Alles kann gehackt werden,

auch Medizinprodukte!

younix / panic

https://muc.ccc.de/

Warum ist IT unsicher?

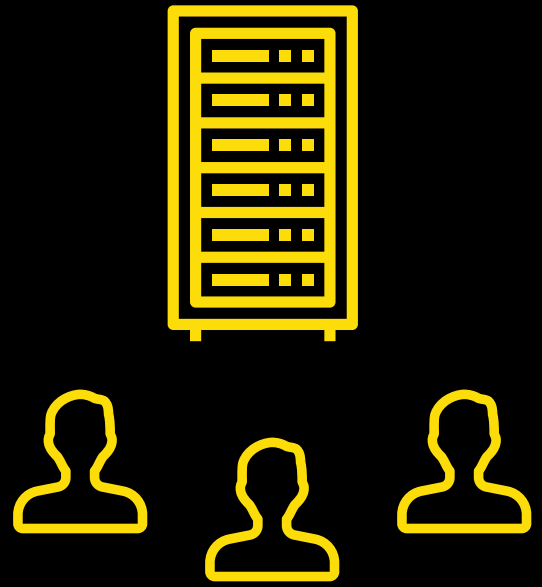
Warum ist IT unsicher?

errare humanum est

Warum ist IT unsicher?

irren ist menschlich

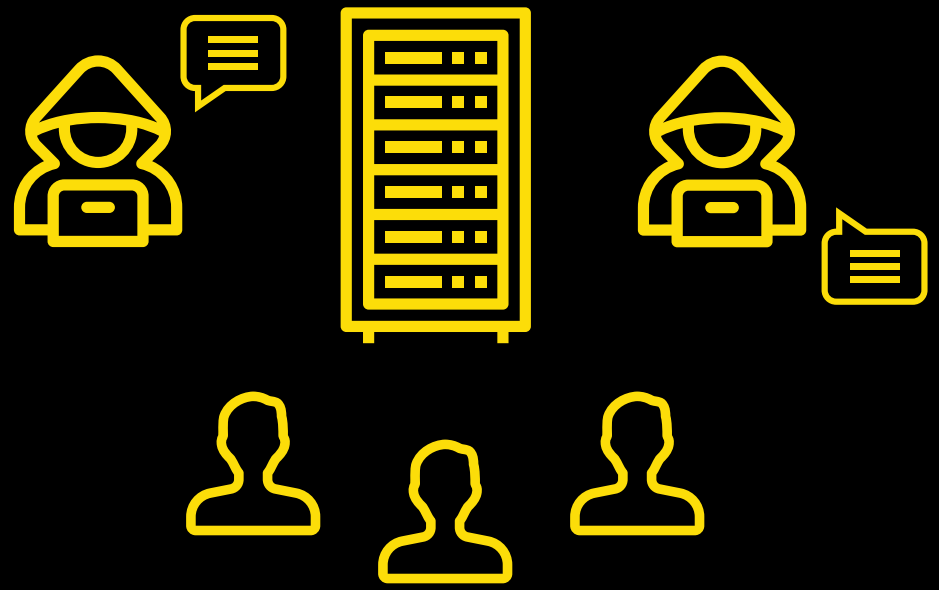
Was ist die Konsequenz?



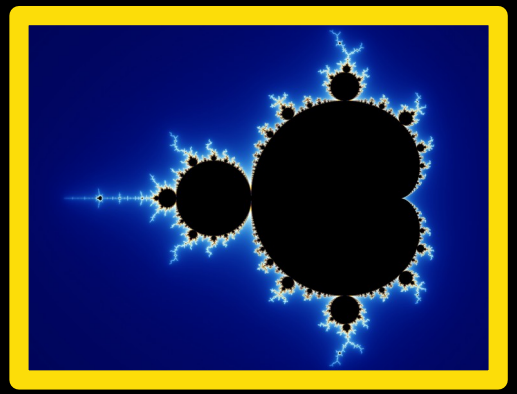
Was ist die Konsequenz?

Was machen Hacker?

Was machen Hacker?



Was machen Hacker?

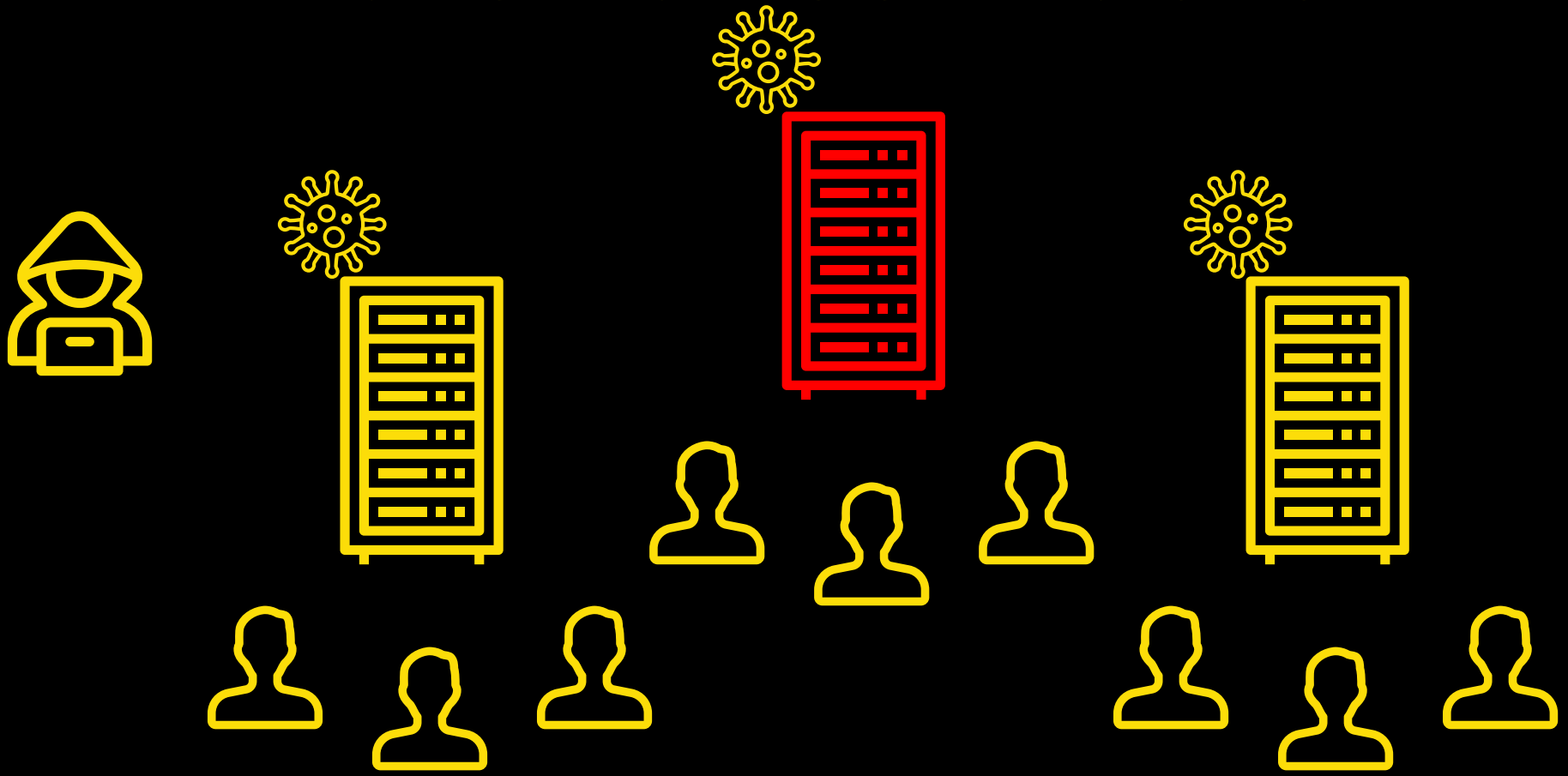


Automatisch hacken?

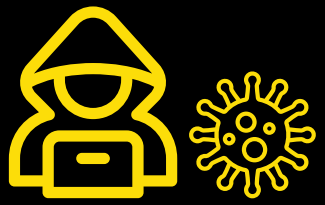
Automatisch hacken?

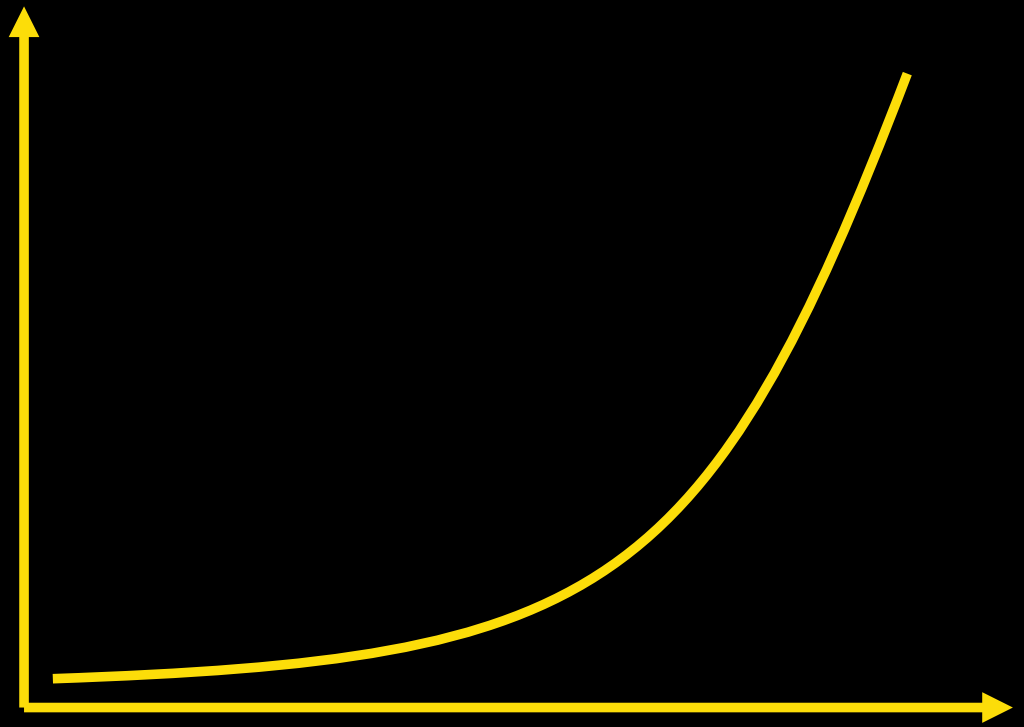
Automatisch hacken?

Automatisch hacker?

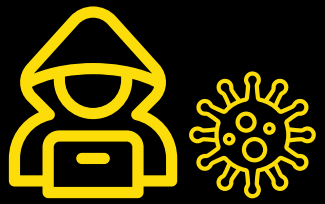


Geht da noch mehr?

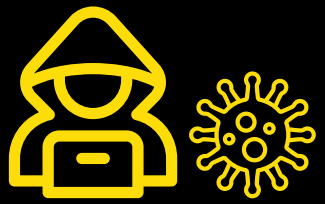


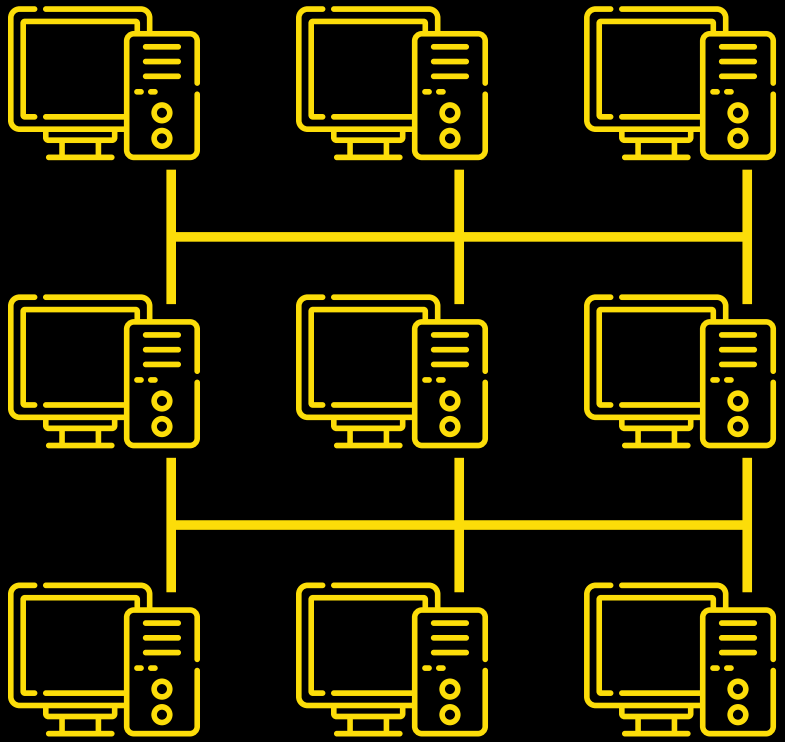


Warum ist das möglich?

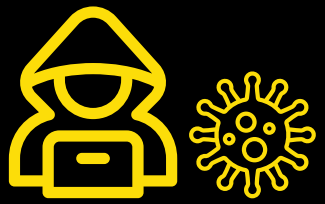


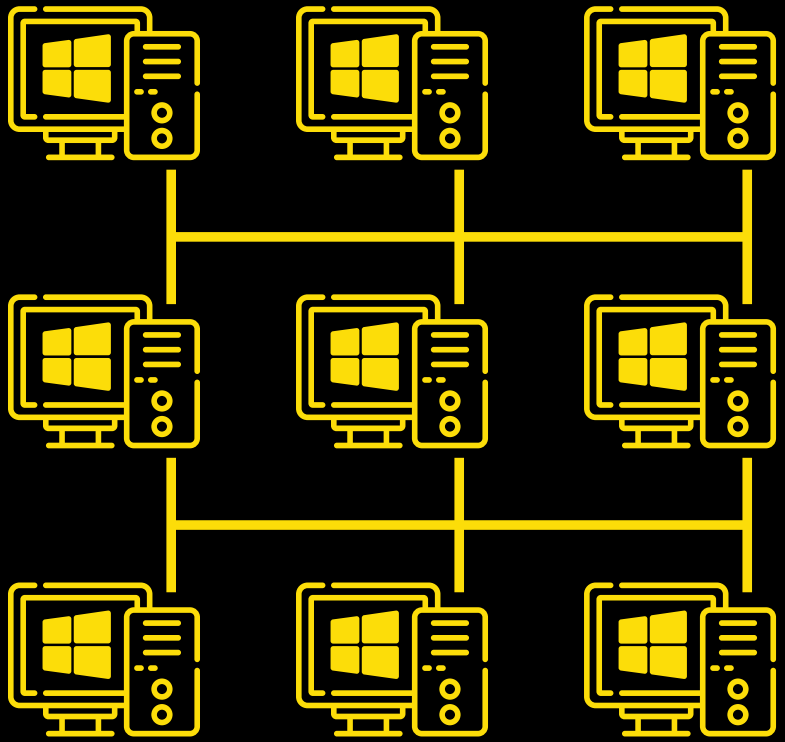
Warum ist das möglich?



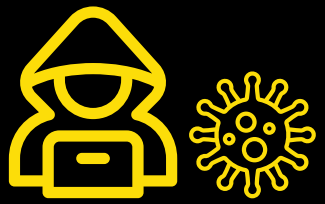


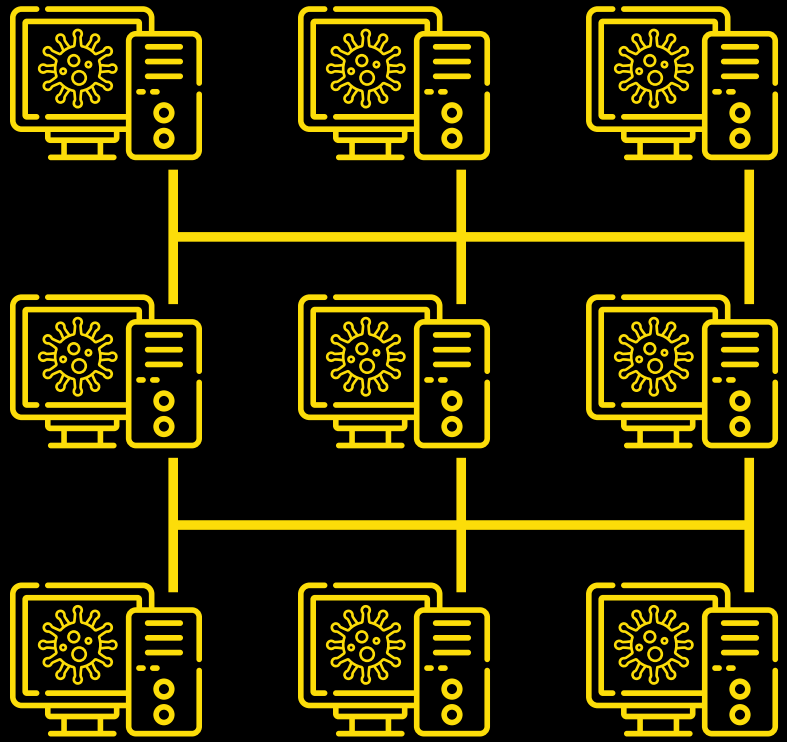
Warum ist das möglich?





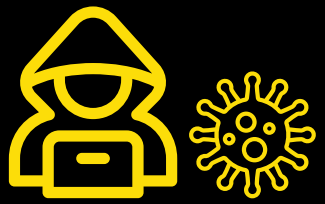
Warum ist das möglich?





Wer macht sowas?

unauffälliger Teenager aus Niedersachsen



[...] "dass ich etwas hinzufügen soll, das Schaden macht.

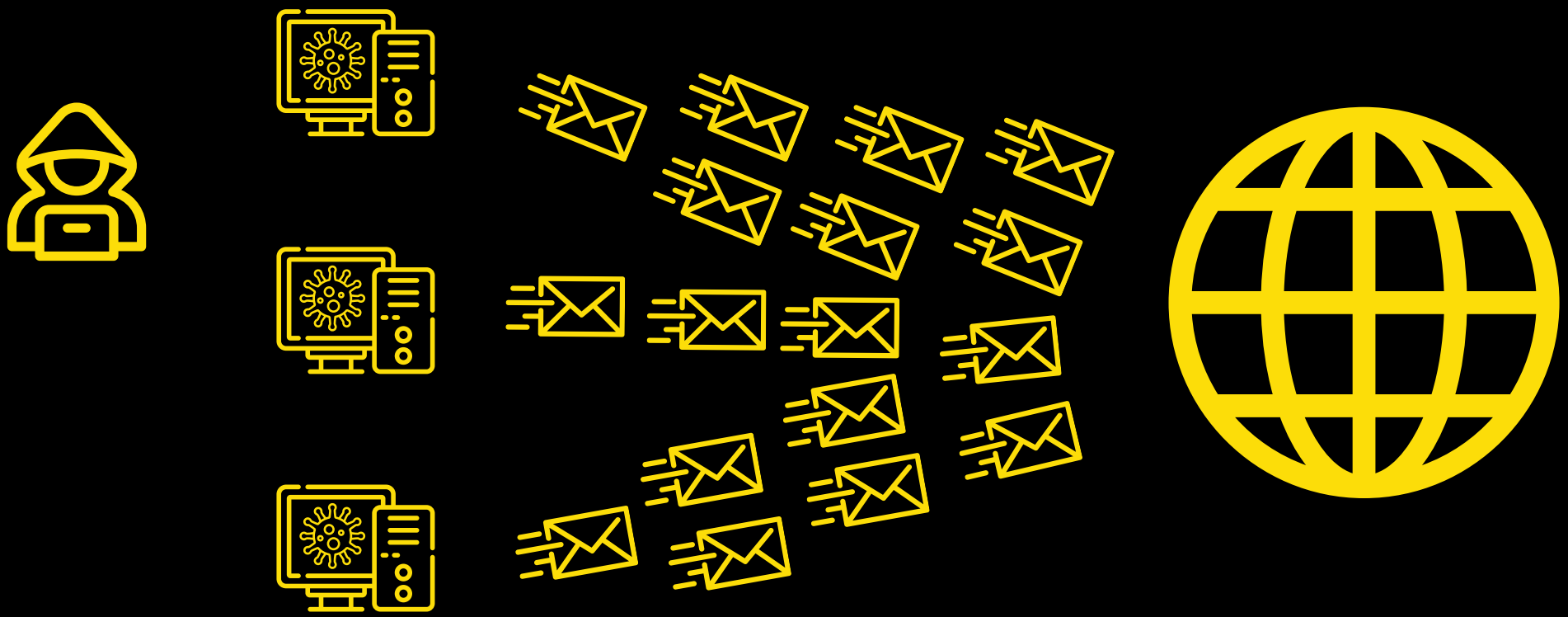
Aber das wollte ich nie."

Er will besser sein als andere Virenprogrammierer. Nicht böser.

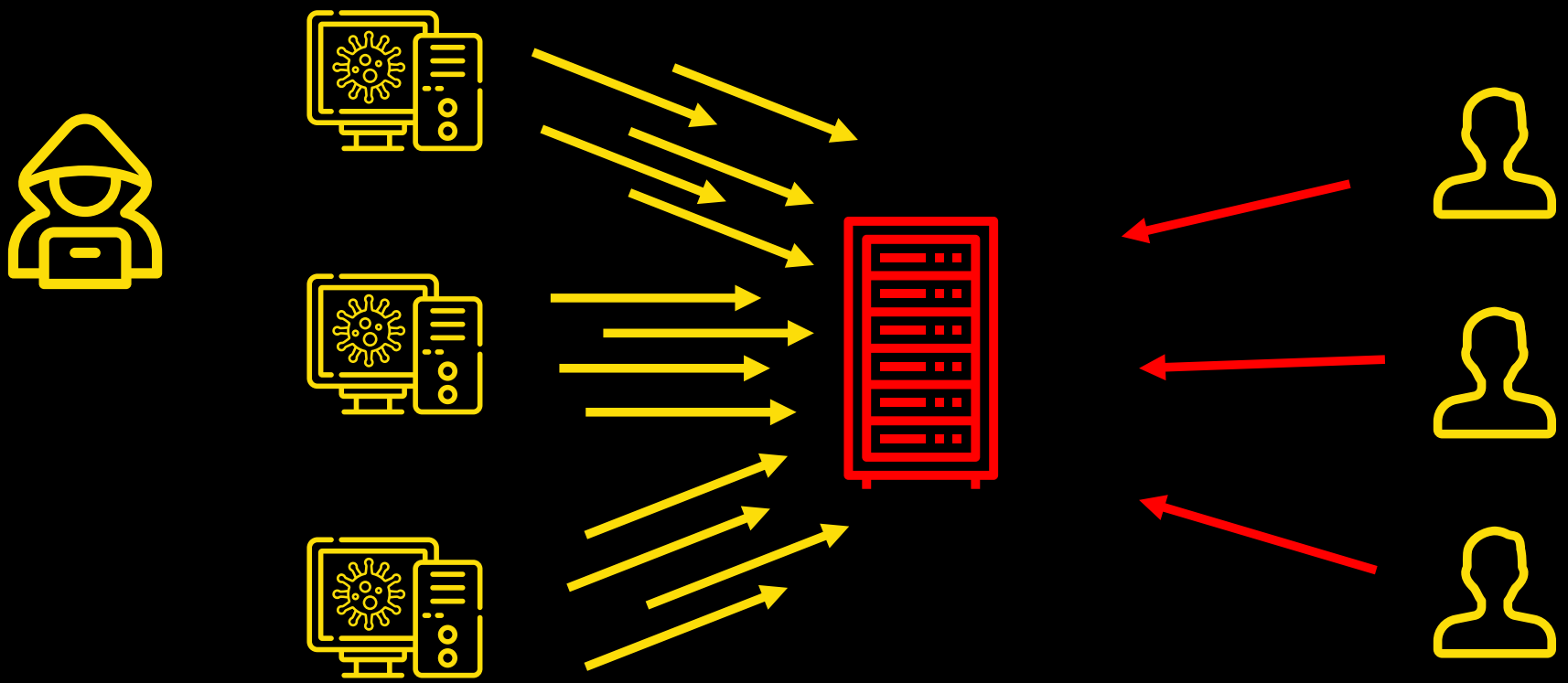
https://www.stern.de/digital/online/-sasser--programmierer-der-wurm-von-der-wuemme-5801568.html

Fun to Profit!

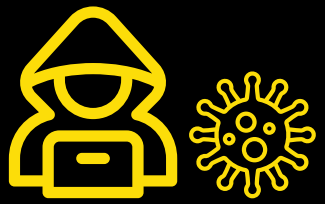
SPAM-E-Mails

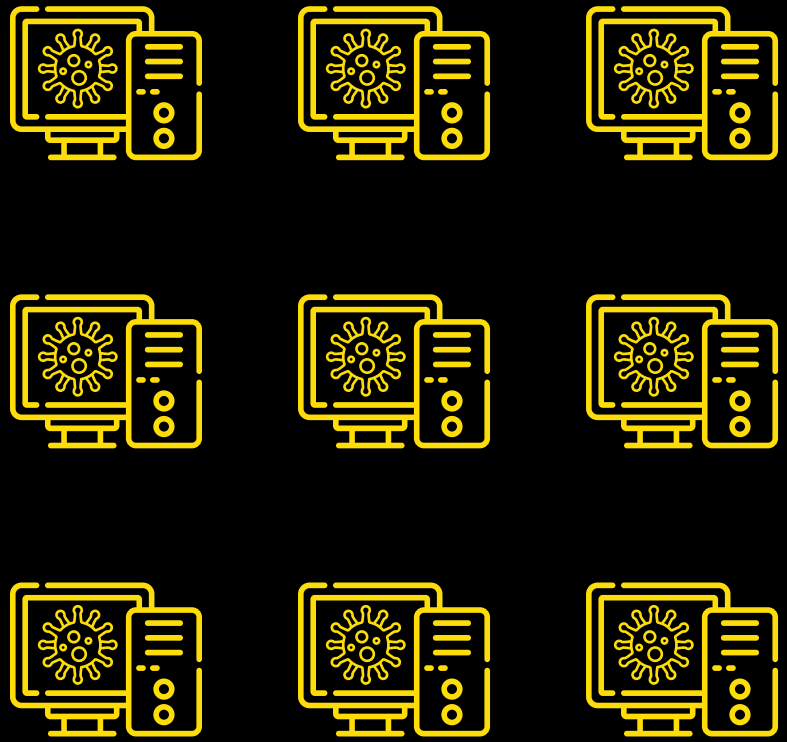


Überlastungsangriffe

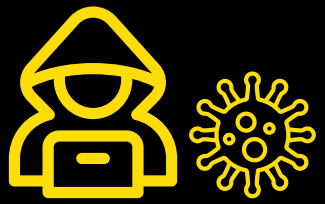


Was ist noch möglich?

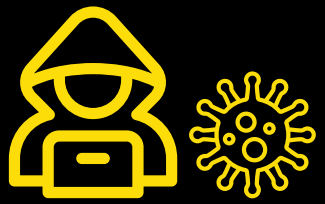




Ransomware



Wer macht sowas?



Anführer […] ein neuseeländischer Teenager […].

Brains behind Mirai were a 21-year-old college student and his two college-age friends.

“They didn’t realize the power they were unleashing,” says FBI

Was bedeutet das für Sie?

Safety vs. Security

Funktions- und Betriebssicherheit, Zuverlässigkeit (Safety):

- **Erkennung und Vermeidung von Störungen *innerhalb* des Systems, die Menschen schaden könnten.**
- **„*Technische Begrenzung* des erzeugbaren Schalldrucks des Lautsprechers in einem Hörgerät“**

Safety vs. Security

Daten- und Informationssicherheit (IT-Security):

- **Schutz vor gezielter oder unabsichtlicher Manipulation des Systems von *außen*.**
- **„Funkbefehl zur Lautstärkeänderung eines Hörgerätes darf nur von *bestimmten* Geräten kommen.“**
  (*Schutzziele*: Integrität, Authentizität)

Safety vs. Security

- **Safety und Security stehen manchmal in Konflikt**
- **Security ist oft notwendig für Safety**

Situation: Medizingeräte

- **Aufwändige und langwierige Entwicklung**
- **Lange Nutzungsdauer (Jahre – Jahrzehnte)**
- **Software lässt sich oft nicht updaten**

- **Software kann unbekannte Fehler enthalten**
- **Zunehmende Vernetzung (auch zu Nicht-Medizingeräten)**
- **Veränderung der *Umgebung* von Geräten**

  Systeme werden mit der Zeit unsicher

Persönliche Maßnahmen

Prävention und Risikominimierung

- **Datensparsamkeit, Dezentralisierung**
- **Vernetzung von Geräten nur soweit nötig**
- **Verwendung *langer* Passwörter (Passsatz)**
- **Getrennte Nutzerkonten (z.B. E-Mail) für Aufgaben und Personen, Rechteverwaltung**
- **Regelmäßige Backups**

Persönliche Maßnahmen

IT-Hygiene

- **Wissen, ob und wo es Updates gibt (Hersteller)**
- ***Zeitnahes* Updaten (Stunden – Tage)**

Übung von Abläufen

- **Wiederherstellen von Daten aus Backups**
- **Handlungsabläufe bei eingeschränkter Infrastruktur oder -ausfall**

Herstellerseitige Maßnahmen

- **IT-Sicherheit und Technologietrends von Anfang an berücksichtigen**

- **Transparenz bei Sicherheitslücken**

  Schnelle Benachrichtigung der Nutzer

- **Verwendung von etablierten und offenen Standards, Protokollen,**

  kryptographischen Algorithmen

Herstellerseitige Maßnahmen

- **Öffentliche Dokumentation der Schnittstellen**
  - **Erleichtert die Forschung durch IT-Sicherheitsexperten**
  - **Erleichtert die Entscheidung von Kunden/Nutzern**
  - **Verringert die Abhängigkeit vom Hersteller**
    (Vendor-Lock-In; z.B. Bedienungssoftware)

- **Code- und Protokoll-Audits**

Beispiel: Protokoll-Audit

Beispiel: Protokoll-Audit

The [**…**Lab] performed [**…**a] **gray box** test and a **conceptual review** of the wireless communication interface [**…**]

The **Twofish** and **CBC-MAC** implementation is compliant to the standard**. Random numbers and keys** are generated and used properly**.** The security properties of the communication protocol are **not reliant** on the features of the underlying Bluetooth protocols**.** [**…**This] results in a sufficient protection of the **integrity** and **authenticity** of information [**…**] Furthermore**,** it is ensured**,** that the association of an insulin pump with a specific blood**-**glucose meter **can not be altered** via the the wireless interface**.**

Politische Maßnahmen

- **Audits zur IT-Sicherheit einfordern**
- **Transparenz bei Schnittstellenprotokollen einfordern**
- **Freie und Open Source Software fördern (z.B. Verwaltung)**
- **„Integrität und Vertraulichkeit informationstechnischer Systeme” nicht gefährden**
- **Sicherheitslücken in populärer oder kritischer Software suchen, beheben (lassen) und veröffentlichen**
- **Unabhängige IT-Sicherheitsforschung fördern (z.B. Bug Bounties)**

Fragen?

Bildquellen

https://www.flaticon.com/de/autoren/photo3idea-studio

https://www.flaticon.com/de/autoren/monkik

https://www.flaticon.com/de/autoren/freepik

http://www.freepik.com/