

Aktuelle IT-Security-Risiken und mögliche Gegenmaßnahmen



InfoTechDay, 16.11.2023 14:00 (UTC+1), Geinberg

Univ.-Prof. Dr. **René Mayrhofer**

Institut für Netzwerke und Sicherheit und LIT Secure and Correct Systems Lab, JKU Linz
Christian Doppler Labor für Private Digitale Authentifizierung in der Physischen Welt (CDL Digidow)

IT-Sicherheit: Wahrnehmung vs. Realität



No Silver Bullet – Keine Wundermittel!



Aktuelle Angriffstypen

**Kopieren / veröffentlichen
vertraulicher Daten**

Motivation

- (Industrie-) Spionage
- Identitätsdiebstahl
(inkl. Finanztransaktionen)
- Erpressung

Aktuelle Angriffstypen

Kopieren / veröffentlichen vertraulicher Daten

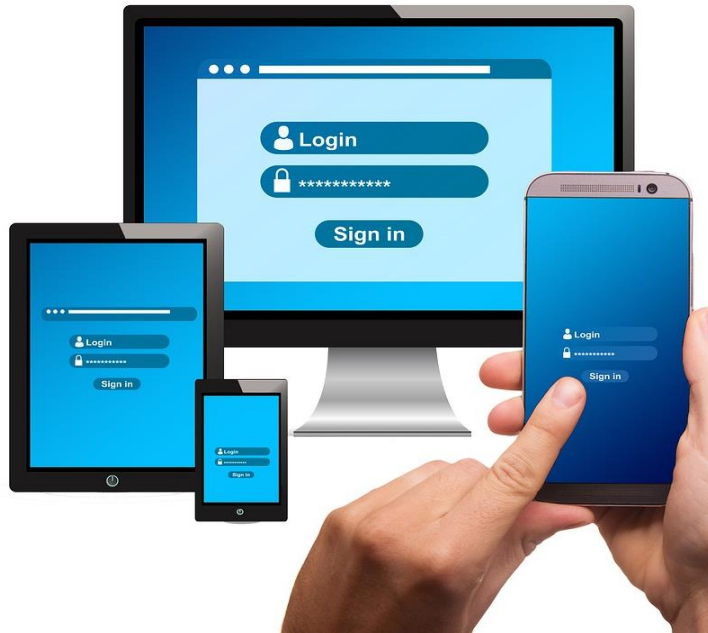
Motivation

- (Industrie-) Spionage
- Identitätsdiebstahl
(inkl. Finanztransaktionen)
- Erpressung

Gegenmaßnahmen

- Account-Sicherheit
- Verschlüsselung
(*in-transit* und *at-rest*)

Authentifizierung



Empfehlungen aus der Praxis:

- **Passwortmanager mit Client-Integration verwenden!**
- Passwörter alleine sind zu wenig (unabhängig von Komplexität ist **Phishing** das Hauptproblem) → **2FA**
 - ideal: **FIDO2** / U2F (per USB, NFC oder eingebettet)
 - ok: TOTP (Achtung: ab hier abwärts **kein Phishing-Schutz**)
 - in Ordnung: HOTP
 - nur wenn nicht anders möglich: SMS
- Wenn möglich, **biometrische Authentifizierung** (Fingerprint)

Login Locations



Clients außerhalb des eigenen Netzwerkes

- Ist das eigene Netzwerk wirklich viel sicherer?
 - Drucker, Projektoren, Bildschirme etc. im LAN
 - Ungepatchte Laptops, „gefundene“ USB-Sticks, etc.
 - VPNs sind eine Möglichkeit, besser ist aber **Zero-Trust Policy in Bezug auf Client-Netzwerke**
- Login von verschiedenen Locations
 - **Zusätzlicher Schritt (2FA Bestätigung) bei Wechsel?**
 - **Definiere „Location“:** IP-Adresse, AS-Nummer, Endgerät, Browser-Session, etc.
- Mitarbeiter:innen oder Kund:innen aus „problematischen“ (zensurierten) Netzwerk-Locations?
 - Logins über Tor ohne sinnvolle IP-Zuordnung
 - Braucht bewusste Entscheidung zum Umgang

FIDO2 Tokens funktionieren

- KrebsOnSecurity: *Google: Security Keys Neutralized Employee Phishing*
<https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/>

“We have had no reported or confirmed account takeovers since implementing security keys at Google”

- Viele Webservices bieten inzwischen FIDO2/WebAuthn an: Google, Github, etc.
- Immer mehr selbst gehostete implementieren es ebenfalls: Nextcloud, Gitlab, etc.

Aktuelle Entwicklungen zu eIDAS / EU-ID Wallets

- Hochaktuelle eIDAS-Verhandlungen im EU-Trilog
- Ziel:
 - (nationale) Smartphone-Wallets für digitale IDs
 - **Öffnung von eIDAS-Anmeldungen mit solchen digitalen IDs für Privatwirtschaft**
 - dediziertes Ziel: Single-Sign-On für Webanwendungen (ähnlich zu „Login with XYZ“)
 - aber auch z.B. starke KYC-Prüfungen
- Security- und Privacy-Mechanismen in aktuellem Draft
 - Selective Attribute Disclosure
 - Unlinkability of Transactions (aus der Sicht der prüfenden Instanzen, leider nur **optional**)
 - Unobservability (aus Sicht der Wallet-Provider)
- ID Austria wird diese Anforderungen implementieren (noch unklar ob in eAusweise-App)

Aktuelle Angriffstypen

Kopieren / veröffentlichen vertraulicher Daten

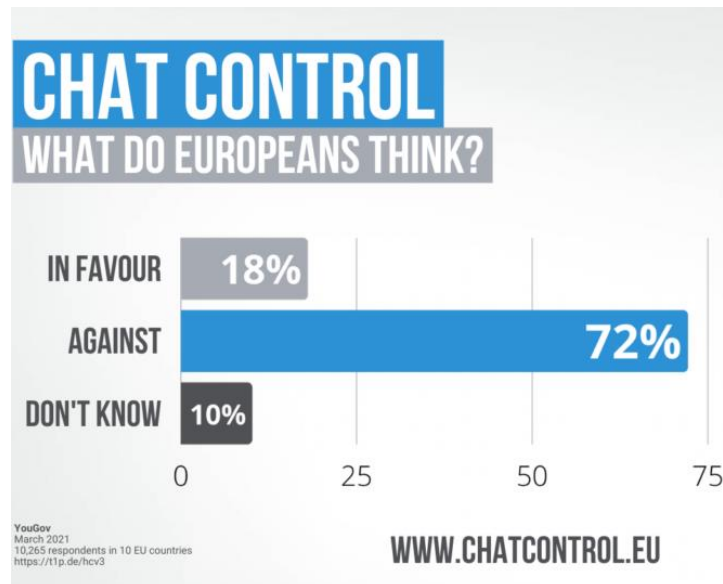
Motivation

- (Industrie-) Spionage
- Identitätsdiebstahl
(inkl. Finanztransaktionen)
- Erpressung

Gegenmaßnahmen

- Account-Sicherheit
- Verschlüsselung
(*in-transit* und *at-rest*)
- **Gar nicht sammeln**

ChatControl – und die Bedeutung für Firmenkommunikation



- Ebenfalls aktuelle Verhandlungen im EU-Trilog
- Pläne, verpflichtende Scanning-Module in Secure Messenger einzubauen
 - Wegen End-to-End-Encryption (E2EE) keine Überwachung auf Provider- und Anbieterseite möglich
 - Daher: *Client-Side Scanning (CSS)* mit Machine Learning
- Probleme:
 - Machine Learning hat immer Fehlerquote
 - Implementierung ist komplex, wird Softwarefehler haben
 - Slippery Slope: neues „böses“ Material in Datenbanken
- Mehr Details:
 - <https://www.patrick-breyer.de/beitraege/chatkontrolle/>
 - <https://www.ins.jku.at/chatcontrol/>

Aktuelle Angriffstypen

Kopieren / veröffentlichen vertraulicher Daten

Motivation

- (Industrie-) Spionage
- Identitätsdiebstahl (inkl. Finanztransaktionen)
- Erpressung

Gegenmaßnahmen

- Account-Sicherheit
- Verschlüsselung (*in-transit* und *at-rest*)
- **Gar nicht sammeln**

Manipulation bzw. Unbrauchbarmachung

Motivation

- Erpressung
- Kollateralschäden

OÖplus OBERÖSTERREICH

Angriff von Cyber-Erpressern auf mehr als 30 Unternehmen

Von Gerhild Niedoba 03. September 2021 00:04 Uhr

LINZ. Kriminelle schleusten Schadsoftware in Linzer IT-Firma ein, von dort verbreitete sie sich weiter auf Computersysteme von Kunden.

26. November 2020 Jens Stark*

Supply Chain Security: Angriff über die Lieferketten

Cyberkriminelle suchen sich gerne das schwächste Glied, um zuzuschlagen. Die immer komplexer werdenden Lieferketten bilden da eine wachsende Angriffsfläche. Doch damit nicht genug: Oft sitzt der Angreifer bereits in der Hardware und Software.

Software supply chain breaches are 'staggeringly high,' report finds

Kyle Wiggers
@Kyle_L_Wiggers

October 12, 2021 4:00 AM



Cyberangriff auf die USA

Der große Rundumschlag

Vorwürfe gegen Russland und ein noch unüberschaubares Ausmaß: Der große Cyberangriff auf die USA sorgt für grundsätzliche Diskussionen.

Von Meike Laaff

20. Dezember 2020, 19:05 Uhr / 180 Kommentare /

Next-gen software supply chain attacks up 650% in 2021

Paul Sawers
@psawers

September 15, 2021 12:35 PM



Aktuelle Angriffstypen

Kopieren / veröffentlichen vertraulicher Daten

Motivation

- (Industrie-) Spionage
- Identitätsdiebstahl (inkl. Finanztransaktionen)
- Erpressung

Gegenmaßnahmen

- Account-Sicherheit
- Verschlüsselung (*in-transit* und *at-rest*)
- **Gar nicht sammeln**

Manipulation bzw. Unbrauchbarmachung

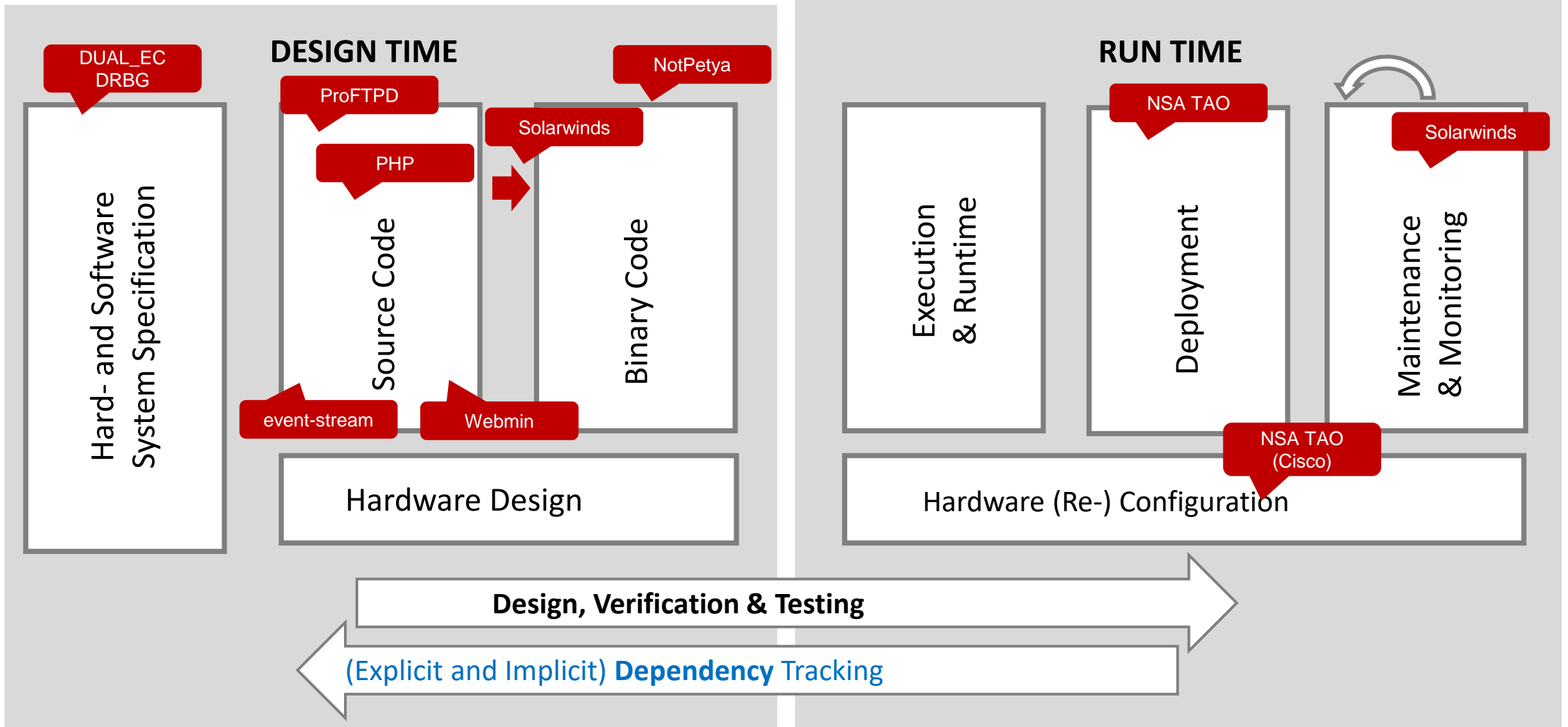
Motivation

- Erpressung
- Kollateralschäden

Gegenmaßnahmen

- Backups!
- Systemredundanz
- Kompartimentalisierung
- **Abhängigkeitsanalyse**

Supply Chain Security betrifft alle Phasen



Supply Chain Security



Komplexe **Abhängigkeitsketten**

- Software-Bibliotheken und *Systems of Systems*
- (Verfügbarkeit von sicherer) Hardware
- Netzwerk-Services
 - lokal – z.B. Logging, Backup, Timesync, etc.
 - remote – notwendige Internet-Services, z.B. DNS, NTP

Abhängigkeitsketten sind interdisziplinär

- technische
- organisatorische
- ökonomische (Lizenz- und Serviceverträge)
- rechtliche / regulatorische

Zusätzliche Herausforderung: Vendor Lock-In



Aktuelle Angriffstypen

Kopieren / veröffentlichen vertraulicher Daten

Motivation

- (Industrie-) Spionage
- Identitätsdiebstahl (inkl. Finanztransaktionen)
- Erpressung

Gegenmaßnahmen

- Account-Sicherheit
- Verschlüsselung (*in-transit* und *at-rest*)
- **Gar nicht sammeln**

Manipulation bzw. Unbrauchbarmachung

Motivation

- Erpressung
- Kollateralschäden

Gegenmaßnahmen

- Backups!
- Systemredundanz
- Kompartimentalisierung
- **Abhängigkeitsanalyse**

Erzeugen / verbreiten gefälschter Daten

Motivation

- Politische Manipulation
- Finanzielle Manipulation
- Diskreditierung von Konkurrenten

Gegenmaßnahmen

- Aufklärung
- ???

ChatGPT, andere Large Language Models (LLMs) und weitere Typen generativer AI

RM

Write an argument piece why Blockchains will solve the misinformation problem generated by AI large language models.



As AI large language models, such as GPT-3, continue to gain popularity and become more sophisticated, the issue of misinformation is becoming increasingly significant. These models can generate realistic-looking text that is difficult to distinguish from human-generated text, making it easier for bad actors to spread false information at scale. This is a growing concern for both businesses and society as a whole, as it undermines the trust and accuracy of information.



One potential solution to this problem is the use of blockchain technology. Blockchains are decentralized digital ledgers that record transactions in a secure and transparent manner. They are resistant to tampering and provide a permanent, auditable record of every transaction that takes place on the network.

By integrating blockchain technology with AI language models, it would be possible to create a system where every generated text is recorded on the blockchain, along with metadata such as the time and date of creation, authorship, and any other relevant information. This would allow for easy verification of the authenticity and accuracy of the text.

Additionally, blockchains could be used to incentivize good behavior and discourage bad behavior. For example, a reputation system could be created where users who consistently produce accurate and trustworthy content are rewarded with tokens or

ChatGPT, andere Large Language Models (LLMs) und weitere Typen generativer AI

Additionally, blockchains could be used to incentivize good behavior and discourage bad behavior. For example, a reputation system could be created where users who consistently produce accurate and trustworthy content are rewarded with tokens or other forms of digital currency. On the other hand, those who produce false or misleading content would be penalized, and their reputation would suffer.

Furthermore, blockchain technology could also be used to create a system of decentralized fact-checking. Anyone with access to the blockchain could verify the accuracy of a piece of text by checking it against trusted sources or other pieces of information that have already been verified on the network. This would help to quickly identify and flag any false or misleading information.

In conclusion, the integration of blockchain technology with AI language models has the potential to address the growing problem of misinformation in a secure and transparent manner. By creating a decentralized system that incentivizes accuracy and provides a mechanism for decentralized fact-checking, it would be possible to restore trust in the accuracy and integrity of information generated by AI language models.

 Regenerate response

|



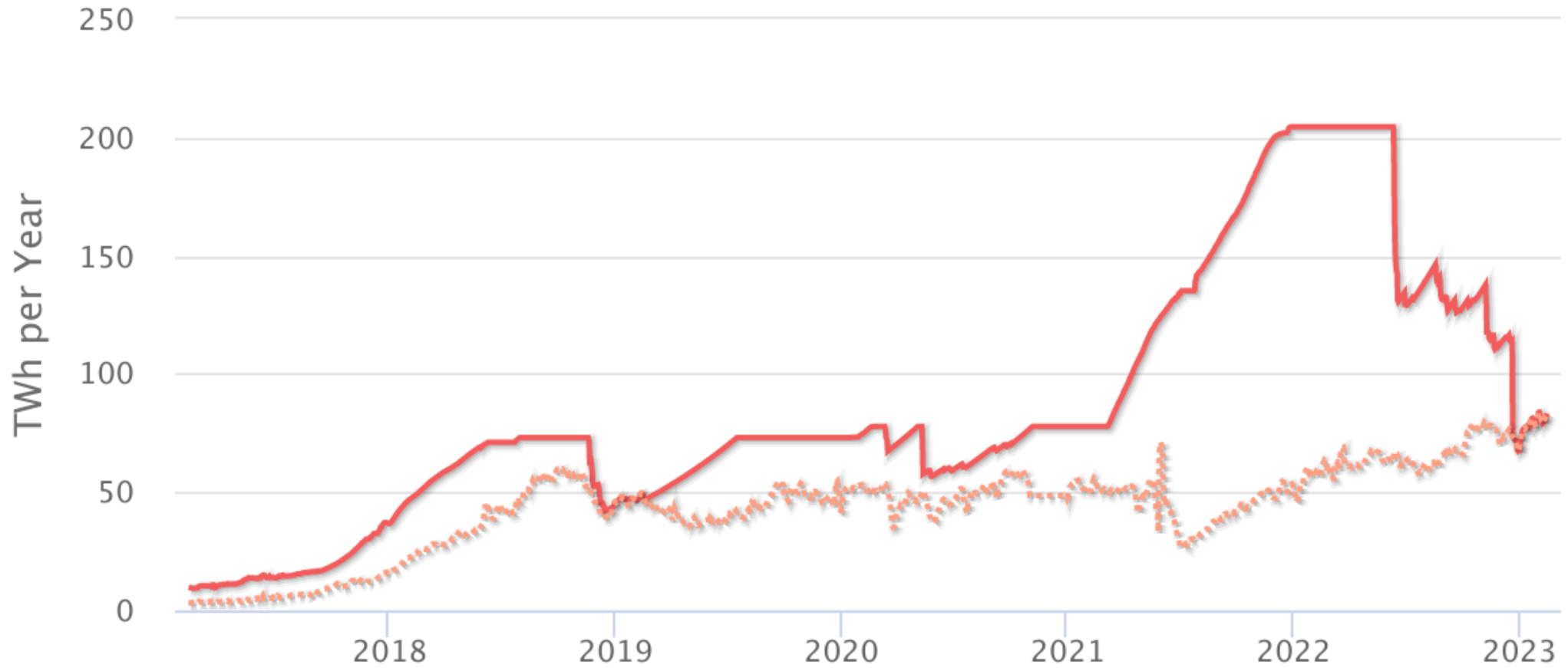
Blockchain als Security-Maßnahme?

BLOCKCHAIN



Bitcoin Energy Consumption

Click and drag in the plot area to zoom in

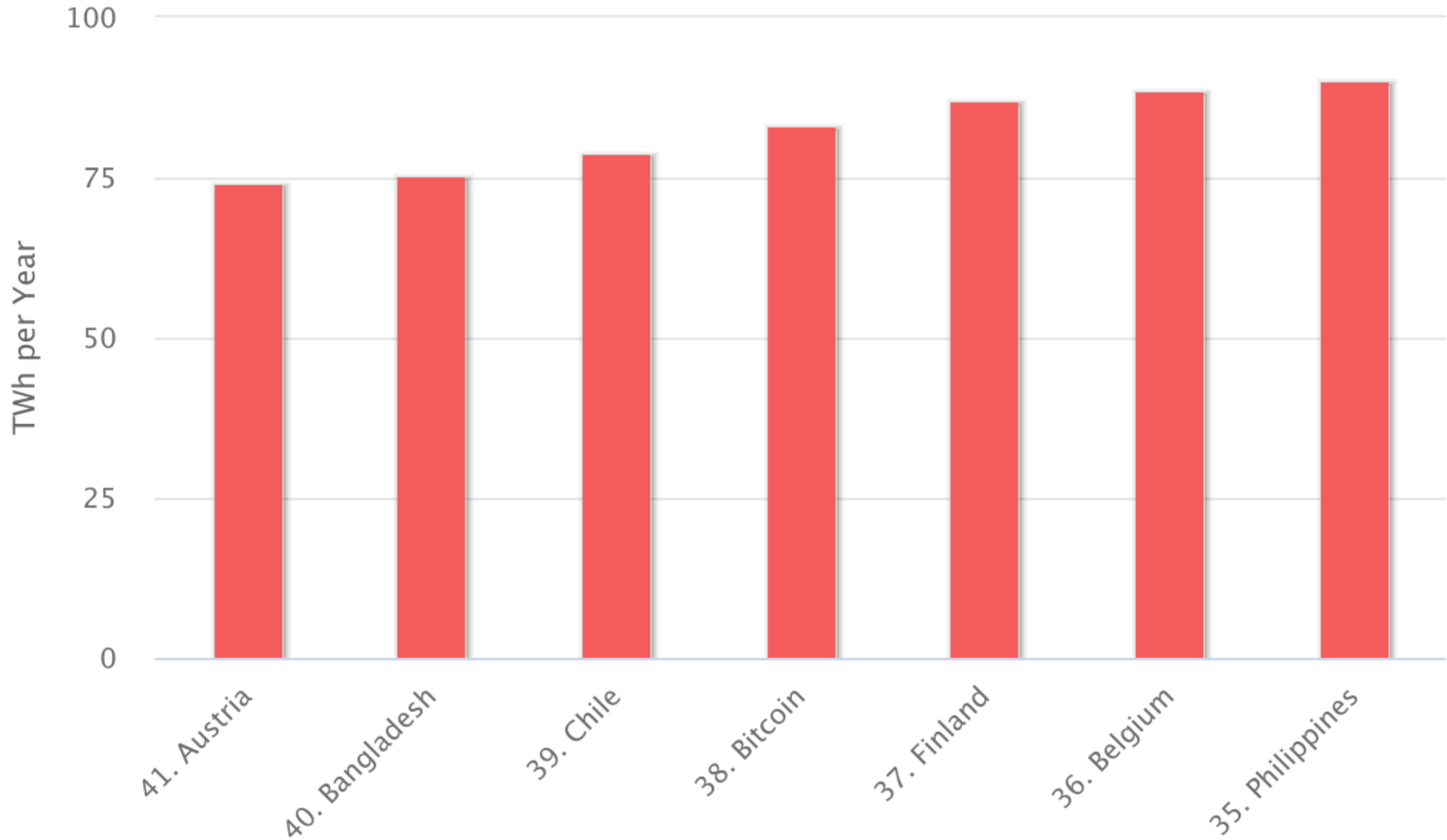


Zoom

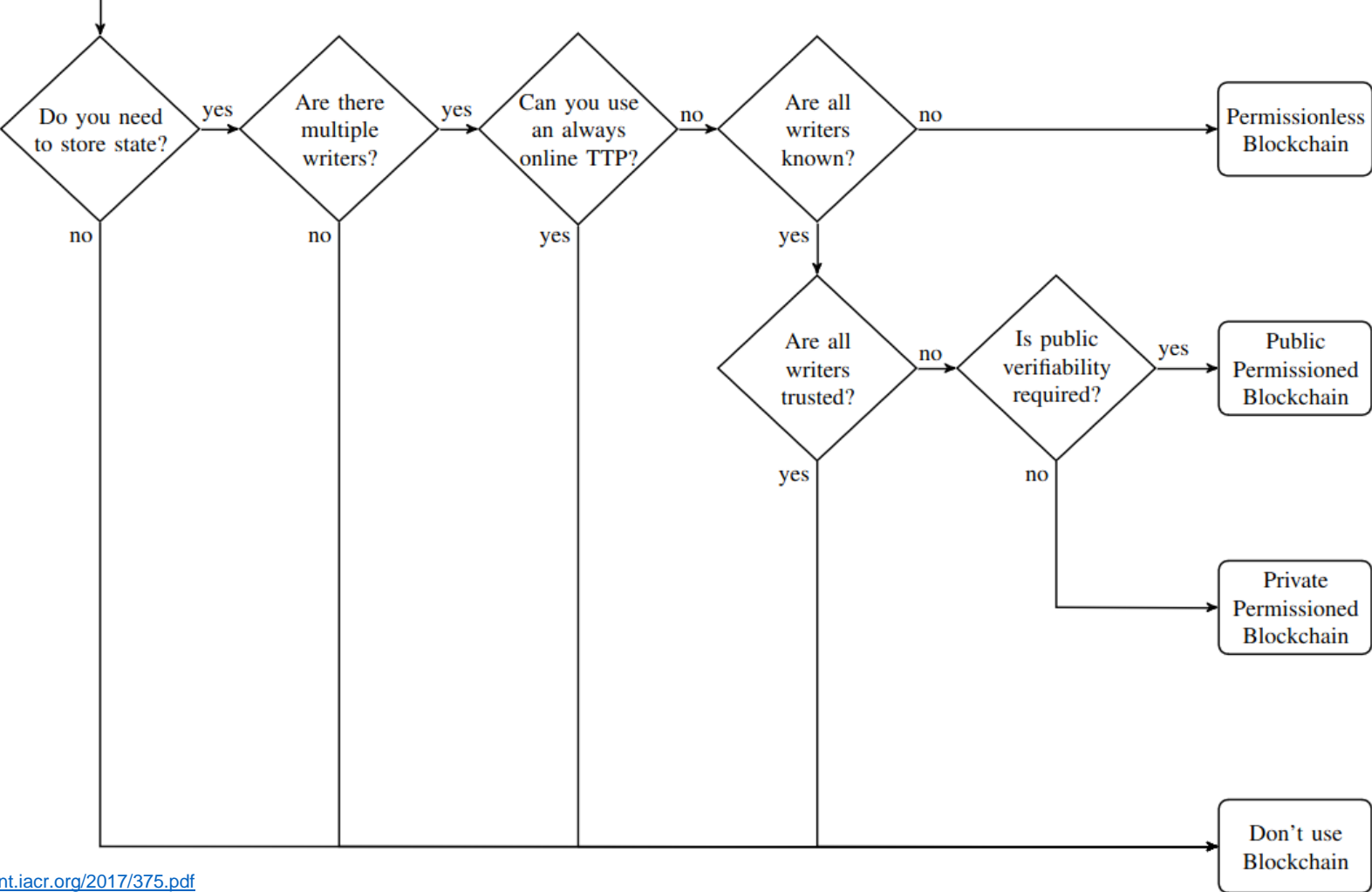
Jan 19, 2017 → Mar 8, 2023

● Estimated TWh per Year ◆ Minimum TWh per Year

Energy Consumption by Country



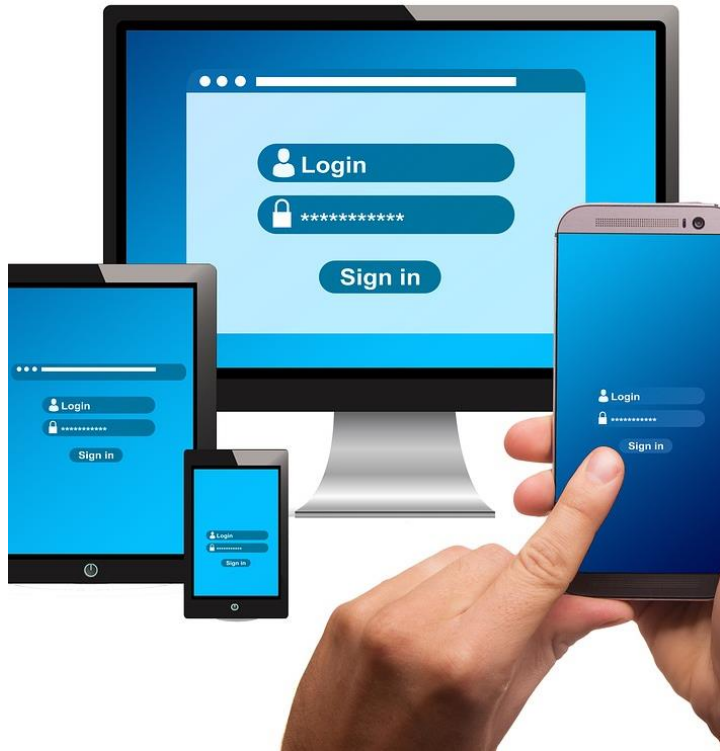
Do you need a Blockchain?



Source: <https://eprint.iacr.org/2017/375.pdf>

Verbessern des Sicherheitsstatus:

1. Passworthygiene



- Gute (lange) Passwörter für “wichtige” Accounts
- Mehrfaktorauthentifizierung – idealerweise FIDO2 – für “wichtige” Accounts
- Passwortmanager für alle anderen Accounts mit zufällig generierten Passwörtern und Integration in Browser
- Ändern von Passwörtern wenn Leaks bekannt werden – auch schon bei Verdacht!
- Regelmäßiges Ändern von Passwörtern ohne Verdacht ist nicht notwendig und eher kontraproduktiv

Verbessern des Sicherheitsstatus:

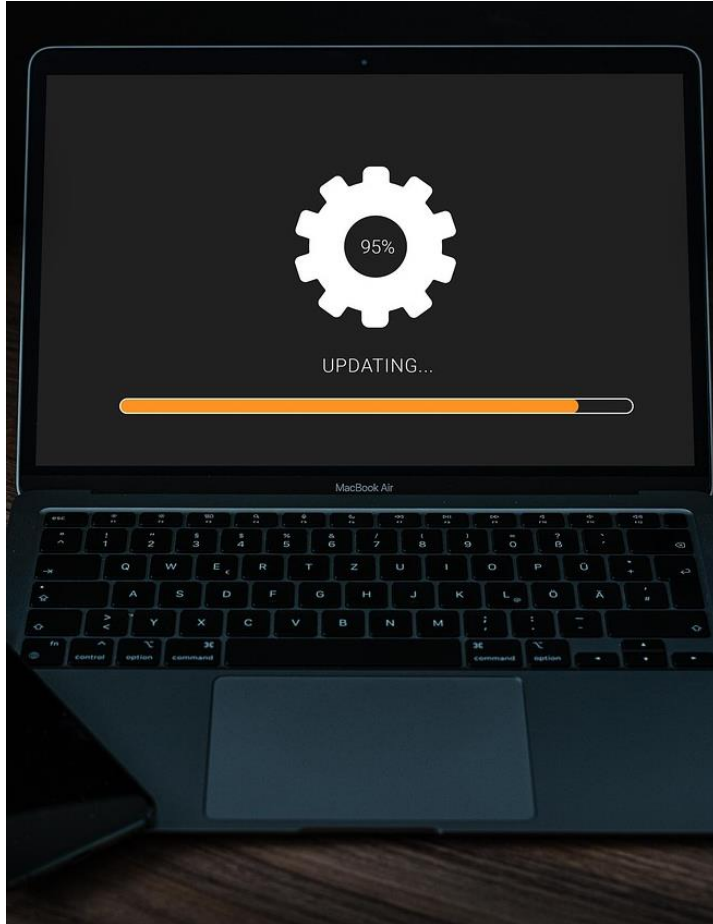
2. Backups



- **Kein Backup – kein Mitleid**
- Aber: Backups ohne getestetes Restore sind keine
- Backups sind das beste Mittel gegen Verschlüsselungstrojaner – und viele andere Probleme
- Aber: Backups helfen nicht gegen Leaks

Verbessern des Sicherheitsstatus:

3. Updates



- Software hat (immer noch) viele sicherheitskritische Fehler
- Updates beheben diese – müssen (wenn verfügbar) zeitnah installiert werden
- Aber: Potenzielle Probleme mit Kompatibilität oder geändertem Verhalten (sowie manchmal neue Fehler)

Verbessern des Sicherheitsstatus: 4.: Erledige zuerst 1. – 3.



- Ist die Basis erledigt?
- Wirklich?
- Wenn ja, dann ist die Organisation schon besser als der Durchschnitt – Gratulation!
- Nächste Schritte zur Verbesserung:
 - „Principle of least privilege“ (z.B. **Fileshare-Berechtigungen**, automatisches **Verschieben** in Archiv nach X Tagen/Monaten, **Windows AppLocker**, etc.)
 - **Monitoring** wichtiger Parameter (z.B. Logins, Netzwerkverkehr, etc.)
 - **Canary Tokens** für Früherkennung von Zugriff auf (eigentlich private) Daten
 - „**Plan B**“ für Ausfall von Systemen – im Vorhinein planen

Fragen?



Web: <https://jku.at/ins>

Email: rm@ins.jku.at

Signal: (phone number by request) Twitter: [@rene_mobile](https://twitter.com/rene_mobile) Mastodon: [@rene_mobile@infosec.exchange](https://mastodon.social/@rene_mobile)

