KEYNOTE

Cybersicherheit

als organisationsstrategische Aufgabe

Gerhard Müller

Geschäftsführer, Caritas-Netzwerk IT e. V.

Fachtag Cybersicherheit · Diakonisches Werk Württemberg
futurum, Stuttgart · 21. April 2026

Folien

caritas Netzwerk IT

KURZVORSTELLUNG

Ihr Gesprächspartner.

Caritas-Vertreter auf Diakonie-Fachtag – gemeinsames Handeln beginnt hier.

linkedin.com/in/gerhardmueller

Gerhard Müller

Geschäftsführer · Caritas-Netzwerk IT e. V.

Informatiker · 53 Jahre · Wahlheimat Nähe von München

- IT-Consulting-Unternehmen mitgegründet – über 20 Jahre auf 500 Mitarbeitende aufgebaut
- Seit 2021 in der Sozialwirtschaft
  Start als Interims-Geschäftsführer bei mitunsleben GmbH / mitpflegeleben.de
- Seit Mai 2022 im Caritas-Netzwerk IT e. V. – aktuell Geschäftsführer

Ehrenamt & Netzwerk

- Vorsitzender Fachausschuss Digitalisierung, IHK für München & Oberbayern
- Mitglied IKT-Ausschuss DIHK
- Vorstand German Chapter of the ACM
- Gesellschaft für Informatik, RG München
- Mit-Organisator mehrerer Meetups in München

caritas Netzwerk IT


RANSOMWARE
Your files are encrypted
Time left to recover your files:
23:17:45

GEDANKENEXPERIMENT

Morgen früh geht nichts mehr.

Ein ganz normaler Dienstagmorgen – nur ohne IT.

KEINE ~~E-Mail~~

KEINE ~~Dokumentation~~

KEINE ~~Abrechnung~~

KEIN ~~Dienstplan~~

KEINE ~~Patientenakte~~

KEIN ~~Telefon~~

Kein Szenario.

Realität für viele unserer Kolleg:innen – in den letzten drei Jahren.

caritas Netzwerk IT

SEPTEMBER 2022

Caritasverband der Erzdiözese München und Freising

Anatomie eines Ransomware-Angriffs.

23 Mio. €
wirtschaftlicher Schaden

2 Jahre
bis wirtschaftlich erholt

100
Server verschlüsselt

10.000
Mitarbeitende betroffen

350
Dienste und Einrichtungen

3 Wo.
unbemerkt im Netz

Angreifer: Ransomware-Gruppe BlackCat · seit Mitte August 2022 im Netzwerk · Zugriff in der Nacht zum 10. September

caritas Netzwerk IT

UNSERE NACHBARN

Es trifft uns. Immer wieder.

Drei weitere Vorfälle aus der Wohlfahrt.

SKM Düsseldorf · 2022

Daten verschlüsselt & kopiert
Sozialdienste zeitweise lahmgelegt
Erpressung mit Veröffentlichung

KJF Augsburg · 2024

20+ Einrichtungen betroffen
Personal-, Finanz-, Gesundheitsdaten
Monatelanger Wiederaufbau

Johannesstift Diakonie · 2024

4 Krankenhäuser lahmgelegt
Notaufnahmen abgemeldet
Pflegedokumentation auf Papier

Das sind keine fremden Unternehmen. Das sind unsere Nachbarn in der Wohlfahrt.

caritas

VERTIEFUNG · 11:15 Praxisberichte · Bruderhaus Diakonie & Diakonie Stetten

Informationen zum Cyberangriff

Der **Caritasverband für die Dekanate Dinslaken und Wesel** ist zum 23.11.2025 Opfer eines Cyberangriffs geworden. In den Pressemitteilungen und über untenstehende FAQ finden Sie weitere Informationen zu dem kriminellen Angriff und den Folgen.

Pressemitteilung

Caritas ist Opfer eines Cyberangriffs

Der Caritasverband für die Dekanate Dinslaken und Wesel verzeichnet seit vergangenem Wochenende eine Großstörung zentraler IT-Systeme und ist nach aktuellem Kenntnisstand Opfer eines weitreichenden Cyberangriffs geworden. Der Betrieb der Dienste und

DEUTSCHLAND, PRO JAHR

Die Zahlen sprechen für sich.

Quelle: Bitkom 2024/25 · BSI Lagebericht · TÜV-Studie 2025.

202 Mrd. €

jährlicher Schaden durch Cyberattacken

81 %

aller Unternehmen bereits betroffen

119

neue Schwachstellen – jeden Tag

15 %

wurden 2024 direkt angegriffen (+4 pp)

WELTWEIT · 10,5 BILLIONEN USD · jährlich

Cybercrime wäre – nach USA und China – die drittgrößte Volkswirtschaft der Welt.

Netzwerk IT

DIE AUSGANGSLAGE

IT ist nicht mehr Werkzeug.

IT ist die Lebensader unserer Organisationen.

Pflege-Doku · Dienstplan · Abrechnung · Kommunikation · Medikation – alles digital.

caritas Netzwerk IT

FÜNF STRUKTURELLE SCHWACHSTELLEN

Warum gerade die Sozialwirtschaft?

Die Sozialwirtschaft ist kein Zufallsziel – sie ist ein strukturelles Ziel.

1 Sensible Daten

Gesundheits-, Sozial-, Personaldaten – auf dem Schwarzmarkt hochwertig

2 Kleine Budgets

Historisch geringe IT-Etats – Sicherheit nicht refinanziert

3 Veraltete Systeme

Nicht auf Stand der Technik – ungepatchte Software

4 Dezentrale Struktur

Viele Standorte = viele Einfallstore

5 Wenig Bewusstsein

„Uns trifft es nicht" – trügerische Sicherheit

caritas Netzwerk IT

DIE BITTERE FORMEL

Wir sind oft leichte Beute.

Das Gesundheitswesen zählt zu den acht anfälligsten Sektoren weltweit.

Sensible Daten

Gesundheit
Sozial · Personal

+

Schwacher Schutz

Kleine Budgets
Alte Systeme

=

Perfektes Ziel

für Cyberkriminelle

Wir müssen ehrlich zu uns selbst sein.

caritas
Netzwerk IT

DREI VORFÄLLE, EINE LEHRE

Gesundheitswesen im Fadenkreuz – weltweit.

Cyberangriffe auf Gesundheitseinrichtungen können tödlich sein.

2017	2021	2020
NHS UK	**HSE Irland**	**Uniklinik Düsseldorf**
WannaCry	Conti	Ransomware
92 Mio. GBP	**83–600 Mio. USD**	**Patientin verstorben**
Lehre: Patches hätten gereicht	Lehre: Keine Netzwerk-Segmentierung	Lehre: Menschenleben in Gefahr

caritas Netzwerk IT

BEDROHUNG IN NEUER QUALITÄT

KI verändert die Spielregeln – für die Angreifer.

Die Zeit des „nigerianischen Prinzen" mit Rechtschreibfehlern ist vorbei.

82 %
KI-generiertes Phishing

+300 %
KI-Angriffe (BSI)

Perfekte Grammatik.

Perfekte Personalisierung.

Keine Warnzeichen mehr.

78 % der deutschen Firmen melden bereits mindestens einen KI-gestützten Social-Engineering-Angriff.

caritas Netzwerk IT

KI MACHT BETRUG UNSICHTBAR

Deepfakes & CEO-Fraud.

Alle 5 Minuten ein Deepfake-Angriff – irgendwo auf der Welt.

+2.137 %

Deepfake-Angriffe seit 2022

+244 %
Dokumenten-Fälschungen

60 %
aller Cyber-Schäden = CEO-Fraud

2,77 Mrd. $
BEC-Verluste FBI 2024

caritas Netzwerk IT

PARADIGMENWECHSEL

KI findet Schwachstellen – automatisch.

Anthropic „Claude Mythos" · BSI warnt · Project Glasswing (US-Banken).

Tausende hochriskante Zero-Day-Lücken

in Betriebssystemen und Browsern – von einem KI-Modell gefunden.

Was kann Mythos?

Zero-Days automatisch entdecken
Funktionierende Exploits bauen
Mehrere Lücken kombinieren

BSI-Warnung

Präsidentin Claudia Plattner: „Umwälzungen in der Schwach-stellenlandschaft insgesamt."
Mittelfristig: keine unbekannten klassischen Lücken mehr.

Project Glasswing

US-Finanzminister + Fed: systemrelevante Banken an einen Tisch gerufen.
Lücken schließen – bevor die Kriminellen ähnliche Tools haben.

Patch-Geschwindigkeit wird zur neuen Kerndisziplin. Quelle: heise.de 2026.

caritas Netzwerk IT

RANSOMWARE-AS-A-SERVICE

VERTIEFUNG · 15:00 „The Hacker Mindset" · Maren Sindlinger (SVA)

Cybercrime ist eine Industrie.

Malware mieten. Angreifen. Kassieren. – Mit Support und Kundenportal.

Miete ab 777 USD	80 % / 20 %	2.000+ Opfer
LockBit „Lite Panel" Kundenportal, Anleitung Einstieg für jedermann	Gewinnteilung Angreifer · Plattform Doppelte Erpressung	120 Mio. USD Lösegeld allein LockBit 20 % aller Fälle

Aus Hobby-Hackern ist ein Franchise-Geschäft geworden.

caritas Netzwerk IT

GESAMTKOSTEN EINES ANGRIFFS

Das Lösegeld ist nur die Spitze.

Was Organisationen im Schnitt zahlen – inkl. Ausfall, Wiederherstellung und Folgen.

~550 T$	21–24	1,2–2 Mio. €	~5 Mio. $
Lösegeld	Tage Ausfall	Wiederherstellung	Gesamtschaden

58 % der KMU stellen nach einem Ransomware-Angriff den Betrieb ein.

Quelle: Sophos State of Ransomware

caritas Netzwerk IT

MIT WENIGER MENSCHEN MEHR ERREICHEN

Demografie erzwingt Digitalisierung.

Alles digitalisieren – außer die Arbeit am Menschen.

−3,2 Mio.

Erwerbstätige

bis Mitte 2030er

+690.000

Pflegekräfte

nötig bis 2049

0,5 %

Arbeitsmarktreserve

Pflege bis 2030

Wir müssen mit weniger Menschen mehr leisten.

Alles digitalisieren – außer die Arbeit am Menschen.

caritas Netzwerk IT

DIE PYRAMIDE DER ZUKUNFTSFÄHIGKEIT

Sichere IT – Fundament für alles.

Ohne Fundament bricht alles zusammen – KI wie Digitalisierung.

Cybersicherheit ist kein Kostenfaktor – sie ist Grundvoraussetzung.

Ohne sichere IT keine Digitalisierung. Ohne Digitalisierung keine Antwort auf den Fachkräftemangel.

caritas
Netzwerk IT

DIGITALISIERUNGSDRUCK VOM STAAT

TI, KIM, ePA – neue Pflichten, neue Risiken.

Der Gesetzgeber verlangt Digitalisierung – aber nicht ohne Sicherheit.

Dez. 2024

ePA für 73 Mio.

Automatisch
CCC zeigte Lücken

Juli 2025

TI-Pflicht Pflege

Alle Einrichtungen
an Telematikinfrastruktur

Dez. 2026

KIM-Abrechnung

Elektronisch
verpflichtend

Nur 50–60 % der Einrichtungen sind bereits angebunden – Handlungsdruck steigt.

EUDI-Wallet Deutschland-Stack …

caritas
Netzwerk IT

SONDERN

Chefsache

Auf der Agenda von
Vorstand und Geschäftsführung.

Seit NIS-2 auch rechtlich klargestellt.

caritas
Netzwerk IT

SEIT 6. DEZEMBER 2025 IN KRAFT

NIS-2 – der Weckruf.

Ohne Übergangsfrist – Registrierungspflicht bereits verstrichen.

30.000

betroffene Unternehmen

vorher 4.500

18

Wirtschaftssektoren

inkl. Gesundheit

NEU

Sozialversicherung

erstmals erfasst

6.3.2026

Registrierung BSI

Frist verstrichen

Wer die Registrierung verpasst hat, hat ein Problem.

caritas Netzwerk IT

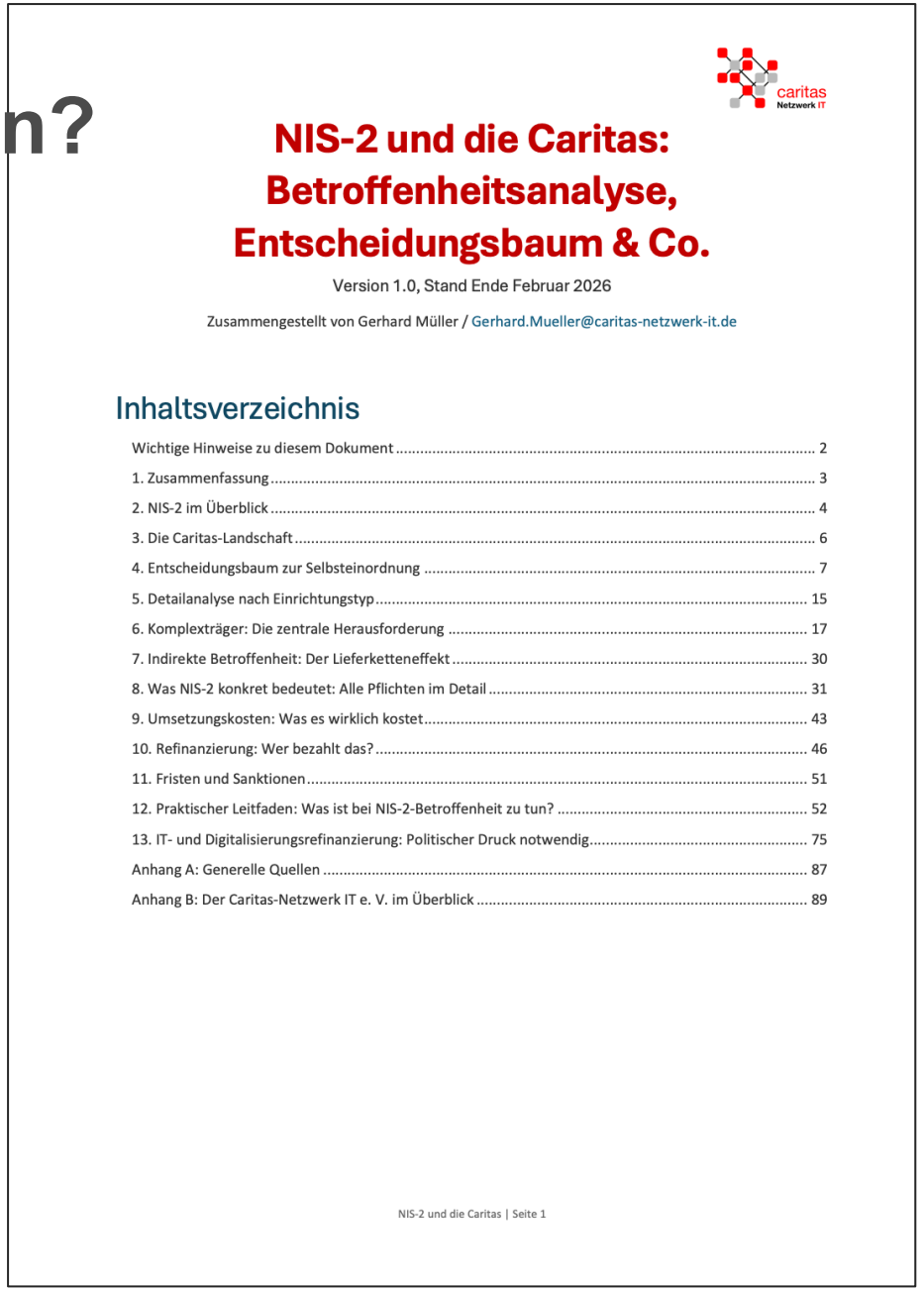
VIELE HABEN SICH NOCH NICHT AUSREICHEND INFORMIERT – SIND ABER VIELLEICHT BETROFFEN

NIS-2 – Wer ist betroffen? Was ist zu tun?

Nicht alle Bereiche der freien Wohlfahrt betroffen – NIS-2 ist „Mindeststandard“

Ca. 90 Seiten / verfügbar auch ohne LinkedIn-Account unter:

https://www.linkedin.com/posts/gerhardmueller_nis-2-und-die-caritas-ugcPost-7434922815146881024-A4jH



caritas Netzwerk IT

NIS-2 und die Caritas: Betroffenheitsanalyse, Entscheidungsbaum & Co.

Version 1.0, Stand Ende Februar 2026

Zusammengestellt von Gerhard Müller / Gerhard.Mueller@caritas-netzwerk-it.de

Inhaltsverzeichnis

NIS-2 und die Caritas | Seite 1

MINDESTSTANDARD

§ 30 BSIG – Die 10 Mindestmaßnahmen.

Kein Maximalwunsch – gesunder Menschenverstand in Gesetzesform.

1. Risikoanalyse & Sicherheitskonzept
2. Wirksamkeitsbewertung
3. Incident Management
4. Business Continuity & Backup
5. Lieferkettensicherheit
6. Sichere IT-Beschaffung & -Wartung
7. Schulungen & Awareness
8. Kryptografie & Verschlüsselung
9. Zugangskontrollen
10. Multi-Faktor-Authentifizierung

caritas Netzwerk IT

§ 38 BSIG

Geschäftsleiterhaftung – persönlich!

Ignorieren ist keine Option mehr – Cybersicherheit ist Chefsache mit Risiko.

Privatvermögen	Pflicht	Bußgeld
§ 38	**Schulung**	**10 Mio. €**
Persönliche Haftung der Leitung	Gesetzlich vorgeschrieben – für die Leitung	oder 2 % des weltweiten Jahresumsatzes

caritas Netzwerk IT

DSGVO · B3S · KRITIS

Nicht nur NIS-2.

Mehrere Gesetze greifen gleichzeitig – und alle verlangen dasselbe: belastbare Sicherheit.

10.259

gemeldete Datenpannen 2025

Vorjahr 8.623

72 h

DSGVO-Meldepflicht

Gesundheitsdaten = hohes Risiko

20 Mio. €

DSGVO-Bußgeld

oder 4 % Jahresumsatz

Bei Gesundheitsdaten gilt fast immer ein „hohes Risiko" – unverzüglich informieren.

caritas Netzwerk IT

PFLEGESÄTZE KENNEN KEINE IT-SICHERHEIT

Das Refinanzierungsproblem.

Der Staat verlangt TI, ePA, NIS-2 – refinanziert aber nichts davon.

DER STAAT VERLANGT

TI-Pflicht
ePA
NIS-2 / § 30 BSIG
…

REFINANZIERUNG

kein Cent

Das System ist kaputt.

Wer Sicherheit verlangt, muss sie auch bezahlen.

caritas Netzwerk IT

Cyberversicherung – kein Freifahrtschein.

Versicherer lehnen ab, wenn Grundlagen fehlen – und das ist die neue Normalität.

Ablehnungsgründe

Jeder 3. Antrag abgelehnt
85 % der Versicherer: höhere Anforderungen
Deckungslücken bei Krieg und KI
Ausschluss bei unbekanntem Schaden

Pflicht-Anforderungen

Multi-Faktor-Authentifizierung
Backup-Strategie (dokumentiert)
Patch-Management
Regelmäßige Schulungen
Netzwerk-Segmentierung

caritas
Netzwerk IT

SOCIAL ENGINEERING IN ZAHLEN

Der Mensch – größte Schwachstelle, beste Firewall.

84 % der Sicherheitsvorfälle beginnen mit einer einzigen E-Mail.

700+

SE-Attacken

pro Org. / Jahr

84 %

Vorfälle

starten mit Phishing

65 %

SE-Fälle

beginnen per E-Mail

60 %

Cyber-Schäden

= CEO-Fraud

caritas Netzwerk IT

VIER PSYCHOLOGISCHE HEBEL (NACH CIALDINI)

Angreifer nutzen unsere besten Eigenschaften.

Unsere Hilfsbereitschaft wird gegen uns verwendet.

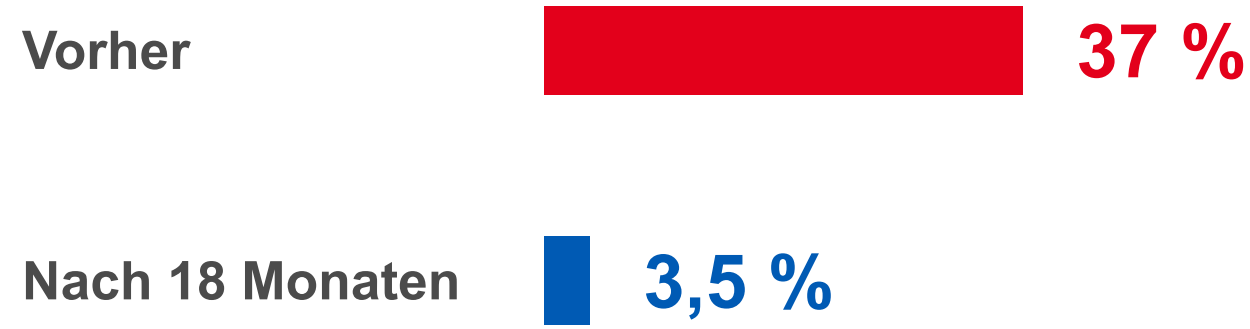
Autorität	Zeitdruck	Hilfsbereitschaft	Social Proof
„Ihr Vorstand bittet um Überweisung."	„Dringend! Innerhalb einer Stunde!"	In der Sozialwirtschaft besonders stark – wir helfen gern und fragen nicht nach.	„Alle Kollegen haben das schon gemacht."

caritas
Netzwerk IT

PHISHING-KLICKRATE VOR VS. NACH 18 MONATEN

Awareness-Training wirkt.

Quelle: SoSafe Human Risk Review 2024.



Investition: Mehrere Tausend € pro Jahr für 200 Mitarbeitende

Meldequote steigt von 0 % auf 70 % – Mitarbeitende werden zur aktiven Firewall.

caritas Netzwerk IT

UNBEQUEME WAHRHEIT

Schulung beginnt an der Spitze.

Führungskräfte sind anfälliger – nicht widerstandsfähiger.

+60 %	62 %	52 %
höhere Klickrate bei Führungskräften	**klickten auf** „Gehaltsabrechnungsfehler"	**Vorfälle durch** menschliches Versagen

Auch Digital Natives klicken häufiger als ältere Kollegen – Vertrautheit ist kein Schutz.

caritas Netzwerk IT

DIE GUTE NACHRICHT - MULTI-FAKTOR-AUTHENTIFIZIERUNG

99,2 %

weniger Risiko – mit einer einzigen Maßnahme.

Aktivieren für E-Mail, VPN, Cloud und alle Admin-Konten. Ohne MFA keine Cyberversicherung.
Quelle: Microsoft Digital Defense Report.

caritas
Netzwerk IT

96 % DER RANSOMWARE ZIELT GEZIELT AUF BACKUPS

3-2-1-1-0 – Backup, das wirklich trägt.

Ein ungetestetes Backup ist kein Backup – es ist eine Hoffnung.

Kopien der Daten | **verschiedene Medien** | **offsite (außer Haus)** | **offline / air-gapped** | **Fehler im Restore-Test**

Tägliches Backup. Wöchentlich extern. Monatlich offsite. Vierteljährlich Restore-Test.

caritas Netzwerk IT

DREI SUPPLY-CHAIN-FÄLLE

Lieferkette – die unsichtbare Gefahr.

Ein kompromittierter Dienstleister – alle Kunden betroffen.

NIS-2 fordert explizit Sicherheit der Lieferkette.

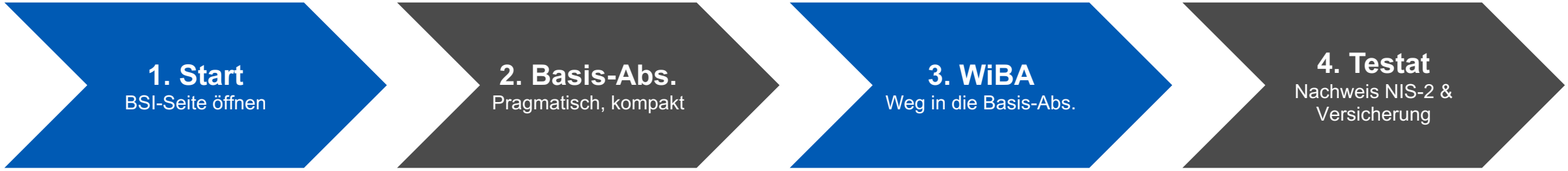
Besonders relevant für die Sozialwirtschaft: ein Dienstleister für viele Einrichtungen.

caritas Netzwerk IT

NICHT DAS RAD NEU ERFINDEN

BSI-Grundschutz – der pragmatische Einstieg.

Alle Materialien kostenlos verfügbar – mit BSI-Testat als Nachweis.



Sie müssen das Rad nicht neu erfinden.

Der BSI-IT-Grundschutz bietet Rahmen, Methoden, Checklisten – alles frei verfügbar.

caritas Netzwerk IT

DER LEICHTERE WEG ZUM ISMS

Alternative: ISO 27001 + NIST CSF 2.0

International, flexibel, risikobasiert – wenn BSI-Grundschutz zu schwer wirkt.

NIST Cybersecurity Framework 2.0 · 6 Kernfunktionen

GOVERN	IDENTIFY	PROTECT
Strategie · Rollen	**Assets · Risiken**	**Schutzmaßnahmen**
NEU in 2.0	verstehen	umsetzen

DETECT	RESPOND	RECOVER
Ereignisse	**Vorfälle**	**Systeme**
erkennen	bearbeiten	wiederherstellen

ISO 27001:2022 als zertifizierbarer Standard

93 Controls · risikobasiert · international anerkannt · Cyberversicherer + NIS-2 akzeptieren

BSI für KRITIS · ISO + NIST wenn international, flexibel, risikobasiert.

caritas Netzwerk IT

SECHS SCHRITTE

Was tun, wenn es passiert?

Geübt, dokumentiert – und im Ernstfall griffbereit.

Haben Sie diese sechs Schritte dokumentiert? Wenn nicht: erste Aufgabe nach diesem Fachtag.

caritas Netzwerk IT

2 STUNDEN TABLETOP-EXERCISE

Das Papier allein rettet nicht. Proben Sie es.

Der schnellste Weg zu ehrlicher Betroffenheit – und der beste, um Lücken zu finden, bevor es ernst wird.

SO GEHT ES

1. **Acht bis zehn Personen an einen Tisch**:
   GF, IT, Pflegedienst, Kommunikation, Personal, Datenschutz, Haustechnik, Buchhaltung.

2. **Moderator stellt ein konkretes Szenario vor:**
   „Freitag 14:30 – auf allen Bildschirmen:
   Ihre Daten sind verschlüsselt. Zahlen Sie 2 Mio. €."

3. **Jede Rolle muss reagieren – in Echtzeit:**
   Wen rufen Sie in den ersten 15 Minuten an?
   Wer informiert welchen Kostenträger?
   Wer spricht (oder schweigt) mit der Presse?

4. **Nach 2 h: Debriefing mit Action-List.**

SO WIRKT ES

- **Emotionale Betroffenheit** in den ersten 30 Minuten – das schafft kein Vortrag.
- **Lücken werden sichtbar**, bevor ein echter Angreifer sie findet:
  – Haben wir die Handynummern?
  – Wer darf die Presse informieren?
  – Wo liegt das Notfallhandbuch?
  – Funktioniert die Offline-Kopie?
- **Das Team lern**t aus eigenen Fehlern, nicht aus Papier.

RESSOURCEN (kostenlos)

BSI Notfallhandbuch-Vorlage · LSI Bayern Tabletop-Übungen · TU Braunschweig Handout · Szenario Ransomware (Caritas-Netzwerk IT)

Wer nach 30 Minuten keine Bauchschmerzen hat, hat das Szenario zu harmlos gewählt.

caritas Netzwerk IT

INVESTITION 50–100 T€ · SCHADEN 1,2–23 MIO. € · ROI 12–40 ×

Ihr Fahrplan – 30 / 90 / 365 Tage.

Klingt nach viel? Gegenüber dem potenziellen Schaden verschwindend gering.

30 Tage
~5.000 €

- MFA aktivieren
- Passwörter neu
- Updates Auto
- Notfallkontakte
- Backup-Status
- Phishing-Briefing

90 Tage
~30.000 €

- Awareness-Training
- Backup 3-2-1-1-0
- Netzwerk segmentieren
- Berechtigungen
- Notfallplan dok.
- Dienstleister-Verträge

365 Tage
~80.000 €

- ISMS nach BSI-Basis
- Phishing-Simulationen
- Penetrationstest
- Cyberversicherung
- IR-Übung
- Lieferanten-Bewertung

caritas Netzwerk IT

KOMPLEXITÄT ÜBERSTEIGT DIE EINZELORGANISATION

Alleine schafft es niemand mehr.

IT-Sicherheits-Fachkräfte sind knapp – gemeinsame Lösungen werden zur Pflicht.

Dienstleister

Externe Spezialisten – was man selbst nicht kann.

Software-as-a-Service

Stand der Technik – automatisch, nicht selbstgebaut.

Gemeinsame Lösungen

Über Trägergrenzen hinweg – ökumenisch, solidarisch.

Solidarität ist unser Markenkern – auch in der IT.

caritas Netzwerk IT

CARITAS-NETZWERK IT · SEIT NOV. 2024

Cyber-Feuerwehr

1 € pro VZÄ und Monat.

24/7	100 h	Partner SVA
Notfall-Hotline	Experten-Hilfe pro Vorfall	ein Euro. Weniger als ein Kaffee.

Details: https://www.caritas-netzwerk-it.de/leistungen

caritas Netzwerk IT

Erfahrungsaustausch – wir tauschen, was wir wissen.

Regelmäßige Gruppen für Mitglieder – mit KI-unterstützten Zusammenfassungen.

AKTUELLE GRUPPEN

- **Notfallmanagement**
- **Nutzung von Microsoft 365**
- **Austausch zu Connext Vivendi**
- **Einführung und Nutzung von KI**
- **SoCura-Kunden**

Demnächst zusätzlich:

- **Strategie & Digitalisierung**

ZIELE & ERGEBNISSE

Ziele

- Erfahrungsaustausch, gegenseitige Anregungen
- Konkrete Hilfestellungen
- Identifikation gemeinsamer Themenfelder

Ergebnisse

- KI-generierte ausführliche Zusammenfassungen
- Mehr aktuelle Informationen
- Gemeinsames Verständnis

Mitglied und Interesse? → Gerhard.Mueller@caritas-netzwerk-it.de · Mirco.Beyer@caritas-netzwerk-it.de

caritas Netzwerk IT

POLITISCHER DRUCK – GEMEINSAM FORMULIERT

Fachkongress Cybersecurity 2026.

Dialog mit Politik und Ministerien. Wer Sicherheit verlangt, muss sie auch bezahlen.

11.–12. Juni 2026 · Berlin

VERANSTALTER

Deutscher Caritasverband
Diakonie Deutschland
Caritas-Netzwerk IT
V3D und Partner

ZIELGRUPPE

Führungskräfte und IT-Leitung der Wohlfahrtsverbände

TEILNAHME

https://www.v3d.de/veranstaltungen/veranstaltung/fachkongress-cybersecurity-stark-gegen-cyberangriffe/

caritas Netzwerk IT

WO SIE MEHR ERFAHREN

Weitergehende Informationen.

Webseite · Newsletter · Carinet-Gruppe mit allen Dokumenten.

Webseite

caritas-netzwerk-it.de
Alle Angebote · News · Ansprechpartner

caritas-netzwerk-it.de

Newsletter

Via Homepage & Caritas abonnierbar
Archiv in der Carinet-Gruppe

Carinet-Gruppe

„Allgemeine Infos Caritas-Netzwerk IT e. V."
Satzung · Mitgliederliste · I&R-Details

Auch dabei: genaue Informationen zum „Incident & Response-Angebot" (Cyber-Feuerwehr).

caritas Netzwerk IT

UNSERE VERANTWORTUNG

Wir sind die soziale Infrastruktur.

Krankenhäuser	Pflegeheime	Beratungsstellen	Kitas	Werkstätten	Wohngruppen

Wenn wir ausfallen, gibt es keinen Plan B.

Lassen Sie uns dieser Verantwortung gerecht werden. Gemeinsam.

caritas Netzwerk IT

Vielen Dank.

Folien

KONTAKT

Gerhard Müller

Geschäftsführer · Caritas-Netzwerk IT e. V.

E-MAIL
Gerhard.Mueller@caritas-netzwerk-it.de

MOBIL
+49 179 133 80 60

LINKEDIN
https://linkedin.com/in/gerhardmueller

caritas-netzwerk-it.de

Cybersicherheit ist nicht die Aufgabe der IT-Abteilung.

Sie ist die Aufgabe von uns allen.

caritas Netzwerk IT