

Unwissenheit schützt vor Strafe nicht: Außer in der IT

Tobias Fiebig



- B.Sc. Cognitive Science (2012)
- M.Sc. System & Network Engineering (2013)
- Dr.-Ing. Network Measurement and IT Security (2017)
- Bis März 2022 Assistant Professor for Information System Security at TU Delft
- Seit April 2022 Max-Planck-Institut für Informatik





Jurist:innen

- Legen jedes Wort auf die Goldwaage
- Arbeiten mit einem großen Regelwerk mit vielen Kommentaren und noch mehr Interpretationsmöglichkeiten
- Antworten auf die einfachste fachliche Frage *immer* mit: "*Kommt drauf an...*"

Informatiker:innen

- Legen jedes Wort auf die Goldwaage
- Arbeiten mit einem großen Regelwerk mit vielen Kommentaren und noch mehr Interpretationsmöglichkeiten
- Antworten auf die einfachste fachliche Frage *immer* mit: "*Kommt drauf an...*"

Wir waren die mit der Definition von 'MUSS'



- The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.
 1. **MUST:** This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
 2. **MUST NOT:** This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.
- The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] **when, and only when, they appear in all capitals, as shown here.**

Die Vier Klassischen (Höheren) Naturgewalten



Sturm



5

Unwissenheit schützt vor Strafe nicht:
Außer in der IT

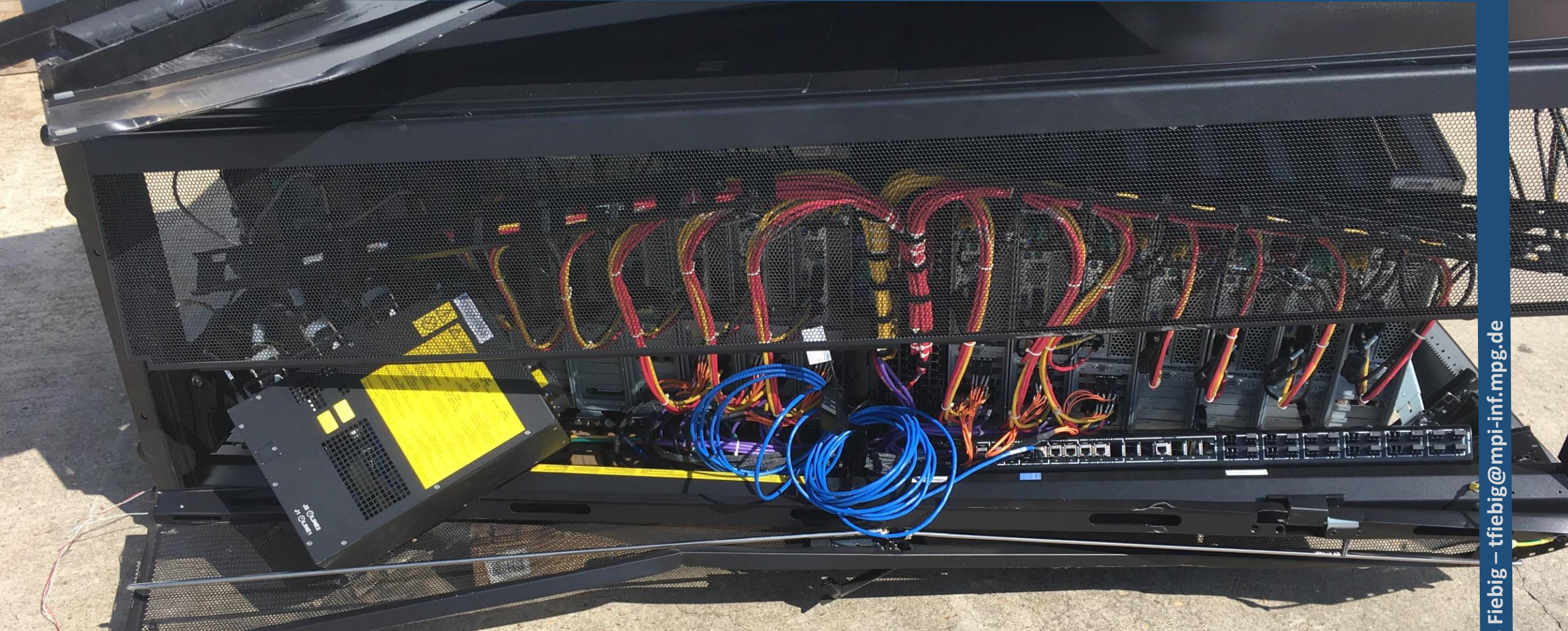
Feuer



Krieg



IT Sicherheitsumfälle



IT Sicherheitsumfälle



!?

Wir haben alles fuer die Sicherheit getan...



- "Mit hoher krimineller Energie..."
- "Das waren Hacker!"
- "Das war aber Illegal!"
- "Hochgradig professionelle staatlich instruierte Angreifer..."
- "Wir haben erst einmal Strafanzeige gg. Fr. W. erstellt."
- "Trotz AI-unterstützter Sicherheitsmaßnahmen..."
- "Nach dem Durchbrechen aller sechs Blockchains..."
- "Auch unsere Next-Generation-Firewall konnte nicht..."
- "Obwohl wir ISO-27001 und Common Criteria Certified sind..."



Search Results for "pass:"

www.linkedin.com/company/...
www.linkedin.com/company/...
www.linkedin.com/company/...

www.linkedin.com/company/...
www.linkedin.com/company/...
www.linkedin.com/company/...

www.linkedin.com/company/...
www.linkedin.com/company/...
www.linkedin.com/company/...

www.linkedin.com/company/...
www.linkedin.com/company/...
www.linkedin.com/company/...

www.linkedin.com/company/...
www.linkedin.com/company/...
www.linkedin.com/company/...

www.linkedin.com/company/...
www.linkedin.com/company/...
www.linkedin.com/company/...

www.linkedin.com/company/...
www.linkedin.com/company/...
www.linkedin.com/company/...

www.linkedin.com/company/...
www.linkedin.com/company/...
www.linkedin.com/company/...

www.linkedin.com/company/...
www.linkedin.com/company/...
www.linkedin.com/company/...

www.linkedin.com/company/...
www.linkedin.com/company/...
www.linkedin.com/company/...

www.linkedin.com/company/...

www.linkedin.com/company/...

www.linkedin.com/company/...
www.linkedin.com/company/...
www.linkedin.com/company/...

Security Misconfigurations





"Users Menschen finden eine Weg."

Menschliche Wegfindung



Secure | <https://www.shodan.io/host/79.7.88.196>

79.7.88.196 host196-88-static.7-79-b.business.telecomitalia.it

City	Turin
Country	Italy
Organization	Telecom Italia Business
ISP	Telecom Italia Business
Last Update	2017-12-20T12:13:45.187316
Hostnames	host196-88-static.7-79-b.business.telecomitalia.it
ASN	AS3269

Ports

- 8080

Services

- 8080 **trp** **http**
HTTP/1.0 200 OK
Content-Length: 1148
Cache-Control: no-cache no-store
Content-Type: text/html

© 2013-2017, All Rights Reserved - Shodan®



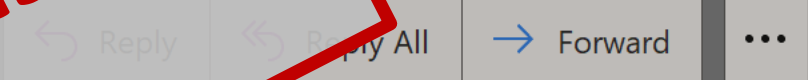
File Message Help Acrobat



A Data Management Plan in dmponline has been shared with you

 do-not-reply@[dcc.ac.uk](mailto:do-not-reply@dcc.ac.uk)
To t.fiebig@[tudelft.nl](mailto:t.fiebig@tudelft.nl)

← Andere Organisation



Tue 06/07/2021 00:48

Hello First Name Surname ← Keine persönliche Anrede

Your colleague do-not-reply@tudelft.nl has invited you to edit your Data Management Plan in dmponline

[Click here](#) to accept the invitation, (copy https://dmponline.tudelft.nl/users/invitation/accept?invitation_token=z_ez#/ into your browser). If you don't want to accept this invitation, please ignore this email.

All the best
The dmponline team

Please do not reply to this email. If you have any questions or need help, please contact us at dmponline@dcc.ac.uk

← Externe Kontaktadresse

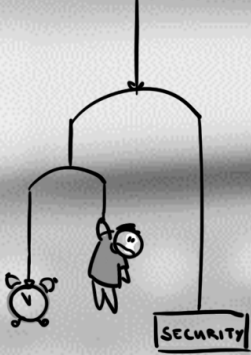
<https://dmponline.tudelft.nl/contact-us>

← Interner Dienst mit anderer Domain

Definitiv Echt und kein Phishing, trust me bro!



Enterprise ‚Security‘



"Equifax was ISO-27001 certified."

- Me

"And then he said: 'There is no way they are not getting certified, if they buy it from us.'"

- Anonymous Big-4 Intern

Network Segmentation





- Schlicht *DIE* Definition von 'Enterprise'
 - Kein segmentiertes Netzwerk
 - Keine Backups des zentralen Active Directory
 - Kein...
-
- "Was machen die eigentlich Beruflich?!"

Unmittelbarer (Betrieblicher) Zwang (UBZ / [ʊps])



- "Da muss erstmal einer drauf kommen."
- "Das fixen wir, wenn es erstmal live ist!"
- "Ach, mein Neffe kann das auch."
- "Das haben wir schon immer so gemacht."
- "Ja, aber dann wird das so kompliziert!"
- "Das hat mir die Maria beim Golfen erzählt; Bei \$big_corp machen die jetzt alles so!"
- "Natürlich muss die Rechnungsabteilung auch voll integrierte AD-Managed Clients haben! COMPLIANCE!"
- "Also die Systemadministration macht der CTO bei uns ja so nebenbei."



VIRT04.DUS01.AS59645.NET



VIRT03.DUS01.AS59645.NET



VIRT02.DUS01.AS59645.NET



“Sicherheit ist ein Effekt, und kein Ziel.”

Email: contact@as59645.net

Phone:

VIRT01.DUS01.AS59645.NET





Max-Planck-Institut
für Informatik

-- FOR PUBLIC RELEASE --

Confidential information has been redacted in this version of the document.

Report on the Security State of Networks of Max-Planck Institutes

Findings and Recommendations

Ein Ring...

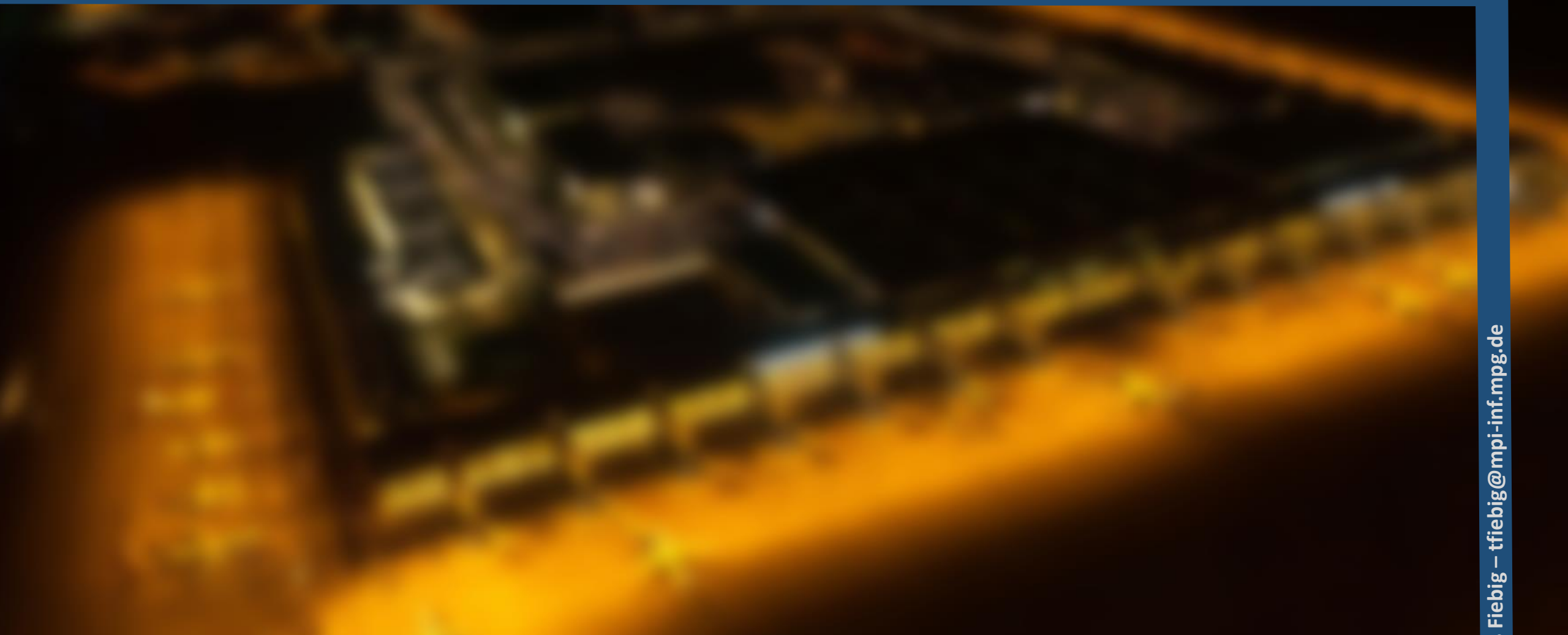


Sicherheit ist, wenn man es richtig macht...



"(IT) Sicherheit ist ein Effekt davon, 'alles' richtig zu machen, auch wenn dies of nicht offensichtlich sicherheitsrelevantes oder gar technisches betrifft. Es ist kein 'Ziel' was sich durch Technologie allein erreichen lässt."

“Wie lassen ja auch keinen Bauzeichner
eine Brandschutz-Anlage planen...”



“Wie lassen ja auch keinen Bauzeichner eine Brandschutz-Anlage planen...”



Vor der Heimfahrt Tanken



Laut einer Pressemitteilung der Polizei trug die Laterne weder eine Warnweste, noch einen Helm; Das Licht war jedoch eingeschaltet.

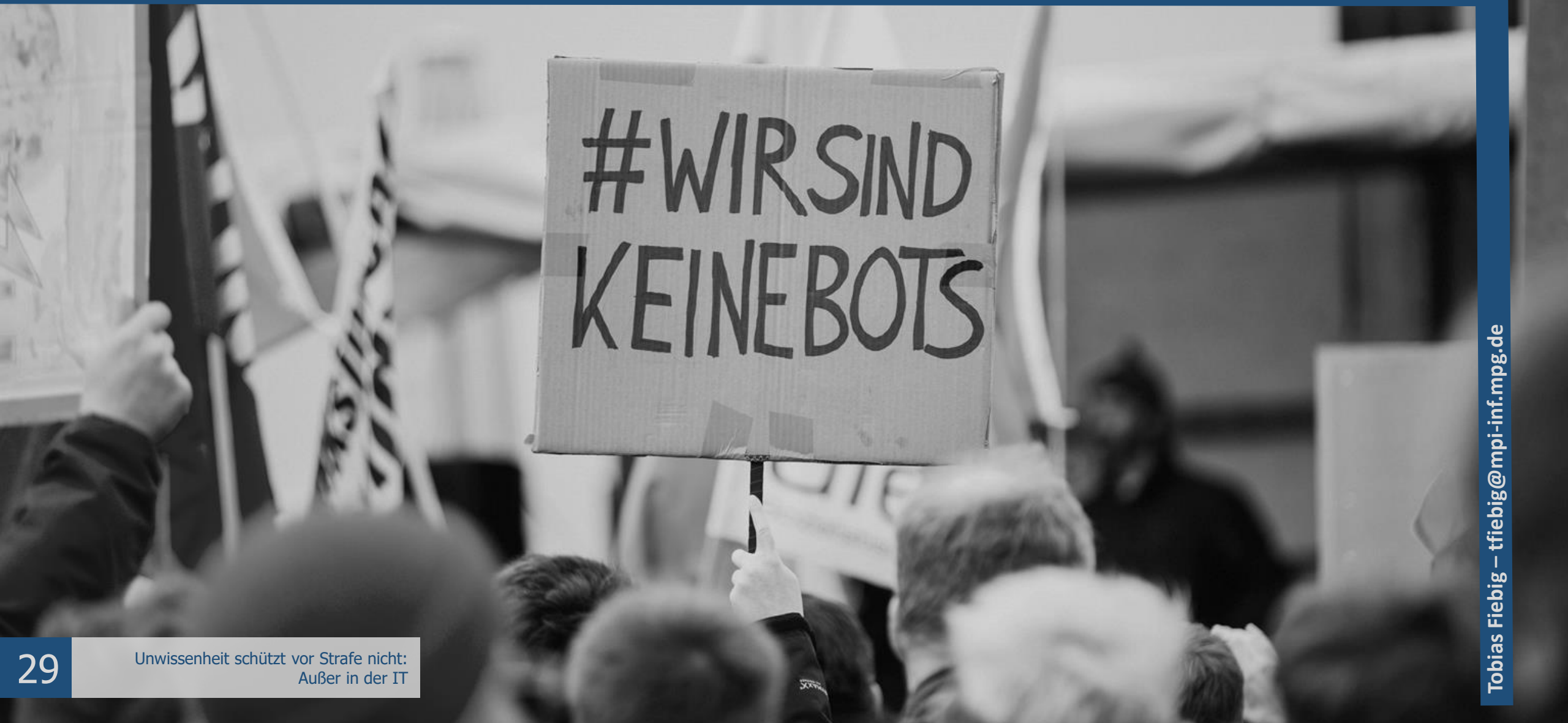


Spontanmeldung zur Hauptuntersuchung



Reverse Engineering & Aktive Forschung

(Nach Prof. Dr. Grimm, einer Pause, Dr. Heck & Dr. Stock)



#WIRSIND
KEINEBOTS



- Grade Firmen neigen dazu, eigene Nachlässigkeit im Infrastrukturbetrieb herunter zu spielen
- Das Strafrecht ist für Firmen hier leider oft Hilfreich
- Top-Down Governance macht die Welt nicht zwangsläufig besser
- Wir brauchen einen generellen Wandel hin zu einem ordentlichen IT Ingenieurwesen; In der Medizin wird auch schneiden gelernt.
- Ich suche eine Staatsanwaltschaft mit Interesse an einer Bestandsdatenauskunft; Kontakt: tfiebig@mpi-inf.mpg.de