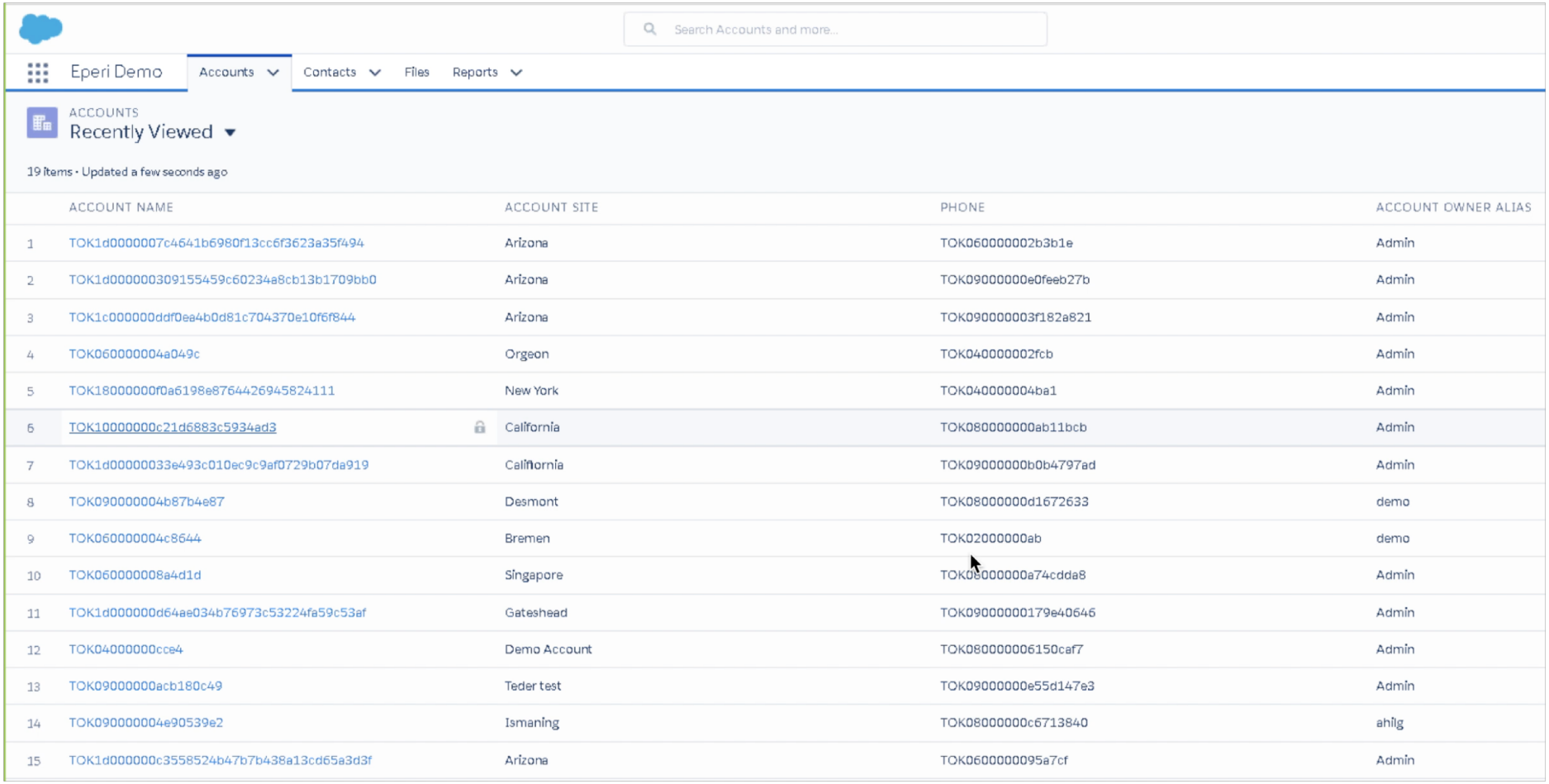
CDP (Cloud Data Protection)

- Schützt die Daten in der Cloud durch Verschlüsselung oder Tokenisierung
- CDP fängt sensible Daten noch On-Premises ab und ersetzt sie durch ein zufälliges Token oder einen verschlüsselten Wert
- Einhaltung von Datenschutzvorgaben und Compliance-Anforderungen
- Daten sind für Angreifer, die außerhalb des Unternehmens darauf zugreifen, nutzlos.

Anonymisierte Daten fallen nicht mehr in den Geltungsbereich des Datenschutzes!

Office 365 über CASB (BoxCryptor)

SalesForce über CASB (eperi)



	ACCOUNT NAME	ACCOUNT SITE	PHONE	ACCOUNT OWNER ALIAS
1	TOK1d0000007c4641b6980f13cc6f3623a35f494	Arizona	TOK060000002b3b1e	Admin
2	TOK1d000000309155459c60234a8cb13b1709bb0	Arizona	TOK09000000e0feeb27b	Admin
3	TOK1c000000ddf0ea4b0d81c704370e10f6f844	Arizona	TOK090000003f182a821	Admin
4	TOK060000004a049c	Orgeon	TOK040000002fcb	Admin
5	TOK18000000f0a6198e8764426945824111	New York	TOK040000004ba1	Admin
6	TOK10000000c21d6883c5934ad3	California	TOK080000000ab11bcb	Admin
7	TOK1d00000033e493c010ec9c9af0729b07da919	California	TOK09000000b0b4797ad	Admin
8	TOK090000004b87b4e87	Desmont	TOK08000000d1672633	demo
9	TOK060000004c8644	Bremen	TOK02000000ab	demo
10	TOK060000008a4d1d	Singapore	TOK09000000a74cdda8	Admin
11	TOK1d000000d64ae034b76973c53224fa59c53af	Gateshead	TOK090000000179e40646	Admin
12	TOK04000000cce4	Demo Account	TOK080000006150caf7	Admin
13	TOK09000000acb180c49	Teder test	TOK09000000e55d147e3	Admin
14	TOK090000004e90539e2	Ismaning	TOK08000000c6713840	ahilg
15	TOK1d000000c3558524b47b7b438a13cd65a3d3f	Arizona	TOK0600000095a7cf	Admin

Regulierung des Internets?

"Die DSGVO ist nicht perfekt, aber es ist ein guter erster Aufschlag der Politik",

[Bruce Schneier, 2019; Veranstaltung im Rahmen der Münchner Sicherheitskonferenz]

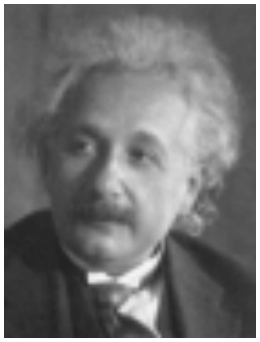
- "smarte Regulierung“ des Netzes
- mehr Technikexperten in der Politik
- Stärkung der Medienkompetenz
- "Es ist unser Job, die Sachen so sicher zu machen, dass der normale Nutzer sicher ist“
- Wenn ich wieder ins Flugzeug steige, "checke ich den Motor nicht, ich schaue nicht nach Software-Updates und ich prüfe auch nicht, ob der Pilot seine Fortbildungen besucht hat.“
- Das alles regelt der Staat, damit man sicher reisen kann. "Warum soll das Internet die Ausnahme sein?"

THANK YOU

MERCI

DANKE

GRACIAS



Die Welt wird nicht bedroht von den Menschen, die böse sind, sondern von denen, die das Böse zulassen.

[Albert Einstein]