Krisenkommunikation nach Ransomwareattacken

Krisenkommunikation nach Ransomwareattacken

2023

#HSMAday 2023

Zur Person

Journalist seit 2004

Copywriter seit 2009

Chefredakteur eines Verlags für Wirtschaftsmagazine 2013-2020

Freiberuflicher Berater für strategische Kommunikation

Stabsarbeit Kommunen und KatSchutz

Pressesprecher einer Mittelstadt, NRW

Privatpilotenlizenz
Heißluftballon + Hotair-Airship

Ad-hoc Krisenkommunikation für Behörden und Unternehmen (DACH, 24/7)

Beratung in der Akzeptanz-, Risiko- und Krisenkommunikation

Aufbau, Revision und Weiterentwicklung von Krisenkommunikationsplänen

Workshops zur Risiko- und Krisenkommunikation

Durchführung und Begleitungen von Stabsübungen

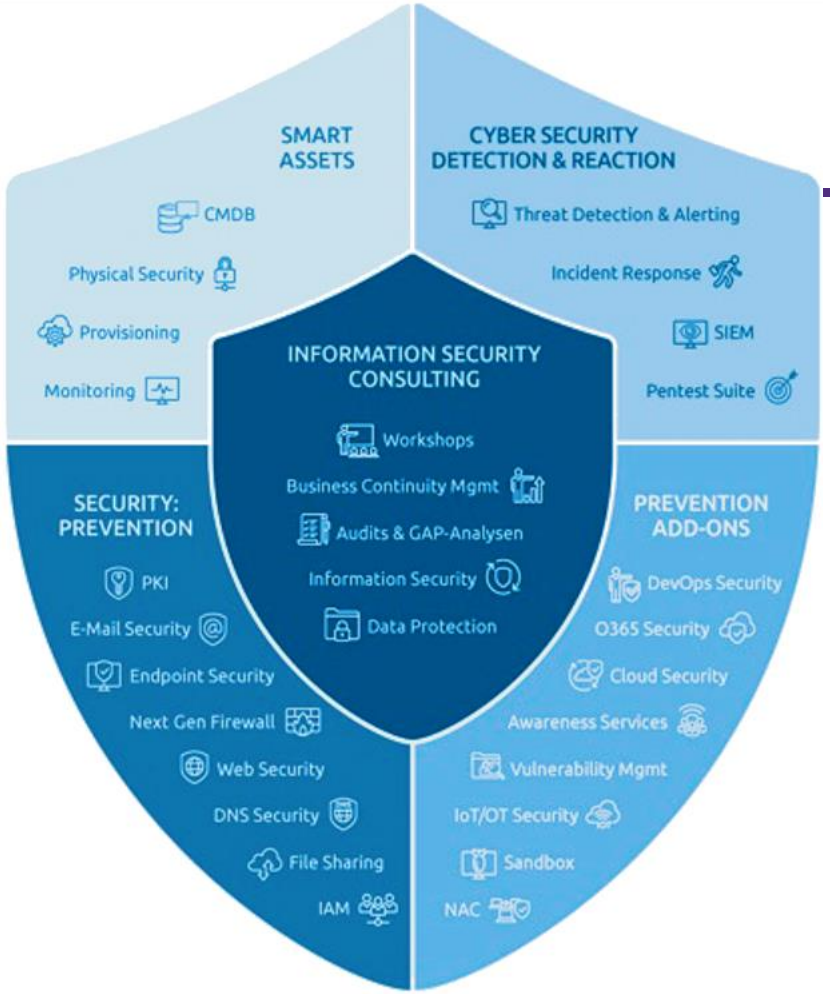
2023

HSMA day
2023

magellan netzwerke
Kommunikationssysteme NETZWERK
Somnitec
cano systems
globits
we°novate
OPTIMAbit Pentest Professionals
xiv-CONSULT
IUGITAS BUSINESS RESILIENCE EXPERTS
datadirect network technology

FERNAO NETWORKS

10 Unternehmen
>650 Mitarbeiter
22 Standorte Weltweit



Unsere Partner:

ITSMgroup
TÜVRheinland® Genau. Richtig.

Unsere Lehraufträge:

Technology Arts Sciences TH Köln
Technische Hochschule Brandenburg University of Applied Sciences

Unsere Mitgliedschaften:

ASW
IBCRM
DAKEP Zertifizierung
CYBER SECURITY CLUSTER BONN

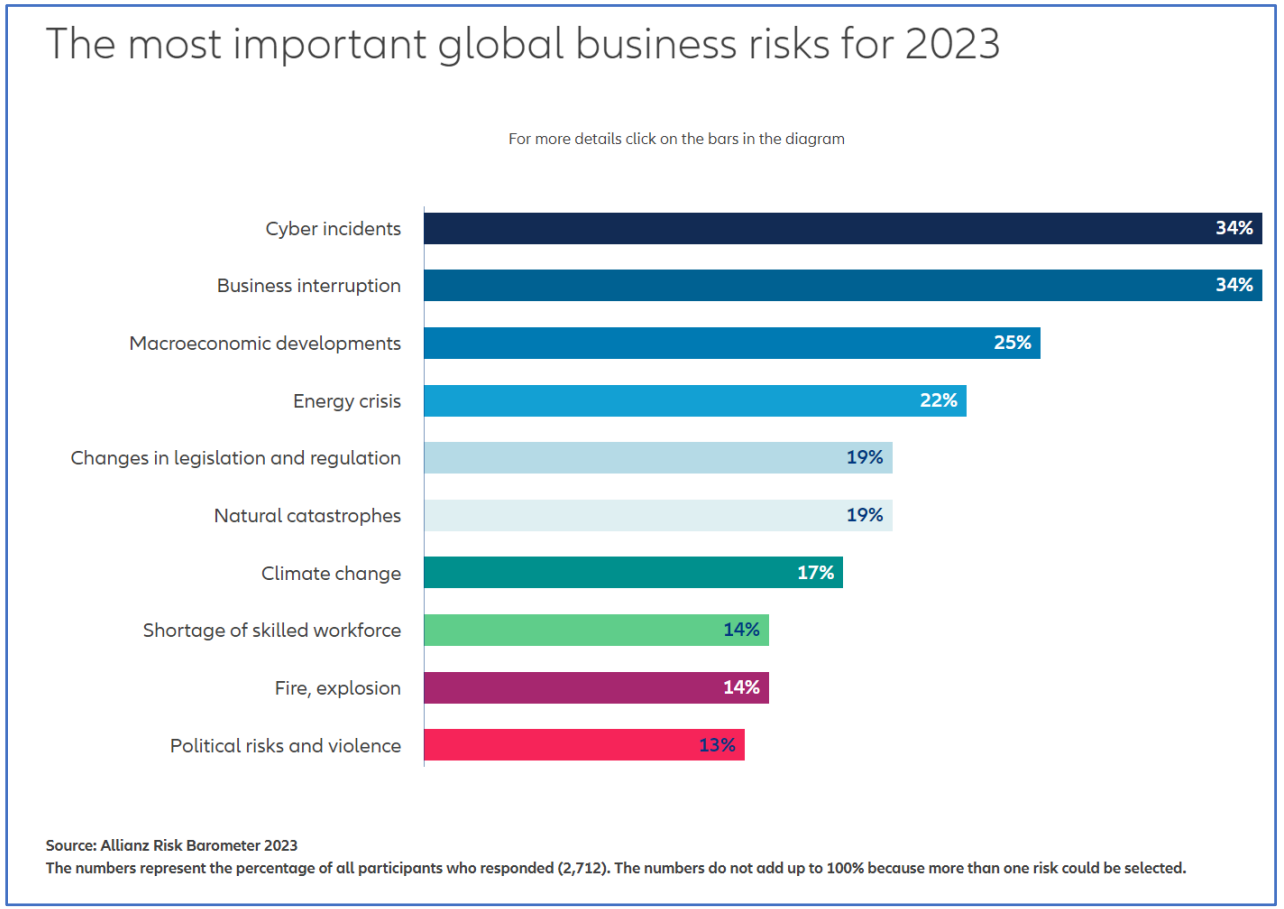
HSMA day 2023

2023

Agenda

- Auf Beutezug in der digitalen Welt
- Was wollen Cyberkriminelle in der Hospitality-Branche?
- Erstreaktionen nach einem Angriff
- Crashkurs Krisenkommunikation
- Impulse zur Vorbereitung auf den Ernstfall

Cybercrime



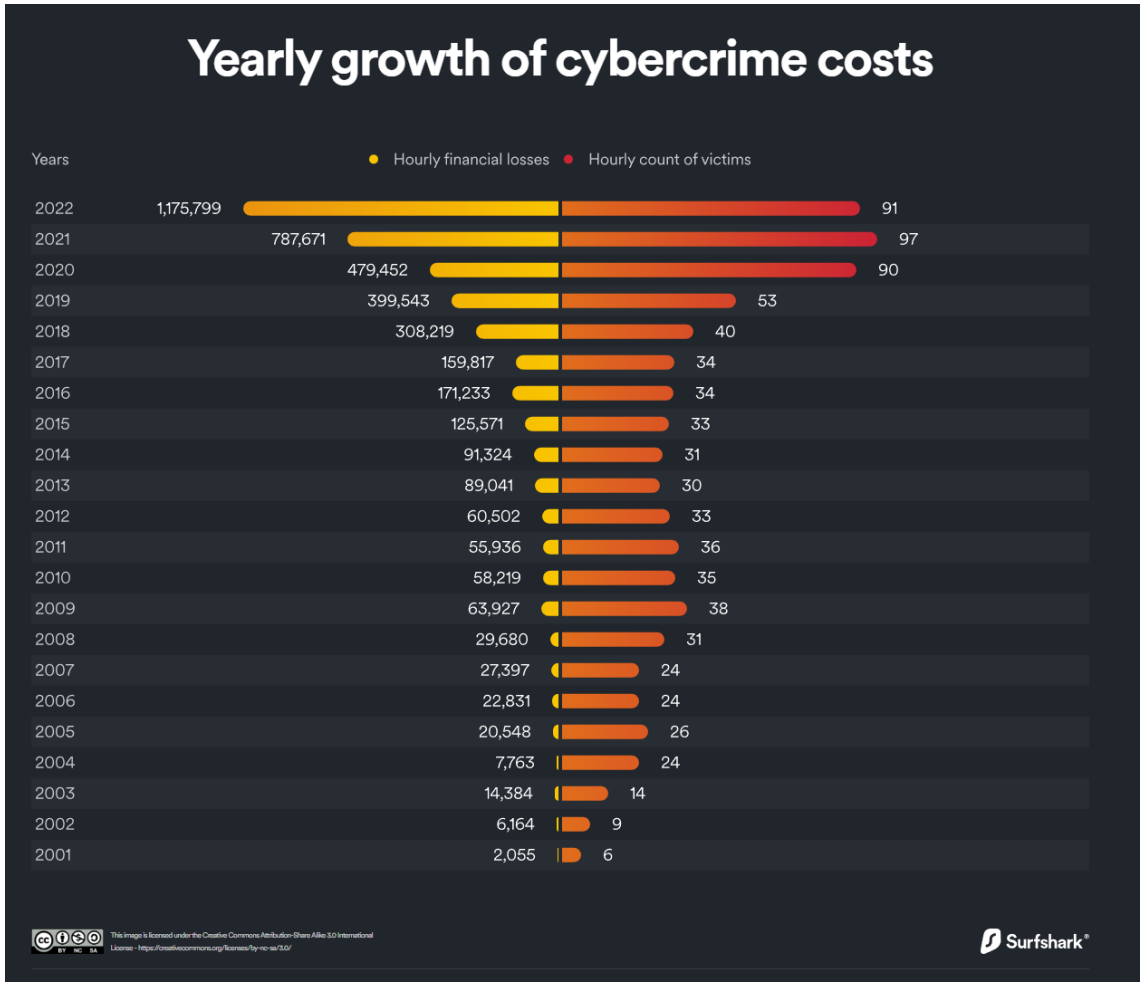
typical effects of cyberattacks on business:

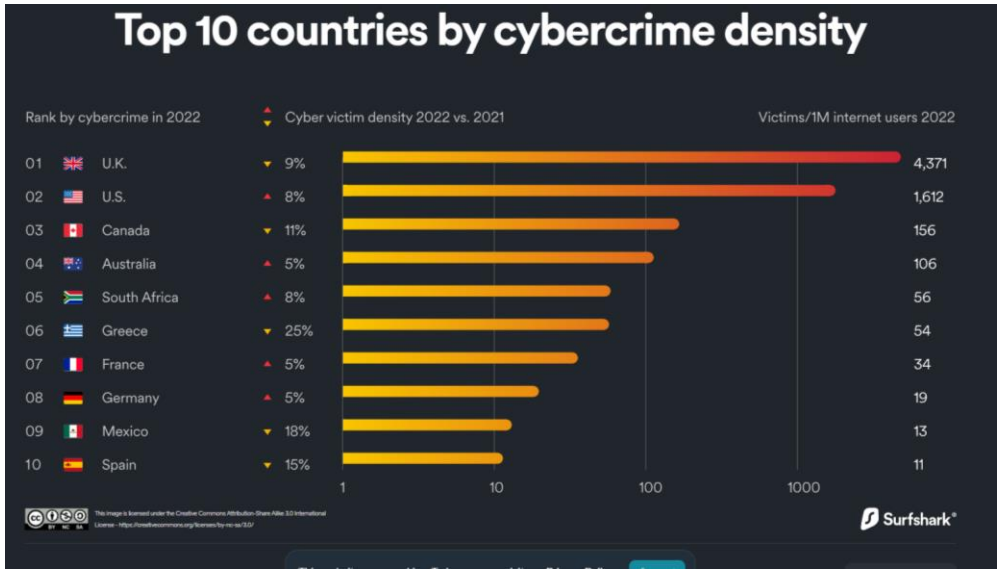
- business interruption
  - minimum 1 week
  - average 2 to 4 weeks
  - occasionally 12 weeks or longer
- data loss due to encrypted or compromised backups
- data leak / data breach in public
- “digital isolation”

2023

HSMA day 2023

Cybercrime



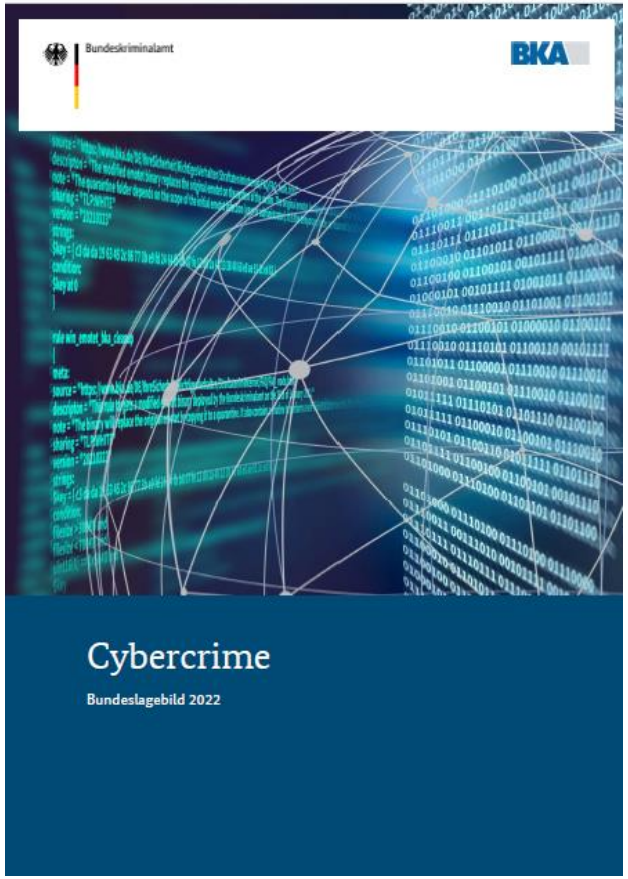


- höhere Professionalisierung der Gruppen
- steigende Professionalisierung der Angriffe
- zielgerichte, strategische Angriffe

2023

HSMA day 2023

Cybercrime



3.4 RANSOMWARE

Von allen Malware-Arten hat Ransomware weiterhin das höchste Schadenspotential. Im Jahr 2022 wurde im Durchschnitt täglich mindestens ein deutsches Unternehmen Ziel eines Ransomware-Angriffs. [11] Bei diesen Angriffen wurden insgesamt 42 unterschiedliche Ransomware-Varianten identifiziert. Am häufigsten waren deutsche Geschädigte im vergangenen Jahr von Angriffen mit der Ransomware-Variante LockBit betroffen.

TOP 10 Ransomware-Varianten[a]

1. LockBit
2. Phobos
3. Deadbolt
4. BlackCat / AlphV
5. Hive
6. BlackBasta
7. Conti
8. Royal
9. MedusaLocker
10. ViceSociety

Durchschnittlich gezahlte Lösegeldsumme:

276.619 US-Dollar

Aber: Unternehmen gehen seltener auf Täterforderungen ein[c].

Angriffe mit

42

unterschiedlichen Ransomware-Varianten[b].

Kriminelle Einnahmen:

457 Millionen US-Dollar

Festgestellte Lösegeldzahlungen auf Kryptowallets von Ransomware-Akteuren[d]

2023

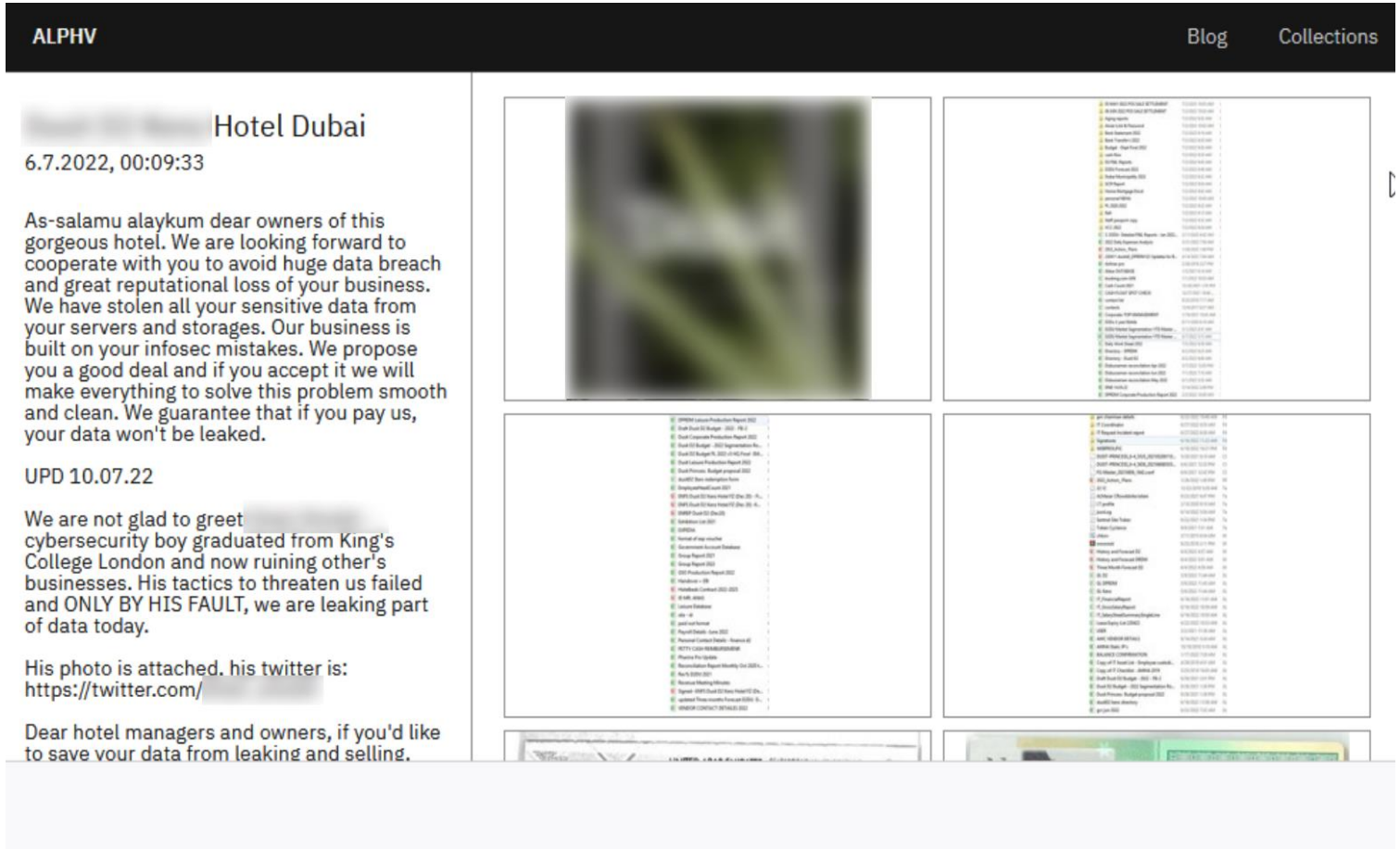
HSMA day 2023

Cybercrime vs. Hospitality

2023

#HSMAday 2023

Cybercrime vs. Hospitality



2023

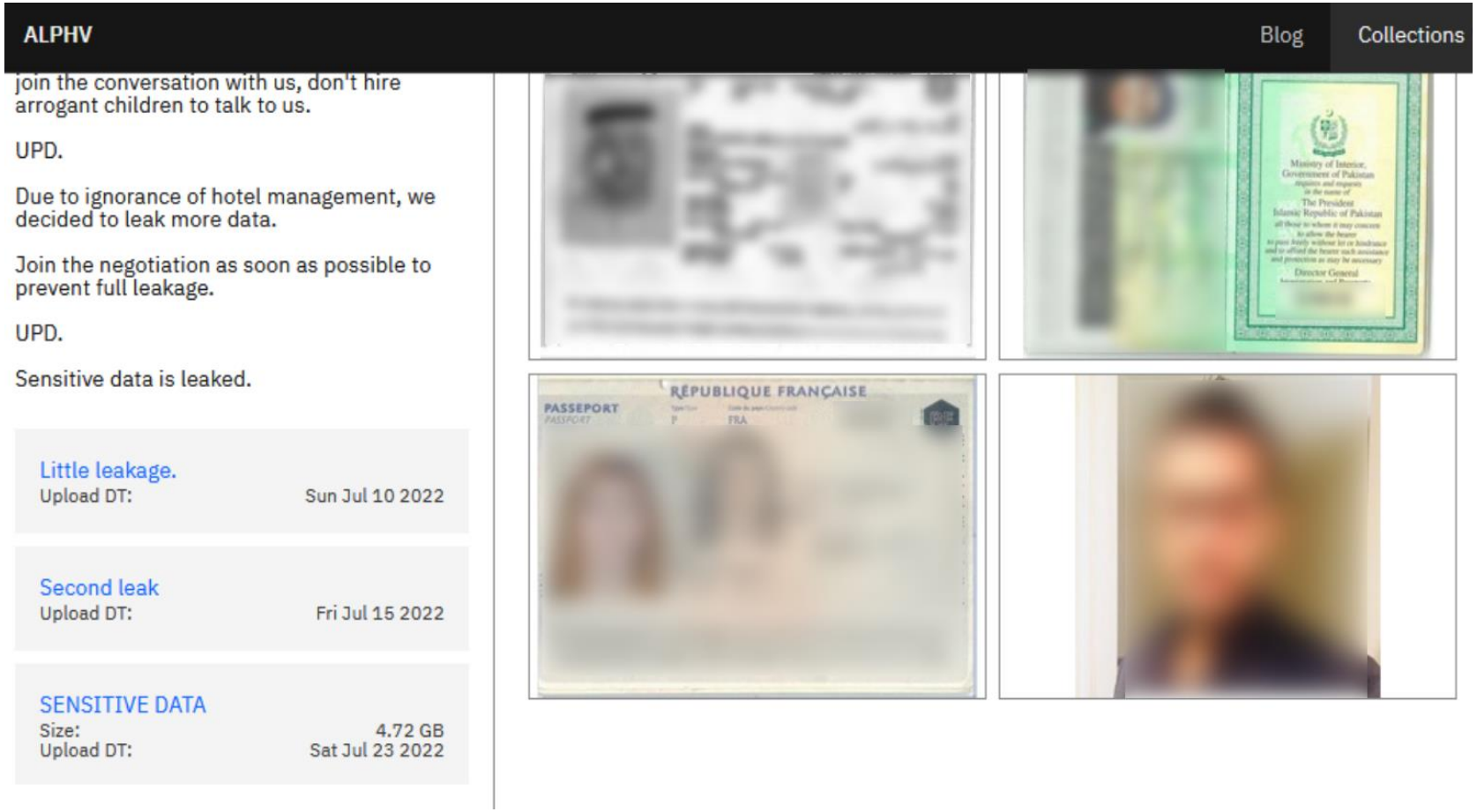
HSMA day
2023

Cybercrime vs. Hospitality

2023

HSMA day 2023

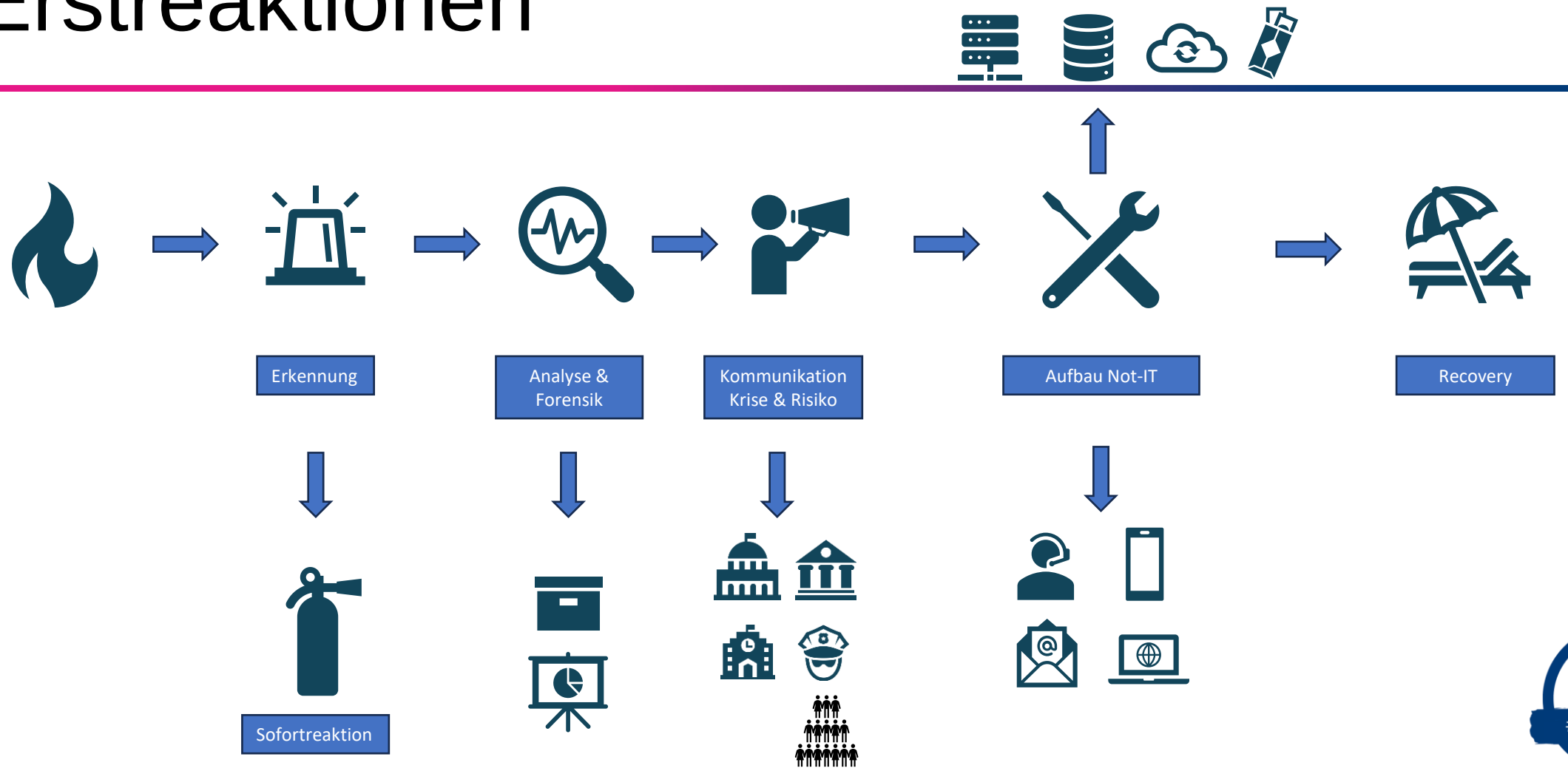
Cybercrime vs. Hospitality



2023

HSMA day
2023

Erstreaktionen



2023

HSMA day 2023

Crashkurs Krisenkommunikation

Schnelligkeit

- frühzeitig
- proaktiv > reaktiv
- im Idealfall: vor der Presse

Konsistenz

- Fakten, Fakten, Fakten
- einheitlich und koordiniert auf allen Kanälen
- keine Widersprüche, keine Interpretationen

Handlung (Reputation)

Wahrhaftigkeit

- sachlich, nüchtern
- transparent und wahr
- Cave: Emotionen/Empathie

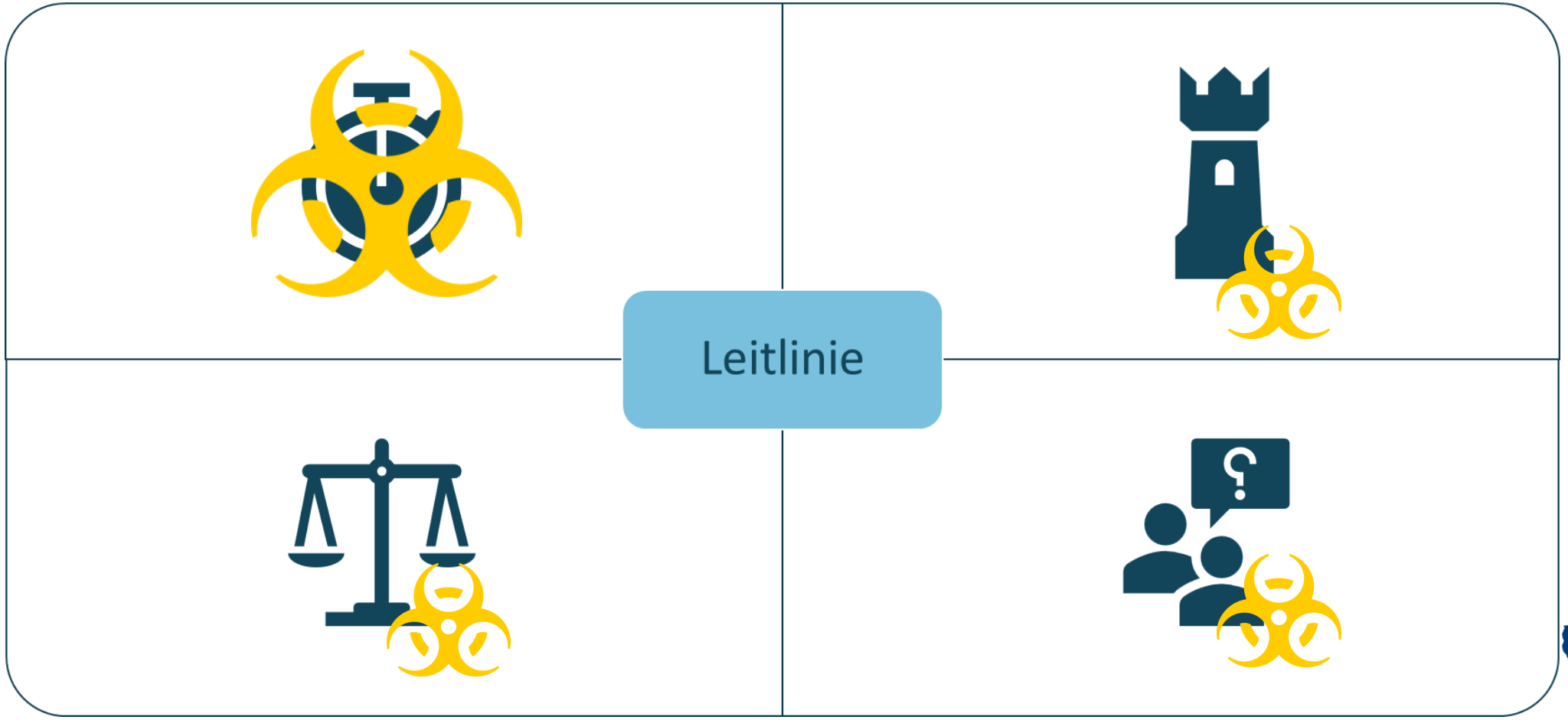
Verständlichkeit

- auf Augenhöhe
- kurze, einfache, unkomplizierte Sätze
- bildhafte Sprache, sofern möglich

2023

HSMA day 2023

Krisenkommunikation



2023

Krisenkommunikation

„Wer sagt was wann wo und wie an wen?“

- Technische Ressourcen (Redundanzen)
- Vorlagen Textbausteine FAQ intern/extern
- Sprachregelung
- Sprechfähigkeit (DA/VA)
- Dialogoption Kunden
- Zielgruppen der Krisenkommunikation
- Adresslisten Kontaktdaten

2023

HSMA day 2023

Impulse zur Vorbereitung

1. Risikokommunikation:
Werden Sie Unterstützer Ihrer IT und Multiplikator*in für Awareness

2. Sensibilisieren Sie Ihre Geschäftsführung für den IT-Grundsatz:
„es ist nicht die Frage, ob man Opfer eines Cyberangriffs wird,
sondern die Frage ist, wann man Opfer wird und wie gut man darauf vorbereitet ist.“

3. Bereiten Sie sich und Ihre Krisenkommunikation vor
mit Textvorlagen und Redundanzen

4. Üben, üben, üben.

5. Achten Sie auf Ihre Kolleg*innen und auf sich selbst!

2023

HSMA day 2023

Wenn es für Vorbereitungen zu spät ist…

*Wir versuchen Ihnen nach Verfügbarkeit schnellst möglich zu helfen. Mit unserem "**Krisenmanager as a Service**" garantieren wir Ihnen aber auch gerne über ein SLA eine bestimmte Verfügbarkeit.

…rufen Sie uns an damit wir Sie
vor die Lage bringen können.

2023

- Erfahrener **Krisenmanager** Remote oder vor Ort
- **Krisenkommunikation** zu Mitarbeitern, Kunden, Lieferanten, Öffentlichkeit, etc. inkl. proaktivem (Social) Media Monitoring
- Koordination der **IT Incident Response** gemeinsam mit Ihrer IT und Ihren IT Dienstleistern
- Mit **IT Forensik** zu einer geeignete Dokumentation für (Cyber-)Versicherungen und Behörden
- **Kommunikation** mit (Ermittlungs- und Datenschutz-)Behörden, Versicherung, Dienstleistern und anderen Parteien
- Ad-hoc Aufbau & Moderation **Krisenstab / IT-Notfallstab**
- Ad-hoc **Notfallprozesse** aufsetzen und etablieren
- **Lagedarstellung** und **Dokumentation**
- Unterstützung durch großes **Expertennetzwerk**

HSMA day
2023