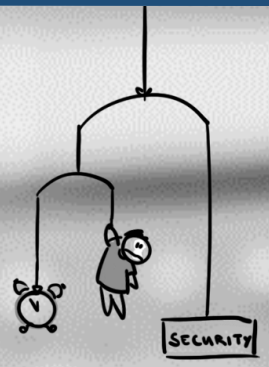
Lassen Sie mich durch, ich bin IT Sicherheitsforscher



Vom Dilemma zwischen aktiver IT Sicherheitsforschung und Recht

Tobias Fiebig

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

IT Sicherheit

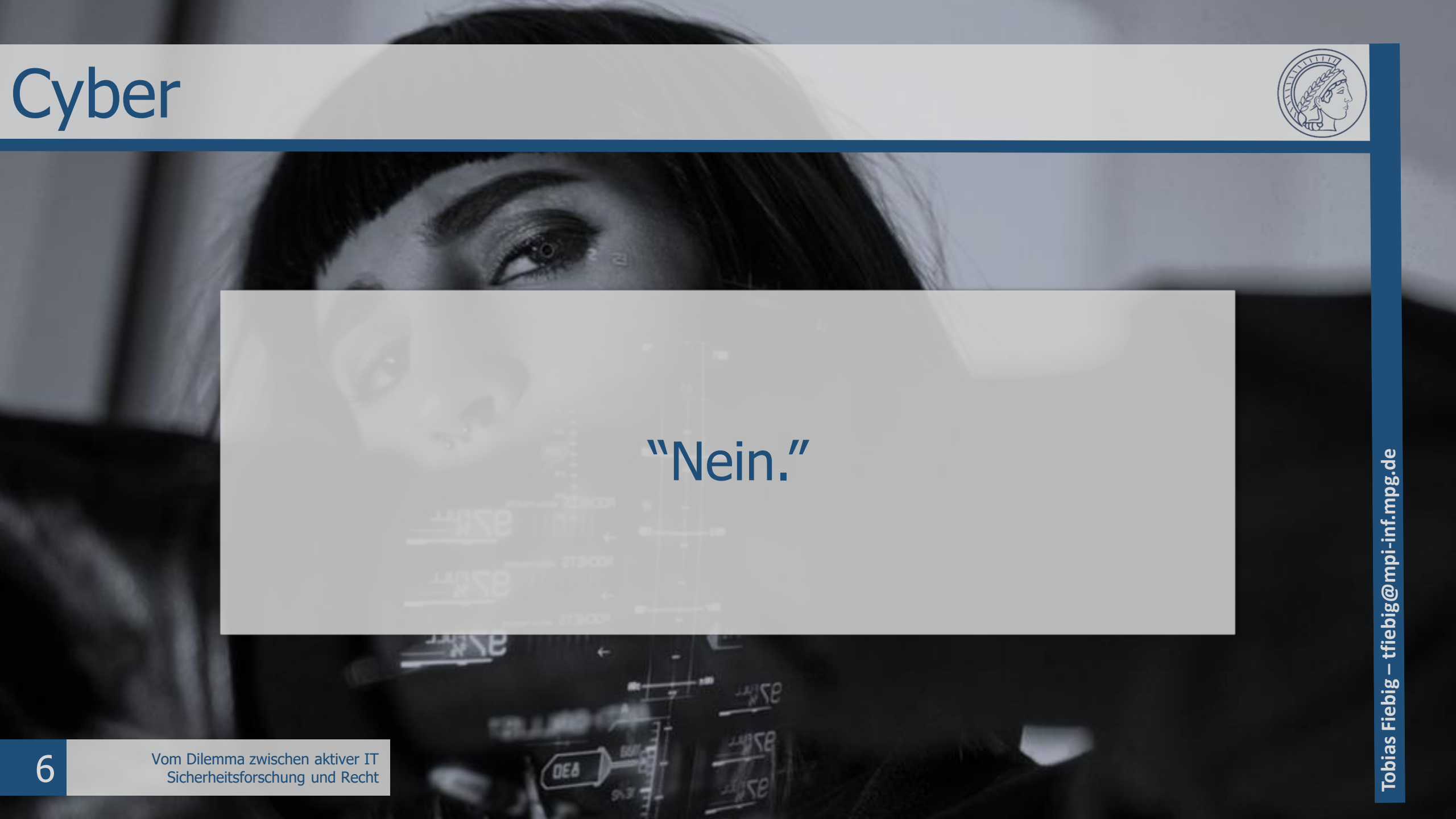
"Ein Computer tut *immer* EXAKT das, was man ihm sagt."

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

Cyber

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

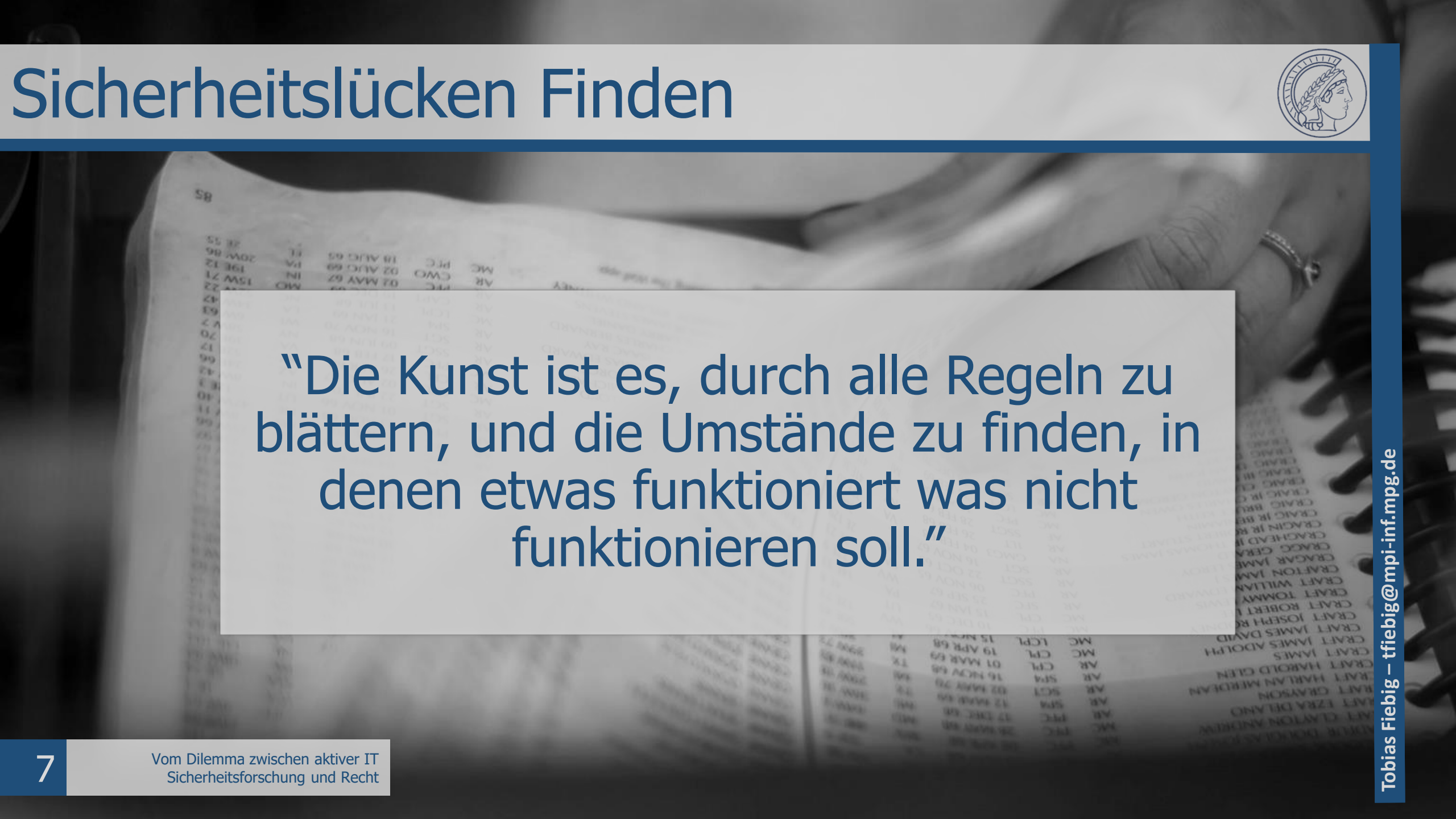
Cyber



"Nein."

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

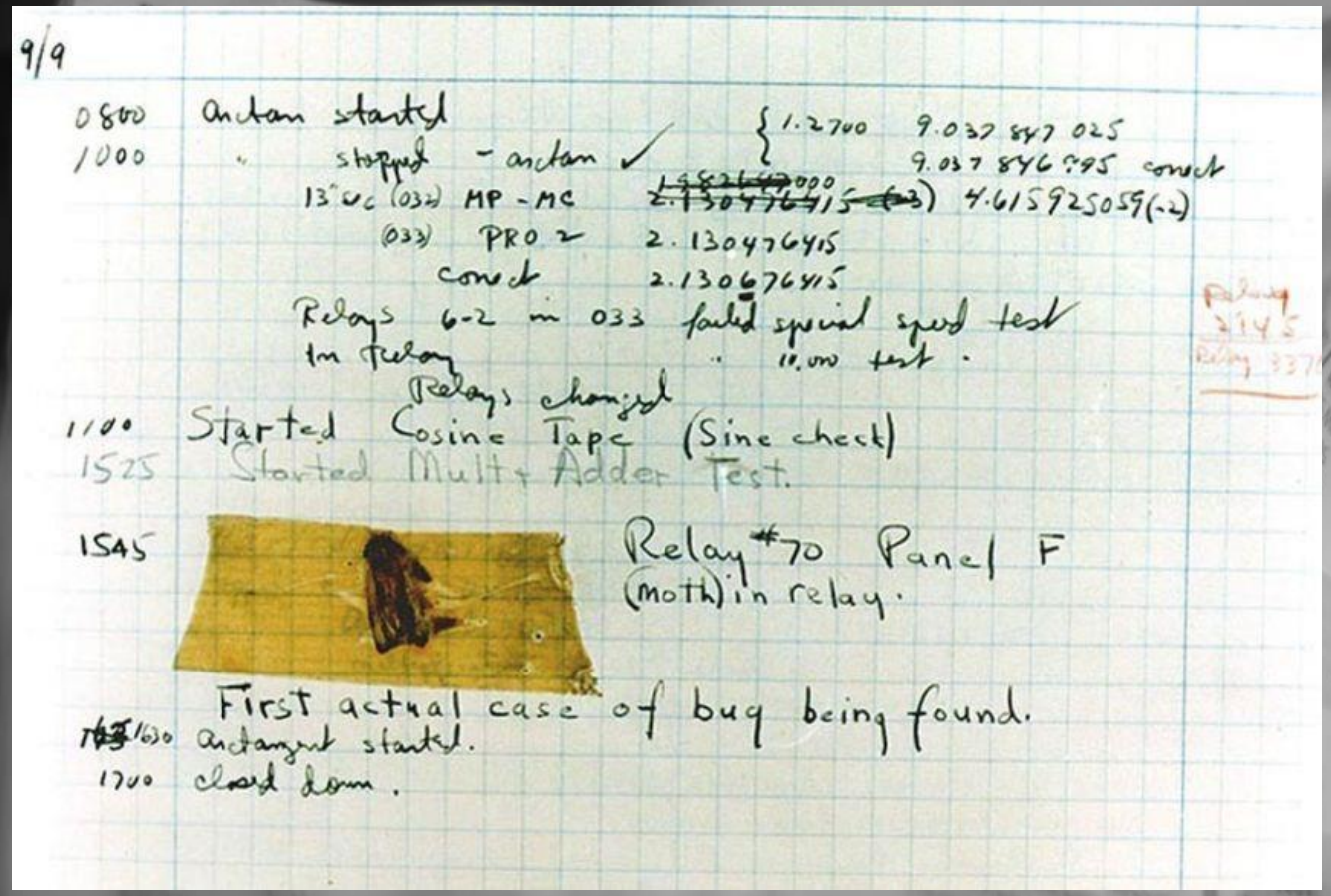
Sicherheitslücken Finden



"Die Kunst ist es, durch alle Regeln zu blättern, und die Umstände zu finden, in denen etwas funktioniert was nicht funktionieren soll."

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

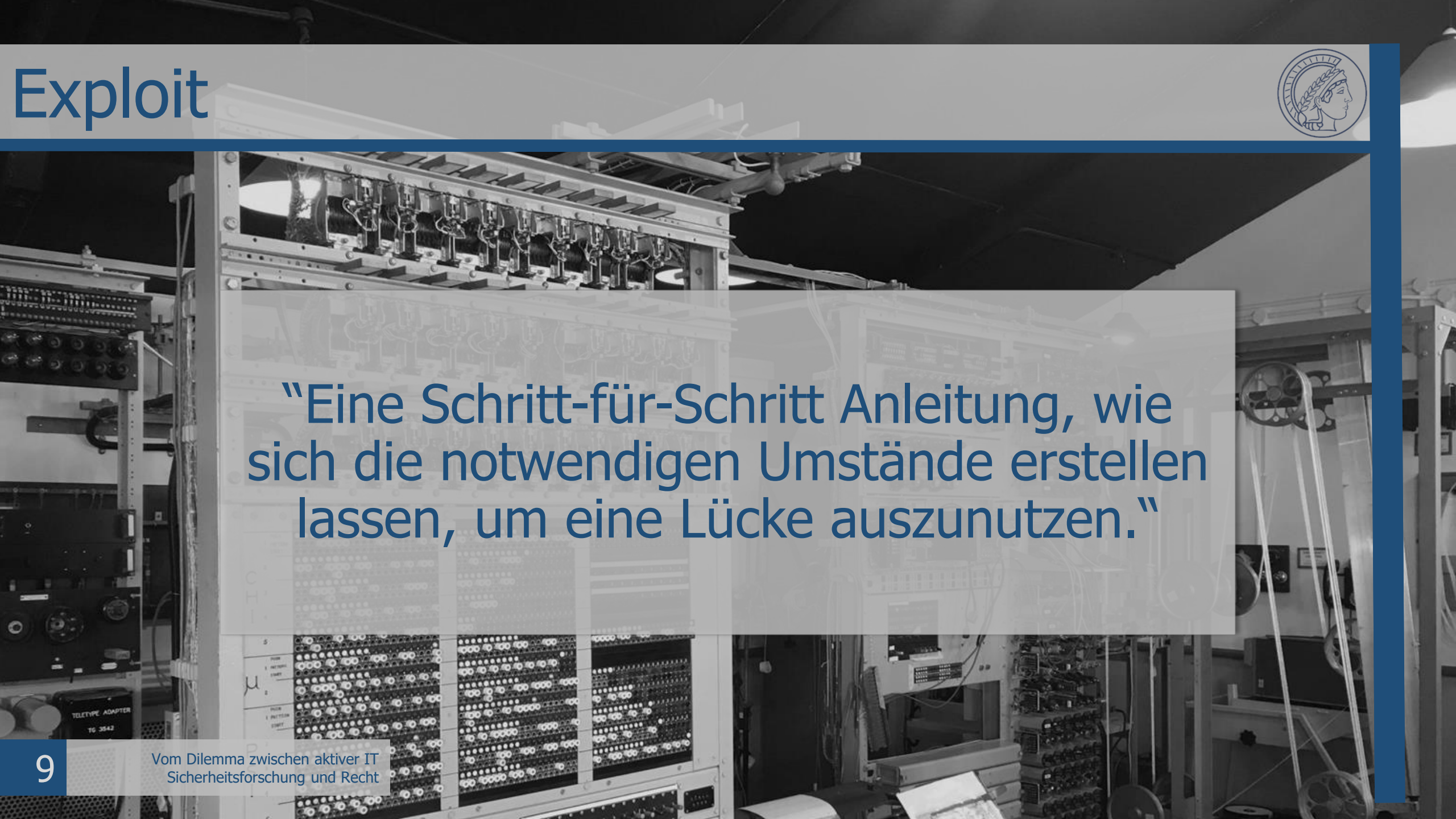
Sicherheitslücken Finden



Rear Adm. Grace Hopper,
1st Bug, 1st Compiler,…

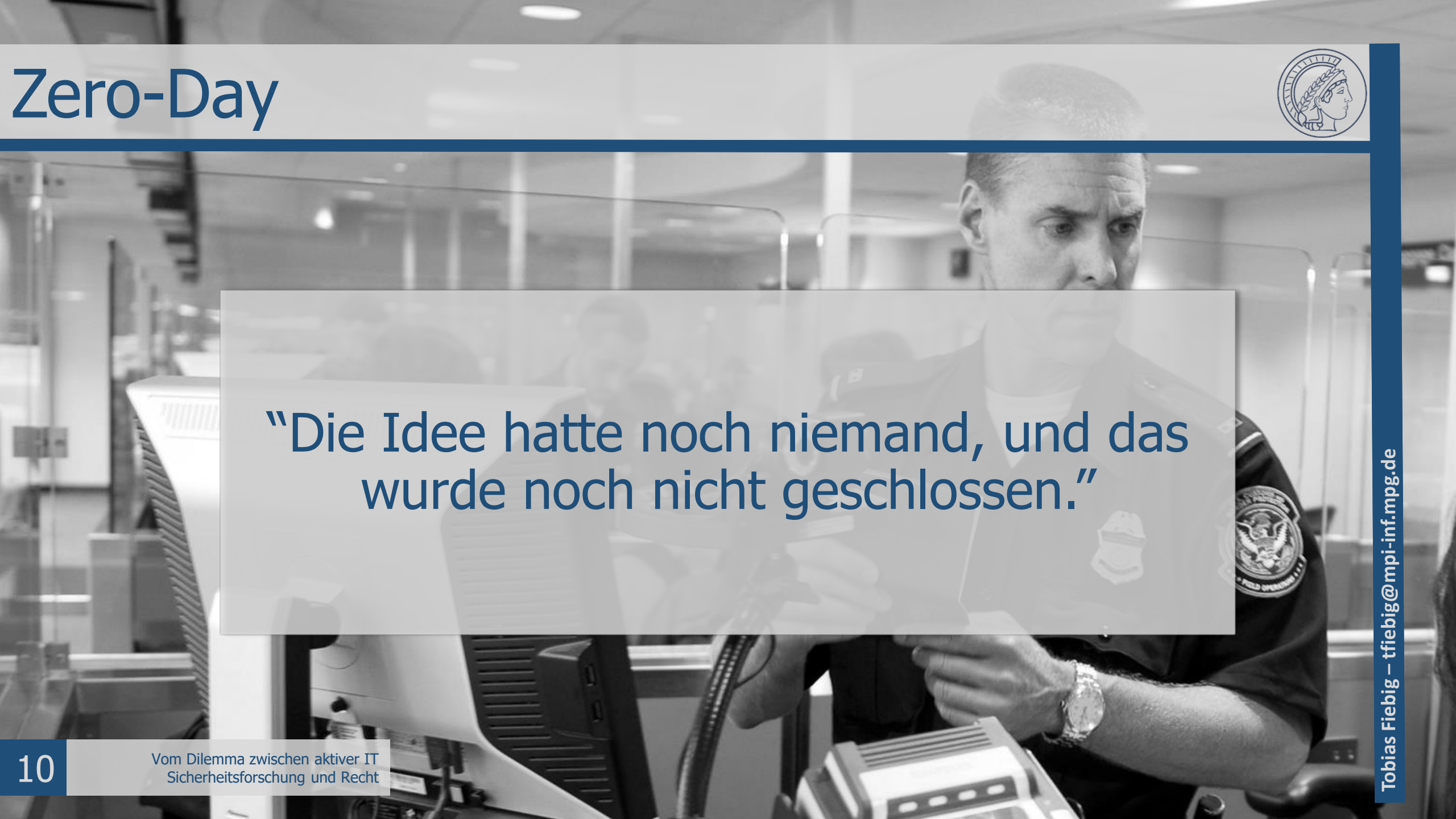
Tobias Fiebig – tfiebig@mpi-inf.mpg.de

Exploit



"Eine Schritt-für-Schritt Anleitung, wie sich die notwendigen Umstände erstellen lassen, um eine Lücke auszunutzen."

Zero-Day



"Die Idee hatte noch niemand, und das wurde noch nicht geschlossen."

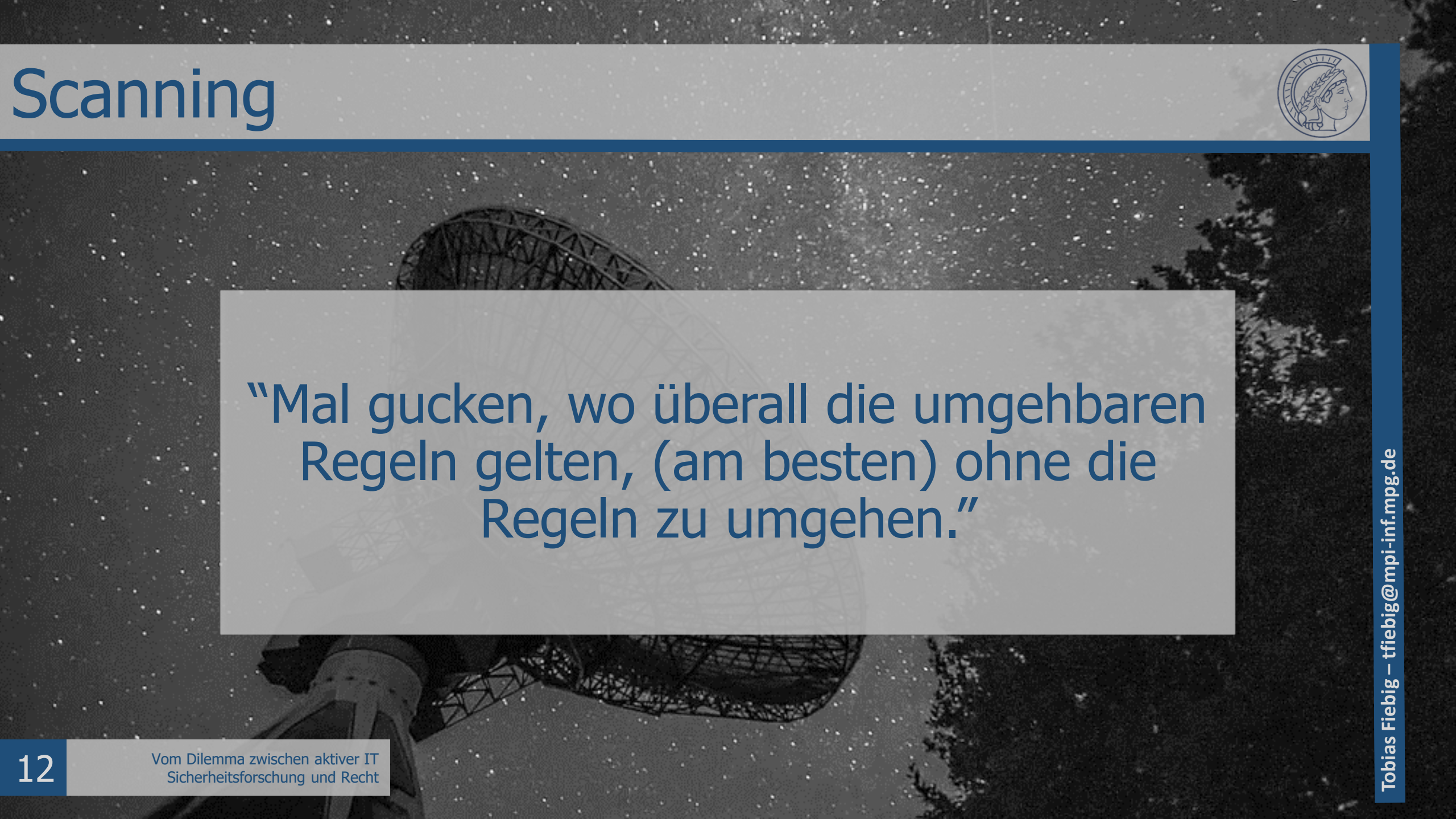
Tobias Fiebig – tfiebig@mpi-inf.mpg.de

Reverse Engineering

"Mal gucken, was die Regeln sind."

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

Scanning



"Mal gucken, wo überall die umgehbaren Regeln gelten, (am besten) ohne die Regeln zu umgehen."

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

Was wir so machen…

- Unter Nutzung einer Mechanik im Challenge-Response Mechanismus während der Authentifikation an einem SSH Server lässt sich bestimmen, ob ein bestimmter öffentlicher Schlüssel installiert wurde.
- Wir haben von einer AntiVirus Firma 52 öffentliche Schlüssel bekannter Angreifer erhalten; Dadurch können wir feststellen, ob diese Angreifer ein System kompromittiert haben.
- Wir führen nun Netzwerkscans durch, um kompromittierte Systeme zu finden. Diese Melden wir u.a. über das CERT-BUND automatisiert an Betroffene
- Wir konnten nahezu 20.000 kompromittierte Systeme im Internet identifizieren, und weitere Informationen zum MO und Systemen der Angreifer aus der Analyse der gesammelten Daten erlangen

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

“Freundliches Feed-Back”

Subject **Re: Abuse from 2a02:d480:4c0:10d4:42::1**

You know that those kind of measurements are illegal to addresses that do not explicitly authorize them?

Unless you refrain to scan our address space, we will open a courts case against the persons and institutions responsible for that scanning.

Subject **Re: Abuse from 2a02:d480:4c0:10d4:42::1**

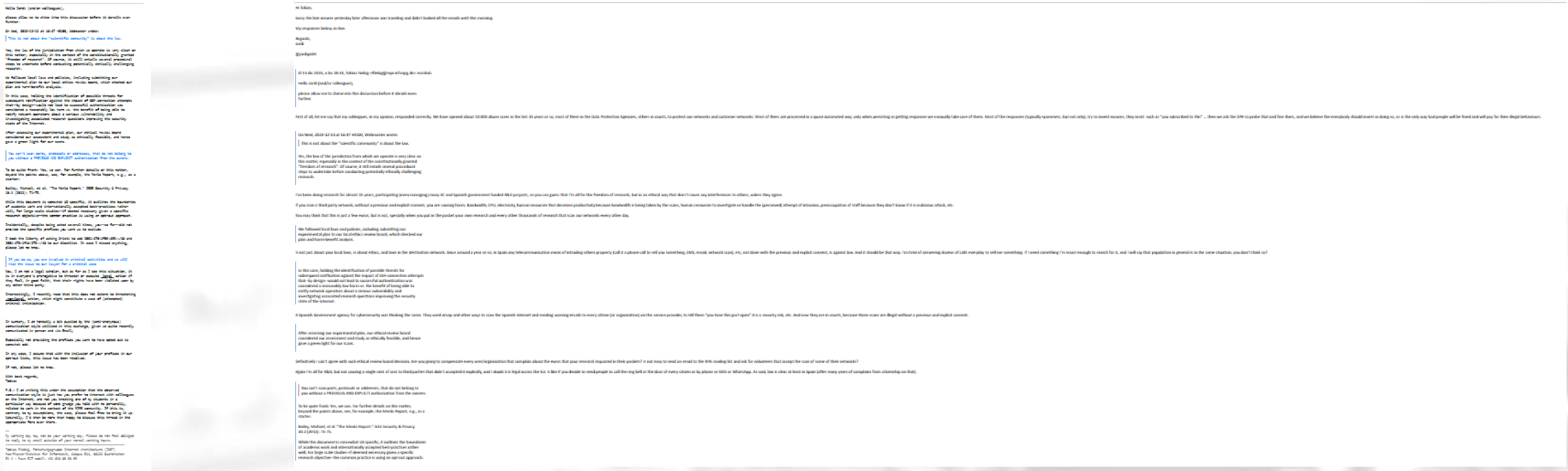
This is not about the "scientific community” is about the law.

You can’t scan ports, protocols or addresses, that do not belong to you without a PREVIOUS AND EXPLICIT authorization from the owners.

If you do so, you are involved in criminal activities and we will rise the issue to our lawyer for a criminal case and make it public in social networks.

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

“I am not a lawyer,…
…but if your lawyer let you do that, you *need* a new one…”



From Cristian Munteanu <cmuntean@mpi-inf.mpg.de>

To Tobias Fiebig <tfiebig@mpi-inf.mpg.de>

Subject **Fwd: Abuse from 2a02:d480:4c0:10d4:42::1**

Fallbeispiel I

- In *S*-Stadt treibt sich die Gruppe *G* herum, welche in Wohnungen einbricht. Nach einem Einbruch manipuliert die Gruppe das Schloss der Wohnungstür für einen einfachen Zugang. Alle Wohnungen eines Viertels werden dann zu einem späteren Zeitpunkt gleichzeitig geräumt.
- *A,* Wohnungssicherheitsforscher an der Univ. *S*-Stadt findet eine Methode um zu erkennen, ob eine Wohnungstür von der Gruppe *G* geöffnet und manipuliert wurde. Dabei wird ein Schlüssel in das Schloss gesteckt, welcher sich nur einführen lässt, wenn das Schloss von der Gruppe verändert wurde. Auch wenn er sich einführen lässt, lässt er sich nicht drehen, d.h., lässt sich das Schloss nicht öffnen.
- *A* geht nun alle Türen in *S*- Stadt ab, und meldet jene in welche sich der Test-Schlüssel einführen lässt, an die Polizei und die Bewohner.
- *A* identifiziert Über 10.000 gefährdete Wohnungen, und kann den Unterschlupf der Gruppe *G* identifizieren.
- *B* beobachtet *A* beim Einführen des Schlüssels, und erstattet Strafanzeige.

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

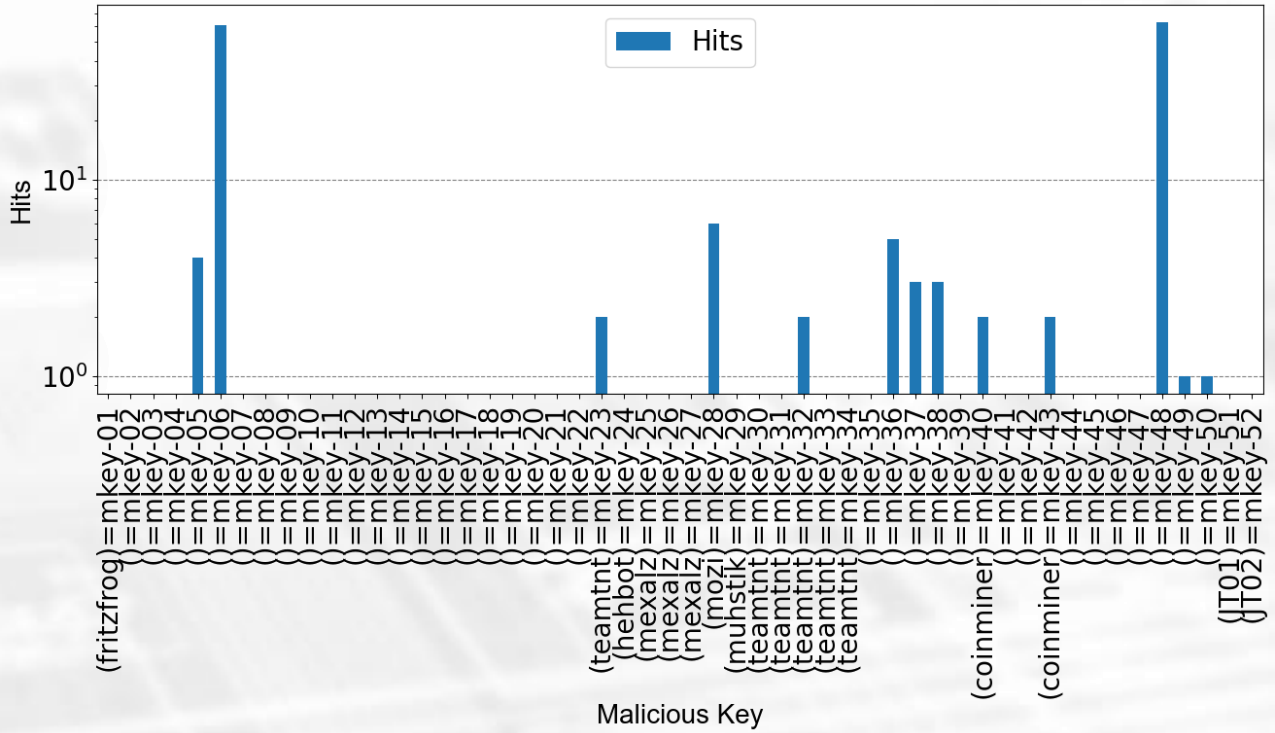
Regeln beim Scannen (Menlo Report)

- Identifizierbar sein
- Informationen Über das Forschungsvorhaben teilen (Website auf Scan-Maschinen)
- Freigabe der Ethikkommission einholen
- Opt-Out anbieten << !

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

Drehtür

- "Großer Hoster in einem großen zentraleuropäischem Land mit einer generell sehr ansprechenden Preisgestaltung"
- Opt-out vor recht langer Zeit
- Nach etwas Diskussion wieder in unserer Target-Liste



Tobias Fiebig – tfiebig@mpi-inf.mpg.de

Fallbeispiel II

- Gleiche Grundzustände wie in Fallbeispiel I
- Immobilienverwalter *V* verbietet *A* in von *V* betreuten Liegenschaften die Schlösser zu testen.
- *V* informiert die eigenen Mieter nicht über die Möglichkeit dieses Tests und führt diesen auch nicht selbst durch.
- *B* mietet eine von *V* verwaltete Wohnung und wird Opfer der Gruppe *G.*
- *B* lernt von *C*, dass *V* die Test welche die Vorhaben der Gruppe *G* bei *C* verhinderten verbot.
- *B* verlangt nun Schadenersatz von *V*.

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

Reverse Engineering

"Mal gucken, was die Regeln sind."

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

Das ist der Sonderzug…

…ins Wartungsdepot des Herstellers,…

…oder halt nirgendwo mehr hin.

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

Who you gonna call… ?

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

Beschaffungsrecht 101

- Genau so in Polen passiert; Neuausschreibung der Wartung.
- Korrekt:
  - Ausgeschrieben
  - Günstigsten Anbieter Ausgewählt
  - Beauftragt
  - Geliefert
- Natürlich mit Strafanzeige gg. die Hacker…
  - Talk: https://media.ccc.de/v/37c3-12142-breaking_drm_in_polish_trains
  - Bericht: https://arstechnica.com/tech-policy/2023/12/manufacturer-deliberately-bricked-trains-repaired-by-competitors-hackers-find/
- Something-something ‘Reverse Engineering’

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

SLAPP!

(Strategic Lawsuit Against Public Participation)

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

Klingt bekannt…

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

“Digitale Souveränität wird falsch verstanden.”

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

Was wir brauchen…

- Einfache(!) Rechtssicherheit
- Schutz vor SLAPP
- Klare Meldeketten
- Unabhängige, kompetente, proaktive Stellen
- Digitale Souveränität (Aber richtig!)
- Scans
  - Ausschalten statt sperren
- Reverse-Engineering
  - Keep em honest, keep it working.
- ‘Capabilities’. Viele.

Tobias Fiebig – tfiebig@mpi-inf.mpg.de