TeleTrusT-Konferenz

Berlin, 29.06.2023

Warum wir IT-Sicherheit in Zukunft anders denken müssen.

Prof. Dr. Tobias Eggendorfer

Agentur für Innovation in der Cybersicherheit

cyberagentur

cyberagentur

Wieso wir IT-Sicherheit in Zukunft umdenken müssen

Prof. Dr. Tobias Eggendorfer

Berlin, 29.06.2023

IT-Sicherheit: Früher und in Zukunft

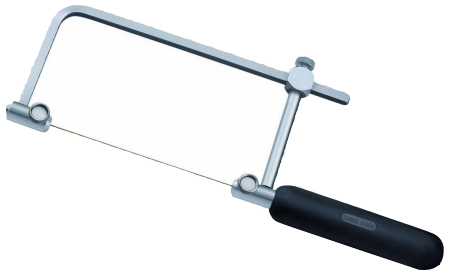
Früher

- Vorfälle „passieren halt“
- Softwarefehler – kann man nichts machen
- „Hohe kriminelle Energie“
- IT-Sicherheit als Nachrüstlösung
- **Fatalistische Einstellung**

In Zukunft

- IT-Sicherheit von Anfang an
- Meß- und prüfbar
- Nur noch anspruchsvolle Angriffe
- Sicherheit als Auswahlkriterium
- **Verlässliche und sichere IT**

Vielleicht wie bei Autos?



Aktuelle Idee von IT-Sicherheit

- Software sei zu **komplex**, um sicher zu sein (angeblich: BGH)
- Sicherheit braucht **zusätzlichen Programmcode**
  - Anti-Malware
  - Firewall
  - IDS / IPS
- Sicher ist „eigentlich“ **unmöglich**

Buffer Overflow - ein typischer Angriff

„Hohe kriminelle Energie“

- **1972** erstmalig beschrieben
- **1990** ISO C führt z.B. strncpy ein
- **1996** Phrack-Magazine
  „Smashing the Stack for Fun and Profit“
- **2022** 50 Jahre 🎂
- **2023** Weiterhin ein Haupteinfallstor

Sicherheitslücken tauchen nicht einfach auf …

- `sql_query("GET * FROM user WHERE username=$GET['username'];")`
- `printf(userinput)`
- `strcpy(src,dest)`
- `exec(userinput)`
- …

- … **sie sind angelegt**.

Wie Sicherheit verkauft wird…

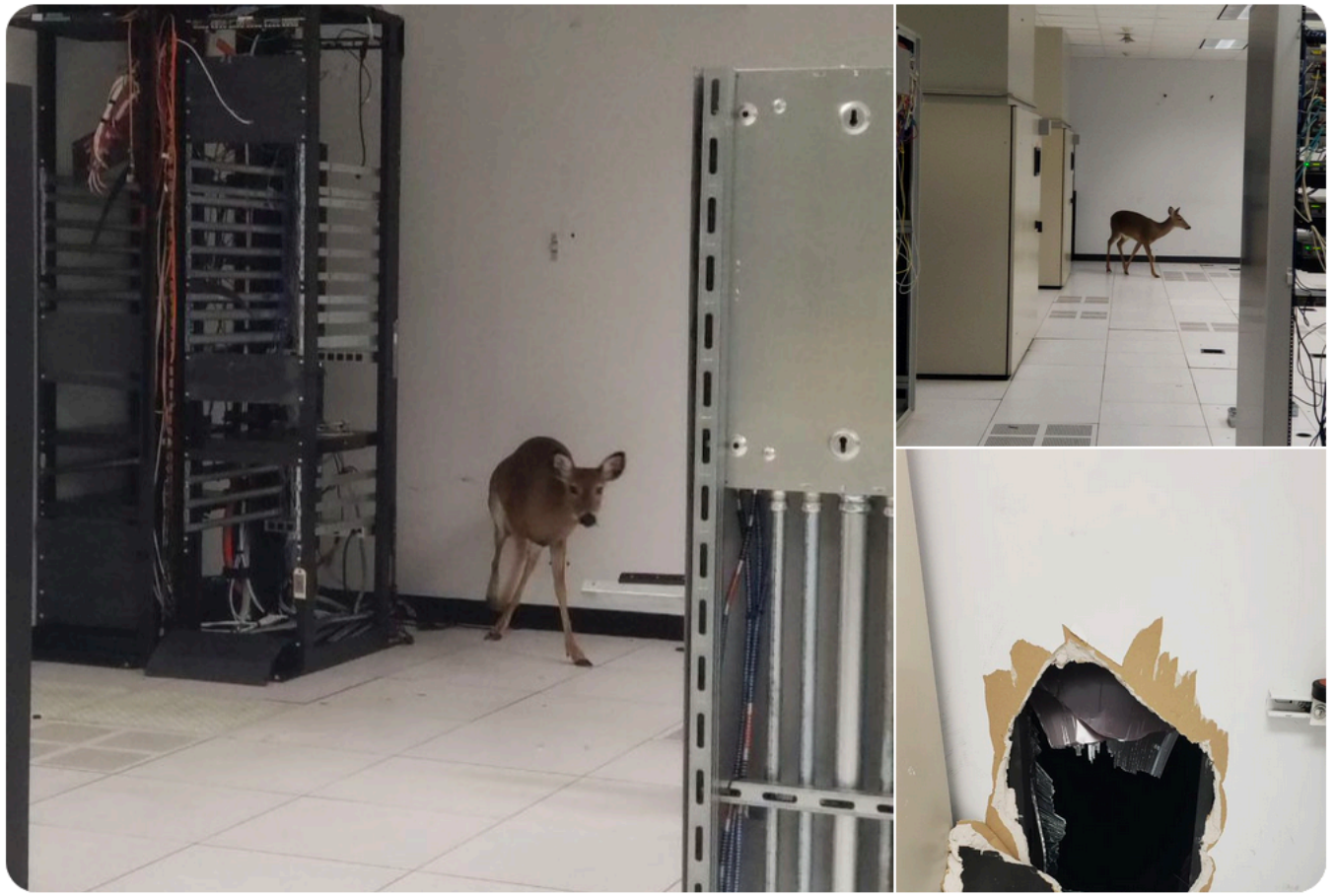
Aber unser Rechenzentrum ist sicher.

DEFCON Furs @DCFurs · 22. Jan.

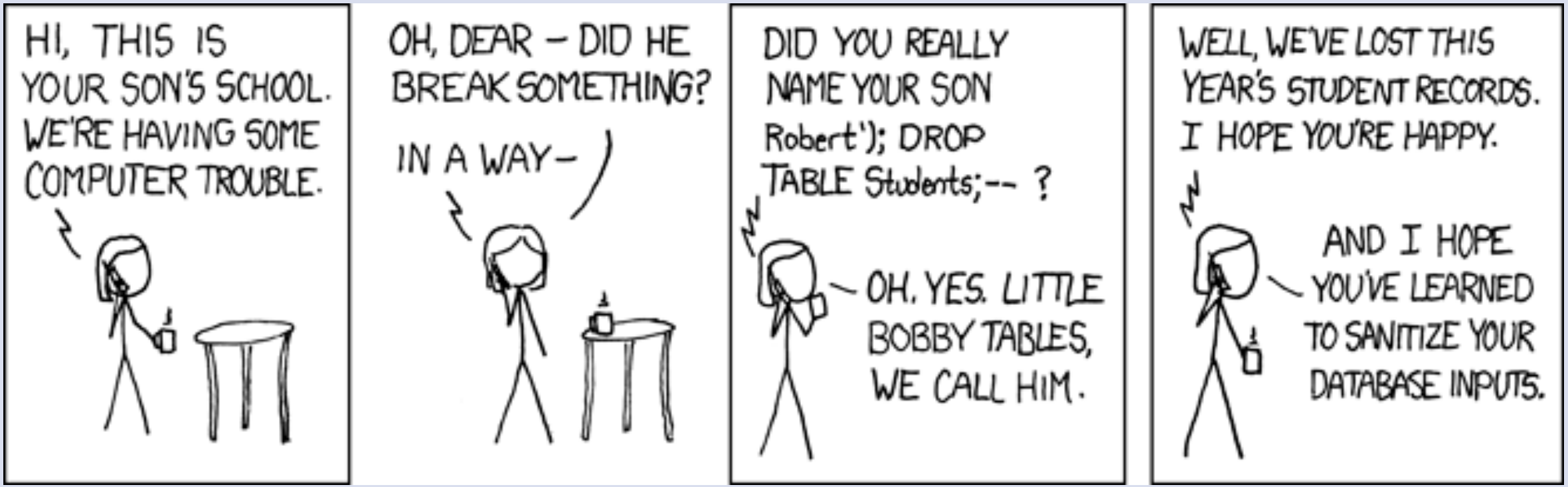
Breaking Mews: Just when you thought it was going to be routine Monday night 2 am server maintenance... The Venison Red Team gets past your fancy guards and biometrics.

Posted with permission. #Pentesting #redteam

Tweet übersetzen



Wir verschlüsseln unsere Festplatten.
Natürlich verwenden wir TLS.
Ihre Daten sind sicher.

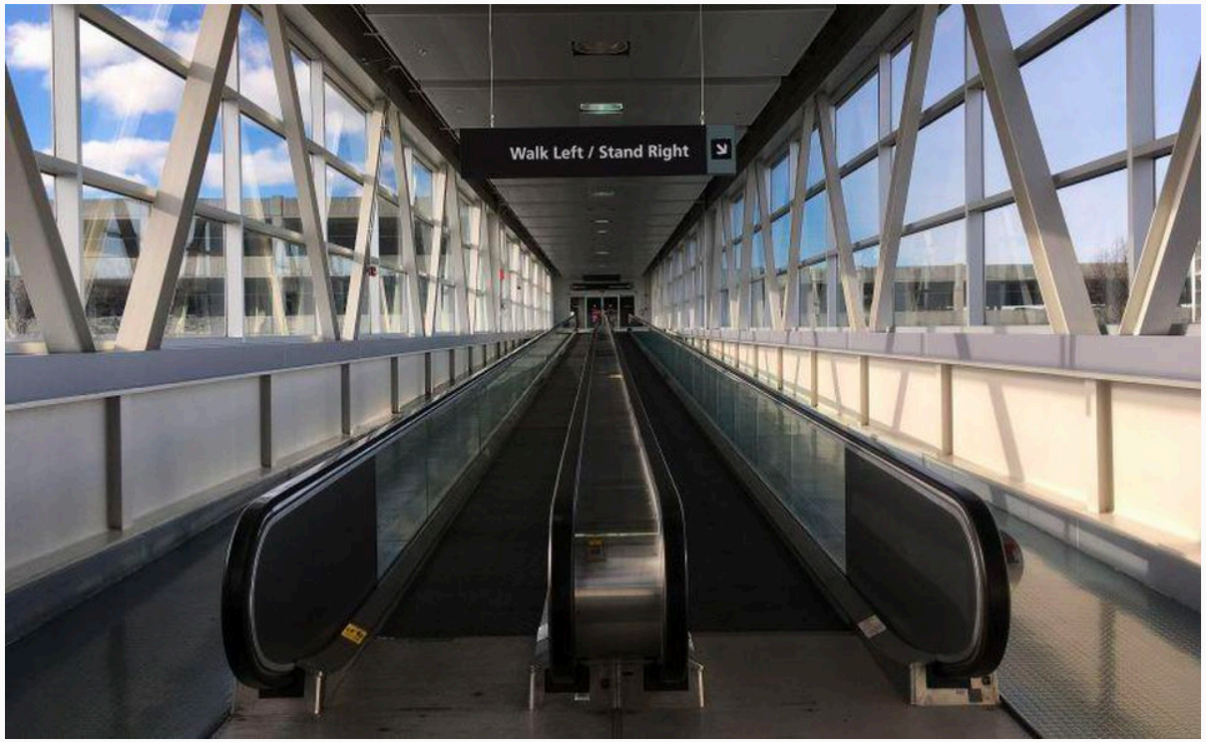


Natürlich haben wir Virenscanner.

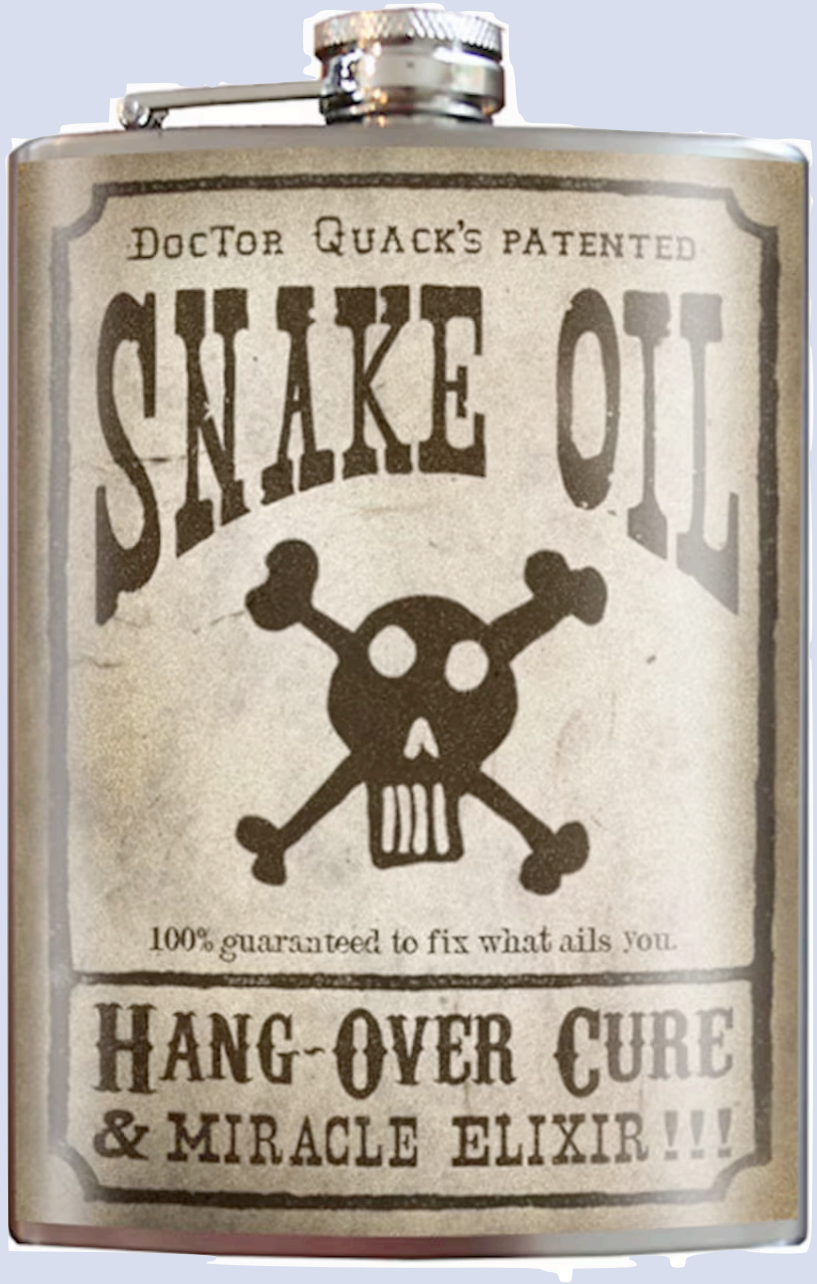
Ransomware Hits Yet Another U.S. Airport

Lee Mathews Contributor ⓘ
Security
Observing, pondering, and writing about tech. Generally in that order.

It wasn't exactly business as usual at Cleveland Hopkins International Airport last week. Several information systems were disrupted by a ransomware outbreak.



Außerdem haben wir …



Wo ist da das Problem?

Fehlannahmen

- Sicherheit als „Add-On“
- Sicherheit ist nachrüstbar
- Mehr Software macht sicherer
- Sicherheitslücken „tauchen einfach auf“

Was wir brauchen

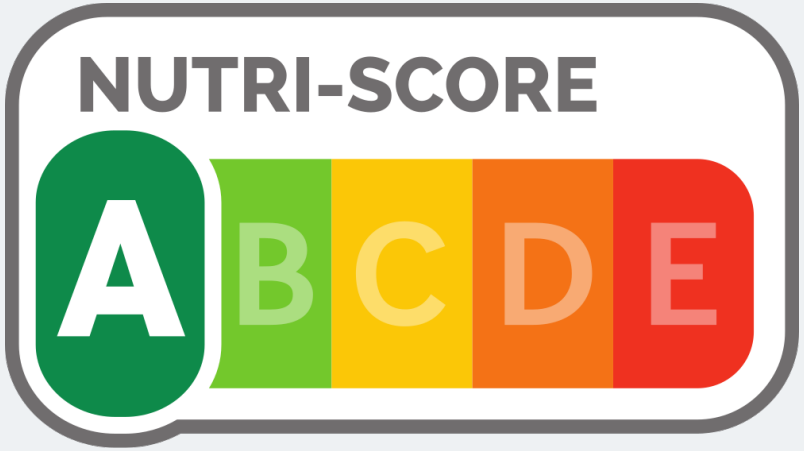
- Echtes Software-**Qualitätsmanagement**
- Verbesserte **Qualifikation** der Entwickler
- Abnahme: Verpflichtende **Penetrationtests**
- **Sicherheitsmetriken**
- **Sachmängelhaftung**

Cloud	Deep discovery	APT	Comprehensive
Entitlement	Mobile	Embedded	Continuous
Policy-based	Persistent Security	BYOD	Enforcing trust
Next Generation	Complete Visibility	Proactive	Insider Threat
Real-time	Zero Day	Automated	Adversary

Statt Buzzword-Bingo

Sicherheitsmetriken

- Sicherheit **meßbar** und **vergleichbar** machen
- Kombinationen von Systemen bewerten
  - Ist LibreOffice sicherer auf
    - Linux
    - MacOS
    - NetBSD
- **Objektiv** und **prüfbar**



Formale Verifikation

- Mathematischer **Nachweis**, daß Programm nur und genau das leistet, was es leisten soll
- Doppelter Effekt:
  - **Verhindert Sicherheitslücken**
  - **Ändert** Entwickler-**Mindset**

Chancen und Risiken

Chancen

- Echte Sicherheit statt Security Theatre
- Konzentration auf Software-Entwicklung statt Patch-Management
- Feuerwehr-Funktion der IT-Abteilung endet
- Langfristig sinkende Kosten

Risiken

- Marketing entdeckt die Terminologie
  - „Wir haben formal verifiziert“ - Mißbrauch des Begriffes
  - Bogus-Sicherheits-Scores
- Kunden akzeptieren den Mehraufwand nicht
  - Längere Entwicklungszyklen
  - ggf. kurzfristig höhere Kosten

Unterstützend: Cyber Resiliance Act

- Fordert IT-Sicherheitsmaßnahmen
- Aber:
  - **Selbstbewertung** möglich
  - Maßstäbe noch eher abstrakt

Was die Cyberagentur dafür leistet:

- Wir beauftragen Forschung für
  - **innovative**,
  - potentiell **disruptive**
  - wissenschaftlich **riskante**
- Projekte im Bereich der Cybersicherheit.

Was Unternehmen & Politik leisten können

- Sicherheit von Buzzword-Bingo und Schlangenöl zu
  - **prüfbaren** (z.B. Penetrationtest)
  - **verpflichtenden**
- Ausschreibungskriterium erheben.
- **Sicherheitsmängel** als **Sachmängel** gelten machen.

Updates und Sicherheitsvorfälle müssen Ausnahmen werden.

cyberagentur

der Souveränität
von übermorgen