IT-Sicherheit:
Ein Kampf gegen Windmühlen

Prof. Dr.
Dominik Herrmann

Privacy and Security Group
Universität Bamberg

Twitter: @herdom

Folien: dhgo.to/vlexplus22

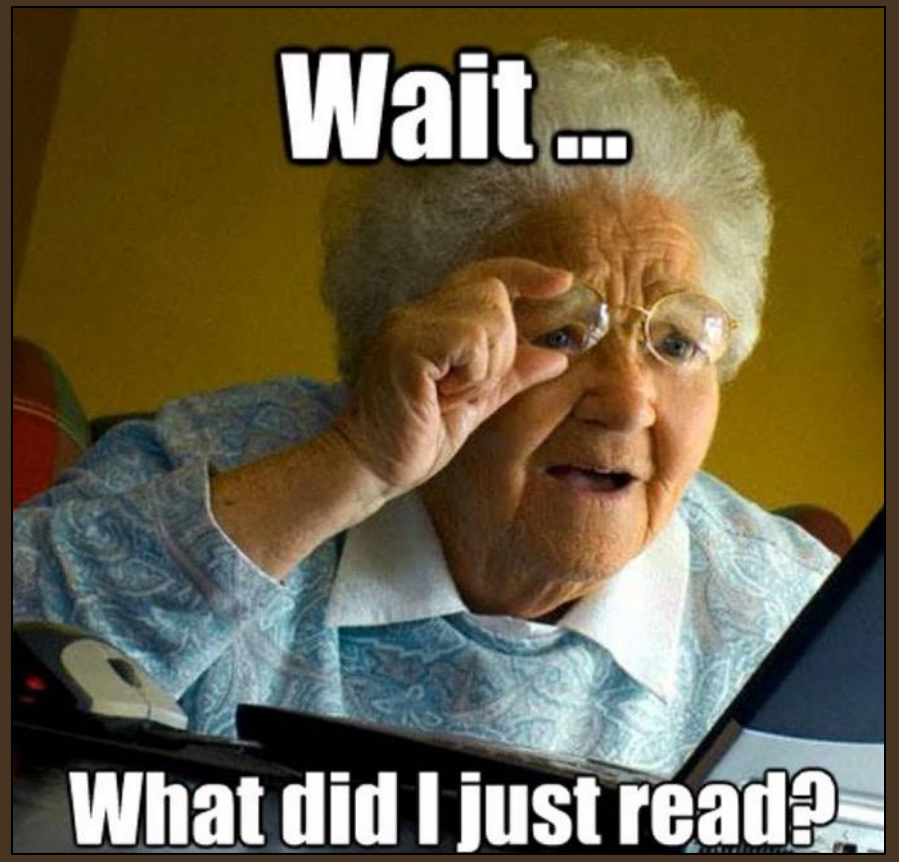
Wem müssen wir vertrauen, damit wir gut geschützt sind?

unseren Anwendern und Administratoren,

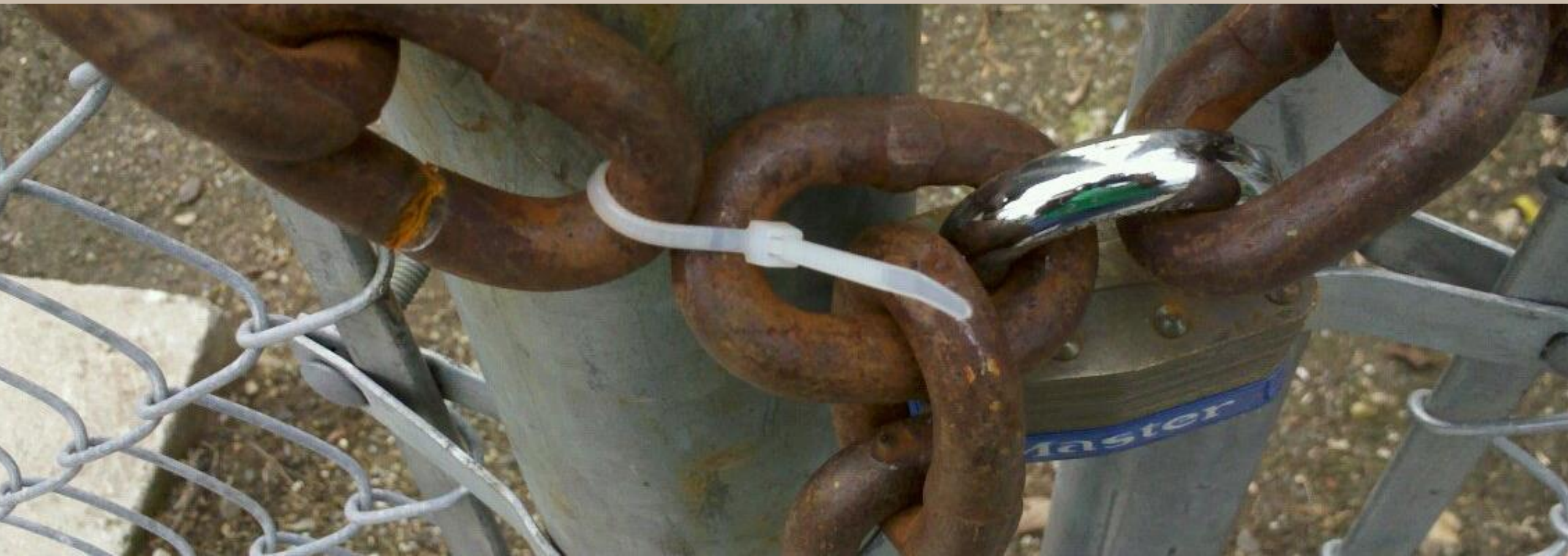
unseren Zulieferern und deren Zulieferern,

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

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



Menschen sind bekanntlich das schwächste Glied in der Kette



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

10

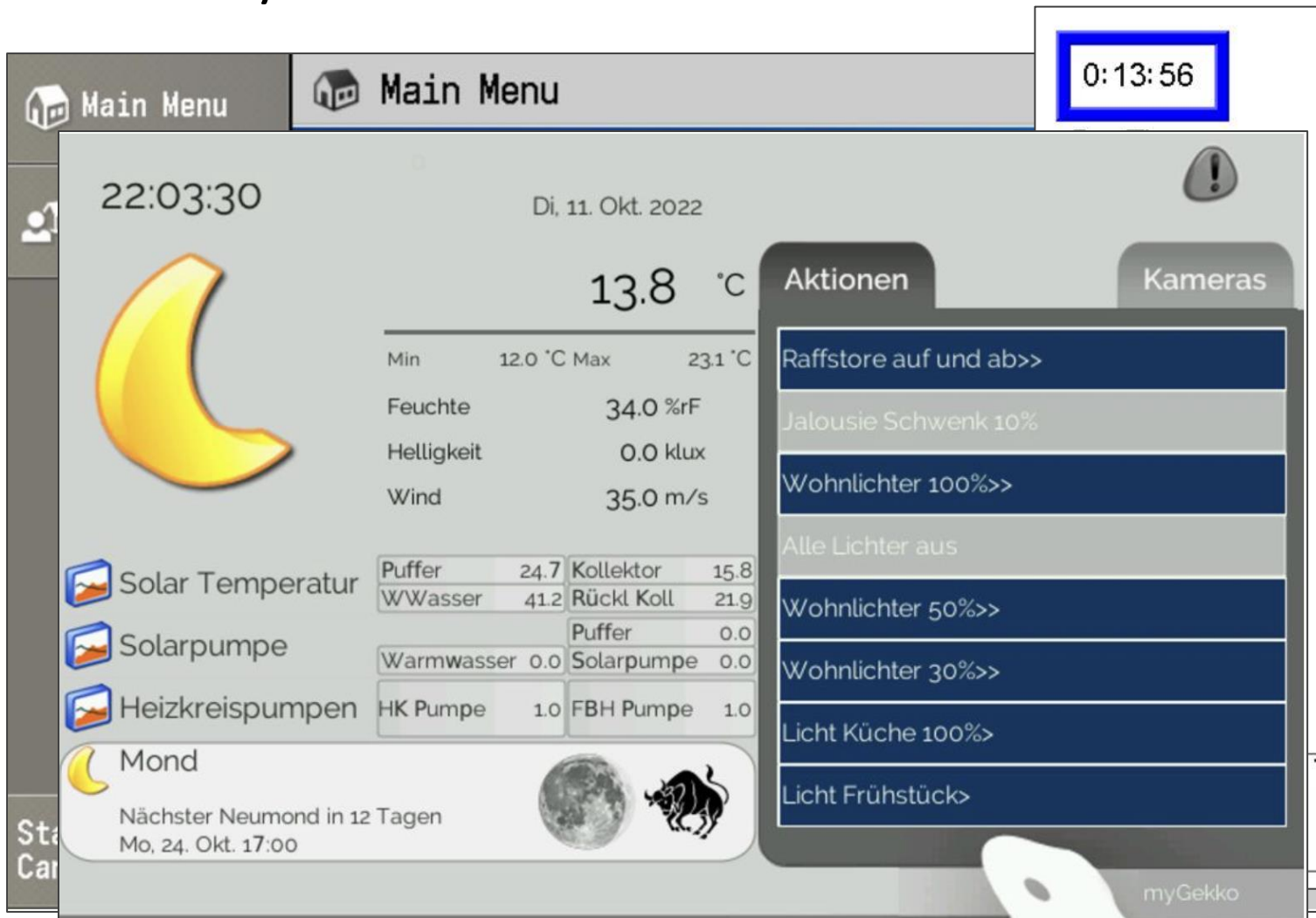
The company is still investigating

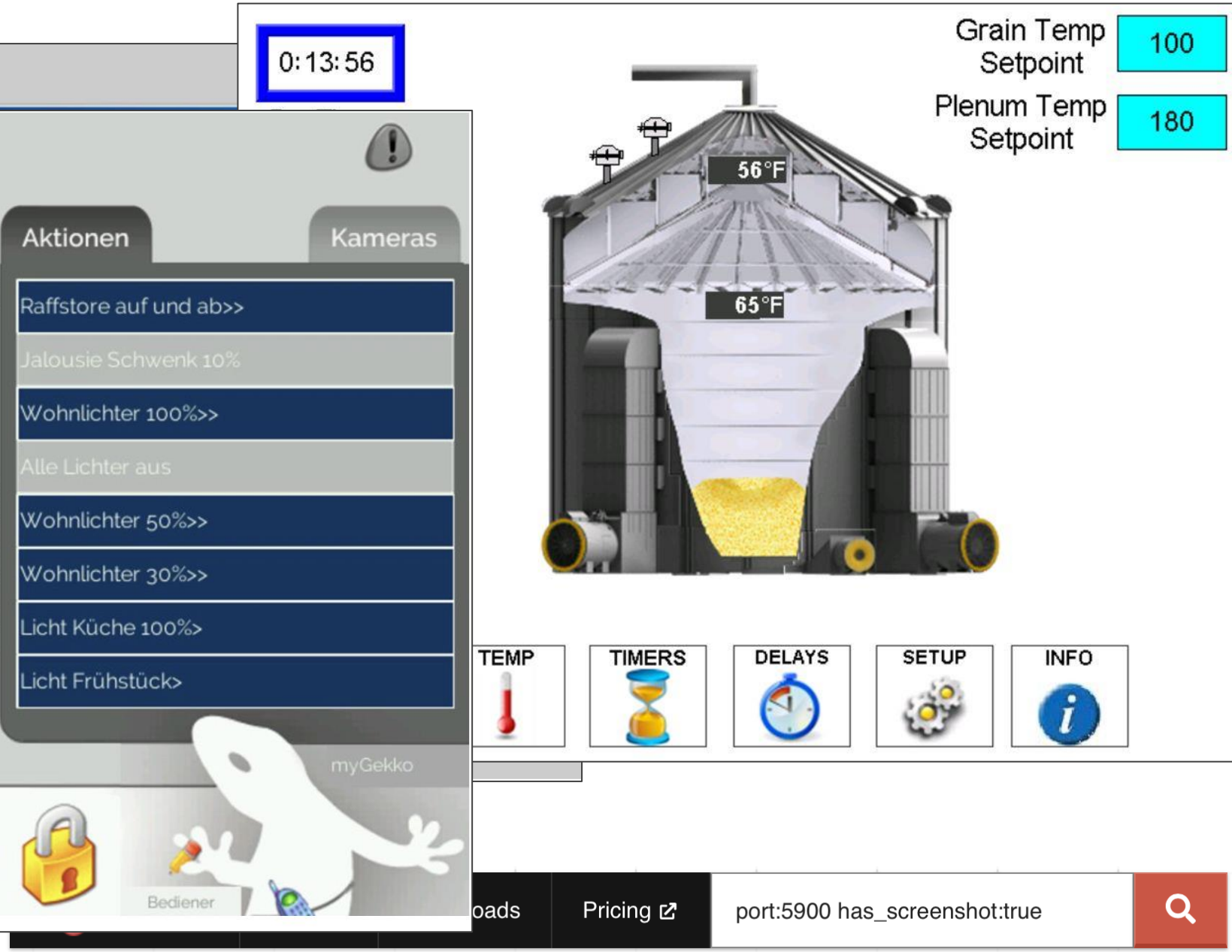
By Russell Brandom | Oct 3, 2017, 1:03pm EDT | 10 comments

... 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.

Auch Sysadmins machen Fehler…





Auch Zulieferer machen Fehler…

Claudia Pellegrino @c_pellegrino · Apr 4

Does T-Mobile Austria in fact store customers' passwords in clear text @tmobileat? @PWTooStrong @Telekom_hilft

> **SeloX** @SeloX_AUT
>
> Replying to @c_pellegrino @PWTooStrong @Telekom_hilft
>
> Had the same issue with T-Mobile Austria. Apparently they are saving the password in clear because employees have access to them (you have tell them your password when you're taking to them on the phone or in a shop) and they are not case sensitive

111 898 2.0K

T-Mobile Austria @tmobileat

Follow

Replying to @c_pellegrino @PWTooStrong @Telekom_hilft

Hello Claudia! The customer service agents see the first four characters of your password. We store the whole password, because you need it for the login for mein.t-mobile.at ^andrea

8:29 AM - 4 Apr 2018

T-Mobile Austria @tmobileat · Apr 5

Hi @c_pellegrino, I really do not get why this is a problem. You have so many passwords for evey app, for every mail-account and so on. We secure all data very carefully, so there is not a thing to fear. ^Käthe

319 378 343

Eric™ @Korni22 · Apr 6

Well, what if your infrastructure gets breached and everyone's password is published in plaintext to the whole wide world?

5 86 1.7K

T-Mobile Austria @tmobileat · Apr 6

@Korni22 What if this doesn't happen because our security is amazingly good? ^Käthe

462 693 876

Daniel @dhommel · Apr 6

Just to link this here: First XSS vulnerability already demonstrated. This means people can inject code in your website and potentially have it executed on somebody else‘s machine/account. Do you still want to discuss?

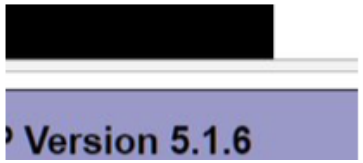
Fabrício Giglio @fabricio_giglio

Am I late for the T-Mobile party? 😅 @c_pellegrino, @tmobileat

4 30 232

Daniel @dhommel · Apr 7

And there‘s more regarding the security claim...



alexander @alessandrinoino

fortunately, the systems are updated .. 🧐

hanno
@hanno

Follow

Three of their subdomains (blog/kids/newsroom) were running wordpress blogs, the code managed via a git repository. You could download that git repo, you can test that by appending .git/config to the URL.

10:07 AM - 7 Apr 2018

59 Retweets **336** Likes

3 59 336

hanno @hanno · Apr 7

(for more context on this issue see this post by @internetwache en.internetwache.org/dont-publicly-… and their tool to scrape git repos github.com/internetwache/…)

internetwache/GitTools

GitTools - A repository with 3 tools for pwn'ing websites with .git repositories available

github.com

1 24 199

hanno @hanno · Apr 7

thus I was able to download their repo. The wordpress config (wp-config.php) was in the repository. That config file contains the database/mysql username/password.

2 44 310

Was sollen wir denn nun tun?

Wer ist **verantwortlich**?

Führen Sie regelm. eine **Datensicherung** durch?

Haben Sie **Makros** deaktiviert?

Haben Sie eine Richtlinie für sichere **Passwörter**?

Haben Sie eine **Firewall** eingerichtet?

Wie sichern Sie Ihre **Mailaccounts** ab?

Wie **trennen** Sie unterschiedliche IT-Bereiche?

Haben Sie IT-Risiken im **Homeoffice**
und bei **Geschäftsreisen** im Griff?

Wie **informieren** Sie sich?

Wie **sensibilisieren** Sie Ihre Mitarbeiter?

Deckt Ihre **Versicherungspolice** auch Cyber-Risiken ab?

Wissen Sie, wie Sie bei einem Angriff **reagieren** müssen?

Wie gut **kennen** Sie Ihre IT-Systeme?

Spielen Sie regelmäßig **Updates** ein?

Verwenden Sie **Virenschutzprogramme**?

FRAGE 5

Haben Sie Makros deaktiviert?

WARUM SOLLTEN SIE MAKROS DEAKTIVIEREN?

Eines der Haupteinfallstore für Ransomware sind Makros, die sich in mit E-Mails verschickten Dateianhängen verbergen. Dieses Einfallstor können Sie schließen – und zwar kostenlos!

Makros sind kleine Programme, die man beispielsweise in Word-, Excel-, PowerPoint- oder PDF-Dateien einbetten kann. Damit lassen sich Vorgänge automatisieren, was für manche Anwendungen durchaus nützlich sein kann. **Leider gilt das aber auch für Angreiferinnen und Angreifer, die Ihr IT-System unter Kontrolle bringen wollen.**

Wenn man eine Datei öffnet, die ein Makro enthält, fragt das öffnende Programm den Nutzer oder die Nutzerin dafür in der Regel um Erlaubnis. Das Problem ist, dass die meisten Nutzerinnen und Nutzer nicht beurteilen können, ob die Datei, die sie da gerade öffnen, legitim ist oder nicht. Cyber-Kriminelle versenden ihre Schadsoftware oftmals über die E-Mail-Adressen von Absendern, die die Empfänger kennen und denen sie vertrauen. Oftmals bezieht sich der Betreff einer Schadcode-E-Mail sogar auf eine bereits bestehende Mailkonversation (was in der Regel heißt, dass der vermeintliche Absender bereits selbst Opfer der Schadsoftware geworden ist).

Überlassen Sie die Entscheidung, ob ein Makro ausgeführt werden darf oder nicht, keinesfalls den Nutzern – denn diese haben schlicht nicht die erforderlichen Kenntnisse, um so eine Entscheidung treffen zu können. Verbieten Sie (zum Beispiel in den Windows-Gruppenrichtlinien) das Ausführen von Makros generell. Die meisten KMU verwenden ohnehin keine Makros. Und falls doch, kann Ihr Administrator die benötigten Makros signieren und ihre Ausführung damit erlauben. Alle anderen Makros bleiben aber weiterhin verboten. Das alles lässt sich mit ein paar Mausklicks erledigen.

WEITERE INFORMATIONEN FINDEN SIE HIER:

10 *https://www.bsi.bund.de/dok/531534*
BSI IT-Grundschutz-Baustein APP.1.1: Office-Produkte



Maßnahmen bei Geschäftsreisen: Falls Sie mit sehr sensiblen Daten arbeiten [und] einen Grund haben anzunehmen, Sie könnten Opfer von Wirtschafts- oder Industriespionage werden …, sollten Sie weitere Dinge beachten:

Bewahren Sie Ihre Geräte, Speichermedien und Dateien sowohl während der Reise als auch während des Aufenthalts **bei sich auf** (lassen Sie sie auch nicht in einem Hotelsafe liegen).

Verbinden Sie Ihre Hardware nicht mit Geräten, **in die Sie kein Vertrauen haben**. … Wenn Sie Ihr Mobiltelefon aufladen müssen, schließen Sie es nicht an einen nicht kontrollierten Computer oder an ein **fremdes USB-Ladegerät** (z. B. an Flughäfen) an.

Ändern Sie die Passwörter, die Sie während der Reise verwendet haben. Lassen Sie … Ihre Geräte nach der Reise überprüfen. Andernfalls schaffen Sie **zusätzliche Geräte** an und **sondern Sie diese** nach der Dienstreise **aus**.

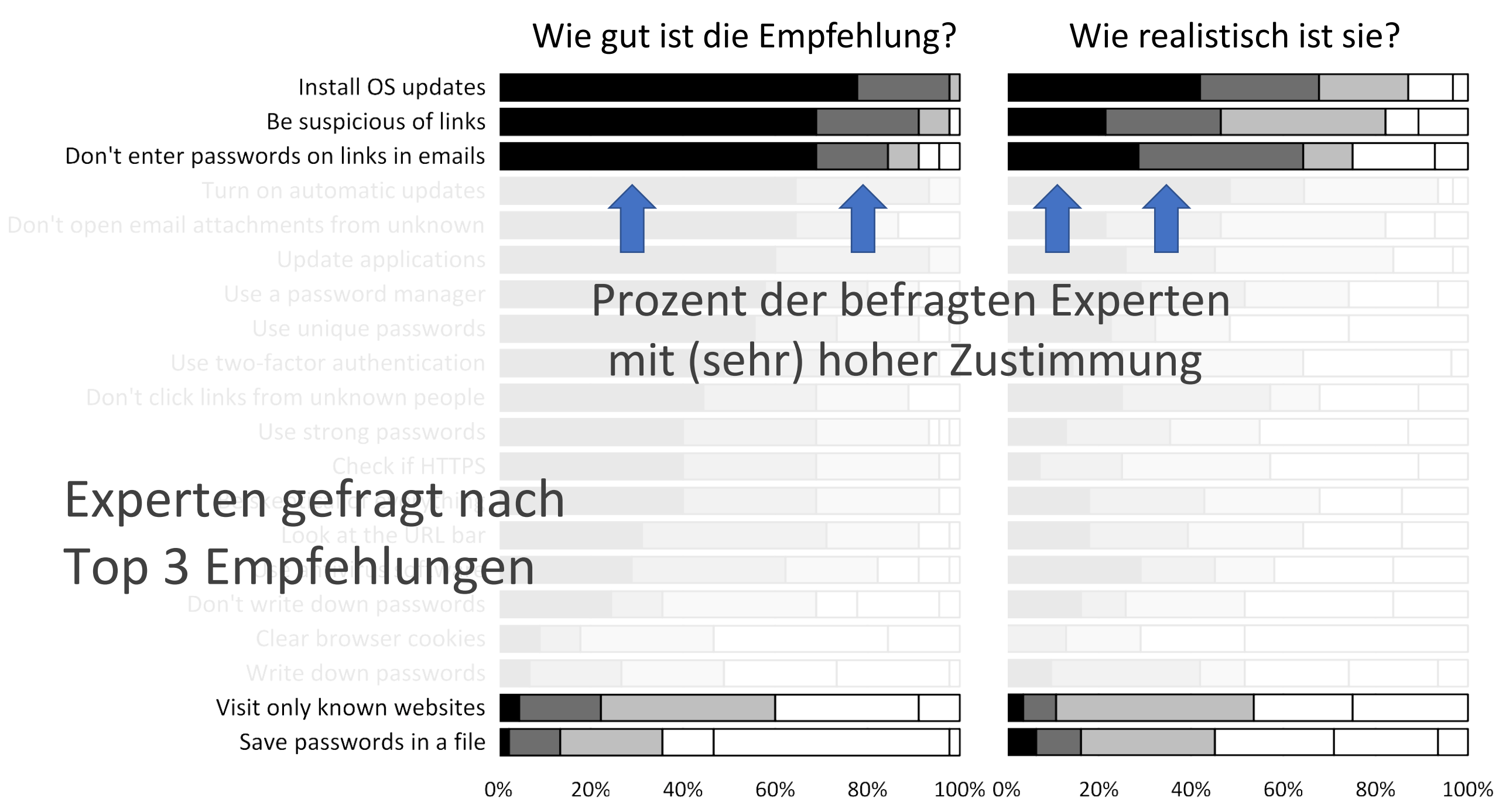
Aufwand: „leicht“ – ah-ja.


100%-ige
Sicherheit
gibt es halt
nicht.

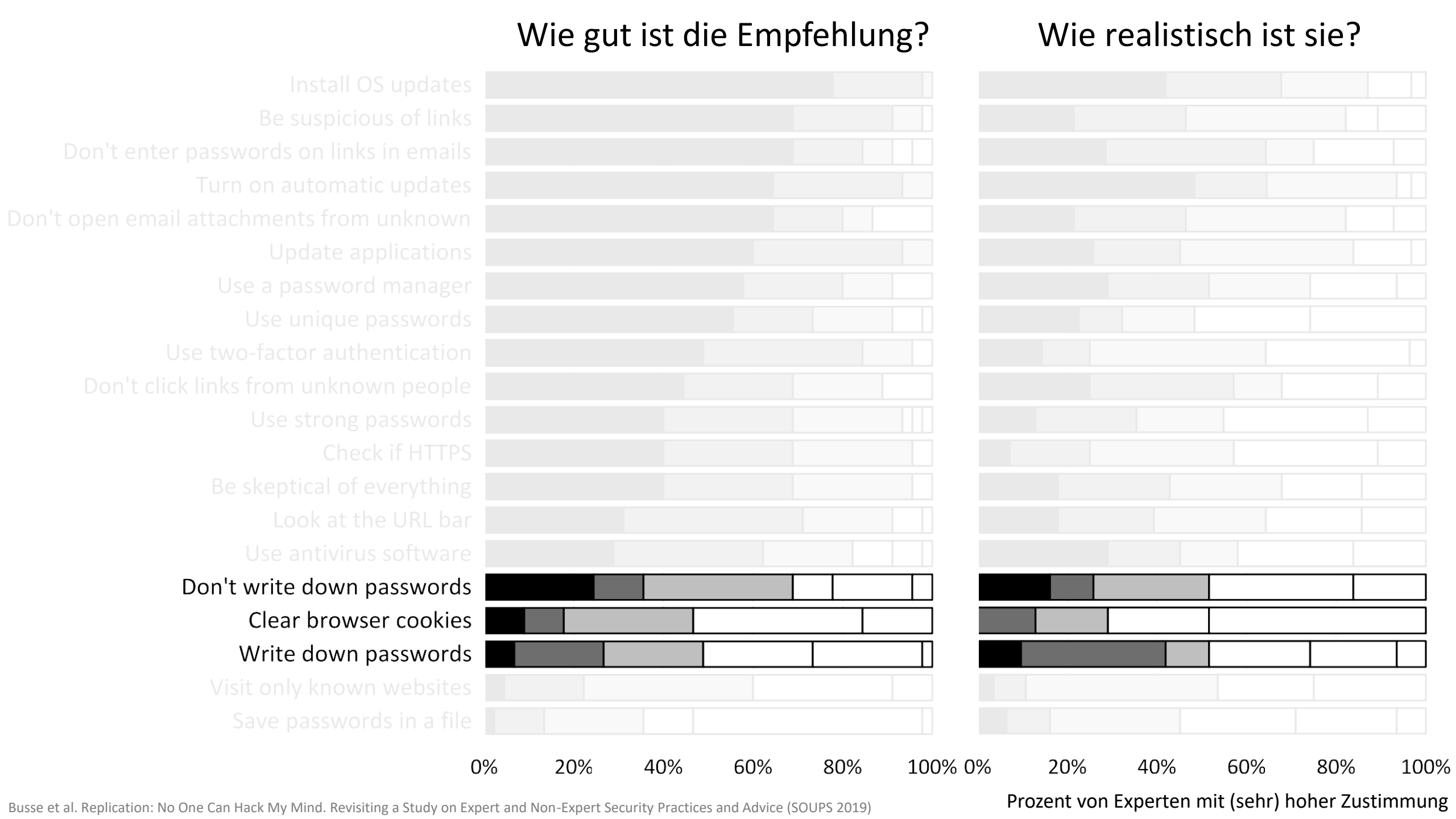
Experts vs Users

Experten mit imperfekten Lösungen zufrieden, aber die **Anwender** resignieren.

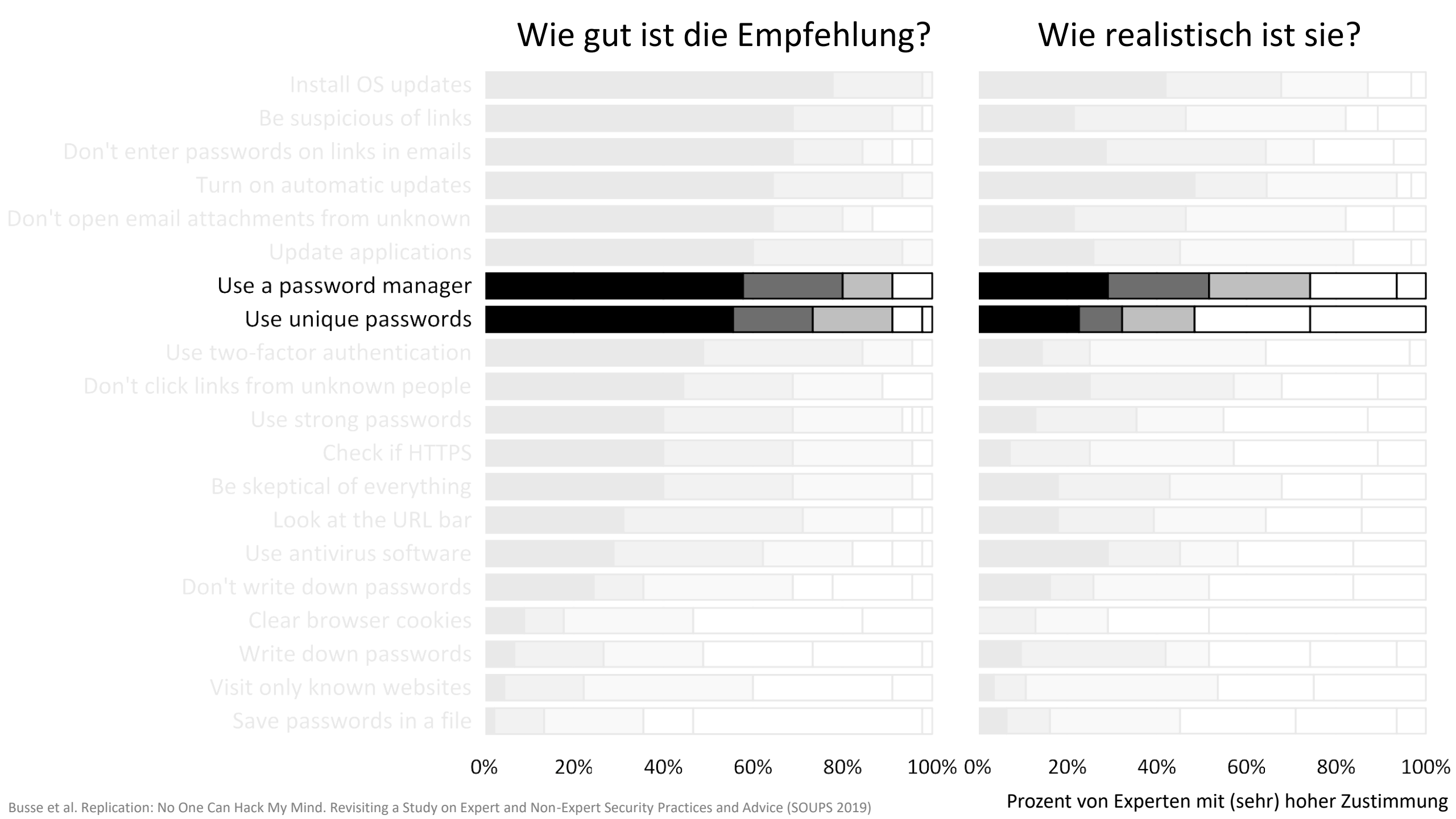
Beispiel Passwortmanager: Vertrauensverlust trotz klarer Sicherheitsvorteile



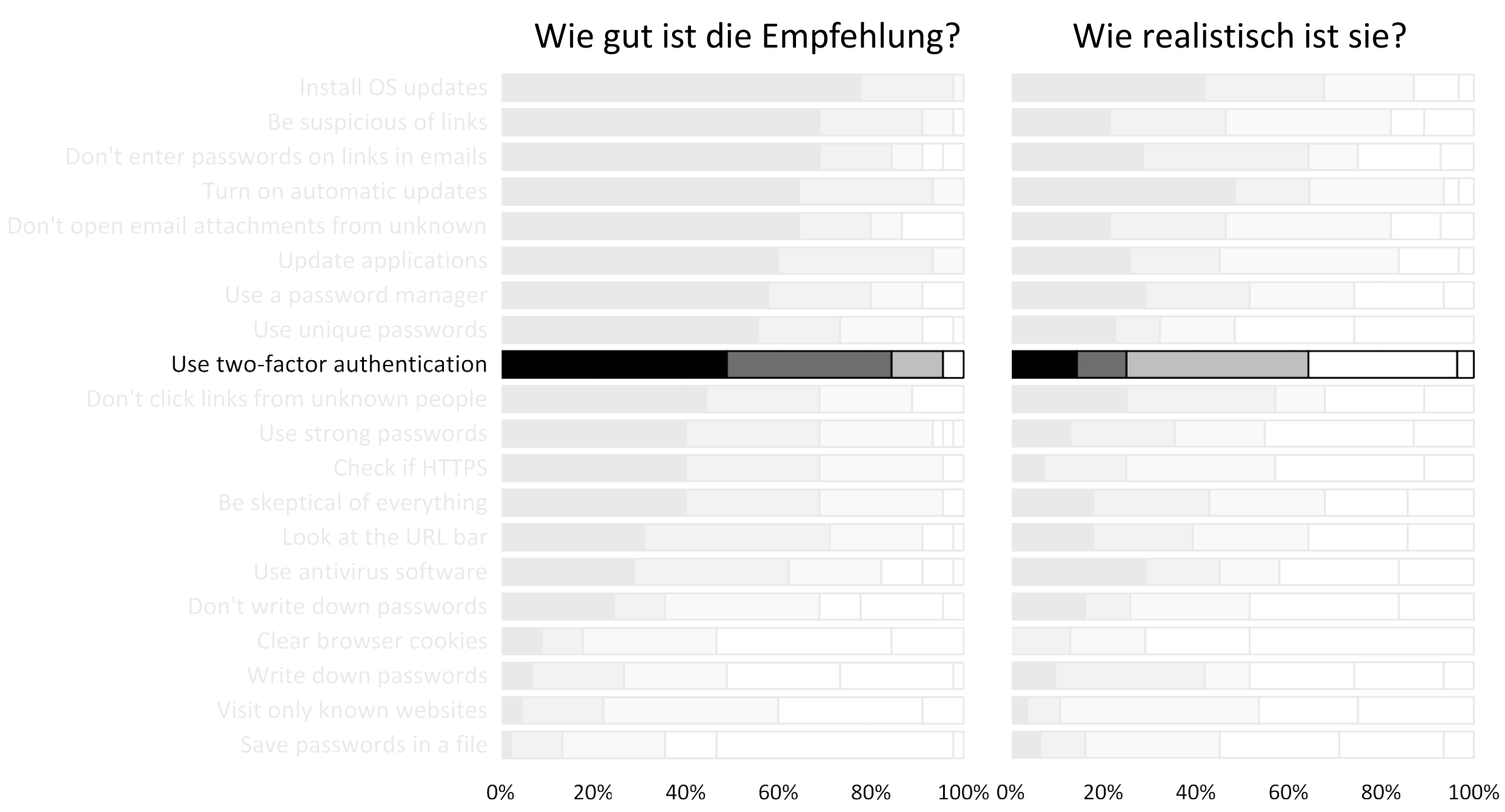
Busse et al. Replication: No One Can Hack My Mind. Revisiting a Study on Expert and Non-Expert Security Practices and Advice (SOUPS 2019)



Busse et al. Replication: No One Can Hack My Mind. Revisiting a Study on Expert and Non-Expert Security Practices and Advice (SOUPS 2019)



Busse et al. Replication: No One Can Hack My Mind. Revisiting a Study on Expert and Non-Expert Security Practices and Advice (SOUPS 2019)



Busse et al. Replication: No One Can Hack My Mind. Revisiting a Study on Expert and Non-Expert Security Practices and Advice (SOUPS 2019)

Wozu eigentlich 2-Faktor-Authentifizierung?

amazon.de

Sign in

Email or mobile phone number

Continue

By signing-in you agree to Amazon's Conditions of Use & Sale. Please see our Privacy Notice, our Cookies Notice and our Interest-Based Ads Notice.

Need help?

Sign in

dh@mail.com Change

Password Forgot Password

••••••••••••••••••

Sign in

Keep me signed in. Details

Zwei-Schritt-Verifizierung

Für mehr Sicherheit geben Sie bitte das Einmalkennwort ein, das an die Telefonnummer mit der Endziffer 995 gesendet wurde.

OTP eingeben:

In diesem Browser nicht mehr nach Codes fragen

Anmelden

Haben Sie das OTP nicht erhalten?

Amazon Business 11. October 2022 at 13:01

Tolle Geschäftsangebote beginnen heute!

To: Dominik Herrmann

AB

Online-Ansicht

https://www.amazonbusiness.eu/e/317391/ow-email-PEAS22-DO-NONBP-DE-e5/k3j3g4/2724405417?h=JRq3vlRz8vWq2SMBZDkl4MjMFIA1bvEYUCip_54KKj4

Jetzt anmelden

https://www.amazonbusiness.eu/e/317391/ow-email-PEAS22-DO-NONBP-DE-e5/k3j3g4/2724405417?h=JRq3vlRz8vWq2SMBZDkl4MjMFIA1bvEYUCip_54KKj4

Schalte diese und weitere Vorteile mit Business Prime frei

amazon.de

Sign in

Email or mobile phone number

Continue

Keep me signed in. Details

Zwei-Schritt-Verifizierung

Für mehr Sicherheit geben Sie bitte das Einmalkennwort ein, das an die Telefonnummer mit der Endziffer 995 gesendet wurde.

Text Message
Today 23:49

200378 ist Ihr Amazon-Einmalkennwort (OTP). Teilen Sie dieses Einmalkennwort nicht mit anderen Personen.

amazon

Jemand hat sich bei Ihrem Konto angemeldet.

Wenn	12. Okt. 2022 23:52
Gerät	Google Chrome for macOS (Desktop)
In der Nähe	Stimmt mit aktueller IP-Adresse (14X.1X.21X.2X5) überein

Das waren nicht Sie?
Teilen Sie uns mit, dass Sie es nicht waren.

Text Message
Today 23:49

200378 ist Ihr Amazon-Einmalkennwort (OTP). Teilen Sie dieses Einmalkennwort nicht mit anderen Personen.

https://amazon.de/a/c/r/x3XIs7haFmelUb7lFn4m86o5l

Amazon: Sign-in from BY, DE. Tap link to respond.

Zwei-Schritt-Verifizierung

Für mehr Sicherheit geben Sie bitte das Einmalkennwort ein, das an die Telefonnummer mit der Endziffer 995 gesendet wurde.

OTP eingeben:

In diesem Browser nicht mehr nach Codes fragen

Anmelden

- Haben Sie das OTP nicht erhalten?

Schneier on Security

Man-in-the-Middle Phishing Attack

Here's a phishing campaign that uses a man-in-the-middle attack to defeat multi-factor authentication:

> Microsoft observed a campaign that inserted an attacker-controlled proxy site between the account users and the work server they attempted to log into. When the user entered a password into the proxy site, the proxy site sent it to the real server and then relayed the real server's response back to the user. Once the authentication was completed, the threat actor stole the session cookie the legitimate site sent, so the user doesn't need to be reauthenticated at every new page visited. The campaign began with a phishing email with an HTML attachment leading to the proxy server.

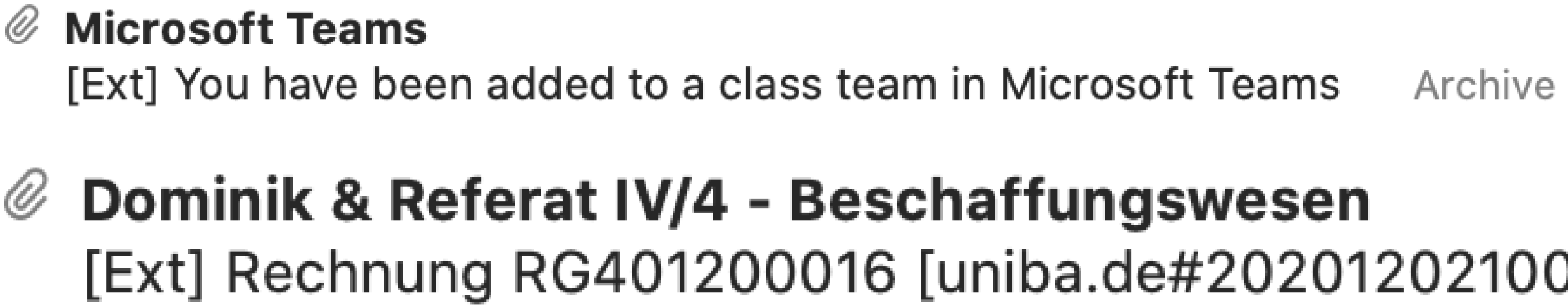
Tags: authentication, man-in-the-middle attacks, phishing, scams, two-factor authentication

Posted on August 25, 2022 at 6:45 AM • 29 Comments

Abhilfe:
FIDO2-basierte 2FA

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 beispiels-weise 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)

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

aber: nicht besonders effektiv (nur kurzfristig)

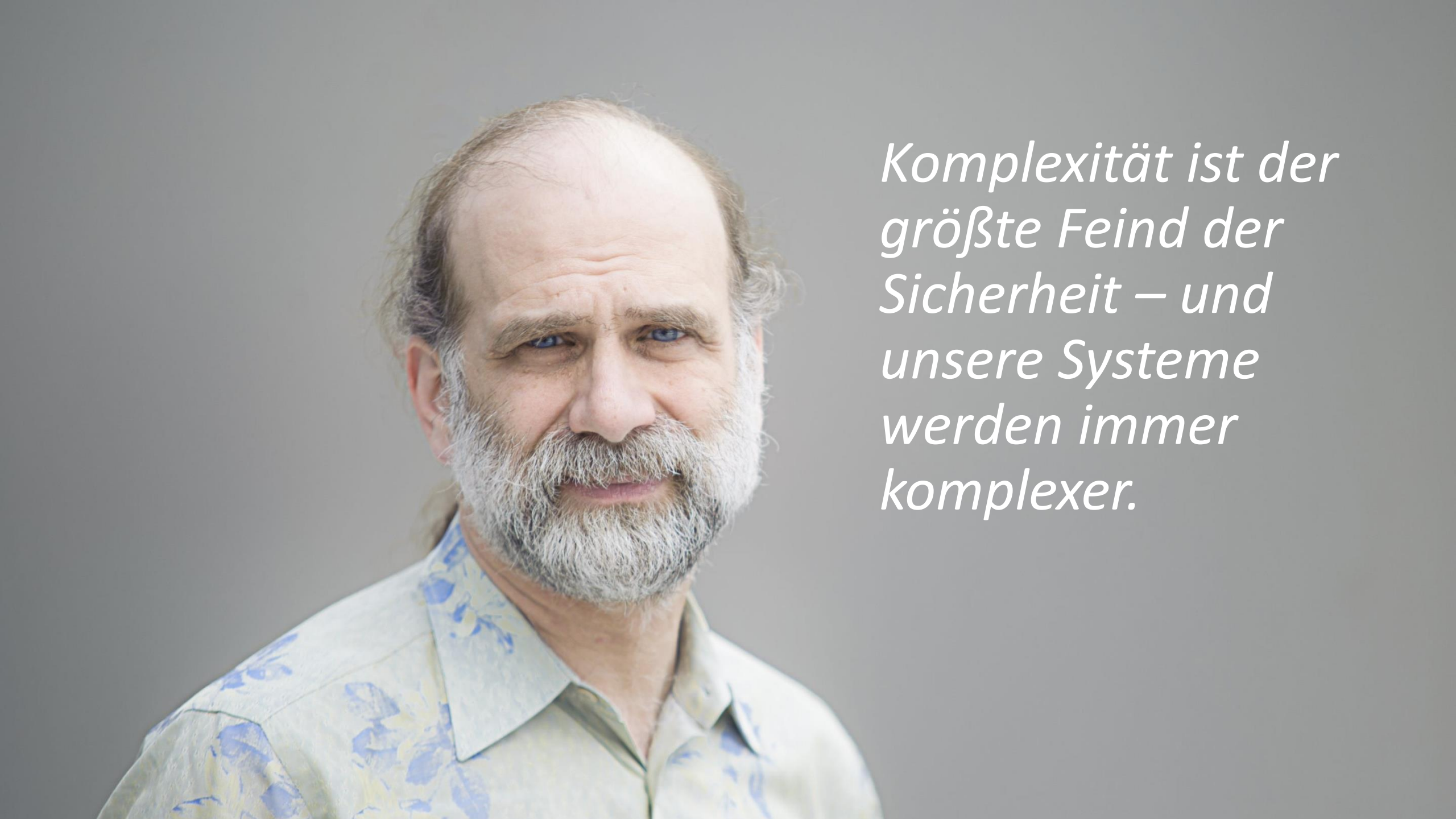
Sicherheit nur so gut wie das schwächste Glied der Kette – na hoffentlich nicht!

#2 Defense in Depth: Fehlertoleranter werden

#3 Fail Safely

#4 Least Privilege
nur so viele Berechtigungen wie nötig

#5 Compartmentalization
Abschottung einzelner Systeme

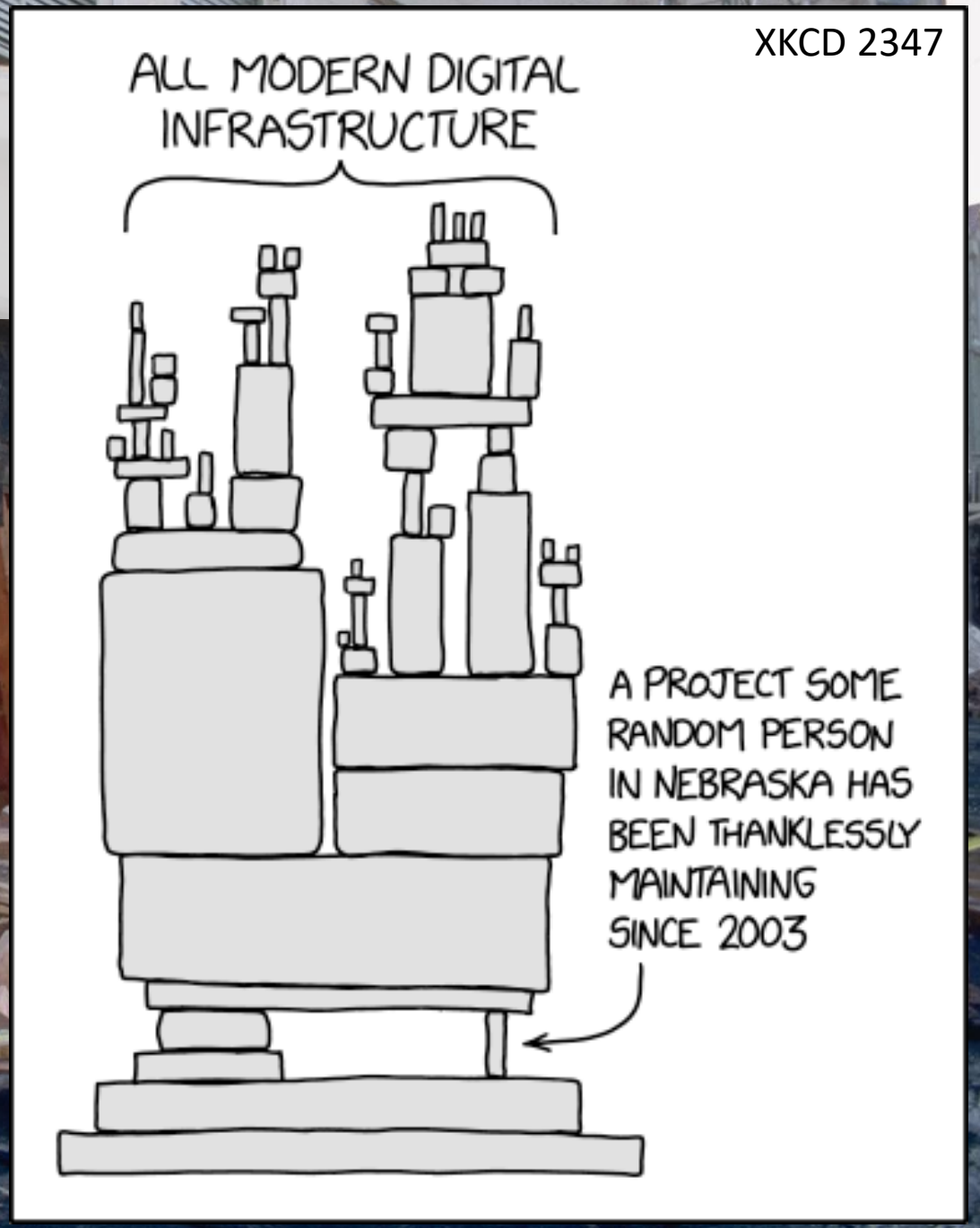

Komplexität ist der größte Feind der Sicherheit – und unsere Systeme werden immer komplexer.

#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

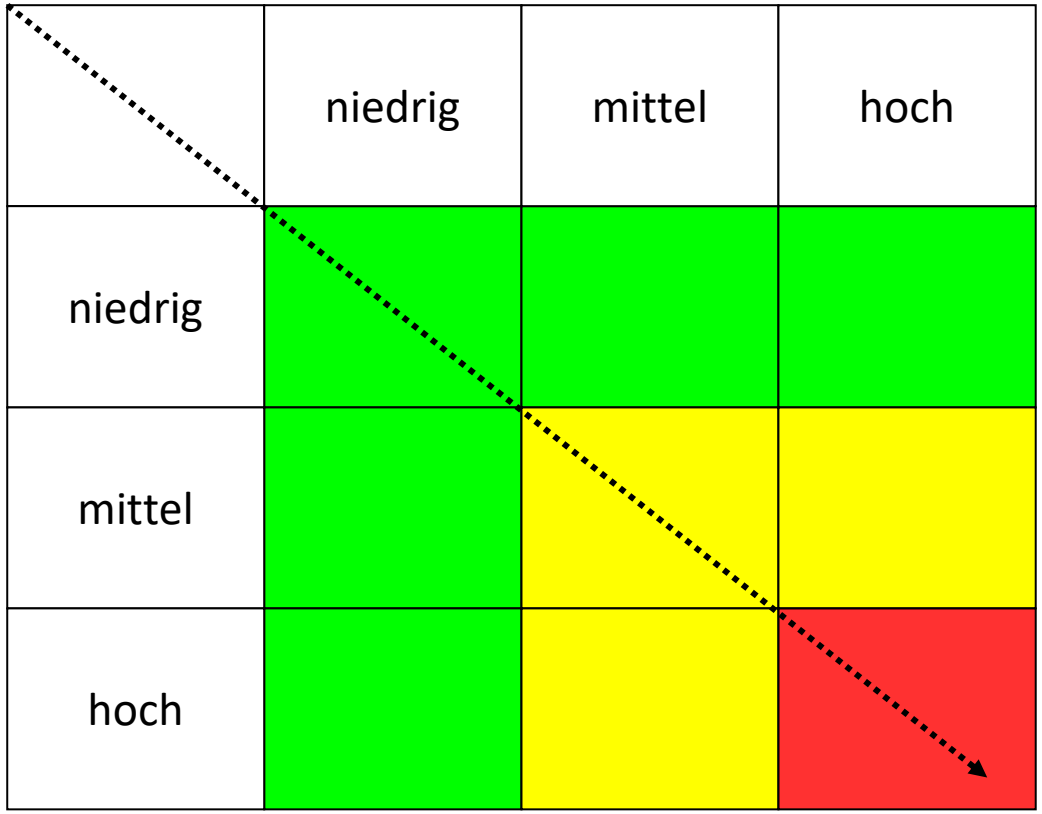
Jira und Confluence: Atlassian rechnet mit weiteren 2 Wochen Ausfall

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

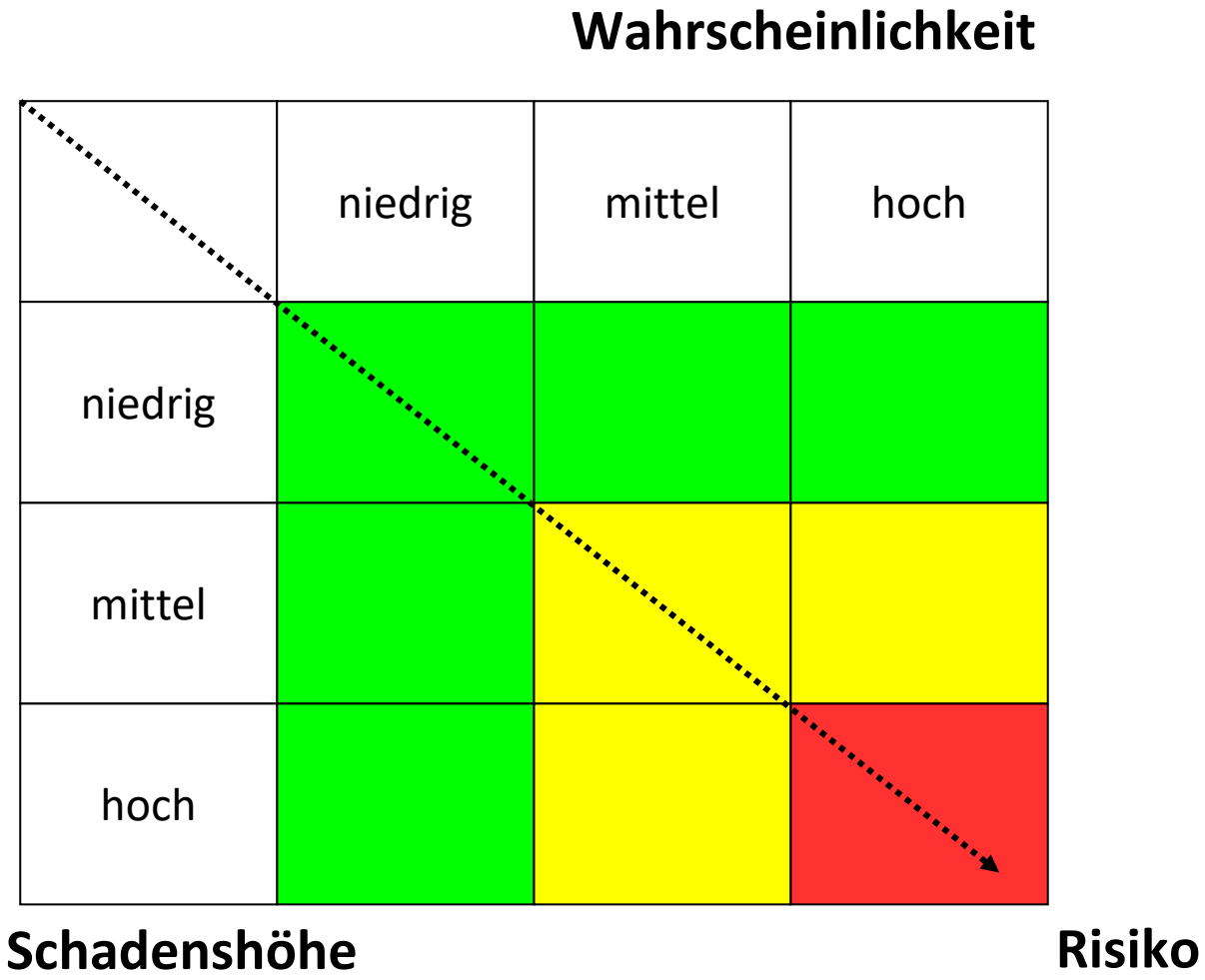
Wahrscheinlichkeit

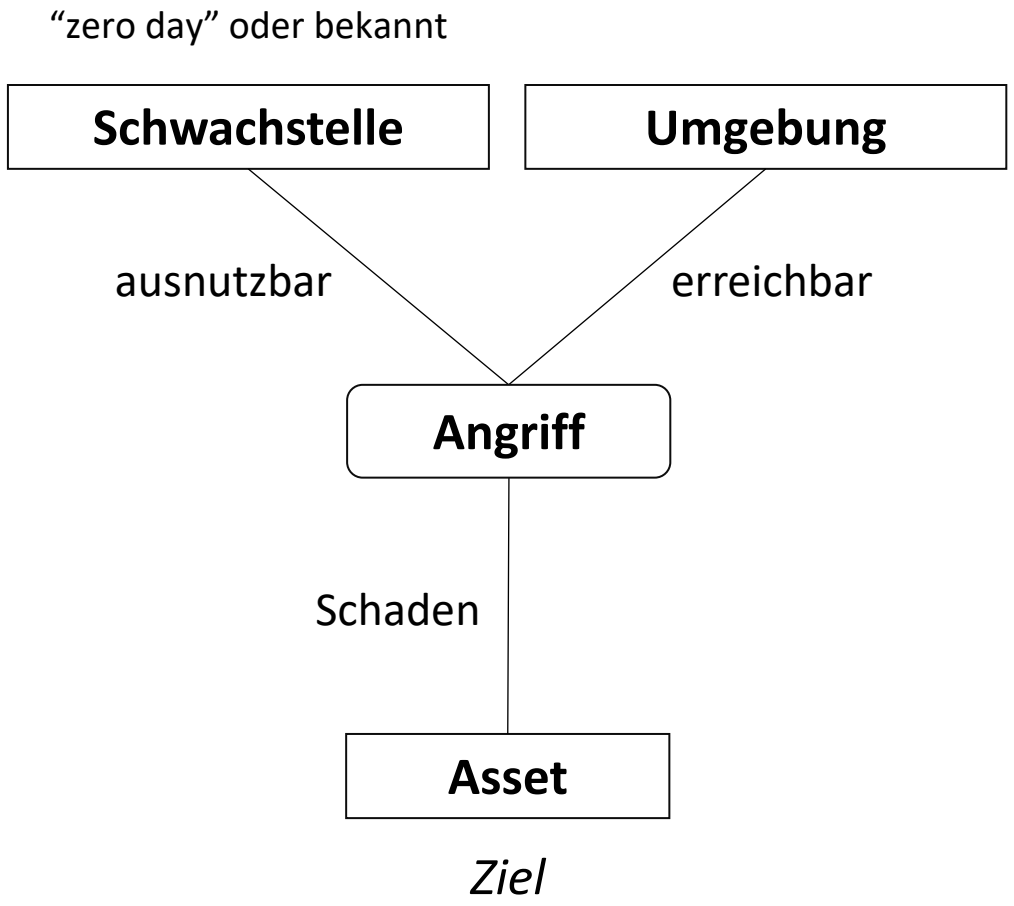


Schadenshöhe

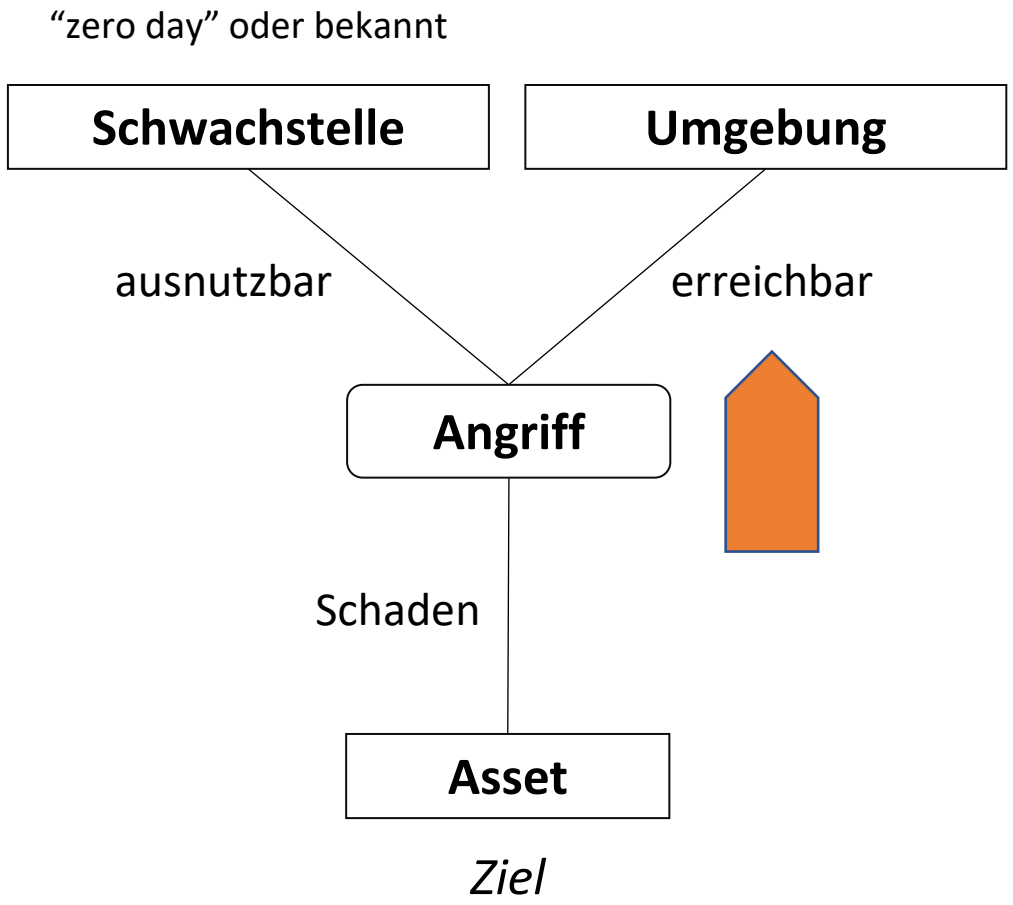
Risiko

Haben Sie Ihre Risiken erhoben?


Wahrscheinlichkeit
niedrig
mittel
hoch
niedrig
mittel
hoch
Schadenshöhe
Risiko


“zero day” oder bekannt
Schwachstelle
Umgebung
ausnutzbar
erreichbar
Angriff
Schaden
Asset
Ziel

#9 Angriffsfläche verkleinern



#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


So viel zu tun
und alles sehr
kompliziert …

How can AI help cybersecurity in solving complex security problems?

THESECMASTER.COM

- MANAGING THE MASSIVE AMOUNT OF DATA
- THE PROBLEM OF CONTEXT IN CYBERSECURITY
- THE PROBLEM OF PRECISION AND ACCURACY
- THE PROBLEM SPEED

Statt **Technological Solutionism**:
lieber in *Personal* und besseres
Organisationsdesign investieren.

Organisatorische Maßnahmen
oft vernachlässigt!

Evgeny Morozov. To Save Everything, Click Here: The Folly of Technological Solutionism, PublicAffairs (2013).

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

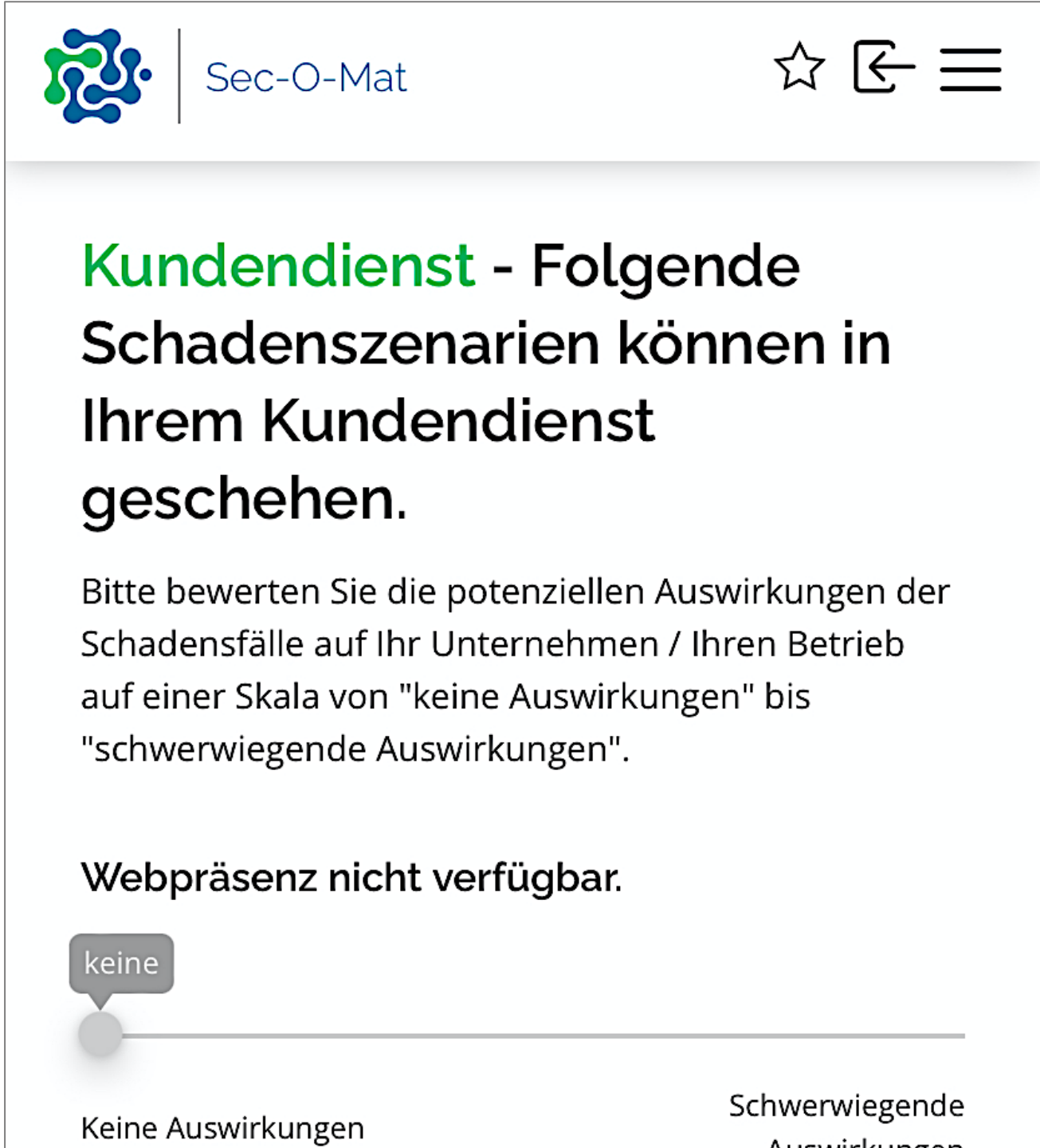
regelmäßige Sicherheitsübungen

decken Schwächen in Dokumentation und Prozessen auf

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

Zentral: Systematische Risikobewertung

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



Die Windmühlen lassen sich nicht besiegen. Warum?

Cargo Cult Security:

„Niemand wurde jemals gefeuert, weil er IBM gekauft hat.“

Kosten eines erfolgreichen Angriffs nicht hoch genug.

>> Kaum Bereitschaft für radikale Änderungen (Linux für gefährdete User)

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

(Quelle unbekannt)

Sicherheitsmaßnahmen, die Menschen nicht überfordern (psychologische Defizite)

Organisation/Prozesse mitdenken (z.B. konkrete Notfallpläne)

Komplexität hinterfragen