DER ENTSCHEIDENDE SCHRITT FÜR MEHR CYBERSICHERHEIT UND WETTBEWERBSFÄHIGKEIT

AKTUELLES ZU DATENSCHUTZ, TISAX®, ISO 27001 ...

KÄMMER CONSULTING

UND WAS DIE HUMAN FIREWALL DAMIT ZU TUN HAT ...

KÄMMER CONSULTING

KÄMMER CONSULTING GMBH

Seit mehr als 20 Jahren sind wir Berater, Trainer und Recruiter für unsere Kunden in den Regionen Braunschweig, Wolfsburg, Hannover und Magdeburg.

Portfolio

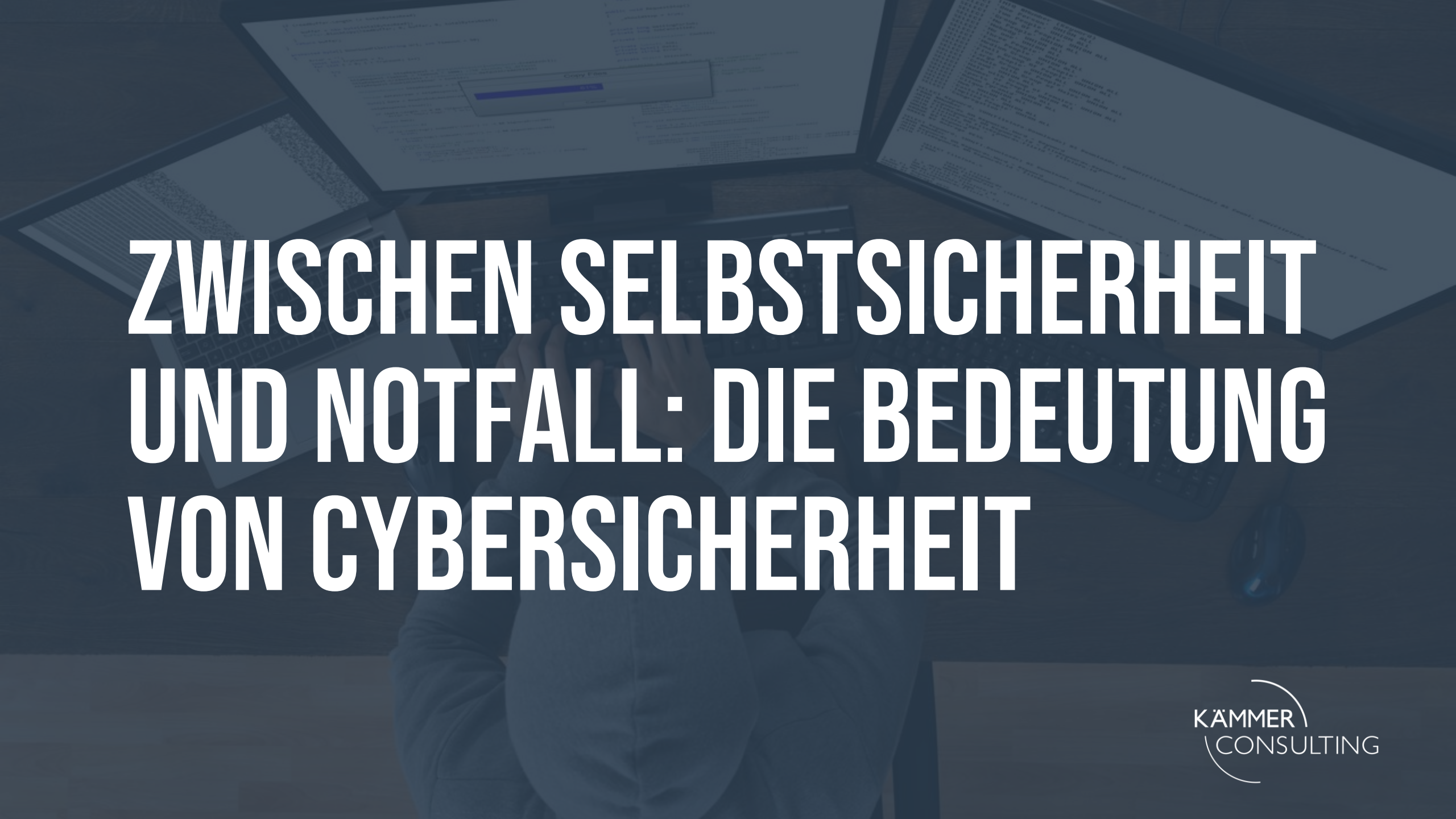
- Datenschutz (DSGVO)
- Informationssicherheit
  - ISO/IEC 27001
  - TISAX® | KRITIS |DIN 27076
- Qualitätsmanagement
  - ISO 9001
- Seminarmanagement

Allianz für Cyber-Sicherheit
Teilnehmer

ALLIANZ FÜR DIE REGION

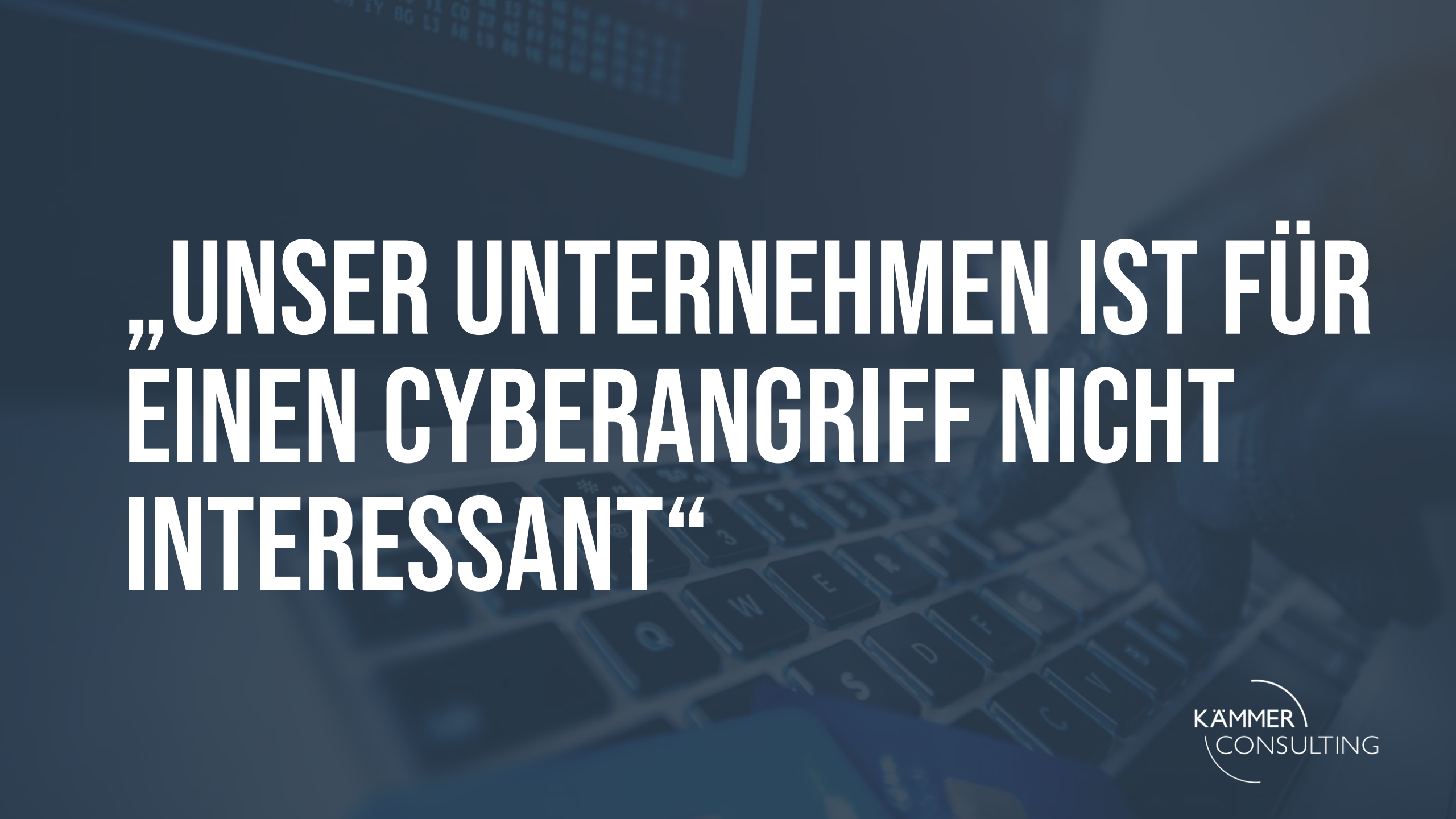
BvD e.V.
MITGLIED

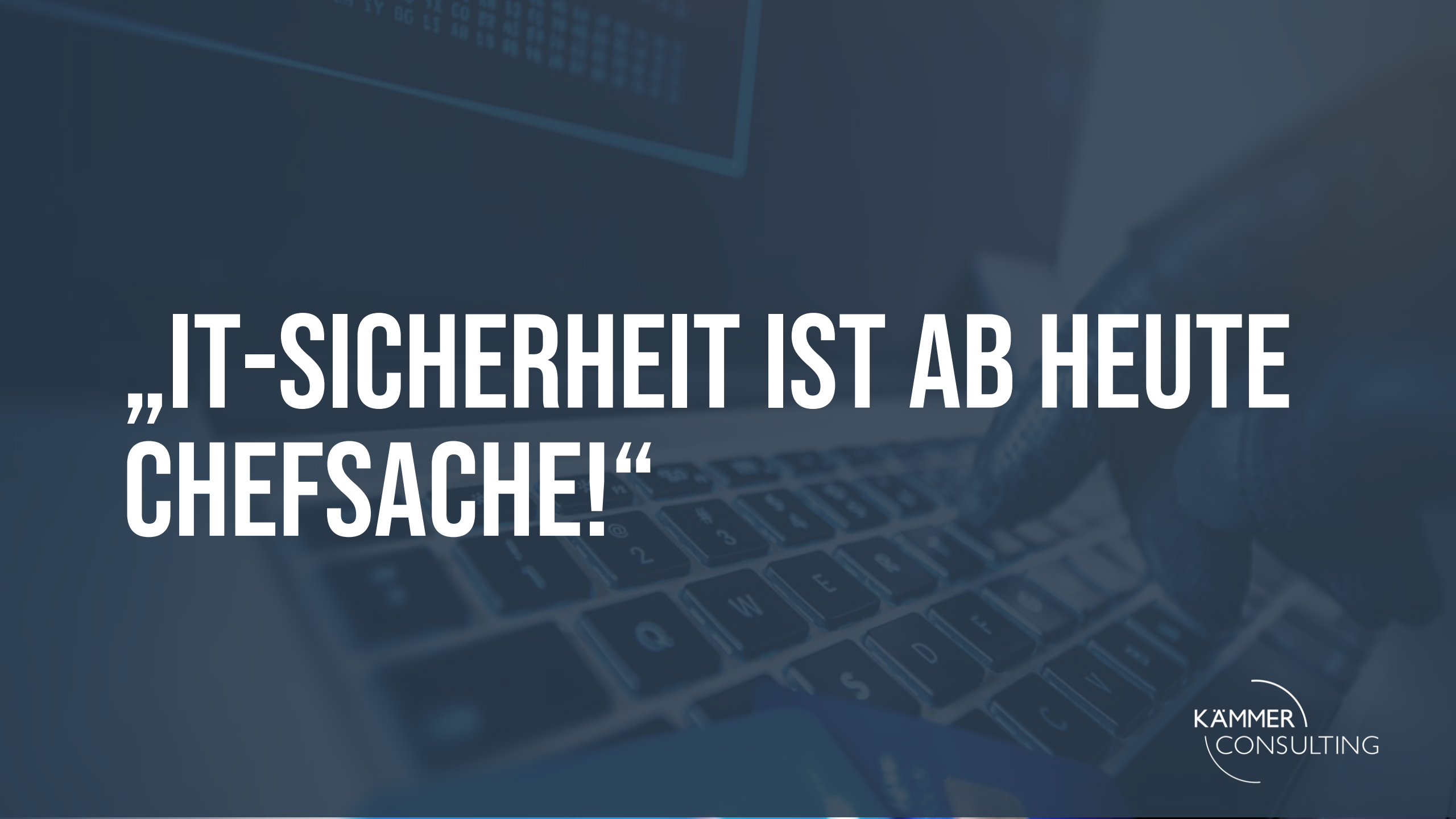
AGV
Arbeitgeberverband Region Braunschweig e.V.

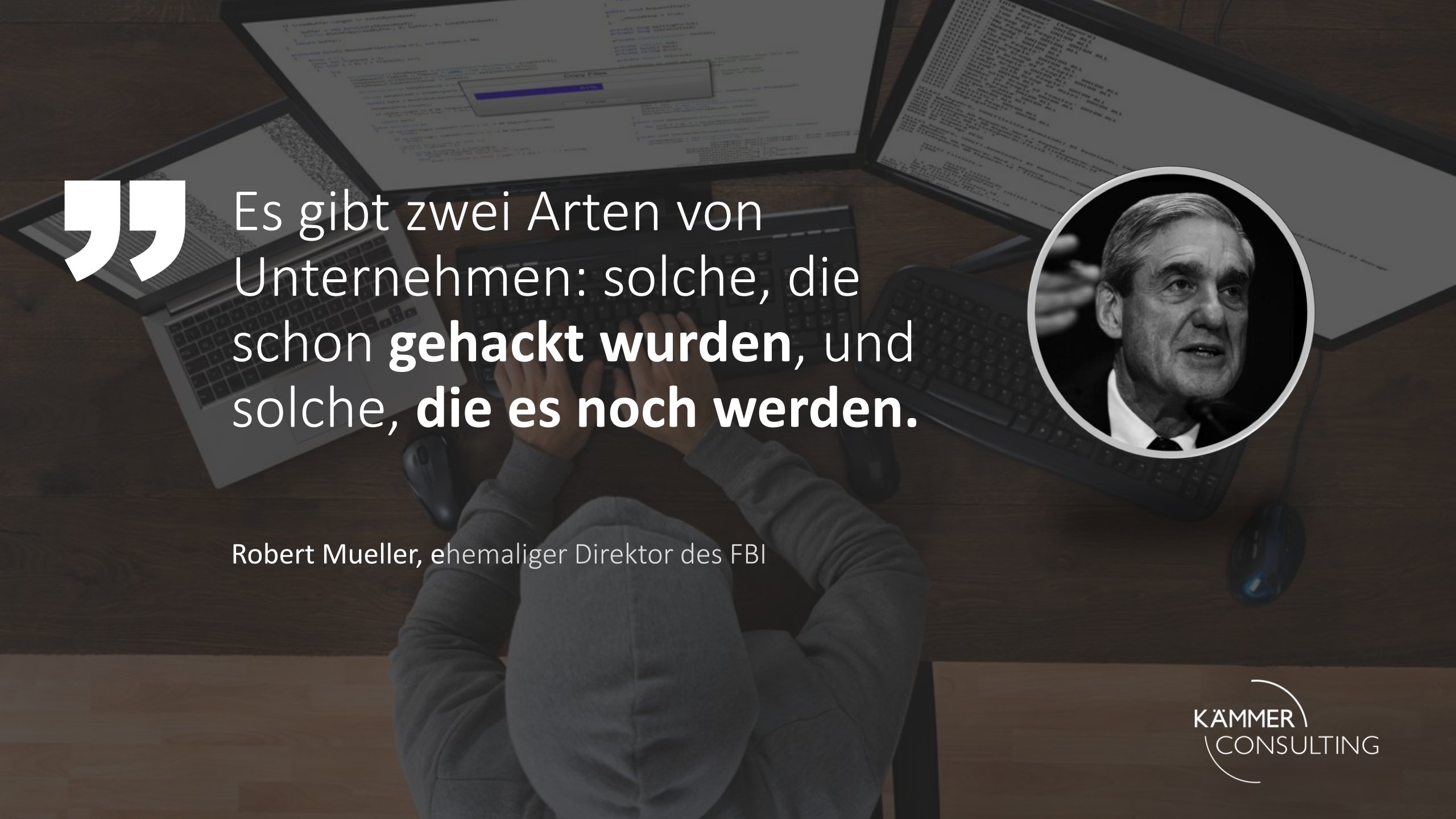


ZWISCHEN SELBSTSICHERHEIT UND NOTFALL: DIE BEDEUTUNG VON CYBERSICHERHEIT

KÄMMER CONSULTING


„UNSER UNTERNEHMEN IST FÜR EINEN CYBERANGRIFF NICHT INTERESSANT“
KÄMMER
CONSULTING


„IT-SICHERHEIT IST AB HEUTE CHEFSACHE!“
KÄMMER
CONSULTING



Es gibt zwei Arten von Unternehmen: solche, die schon **gehackt wurden**, und solche, **die es noch werden.**

Robert Mueller, ehemaliger Direktor des FBI

KÄMMER CONSULTING

Die Lage der IT-Sicherheit in Deutschland 2023 im Überblick

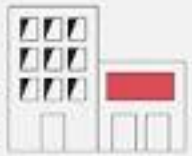
Ransomware

ist weiterhin die größte Bedrohung.

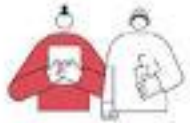
2 **Ransomware-Angriffe** auf Kommunalverwaltungen oder kommunale Betriebe wurden durchschnittlich pro Monat bekannt.

68 erfolgreiche **Ransomware-Angriffe auf Unternehmen** wurden bekannt.

15 davon richteten sich gegen **IT-Dienstleister.**



Top 3-Bedrohungen je Zielgruppe:

Gesellschaft	Wirtschaft	Staat und Verwaltung
		
Identitätsdiebstahl Sextortion Phishing	**Ransomware** Abhängigkeit innerhalb der IT-Supply-Chain Schwachstellen, offene oder falsch konfigurierte Online-Server	**Ransomware** APT Schwachstellen, offene oder falsch konfigurierte Online-Server

Rund **21.000** **infizierte Systeme** wurden täglich im Berichtszeitraum erkannt und vom BSI an die deutschen Provider gemeldet.

2.000

Mehr als **Schwachstellen** in Software-Produkten (**15 % davon kritisch**) wurden im Berichtszeitraum durchschnittlich im Monat bekannt. Das ist ein **Zuwachs von 24 %.**

Eine Viertelmillion

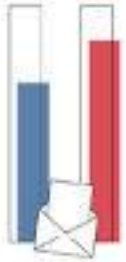
neue **Schadprogramm-Varianten** wurden durchschnittlich an jedem Tag im Berichtszeitraum gefunden.

Durchschnittlich rund **775** **E-Mails mit Schadprogrammen** wurden an jedem Tag im Berichtszeitraum in deutschen Regierungsnetzen abgefangen.

370 **Webseiten** wurden im Durchschnitt an jedem Tag des Berichtszeitraums für den Zugriff aus den Regierungsnetzen gesperrt. **Der Grund:** Die Seiten enthielten Schadprogramme.

66%

aller **Spam-Mails** im Berichtszeitraum waren Cyberangriffe: 34% Erpressungsmails, 32% Betrugsmails



84%

aller betrügerischen E-Mails waren **Phishing-E-Mails** zur Erbeutung von Authentisierungsdaten, meist bei Banken und Sparkassen.

6.220 2022
5.100 2021

7.120

Teilnehmer hatte die **Allianz für Cyber-Sicherheit** im Jahr 2023

Deutschland **Digital·Sicher·BSI·**

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

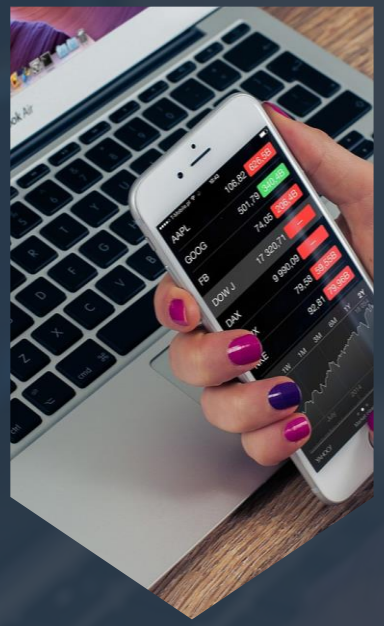
KÄMMER CONSULTING

CYBERRÄUME

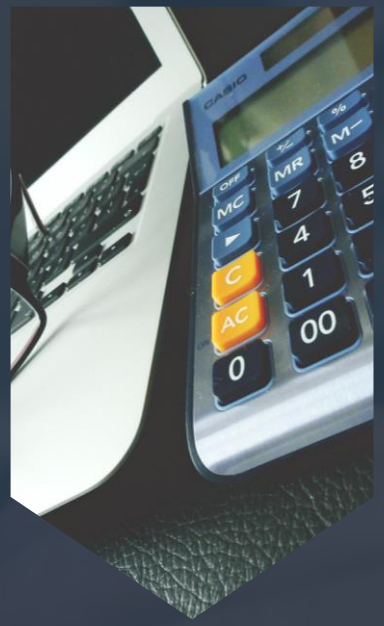
INDUSTRIE

SOZIALE NETZWERKE

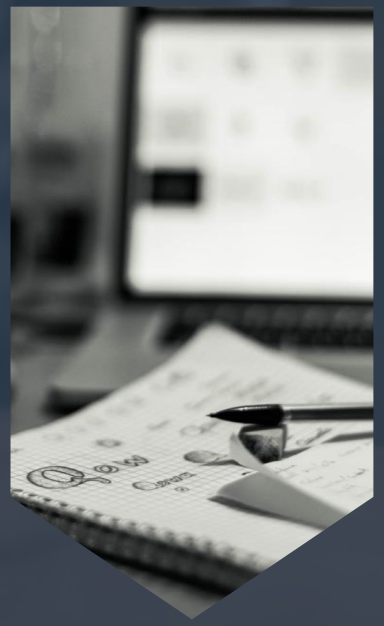
DATENSPEICHER



MARKTPLATZ

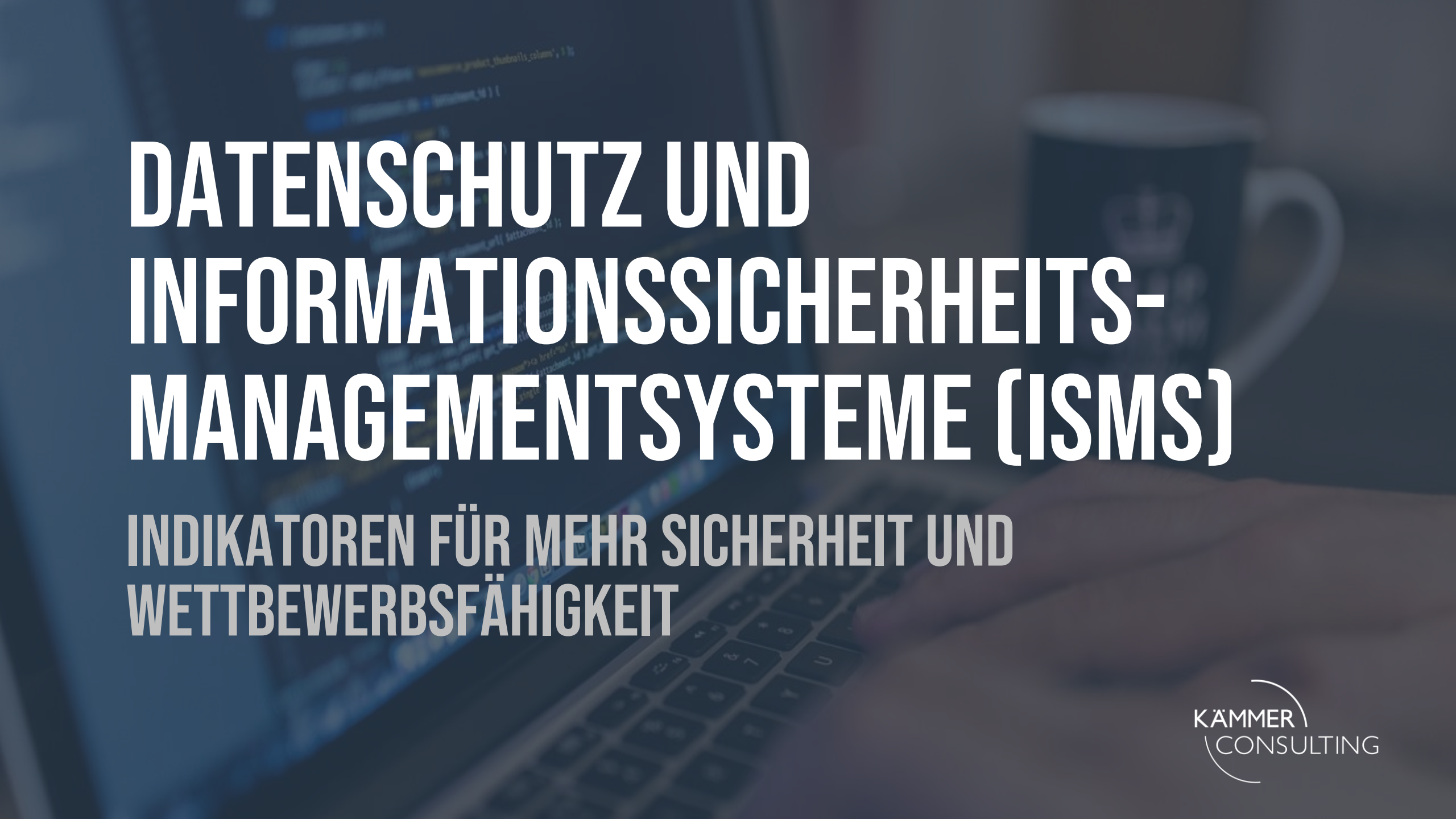


BANKGESCHÄFTE



POLITIK

KÄMMER CONSULTING



DATENSCHUTZ UND INFORMATIONSSICHERHEITS-MANAGEMENTSYSTEME (ISMS)

INDIKATOREN FÜR MEHR SICHERHEIT UND WETTBEWERBSFÄHIGKEIT

KÄMMER CONSULTING


IMPLEMENTIEREN UND LEBEN!!!
KÄMMER
CONSULTING

WAS IST EIN INFORMATIONSSICHERHEITS-MANAGEMENTSYSTEM (ISMS)?

KÄMMER CONSULTING

WAS IST EIN ISMS ?

EIN INFORMATIONSSICHERHEITSMANAGEMENTSYSTEM IST DIE AUFSTELLUNG VON VERFAHREN UND REGELN INNERHALB EINER ORGANISATION, DIE DAZU DIENEN, DIE INFORMATIONSSICHERHEIT DAUERHAFT ZU DEFINIEREN, ZU STEUERN, ZU KONTROLLIEREN, AUFRECHTZUERHALTEN UND FORTLAUFEND ZU VERBESSERN.

Quelle: Wikipedia

KÄMMER CONSULTING

ISMS – 3 SCHUTZZIELE

- VERTRAULICHKEIT (Confidentiality)
  ZUGRIFF AUF DIE INFORMATIONEN IST NUR DEN AUTORISIERTEN PERSONEN MÖGLICH.
- VERFÜGBARKEIT (Availability)
  INFORMATIONEN SIND ZU DEN ERFORDELRICHEN ZEITPUNKTEN VERFÜGBAR.
- INTEGRITÄT (Integrity)
  INFORMATIONEN SIND VERLÄSSLICH, KÖNNEN NICHT MANIPULIERT WERDEN.

KÄMMER CONSULTING

BEISPIELE ISMS

- ISO 27001:2022
  Internationaler Standard für Informationssicherheitsmanagementsysteme (ISMS). Der Standard bietet Informationen zur Planung, Implementierung, Überwachung und Optimierung von Informationen.
- TISAX®
  TISAX ® (Trusted Information Security Assessment Exchange), Prüf- und Austauschmechanismus, nach dem Standard VDA-ISA, der von der ENX Association entwickelt und vom VDA 2017 herausgegeben wurde und vom ISO/IEC 27001-Standard abgeleitet wurde.
- BSI-GRUNDSCHUTZ
- DIN 27076
- ISIS12

KÄMMER CONSULTING

VORTEILE VON DS UND ISMS

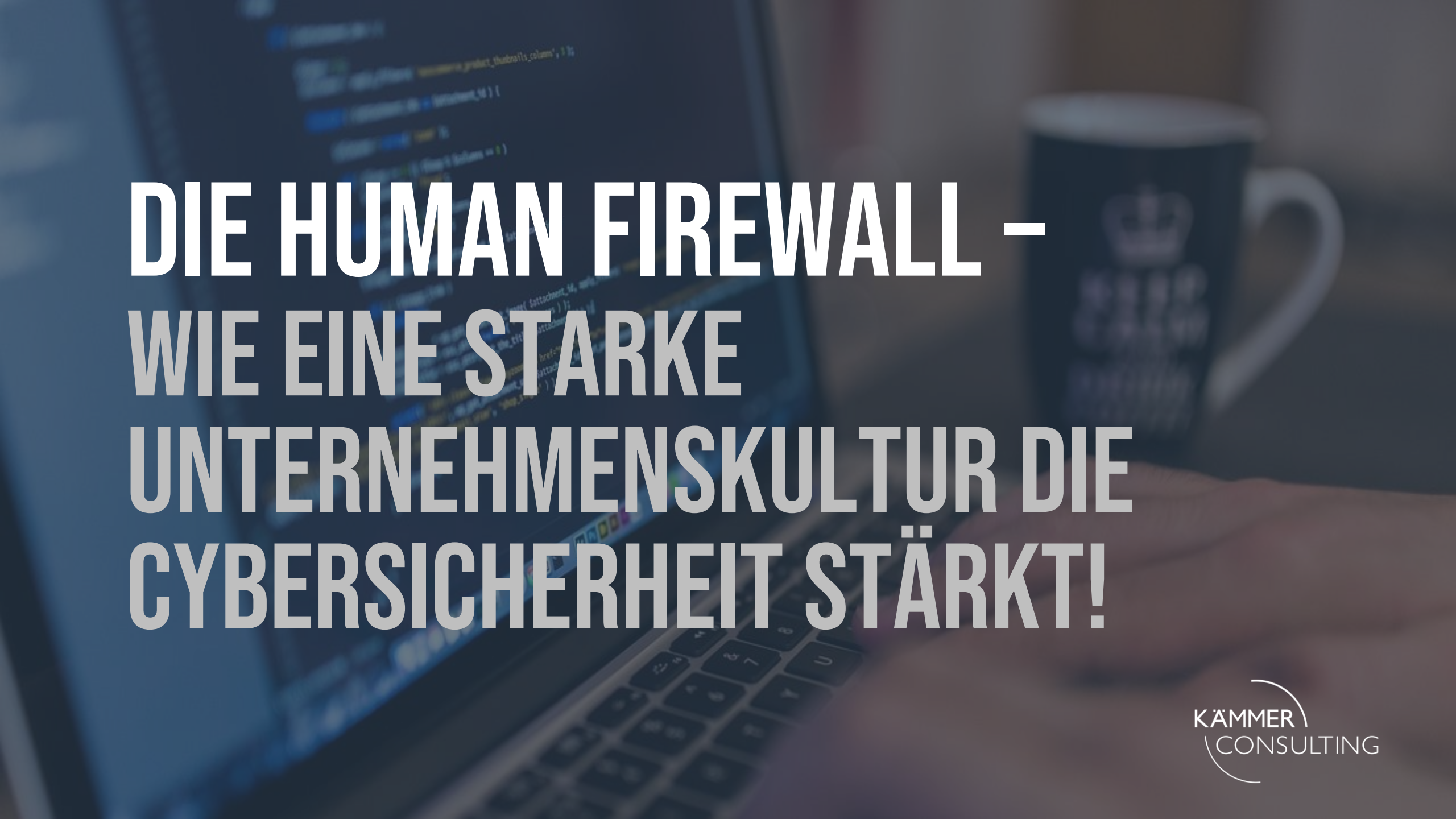
1. SCHUTZ VOR CYBERANGRIFFEN
2. EINHALTUNG VON RECHTLICHEN UND REGULATORISCHEN ANFORDERUNGEN
3. UNTERNEHMENSRUF UND KUNDENVERTRAUEN
4. RISIKOMANAGEMENT
5. WETTBEWERBSVORTEIL

KÄMMER CONSULTING

MESSBARE VORTEILE ...

- 3,86 Millionen US-Dollar durchschnittliche Kosten einer Datenschutzverletzung
(Quelle: Ponemon Institute)
- Return on Investment (ROI) von 2,7 Millionen US-Dollar innerhalb 3 Jahren bei Unternehmen, die in Datenschutz investierten und ein ISMS implementierten. Dieser ROI ergab sich aus Kosteneinsparungen, Risikominderung und dem Aufbau von Kundenvertrauen.
(Quelle: Forrester Research)
- Zertifizierung nach ISO 27001 erhöht die Chancen, bei Ausschreibungen erfolgreich zu sein, um 23%.
(Quelle: BSI)

KÄMMER CONSULTING



DIE HUMAN FIREWALL – WIE EINE STARKE UNTERNEHMENSKULTUR DIE CYBERSICHERHEIT STÄRKT!

KÄMMER CONSULTING

HUMAN FIREWALL - WICHTIG?

- 95 % menschliche Faktoren als grösste Schwachstelle
  (IBM X-Force Threat Intelligence Index 2020)
- 47% der Datensicherheitsverletzungen aufgrund menschlichem Fehlverhalten
  (Ponemon Institute von 2020)
- 50% Schadensreduzierung bei Sicherheitsverletzungen mit einer guten Unternehmenskultur
  (Accenture aus dem Jahr 2020)

KÄMMER CONSULTING


FEHLER
VERBOTEN!
CRITICAL ERROR
SYSTEM
HACKED
CRITICAL ERROR
SYSTEM
HACKED

Sometimes you win,

sometimes you ~~lose~~

learn

VORTEILE GUTER FEHLERKULTUR

KOSTENERSPARNIS

- Laut einer Studie von **Gartner** aus dem Jahr 2019 können Unternehmen, die eine offene Fehlerkultur etablieren, bis zu 30% ihrer Sicherheitskosten einsparen.

KÄMMER CONSULTING

VORTEILE GUTER FEHLERKULTUR

BESSERE FINANZIELLE ERGEBNISSE UND INNOVATION

- **Deloitte**'s High-Impact Leadership-Studie, in der Führungskräfte weltweit befragt wurden, zeigte, dass Unternehmen mit einer positiven Fehlerkultur, besseren Innovationsfähigkeiten und höheren Anpassungsfähigkeiten an Veränderungen aufweisen und auch bessere finanzielle Ergebnisse erzielten.

KÄMMER CONSULTING

DIE NEUE ISO/IEC 27001:2022

ÜBERGANGSFRIST 3 JAHRE, DAS HEIßT, ALLE ZERTIFIKATE MÜSSEN BIS ZUM 31. OKTOBER 2025 UMGESTELLT SEIN.

JEDES AUDIT ZUR ERSTZERTIFIZIERUNG UND REZERTIFIZIERUNG, DAS AB DEM 01.05.2024 BEGINNT, MUSS NACH DER NEUEN VERSION 27001:2022 DURCHGEFÜHRT WERDEN.

KÄMMER CONSULTING

NEU: TITEL UND STRUKTUR

- „INFORMATION SECURITY, CYBERSECURITY AND PRIVACY PROTECTION“
- HARMONIZED STRUCTURE (HS) – ALS NACHFOLGE DER HIGH LEVEL STRUCTURE (HLS)

KÄMMER CONSULTING

ANHANG A (ANNEX A)

- ALT: 114 MAßNAHMEN IN 14 ABSCHNITTEN, 35 KATEGORIEN
- NEU: 93 MAßNAHMEN MIT 4 HAUPT-KATEGORIEN

•ORGANISATORISCHE MAßNAHMEN (37 MAßNAHMEN)

•PERSONENBEZOGENE MAßNAHMEN (8 MAßNAHMEN)

•PHYSISCHE MAßNAHMEN (14 MAßNAHMEN)

•TECHNISCHE MAßNAHMEN (34 MAßNAHMEN)

KÄMMER CONSULTING

FAKTEN ISO 27001:2022

- DIE NEUEN 11 MAßNAHMEN WURDEN UNTER ANDEREM ERGÄNZT UM
- CLOUD-SICHERHEIT,
- THREAT INTELLIGENCE
- UND DATENSCHUTZVERWANDTE THEMEN

KÄMMER CONSULTING

FAKTEN ISO 27001:2022

- > A.5.7 THREAT INTELLIGENCE
- > A.5.23 INFORMATION SECURITY FOR USE OF CLOUD SERVICES
- > A.5.30 ICT READINESS FOR BUSINESS CONTINUITY
- > A.7.4 PHYSICAL SECURITY MONITORING
- > A.8.9 CONFIGURATION MANAGEMENT
- > A.8.10 INFORMATION DELETION
- > A.8.11 DATA MASKING
- > A.8.12 DATA LEAKAGE PREVENTION
- > A.8.16 MONITORING ACTIVITIES
- > A.8.23 WEB FILTERING
- > A.8.28 SECURE CODING

KÄMMER CONSULTING

5 ATTRIBUTE JE MASSNAHME

- :
- CONTROL TYPE (PREVENTIVE, DETECTIVE, CORRECTIVE
- INFORMATION SECURITY PROPERTIES (CONFIDENTIALITY, INTEGRITY AND AVAILABILITY)
- CYBERSECURITY CONCEPTS (IDENTIFY, PROTECT, DETECT, RESPOND AND RECOVER)
- OPERATIONAL CAPABILITIES
- SECURITY DOMAINS

KÄMMER CONSULTING

NEU: TISAX® 6

Information Security Assessment

VDA | Verband der Automobilindustrie

ISA provides the basis for
- a self-assessment to determine the state of information security in an organization (e.g. company)
- audits performed by internal departments (e.g. Internal Audit, Information Security)
- TISAX® Assessments (Trusted Information Security Assessment Exchange, https://enx.com/tisax/)

ISA consists of several tabs, the content and function of which are explained in the tab "Definitions". The corresponding actual requirements can be found in the tabs "Information Security", "Prototype Protection" and "Data Protection".

We recommend gaining an overview of the individual ISA tabs by using the "Definitions" tab.
Then, commence with the "Information Security" tab.

The authors of this document wish you every success.

Publisher: VERBAND DER AUTOMOBILINDUSTRIE e. V. (VDA, German Association of the Automotive Industry), Behrenstr. 35, 10117 Berlin;
www.vda.de

Note: For better guidance, the worksheets are color-coded as follows:

- Cover
- Information/explanations
- Questionnaires and requirements catalogs
- Results overviews

This version is the first release version of ISA Version 6.
ISA Version 6 will become applicable to TISAX Assessments ordered after April 1st 2024.
TISAX Assessments ordered before April 1st 2024 will still be conducted following ISA 5

Quelle: ENX

KÄMMER CONSULTING

UMSTELLUNG AUF TISAX® 6

- 1. APRIL 2024 STICHTAG, AN DEM TISAX 6 WIRKSAM WIRD.
- ALTE ABGESCHLOSSENE PRÜFUNGEN BEHALTEN IHRE GÜLTIGKEIT. WENN IHRE TISAX-LABELS NICHT ABLAUFEN, BESTEHT KEIN GRUND ZU EINER NEUPRÜFUNG.
- NEUE TISAX-ASSESSMENTS, DIE BIS 31. MÄRZ 2024 BEAUFTRAGT WERDEN, KÖNNEN NACH DER ALTEN VERSION DURCHGEFÜHRT WERDEN.

KÄMMER CONSULTING

Quelle: ENX

WAS IST NEU BEI TISAX® 6?

- STÄRKERER FOKUS AUF IT- UND OT-VERFÜGBARKEIT VON PRODUKTIONS-LIEFERANTEN
- FÜHRENDE SPRACHE IST JETZT ENGLISCH
- HINZUFÜGUNG VON WEITEREN IMPLEMENTIERUNGSANLEITUNGEN

Quelle: ENX

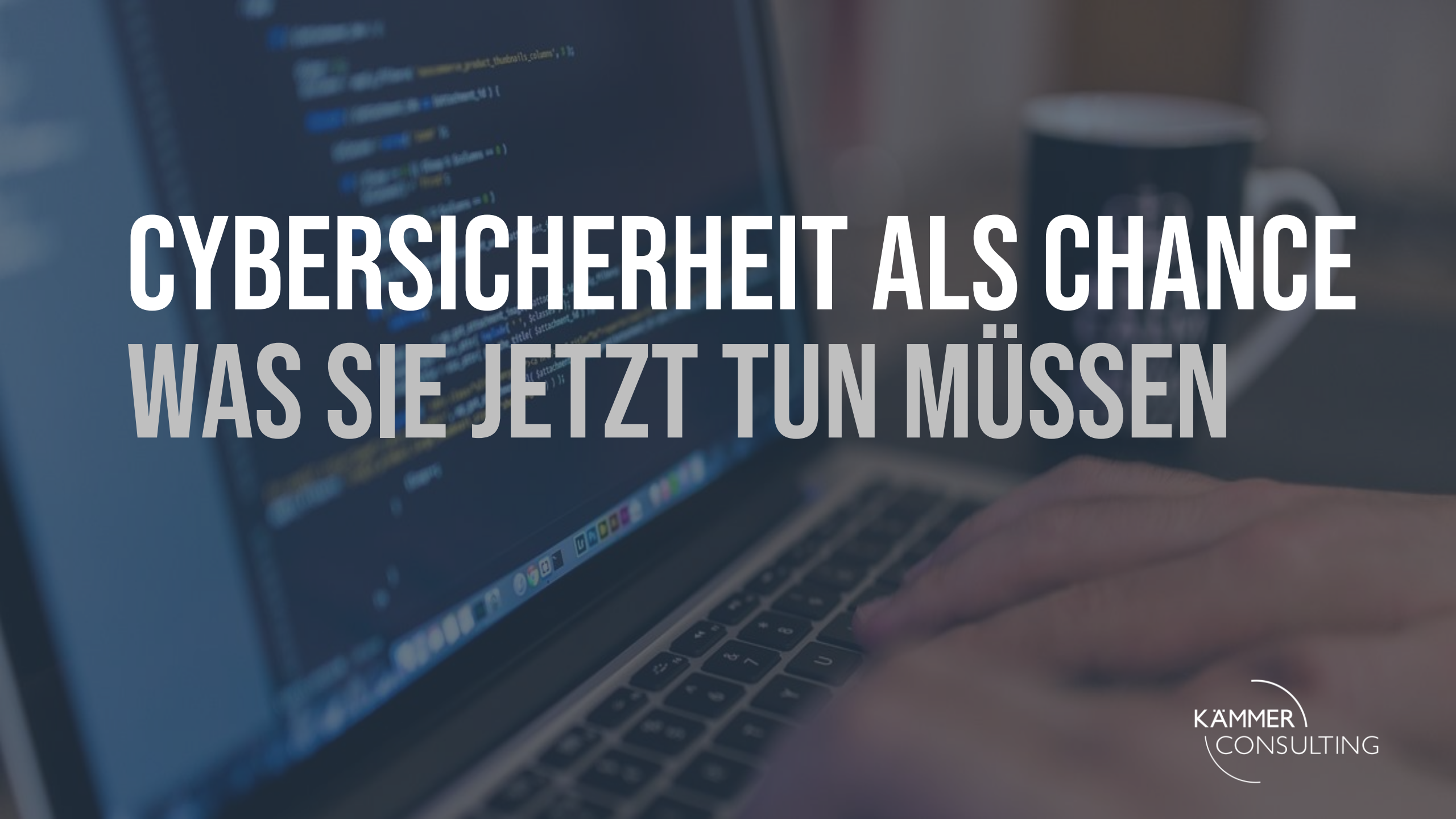
KÄMMER CONSULTING

WAS IST NEU BEI TISAX® 6?

- NEUE VERWEISE AUF ISO/IEC 27001:2022, BSI-GRUNDSCHUTZ UND NIST CYBER SECURITY FRAMEWORK VERSION 1.1
- VOLLSTÄNDIG ÜBERARBEITETER DATENSCHUTZKATALOG
- WEITERE KONTINUIERLICHE VERBESSERUNG UND PFLEGE.

Quelle: ENX

KÄMMER CONSULTING



CYBERSICHERHEIT ALS CHANCE
WAS SIE JETZT TUN MÜSSEN

KÄMMER CONSULTING

WAS SIE JETZT TUN MÜSSEN

1. Etablieren Sie Cybersicherheit im Unternehmen und machen es zu einem strategischen Wettbewerbsvorteil
2. Verstehen Sie, dass Cybersicherheit nicht länger als notwendiges Übel betrachtet werden sollte, sondern als Chance, Ihre Reputation zu stärken, das Vertrauen Ihrer Kunden zu gewinnen und Ihre Wettbewerbsposition zu festigen.

KÄMMER CONSULTING

WAS SIE JETZT TUN MÜSSEN

3. Setzen Sie auf eine starke Unternehmenskultur, in der jeder Mitarbeiter zu einer 'Human Firewall' wird.
4. Investieren Sie in Schulungen und Ressourcen, um das Bewusstsein für Cybersicherheit zu stärken und eine sichere Fehlerkultur zu etablieren.
5. Nutzen Sie Datenschutz und Informationssicherheits-managementsysteme – um die Cybersicherheit und Kundenanforderungen zu erfüllen

KÄMMER CONSULTING

WAS SIE JETZT TUN MÜSSEN

6. Bleiben Sie immer auf dem neuesten Stand der Tricks und Tools, die Angreifer nutzen. Nutzen Sie die Erkenntnisse dieser Fachkonferenz, um effektive Schutzmaßnahmen zu implementieren und Ihren Cyberschutz kontinuierlich zu verbessern.

KÄMMER CONSULTING

AND FINALLY ...

7. Machen Sie Cybersicherheit zur Chefsache und starten Sie bereits heute, um Ihr Unternehmen vor Bedrohungen zu schützen.

KÄMMER CONSULTING

VIELEN DANK

ANDREAS STAMMHAMMER

AXEL VOGELSANG

KÄMMER CONSULTING