NETUNITY

Vier Blickwinkel. Eine Stunde Klartext zu IT-Security & NIS2.

WEBINAR | ALLIANZ DIGITALER INNOVATOREN

11. September 2025

AGENDA

01 Herzlich Willkommen
Tim Voigt | NETUNITY

02 Informationssicherheit
Status, Defizite & Verantwortung
Ulf Lorenzen | VaterIT

03 IT-Sicherheit strukturiert denken
Sebastian Eich | hanseConcept

04 Schwachstellenscan & Pentest
Angriffspunkte erkennen
Carsten Hinz | HOCH.REIN IT

05 NIS2 & Künstliche Intelligenz
Pflicht oder Chance?
Peter Kluge | VaterIT

06 Q&A Session
Tim Voigt & Experten | NETUNITY

07 Anhang Kontaktdaten
aller Experten & Referenten

NETUNITY
ALLIANZ DIGITALER INNOVATOR:INNEN

Wir entwickeln, implementieren und betreiben innovative, wertstiftende und benutzerfreundliche Technologien für KMU und den öffentlichen Sektor.

Unsere Allianz vereint die Stärke etablierter Unternehmen mit der Dynamik von Start-ups, um maßgeschneiderte, innovative Lösungen anzubieten – alles aus einer Hand.

Gemeinsam entfesseln wir Potenziale für exklusive Geschäftsmöglichkeiten und Ihren Erfolg.

400 +

Expert*innen,* die ihr umfangreiches Wissen und ihre Fähigkeiten bündeln

> 4.000

erfolgreiche Tech-Gründungen & Digitalisierungsprojekte

10 +

Standorte in Deutschland

3

Büros Hamburg I Flensburg I Rostock

UNSERE REFRENTEN

ULF LORENZEN

Geschäftsführung,
Beratung & IT-Strategie

Vater Solution GmbH

SEBASTIAN EICH

Geschäftsführung,
Cloud Transformation &
Microsoft 365

hanseConcept GmbH

CARSTEN HINZ

Director Sales,
Schwachstellenanalyse
& Netzwerksicherheit

HOCH.REIN IT Solutions GmbH

PETER KLUGE

Datenschutz &
Informationssicherheit

Vater Solution GmbH

vater
IT

INFORMATIONS-SICHERHEIT

STATUS
DEFIZITE
VERANTWORTUNG

ULF LORENZEN

Geschäftsführung, Beratung & IT-Strategie

Vater Solution GmbH
ulorenzen@vater-gruppe.de
vater-it.de

Definitionen

Informationssicherheit

…ist der Prozess einer Organisation, der sicherstellt, dass **Geschäftswerte** (analoge und digitale Informationen) **vor Bedrohungen stets angemessen geschützt** werden.

IT-Sicherheit

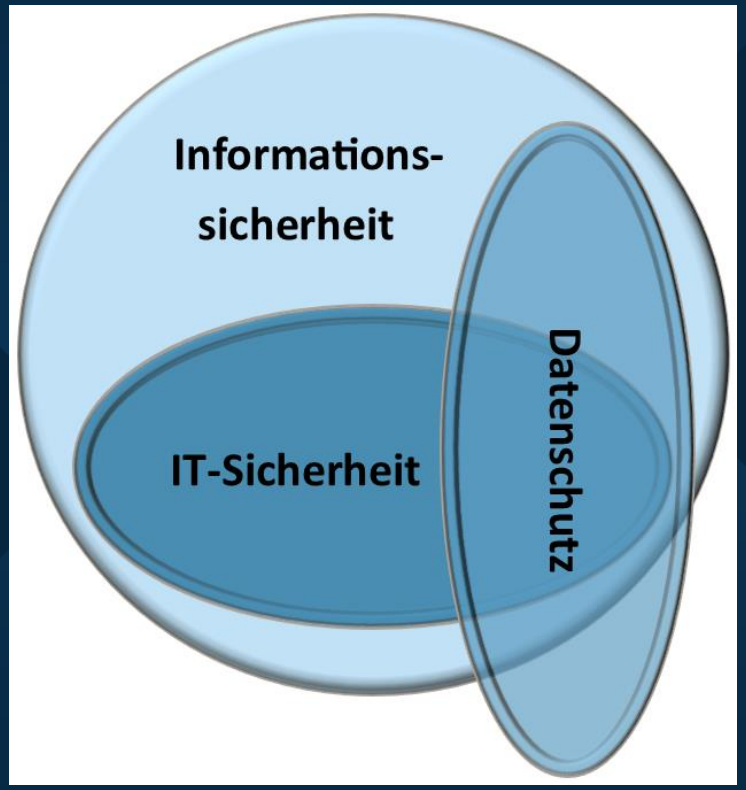
…ist die **technische Sicherheit** von informationsverarbeitenden Anlagen.

Datenschutz

…ist der Prozess, der sicherstellt, dass Personen vor der **Beeinträchtigung ihres Persönlichkeitsrechts** durch den **Umgang mit personenbezogenen Daten** stets angemessen geschützt wird.

Information

…ist unabhängig vom Medium, auf dem sie transportiert wird. Information kann also auch eine mündliche oder auf Papier übermittelte Nachricht sein.



Gefährdungslage

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) sieht

- eine **„besorgniserregende IT-Sicherheitslage“ mit „rasanter Entwicklung“**
- eine **„Zunahme der digitalen Angriffsflächen“** mit Schwachstellen die oft **„gravierende Eingriffsmöglichkeiten“** bieten

Angriffe werden dabei **professioneller**, sind oft arbeitsteilig **organisiert** und werden weitestgehend automatisiert durchgeführt

Handel mit erbeuteten Zugangsdaten **(Access Broker)** – mit und ohne Verschlüsselung

Stark gestiegene Zahl an **DDoS-Attacken**

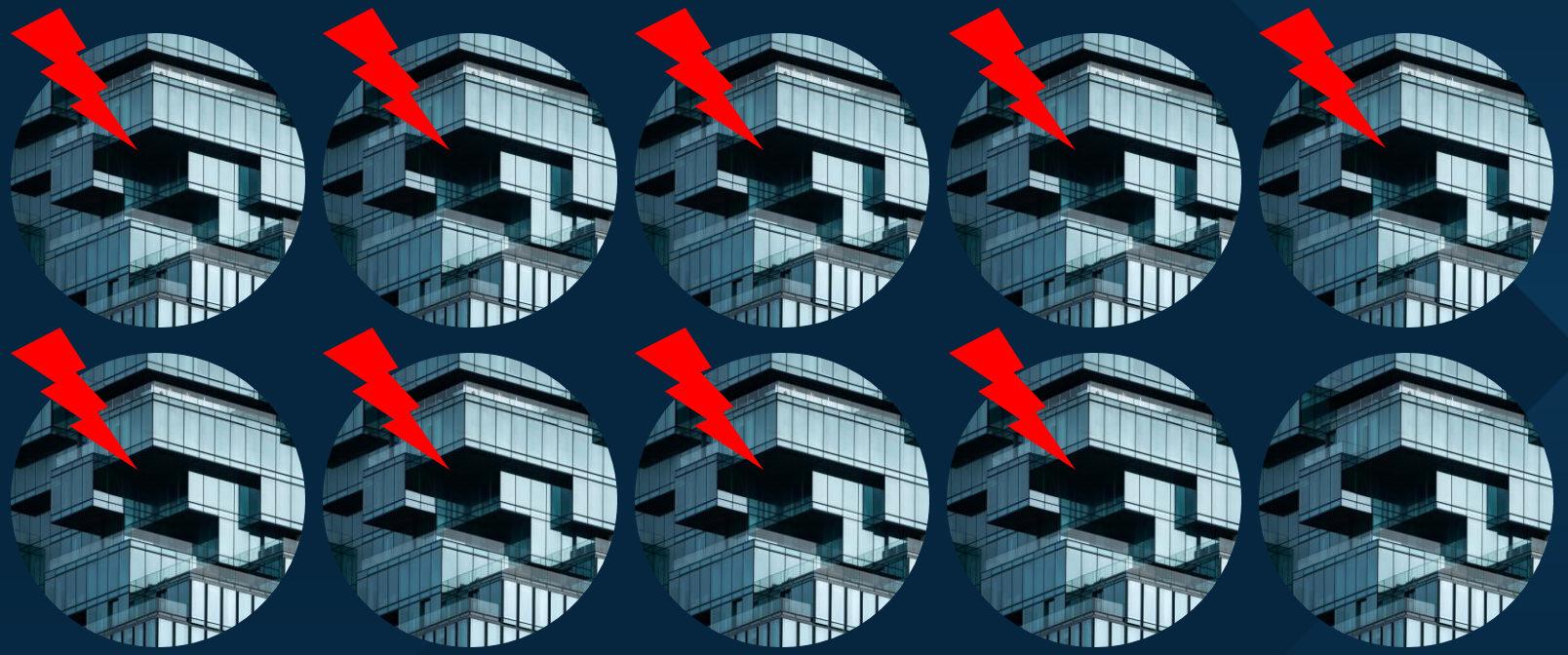
Ransomware-Angriffe nun auch häufig gegen kleine und mittlere Unternehmen

Schadwirkungen waren im Berichtszeitraum (2024) beträchtlich
(Ausfall- und Wiederanlaufzeiten sowie -kosten, Lösegeldzahlungen, Reputationsverluste usw.
→ 148 Mrd. EUR Schaden durch Cyberangriffe für deutsche Unternehmen)

Quelle der Daten: BSI → Lage der IT-Sicherheit in Deutschland 2024

Gefährdungslage

9 von 10 Unternehmen in Deutschland sind innerhalb der letzten 12 Monate von Cyber-Attacken betroffen gewesen



Quelle der Daten: BITKOM© -Studie, es wurden 1000 Unternehmen in Deutschland befragt

Gefährdungslage

82% der erfolgreichen Angriffe werden **durch menschliches Zutun** ermöglicht, **nicht durch die Technik**

Social Engineering
Bedienfehler
Missbrauch

Quelle der Daten: Verizon© "Data Breach Investigations Report" aus 2022

Gefährdungslage

69% aller Spam-E-Mails waren Cyber-Angriffe wie zum Beispiel Phishing E-Mails und E-Mail-Erpressung

Quelle der Daten: BSI -Lagebericht 2022

Gefährdungslage

Zusammenfassung

- die Bedrohungslage ist laut BSI besorgniserregend
- **90%** der befragten Unternehmen waren schon betroffen
- rein technische Abwehrmaßnahmen bieten **keinen** ausreichenden Schutz
- **der Faktor Mensch** ist mit die größte Schwachstelle

Fazit

- je wachsamer die Belegschaft für Risiken und Bedrohungen ist,
- je besser sie die Maßnahmen zur Abwehr der Angriffe beherrschen,
- umso erfolgreicher können Cyberangriffe abgewehrt werden.

Es ist nicht mehr die Frage ob man angegriffen wird, sondern nur noch die Frage, wann man erfolgreich angegriffen wurde!

Verantwortung

Cyberangriff verursacht Kosten und Schäden

- Feststellung der Ursache (Forensik)
- Wiederherstellung von Daten und Systemen
- Umsatzeinbußen (Kundenvertrauen, Produktionsausfälle, Wertverlust)
- Schadenersatzzahlungen an Dritte (Art. 82 DSGVO, §280 BGB)

Haftung

- IT muss nach Stand der Technik betrieben werden (Art. 24 I und II DSGVO)
- Einhaltung von Gesetzen (DSGVO, NIS-2, CRA usw.)
- Konsequenzen treffen immer den Geschäftsführer
- Unternehmen muss Schutzmaßnahmen nachweisen (Dokumentationen)
- Rückgriff auf Mitarbeiter kaum erfolgversprechend

Informationssicherheit als Teil der Geschäftsstrategie

… und damit in der Verantwortung des Managements

- Einhaltung von Gesetzen (KRITIS, NIS-2, CRA, CSA usw.)
- Vertragliche Regelungen bzw. Ausschreibungen (z.B. Nachweis ISMS)
- Bestandteil einer Lieferkette
- Reputation, Wettbewerbsvorteil
- Schaffung einer sicherheitssensiblen Unternehmenskultur
- Dokumentierte Erkenntnisse hinsichtlich Werten und Risiken
  → gezielte Investitionen in Informationssicherheit
- Optimierung von Geschäftsprozessen

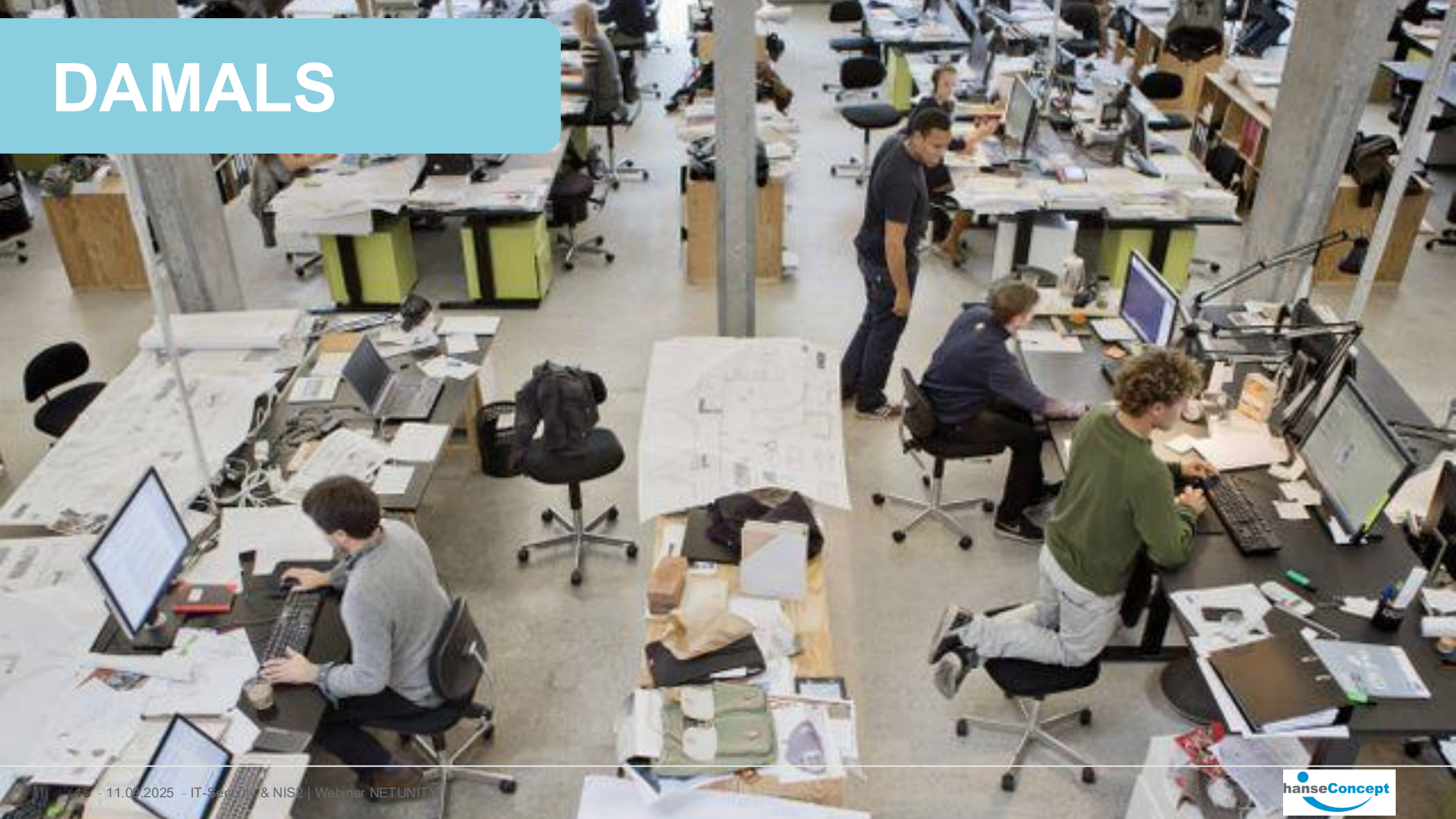
IT-SICHERHEIT

STRUKTURIERT DENKEN!

SEBASTIAN EICH
Geschäftsführung, Cloud Transformation & Microsoft 365

hanseConcept GmbH
sebastian.eich@hanseconcept.de
hanseconcept.de

DAMALS



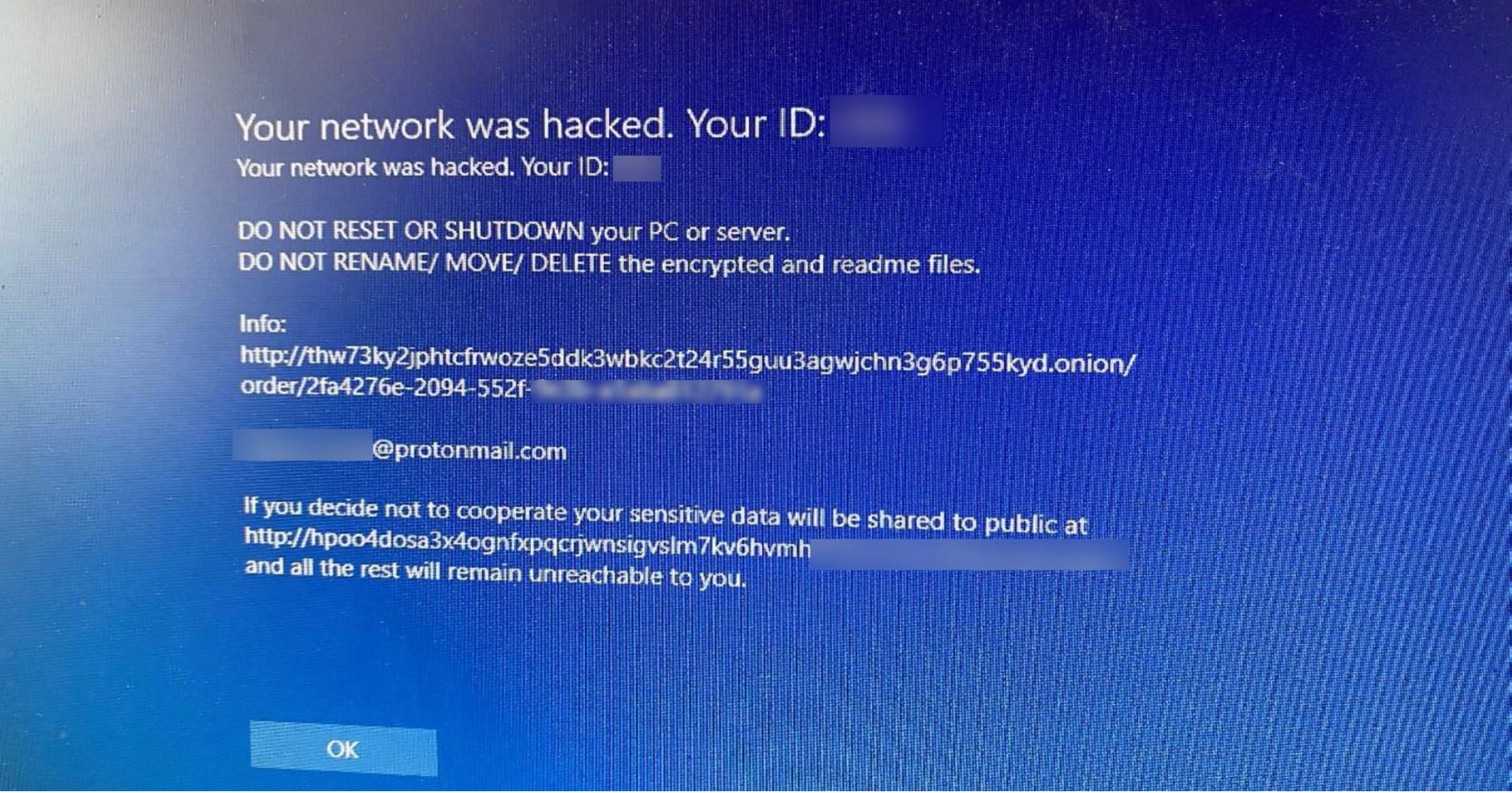
HEUTE

CYBERCRIME
LAGEBERICHT

Quelle: https://sosafe-awareness.com/

Herausforderungen für Unternehmen

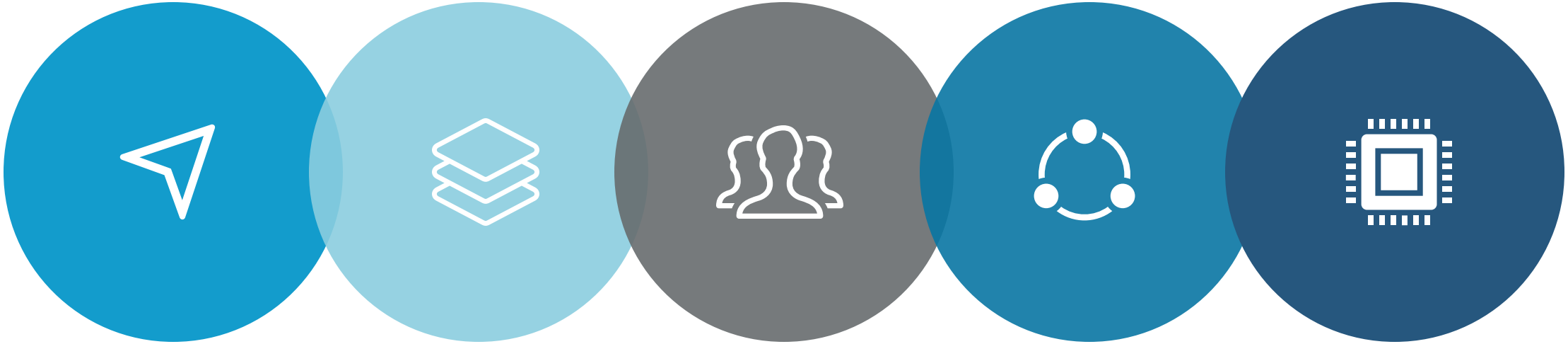
- Sensibilisierung aller Mitarbeiter
  - insbesondere Führungskräfte und Administratoren!
- Auskömmliche Budgets für Verteidigung und Risikomanagement
- Erkennungs- und Reaktionsgeschwindigkeit
- Fachexpertise in Cybersecurity
- Notfallplanung mit Cyberrisiko-Szenarien
- Ganzheitliche Sicherheitsarchitektur


Your network was hacked. Your ID:
Your network was hacked. Your ID:
DO NOT RESET OR SHUTDOWN your PC or server.
DO NOT RENAME/ MOVE/ DELETE the encrypted and readme files.
Info:
http://thw73ky2jphtcfrwoze5ddk3wbkc2t24r55guu3agwjchn3g6p755kyd.onion/
order/2fa4276e-2094-552f-
@protonmail.com
If you decide not to cooperate your sensitive data will be shared to public at
http://hpoo4dosa3x4ognfxpqcrjwnsigvslm7kv6hvmh
and all the rest will remain unreachable to you.
OK

Ganzheitliche

SICHERHEITSARCHITEKTUR

VERTEIDIGUNG
SICHERHEITSARCHITEKTUR



Ziele

Unternehmensziele
IT-Sicherheitsstrategie

Governance

Strukturen und Gremien,
BIA & Schutzbedarf,
Risikomanagement
ISMS

Menschen

Training
Sensibilisierung
Bewusstsein

Prozesse

Asset Management,
Identity- & Access-Management
Notfallmanagement
Incident Response…

Technologie

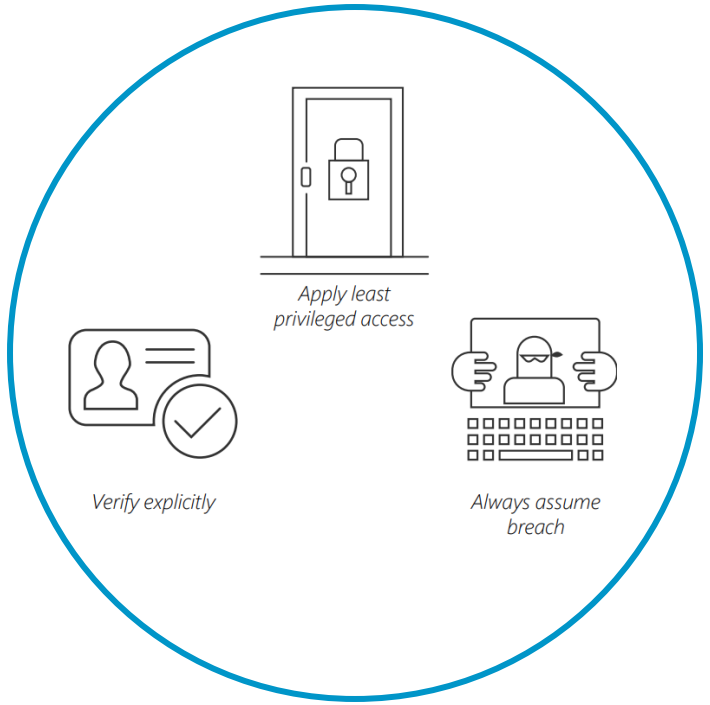
Security Monitoring, XDR,
SIEM, MFA, PIM, PAM,
Endpoint Security, IDS/IPS,
Verschlüsselung, DLP…

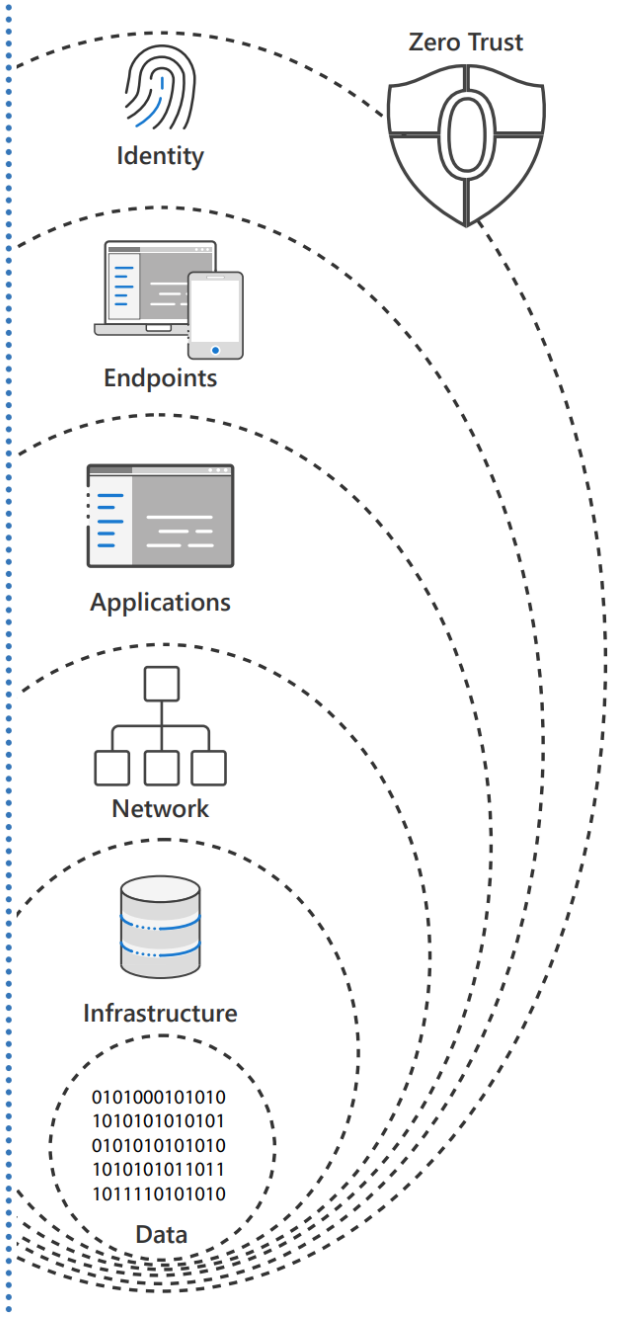
Never trust, always verify!

Zero Trust

ZERO TRUST
Grundsätze

- Jeden Zugriff explizit überprüfen, Authentifizierung und Autorisierung basierend auf allen verfügbaren Datenpunkten
- Immer von einer Sicherheitsverletzung ausgehen >> Sicherheitsvorfall
- Zugriff nur nach dem Minimalprinzip, zeitlich begrenzt, rollenbasiert, „just in time“ & „just enough access“





hanseConcept

HOCH REIN IT SOLUTIONS

SCHWACH-STELLENSCAN & PENTEST

ANGRIFFSPUNKTE ERKENNEN

CARSTEN HINZ
Director Sales, Schwachstellenanalyse & Netzwerksicherheit

HOCH.REIN IT Solutions GmbH
carsten.hinz@hoch-rein.com
it.hoch-rein.com

Wer ist „Hoch.rein IT Solutions“

Von der internen IT-Abteilung zum weltweit agierenden Full Service Provider.

2001 Eigenständige IT-Abteilung der BELECTRIC

2006 Ausbau zum Shared Service der HOCH.REIN GROUP

2017 Gründung der HOCH.REIN IT Solutions als eigenständige Unternehmung

Ausbau des ERP-Bereichs mit der Erweiterung auf Alphaplan, Sage und später Navision.

2019 Weltweit agierender Full Service IT-Provider für den Mittelstand

Wachstum – Erweiterung des Geschäfts um Kunden außerhalb der HOCH.REIN Organisation.

Was wir nicht wollen…

…uns aber leider passieren kann:

SITUATION:

Montag 9:30Uhr

nach einem

langen Wochenende

```
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorythm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

        DO NOT RESET OR SHUTDOWN - files may be damaged.
        DO NOT RENAME OR MOVE the encrypted and readme files.
        DO NOT DELETE readme files.
        DO NOT use any recovery software with restoring files overwriting encrypted.
        This may lead to the impossibility of recovery of the certain files.


To get info (decrypt your files) contact us at your personal page:

        1. Download and install Tor Browser: https://www.torproject.org/download/
        2. After a successful installation, run the browser and wait for initialization.
        3. Type in the address bar:

                        REDACTED

        4. Follow the instructions on the site
        5. You should get in contact in 48 HOURS since your systems been infected.
        6. The link above is valid for 7 days.
           After that period if you not get in contact
           your local data would be lost completely.



The faster you get in contact - the lower price you can expect.

DATA
AQAAAD0BAgAAEGYAAACkAAAVZbpNets6EP1bQXd7Gb8IcODGmeKDm5FmsMelp/RYzI0ljRcE2tH4
jZ2CksvKFzlBulRwa7P5l6dvX5VhxEHyj0TeLTwSFpIsBbJyRHNbl/G6biex/0RKKmkCkJ9gqIvi
vy8o9Ulz2c6jdeqr+ViaYpYYODwOwCa2AJsolFYqJ4B9ek7TCOBdjNKMSAyBz+M5gQrlNeOmYgGs
itXGyCwiwTN3rGDdXFINkSTRw1mM3bg6D8gxOHUnfbjIi1VA3ikHO3ORs/9kQ0CliOfF32owhwLQ
iE66ds59Dq/aSby/3RKuFrPSatuwf6TqLhXTKn6CnCqT1fNJY0dlzZiMxJSV
```

LAGEBILD DEUTSCHLAND 2024 (BSI)

Ransomware-as-a-Service (RaaS): Durch die Verfügbarkeit von RaaS-Angeboten ist der technologische Aufwand für Angreifer deutlich gesunken, wodurch Ransomware-Angriffe zum "Massengeschäft" geworden sind.

Weg des geringsten Widerstands: Cyberkriminelle suchen sich gezielt leicht angreifbare Ziele. KMU sind aufgrund ihrer oft schwächeren Sicherheitsmaßnahmen besonders gefährdet.

Begrenzte Ressourcen: KMU verfügen häufig über ein niedrigeres Budget für Cybersicherheit und haben das Thema generell nicht ausreichend auf der Management-Agenda.

78 neue Schwachstellen werden täglich bekannt

Ransomware-Angriffe betreffen zunehmend nicht nur Großunternehmen, sondern durch Ransomware-as-a-Service auch KMU, Kommunen und Forschungseinrichtungen13% der DDoS-Angriffe sind hochvoluminös (>10.000 Mbit/s) - mehr als doppelt so viel wie im langjährigen Durchschnitt.

18 Meldungen über Zero-Day-Schwachstellen deutscher Hersteller erreichen das BSI monatlich

1. FALLE

DIE UNSICHTBARKEIT DER BEDROHUNG

2. FALLE

DIE FEHLENDE EMOTIONALE ERFAHRUNG

3. FALLE

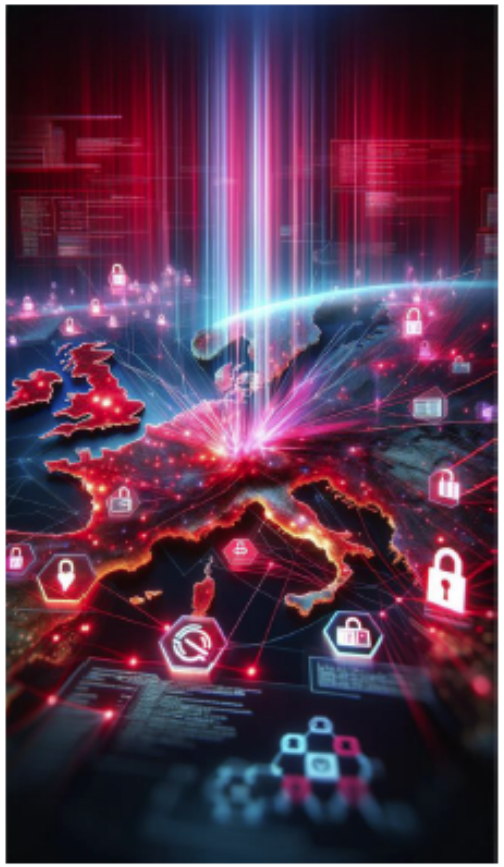
DER OPTIMISMUS DER ERFOLGREICHEN

4. FALLE

VERANTWORTUNG ABGEBEN

Herausforderungen

Vorsorge ist besser als Nachsicht



zu viele Insel-Tools

menschlicher Faktor

Übersicht behalten

andere Prioritäten

aufwändiges Reporting

fehlende Ressourcen

Reputation

Betriebskontinuität gewährleisten

Haftung

steigende Angriffszahlen

fehlende Automatisierungen

Risikominimierung

IT-Hygiene

Schwachstellen proaktiv schließen

Vorgaben der Cyberversicherung

Sicherheit hinter der Firewall

Compliance

DORA

TISAX

NIS-2 Direktive

DSGVO

KRITIS

ISO & VDS

Pentest HITS - Vektoren

Der automatisierte Pentest von HITS besteht aus vier Elementen:

Information Gathering: Durch Basis und Deep Scans erstellen unsere Tools ein Footprinting der Anwendungsumgebung.

CVE-Scan: Die ermittelten Anwendungen untersuchen wir automatisiert auf bekannte Sicherheitslücken.

Service Bruteforce: Durch das automatisierte ausprobieren von Benutzer-Passwort-Kombinationen werden unsichere Login-Daten aufgedeckt.

Service Discovery: Spezielle Checks z.B. der Verschlüsselung, Authentifizierung und Privilegien bestimmter Services decken sicherheitsrelevante Konfigurationsmängel auf

Die Hoch.rein IT Solutions GmbH ermittelt automatisiert, welche Tests für das jeweilige Zielsystem herangezogen werden müssen.

Pentest HITS

Sie erhalten :

- Infos zum aktuellen Sicherheitszustand Ihrer IT
- Funktionscheck Ihrer vorhandenen Security-Tools und -Maßnahmen
- Report inklusive Handlungsempfehlungen
- Oberflächen- und Tiefenscans (Penetrationstest) im definierten Test-Set
- Schwachstellenscan und Auswertung des Netzwerkverkehrs
- Angriffssimulation auf Ihre IT-Umgebung von außen und von innen
- Zustandsanalyse von Server und Clients
- Analyse des Sicherheitszustandes vorhandener Webanwendungen
- Service Discovery - Spezielle Checks zur Verschlüsselung, Authentifizierung und Privilegien bestimmter Services decken sicherheitsrelevante Konfigurationsmängel auf

Beispiel einer Liste für Schwachstellen Scan

■ Kompakte Checkliste: Netzwerk-Schwachstellenscan

■	Aufgabe
	1. Vorbereitung
■	Scope festlegen: Welche Systeme, Subnetze, IPs gehören dazu?
■	Ausschlüsse definieren: Systeme, die nicht gescannt werden sollen.
■	Freigabe einholen: Schriftliche Genehmigung von Management/IT-Leitung.
■	Ziel(e) des Scans definieren: Extern, intern, Compliance, Patchstand etc.
■	Risikobewertung im Vorfeld: Mögliche Störungen oder Ausfälle berücksichtigen.
	2. Scanner & Konfiguration
■	Scanner auswählen: z. B. Nessus, OpenVAS, Qualys, Rapid7.
■	Signaturen/Plugins aktualisieren: Aktueller Stand der CVEs erforderlich.
■	Art des Scans festlegen: Unauthentifiziert oder Authentifiziert.
■	Scan-Tiefe anpassen: Ports, Protokolle, Dienste.
■	Leistung berücksichtigen: Scans auf kritischen Systemen möglichst in Wartungsfenstern.
	3. Durchführung
■	Testlauf starten (Pilot-Scan auf kleinem Bereich).
■	Vollständigen Scan durchführen.
■	Protokollieren: Datum, Uhrzeit, Zielsysteme, Scanner-Version.
	4. Auswertung
■	Ergebnisse analysieren: CVSS-Scores, Kritikalität.
■	False Positives prüfen.
■	Systemkritikalität berücksichtigen (Server vs. Testsystem).
■	Bericht erstellen: technisch (für Admins) & Management-tauglich.
	5. Maßnahmenplanung
■	Quick Wins identifizieren (leichte Fixes, z. B. fehlende Patches).
■	Remediation-Plan erstellen: Patchmanagement, Konfigurationsänderungen.
■	Verantwortlichkeiten festlegen (wer fixt was, bis wann).
	6. Nachbereitung & Kontinuität
■	Re-Scan durchführen (Überprüfung der umgesetzten Maßnahmen).
■	Regelmäßige Scans einplanen (z. B. monatlich, nach jedem größeren Update).
■	Integration ins Security-Programm: Vulnerability Management, Incident Response.
■	Lessons Learned dokumentieren.

NIS2 & Künstliche Intelligenz

Wie moderne Technik Regulatorik unterstützen kann

PETER KLUGE
Head of Information Security & Cybersecurity

Vater Solution GmbH
pkluge@vater-gruppe.de
vater-it.de

NIS2 & KI – Pflicht oder Chance?

NIS2 & KI – Pflicht oder Chance?

Wie moderne Technologien helfen können, regulatorische Anforderungen pragmatisch umzusetzen.

NIS2 = neue EU-Sicherheitsanforderungen

Management trägt die Verantwortung

Pflicht → Chance

KI als Hebel: von Pflicht zur Chance

Verantwortung, Nachweise, Resilienz

Rolle der KI in der Praxis

KI & NIS2 — Chancen nutzen, Risiken steuern

Chancen

- Tempo & Skalierung
- Bessere Priorisierung
- Nachweisfähigkeit

Risiken

- Datenqualität & Bias
- KI-Halluzinationen
- Datenschutz
- Lieferantenabhängigkeit

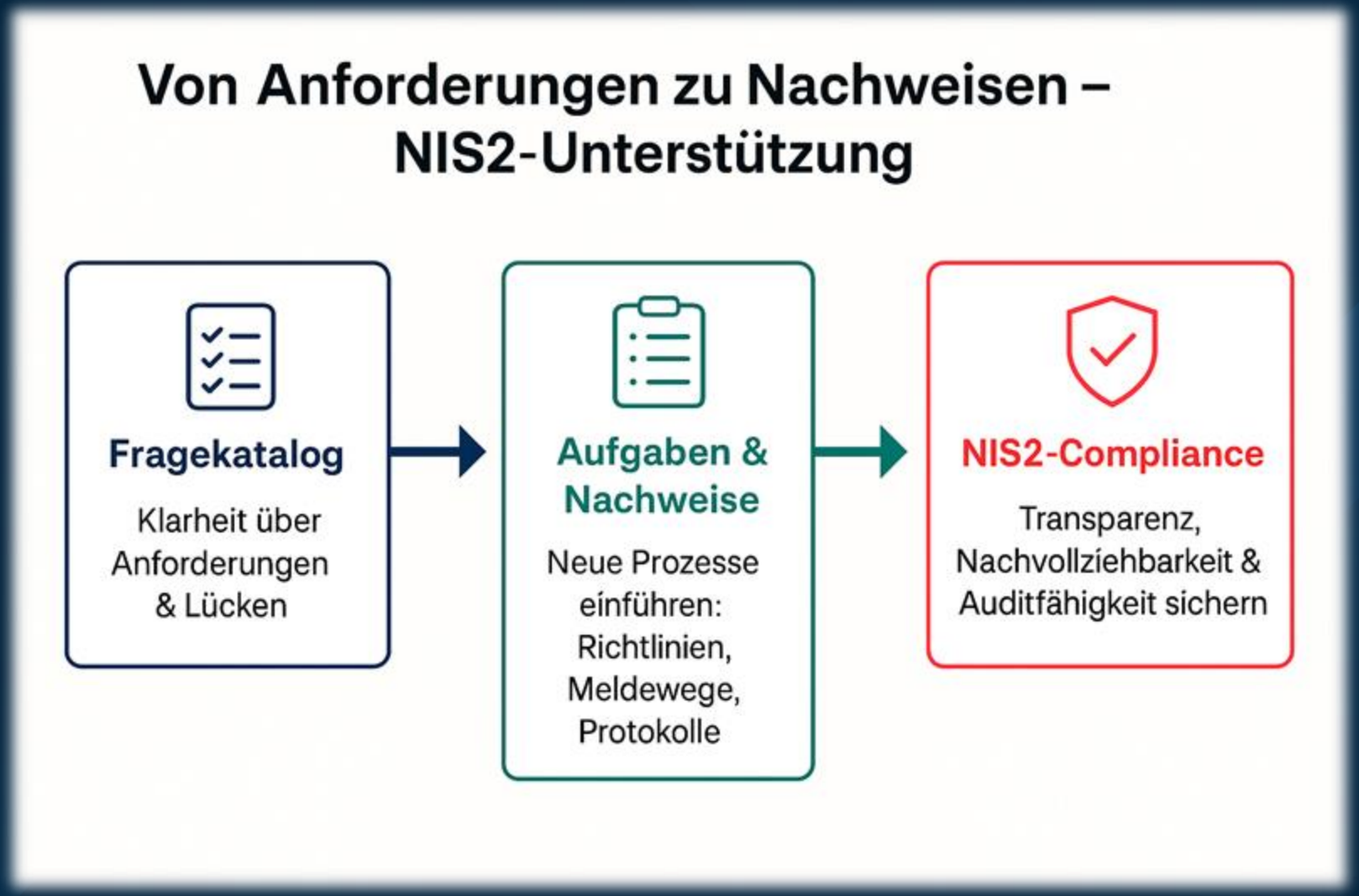
Hebel statt Autopilot: Kontrollen & Verantwortung bleiben beim Management.

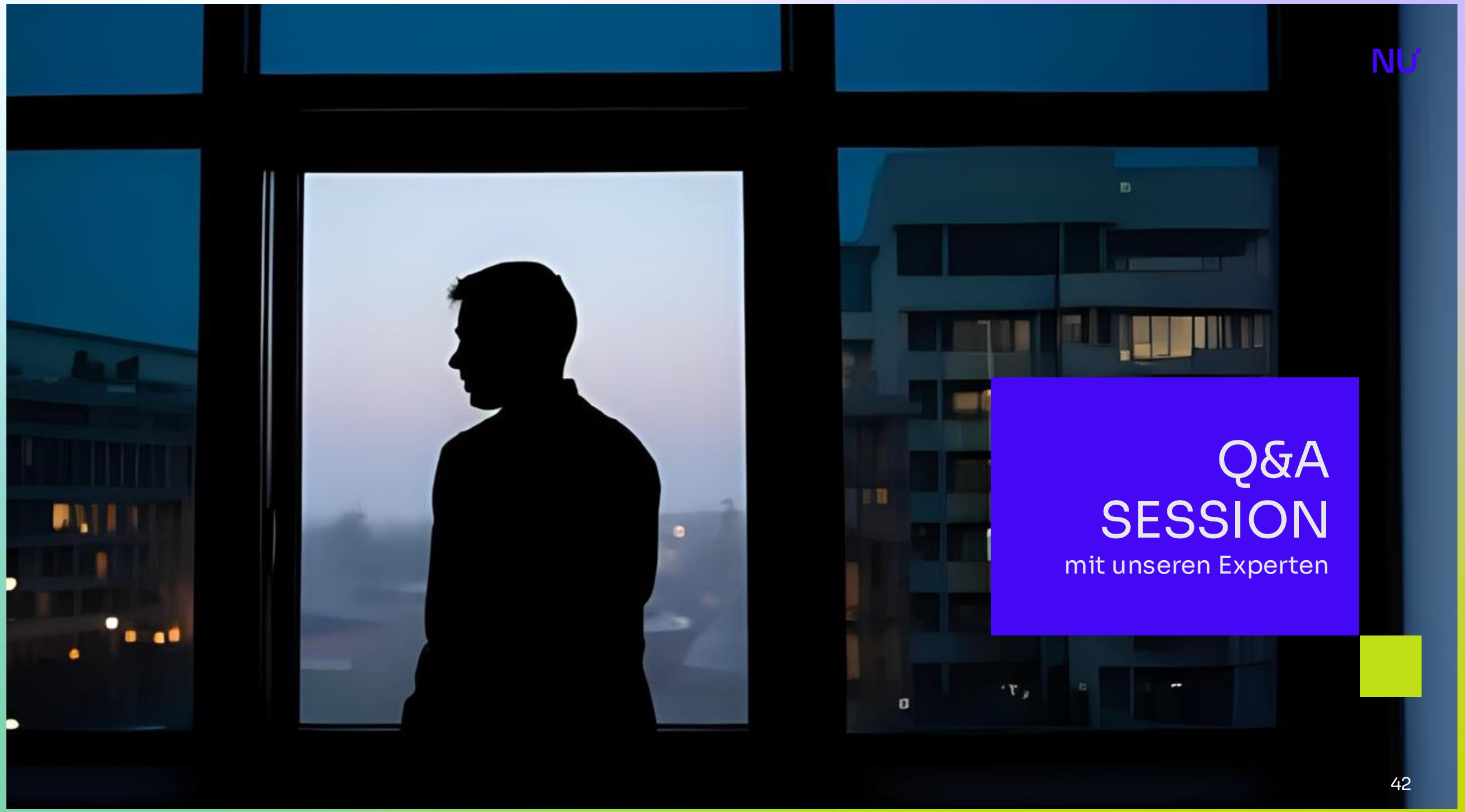
NIS2 & KI – Pflicht oder Chance?

- Chancen (Business-Nutzen)
- Risiken (realistisch)
- Kontrollen & Governance

- Essenz
- KI = Hebel, kein Autopilot.
- Verantwortung bleibt beim Management.

Empfehlungen für den Einstieg





Q&A SESSION

mit unseren Experten

NETUNITY

ALLIANZ DIGITALER INNOVATOREN

Lassen Sie uns gemeinsam Lösungen für Ihre Herausforderungen finden!

TIM VOIGT
Leitung IT-Projekte &
Business Development

tim.voigt@netunity.de

NETUNITY

ANHANG
KONTAKTDATEN REFERENTEN

VIELEN DANK
FÜR IHRE AUFMERKSAMKEIT!

Ulf Lorenzen

Geschäftsführer

T. +49 431 20084-203

E. ulorenzen@vater-gruppe.de

Vater Solution GmbH

Boschstraße 5

24118 Kiel

REFERENT

Sebastian Eich
Geschäftsführer
Tel.: +49 331 23187 206
E-Mail: Sebastian.Eich@hanseconcept.de
hanseConcept GmbH & Co. KG

“Cyberkriminalität ist ein lukratives Geschäftsmodell. JEDER ist Kunde – viele wissen es nur noch nicht!”

STANDORT HAMBURG

Holzdamm 28-32
20099 Hamburg
Tel.: +49 40 808103 600

E-Mail: kontakt@hanseconcept.de
Internet: www.hanseconcept.de

STANDORT POTSDAM

Dianastr. 46
14482 Potsdam
Tel.: +49 331 23187 200

E-Mail: kontakt@hanseconcept.de
Internet: www.hanseconcept.de

Kontakt

Carsten Hinz –
Director Sales
carsten.hinz@hoch-rein.com
Mobil: +49 160 97380726

hoch.rein IT Solutions GmbH
Gräsleinsgasse 1
97509 Kolitzheim
Germany

Phone +49 (0) 9385 98045 770
Email sales.it@hoch-rein.com
Web https://it.hoch-rein.com

Management Board:
Thomas Neußner, André Simon

Registered Office
Kolitzheim, Germany

Amtsgericht Würzburg
HRB 6376
USt-Id Nr.: DE270523145

IT SOLUTIONS

Member of GROUP

VIELEN DANK
FÜR IHRE AUFMERKSAMKEIT!

Peter Kluge

Position

T. +49 431 20084-272

E. pkluge@vater-gruppe.de

Vater Solution GmbH

Boschstraße 5

24116 Kiel