
PASSION4IT
CYBER SECURITY
STATUS QUO
IM MITTELSTAND
Florian Laumer | 16.11.2023 | BFMT Fachtag Viechtach

TOPICS

01 Cyber Security Status Quo

02 Aktuelle Gefährdungslage in Deutschland

03 Lage im Mittelstand

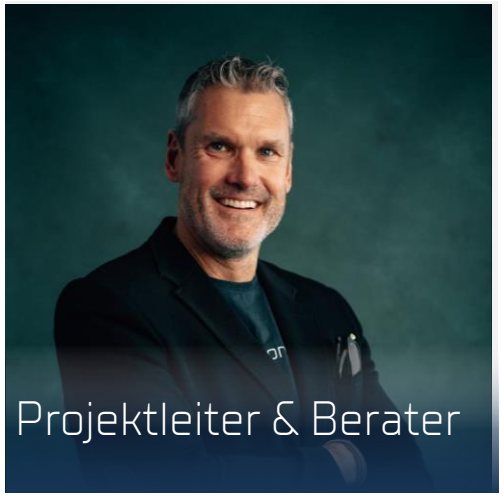
04 einen Hauch NIS-2

05 Welche Rolle spielt KI

06 Was sollten KMUs jetzt machen?

FLORIAN LAUMER

PASSION4IT



+49 151 11676 502

Florian.laumer@passion4it.de

https://www.linkedin.com/in/florianlaumer/

www.passion4it.de

- ✓ 25 Jahre Leidenschaft für IT, Digitalisierung, digitale Transformation und Innovation
- ✓ Hands On Mentalität
- ✓ ITQ-Auditor (Informationssicherheit)
- ✓ LEAD Digital Transformation Analyst (LEADing Practice)
- ✓ Certified SAFe 6 Agilist
- ✓ ICO ISMS Security Officer according to ISO/IEC 27001:2022

SA SAFe 6

LEADing Practice · LEAD DIGITAL TRANSFORMATION ANALYST · Global University Alliance

ICO-CERT International Certification Organization

Zertifizierter Auditor für IT-Sicherheit

ITQ Institut für Technologiequalität

PASSION4IT

PASSION4IT GMBH
ÜBER UNS

Danke das wir uns vorstellen dürfen!

ZAHLEN, DATEN, FAKTEN

2019
Gegründet

8
Digitale Bergführer

60+
Kunden D-A-CH

3,0
Millionen € Umsatz

SKILLS. TOOLS. MINDSET.

So gelingt der Aufstieg in der Digitalisierung!

1

DIGITAL CHECK.

Welchen digitalen Reifegrad hat Dein Unternehmen? Mach den Leistungstest - und wir planen die Route für heute, morgen und übermorgen.

2

CYBER SECURITY.

Safety first! Hier geht es nicht nur um das Gelingen der Expedition, sondern um dein gesamtes Business und deine Reputation.

3

DIGITAL WORK.

... ist mehr als das Installieren von Software! Basierend auf Microsoft365 und verfeinert mit den richtigen KI-Tools schaffen wir den Arbeitsplatz der Zukunft!

SKILLS. TOOLS. MINDSET.

So gelingt der Aufstieg in der Digitalisierung!

PASSION4IT

4

DIGITAL HR

Das vielleicht größte Effizienz-Potenzial in jedem Unternehmen: Vom Bewerbungsprozess bis zur Verrentung, alles in einer Lösung.

5

SMARTE SOFTWARE AUSWAHL.

Ein intelligenter und mehrstufiger Prozess, mit der die Entscheidung für die richtige Lösung gelingt!

6

IT TRANSITION

Make or Buy? Wir analysieren mit unserer Erfahrung und dem Blick von außen Chancen und Risiken in deinem IT-Management.

IMMER WEITER. IMMER BESSER.

Eat. Sleep. Climb. Repeat.

PASSION4IT

TOP 100

top100.de

Top-Innovator 2022

ARBER LAND PREMIUM

DIGITAL SUMMIT COMMUNITY

Club of Climbers

BFMT Fachtag 2023

PASSION4IT

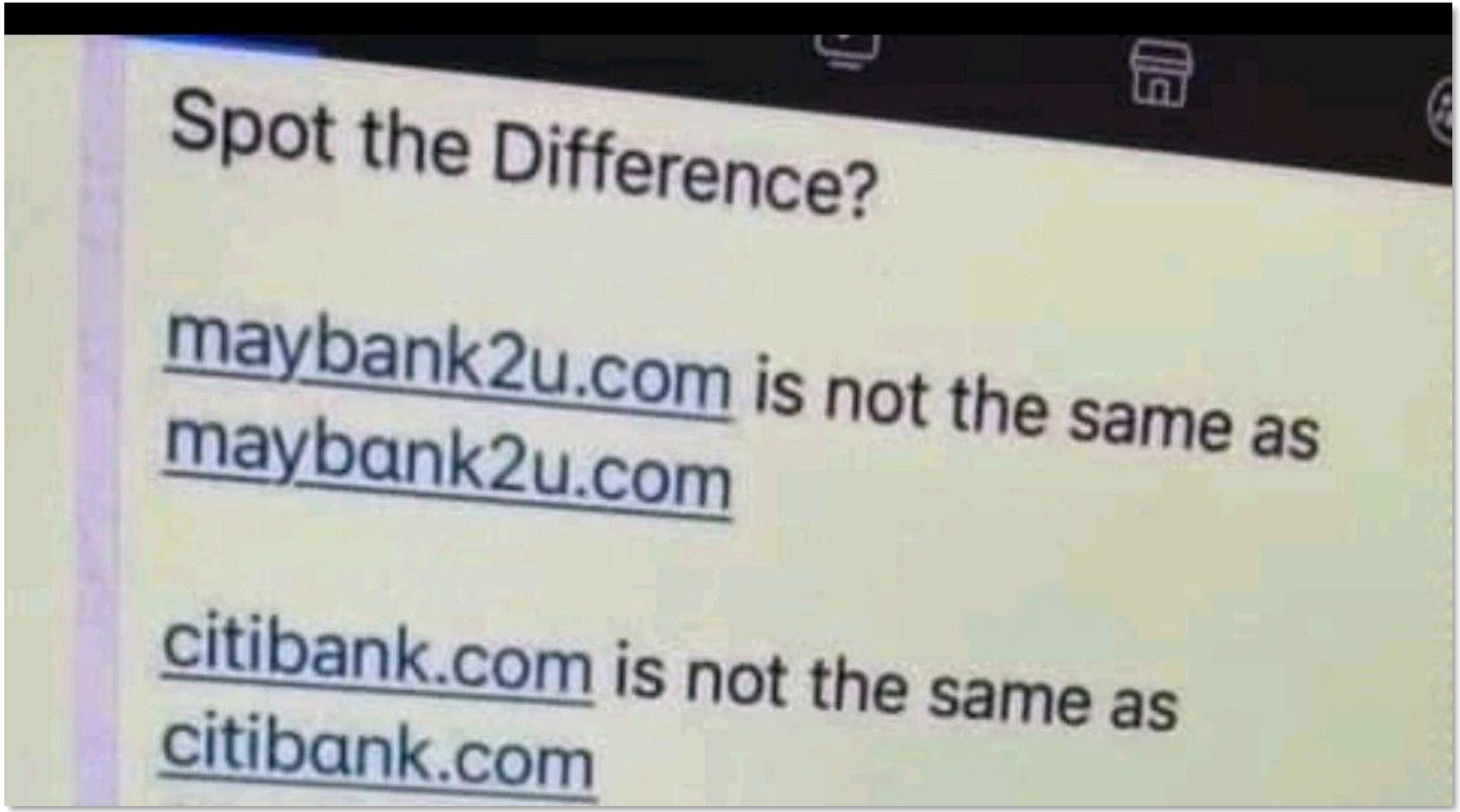
DAS BUSINESS BLIND-DATE FÜR BERGSTEIGER.

- Die Digital Summit Community bietet dir die vielleicht spannendste Kaffeepause der Woche.
- Das Prinzip ist einfach: Melde dich auf der Plattform an und du bekommst eine/n Gesprächspartner/in nach dem Zufallsprinzip zugelost.
- Für 15 Minuten zum virtuellen Erfahrungsaustausch, zum Networking, zum Inspirieren.

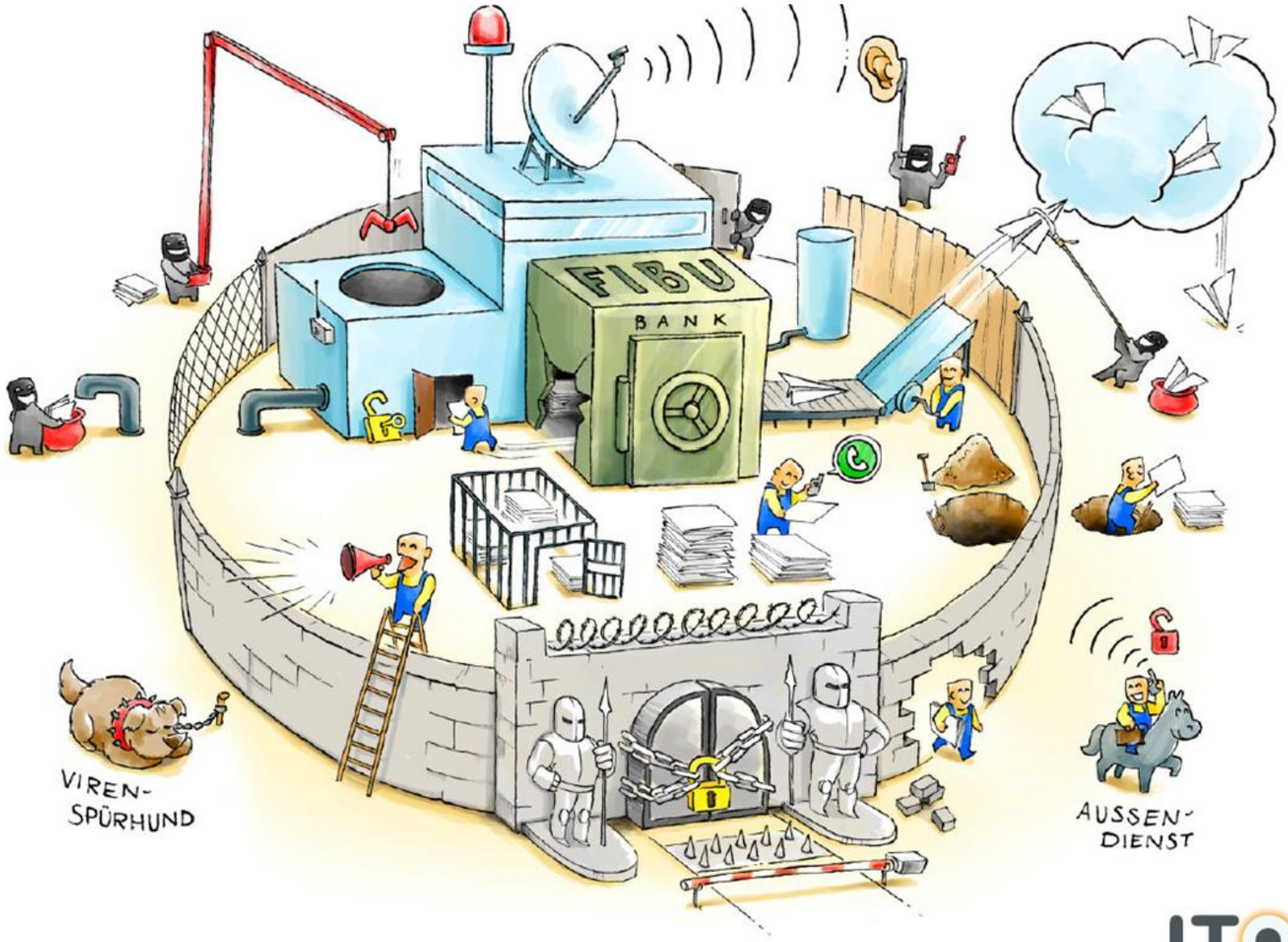
SCAN ME

01

AKTUELLE GEFÄHRDUNGSLAGE IN DEUTSCHLAND


Spot the Difference?
maybank2u.com is not the same as
maybank2u.com
citibank.com is not the same as
citibank.com

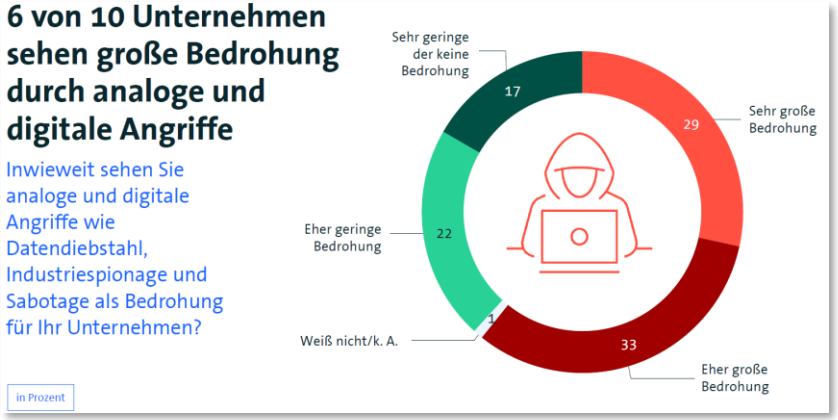
WIE SIEHT ES IM MITTELSTAND AUS?

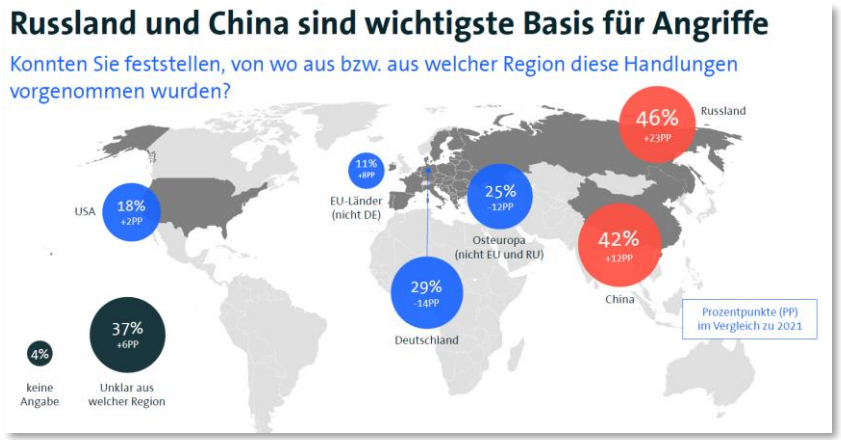


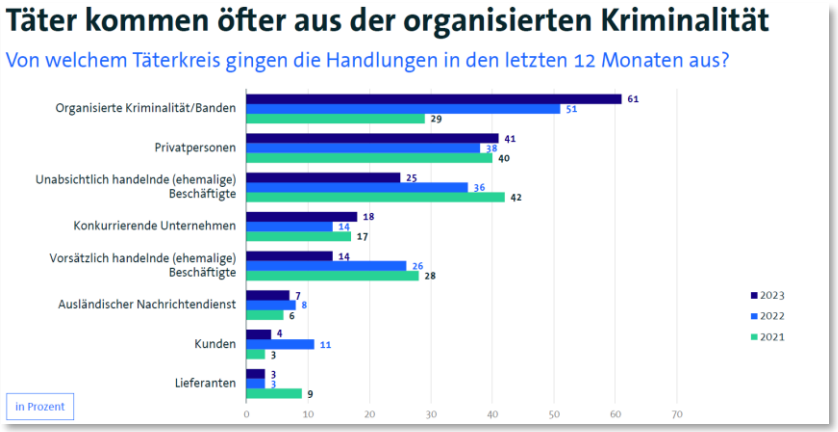
Eine ITQ Graphik

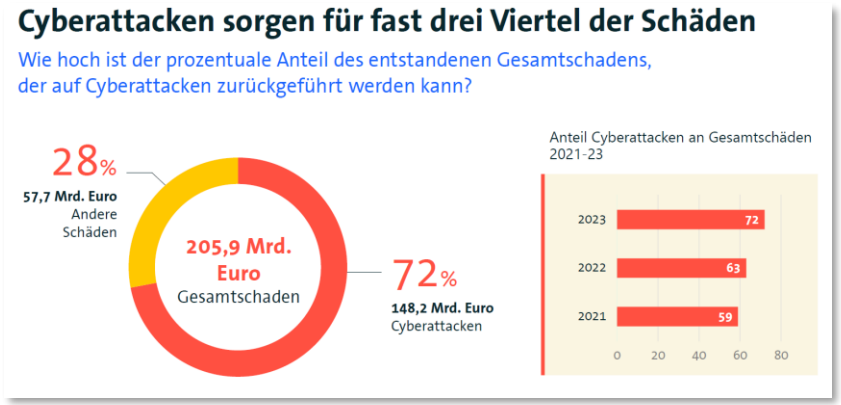
DIE LAGE IM ÜBERBLICK I

BITKOM Wirtschaftsschutz 2022









https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022

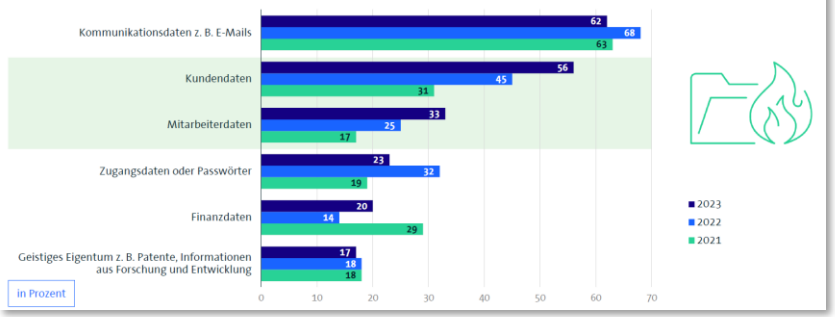
DIE LAGE IM ÜBERBLICK II

BITKOM Wirtschaftsschutz 2022

PASSION4IT

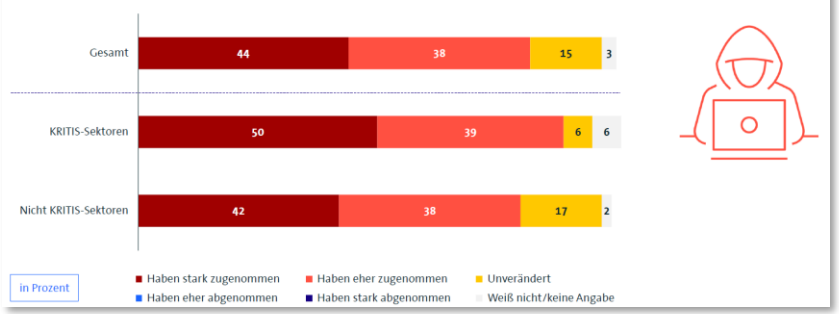
Datendiebstahl: Kunden- und Mitarbeiterdaten im Fokus

Welche der folgenden Arten von digitalen Daten wurden in Ihrem Unternehmen gestohlen?



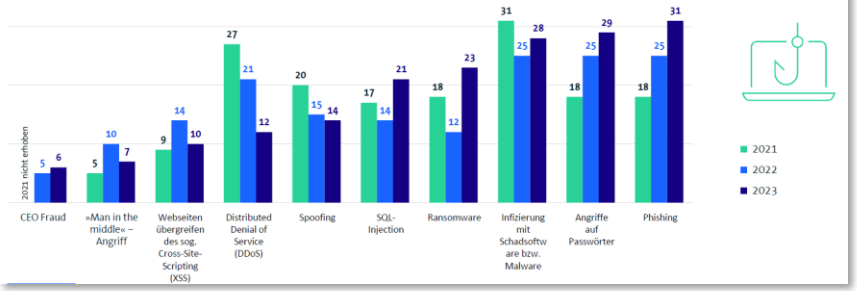
8 von 10 Unternehmen wurden häufiger angegriffen

Wie hat sich die Anzahl der Cyberattacken auf Ihr Unternehmen in den vergangenen 12 Monaten entwickelt?



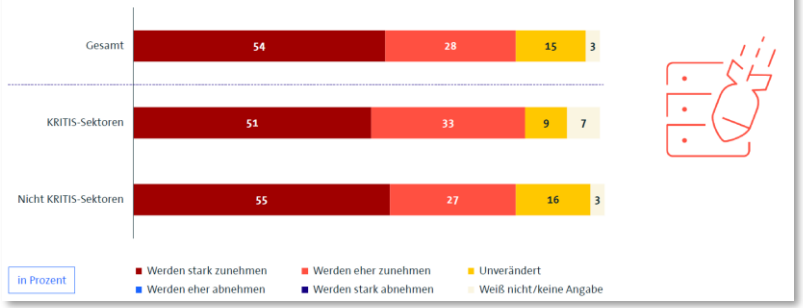
Häufige Schäden durch Phishing, Passwortklau & Malware

Welche der folgenden Arten von Cyberangriffen haben innerhalb der letzten 12 Monaten in Ihrem Unternehmen einen Schaden verursacht?



Wirtschaft erwartet deutliche Zunahme von Cyberattacken

Wie wird sich die Anzahl der Cyberattacken auf Ihr Unternehmen in den nächsten 12 Monaten im Vergleich zu den letzten 12 Monaten voraussichtlich entwickeln?



https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022

03

LAGE IM MITTELSTAND

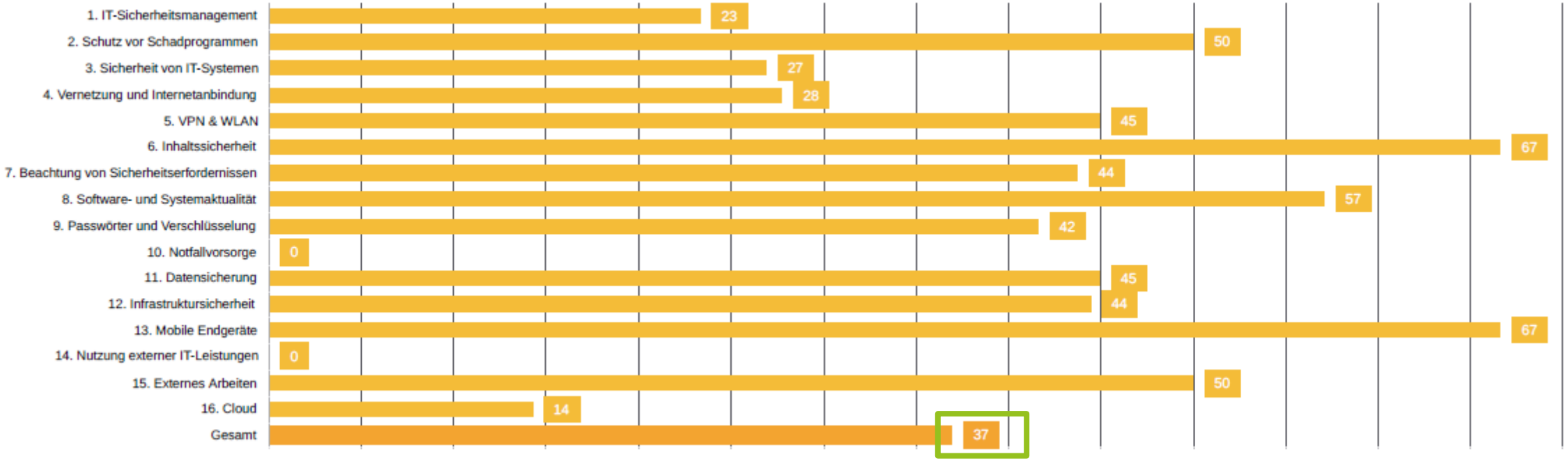
Mehrheit der Unternehmen verschweigt IT-Sicherheitsvorfälle

Redaktion / rh, 5.11.2023, 10:31 Uhr

TÜV-Verband: 82 Prozent der deutschen Unternehmen, die in den vergangenen 12 Monaten IT-Sicherheitsvorfall zu verzeichnen hatten, hielten diesen geheim.


THIS
OPOSSUM
IS NOT
DEAD

ERFÜLLUNGSGRAD NACH PRÜFGRUPPEN



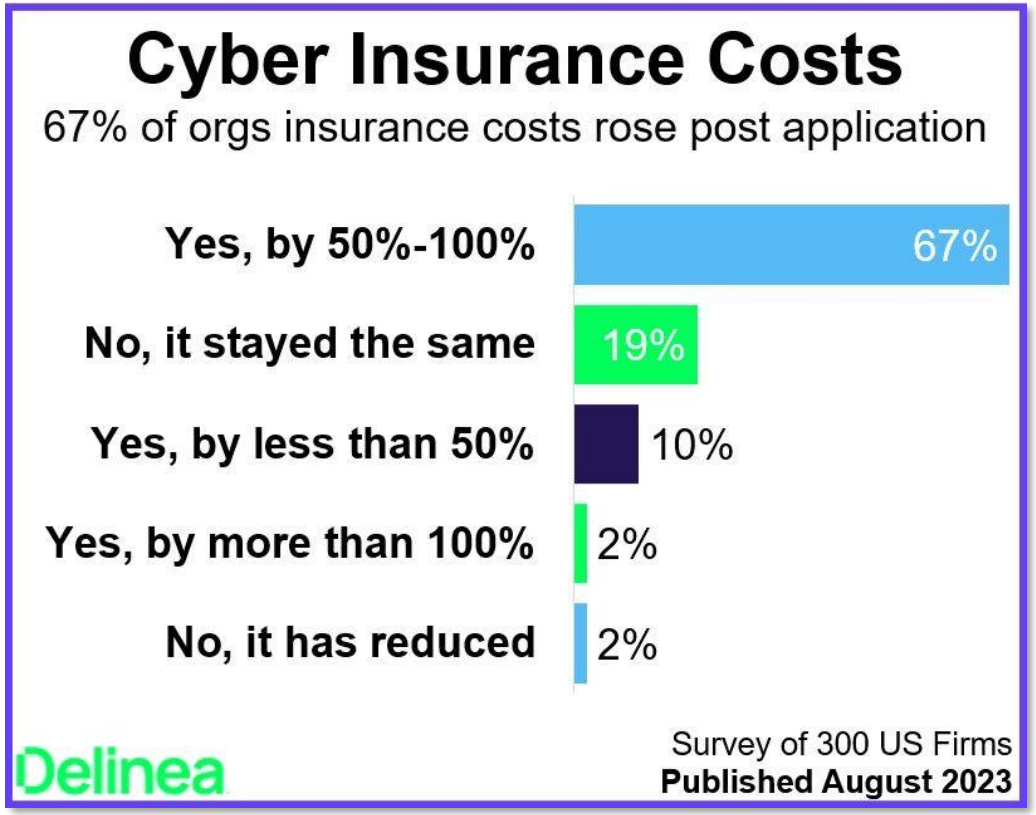
„KRIEGSKLKAUSEL“

PASSION4IT

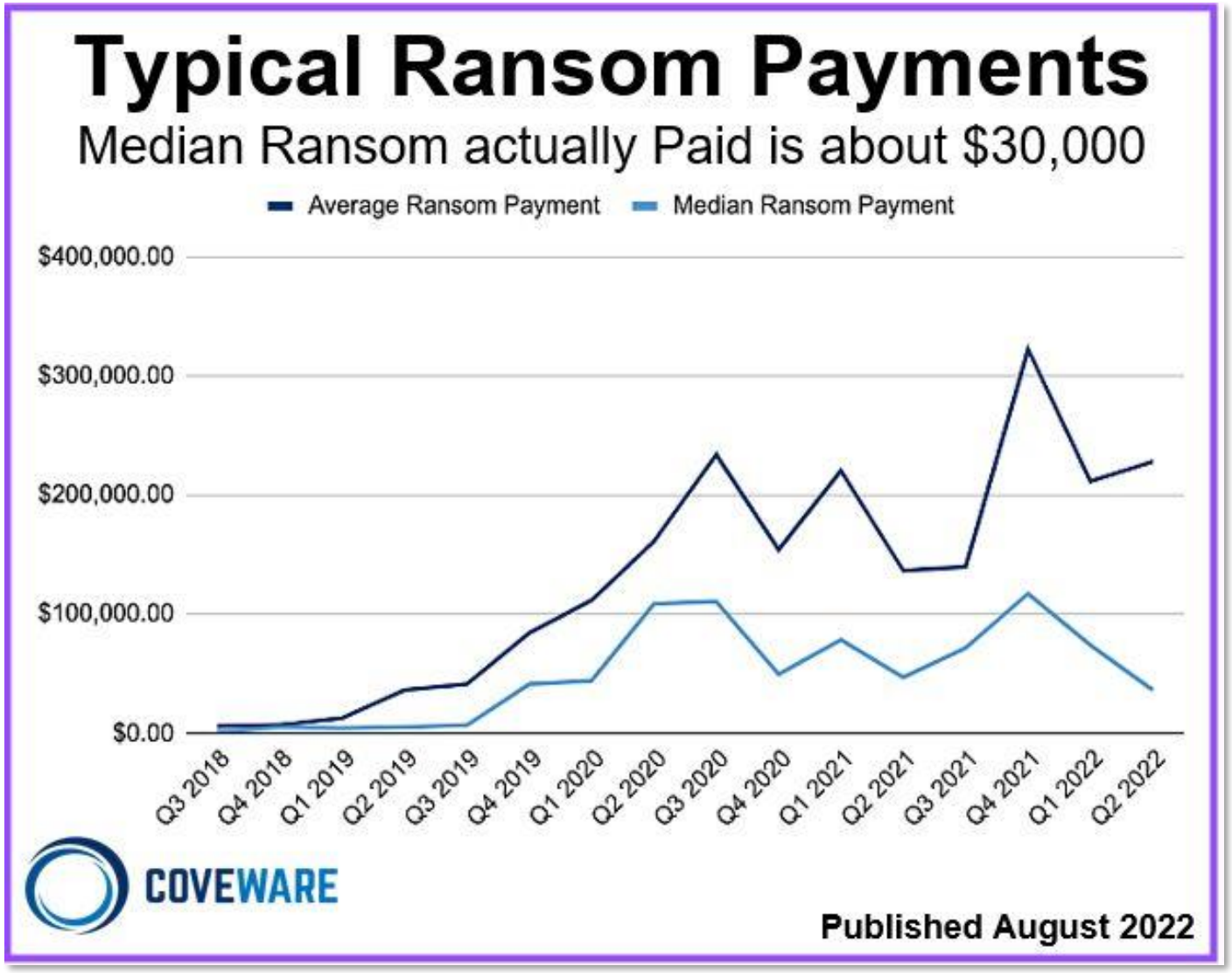
Streichung des bisherigen Ausschlusses 4.1.6 "Krieg und hoheitliche Eingriffe" und Ersatz durch den neuen Ausschluss 4.1.6 "Krieg, hoheitliche Eingriffe und staatliche Cyber Operationen"

Kriegsausschluss im Cybermarkt; Fortschritt ist geboten | Munich Re

STEIGERUNG DER KOSTEN ZUR CYBERVERSICHERUNG



Cyber-Versicherung: Risiken und Trends 2023 | Munich Re


Typical Ransom Payments
Median Ransom actually Paid is about $30,000
Average Ransom Payment
Median Ransom Payment
$400,000.00
$300,000.00
$200,000.00
$100,000.00
$0.00
Q3 2018
Q4 2018
Q1 2019
Q2 2019
Q3 2019
Q4 2019
Q1 2020
Q2 2020
Q3 2020
Q4 2020
Q1 2021
Q2 2021
Q3 2021
Q4 2021
Q1 2022
Q2 2022
COVEWARE
Published August 2022

- MFA
- Backup
- Awarenesstrainings
- Segmentierung
- Notfallplan

04

EIN HAUCH NIS-2

SUPPLY CHAIN-ANGRIFFE

NIS-2

Supply Chain-Angriffe

- „Supply Chain: Sicherheit in der Lieferkette — bis zur sicheren Entwicklung bei Zulieferern“
- „Cyber Security: Die Anforderungen an Betreiber und Mitgliedstaaten steigen, Cyber Security muss auch in Lieferketten betrachtet werden“

Quelle: EU NIS-2 Direktive: Cybersecurity in Kritischen Infrastrukturen (openkritis.de)

NIS-2

Supply Chain-Angriffe

- "Den größten Nachholbedarf gibt es bei den Anforderungen zur Kontrolle von Lieferanten, Dienstleistern und Dritten: Hier liegt der Umsetzungsstand bei 65 Prozent."

Quelle: Untersuchung der Wirksamkeit der IT-Sicherheitsgesetze unter Betreibern Kritischer Infrastrukturen (bund.de)

NIS-2

Supply Chain-Angriffe

„Die wesentlichen und wichtigen Einrichtungen sollten daher die Gesamtqualität und Widerstandsfähigkeit der Produkte und Diensten, die darin enthaltenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit und die Cybersicherheitsverfahren ihrer Lieferanten und Diensteanbieter, einschließlich ihrer sicheren Entwicklungsprozesse, bewerten und berücksichtigen."

Quelle und Vollständige Version der aktuellen Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022: EUR-Lex - 32022L2555 - EN - EUR-Lex (europa.eu)

NIS-2

Supply Chain-Angriffe

- Kunden könnten NIS2-Pflichten an ihre Lieferanten vertraglich übertragen.
- Kunden könnten aus Haftungsgründen einen Nachweis für Cybersecurity von ihrem Lieferanten verlangen.

Quelle und Vollständige Version der aktuellen Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022: EUR-Lex - 32022L2555 - EN - EUR-Lex (europa.eu)

NIS-2

Supply Chain-Angriffe

Es bleibt abzuwarten,

wie die jeweiligen Mitgliedsstaaten der

EU die NIS-2-Richtlinie umsetzen werden,

weil diesbezüglich durchaus Spielräume bestehen.

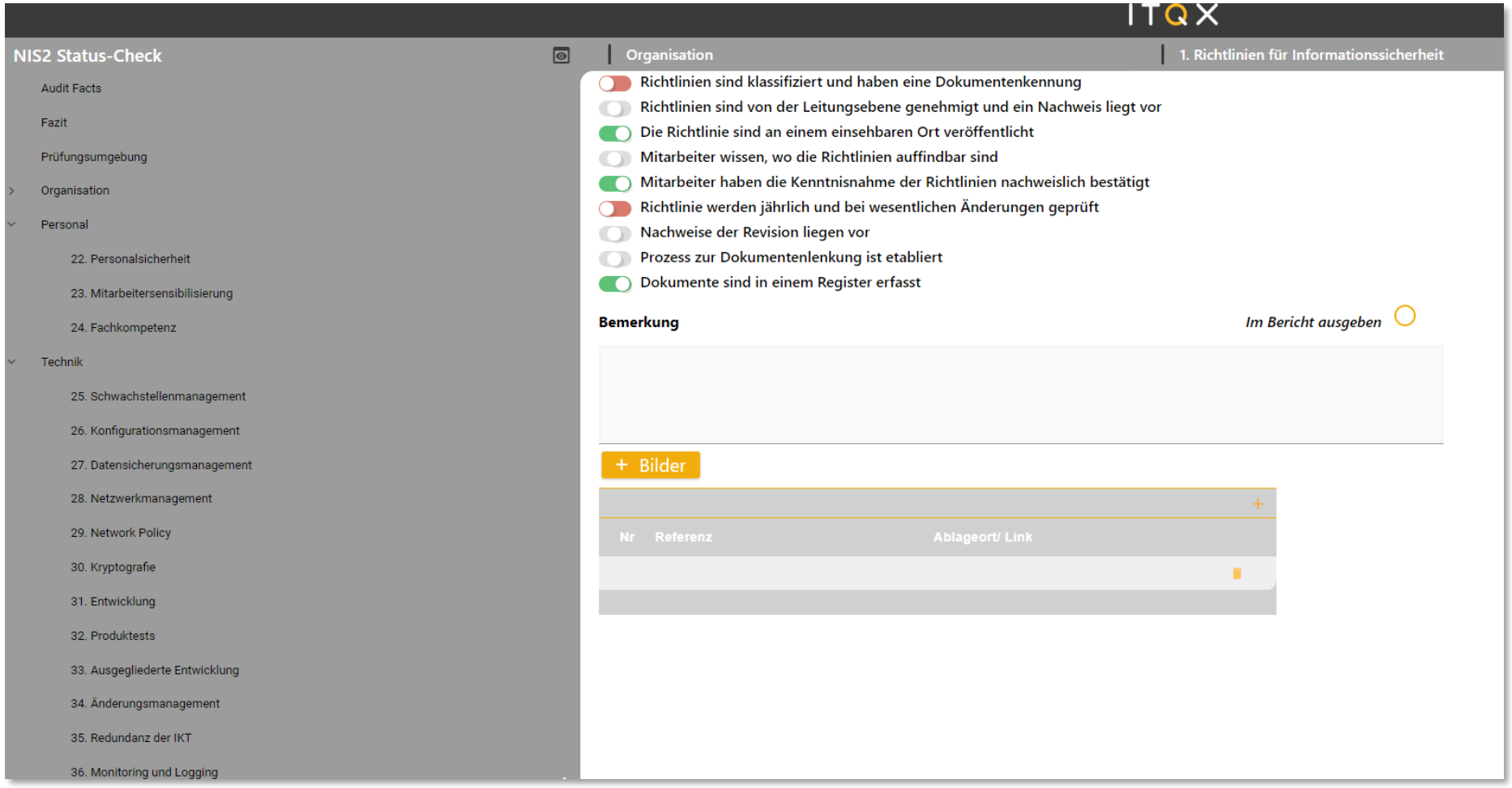
NIS-2 PASSION4IT

Whitepaper

SCAN ME

NIS-2 STATUS CHECK

Professionelle Portallösung (SaaS) für PASSION4IT und Kunden



05

WELCHE ROLLE SPIELT DIE KI

WELCHE ROLLE SPIELT DIE KI

- Erstellung von Deepfakes
- Sprachsynthese für Betrug
- Phishing-Angriffe
- Automatisierung von Netzwerkangriffen
- Verfeinerung von Malware

06

WAS SOLLTEN KMUS JETZT MACHEN?

WIR MÜSSEN 3 DIMENSION BEACHTEN

PASSION4IT

TECHNISCH

- Firewalls und Netzwerksicherheit
- Verschlüsselung
- Anti-Malware-Software
- Patch-Management

ORGANISATORISCH

- Richtlinien und Verfahren
- Schulung und Awareness
- Plan zur Reaktion auf Vorfälle
- Zugriffskontrollen

MENSCHLICH

- Awareness Trainings
- Passwortrichtlinien
- Arbeitskultur
- Humaner Faktor bei Fehlern

CYBER SECURITY CHECK

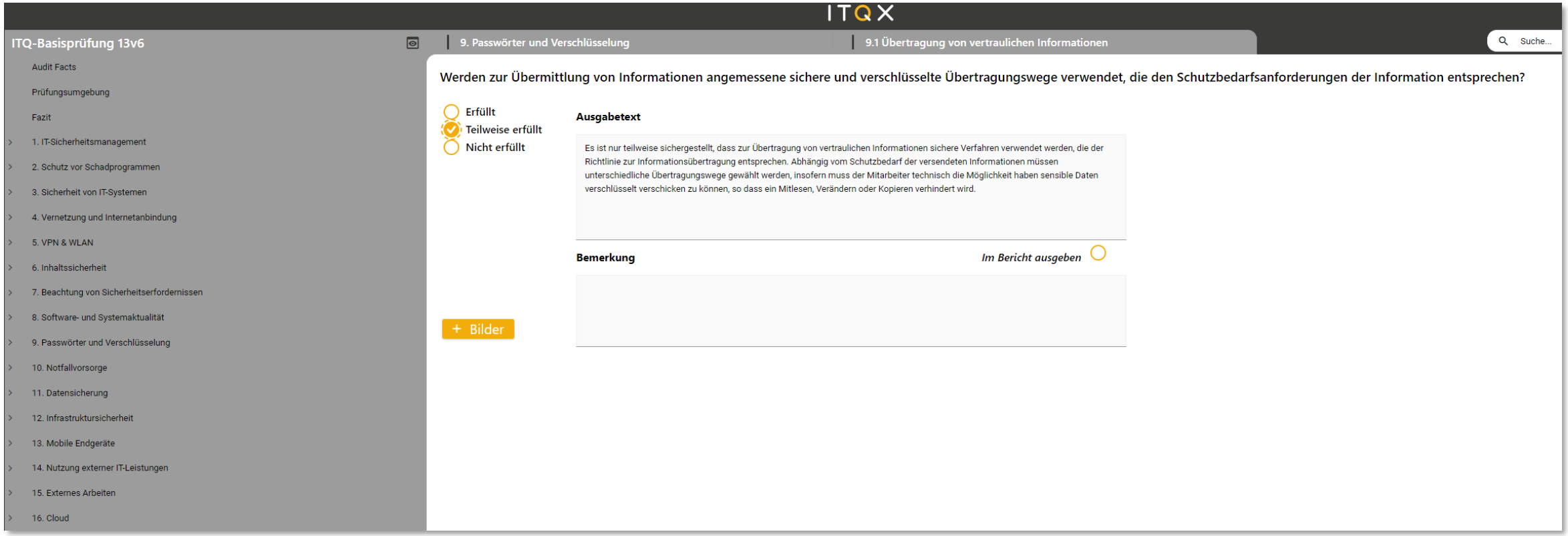
PASSION4IT

Der Ideale Einstieg in die IT-Sicherheit basierend auf dem BSI-IT Grundschutz und der ISO-270001

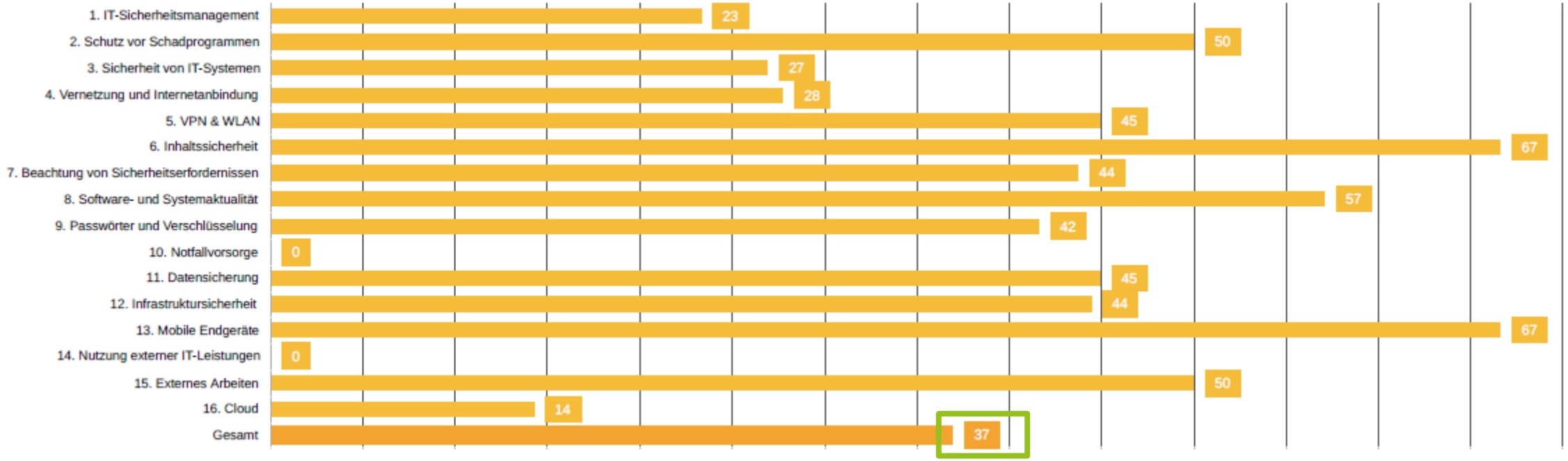
- 126 Fragen aus 16 Prüfgruppen
- Prüfung der technischen, menschlichen und organisatorischen Schutzmaßnahmen
- Ausführlicher Bericht mit Abschlusspräsentation
- konkrete und Maßnahmenempfehlungen
- Gemeinsame Priorisierung der Maßnahmen
- Vergleichender Benchmark aus über 1550 durchgeführten Audits

CYBER SECURITY CHECK

Professionelle Audit-Plattform

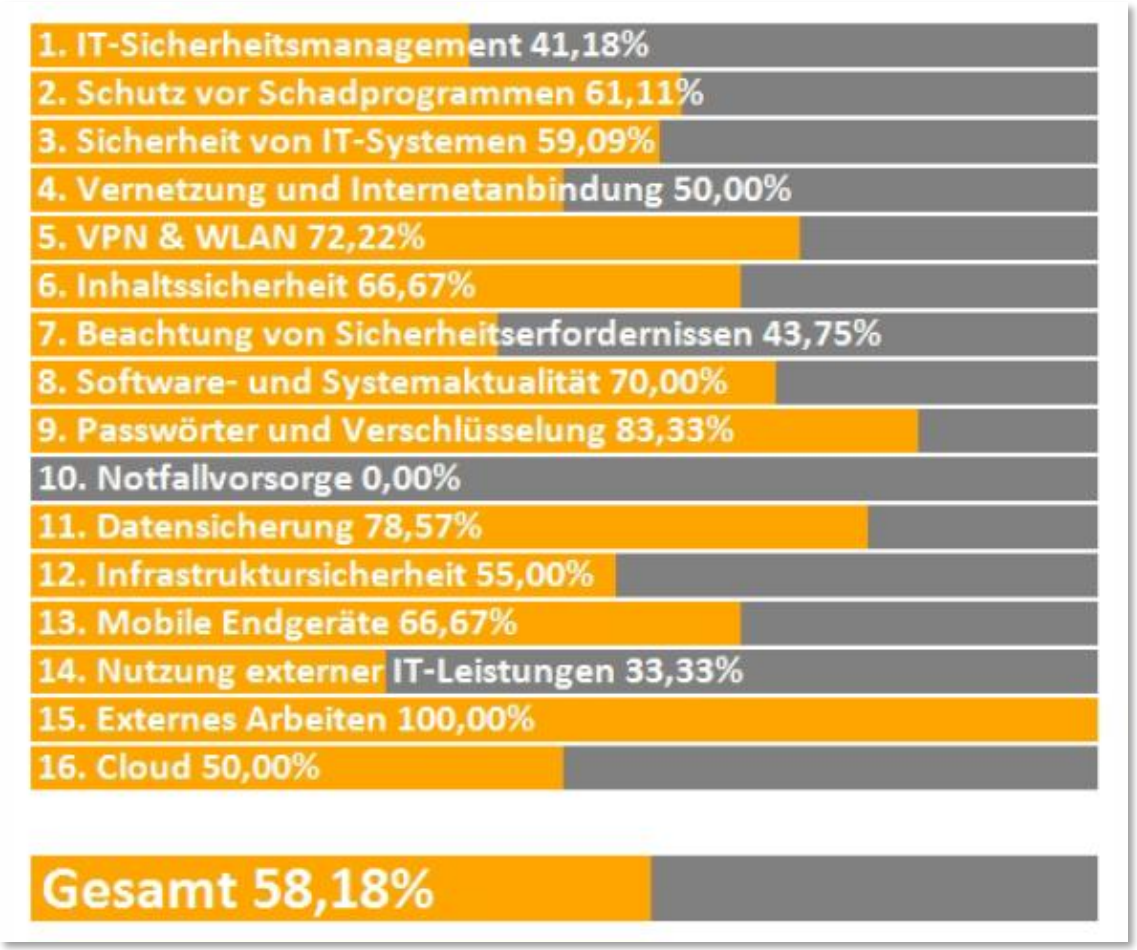


ERFÜLLUNGSGRAD NACH PRÜFGRUPPEN



CYBER SECURITY CHECK

Benchmark Ergebnisse und Maßnahmenempfehlungen



Probleme mit **hohem Risikograd** sind rot gekennzeichnet.
Probleme mit **mittlerem Risikograd** orange.
Probleme ohne Farbkodierung weisen einen **niedrigeren Risikograd** auf.

Kennung	Maßnahmenempfehlung	Prüfpunkt
A02	Erstellen eines Sicherheitskonzeptes	1.2
A03	Übersicht der gesetzlichen Anforderungen	1.3
A04	Ernennen eines IT-Sicherheitsbeauftragten	1.4
A07	Durchführen einer Schutzbedarfsanalyse	1.7
A10	Stellvertretungsregelungen definieren	1.10
A11	Passworthinterlegung regeln	1.11
A14	Bereitstellen von verschließbaren Behältnissen	1.14
A17	Erstellen einer Richtlinie zum Informationsaustausch	1.17
A18	Jährliche Revision des Sicherheitsstatus	1.18
B04	Dedizierter Virenschutz für E-Mail Server	2.4
B07	Handlungsanweisung zur Verhaltensweise bei Virenbefall	2.7
B08	Routineaufgabe zur regelmäßigen Überprüfung der Virenschutzprogramme	2.8
C10	Systemdokumentationen erstellen oder aktualisieren	3.10
D07	Netzwerk-Topologieplan erstellen	4.7
D08	Erstellen einer Sicherheitsrichtlinie für Router und Switches	4.8
E06	Erstellen einer WLAN-Sicherheitsrichtlinie	5.6
F03	Erstellung einer E-Mail-Richtlinie	6.3

06

CYBER SECURITY GOVERNANCE

- NOTFALLHANDBUCH
- IT-RICHTLINIEN

CYBER SECURITY GOVERNANCE

NOTFALLHANDBUCH

- Risikoanalyse
- Kritische Ressourcen und Systeme
- Rollen und Verantwortlichkeiten
- Backup- und Wiederherstellungsstrategien
- Kommunikationsplan

VERHALTEN BEI IT-NOTFÄLLEN

Ruhe bewahren & IT-Notfall melden
Lieber einmal mehr als einmal zu wenig anrufen!

IT-Notfallrufnummer:

Wer meldet?

Welches IT-System ist betroffen?

Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?

Wann ist das Ereignis eingetreten?

Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

Weitere Arbeit am IT-System einstellen	Beobachtungen dokumentieren	Maßnahmen nur nach Anweisung einleiten

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

CYBERSECURITY GOVERNANCE

IT-RICHTLINIEN UND PROZESSBESCHREIBUNGEN

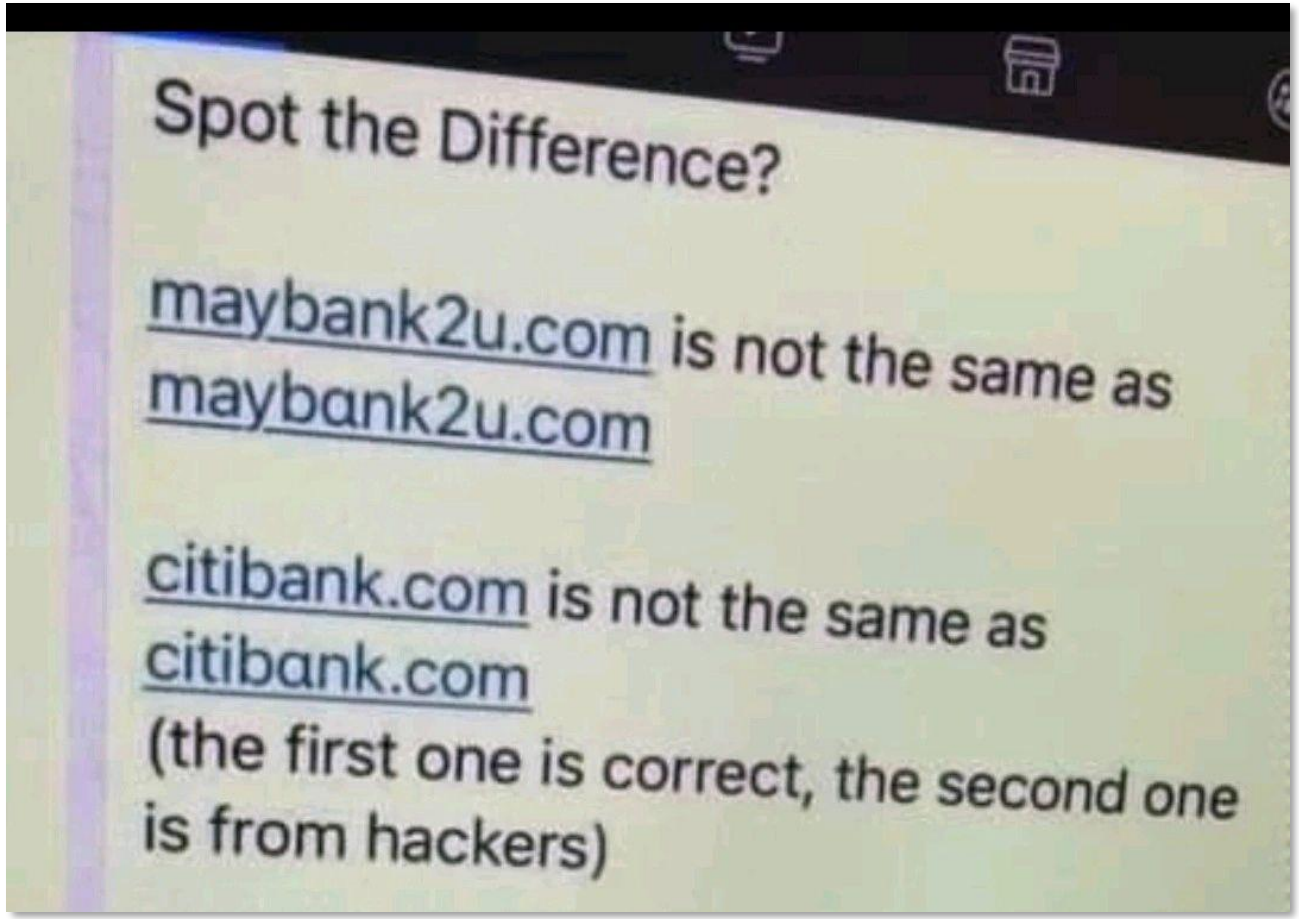
PASSION4IT

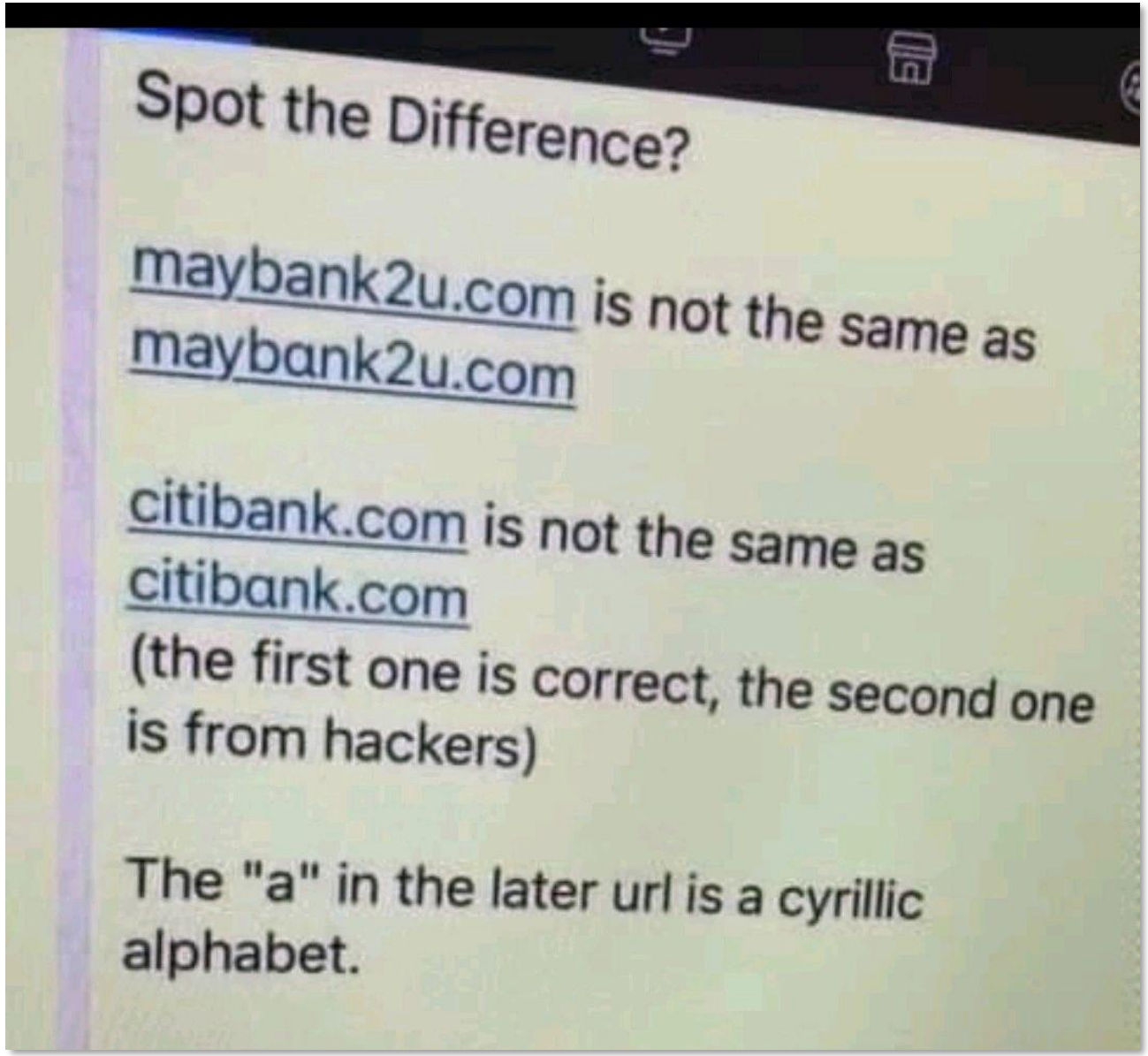
- Schutzbedarfsanalyse
- Umfassende Sicherheitsrichtlinien
- Datenschutz und Compliance
- Benutzerzugriff und -verwaltung
- Netzwerksicherheit

- Incident Response Plan
- Mobile Geräte und BYOD
- Sicherheitsbewusstsein und Schulung
- Organisatorische Zugriffsrechte
- Revisionierung

AWARENESSTRAININGS

AWARENESSTRAININGS


Spot the Difference?
maybank2u.com is not the same as
maybank2u.com
citibank.com is not the same as
citibank.com
(the first one is correct, the second one
is from hackers)


Spot the Difference?
maybank2u.com is not the same as
maybank2u.com
citibank.com is not the same as
citibank.com
(the first one is correct, the second one is from hackers)
The "a" in the later url is a cyrillic alphabet.


PASSION4IT