HUMAN FIREWALL – KEINE VERBRANNTEN FINGER MEHR

IHR UPDATE ZU MEHR CYBERSICHERHEIT

KÄMMER CONSULTING

ANDREAS STAMMHAMMER

LEITER VERTRIEB | INFORMATIONSSICHERHEITSBERATER

**(ISO/IEC 27001 IMPLEMENTER, ICO ISMS FOUNDATION ACCORDING TO TISAX,
DEKRA ZERT. DATENSCHUTZBEAUFTRAGTER)**

KÄMMER CONSULTING GMBH

FON +49 531 702249 – 42
MOBIL +49 152 5136 3456
MAIL: A.STAMMHAMMER@KAEMMER-CONSULTING.DE

KÄMMER CONSULTING

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®
- Qualitätsmanagement
  - ISO 9001
- Seminarmanagement

Allianz für Cyber-Sicherheit
Teilnehmer

ALLIANZ FÜR DIE REGION

BvD e.V.
MITGLIED

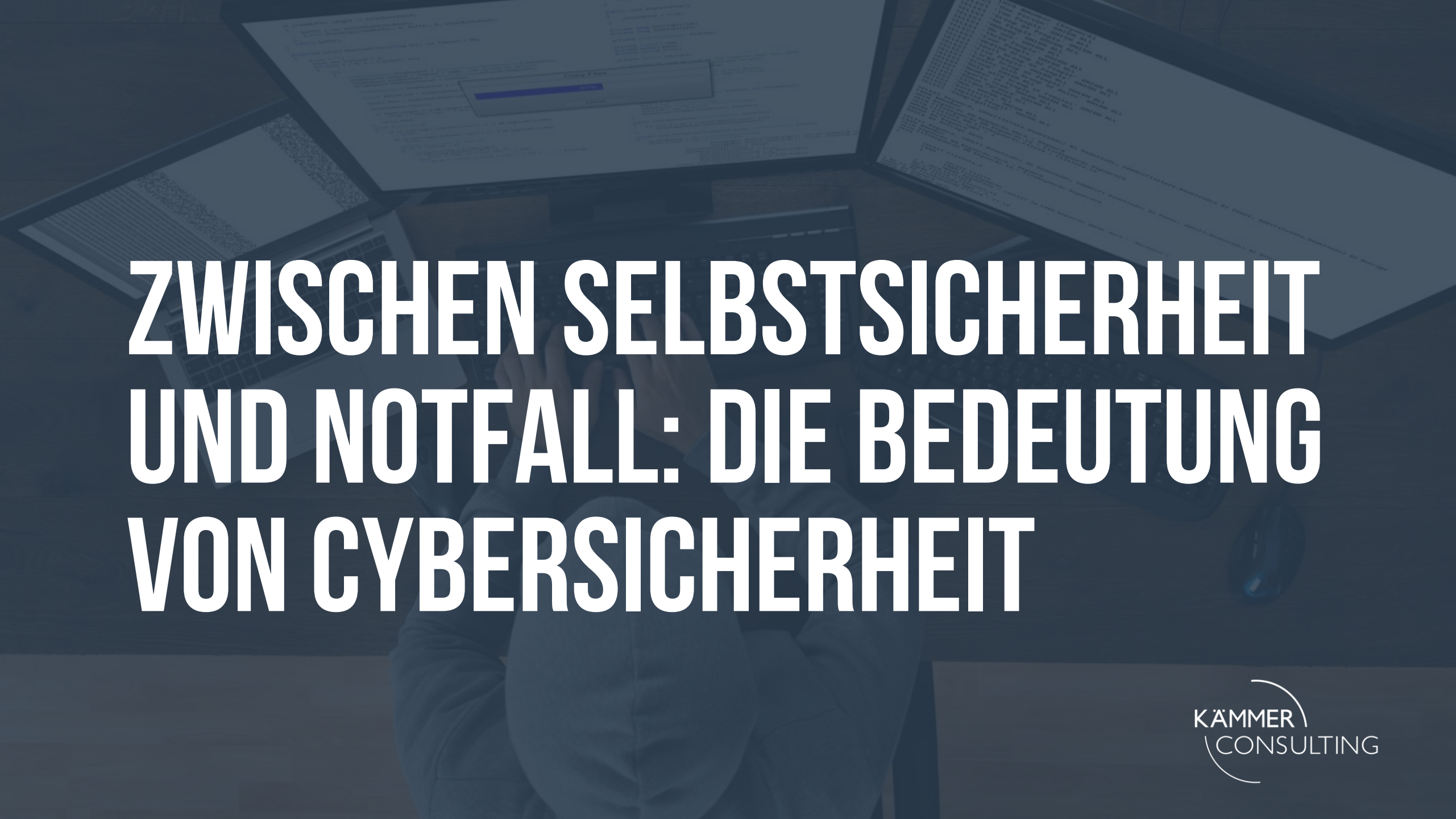
AGV Arbeitgeberverband Region Braunschweig e.V.

AGENDA

Human Firewall – Keine verbrannten Finger mehr

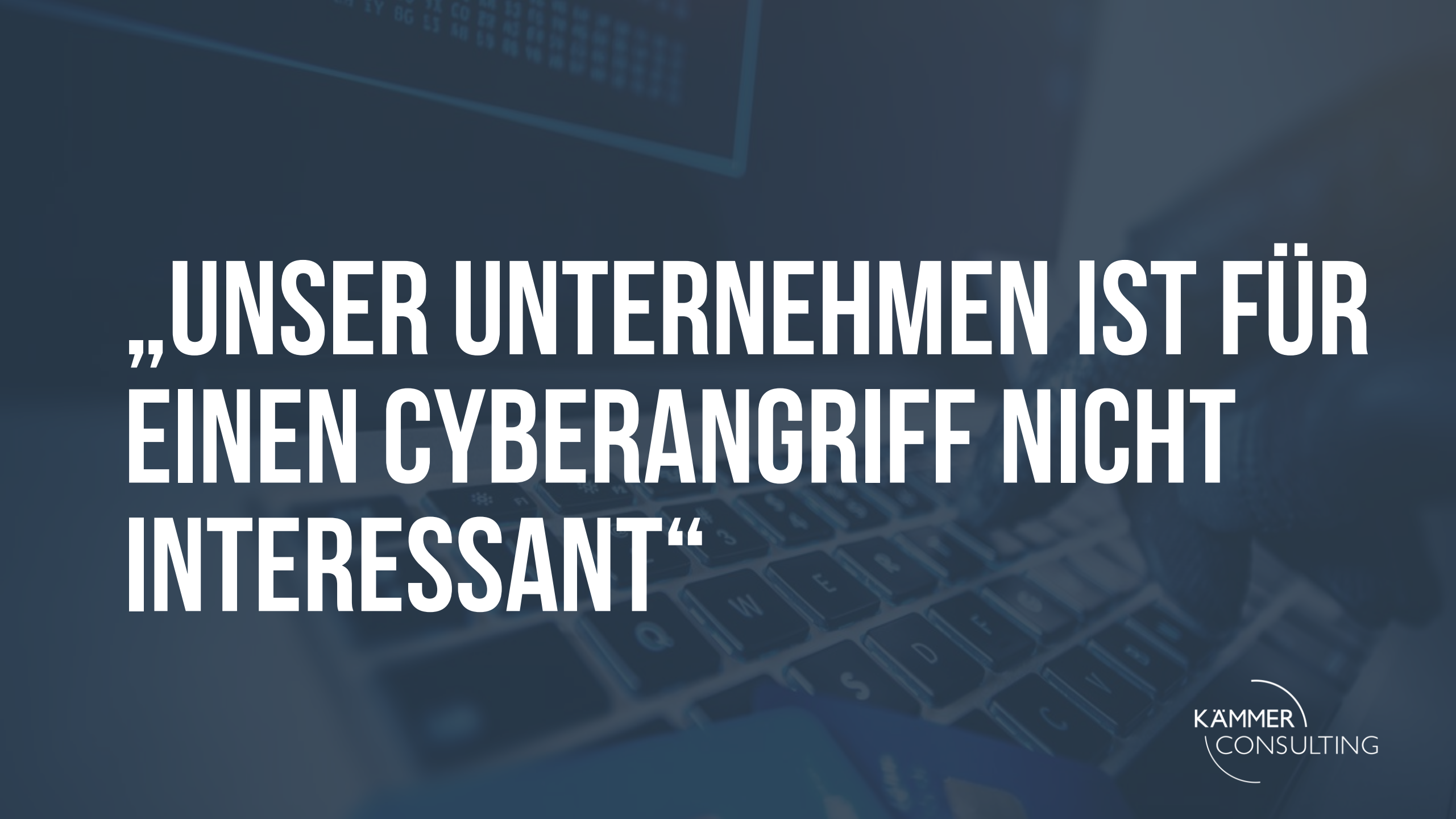
Ihr Update zu mehr Cybersicherheit

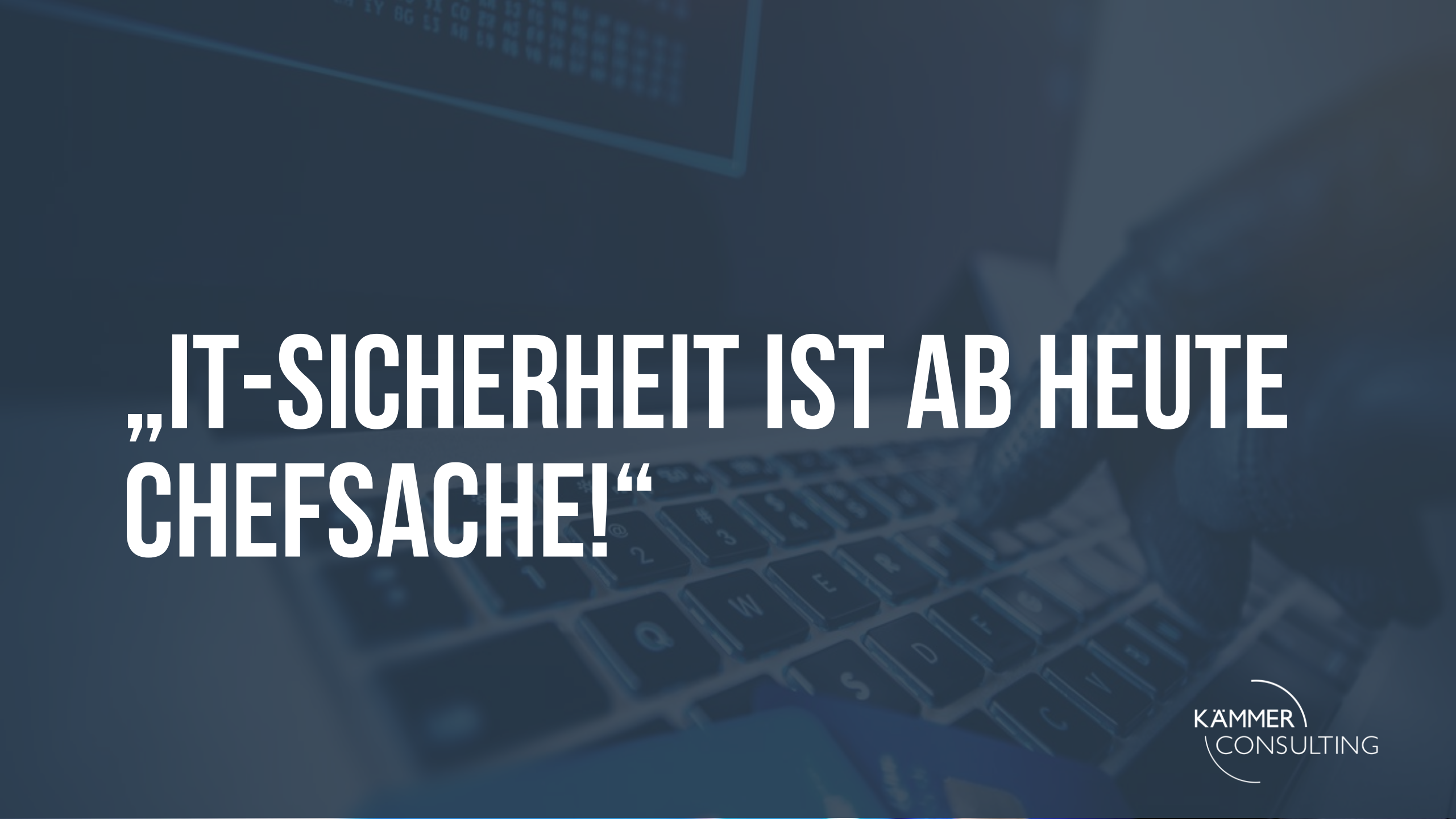
- Zwischen Selbstsicherheit und Notfall -
  Die Bedeutung von Cybersicherheit
- Die „Human“ Firewall –
  Wie eine starke Unternehmenskultur die Cybersicherheit stärkt
- Datenschutz und Informationssicherheits-managementsysteme –
  Indikatoren für mehr Sicherheit und Wettbewerbsfähigkeit
- Trends und Tricks der Angreifer:
  Wie bleiben Sie einen Schritt voraus?
- Cybersicherheit als Chance –
  Was Sie jetzt tun müssen

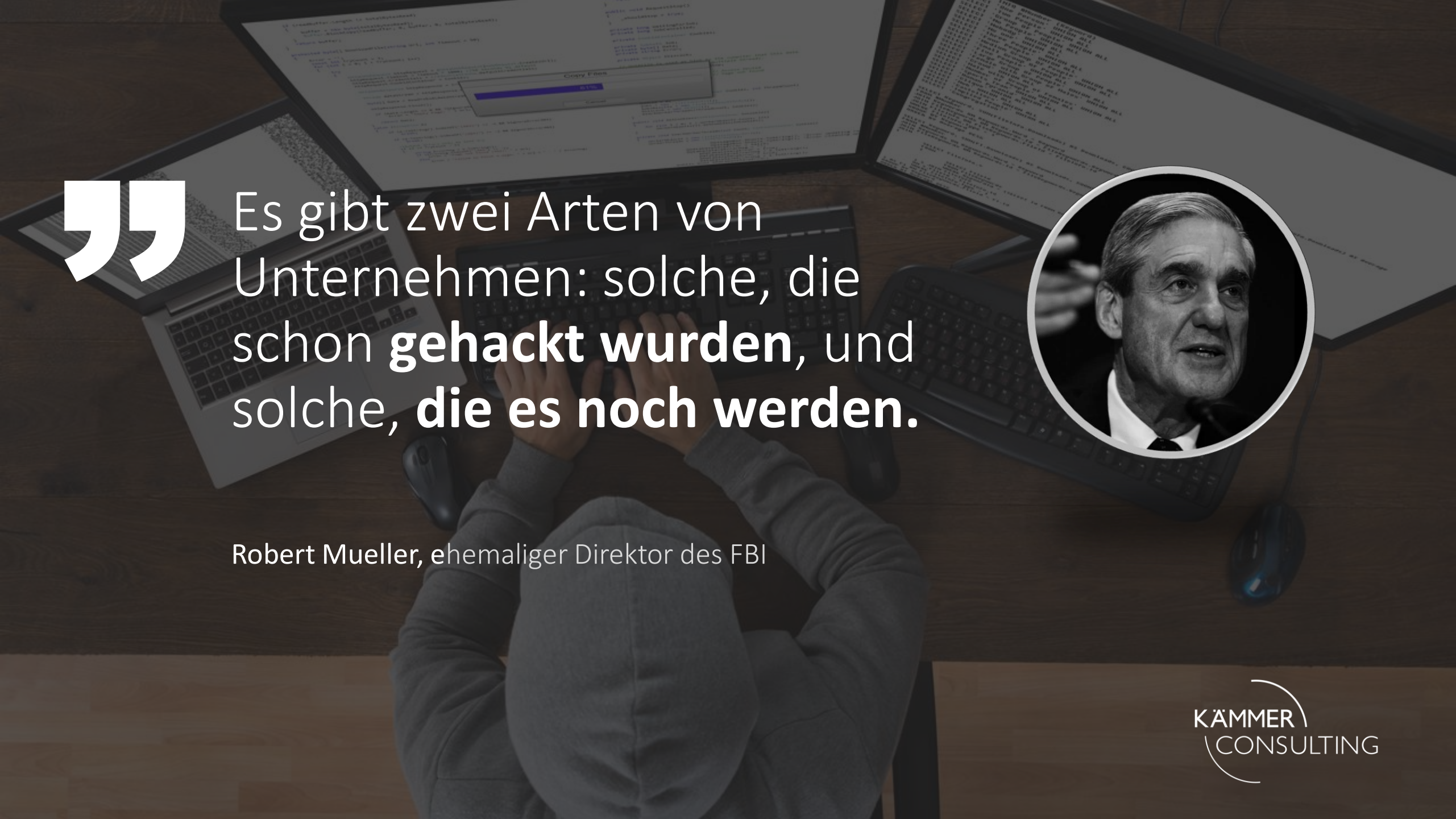


ZWISCHEN SELBSTSICHERHEIT UND NOTFALL: DIE BEDEUTUNG VON CYBERSICHERHEIT

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 2022 im Überblick

Top 3-Bedrohungen je Zielgruppe:

Gesellschaft	Wirtschaft	Staat und Verwaltung
		
Identitätsdiebstahl Sextortion Fake-Shops im Internet	Ransomware Schwachstellen IT-Supply-Chain: Abhängig	Ransomware APT Schwachstellen, offene oder falsch konfigurierte Online-Server

Erster digitaler Katastrophenfall in Deutschland

207 Tage Katastrophenfall

Nach Ransomware-Angriff konnten Elterngeld, Arbeitslosen- und Sozialgeld, KfZ-Zulassungen und andere bürgernahe Dienstleistungen nicht erbracht werden.

Die Anzahl der Schadprogramme steigt stetig.
Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund

116,6 Millionen zugenommen.

Hacktivismus im Kontext des russischen Krieges:
Mineralöl-Unternehmen in Deutschland muss kritische Dienstleistung einschränken.

Kollateralschaden
nach Angriff auf Satelliten-kommunikation

20.174

Schwachstellen in Software-Produkten (13% davon kritisch) wurden im Jahr 2021 bekannt. Das entspricht einem **Zuwachs von 10%** gegenüber dem Vorjahr.

15 Millionen Meldungen zu Schadprogramm-Infektionen in Deutschland übermittelte das BSI im Berichtszeitraum an deutsche Netzbetreiber.

34.000
Mails mit Schadprogrammen wurden monatlich durchschnittlich in deutschen Regierungsnetzen abgefangen.

78.000
neue Webseiten wurden wegen enthaltener Schadprogramme für den Zugriff aus den Regierungsnetzen gesperrt.

69%
aller Spam-Mails im Berichtszeitraum waren Cyber-Angriffe wie z.B. Phishing-Mails und Mail-Erpressung.

90%
des Mail-Betrugs im Berichtszeitraum war Finance Phishing, d.h. die Mails erweckten betrügerisch den Eindruck, von Banken oder Sparkassen geschickt worden zu sein.

BSI ist weltweit der führende Dienstleister im Bereich Common-Criteria-Zertifikaten.

4.400 (2020) → **5.100** (2021)

Zehn Jahre Allianz für Cyber-Sicherheit:
2022 sind wir bereits
6.220 Mitglieder.

Bundesamt für Sicherheit in der Informationstechnik

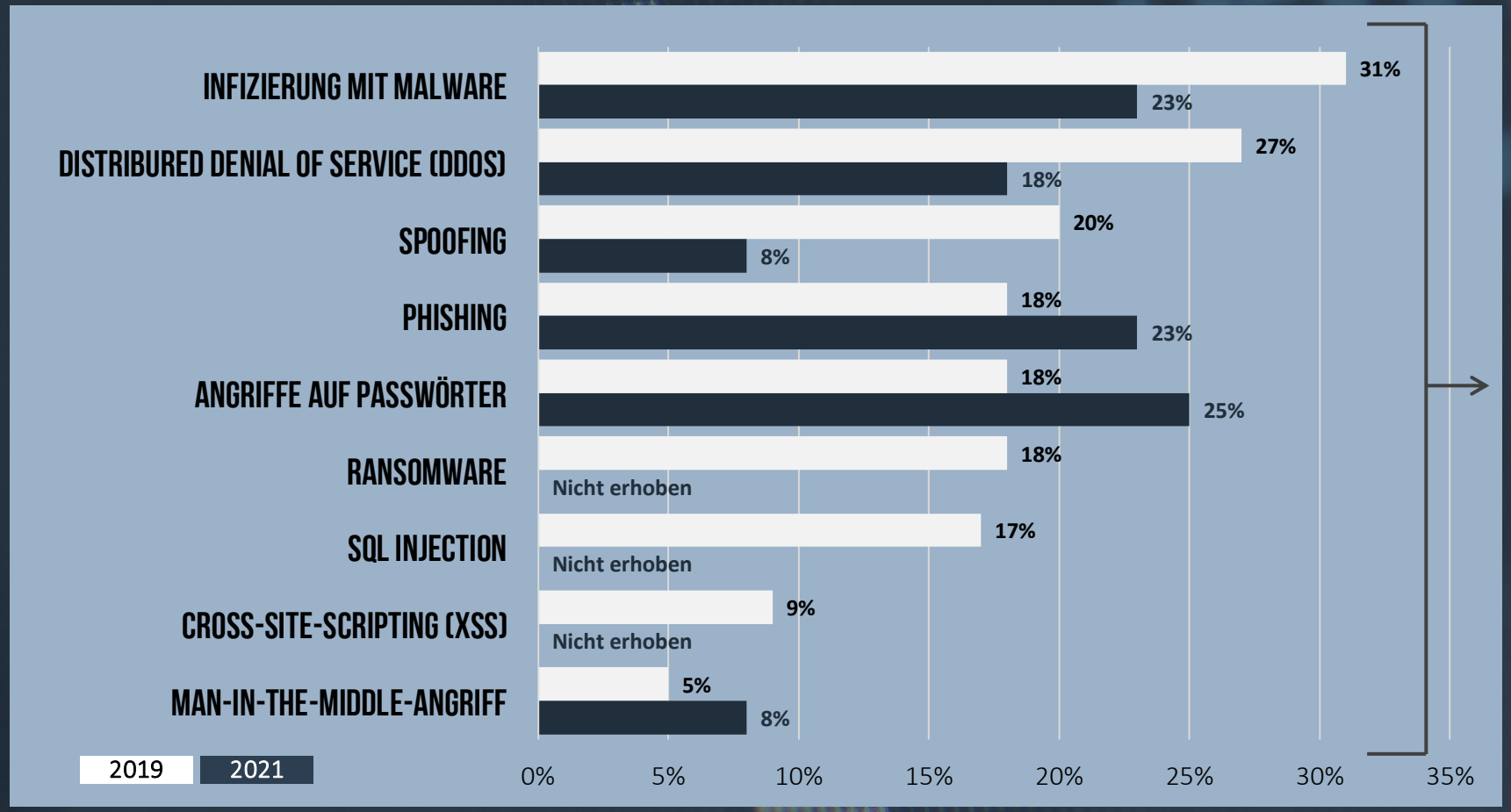
Deutschland Digital•Sicher•BSI•

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

KÄMMER CONSULTING

CYBERBEDROHUNGEN

Arten von Cyberangriffen (in %), die in Unternehmen in den jeweils letzten 12 Monaten Schaden anrichten



BEI 86% DER UNTERNEHMEN HABEN CYBERANGRIFFE 2021 SCHADEN ANGERICHTET –

2019 BEI 70% DER UNTERNEHMEN.

Quelle: Bitkom Research, 2021

KÄMMER CONSULTING

DEFINITION

„Als Cybersicherheit oder Informationssicherheit bezeichnet man Eigenschaften von technischen oder nicht-technischen Systemen zur Informationsverarbeitung, -speicherung und -lagerung, die die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen. Informationssicherheit dient dem Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von wirtschaftlichen Schäden und der Minimierung von Risiken.

Quelle: Wikipedia

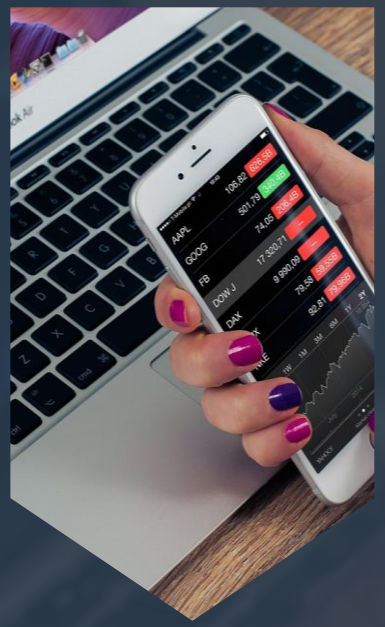
KÄMMER CONSULTING

CYBERRÄUME

INDUSTRIE

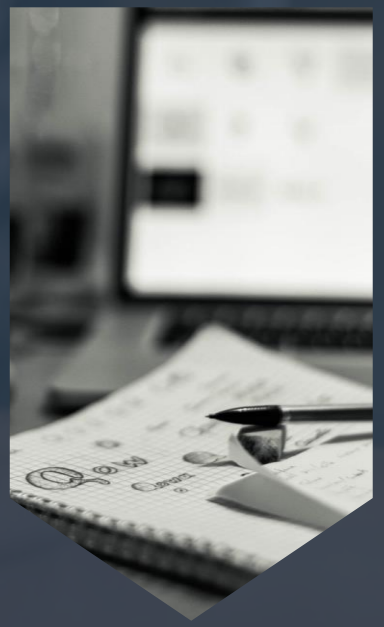
SOZIALE NETZWERKE

DATENSPEICHER



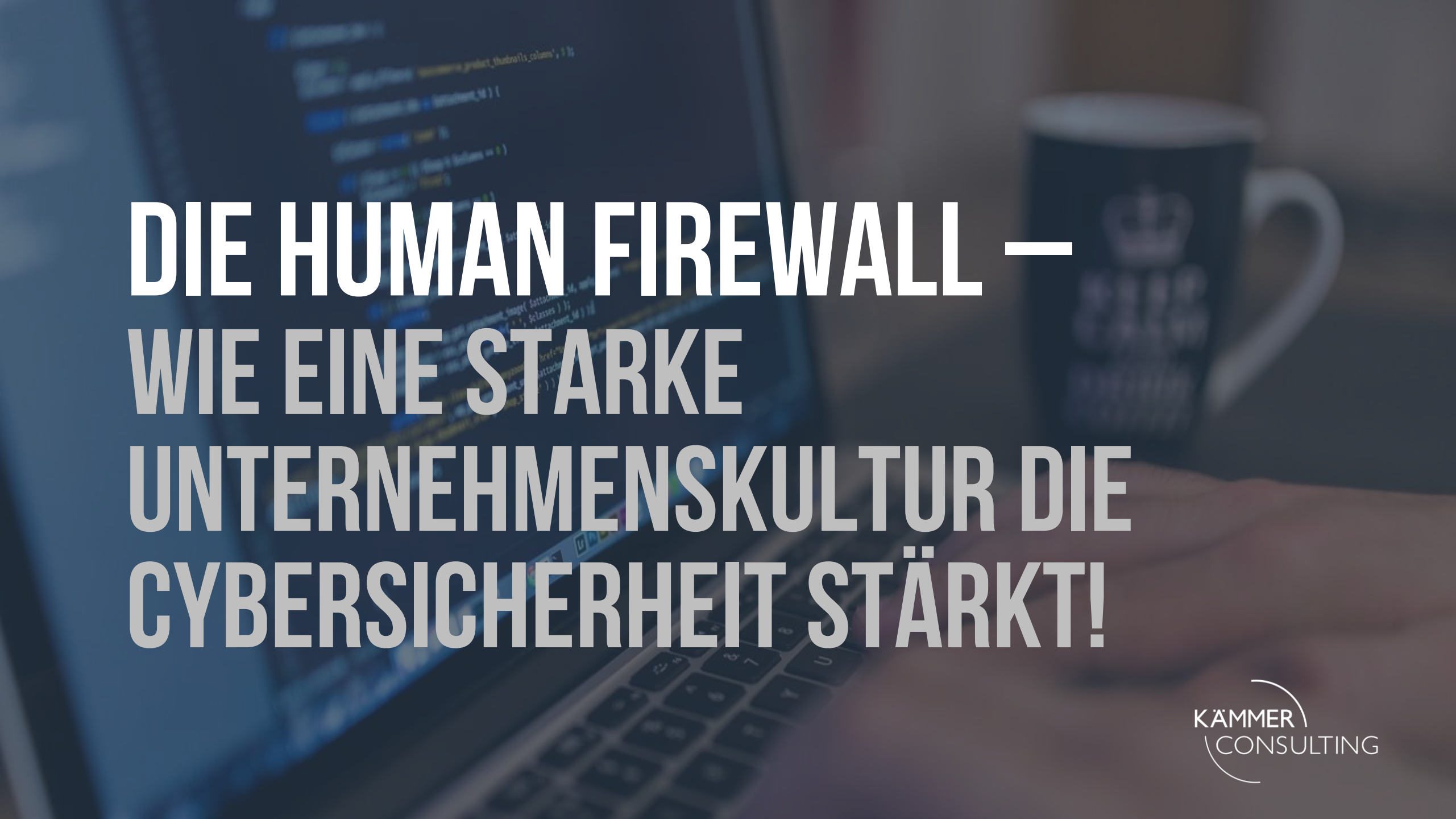
MARKTPLATZ

BANKGESCHÄFTE



POLITIK

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

5 FACTS FÜR EINE GUTE FEHLERKULTUR

1. Fördern von Offenheit und Transparenz
2. Etablieren einer Lernkultur
3. Schaffen einer unterstützenden Umgebung
4. Förderung der Mitarbeiterbeteiligung
5. Investitionen in Cybersicherheit

KÄMMER CONSULTING

5 FACTS FÜR EINE STARKE UNTERNEHMENSKULTUR

1. Klare Sicherheitsrichtlinien und –verfahren
2. Schulung und Sensibilisierung der Mitarbeiter
3. Angemessene Ressourcen für Cybersicherheit
4. Regelmäßige Überprüfung und Aktualisierung der Sicherheitsmaßnahmen
5. Partnerschaft mit externen Experten

KÄMMER CONSULTING

DATENSCHUTZ UND INFORMATIONSSICHERHEITS-MANAGEMENTSYSTEME (ISMS)

INDIKATOREN FÜR MEHR SICHERHEIT UND WETTBEWERBSFÄHIGKEIT

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.
- ISIS12
- BSI-GRUNDSCHUTZ
- VDS-RICHTLINIEN 10000

KÄMMER CONSULTING

CYBERSICHERHEIT LEITFÄDEN

- ISACA - Cyber-Sicherheits-Check
- Bitkom Leitfaden-IT-Sicherheitskatalog
- BSI - Leitfaden zur Basis-Absicherung nach IT-Grundschutz
- BSI - Allianz für Cybersicherheit - Leitfaden-Cyber-Sicherheits-Check

KÄMMER CONSULTING

VORTEILE VON DS UND ISMS

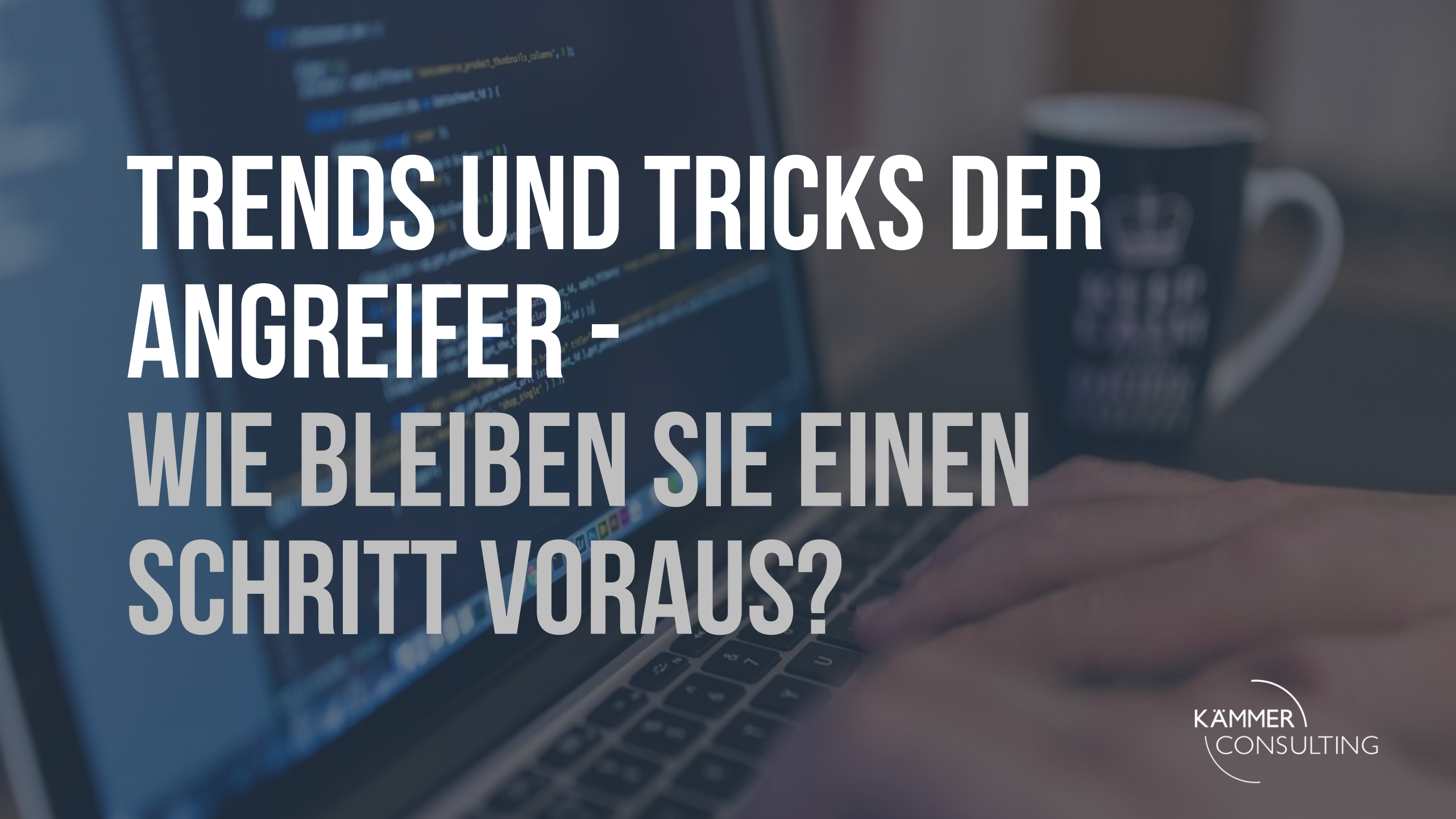
1. SCHUTZ VOR CYBERANGRIFFEN
2. EINHALTUNG VON RECHTLICHEN UND REGULATORISCHEN ANFORDERUNGEN
3. UNTERNEHMENSRUF UND KUNDENVERTRAUEN
4. RISIKOMANAGEMENT
5. WETTBEWERBSVORTEIL

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



TRENDS UND TRICKS DER ANGREIFER - WIE BLEIBEN SIE EINEN SCHRITT VORAUS?

KÄMMER CONSULTING

Mit Enginsight zu durchgängiger Informationssicherheit

Ihr Ansprechpartner für die Bereiche KRITIS und Public

Michael Rainer

Michael.Rainer@enginsight.com

01511 60 16 249

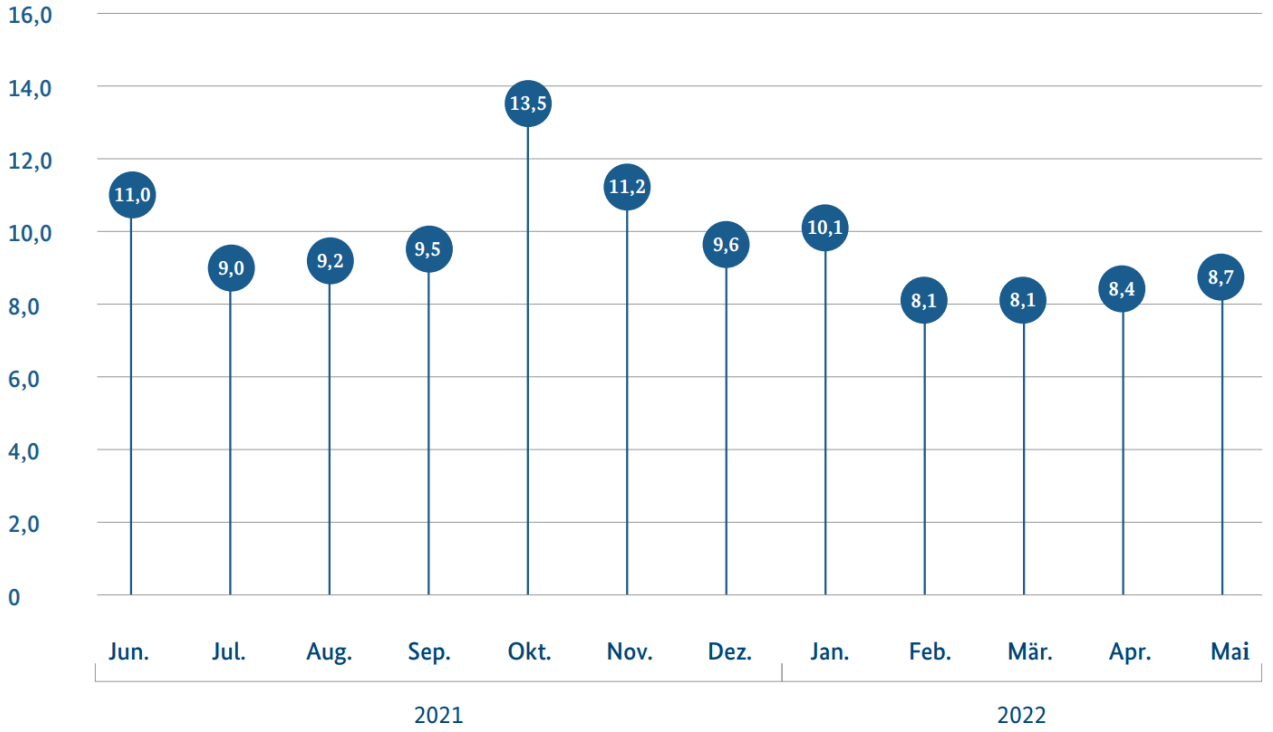
ENGINSIGHT


Weg vom Produkt
hin zur Lösung

Passende Informationen sammeln

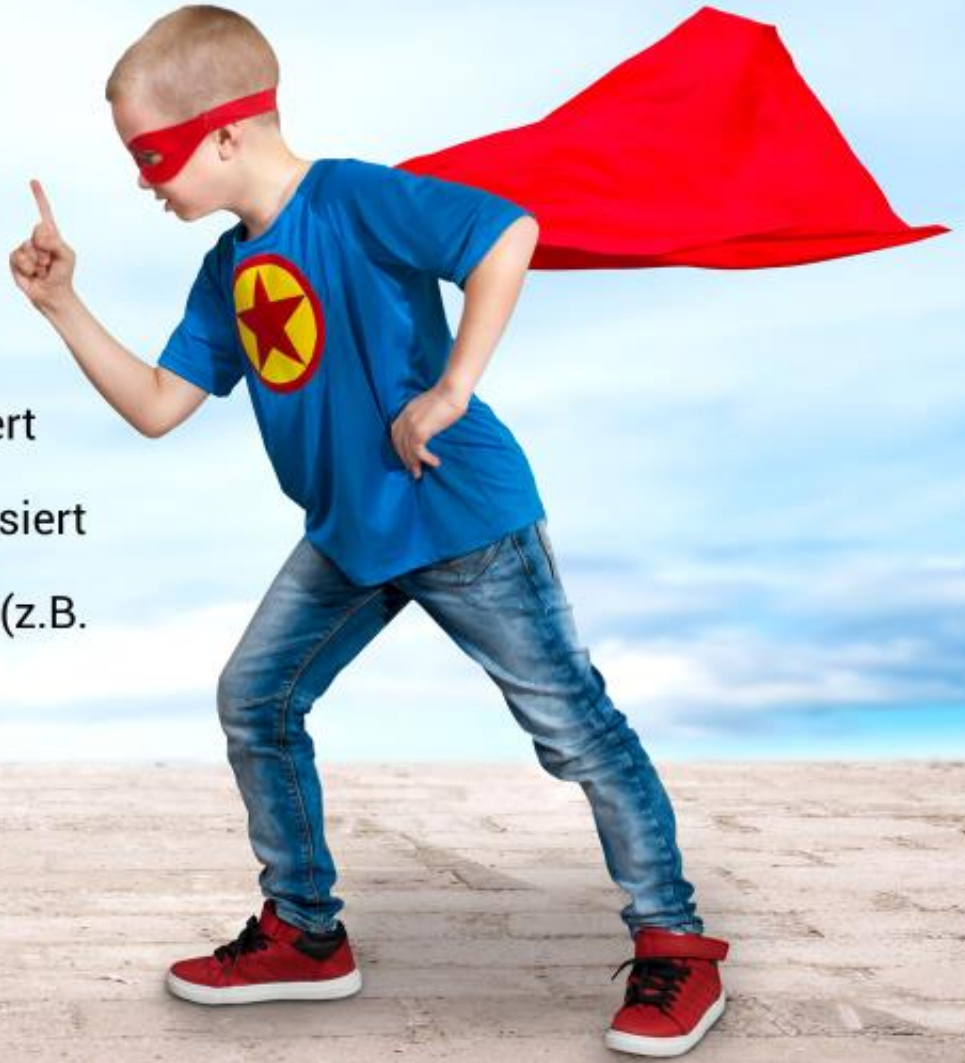
Neue Malware-Varianten von Juni 2021 bis Mai 2022
Anzahl in Millionen

Abbildung 1:
Quelle: Malware-Statistik des BSI auf Basis von Rohdaten des Instituts AV-Test GmbH



ENGINSIGHT

Ihre Motive für Cybersicherheit?



- Es ist bereits was passiert
- Dem „Nachbarn“ ist es passiert
- Anforderungen von Dritten (z.B. Normen)
- Sicherheitsstrategie

ENGINSIGHT


> 90% männlich
< 30 Jahre
gutes soziales Umfeld

ENGINSIGHT


Wana DecryptOr 2.0
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/15/2017 16:32:52
Time Left
02:23:59:49
Your files will be lost on
5/19/2017 16:32:52
Time Left
06:23:59:49
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

ENGINSIGHT

Ich doch nicht...

- Schutzziel
- Branche
- Finanzielles Potential
- Technische Schwachstellen
- Menschliche Schwachstellen

ENGINSIGHT

Reduktion der Komplexität auf den Gesamtprozess

ENGINSIGHT

Wir erschweren das Eindringen und reduzieren die Auswirkung!

Was ist da los?

Die Lage der IT-Sicherheit in Deutschland 2022 im Überblick

Top 3-Bedrohungen je Zielgruppe:

Gesellschaft	Wirtschaft	Staat und Verwaltung
		
Identitätsdiebstahl Sextortion Fake-Shops im Internet	Ransomware Schwachstellen, offene oder falsch konfigurierte Online-Server IT-Supply-Chain: Abhängigkeiten und Sicherheit	Ransomware APT Schwachstellen, offene oder falsch konfigurierte Online-Server

Erster digitaler Katastrophenfall in Deutschland

207 Tage Katastrophenfall

Nach Ransomware-Angriff konnten Elterngeld, Arbeitslosen- und Sozialgeld, KfZ-Zulassungen und andere bürgernahe Dienstleistungen nicht erbracht werden.

Die Anzahl der Schadprogramme steigt stetig.

Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund

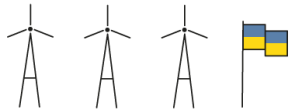
116,6 Millionen zugenommen.

Hacktivismus im Kontext des russischen Krieges:

Mineralöl-Unternehmen in Deutschland muss kritische Dienstleistung einschränken.

Kollateralschaden

nach Angriff auf Satelliten-kommunikation



20.174

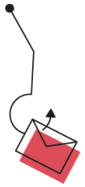
Schwachstellen in Software-Produkten (13% davon kritisch) wurden im Jahr 2021 bekannt. Das entspricht einem **Zuwachs von 10%** gegenüber dem Vorjahr.

15 Millionen Meldungen zu Schadprogramm-Infektionen in Deutschland übermittelte das BSI im Berichtszeitraum an deutsche Netzbetreiber.

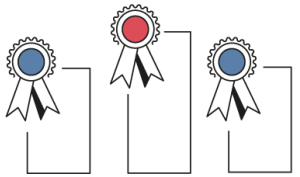
34.000 Mails mit Schadprogrammen wurden monatlich durchschnittlich in deutschen Regierungsnetzen abgefangen.

78.000 neue Webseiten wurden wegen enthaltener Schadprogramme für den Zugriff aus den Regierungsnetzen gesperrt.

69% aller Spam-Mails im Berichtszeitraum waren Cyber-Angriffe wie z.B. Phishing-Mails und Mail-Erpressung.



90% des Mail-Betrugs im Berichtszeitraum war Finance Phishing, d.h. die Mails erweckten betrügerisch den Eindruck, von Banken oder Sparkassen geschickt worden zu sein.



BSI ist weltweit der führende Dienstleister im Bereich Common-Criteria-Zertifikaten.

4.400 (2020) → **5.100** (2021)

Zehn Jahre Allianz für Cyber-Sicherheit: 2022 sind wir bereits

6.220 Mitglieder.

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

Quelle: BSI Lagebericht 2022

ENGINSIGHT

Mit Enginsight zu durchgängiger Informationssicherheit

Mit der einmaligen Kombination aus

ANGRIFF und VERTEIDIGUNG

IT Management	IT-Sec Frühwarnsystem	Security Automation	KI-Monitoring	Netzwerksicherheit
▪ Live Inventar	▪ Schwachstellen-Scans	▪ Automatische Pentests	▪ Individuelle Metriken	▪ Intrusion Detection
▪ Asset Management	▪ Sicherheits-Konfigurationen	▪ Remote Actions	▪ Monitoring Prozesse/Services	▪ Intrusion Prevention
▪ Health Checks (Ping,Port,SNMP)	▪ Ports, Software, Verbindungen	▪ Patchmanagement	▪ Anomalieerkennung	▪ Mikrosegmentierung

Technischer Lösungsansatz

Das große Ganze

Die Lösung muss zum Unternehmen passen,
nicht das Unternehmen zur Lösung!

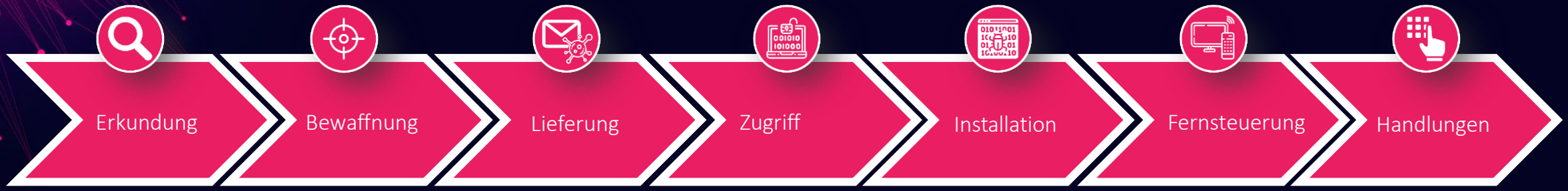
- Simplifizierung
- Flexibilität
- Effizienz
- Unterstützung / Erfüllung von Anforderungen und Gesetzen
- Transparenz
- Prozessintegrität
- Aussagekräftige Berichte für alle Interessensvertreter
- Risikomanagement

ENGINSIGHT

Technischer Lösungsansatz

- Technische Anforderungen – IDS / IPS, Schwachstellenmanagement, Rechtekonzepte
- Kernfunktionen BSI OH SzA: Detektion, Protokollierung, Reaktion
- Kontinuierliche Betriebsfähigkeit mit KVP nach PDCA
- Implementierungszeit und Aufwand – Machbarkeit
- Integrationsmöglichkeit – SOC, SIEM, Ticketsystem
- Automation
- DSGVO konform
- Berücksichtigung Betriebsrat (IP-Anonymisierung)
- Backdoorfreiheit
- Prozessorientiertes Framework – Möglichkeit und Kontrolle zur Auslagerung an Dienstleister

Cyber Kill Chain



PRÄVENTION

- Schwachstellenmanagement und autom. Pentest
- Mikrosegmentierung
- IDS / IPS
- Security-Monitoring
- Systemhärtung

RESILIENZ

- IDS
- IPS
- Alarme (Dienste, Prozesse, Plugins etc.)
- Machine Learning
- Mikrosegmentierung
- FIM

ENGINSIGHT

Schwere der Auswirkungen

Kosten des Sicherheitsvorfalls

Abwehr im Prozess

Enginsight für autonome und proaktive Informationssicherheit:

- Automatischer Pentest
- Erweiterter Schwachstellenscan
- Schwachstellenmanagement
- Überwachung von Anmeldungen, Diensten, Prozessen

  etc.
- IPS

Kenne Deinen Gegner!

ENGINSIGHT

FAZIT

Die Lösung prozessorientiertes Framework betrachtet:

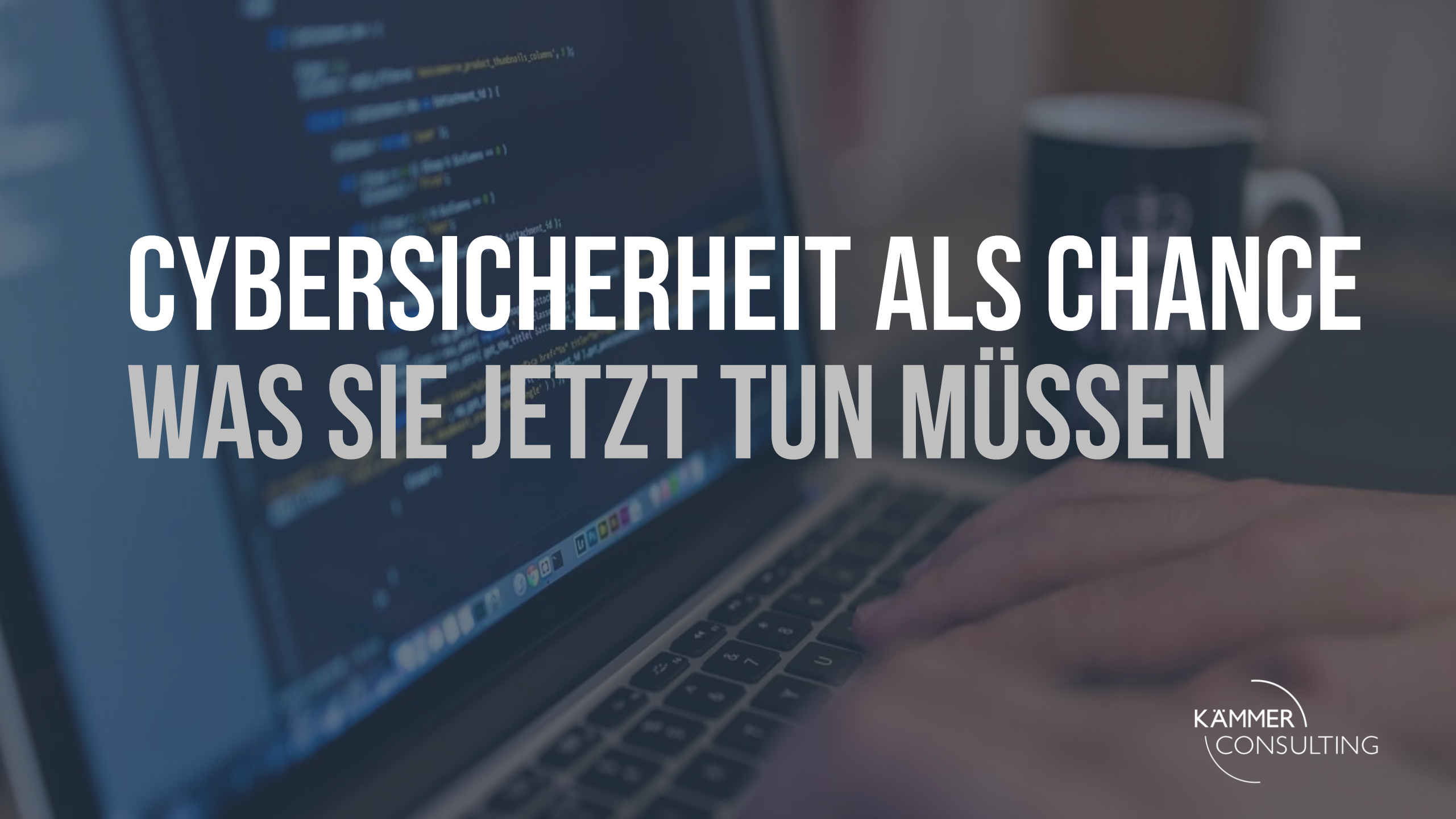
- Prävention UND Resilienz
- die Prozessebene
- Handlungen und Mechanismen
- das Vorgehen von Hackern in der Praxis
- SIEM use cases
- Schutzziele

KÄMMER CONSULTING

&

ENGINSIGHT

Mit SICHERHEIT in eine gemeinsame Zukunft!



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 Session, 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

LEITER VERTRIEB | INFORMATIONSSICHERHEITSBERATER
(ISO/IEC 27001 IMPLEMENTER,
ICO ISMS FOUNDATION ACCORDING TO TISAX,
DEKRA ZERT. DATENSCHUTZBEAUFTRAGTER)

FON +49 531 702249 – 42
MOBIL +49 152 5136 3456