IT-Sicherheit:
Ein Kampf gegen Windmühlen

Prof. Dr.
Dominik Herrmann

Privacy and Security Group
Universität Bamberg

Twitter: @herdom

Folien: dhgo.to/windmuehlen

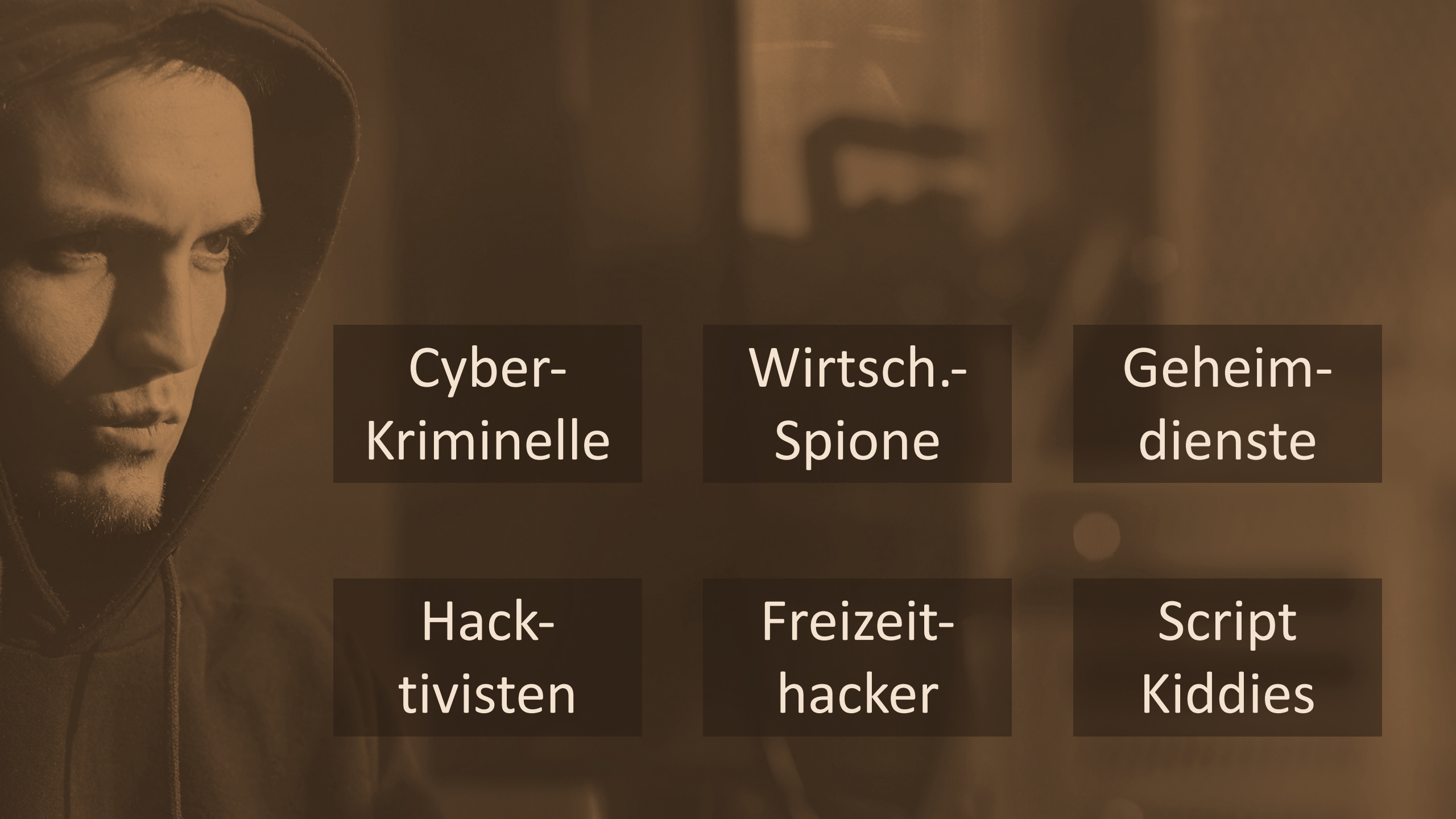
Ist die Aufrechterhaltung der IT-Sicherheit (in Zeiten von Ransomware, Home Office, IoT und Industrie 4.0) wirklich ein aussichtsloser Kampf?

Ja*

Brauchen wir neue Tools?

Nein

*Gabler Wirtschaftslexikon zu „Cybersecurity“


Cyber-
Kriminelle
Wirtsch.-
Spione
Geheim-
dienste
Hack-
tivisten
Freizeit-
hacker
Script
Kiddies

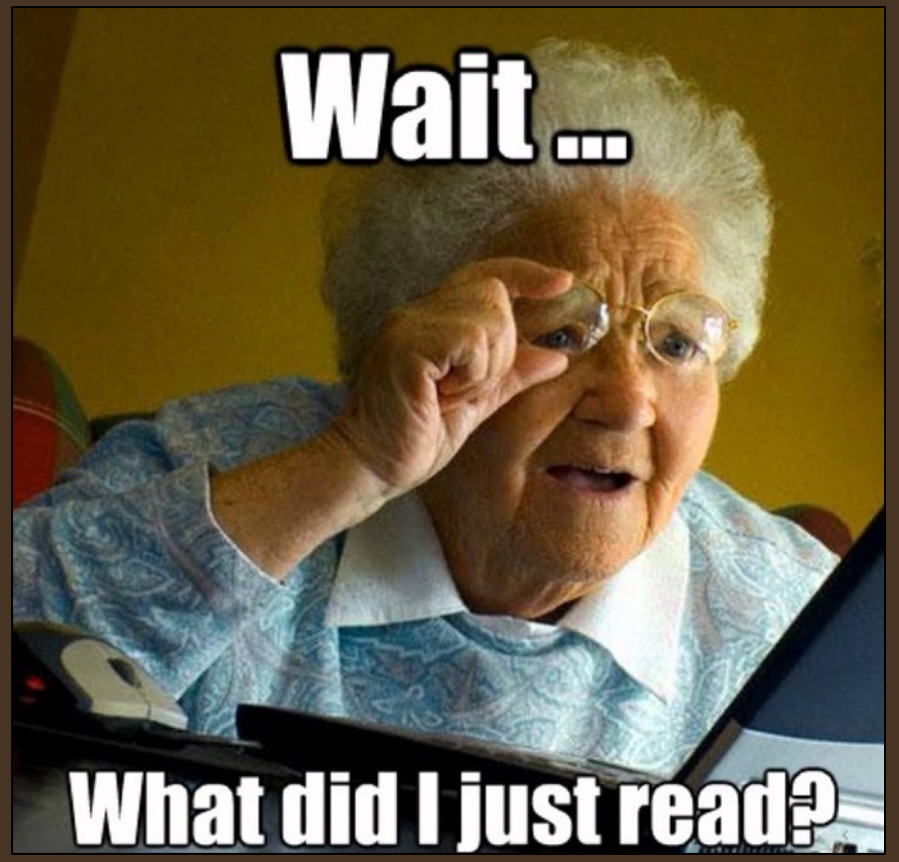
Wem müssen wir vertrauen, damit wir gut geschützt sind?

unseren Anwendern und Administratoren,

unseren Zulieferern und deren Zulieferern,

den Herstellern der bei uns und dort eingesetzten Hard- und Software,

den Zulieferern dieser Hersteller …
… und deren Zulieferern … deren Hard- …




100%-ige
Sicherheit
gibt es halt
nicht.

Fehlende IT-Sicherheit verursacht enorme Schäden! (sagt wer?)

Gartner: $ 3,2 Mrd.

FTC: $ 57 Mrd.

Norton: $ 114 Mrd.

McAfee: $ 1 Bio.

Vorteil der Angreifer – Dilemma der Verteidiger

M. Howard and D. LeBlanc: Writing Secure Code. Microsoft Press, 2002.

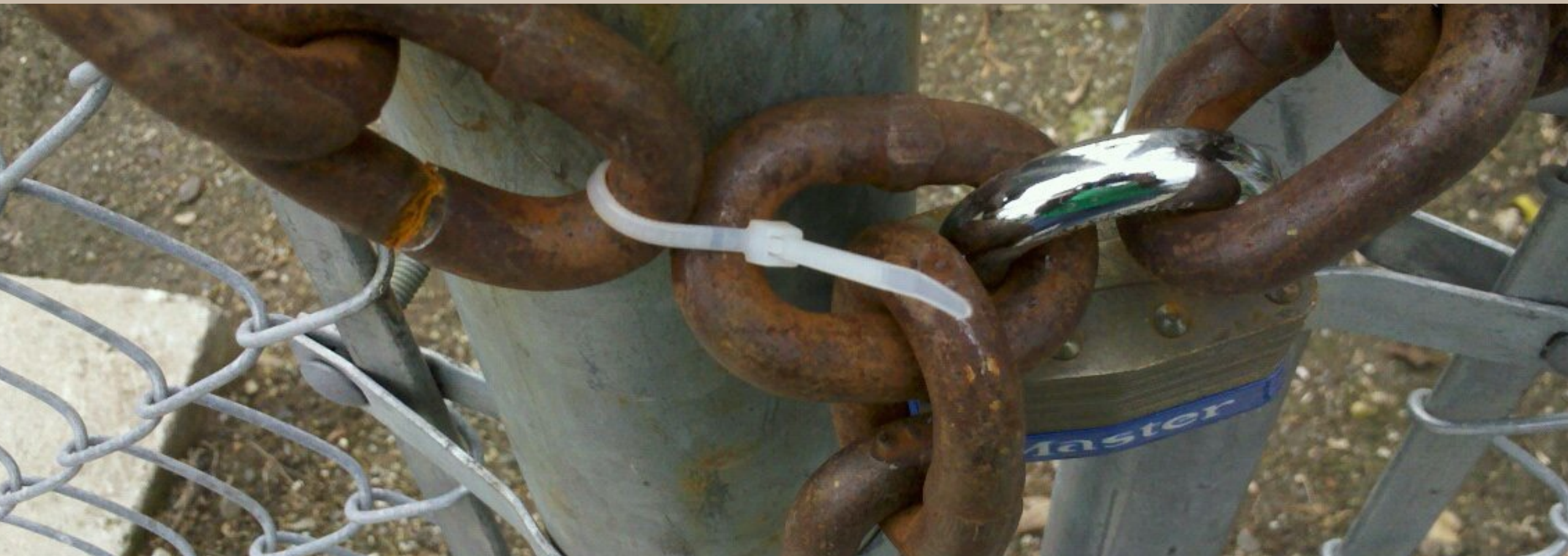
#1: Verteidigung **überall** erforderlich, Angreifer kann sich schwächste Stelle aussuchen.

#2: Verteidigung nur **gegen bekannte Angriffe** möglich, Angreifer kann nach unbekannten Schwachstellen suchen.

#3: Verteidigung erfordert **ununterbrochene Wachsamkeit**, Angreifer kann sich Zeitpunkt aussuchen.

#4: Verteidigung muss sich **an die Regeln halten**, Angreifer kann schmutzige Tricks einsetzen.

Menschen sind bekanntlich das schwächste Glied in der Kette



Former Equifax CEO blames breach on a single person who failed to deploy patch

10

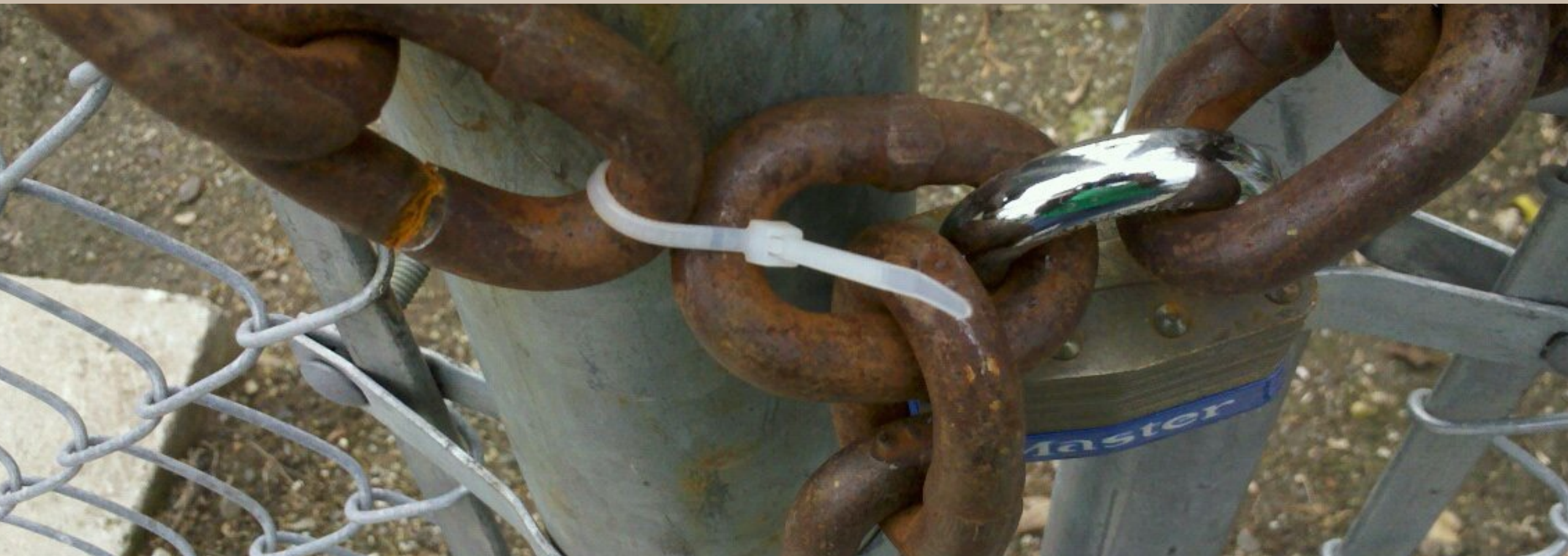
The company is still investigating

By Russell Brandom | Oct 3, 2017, 1:03pm EDT | 10 comments

... Im Sommer wurden durch einen Einbruch bei der Kreditauskunftei Equifax sensible Daten von mehr als 145 Mio. Menschen kompromittiert ... Die Angreifer scheinen eingedrungen zu sein, indem sie eine **öffentliche Schwachstelle in der Apache Struts-Software ausnutzten**, aber zum Zeitpunkt der Kompromittierung war ein Patch für diese Schwachstelle bereits **seit Monaten verfügbar**.

Smith machte **eine bestimmte Person**, deren Namen er nicht nennen wollte, für das anfängliche Versäumnis des Patches **verantwortlich**. "Der menschliche Fehler bestand darin, dass **die Person, die für die Kommunikation in der Organisation verantwortlich ist, um den Patch anzuwenden**, dies nicht tat", sagte Smith in der Anhörung.

Menschen sind bekanntlich das schwächste Glied in der Kette



Alles hängt also von **EINER** Person ab?

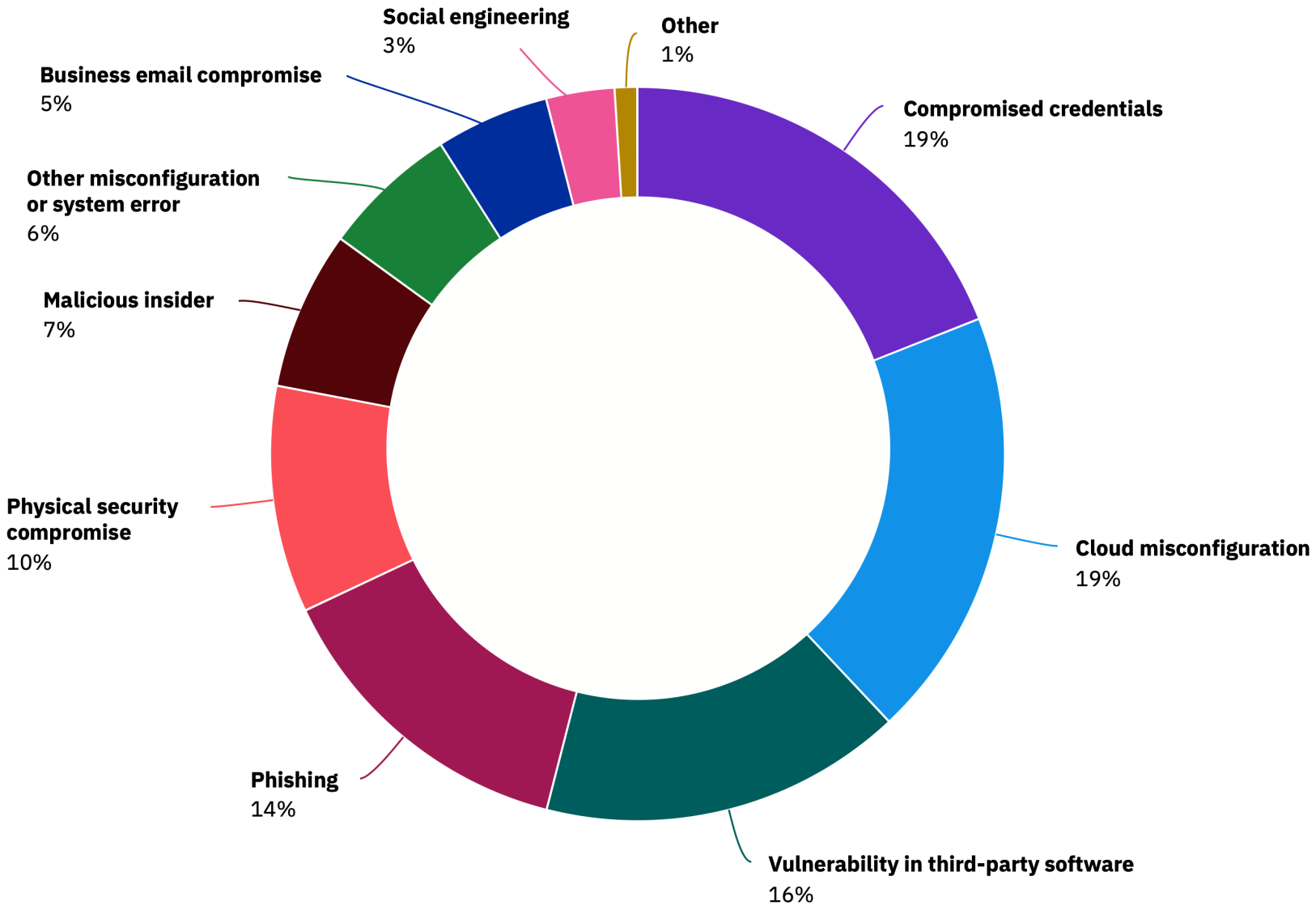
Ja, Menschen sind **sehr oft** die Ursache für erfolgreiche Angriffe.

Sie werden daher oft als **Gegner** angesehen, die im Zaum gehalten werden müssen.

Ponemon Institute
2020 *Cost of Data Breach Report*

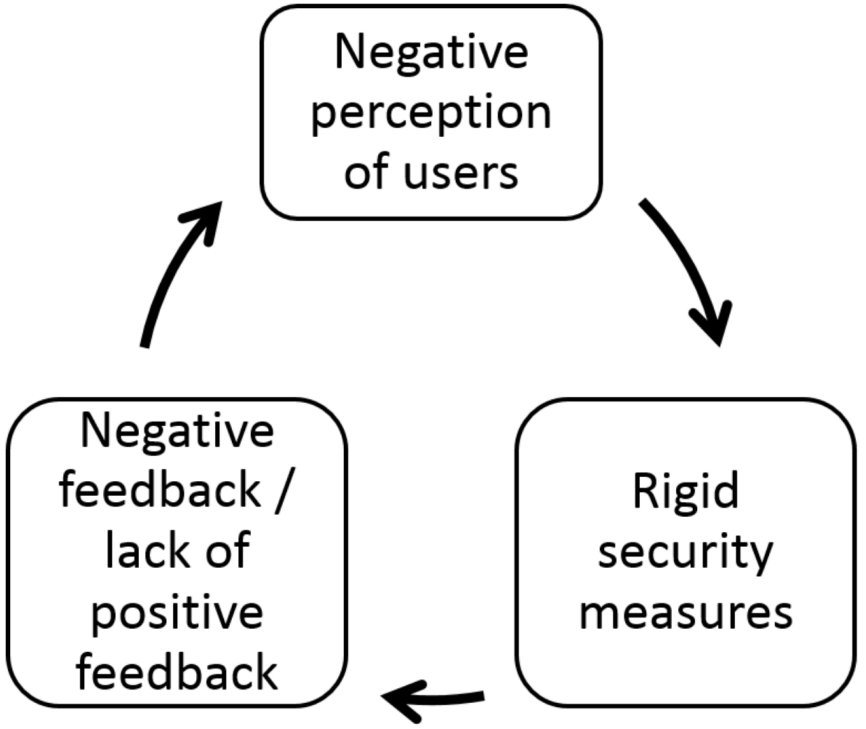
Breakdown of malicious data breach root causes by threat vector

Percentage of breaches caused by malicious attack



Wie denken IT-Sicherheitsmanager über Anwender?

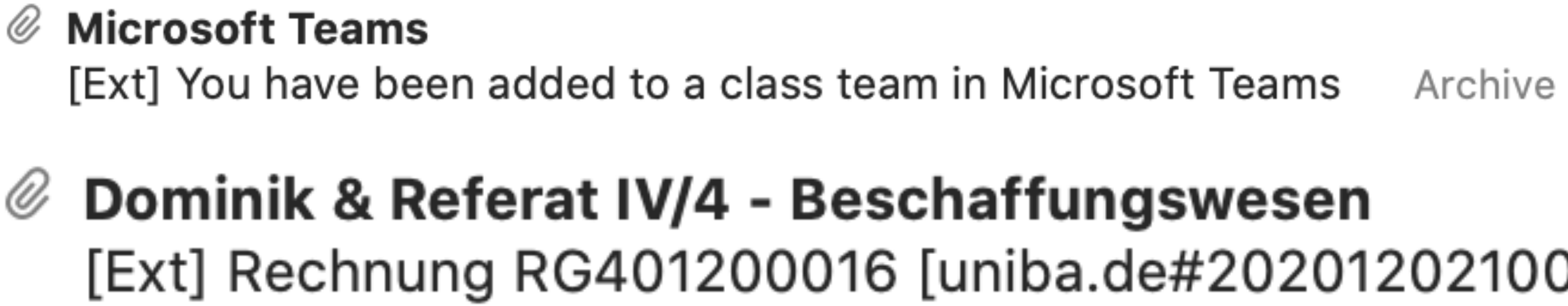
- Benutzer sind unkontrollierbar.
- Tappen trotz aller Sicherheitsmaß-nahmen in die Fallen der Angreifer.
- Meist negative Rückmeldungen, z.B. dass etwas nicht funktioniert oder länger dauert.
- Wenn eine Sicherheitsmaßnahme nicht nach ihrem Geschmack ist, gehen sie „auf die Barrikaden“.



Reinfelder et al. Security Managers Are Not The Enemy Either (CHI19).

Technische Maßnahmen
sind oft unbenutzbar.

„ab … werden alle E-Mails im Betreff mit **[EXT]** (für extern) ergänzt, wenn sie von außerhalb der Universität Bamberg stammenden E-Mail-Servern kommen. Damit sollen E-Mail-Empfänger unterstützt werden, Phishing-E-Mails leichter zu erkennen. Es wäre nämlich seltsam, wenn Sie beispielsweise eine E-Mail von einem Mitarbeiter der Universität Bamberg erhalten würden, die zusätzlich mit [EXT] im Betreff versehen ist. Bitte richten Sie besonderes Augenmerk auf alle E-Mails, die die Ergänzung "[EXT]" haben, insbesondere wenn der übrige Inhalt vorgibt, dass er von einem Absender aus der Universität Bamberg stammt."



Technische Maßnahmen
sind oft unbenutzbar.

Security Fatigue
(Konditionierung)

Kein Wunder, dass Anwender Warnungen ignorieren. Tatsächlich handeln sie dabei völlig rational!

So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users
Cormac Herley (Microsoft), NSPW, April 2009.

„Es wird oft behauptet, dass die Benutzer hoffnungslos faul und unmotiviert sind, wenn es um Sicherheitsfragen geht.

Wir argumentieren, dass **die Ablehnung der Sicherheitshinweise**, die die Nutzer erhalten, **aus wirtschaftlicher Sicht** völlig rational ist.

Die Hinweise schützen vor den **direkten Kosten der Angriffe**, belasten sie aber mit indirekten Kosten, den **externen Effekten**.

… zeigt sich, dass der Aufwand für die Befolgung der Sicherheitsempfehlungen tatsächlich **größer ist als die direkten Verluste**, die durch den Angriff verursacht werden.“

Schätzungen: US-Bürgern entsteht nur 20–30 USD Schaden durch Cybercrime (Breen et al.: A Large-Scale Measurement of Cybercrime Against Individuals, CHI 22)

Was sollen wir denn nun tun?

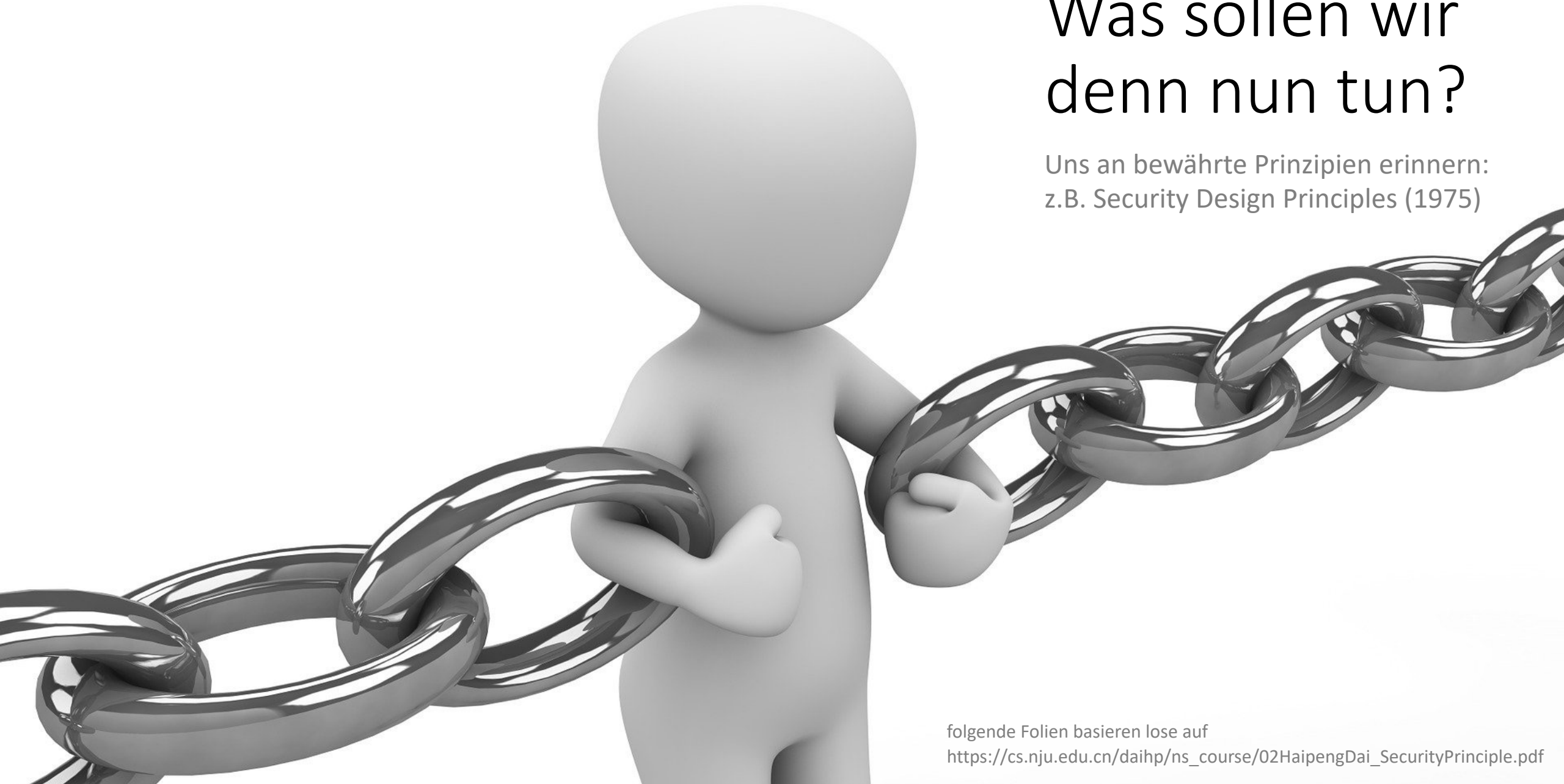
Was davon machen Sie?

regelmäßige Backups	Antivirus-Software	Firewall	
Regelmäßige Updates	Backups getrennt speichern	feingranulare Zugriffskontrolle	Passwort-richtlinie
Security Policy	Plan für Vorfalls-behandlung	Security Policy durchsetzen	Sicherheits-Trainings
Risiko-analyse	Notfall-übungen	IT-Sicherheits-zertifizierung	

Huaman et al. (2021). A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises. USENIX Security.

Was sollen wir denn nun tun?

Uns an bewährte Prinzipien erinnern:
z.B. Security Design Principles (1975)



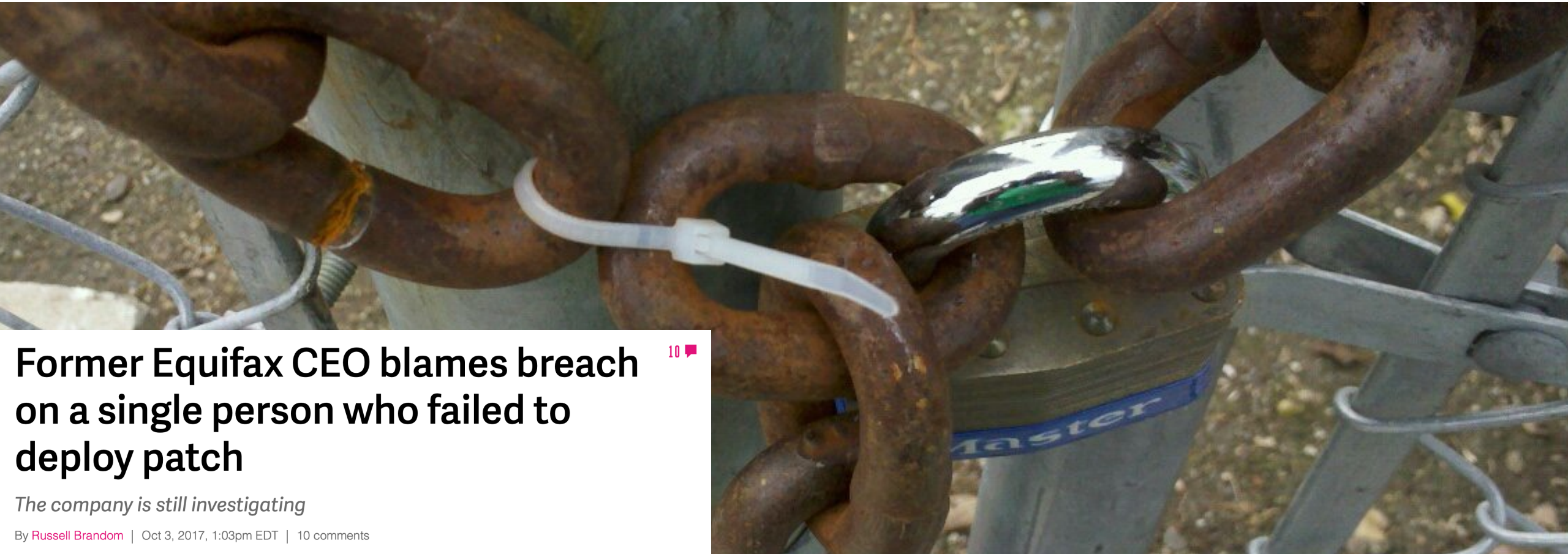
folgende Folien basieren lose auf
https://cs.nju.edu.cn/daihp/ns_course/02HaipengDai_SecurityPrinciple.pdf

#1 Das schwächste Glied stärken: Awareness-Kampagnen und Trainings

etwa Fake-Phishing-Kampagnen

nicht besonders effektiv (nur kurzfristig)

Sicherheit nur so gut wie das schwächste Glied der Kette – na hoffentlich nicht!



10

Former Equifax CEO blames breach on a single person who failed to deploy patch

The company is still investigating

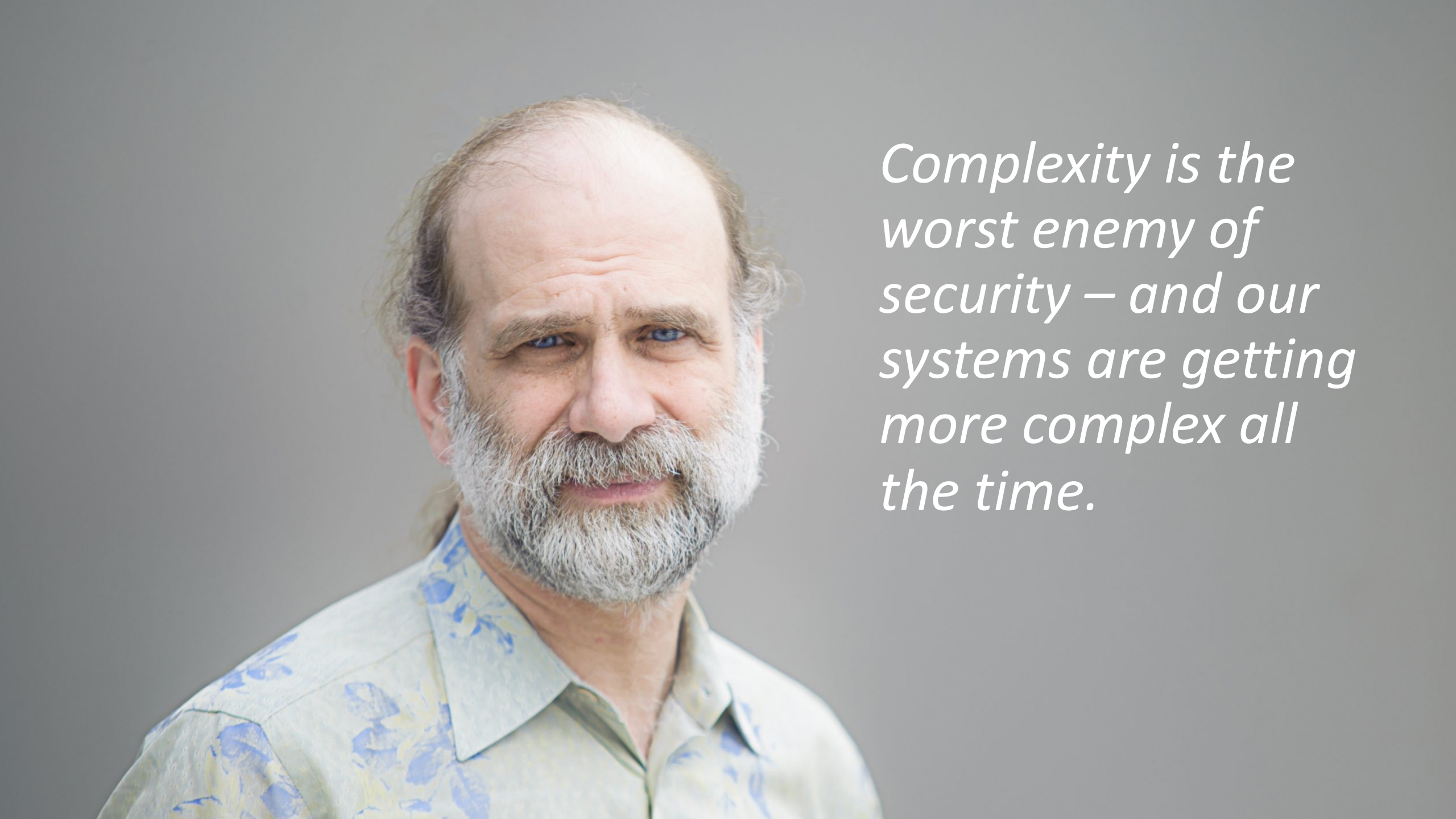
By Russell Brandom | Oct 3, 2017, 1:03pm EDT | 10 comments

#2 Defense in Depth: Fehlertoleranter werden

#3 Fail Safely

#4 Least Privilege
nur so viele Berechtigungen wie nötig

#5 Compartmentalization
Abschottung einzelner Systeme

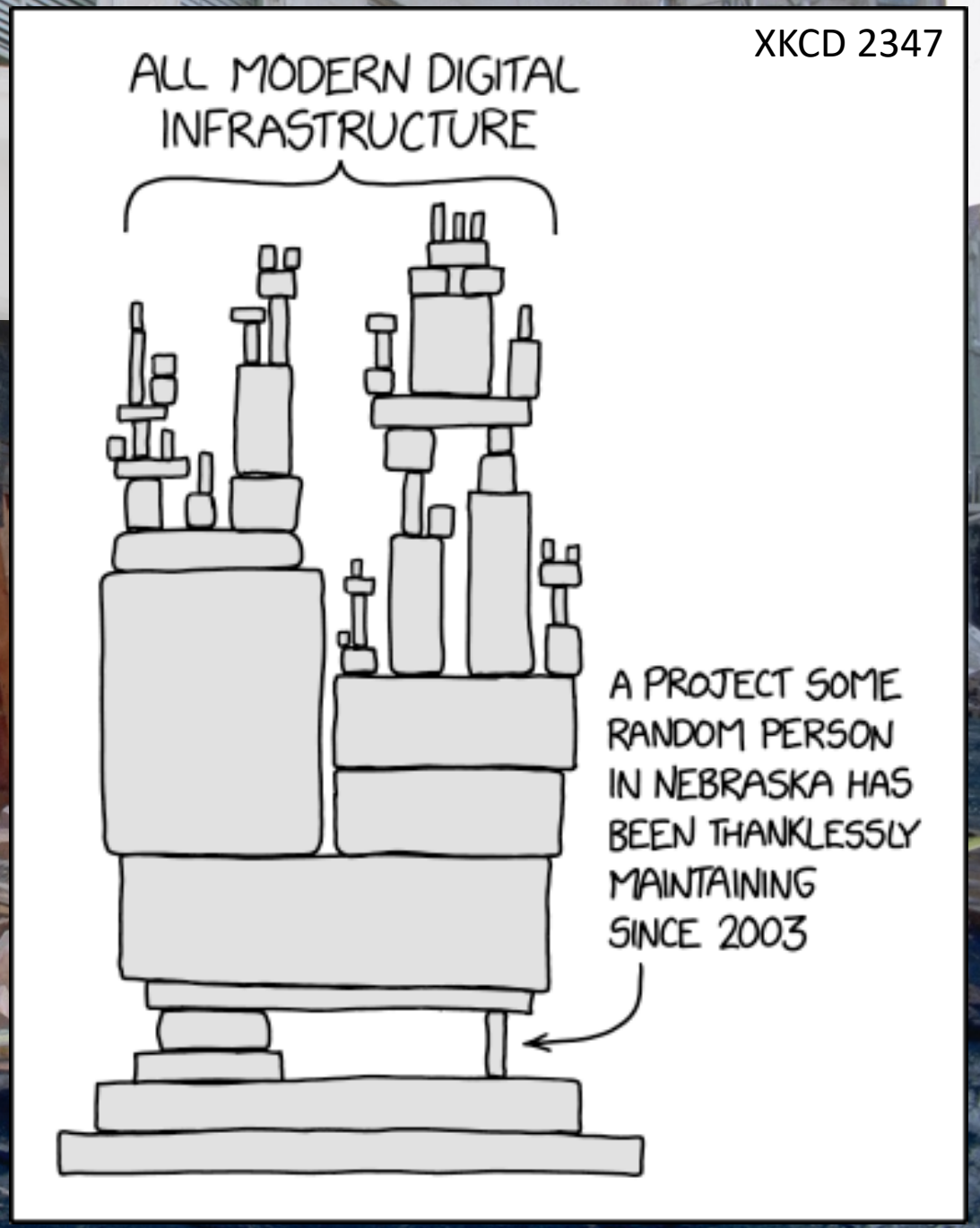

Complexity is the worst enemy of security – and our systems are getting more complex all the time.

#6 Einfachheit

#7 Keine “Security by Obscurity”

#8 Sparsamer Umgang mit Vertrauen

Schwer kalkulierbare Risiken durch Abhängigkeit von Drittanbietern



https://imgs.xkcd.com/comics/dependency_2x.png

Schwer kalkulierbare Risiken durch Abhängigkeit von Drittanbietern

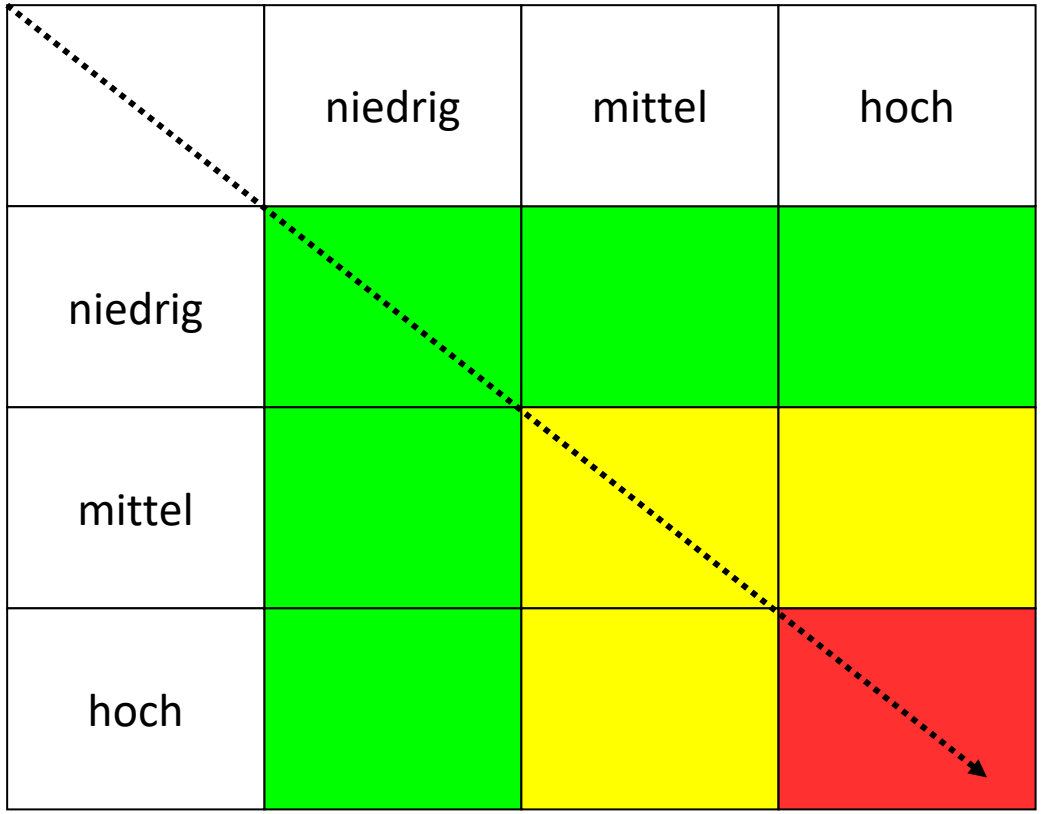
Jira und Confluence: Atlassian rechnet mit weiteren 2 Wochen Ausfall

Seit einer Woche hält der Ausfall der Cloud-Dienste des Softwareentwicklers Atlassian bereits an. Für viele Kunden ist das mehr als ärgerlich. Jetzt gibt es zumindest eine Schätzung, wann die Dienste wieder voll einsatzfähig sein werden.

Von **Brian Rotter**

12.04.2022, 15:30 Uhr • 1 Min. Lesezeit

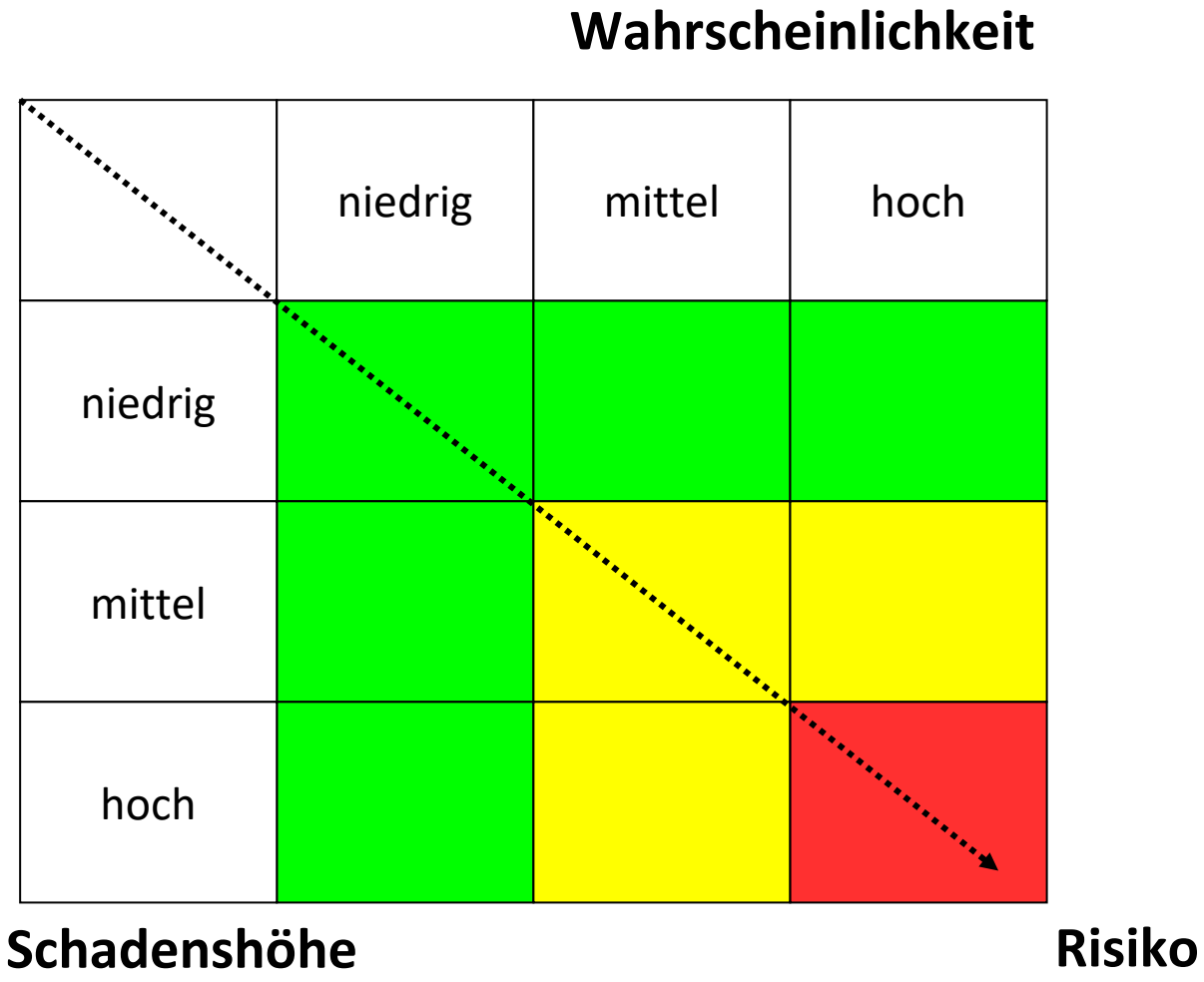
Wahrscheinlichkeit

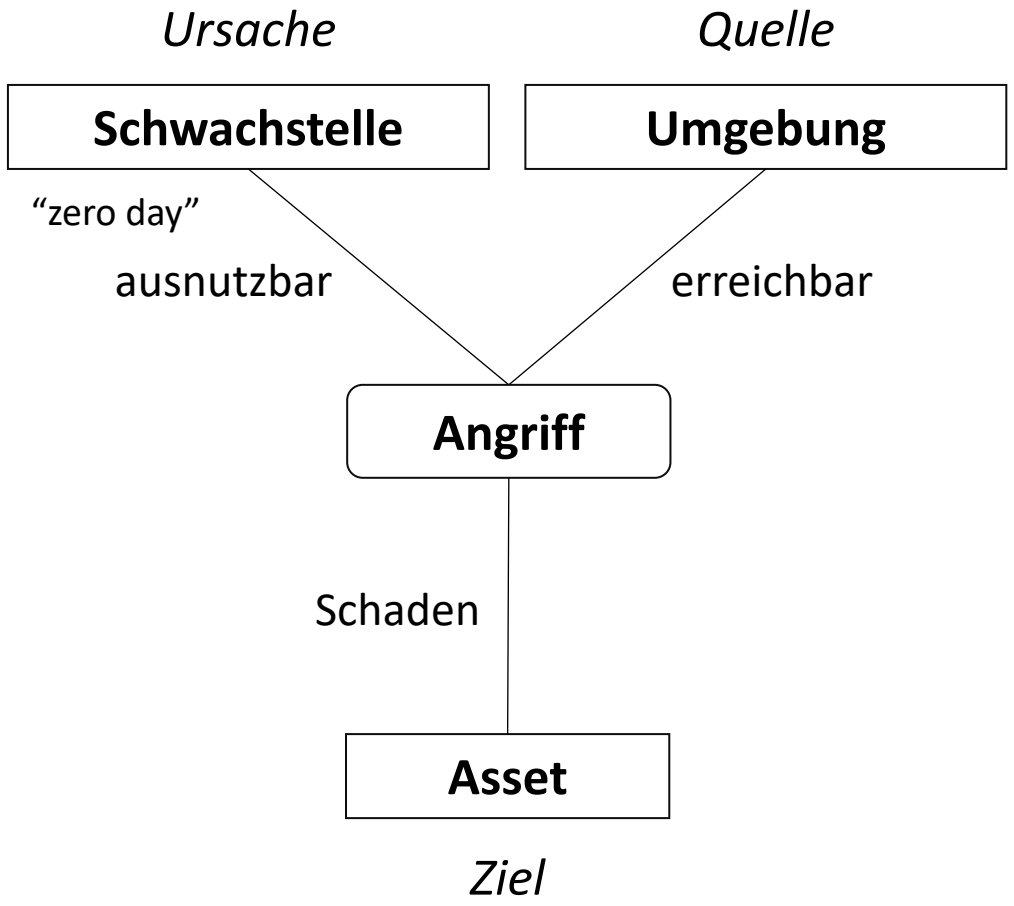


Schadenshöhe

Risiko

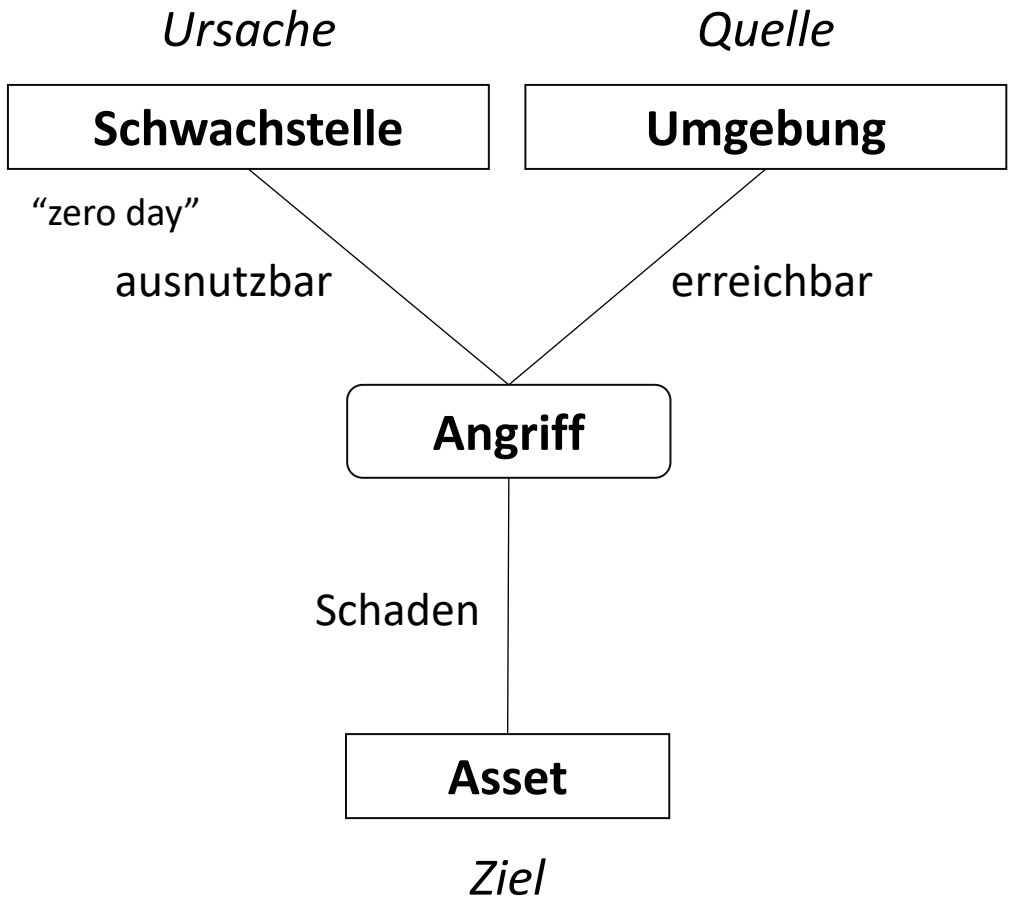
Haben Sie Ihre Risiken erhoben?


Wahrscheinlichkeit
niedrig
mittel
hoch
niedrig
mittel
hoch
Schadenshöhe
Risiko


Ursache
Quelle
Schwachstelle
Umgebung
“zero day”
ausnutzbar
erreichbar
Angriff
Schaden
Asset
Ziel

Wann und wo entstehen Schwachstellen?

– Design
– Programmierung
– Konfiguration
– Betrieb



Wann und wo entstehen Schwachstellen?

– Design
– Programmierung
– Konfiguration
– Betrieb

Alert!

Jetzt patchen! Lage um Attacken auf Atlassian Confluence spitzt sich zu

Aufgrund von öffentlich verfügbarem Exploit-Code steigen die Attacken auf Confluence-Instanzen. Patches sind jetzt verfügbar.

Lesezeit: **2 Min.** In Pocket speichern 4

06.06.2022 10:57 Uhr | **Security**

Von Dennis Schirrmacher

Alert!

Nutzer-Account mit Standard-Passwort gefährdet Atlassian Confluence

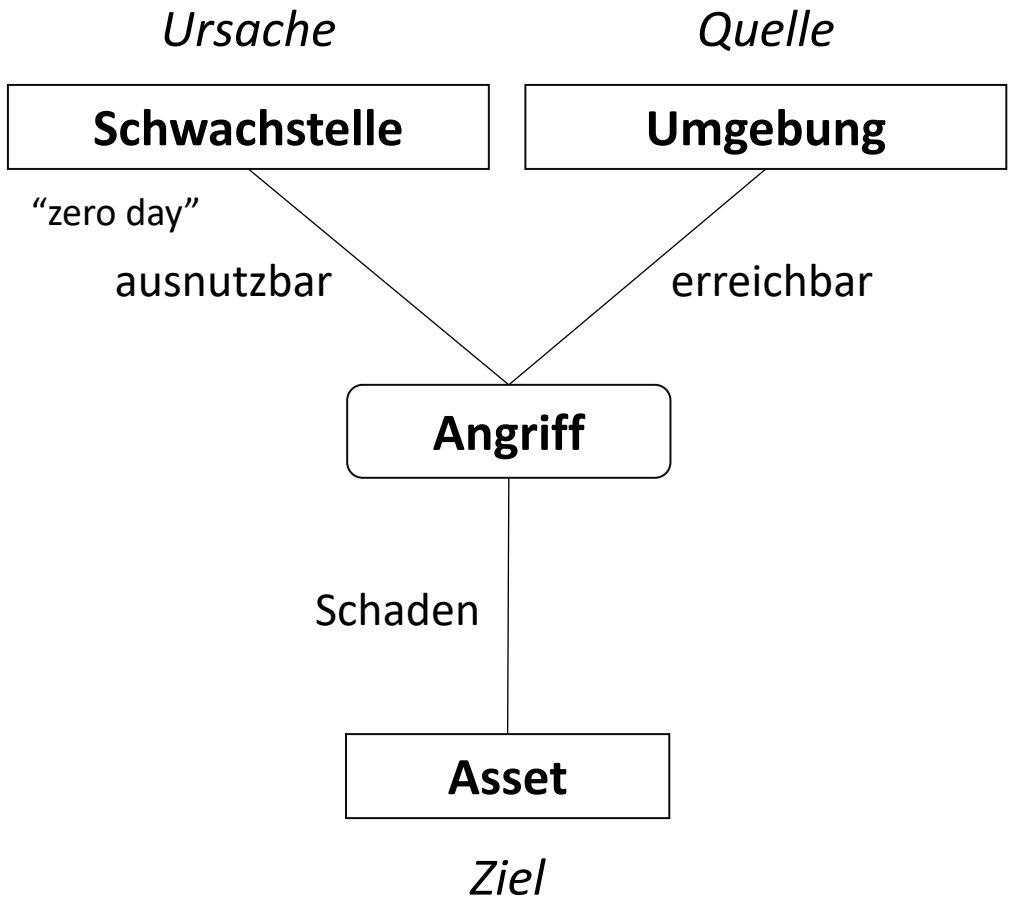
Unter bestimmten Voraussetzungen könnten Angreifer Atlassian Confluence Server und Data Center attackieren. Das Sicherheitsrisiko gilt als kritisch.

Lesezeit: **2 Min.** In Pocket speichern 18

21.07.2022 10:22 Uhr | **Security**

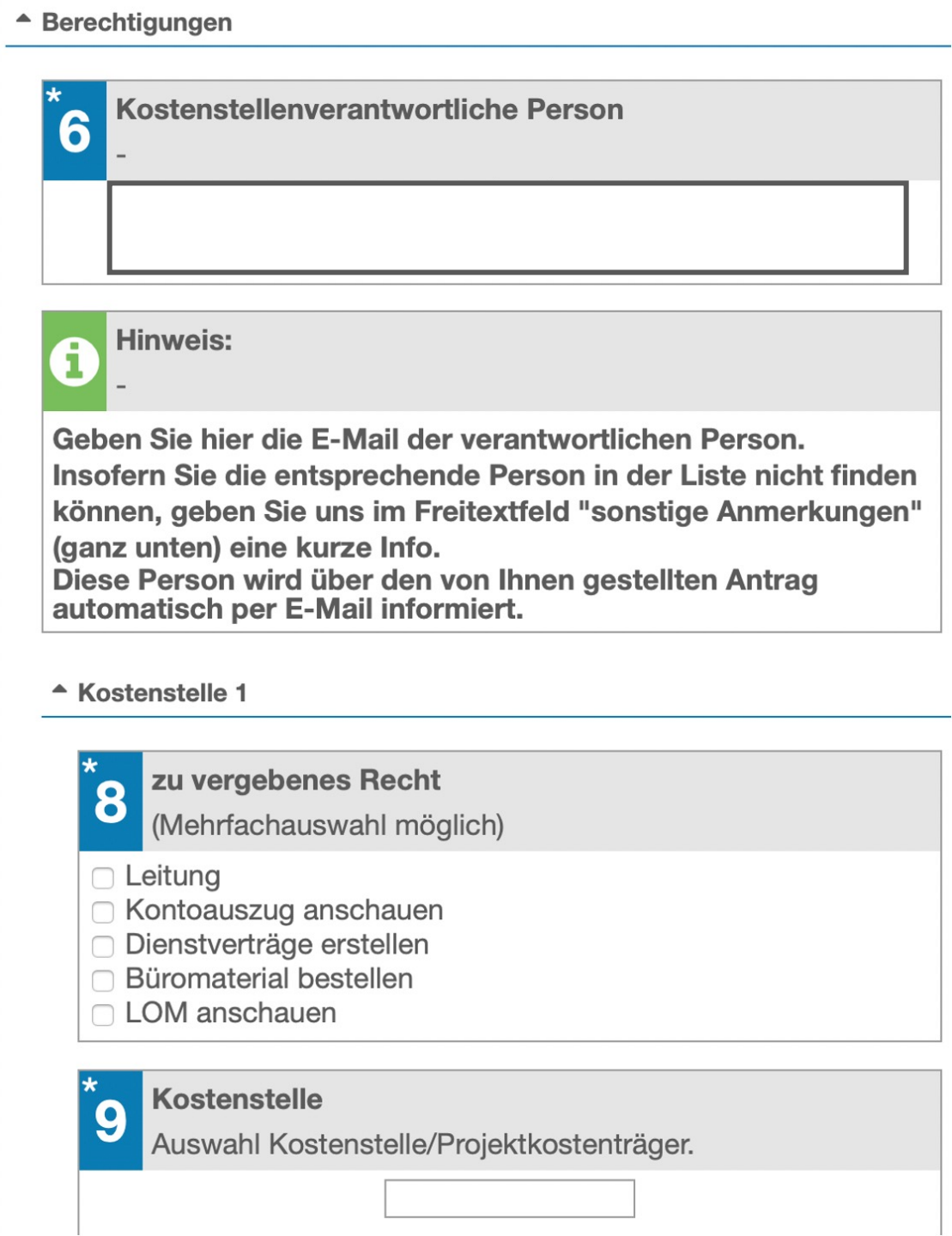
Von Dennis Schirrmacher

#9 Angriffsfläche verkleinern



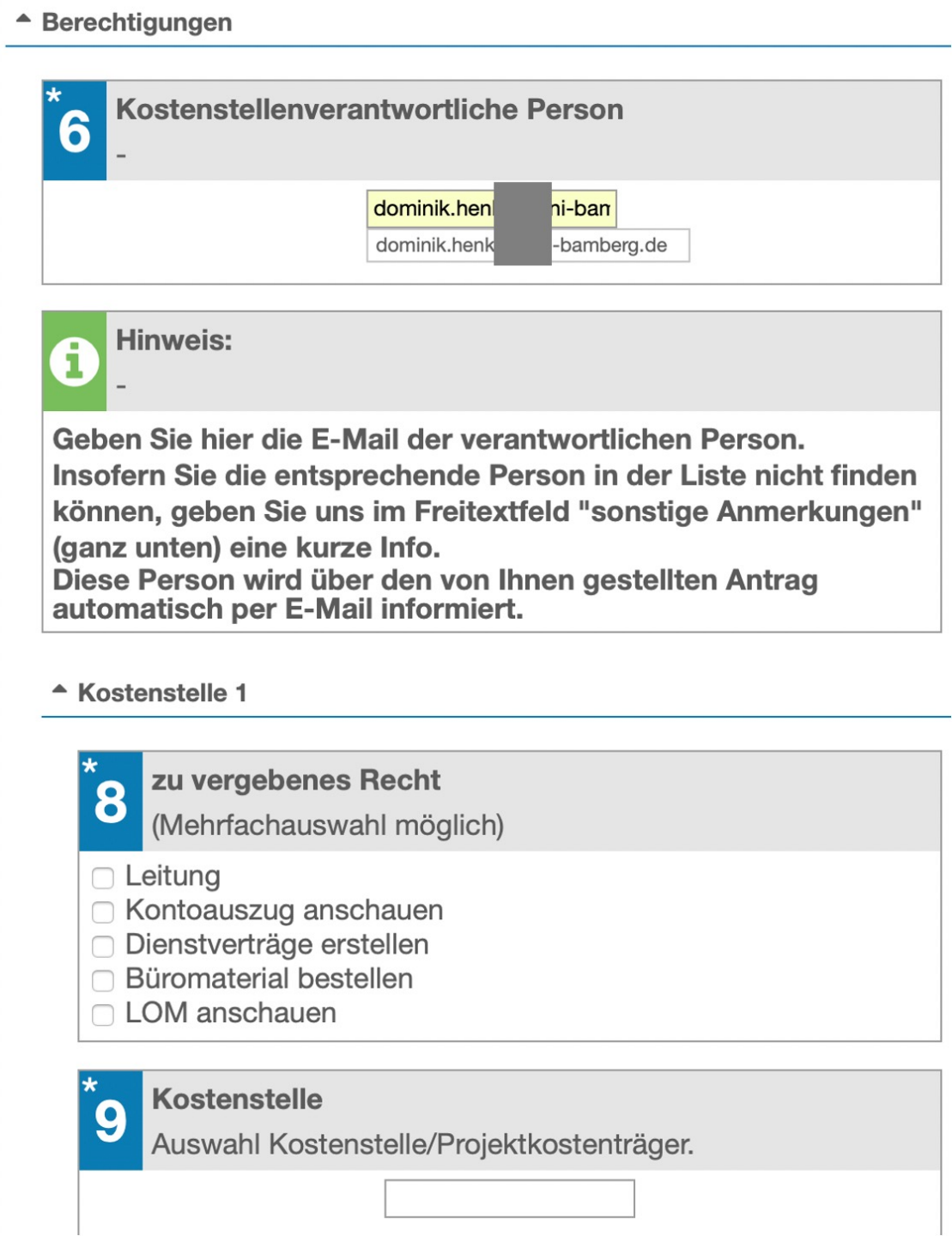
Webanwendung um Rechte zu beantragen

Hiermit beantrage ich Kostenstelleneinsicht …



Webanwendung um Rechte zu beantragen

Hiermit beantrage ich Kostenstelleneinsicht …



#10 Annahmen klarstellen

#11 Gute Benutzbarkeit

„Nach Bekanntwerden der Log4j-Lücke wurden wir von unserem Dienstleister sehr schnell mit entsprechenden Sicherheits-Patches versorgt. Diese wurden umgehend eingespielt. Danach wurden die Systeme auf unserer internen Checkliste als „gefixt“ betrachtet. Einige Tage später gab es aber einen weiteren Sicherheits-Patch, der im trügerischen Gefühl, die Systeme bereits gefixt zu haben, übersehen wurde.“

#12 Klar geregelte Zuständigkeiten

#13 Regelmäßige Überprüfungen


Das ist ja alles
schon wieder
so abstrakt!

Organisatorische Maßnahmen
oft vernachlässigt!

Statt in noch mehr technische Lösungen
lieber in *Personal* und besseres
Organisationsdesign investieren.

Beispiele >>>

Organisatorische Mittel für mehr Spaß beim Kampf gegen Windmühlen:

verständliche Dokumentation

jeder muss verstehen können wie ein System funktioniert

klare Verantwortlichkeiten

eine Stelle ist zuständig und hat Autorität (aber nicht eine Person allein)

Prozesse für Änderungen

manuelle Änderungen sind zu planen, häufige Änderungen sind zu vermeiden

bei Vorfall keine Schuldzuweisungen

konstruktive Aufklärung von Ursachen, Budget für Fehlerbehebung vorhsehen.

Automatisierung

sowohl für Infrastrukturmaßnahmen als auch wiederkehrende Prozeduren

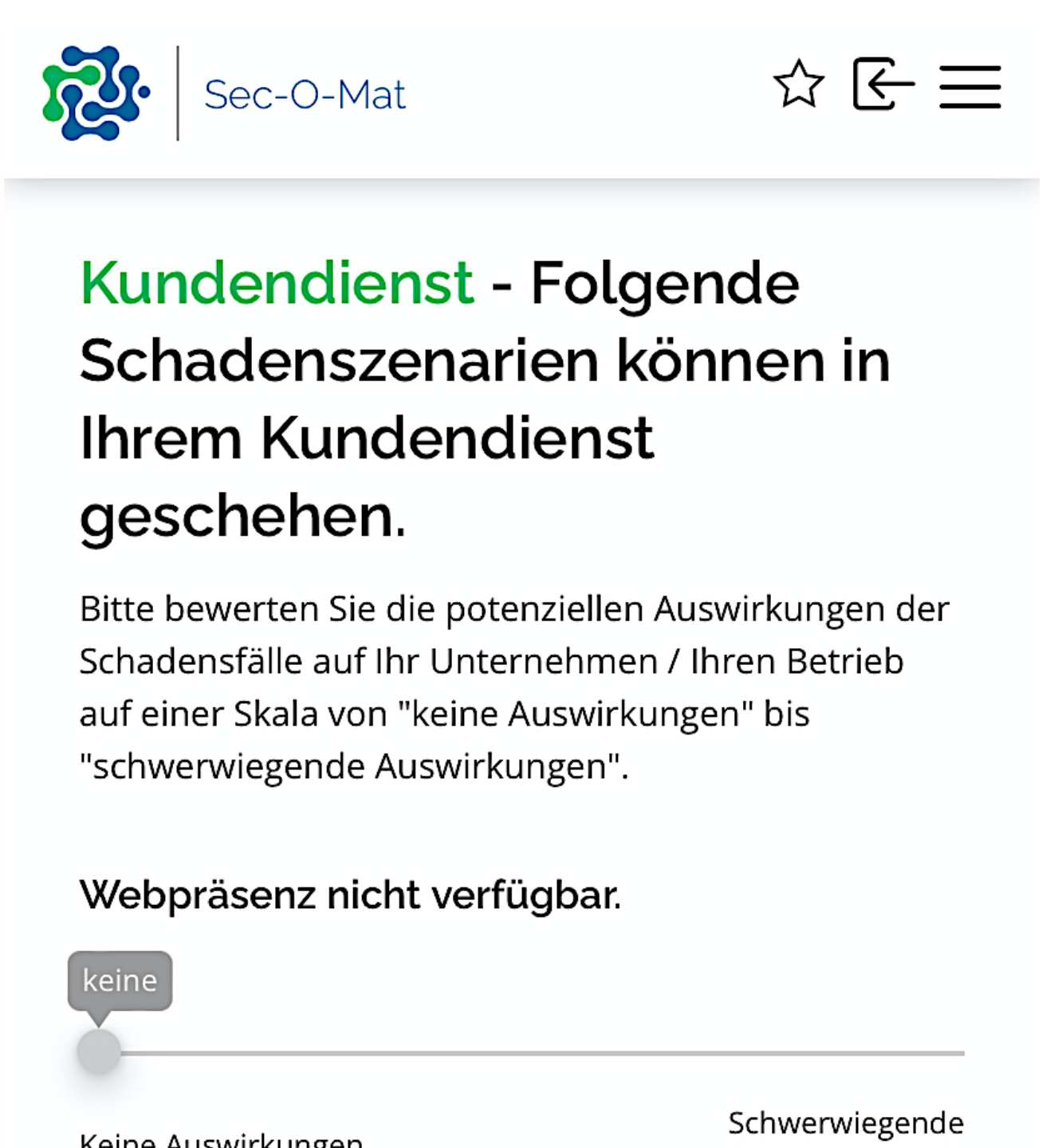
regelmäßige Sicherheitsübungen

decken Schwächen in Dokumentation und Prozessen auf

Dietrich et al. (2018). Investigating System Operators' Perspective on Security Misconfigurations, CCS 2018.

Systematischhe Risikobewertung

niedrigschwellig mit **sec-o-mat.de**



Wird der Kampf gegen Wind-mühlen irgendwann enden?

„Nobody ever got fired for buying IBM!“ (Cargo Cult Security)

Kosten eines erfolgreichen Angriffs sind noch nicht hoch genug.

>> Kaum Bereitschaft für radikale Änderungen (Linux für gefährdete MA?)

„Es wurde noch nie jemand dafür befördert, einen Angriff verhindert zu haben, der dann *nicht* stattfand.“ (Quelle unbekannt)

Ihre Mitarbeiter sind nicht die Gegner – wenn, dann sind es unsere psychologischen Defizite.

Komplexität hinterfragen

An organisatorische Maßnahmen denken (v.a. konkrete Notfallpläne)

Gut wäre mehr Bildung: Digital *Literacy* und *Security-Mindset*