SO KLAPPT‘S MIT DEM TISAX®-ASSESSMENT

DataGuard

Christian Taube
Team Lead Information Security

SoSafe
Cyber Security Awareness

Dr. Christian Reinhardt
Awareness Evangelist

CHRISTIAN TAUBE

Team Lead Information Security

Zertifizierter ISMS Security Officer und Auditor nach ISO 27001

ERFAHRUNG

Geschäftsführer, LanguageWire München GmbH

Chief Solutions Officer, Xplanation NV (Leuven)

Mitgründer, Technischer Leiter und Aufsichtsrat, Matrix Communications AG (München)

Einführung von DS-GVO + ISO 27001 Compliance und erfolgreiche Audits nach TISAX® und ISO 27001 in internationalen Unternehmen

DR. CHRISTIAN REINHARDT

Awareness Evangelist

ERFAHRUNG

Awareness Evangelist bei SoSafe

Geschäftsführer Fußballverband Sachsen-Anhalt

IT-Kommission des Deutschen Fußball-Bundes (DFB)

Human Risk Audits

Implementation von DS-GVO Compliance

WARUM INFORMATIONSSICHERHEIT?

3,3 Millionen Personen betroffen

"VW says data breach at vendor impacted 3.3 million people"

"[…] an unauthorized third party obtained limited personal information about customers and interested buyers from a vendor that its Audi Volkswagen brands and some U.S. and Canadian dealers used for digital sales and marketing"

The information was […] was in an electronic file the vendor left unsecured.

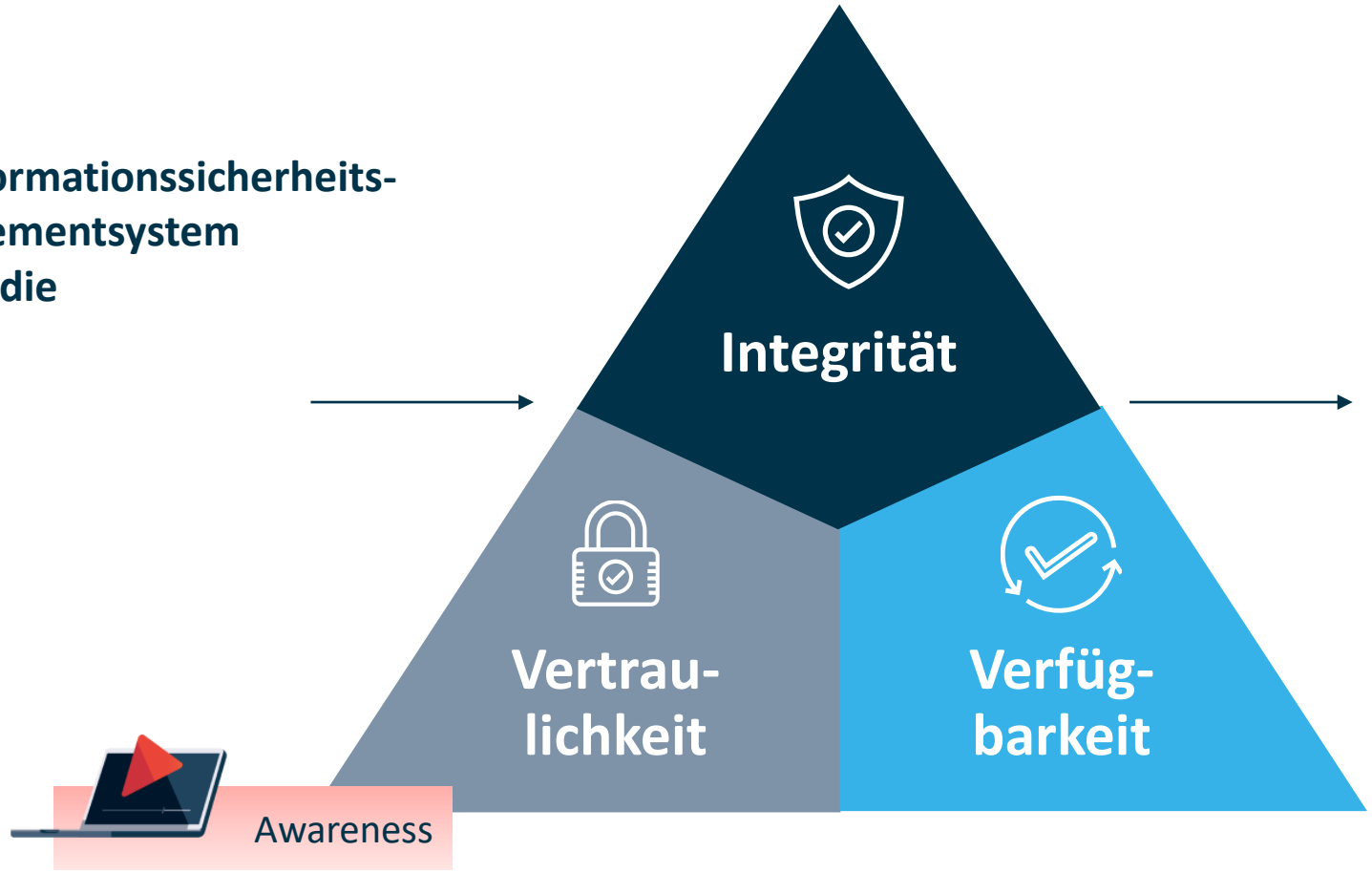
Data stored […] from multiple other sources not only Azure blobs.

The hacker said she just created a script that would look for exposed backups by checking for known company domains

*Quellen: Reuters, Vice

Was versteht man unter Informationswerten?

Das Informationssicherheits-Managementsystem schützt die



Ihrer Informationswerte vor Risiken und Schwachstellen

WIE FUNKTIONIERT TISAX®?

Warum TISAX®?

Awareness

- Ihr Kunde („Business Partner“) besitzt vertrauliche Informationen.
  Er will sie mit dem Zulieferer – Ihnen - teilen.
- Informationen, die Ihr Kunde mit Ihnen teilt, sind wichtiger Teil
  der Wertschöpfung → angemessener Schutz ist notwendig!
- Er möchte sicher sein, dass Sie Informationen
  mit der gleichen Sorgfalt behandeln. → Er braucht Nachweise.

- *Was bedeutet* „sicherer Umgang“ / „Sorgfalt“?
- Dafür gibt es einen Standard!
- Für den VDA = Verband der Automobilindustrie:
  Das „VDA ISA“ = *Information Security Self Assessment*
- *Wie* können Sie den sicheren Umgang nachweisen, z.B. anderen OEMs?
- Über TISAX® = *Trusted InformationSecurity Assessment Exchange*

Wie läuft ein TISAX®-Assessment ab?

Ein OEM fordert Sie auf, Ihr Informationssicherheits-Management nach TISAX® nachzuweisen.

Formale Schritte:

1. Registrierung* > Sammeln von Informationen, Festlegen des Prüfumfangs (Scope) auf Basis der Anforderungen Ihres Partners.

   **Die Registrierung ist kostenpflichtig*

2. Prüfung durch einen Prüfdienstleister
3. Teilen Ihres Prüfergebnisses

Tatsächliche Schritte:

- Einführung des ISMS > hier steckt der meiste Aufwand (mind. 4 Monate, 6 bis 9 wären normal)
- Registrierung bei ENX und Scope-Festlegung
- Interner Audit Ihres ISMS > Maßnahmenumsetzung aus internem Audit
- Prüfung durch Prüfdienstleister > Maßnahmenplan
- Abhängig von den Abweichungen und erfolgten Korrekturen ggf. weitere Prüfschritte erforderlich (max. Prüfungsdauer 9 Monate)
- Nach drei Jahren erneuter Audit

TISAX® Prüfziele, Anforderungen…

Die Prüfziele…

verbinden einen der drei Kriterienkataloge Informationssicherheit, Prototypenschutz und Datenschutz mit einem Schutzbedarf:

1. Informationen mit hohem Schutzbedarf
2. … mit sehr hohem Schutzbedarf
3. Prototypenschutz: Bauteile
4. Prototypenschutz: Fahrzeuge
5. Prototypenschutz: Erprobungsfahrzeuge
6. Prototypenschutz: Veranstaltungen / Shootings
7. Datenschutz
8. Datenschutz bei sog. „besonderen Kategorien“ personenbezogener Daten

Awareness

Die Anforderungen…

Modul	„Muss“	„Sollte“	Zusatz „Hoch“	Zusatz „Sehr hoch“
Informations-sicherheit	98	91	25	6
Prototypen-schutz	58	6	3	0
Datenschutz	23	0	0	0
Gesamt	179	97	28	6

➔ Ihr **Kunde** gibt Ihnen in der Regel vor, welche Kriterienkataloge und welchen Schutzbedarf Sie erfüllen müssen.

➔ Denken Sie daran, auch Ihre Lieferanten im Blick zu haben.

… und TISAX®-Assessment Level

Prüfziele werden anhand eines Assessment Levels geprüft:

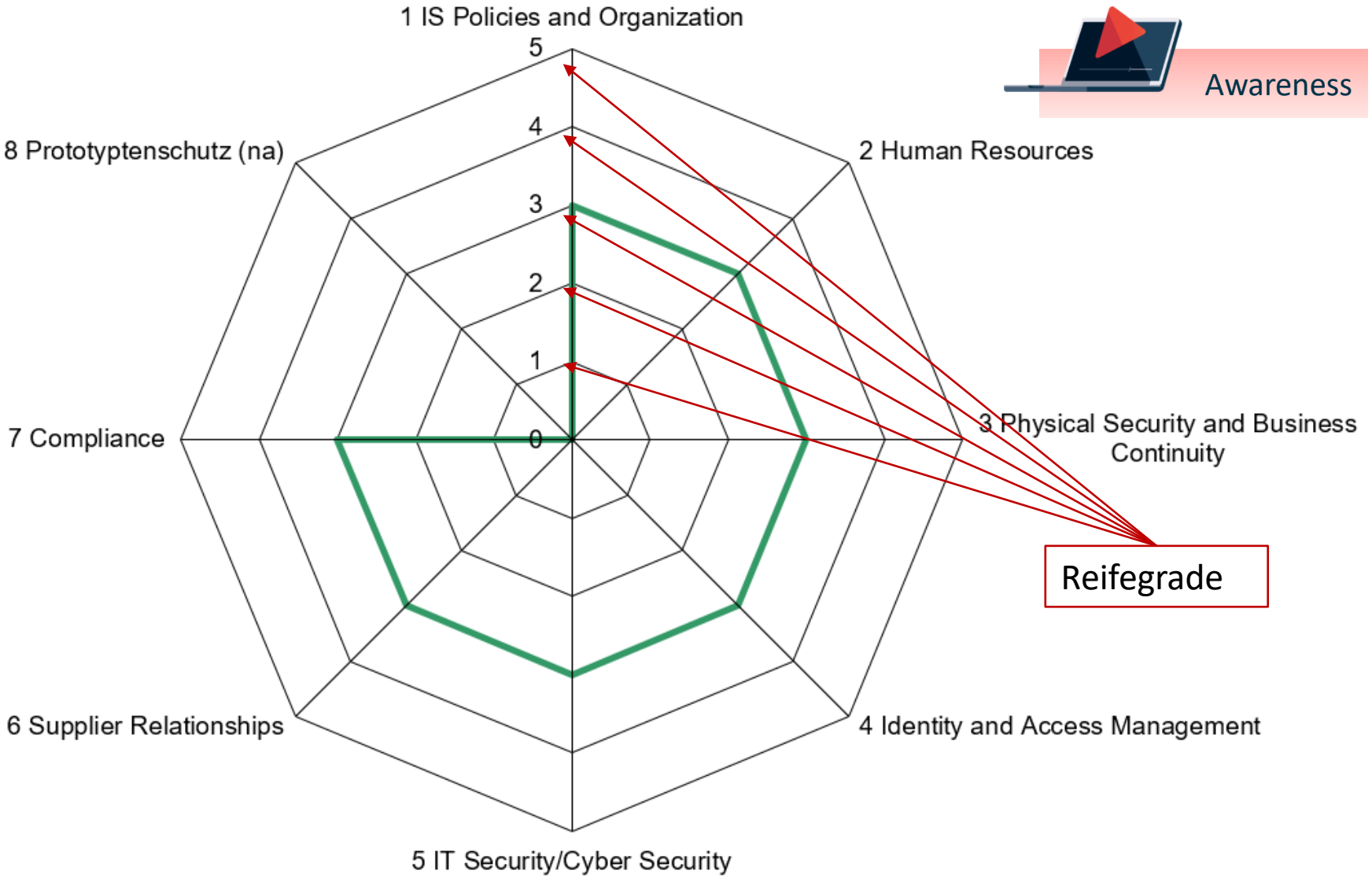
AL 1 – Reine Selbsteinschätzung

AL 2 – Plausibilitäts- und Nachweisprüfung, in der Regel remote

AL 3 – Eingehende Vor-Ort-Prüfung

Erfüllung dieses Prüfziels…	…möglich mit diesem AL
Informationen mit hohem Schutzbedarf	AL 2
Informationen mit sehr hohem Schutzbedarf	AL 3
Prototypenschutz - Bauteile	AL 3
Prototypenschutz – Fahrzeuge	AL 3
Prototypenschutz – Erprobungsfahrzeuge	AL 3
Prototypenschutz – Veranstaltungen	AL 3
Datenschutz	AL 2
Datenschutz bei besonderen Kategorien	AL 3

TISAX® – Maßnahmenziele und Reifegrade



Awareness

Reifegrade

Umfassendes Management-system – nicht nur IT-Sicherheit!

WAS PASSIERT BEIM TISAX®-ASSESSMENT?

Audit-Ergebnisse

Konformität	Wirksamkeit des ISMS ist erwiesen.
Beobachtung	Wirksamkeit des ISMS ist erwiesen. Detailaspekt könnte verändert > verbessert werden.
Nebenabweichung	Wirksamkeit des ISMS ist insgesamt erwiesen. Jedoch fehlen einzelne Nachweise für die Umsetzung der beschriebenen Maßnahme in einem gegebenen Kontrollbereich / ist eine Maßnahme nur teilweise wirksam umgesetzt. => Temporäres TISAX®-Label bis „Heilung“ (max. Dauer 9 Monate)
Hauptabweichung	Wirksamkeit des ISMS ist *nicht* erwiesen. Es fehlen wirksame Richtlinien in einem gegebenen Kontrollbereich / Maßnahmen sind in einem kompletten Kontrollbereich nicht vorhanden oder nachweisbar. => Maximale Dauer des Prüfprozesses 9 Monate => dann kein TISAX® -Label

Top 5 Takeaways zum erfolgreichen TISAX®-Assessment

Sicherheit ist ein Prozess – keine Eigenschaft

Mandat und Zeit der Mitarbeiter

„Dies ist jetzt leichter, weil …“

Keine falschen Annahmen treffen

Management mitnehmen

Ressourcen einplanen

Mitarbeiter mitnehmen

Positive Erlebnisse schaffen

Awareness

Buy-In der Geschäftsführung sichern

Nicht nur die Aufgabe des Informationssicherheits-Beauftragten

Auf Kollisionskurs?

Wie wichtig Cybersecurity im Kontext von Connected Mobility ist – Fokus Human Factor

Dr. Christian Reinhardt, Awareness Evangelist, SoSafe GmbH

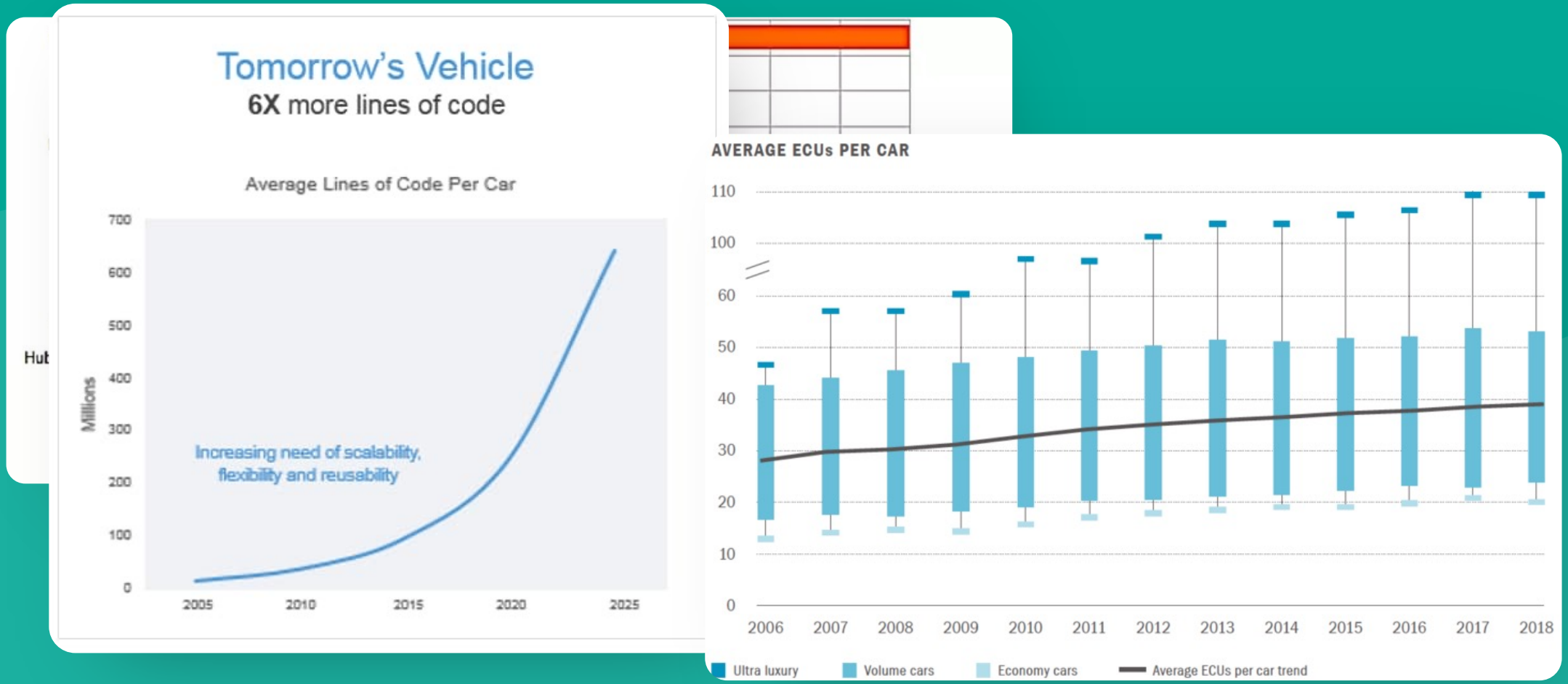
Wir stärken die digitale Selbstverteidigung Europas.

800+ Kunden
von 50 bis 250.000 Mitarbeitenden

1 Mio+ Endnutzer
und über 15.000 Phishing-Mails täglich

NPS: 71
und 4,8 / 5 durchschn. End-Nutzerbewertung

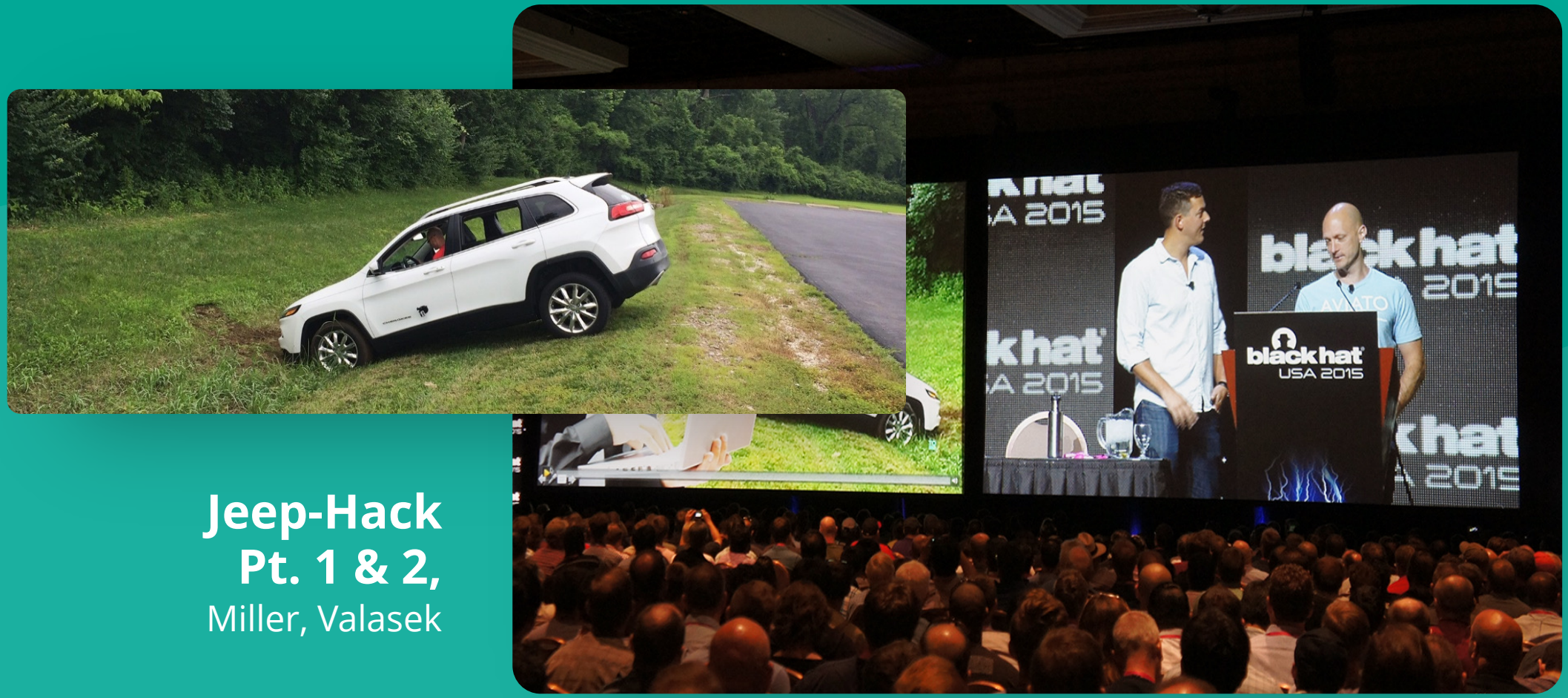
Old news: Daten und Software dominieren Autos bereits länger.



Quellen: Roland Berger, Informationisbeautiful.net, NXP

SoSafe
Cyber Security Awareness

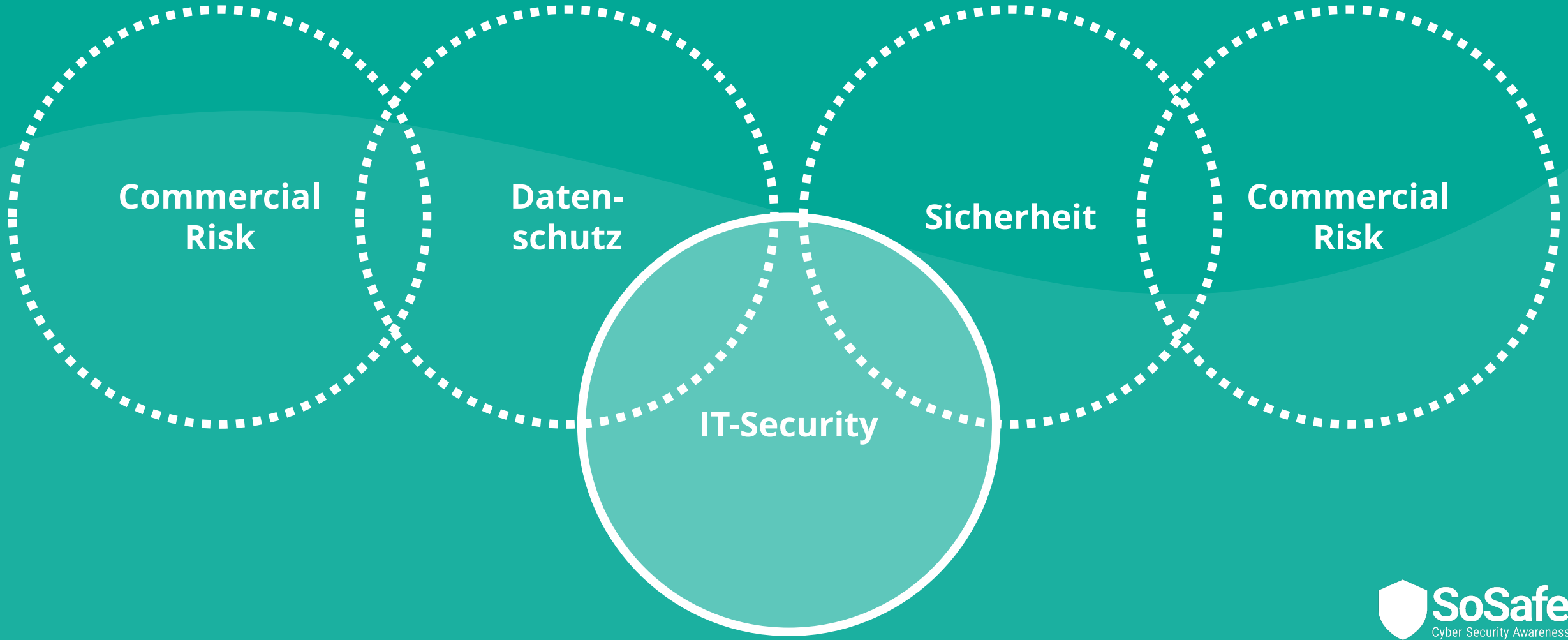
Die Implikationen kennen wir alle nur zu gut.



Jeep-Hack Pt. 1 & 2,
Miller, Valasek

SoSafe
Cyber Security Awareness

IT-Security hat einen Einfluss auf Datenschutz und allgemeine Sicherheit.



SoSafe
Cyber Security Awareness

Das Problem: Die Bedrohungen bestehen entlang des gesamten Lifecycles.

SoSafe
Cyber Security Awareness

Mögliche „Real World“ Szenarien.

Nicht erschöpfend!

Ideologische Angriffe / Erpressung

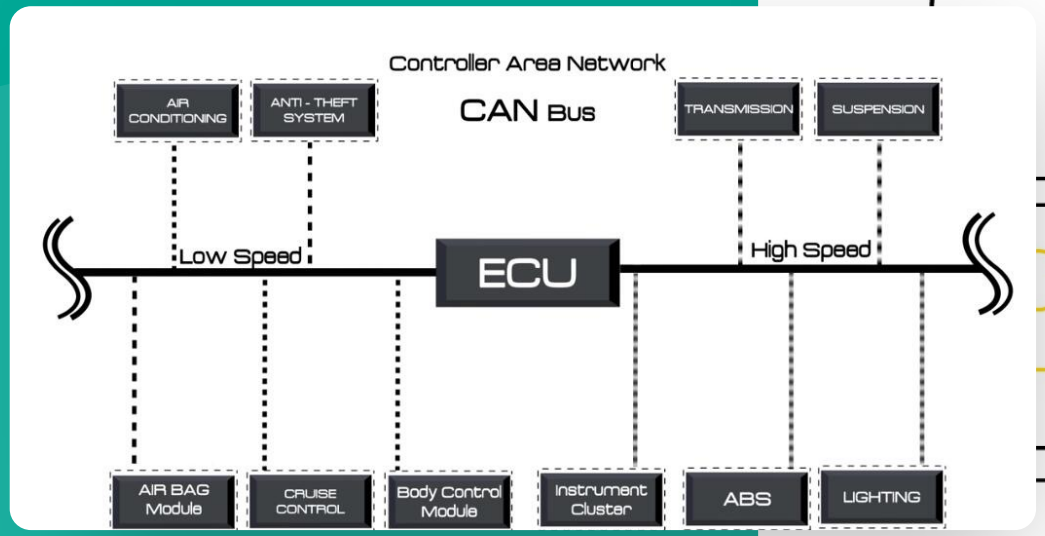
Industrie-spionage

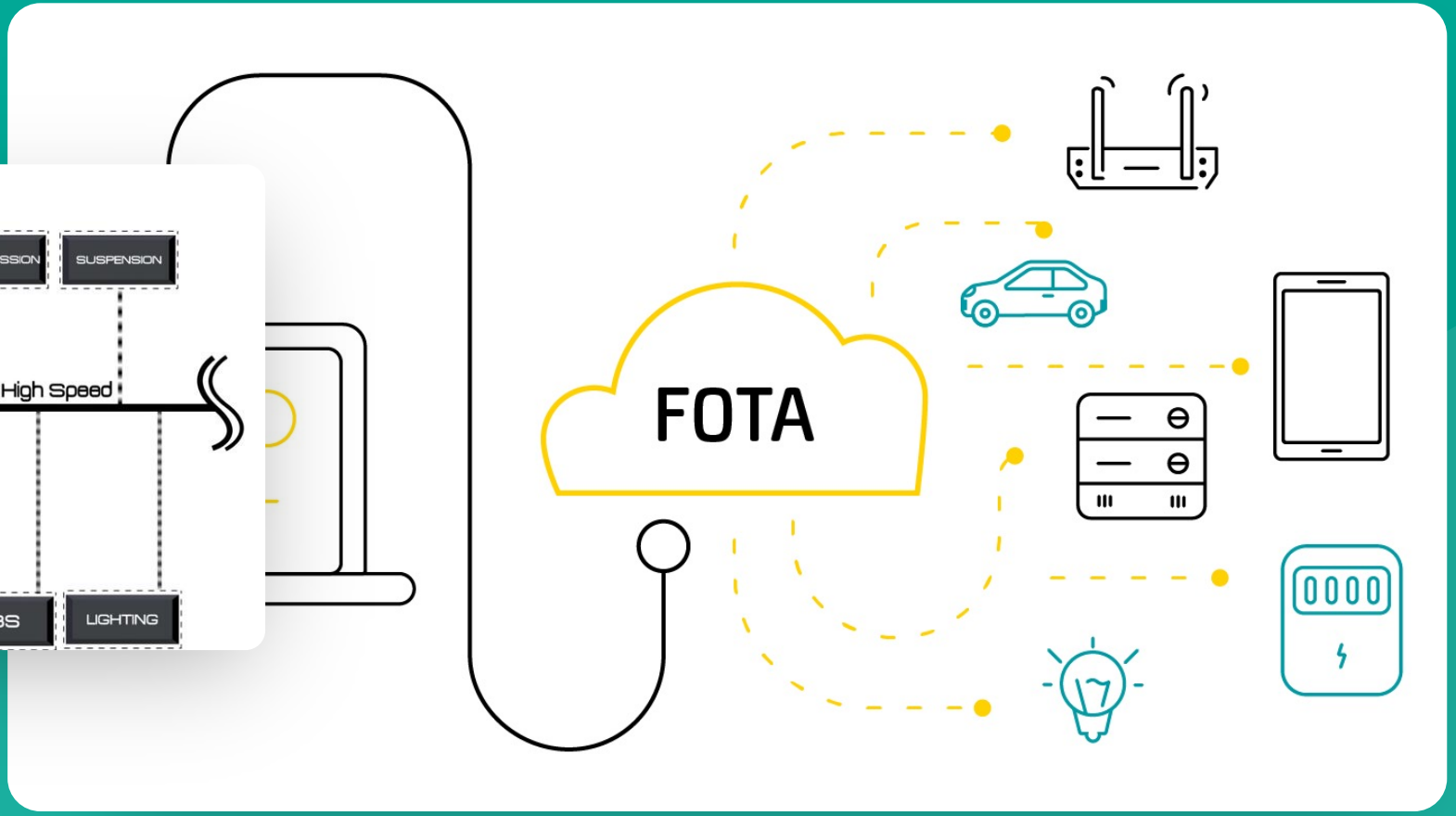
Technische Sabotage

Supply-Chain-Angriffe

SoSafe
Cyber Security Awareness

Angriffe: Wie in anderen Bereichen, gibt es auch hier einen schwierigeren Weg…





SoSafe
Cyber Security Awareness


...und
einen
leichteren.

Hacker greifen Systeme an?

Selten –
9 von 10 Cyberangriffen Starten bei den Mitarbeitenden.

Quelle: Bundesamt für Sicherheit in der Informationstechnik

Die Mitarbeitenden sind häufig die letzte Verteidigungslinie.

3,4 Mrd.
Phishing-Mails werden täglich versandt.

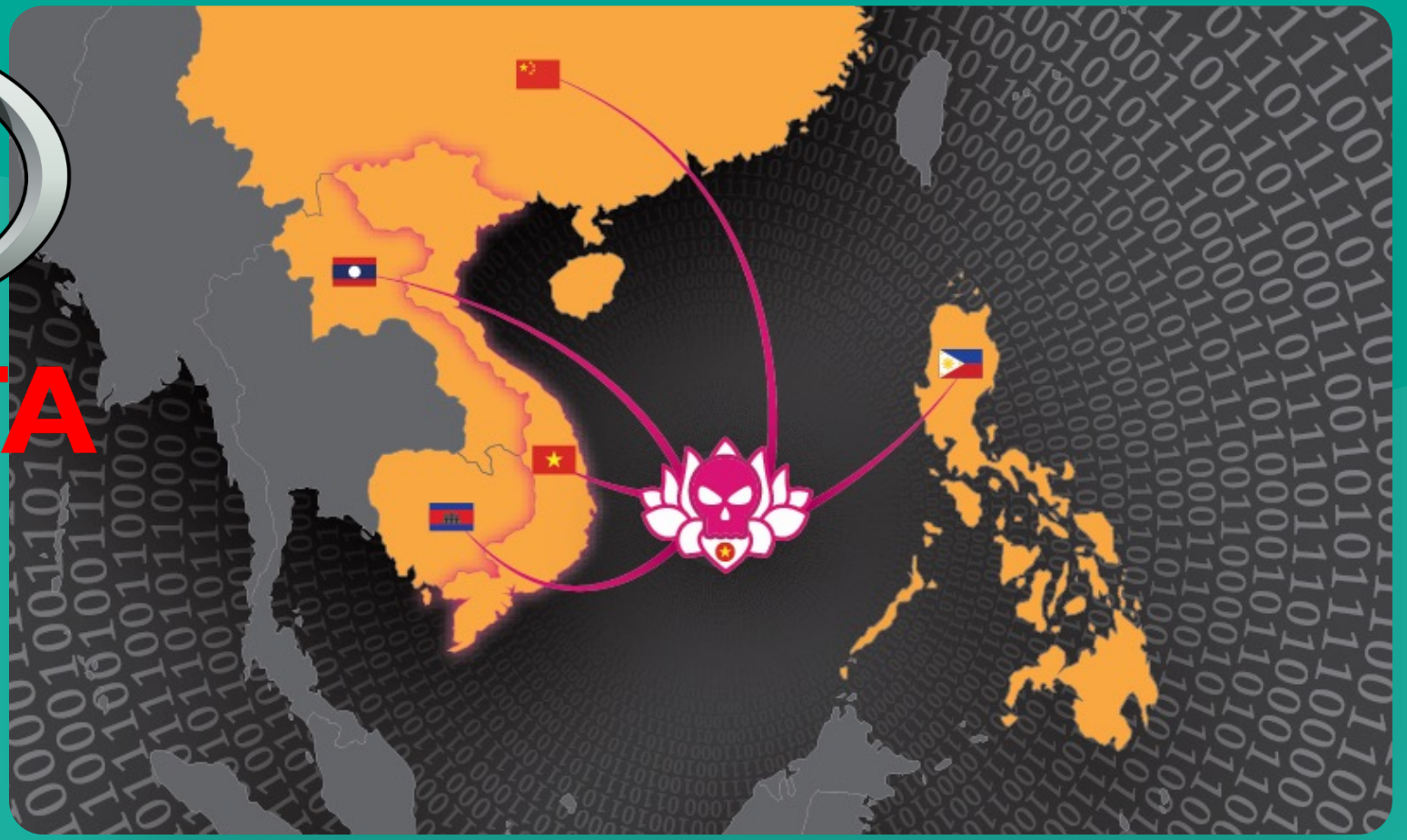
~610 Mio.
kommen durch den Spam-Filter.

~300 Mio.
Phishing-Mails werden geöffnet.

Quellen: Digital Shadows, Phish-Test-de; SoSafe Kundenprojekte 2018-2020

Wer sind die Angreifer?
Zunehmend auch APTs.

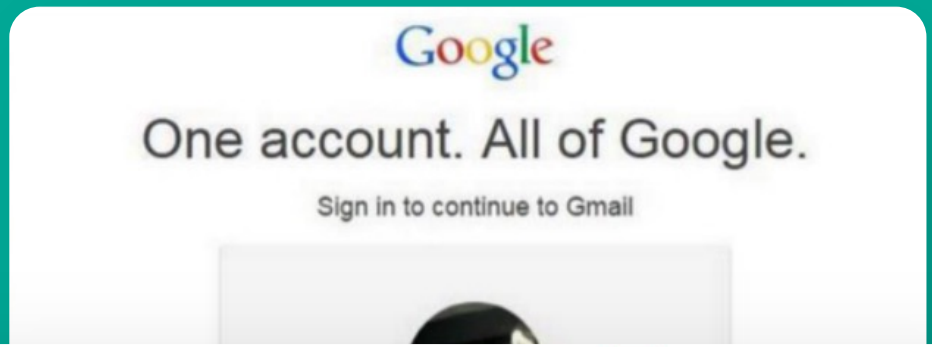
TOYOTA



OceanLotus
(APT32)

SoSafe
Cyber Security Awareness

Fokus auch bei APT-Kill-Chains: Human Factor.



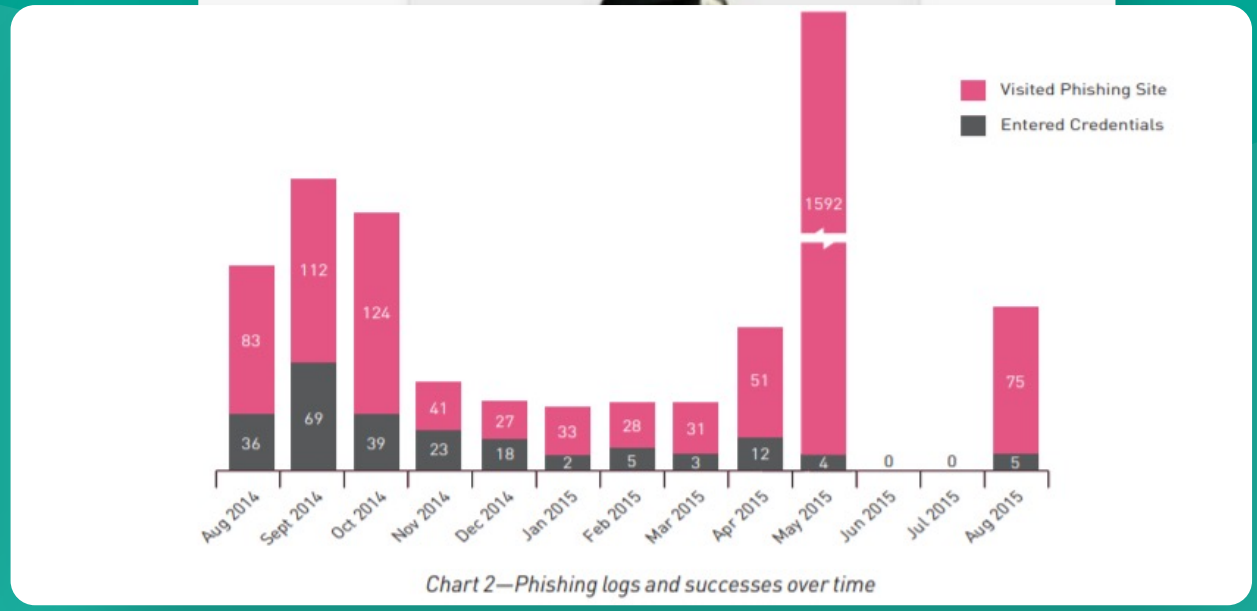
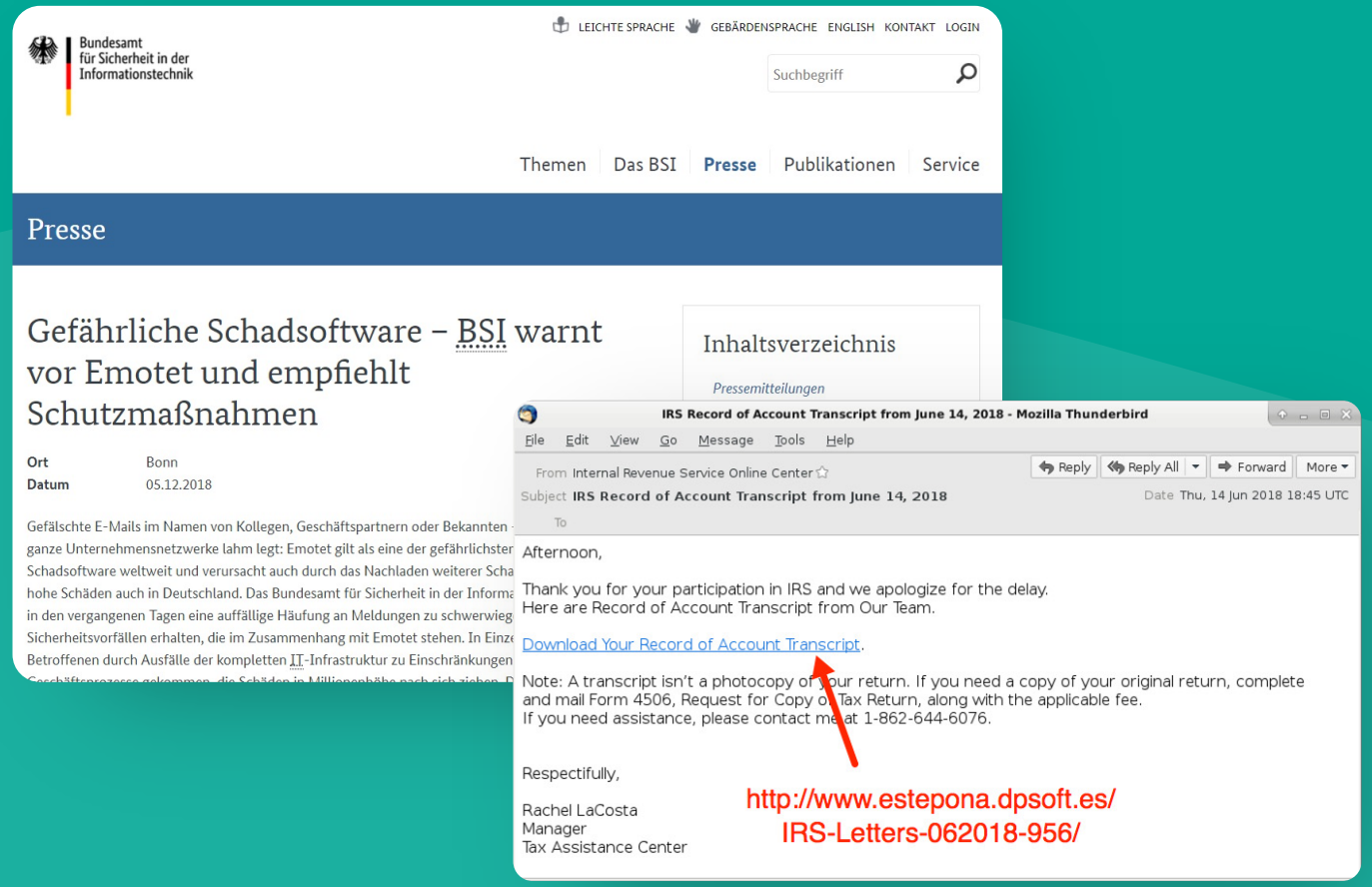


Chart 2—Phishing logs and successes over time

Quellen: Bundesamt für Verfassungsschutz, Check Point, Trend Micro, FireEye, Citizen Lab

SoSafe
Cyber Security Awareness

Tools: Emotet war nur ein Vorgeschmack bei Supply-Chain-Angriffen.



Polymorpher Schadcode
Emotet verändert sich stetig selbst und ist schwerer zu entdecken

Outlook Harvesting
Passende Betreffe und Themen = perfekt für Lieferkettenangriffe

„Dynamite Phishing“:
Zielgerichtete, aber doch großzahlige Angriffe

SoSafe
Cyber Security Awareness

Double Extortion:
Ransomware-Gangs ändern zudem ihre Taktik.

CYBERANGRIFF

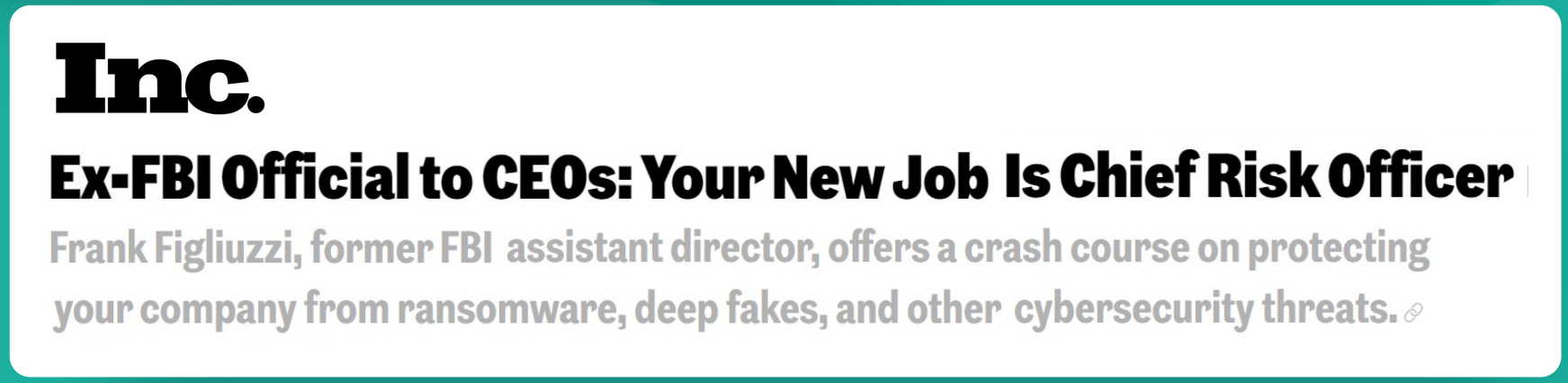
Hackerangriff: Warum Gedia kaum Informationen preisgibt

Flemming Krause 19.02.2020 - 06:00 Uhr

"Now for the tasty. gedia.com . They didn't get in touch. All computers on the network are encrypted. More than 50 GB of data was stolen, including drawings, data of employees and customers. All this is carefully prepared for implementation on the stock exchange of information. What they don't buy, we'll post it for free. 7 days before publication."

SoSafe
Cyber Security Awareness

IT-Sicherheit liegt vermehrt in der Verantwortung der Geschäftsführung.



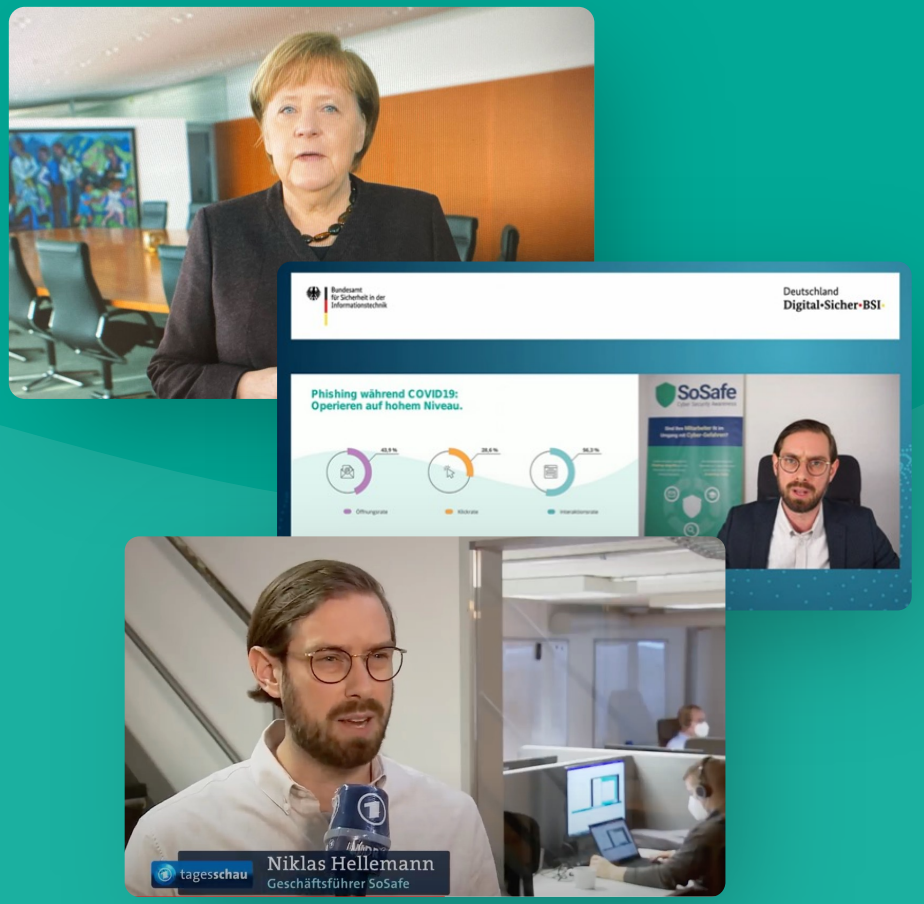
Quellen: Versicherungswirtschaft Heute (2020), Inc. (2021)

SoSafe
Cyber Security Awareness

„New Work“ erhöht die Bedrohung zusätzlich.

x3

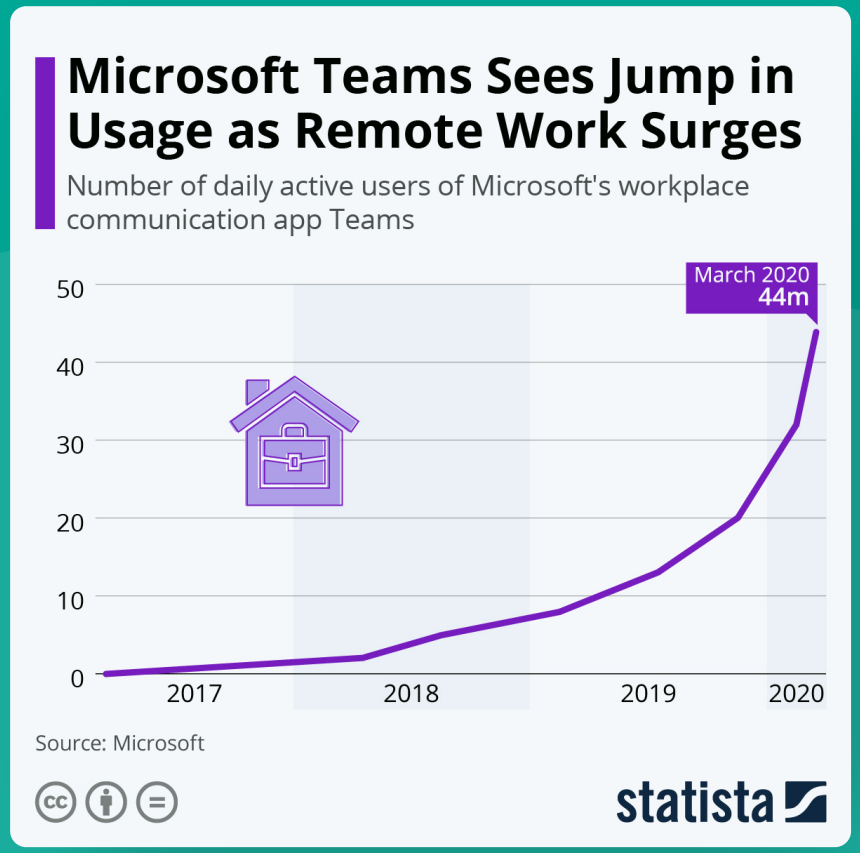
erhöhter Erfolg bei
dezentralem Arbeiten

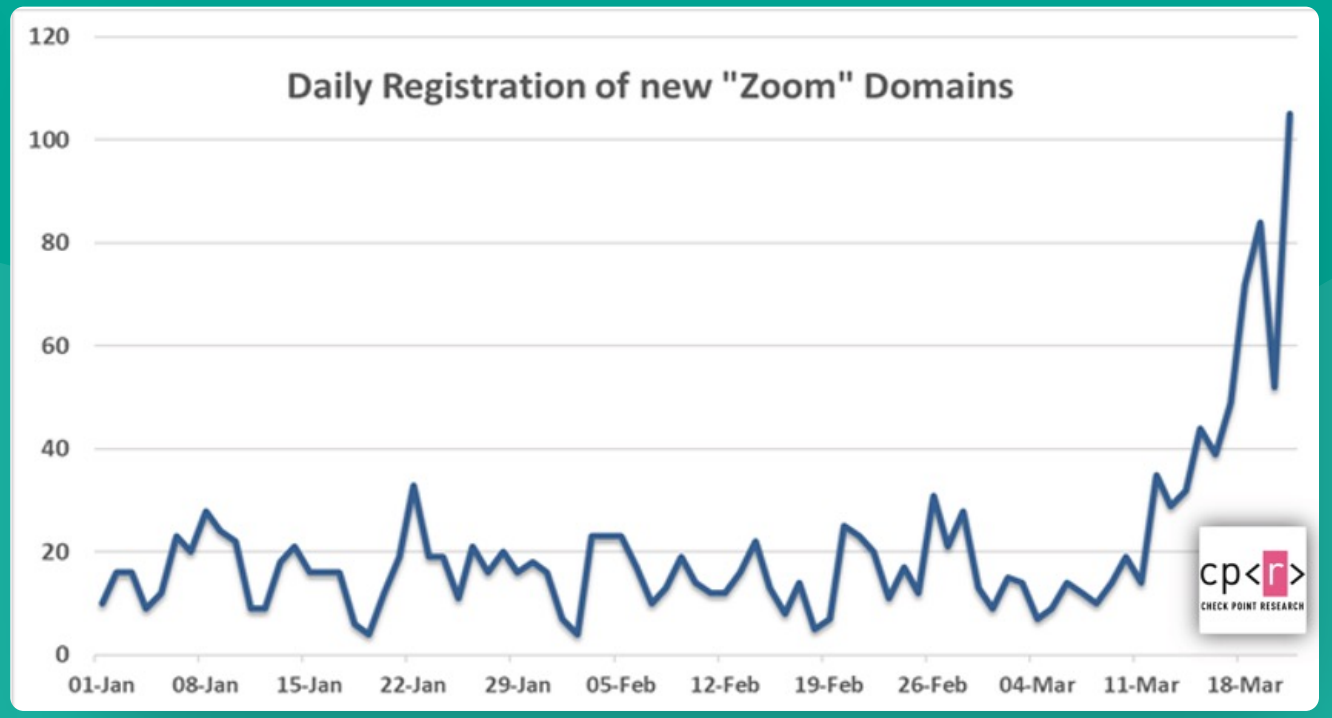


SoSafe
Cyber Security Awareness

Human Risk Review 2021

Denn: Die Angriffsfläche vergrößert sich.

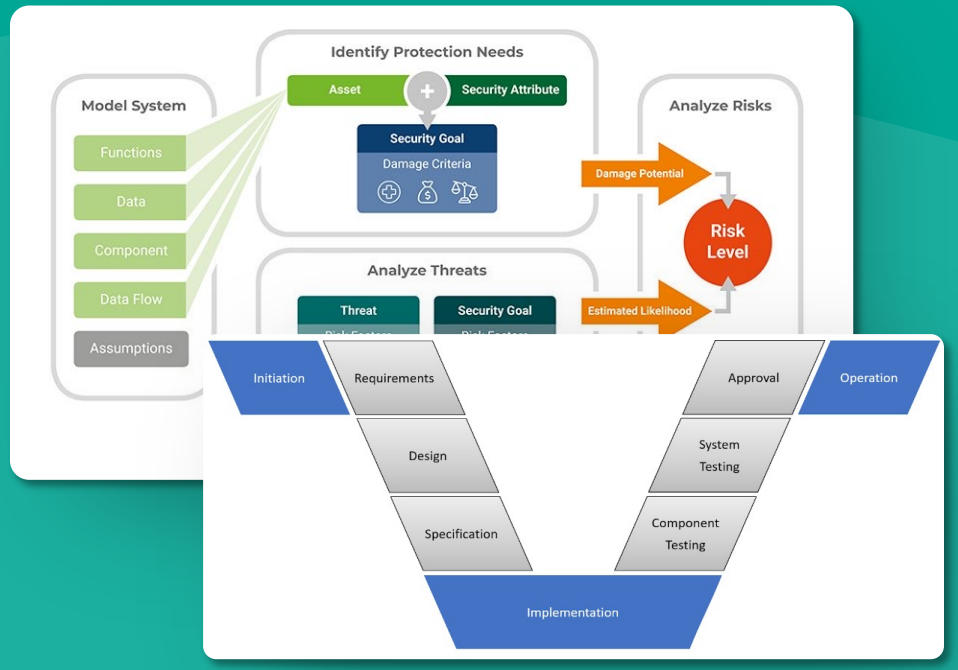




Quellen: Statista 2020, Check Point

Zwei Ansätze zur Risikominimierung.

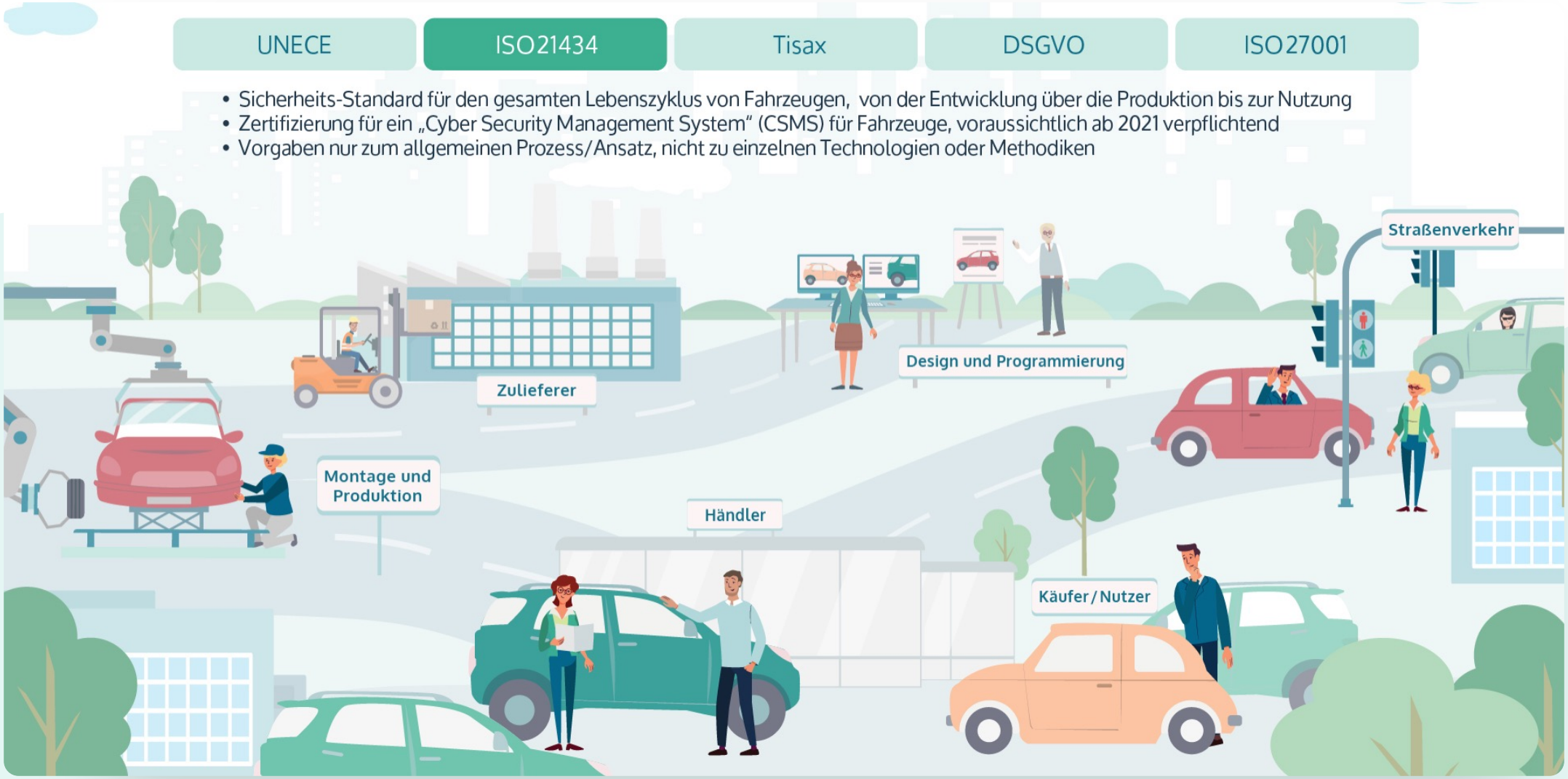
Security by Design



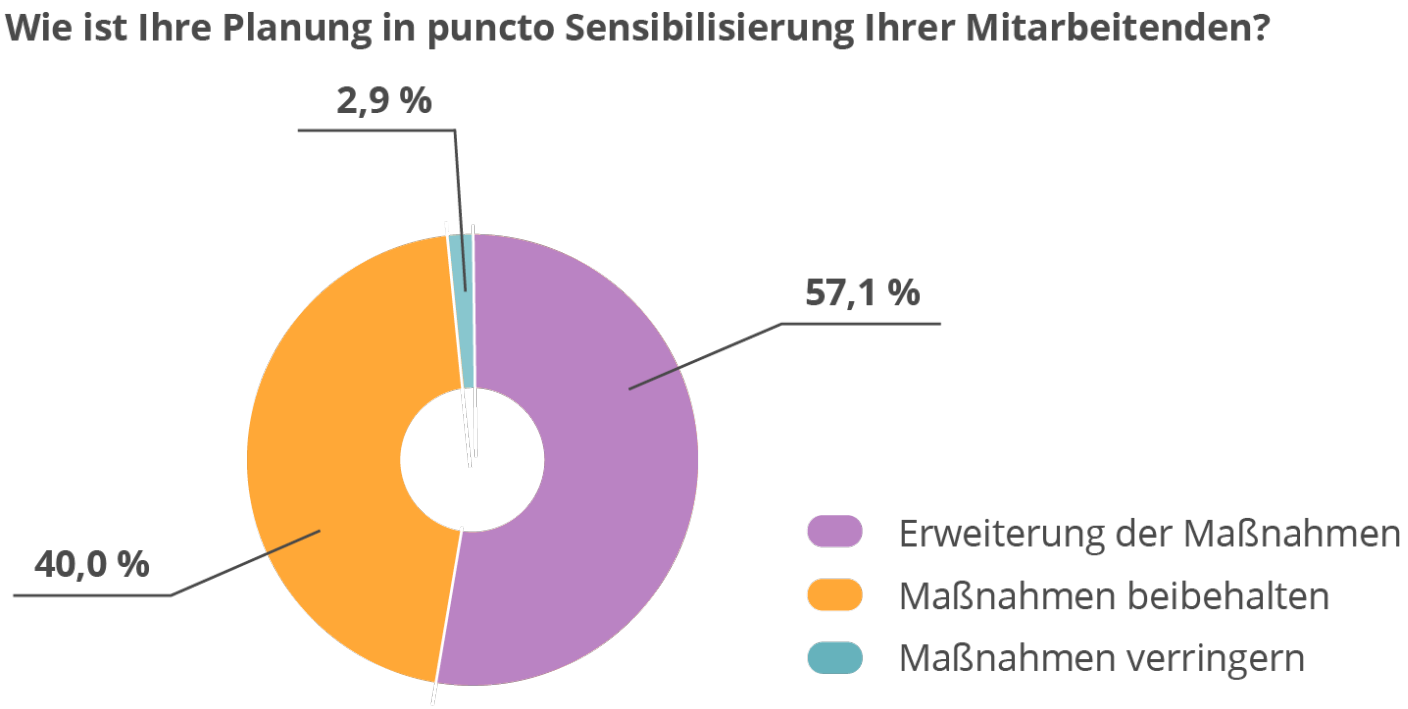
Training und Sensibilisierung

SoSafe
Cyber Security Awareness

Wir müssen entlang des Lifecycles sensibilisieren.



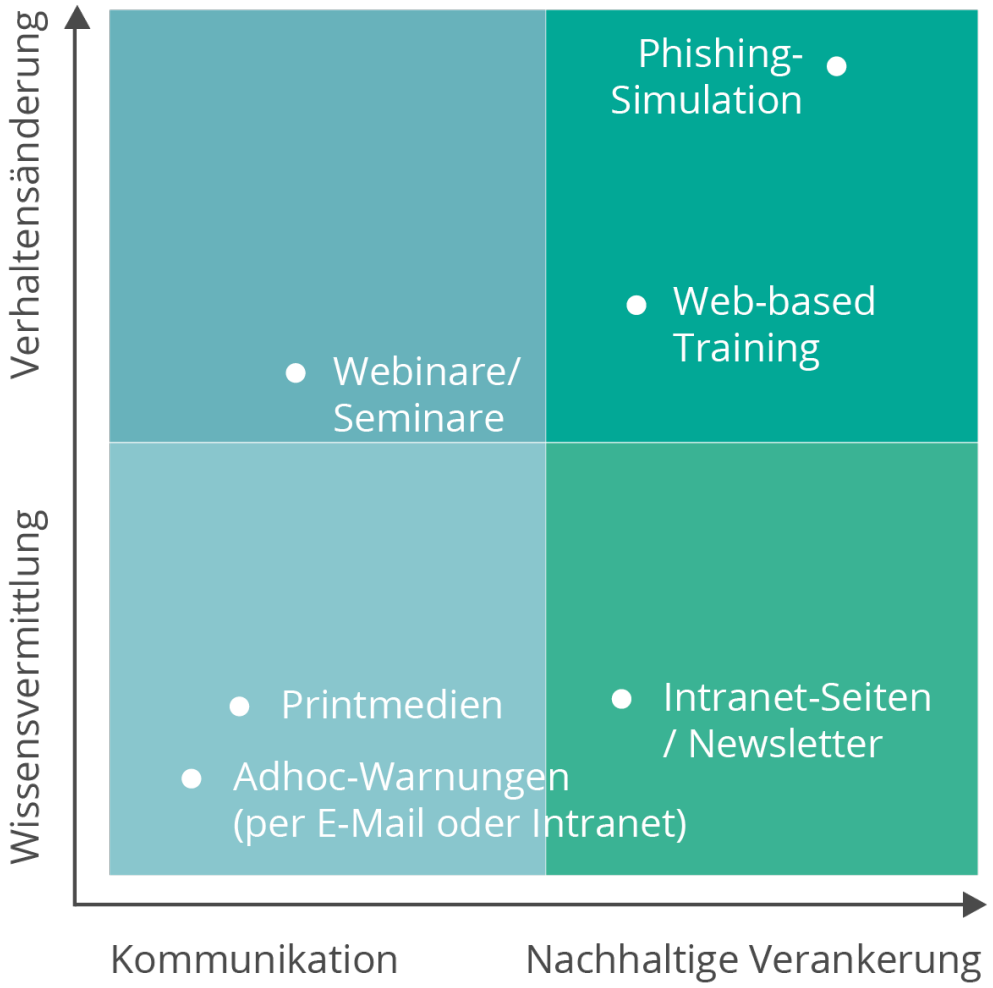
Awareness: Firmen rüsten auf.



Quelle: SoSafe Befragung von IT-Sicherheits-Expertinnen und –Experten.

SoSafe
Cyber Security Awareness

Der Trend geht in Richtung Resilienz und nachhaltiger Verankerung.



Quelle: SoSafe Human Risk Review 2021

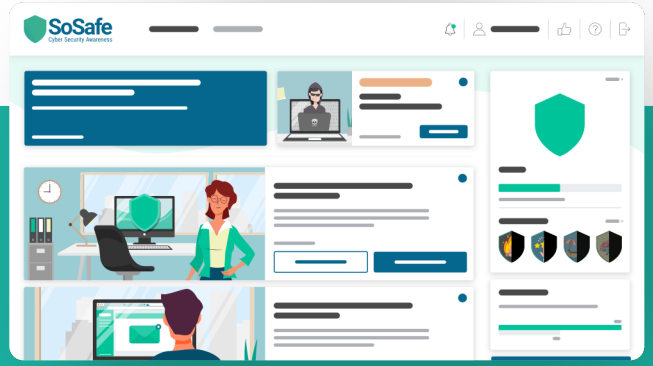
SoSafe
Cyber Security Awareness

Juhu! Die neue IT-Sicherheitsrichtlinie!

SoSafe – The Human Risk OS

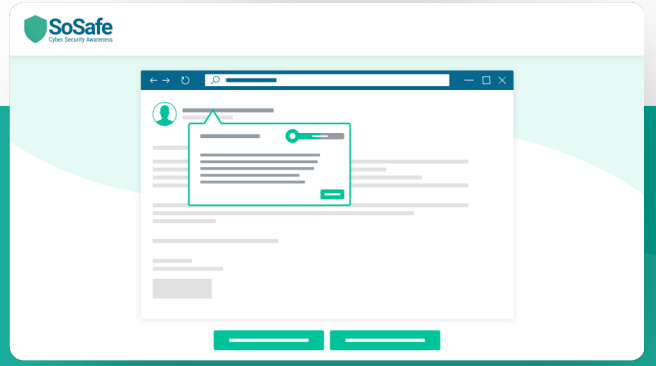
Die SoSafe-Plattform minimiert das Risiko kontinuierlich -
und bindet die Mitarbeitenden aktiv in die Verteidigung ein.

„Teach“



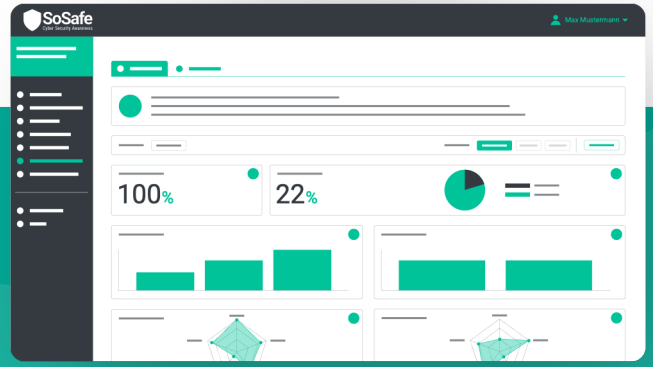
Datenbasierte Micro-Learning-Plattform

„Transfer“



Smarte Angriffs-Simulation

„Act“

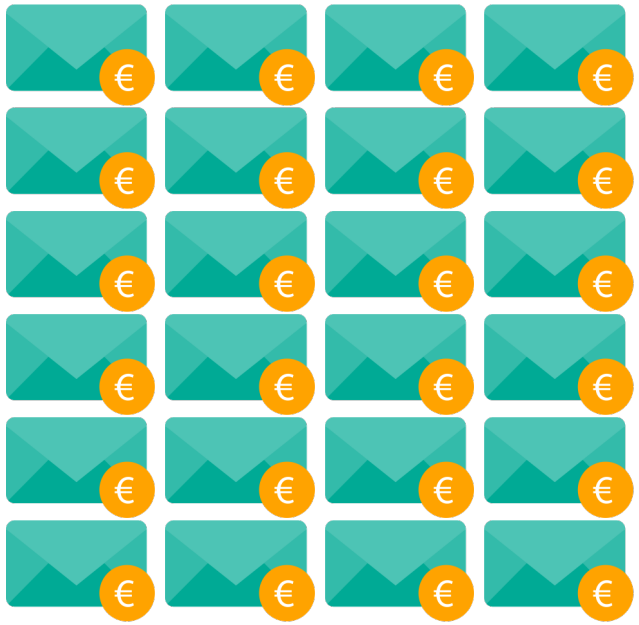


Meldetool & Strategisches Monitoring

Systematische Awareness senkt das Risiko nachweisbar. Und das macht auch noch Spaß!

Erwartungswert des
Schadens in Höhe von

~ 250.000 € p.a.



66 %

Reduktion der
Klickrate

Erwartungswert des
Schadens reduziert sich auf

~ 85.000 € p.a.

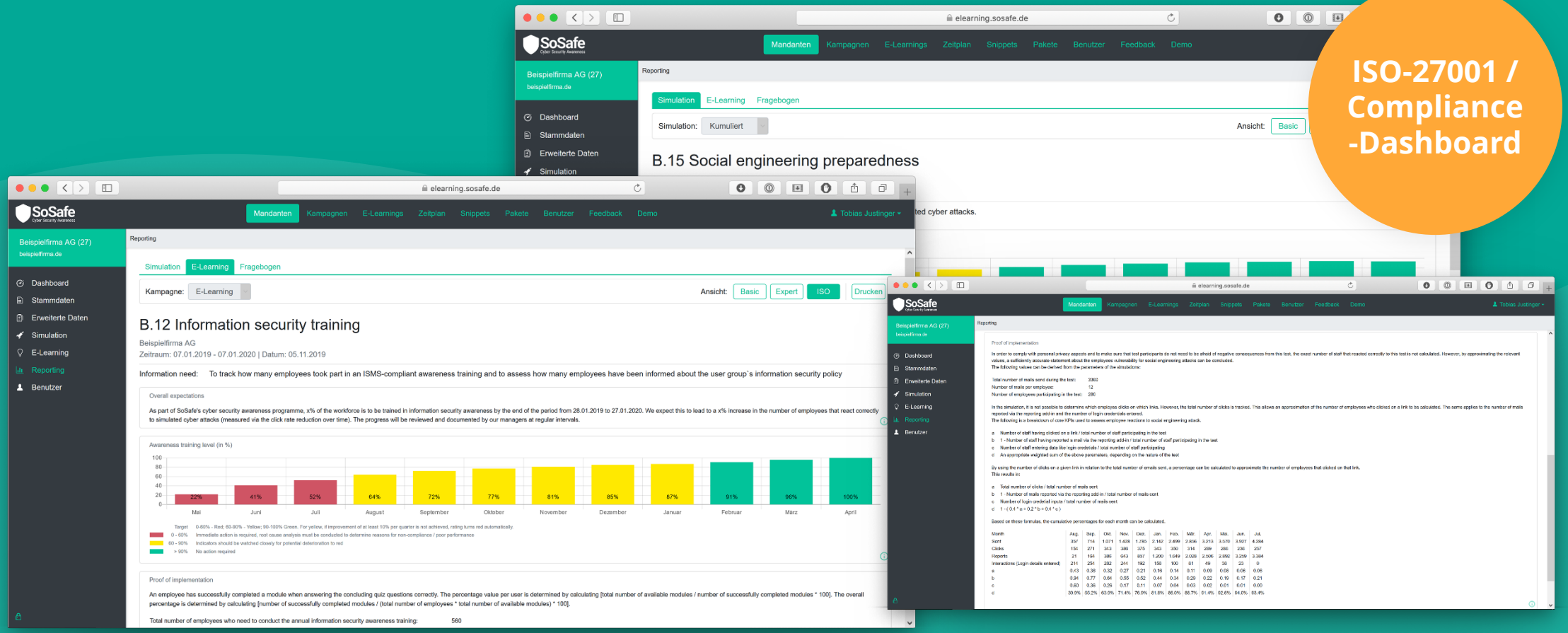
4,8 ★★★★½

Durchschnittliche Bewertung durch die Mitarbeitenden unserer Kunden

Wichtig: Wie in der IT-Sicherheit üblich, senkt sich das Risiko nicht auf 0 % - statistisch kann aber eine Reduktion von 50 % bis 70 % erzielt werden.
Quelle: Bitkom, SoSafe

SoSafe
Cyber Security Awareness

Ob TISAX oder ISO: Mitarbeitersensibilisierung einfach nachweisen.



SoSafe
Cyber Security Awareness

Der SoSafe „Human Risk Review 2021“.

1. Umfangreiche Analysen zur aktuellen Cyber-Bedrohungslage
2. Experten-Interviews zum Faktor Mensch in der IT-Sicherheit
3. Konkrete Empfehlungen zur Minimierung des Human Risks

Sie erhalten ein exklusives Vorab-Exemplar im Nachgang

SoSafe
Cyber Security Awareness

“Amateure hacken Systeme, Profis hacken Menschen.“

Bruce Schneier
Experte für Kryptographie
und Computersicherheit,
Harvard University

SoSafe
Cyber Security Awareness

SoSafe GmbH
Ehrenfeldgürtel 76, 50823 Köln
www.sosafe.de | info@sosafe.de

DIGITAL TOP 50

THE EUROPAS

smart country Startup Award Winner 2020