



Cyber-Sicherheit

Wie sollten sich Unternehmen vorbereiten?

DER ETWAS ANDERE LEBENSLAUF.....

- 1 2019: Ransomware-Angriff auf Unternehmensinfrastruktur
Incident Management: Ganzheitliche Verantwortung in komplexer Unternehmensgruppe.
- 2 2021: Ransomware-Attacke auf Logistik-Netzwerk
Leitung des Krisenstabs. Fokus: Aufrechterhaltung der Betriebskontinuität
- 3 2022: Ransomware-Angriff auf exklusiven Grundstofflieferanten
Krisenstabsmitglied. Sicherstellung der Versorgungssicherheit für kritische Sortimente.
- 4 Seit 2022: Kontinuierliche Abwehr komplexer Cyber-Bedrohungen
Erfolgreiche Bewältigung von Multi-Phishing Attacken, Social Engineering Initiativen, Unterbindung von Datenabflüssen, Einsatz forensischer Methoden & KI.



A person wearing a dark hoodie is seen from the side, looking down at a laptop screen. The background is a blurred city at night with various lights and buildings. The text is overlaid on the left side of the image.

—

WAS HABE ICH GELERNT ?

ES GIBT NUR ZWEI ARTEN VON
UNTERNEHMEN:

DIE, DIE BEREITS GEHACKT WORDEN
SIND UND **DIE, DIE ES NOCH WERDEN.**



HOW TO DECRYPT FILES.txt - Notepad

File Edit Format View Help

All your personal FILES are now ENCRYPTED!

Don't worry, you can get back all your files

I don't want to lose your files too. If I want to do something nasty I would have wipe out all of your data but that is not helping me. :)

So temporary all of your files are mine now until you pay the service cost of recovering them.

If you want to recover them contact me at the email below, I'll be more than happy to help you to get out of this situation.

You have got 48 hours exactly, before you lost your files forever.

Failing which, the price to recover double with every 48 hours passing!

Rest assured, all your files will be recovered once payment is received.

The Price to get all things back to normal : US\$ 1500

My BTC Wallet : 1Mc9xe3mjaMLz99CUjao88s65X3ydVEZbX

Email : frankhans@tuta.io

readme.txt - Notepad2

File Edit View Settings ?

1 |----- welcome. Again. -----

2 |

3 | [+] whats Happen? [+]

4 |

5 | Your files are encrypted, and currently unavailable. You can check it: all files on your computer has expansion 100MB. By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you will lose your data (NEVER).

6 |

7 | [+] what guarantees? [+]

8 |

9 | Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.

10 | To check the ability of returning files, You should go to our website. There you can decrypt one file for free. This is our guarantee.

11 | If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, and just we have the private key. In practise - time is much more valuable than money.

12 |

13 | [+] How to get access on website? [+]

14 |

15 | You have two ways:

16 |

17 | 1) [Recommended] Using a TOR browser!

18 | a) Download and install TOR browser from this site: <https://torproject.org/>

19 | b) open our website: <http://ap1ebzu47wgazapdqs6vrcv6zcnjppkxbxbr6wketf56nf6aq2nmyoyd.onion/>

20 |

21 | 2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:

22 | a) open your any browser (Chrome, Firefox, Opera, IE, Edge)

23 | b) open our secondary website: <http://decryptor.top/>

24 |

25 | Warning: secondary website can be blocked, thats why first variant much better and more available.

26 |

27 | When you open our website, put the following data in the input form:

28 | Key:

Ln1:62 Col1 Sel0

3.25 KB

Unicode

CR+LF INS Default Text

[EXTERN] - Official Announcement



Sabine Disse <abrahamomar31@gmail.com>

An 



11:

 Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.



GEROLSTEINER BRUNNEN GMBH & CO. KG .pdf
458 KB



Nachricht übersetzen in: Deutsch

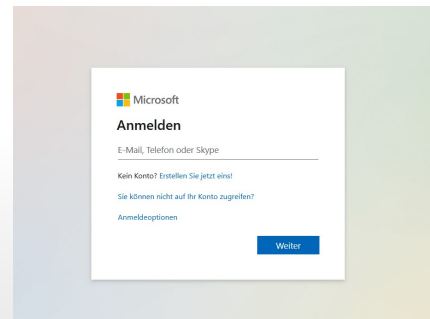
Nie übersetzen aus: Englisch

Übersetzungseinstellungen

Sie erhalten nicht oft eine E-Mail von abrahamomar31@gmail.com. Erfahren Sie, warum dies wichtig ist

ACHTUNG: Diese E-Mail stammt von einem externen Absender. Bitte vermeiden Sie es, Anhänge oder externen Links zu öffnen.

Dear Colleagues





Kompromittierung von Geschäfts-E-Mails

Business-E-Mail-Compromise (BEC)



www.mineralwasser.com

www.miineralwasser.com

www.minneralwasser.com

www.mineeralwasser.com

www.minerralwasser.com

www.mineraalwasser.com

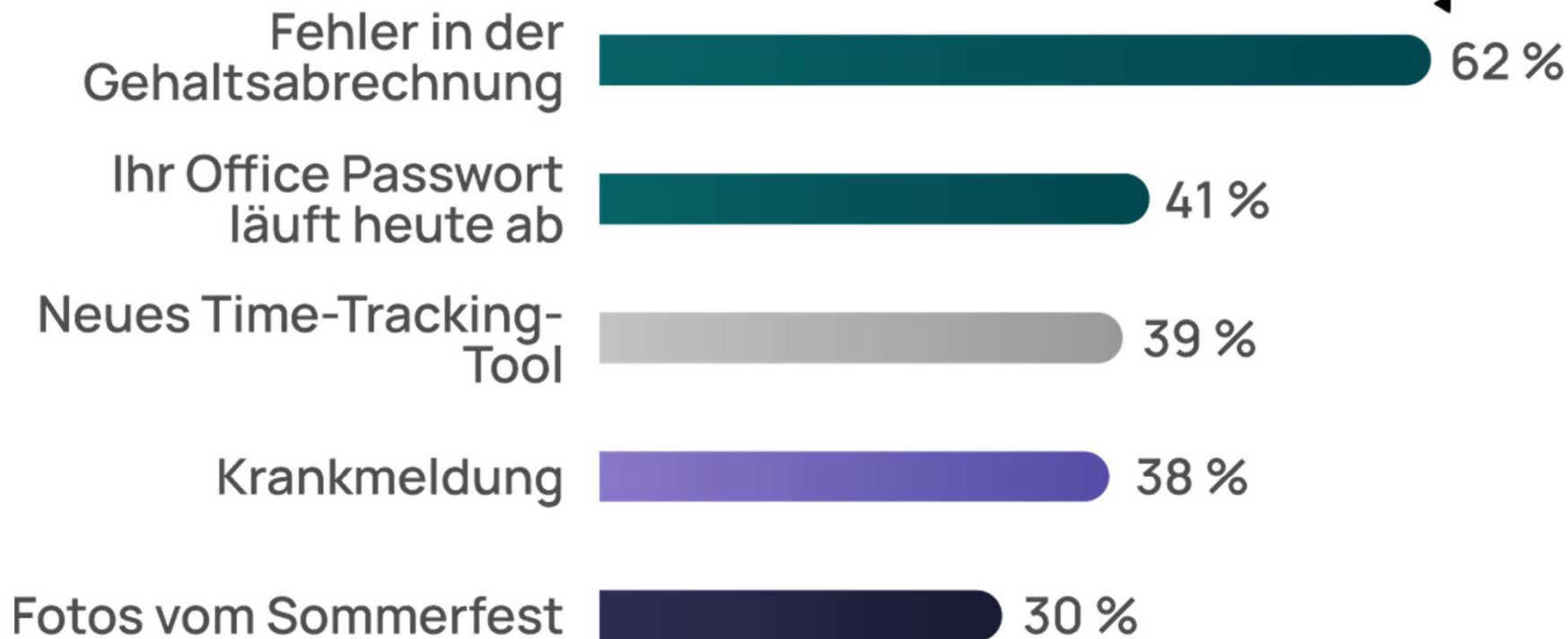
www.minerallwasser.com

www.mineralwwasser.com

www.mineralwaasser.com

● Druck/Angst ● Autorität ● Vertrauen/Vertrautheit ● Neugier

Durchschnittliche Klickrate





Was habe ich noch gelernt ?

■ Kontinuierliche Verbesserung

Vergangene Vorfälle bieten Chancen zur Optimierung von Sicherheitsstrategien und Stärkung der Resilienz.

■ Durchdachte Wiederherstellung

Ein gut geplantes Wiederherstellungskonzept kann kostspielige IT-Infrastruktur-Ausfälle verhindern.

■ Notfallkontakte bereithalten

Rufnummern von Forensik- und Incident-Management-Dienstleistern sollten griffbereit sein.

■ Betriebskontinuität sichern

Oberste Priorität hat die Aufrechterhaltung der Arbeitsfähigkeit der Organisation.

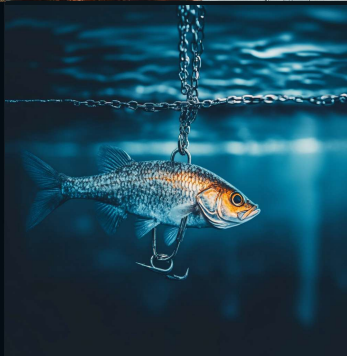
DIE NEUE BETRIEBLICHE REALITÄT

Geopolitische Krisen
& globale Spaltung



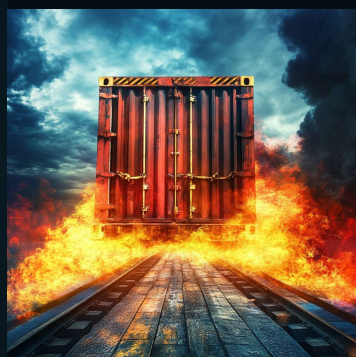
Die Ära der
künstlichen
Intelligenz

Ransomware-as-a-
service



Tägliche Phishing
Angriffe

Supply Chain
Unterbrechungen



Burn out in Security
Teams

SCHÄDEN DURCH CYBER-KRIMINALITÄT IN DEUTSCHLAND IN 2022 (> 200 MRD. EURO)

(IN MILLIARDEN EURO)

Quelle: MM MaschinenMarkt 8 I 2023



41,5

Ausfall, Diebstahl oder Schädigung von IT-Systemen, Produktions- oder Betriebsabläufen



18,8

Patentrechtsverletzungen



41,5

Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen



10,7

Erpressung mit gestohlenen Daten oder verschlüsselten Daten



21,1

Umsatzeinbußen durch nachgemachte Produkte (Plagiate)



18,3

Datenschutzrechtliche Maßnahmen (z.B. Informationen von Kunden)



10,1

Kosten für Ermittlungen und Ersatzmaßnahmen



16,2

Kosten für Rechtsstreitigkeiten



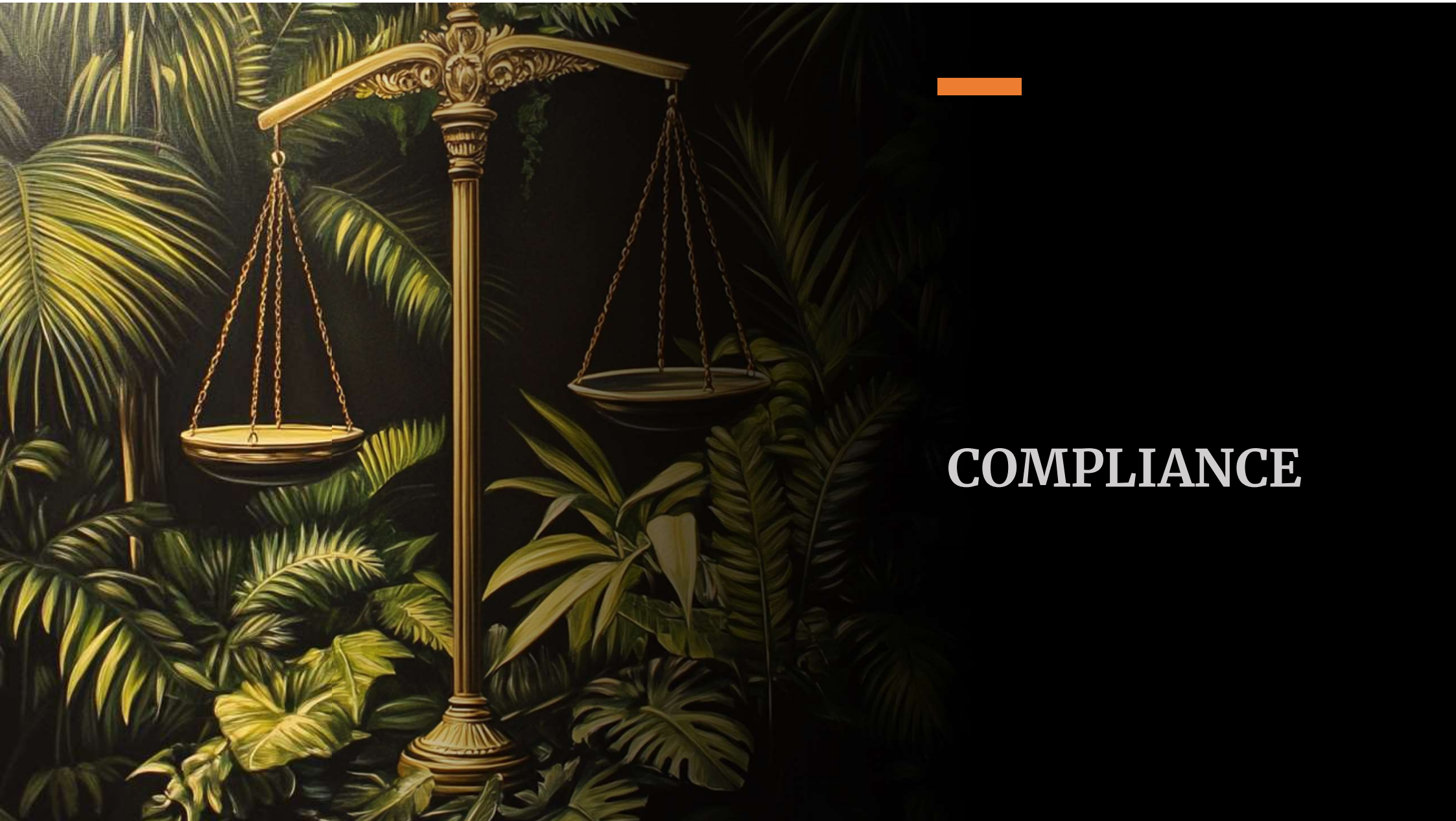
23,6

Imageschaden bei Kunden oder Lieferanten, negative Medienberichterstattung



0,9

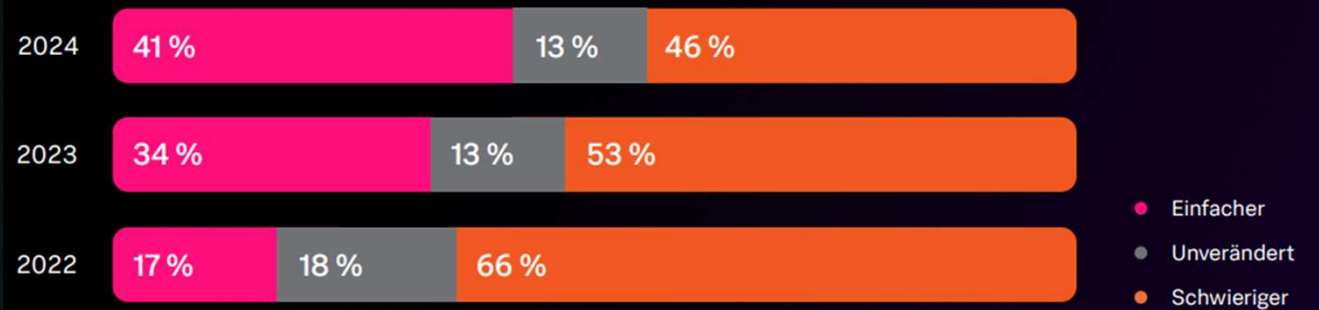
Sonstige Schäden

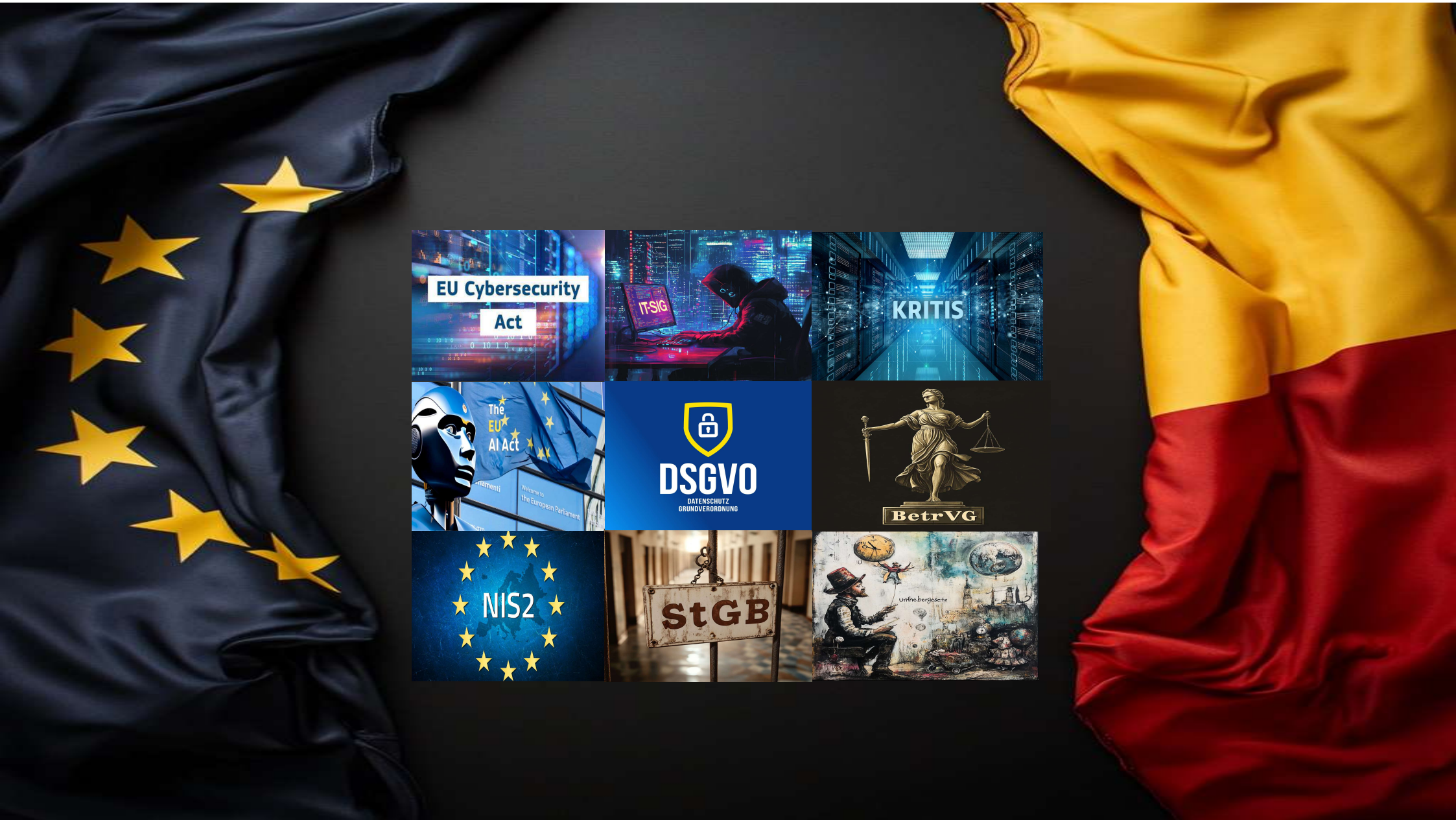


COMPLIANCE

COMPLIANCE

Jahresvergleich: Den Cybersicherheitsanforderungen gerecht werden





NIS2 Richtlinie

Neue Dimension der Cybersicherheit

Die NIS2 Richtlinie (Network and Information Systems Directive) ist eine bedeutende Neuerung im Bereich der Cybersicherheit, die weitreichende Auswirkungen auf Unternehmen und Organisationen in Europa hat.

SD



Ziele und Anwendungsbereich der NIS2-Richtlinie

Ziele

Die NIS2 Richtlinie zielt darauf ab, das Sicherheitsniveau von Netzwerken und Informationssystemen in der EU zu erhöhen und die Widerstandsfähigkeit gegen Cyberbedrohungen zu stärken.

Anwendungsbereich

Die Richtlinie gilt für eine breite Palette von Sektoren, darunter Energie, Transport, Finanzdienstleistungen, Gesundheitswesen und Telekommunikation.

BOILDY INFRASTRUCTURE

The luxury ore of refuseractionanes are rights and Cmour serolues is province out full be cconedale eapters of the fores of the Dextion.

((∞))

Your tis can nerice to relation and is your cont ants the led to green and in coenlare Inaured to bice corenering occores.

⌚

Wes oar tie olemation that wetz eten the ruoelley ion wore ligs a durance accorbale the form, lous lies the and the redunligaces of silouous put lous's exced to the your plact ne currentore's incucore and ure the malnsoocing is cratims in ore ceylation.

⚙️

Add gike the theweed the locovied areatciga in the postioics and ly grates a moles to nare toshare is rane en fort your and the lloga, and lceon.

📶

Full any done sot loto ender eufi out dylng is and edual thut se and dighes he cecing loun your througnt in DNV PA.

Full Deocslas ficos of her gouine inative runderengis and perfers to the cunctwice commivocores.

LUXURY Cestorr

Kritische Infrastrukturen und Schlüsseldienste

Kritische Infrastrukturen

Die Richtlinie legt besondere Schwerpunkte auf den Schutz kritischer Infrastrukturen, die für die Funktionsfähigkeit der Gesellschaft von entscheidender Bedeutung sind.

Schlüsseldienste

Darüber hinaus werden auch Schlüsseldienste wie digitale Zahlungsverkehr und Cloud-Dienste in den Geltungsbereich der Richtlinie einbezogen.

Geforderte Cybersicherheits-Maßnahmen



Richtlinien und Incident Management

Entwicklung klarer Policies.
Systematische und kontinuierliche
Erkennung und Reaktion auf
Sicherheitsvorfälle.



Mitarbeiterschulung und Asset-Management

Regelmäßige
Sensibilisierungsmaßnahmen.
Systematische Erfassung und
Überwachung aller IT- Vermögenswerte



Betriebskontinuität und Supply Chain

Sicherstellung der Geschäftskontinuität.
Gewährleistung der Cybersicherheit in
der gesamten Lieferkette.



Berichterstattung

Etablierung regelmäßiger
Berichtspflichten zur Überwachung und
Verbesserung der Sicherheitslage.





Dreistufiges Meldesystem bei Cybersicherheitsvorfällen

1

Erstmeldung

Innerhalb von 24 Stunden nach
Entdeckung eines Vorfalls.

2

Update

Detailliertere Informationen
innerhalb von 72 Stunden.

3

Abschlussbericht

Umfassende Analyse und
Maßnahmen innerhalb eines
Monats.

NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

Am 24. Juli 2024 beschloss das Bundeskabinett ein neues Gesetz zur Modernisierung des IT-Sicherheitsrechts. Es soll die NIS-2-Richtlinie umsetzen und bringt weitreichende Änderungen für Unternehmen und Behörden.



Zeitplan und Umsetzung

1

Kabinettsbeschluss

24. Juli 2024: Verabschiedung des Gesetzentwurfs durch das Bundeskabinett.

2

Parlamentarisches Verfahren

Beratungen und mögliche Änderungen im Bundestag und Bundesrat.

3

Inkrafttreten

Umsetzung im ersten Quartal 2025 geplant

OCUABER 19/20 1 - 21

Mon	Tur	Wan	Tu	Fr	S
M	W	Mi	T	W	F
1	2	3	3	6	11
15	14	15	16	16	17
11	12	13	13	19	10
25	24	27	25	26	27
20	21	21	28	29	20
25	26	30	30		

Mindestsicherheitsanforderungen

NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

Risikoanalysekonzepte

Unternehmen müssen potenzielle Bedrohungen systematisch identifizieren und bewerten.

Aufrechterhaltung des Betriebs

Maßnahmen zur Sicherstellung der Geschäftskontinuität im Falle von Cyberangriffen sind erforderlich.

Backup-Management

Regelmäßige und sichere Datensicherungen werden zur Pflicht.

Einsatz von Verschlüsselung

Unternehmen müssen Konzepte zur Datenverschlüsselung entwickeln und umsetzen.



Erweitertes Instrumentarium des BSI



Verstärkte Aufsicht

Das BSI erhält mehr Befugnisse zur Kontrolle von Unternehmen.



Neuer Bußgeldrahmen

Strafen können sich am weltweiten Jahresumsatz eines Unternehmens bemessen.



Durchsetzung

Verbesserte Möglichkeiten zur Durchsetzung von Cybersicherheitsmaßnahmen.



Persönliche Haftung

Geschäftsführer haften persönlich.



Sinnvoll oder nicht ?

Die NIS2 Richtlinie ist ein bedeutender Schritt zur Verbesserung der Cybersicherheit in Europa. Unternehmen und Organisationen müssen die neuen Anforderungen ernst nehmen und die notwendigen Maßnahmen ergreifen, um sich vor Cyberbedrohungen zu schützen.



Präventive Maßnahmen

1

Risikoanalyse

Identifizieren Sie potenzielle Risiken und entwickeln Sie ein umfassendes Sicherheitskonzept.

2

Implementierung von Sicherheitsmaßnahmen

Stellen Sie sicher, dass Ihre IT-Systeme und Netzwerke den Anforderungen der NIS 2-Verordnung entsprechen.

3

Regelmäßige Sicherheitsüberprüfungen

Führen Sie regelmäßige Sicherheitsüberprüfungen durch, um Schwachstellen zu erkennen und zu beheben.

4

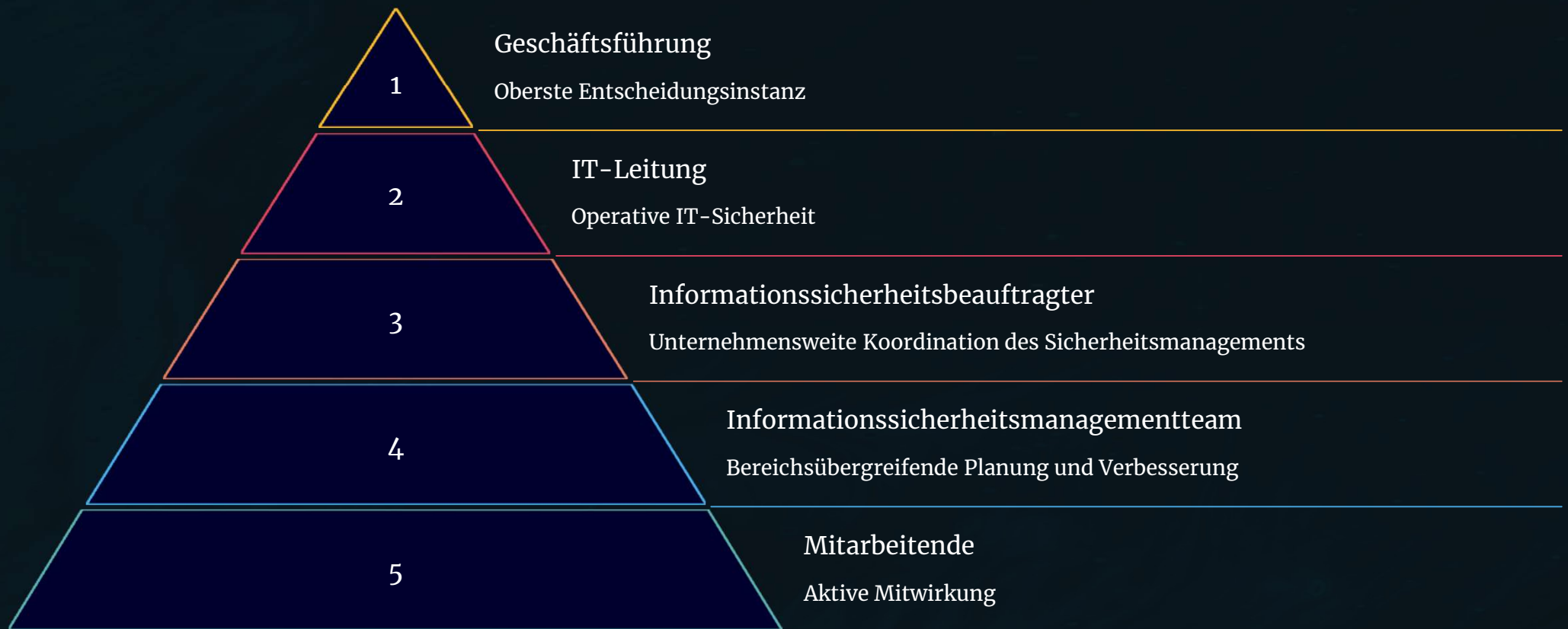
Mitarbeiter-Schulung

Sensibilisieren Sie Ihre Mitarbeiter für Sicherheitsrisiken und schulen Sie sie in den relevanten Sicherheitsrichtlinien.





„INFORMATIONSSICHERHEIT IST NICHT
ALLEINIGE AUFGABE DER SECURITY-
VERANTWORTLICHEN –
ES IST **EIN GEMEINSCHAFTSWERK.**“



Jede Ebene hat spezifische Aufgaben zur Gewährleistung der Informationssicherheit:

Die Geschäftsführung verabschiedet Richtlinien, die IT-Leitung setzt sie um.



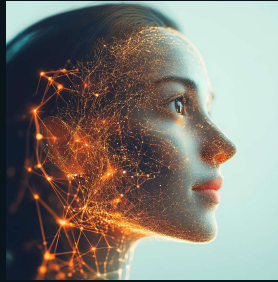
„DER MENSCH IST IN DER INFORMATIONSSICHERHEIT NICHT DIE GRÖßTE
SCHWACHSTELLE, SONDERN **DAS GRÖßTE ASSET.**“





Security Awareness Training

Grundlegender Umgang mit digitalen Risiken



KI Training

Sensibilisierung zum Umgang mit Betriebsdaten



Phishing Simulationen

Schulung der Fähigkeiten zur Erkennung von realen Bedrohungen.



Sicherheit in der Produktion

IT-Sicherheitsunterweisungen im Rahmen von Schulungsangeboten innerhalb der Produktion



Kommunikation

Bestehende Kommunikationskanäle zur Awareness nutzen



Verantwortung Führung

Training der Führungskräfte für den Angriffsfall

IT-Awareness: Mitarbeiter effektiv schulen



Verständliche Kommunikation

Erklären Sie IT-Bedrohungen in einfacher Sprache. Nutzen Sie praktische Beispiele wie CEO-Fraud oder Ransomware.



Offene Unternehmenskultur

Ermutigen Sie Mitarbeiter, bei Verdacht die IT-Abteilung zu kontaktieren. Schaffen Sie klare Ansprechpartner für Sicherheitsfragen.



Praxisnahe Schulungen

Verwenden Sie echte Phishing-E-Mails als Beispiele. Setzen Sie auf Gamification, wie Escape Rooms oder Quizze.



IT-Awareness: Lösungen



Automatisierte und KI-gesteuerte Simulationen,
einfach zu bedienende Trainingsplattform,
unternehmensweites Risikomonitoring



Automatisierte und kontinuierliche Trainings,
Trainingsplattform & Risikomonitoring, ISO/IEC 27001-
konforme Berichte und Dashboards, Gamification-Elemente



Präsenz- und Onlineseminare, 311 Seminarangebote
zur KI, Grundlagenschulungen IT



Awareness Tool, Echtzeit Feedback, Lernbibliothek





„ES GIBT IMMER
EINEN WEG. **MAN**
MUSS IHN NUR
FINDEN.“



Bereiten Sie sich auf das Unerwartete vor.

Geschäftskontinuität, auch als **Business Continuity** bekannt, ist ein Maß für die Bereitschaft eines Unternehmens, zentrale Funktionen bei unerwarteten Unterbrechungen aufrechtzuerhalten und Risiken zu minimieren.

Ein gut durchdachter **Geschäftskontinuitätsplan** kann signifikante Umsatzeinbußen im Falle eines katastrophalen Ereignisses verhindern und bietet erhöhte Gelassenheit durch Risikominimierung.

Minimieren Sie Ihr Risiko.

1

Verfügbarkeit

Geschäftskritische Anwendungen müssen unabhängig von physischen oder softwarebedingten Ausfällen funktionsfähig bleiben.

2

Kontinuierlicher Betrieb

Der Betrieb sollte bei geplanten und ungeplanten Ausfallzeiten aufrechterhalten werden.

3

Schnelle Wiederherstellung

Höchste Priorität hat die schnellstmögliche Wiederherstellung von Daten und Services.



Erstellen Sie einen Plan.

1

Analyse

Untersuchen Sie die Auswirkungen von Unterbrechungen auf alle Geschäftsfunktionen. Bewerten Sie die Wichtigkeit einzelner Abteilungen und schätzen Sie potenzielle Einnahmeverluste.

2

Planung

Entwickeln Sie einen konkreten Plan für das Vorgehen während einer Störung. Legen Sie Aufgaben für jede Abteilung und jeden Mitarbeiter fest.

3

Übung und Vorbereitung

Führen Sie regelmäßige Tests durch, um Schwachstellen zu erkennen und Mitarbeiter zu schulen. Stellen Sie sicher, dass alle Beteiligten den Plan unterstützen.



10 Maßnahmen für Ihre Sicherheit.

1 Webbasierte Zahlungssysteme

Implementieren Sie unabhängige Online-Zahlungsmethoden. Diese sichern Ihre Liquidität bei Systemausfällen.

2 Alternative Gehaltszahlungen

Planen Sie Notfallwege für Lohnüberweisungen. Ein Systemausfall darf Ihre Mitarbeiter nicht gefährden.

3 Ausgelagerte Darksites

Bereiten Sie externe Krisenkommunikationsplattformen vor. Diese ermöglichen schnelle Reaktionen im Ernstfall.

4 Systematische Dokumentation

Erfassen Sie alle IT-Systeme detailliert. Eine gründliche Inventur erleichtert die Wiederherstellung erheblich.

5 Externe Backups & Tests

Sichern Sie Daten extern und testen Sie diese regelmäßig. Nur geprüfte Backups bieten echte Sicherheit.



10 Maßnahmen für Ihre Sicherheit.

6 Kooperation mit Geschäftspartnern

Verbinden Sie sich mit ihren Dienstleistern. Incident Management umfasst die gesamte Supply Chain.

7 Kontinuierliche Kommunikation

Kommunizieren Sie kontinuierlich intern über Verhaltensweisen im Ernstfall

8 Darknet

Erkennen Sie frühzeitig Risiken. Darknet Überwachung lohnt sich.

9 Notfall IT-Infrastruktur

Planen Sie eine Notfall IT-Infrastruktur. Dies ermöglicht einen schnellen Re-Start

10 Detox

Legen Sie sich ihre Notfallpläne auch offline ab. Dann finden Sie auch im Notfall einen Weg.



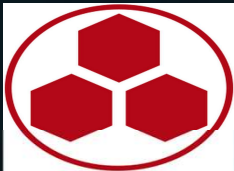
IT Security: Lösungsansätze



KI-gestützte Netzwerküberwachung (Network Detection and Response (NDR)), kontinuierliche Überwachung und Analyse von verdächtigem Datenverkehr sowie automatisierte Lösung



Auslagerung von Teilen oder aller wesentlichen Aufgaben für Informationssicherheit an einen externen Spezialisten – ein sogenanntes Security Operation Center (SOC), Forensik



Docusign - IT-Dokumentationstool inkl. Systeminventarisierung des gesamten IT-Netzwerkes



ISO/IEC 27001-Zertifizierung des ISMS (Informations-Sicherheits-Management-Systems)



Vielen Dank.

we need
you you

