Cybersicherheit als organisations-strategische Aufgabe: Professionelles Risikomanagement und Resilienz

GESELLSCHAFT
FÜR INFORMATIK

Cybersicherheit ist wie Brandschutz: Wer sich nicht angemessen vorbereitet, den gibt es morgen vielleicht nicht mehr

Caritas-Netzwerk IT e.V.
Gerhard.Mueller@caritas-netzwerk-it.de

Vortrag am 15.1.2024 bei der Regionalgruppe der GI / German Chapter of the ACM

caritas
Netzwerk IT

Zum Hintergrund des Vortragenden Gerhard Müller

- Informatiker, 51 Jahre, Wahlheimat München
- IT-Consulting-Unternehmen mitgegründet und über 20 Jahre auf 500 Mitarbeitende mit aufgebaut
- Seit 2021 in der Sozialwirtschaft, gestartet als interims-Geschäftsführung der mitunsleben GmbH („mitpflegeleben.de“)
- Seit Mai 2022 Community-Management Caritas-Netzwerk IT e. V.
- Ehrenamt: Vorsitzender des Fachausschusses Digitalisierung bei der IHK München & Oberbayern, Mitglied im IKT-Ausschuss des DIHK, Vorstand des German Chapter for the ACM, aktiv bei Gesellschaft für Informatik/Regionalgruppe München, Mit-Organisator von mehreren Meetups in München

caritas Netzwerk IT

Caritas-Netzwerk IT e. V.

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

Sozial braucht Digital:

Gemeinsam bessere und sicherere IT organisieren

Eine komplexer werdende Welt braucht komplexere Antworten. Das gilt gerade auch in der Sozialwirtschaft, und damit auch insbesondere für die Caritas. Um wirklich professionelle IT-Strategien und IT-Strukturen nachhaltig und finanzierbar aufbauen und organisieren zu können, braucht es die Bündelung der Bedürfnisse, der Expertise und der Zusammenarbeit von Vielen: den Mitgliedern des Caritas-Netzwerk IT e. V.

„Der Caritas-Netzwerk IT e. V. verfolgt das Ziel, die Interessen der Mitglieder zu bündeln und Meinungsbilder für strategische Fragen der Dienste und Einrichtungen herbeizuführen. Fragestellungen der Informationstechnologie bei den Trägern werden als Unternehmenskooperation bewältigt, die als strategischer Partner mittels innovativer, bedarfsgerechter, sicherer und digitaler Lösungen den Mitgliedern dient." (Ziel Caritas-Netzwerk IT e. V.)

caritas Netzwerk IT

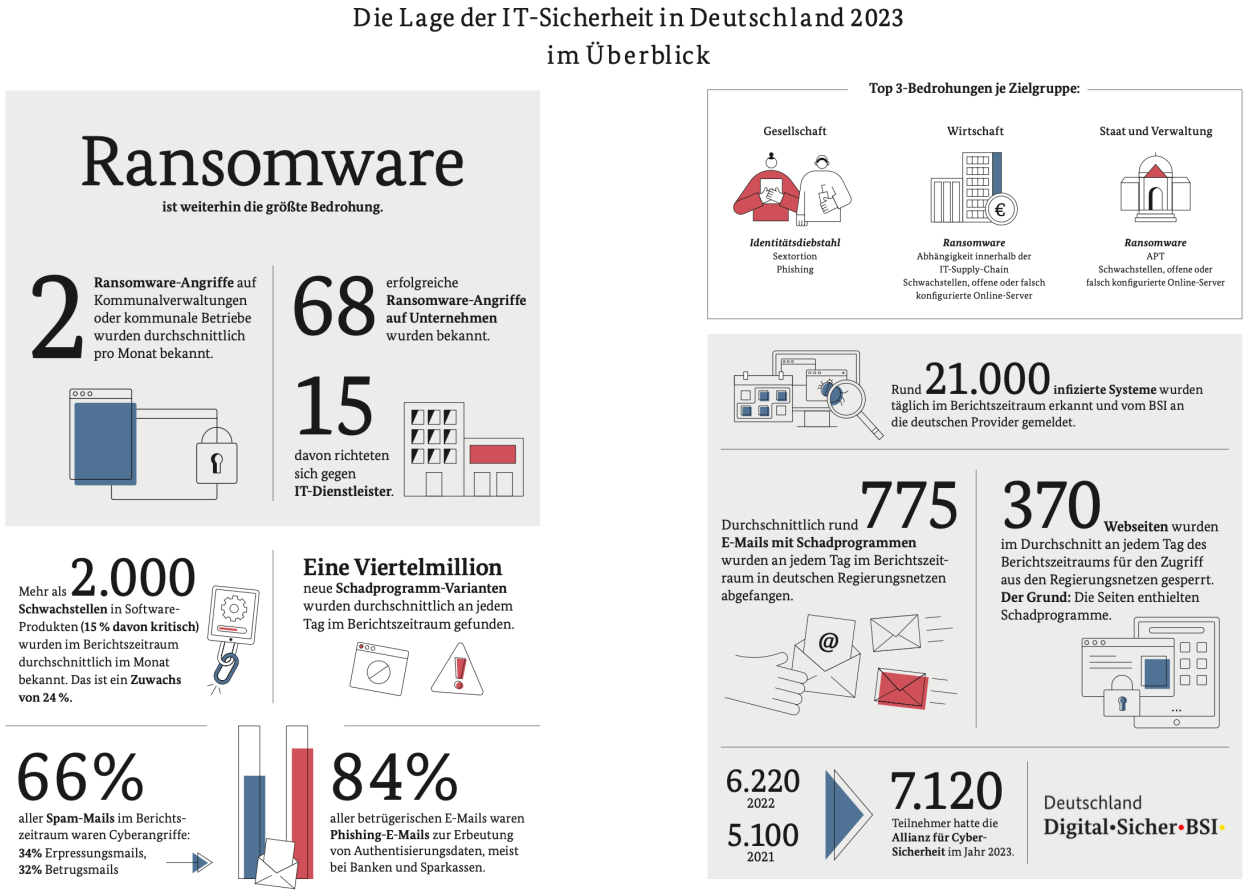
Gliederung

- Aktuelle Cyber-Situation
- Ablauf und Konsequenzen
- Was kann (und muss!) jede Organisation tun?
  - Inklusive Übersicht NIS-2
- Was können wir gemeinsam tun?
- Fazit

caritas
Netzwerk IT

Aktueller Stand

Quelle: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html



caritas Netzwerk IT

Bundesamt für Sicherheit in der Informationstechnik:

„Die Bedrohung im Cyberraum ist so hoch wie nie zuvor. “

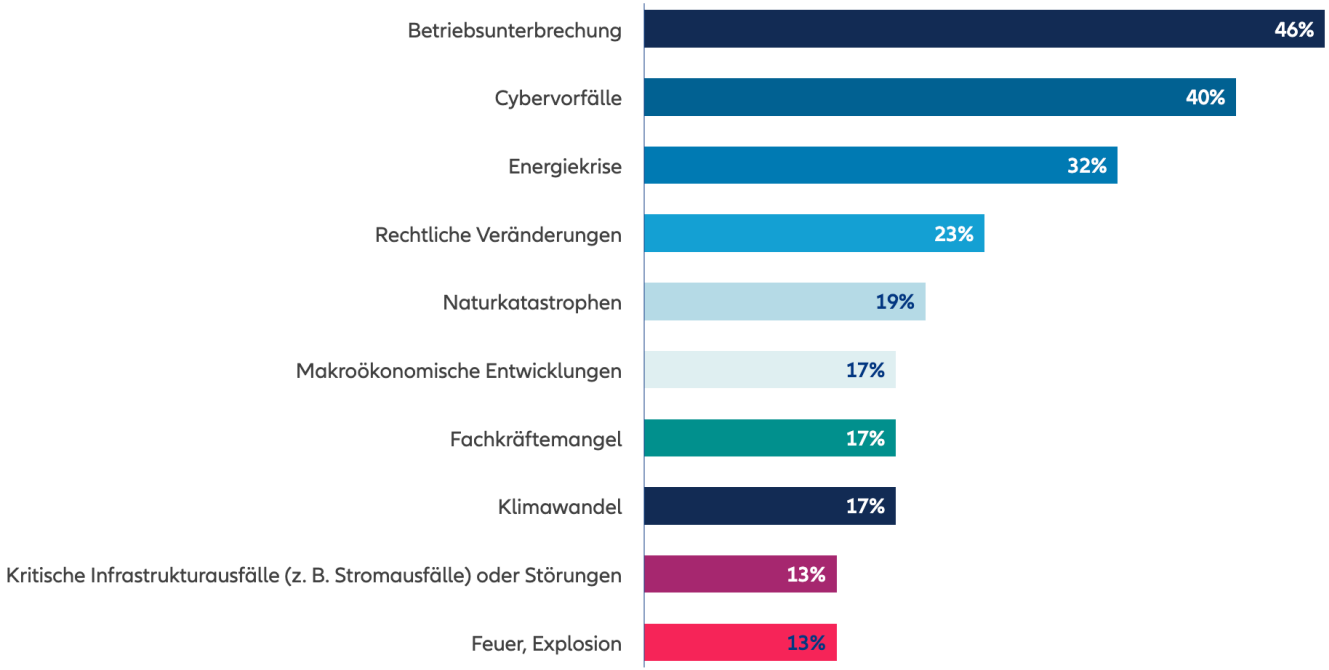
Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html

Allianz

Top 10 Geschäftsrisiken in Deutschland in 2023

Allianz Risk Barometer 2023

Die Zahlen geben an, wie oft ein Risiko als Prozentsatz aller Antworten für das jeweilige Land ausgewählt wurde: 384. Die Zahlen addieren sich nicht zu 100%, da bis zu drei Risiken ausgewählt werden konnten.



AGCS News & Insights

Quelle: Allianz Global Corporate & Specialty

Quelle: https://app.23degrees.io/view/fgnBcGmLqbDTrT4Z-bar-horizontal-top-10-geschaeftsrisiken-in

caritas Netzwerk IT

Top 10 Geschäftsrisiken weltweit in 2023

Allianz Risk Barometer 2023

Basierend auf den Antworten von 2.712 Risikomanagement-Experten aus 94 Ländern und Gebieten (% der Antworten). Die Zahlen ergeben nicht 100%, da jeweils bis zu drei Risiken ausgewählt werden konnten.

AGCS News & Inisghts

Source: Allianz Global Corporate & Specialty

Quelle: https://app.23degrees.io/embed/XGAiTqt7fwhmezAO-bar-horizontal-top-10-geschaeftsrisiken

Warum sind Cyber-Attacken epidemisch geworden?

- Vernetzung & Online-Zugreifbarkeit von fast allen Systemen
- Komplexität gestiegen: Cyber-Kriminelle müssen nur ein Loch finden, wir aber “alles“ absichern
- Internationale Krisen & politische Unterstützung in manchen Ländern (Russland, China, Nordkorea etc.)
- Anonyme Zahlungen (Bitcoin & Co.)
- Routing, das verschleiert, wer / von wo aus angegriffen wird
- Asymmetrische Verschlüsselung
- Dark Web
- Professionalisierung von Cyber-Kriminellen
- Regulierung kommt nicht hinterher
- …

caritas Netzwerk IT

Künstliche Intelligenz erhöht die Möglichkeiten und Wirksamkeit von Attacken

- Mehr Kriminelle können Lücken & Co. finden, verstehen und ausnutzen
- E-Mails (Phishing…) & Co. können trivial in perfektem Deutsch (oder vielen anderen Sprachen) geschrieben werden, und wenn Kontext vorhanden ist, kann dieser sehr gut integriert werden
  - antworten auf geschriebene E-Mails einer Person, deren Postfach kompromittiert wurde, oder wo Daten abgeflossen sind

caritas Netzwerk IT

Rahmenbedingungen beachten: Die fünf Ds…

- Digitalisierung
- Demographieentwicklung
- Deindustrialisierung
- Dekarbonisierung
- Debürokratisierung

caritas Netzwerk IT

Es betrifft leider nicht nur die Wirtschaft und den Staat, sondern alle…

- Aktuell (Beispiele):
  - Internationales Rotes Kreuz (2022)
    - https://www.icrc.org/de/document/ikrk-cyberangriff-analyse
  - Universitätsklinikum Frankfurt
    - https://www.fr.de/frankfurt/geraeten-hessen-groesstes-krankenhaus-frankfurt-uniklinik-hackerangriff-fax-zr-92668271.html
  - Südwestfalen IT (SIT) / 72 Kommunen
    - https://www.heise.de/news/Cyberangriff-auf-Suedwestfalen-IT-Mehr-Kommunen-betroffen-Notbetrieb-haelt-an-9532453.html
- Übersicht über Deutschland, soweit bekannt geworden:
  - https://konbriefing.com/de-topics/hackerangriff-deutschland.html

Es betrifft alle, auch im Caritas-Umfeld (beispielhaft, 2022+2023)

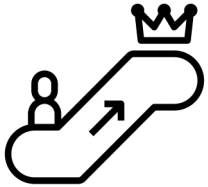
- Caritasverband für die Erzdiözese München und Freising e. V.
  - https://www.aktuelles-und-themen.caritas-nah-am-naechsten.de/infos-cyberangriff
- Caritasverband Eifel
  - https://www1.wdr.de/nachrichten/folgen-des-hacker-angriffs-auf-caritas-eifel-100.html
- SKM Düsseldorf
  - https://www.katholisch.de/artikel/41159-hackerangriff-auf-katholischen-sozialdienstleister-skm
- Deutscher Caritasverband
  - (nicht in der Presse gewesen)
- Caritasverband für den Rhein-Erft-Kreis
  - https://www.caritas-rhein-erft.de/ueber-uns/presse/Medieninformationen/Caritas-Rhein-Erft-ist-Opfer-einer-Cyberattacke/

caritas Netzwerk IT

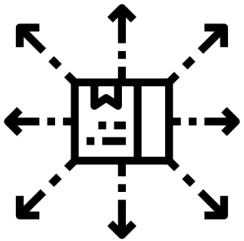
Was passiert da eigentlich… und warum ist das alles so schlimm? Beispiel Ransomware

Zugang
Erstinfektion eines Nutzers/einer Nutzerin über Phishing;
Zugang über erbeutete Zugangsdaten

Rechtevermehrung
Privilege Escalation: lokaler Admin auf Domainadministrator



Verbreitung
Lateral Movement: Cobaltstrike Loader auf weitere Systeme verteilt



Vorbereitung
Einrichtung Datenplattform auf Backup Server, Datenausleitung

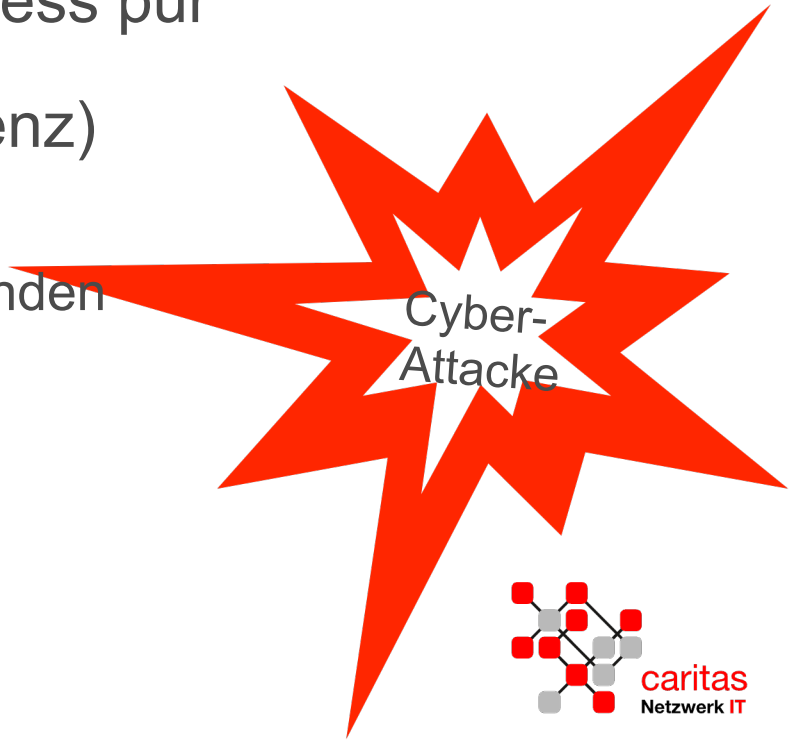
Missbrauch und Erpressung
Verschlüsselung
Erpresserschreiben

Zeit

caritas Netzwerk IT

Auswirkungen am Beispiel Ransomware: Extrem

- Mehrere Monate (oder länger) Stress pur
- Erhebliche Schäden (oder Insolvenz)
  - Finanziell
  - Daten von Klient:innen und Mitarbeitenden
  - Reputation
  - Fluktuation



caritas
Netzwerk IT

Konsequenzen (Beispiele)

- Alle Daten sind WEG
- Alle Backups, falls noch vorhanden, müssen überprüft werden, ob sie bereits befallen sind (ggf. 1 Jahr WEG)
- Alle Rechner / Geräte / Drucker etc. sind potentiell befallen und müssen fachmännisch zurückgesetzt werden, bzw. temporär neue Rechner genutzt werden
- Internet ist WEG bzw. kann nicht genutzt werden
- Telefon und alle Telefon-Kontakte sind WEG (außer vielleicht Handies)
- Krisenstab & Krisenkommunikation brauchen Zeit & Kraft
- Keine Kommunikation mehr mit Mitarbeitenden zentral möglich
- Rückfall auf händische / Papier-Prozesse / Notfall-Modus, oft über viele Monate
- Rechnungen können nicht mehr bezahlt & gestellt werden
- Mitarbeitende können nicht mehr bezahlt werden
- Insolvenz, Burn Outs

caritas Netzwerk IT

Kosten von Cyberattacken

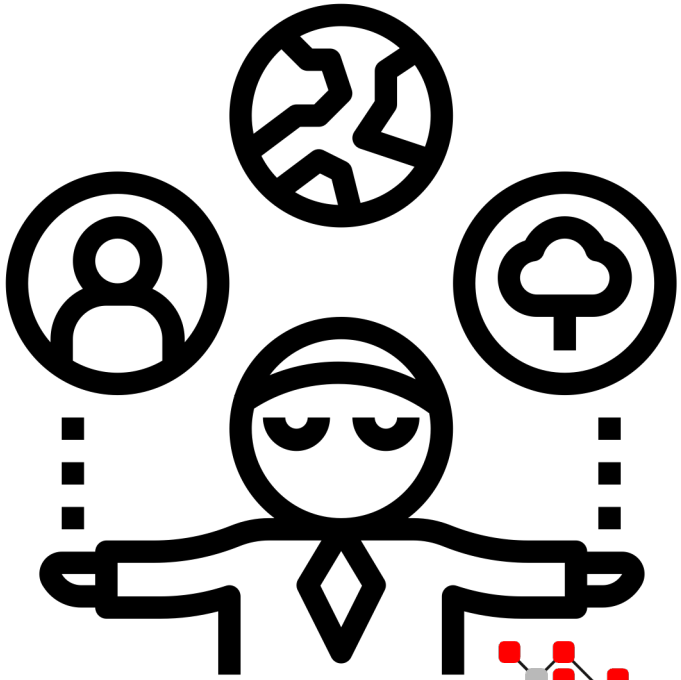
- Eigenschäden
  - Betriebsbeeinträchtigung und -unterbrechung
  - Schadensermittlung und IT-Forensik
  - Management der Schadensbewältigung
  - Wiederherstellungskosten
  - Krisenberatung
  - Verbesserung der Organisations- und IT-Strukturen _
  - Rechtsberatungskosten
  - Informationskosten
  - Erpressung und Lösegeld
  - Vertragsstrafen und Bußgelder
  - Reputationskosten
  - Krisenkommunikation (nach Schadenseintritt)
  - Litigation-PR (Öffentlichkeitsarbeit im Rechtsstreit)
  - Nachhaltige Beseitigung des Reputationsschadens
- Fremdschäden
- Präventionskosten
  - Sichere IT-Infrastrukturen aufbauen und betreiben
  - Aufbau einer IT-sicherheitsaffinen Unternehmenskommunikation/-kultur
  - Beauftragung einer PR-Agentur zur Steuerung der Kommunikationswerkzeuge und –kanäle
  - Abschluss Dienstleistungsvertrag z. B. mit einem Ausweichrechenzentrum

Quelle: https://www.bitkom.org/sites/main/files/file/import/160426-LF-Cybersicherheit.pdf

caritas Netzwerk IT

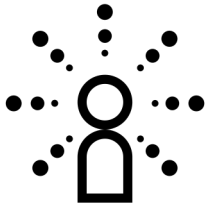
Wer ist verantwortlich für die Behandlungen von Risiken?

- Vorständ:innen, Geschäftsführungen
- Drohende Insolvenz
  - Rechnungsstellung nicht möglich
  - Kreditwürdigkeit sinkt
  - Kosten für Vorfall & Ausfälle
- Personal
  - Gehälter: zahlbar?
  - Attraktivität als Arbeitgeber sinkt
  - Fluktuation / Burn-Out
- Persönliche Haftung
  - Bis hin zum Verlust der Stelle

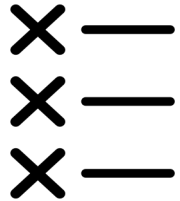


caritas
Netzwerk IT

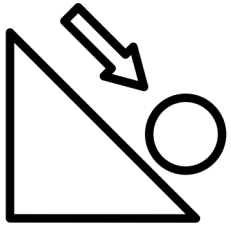
Was kann (und muss!) jede Organisation tun?



- Bewusstsein schaffen



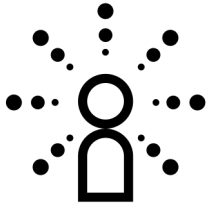
- Erfolgreiche Angriffe unwahrscheinlicher machen



- Folgen eines erfolgreichen Angriffs reduzieren

caritas
Netzwerk IT

Was kann (und muss!) jede Organisation tun? Bewusstsein schaffen



- Bewusstsein auf Führungsebene notwendig
- NIS-2-Direktive („Network and Information Security 2“)
  - https://digital-strategy.ec.europa.eu/de/policies/nis2-directive

caritas
Netzwerk IT

NIS2 – was ist das?

- NIS2 ist eine EU-Richtlinie, die die NIS-Richtlinie von 2013 ersetzt.
- NIS steht für Netz- und Informationssicherheit.
- Die Richtlinie gilt EU-weit für einheitliche Cyber- und Informationssicherheit.
- Ziel: Besserer Schutz kritischer Infrastrukturen und Dienste gegen Cyber-Bedrohungen.
- NIS2 deckt mehr Sektoren ab als die vorherige Richtlinie.
- Verschärfung der Aufsichtsanforderungen.
- Einführung persönlicher Haftung der Unternehmensleitung bei Gesetzesverstößen.

caritas
Netzwerk IT

Quelle: https://digital-strategy.ec.europa.eu/de/policies/nis2-directive

Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union (NIS2-Richtlinie)

Dies ist eine maschinelle Übersetzung durch den eTranslation-Dienst der Europäischen Kommission, der Ihnen hilft, diese Seite zu verstehen. Bitte lesen Sie die Nutzungsbedingungen.
Um die Originalfassung zu lesen, gehen Sie zur Quellenseite.
Beendet

Die NIS2-Richtlinie ist die EU-weite Gesetzgebung zur Cybersicherheit. Sie enthält rechtliche Maßnahmen zur Steigerung des Gesamtniveaus der Cybersicherheit in der EU.

© iStock by Getty Images -1169999045 aismagilov

Die 2016 eingeführten Cybersicherheitsvorschriften der EU wurden durch die 2023 in Kraft getretene NIS2-Richtlinie aktualisiert. Es modernisierte den bestehenden Rechtsrahmen, um mit der zunehmenden Digitalisierung und einer sich entwickelnden Bedrohungslandschaft für Cybersicherheit Schritt zu halten. Durch die Ausweitung des Anwendungsbereichs der Cybersicherheitsvorschriften auf neue Sektoren und Einrichtungen verbessert sie die Resilienz- und Reaktionskapazitäten öffentlicher und privater Stellen, der zuständigen Behörden und der EU insgesamt weiter.

Die Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union (NIS2-Richtlinie) sieht rechtliche Maßnahmen vor, um das Gesamtniveau der Cybersicherheit in der EU zu erhöhen, indem Folgendes gewährleistet wird:

- Vorbereitung derMitgliedstaaten, indem sie verlangt, dass sie angemessen ausgerüstet sind. Zum Beispiel mit einem Computer Security Incident Response Team (CSIRT) und einer zuständigen nationalen Behörde für Netzwerk- und Informationssysteme (NIS),
- Zusammenarbeit zwischen allen Mitgliedstaaten durch Einsetzung einer Kooperationsgruppe zur Unterstützung und Erleichterung der strategischen Zusammenarbeit und des Informationsaustauschs zwischen den Mitgliedstaaten.

NIS-2-Richtlinie (Richtlinie (EU) 2022/2555) >
Fragen & Antworten >

NIS 2 in etwas mehr Detail

- Warum
  - Mehr Organisationen zwingen, professioneller im Cyber-Sicherheitsbereich zu werden
- Wie
  - Ca. 30-40.000 Organisationen in Deutschland werden durch Nachweispflichten gezwungen, sich mit dem Thema Informationssicherheit zu beschäftigen und nachzuweisen, dass die eigene Organisation gut aufgestellt ist
- Was
  - Im Wesentlichen ein ISMS (Informationssicherheitsmanagementsystemen) einführen, wenn eine Organisation noch keines hat
    - Basis für ISMS kann z.B. die ISO-27001 sein, ist alleine aber nicht ausreichend
    - Branchenspezifische Standards (TISAX in der Automobilindustrie etc.) möglich

caritas Netzwerk IT

NIS 2 in etwas mehr Detail: Was (Voraussichtlich)

- Registrierungspflicht
  - Betroffene Unternehmen müssen sich bei einer zentralen Stelle des Bundes registrieren
- Meldepflicht
  - Erhebliche Sicherheitsvorfälle müssen innerhalb von 24 Stunden an eine zentrale Meldestelle berichtet werden
- Risikomanagement
  - Umsetzen von Maßnahmen, um Risiken aus Cybersecurity-Vorfällen zu reduzieren und einen sicheren Betrieb zu gewährleisten

caritas Netzwerk IT

NIS 2 in etwas mehr Detail: Was (Voraussichtlich)

- Nachweispflichten
  - Unternehmen müssen 3 Jahre nach Inkrafttreten den Nachweis der Einhaltung der Anforderungen aus dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) erbringen
- Pflichten für Geschäftsleiter
  - Die Maßnahmen zur Risikominimierung müssen bewilligt werden
  - Fortbildung zum aktuellen Stand der Cyberrisiken
- Unterrichtungspflichten
  - Bei erheblichen Sicherheitsvorfällen kann der Bund das betroffene Unternehmen anweisen, die Nutzer des Dienstes zu informieren

caritas Netzwerk IT

NIS 2 in etwas mehr Detail

- Wer
  - Alle Akteure innerhalb der kritischen Infrastrukturen, einschließlich ihrer Zulieferer
  - Verschiedene Sektoren / Subsektoren (siehe nächste Seite)
  - Betreiber kritischer Anlagen bzw. Dienste
  - Höhere Kritikalität (wichtig, sehr wichtig)
  - Ausschluss (z.B. Finanzen, da bereits woanders reguliert)
  - Anzahl Mitarbeiter bzw. Umsatz (50 MA oder >10 Mio€ Bilanzsumme bzw. 250 MA / 42 Mio€ Bilanzsumme)
    - Ausnahmen: keine Größenbegrenzung in manchen Bereichen

caritas Netzwerk IT

NIS 2 in etwas mehr Detail: Wer

- Sektoren mit hoher Kritikalität
  - Energie
  - Verkehr
  - Bankwesen
  - Finanzmarktinfrastrukturen
  - Gesundheitswesen
  - Trinkwasser
  - Abwasser
  - Digitale Infrastruktur
  - Verwaltung von IKT-Diensten (B2B)
  - Öffentliche Verwaltung
  - Weltraum

- Sonstige kritische Sektoren
  - Post- und Kurierdienste
  - Abfallbewirtschaftung
  - Produktion, Herstellung und Handel mit chemischen Stoffen
  - Produktion, Verarbeitung und Vertrieb von Lebensmitteln
  - Verarbeitendes Gewerbe/Herstellung von Waren
  - Anbieter digitaler Dienste
  - Forschung

Quelle: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022L2555

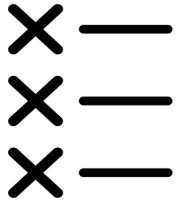
caritas Netzwerk IT

NIS 2 in etwas mehr Detail

- Wann
  - EU-Richtline ist von Deutschland in lokales Recht zu überführen
  - Das Gesetz muss bis 17. Oktober 2024 veröffentlicht werden
  - Vermutlich wird es ab dann Umsetzungsfristen geben, mit erster Nachweispflicht ab ca. 2027
  - Siehe auch https://ag.kritis.info/2023/07/19/referentenentwurf-des-bmi-nis-2-umsetzungs-und-cybersicherheitsstaerkungsgesetz-nis2umsucg/
- Empfehlung
  - Frühzeitig damit auseinander setzen, ob man betroffen sein wird
  - Wenn vermutlich ja (oder auch generell sinnvoll):
    - Umsetzung planen
      - Einführung ISMS dauert typischerweise ca. 2 Jahre
  - Dienstleister in dem Umfeld werden jetzt bereits knapp

caritas Netzwerk IT

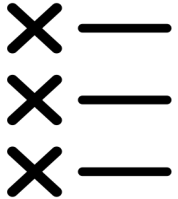
Was kann (und muss!) jede Organisation tun? Angriff unwahrscheinlicher machen



- Security-Awareness-Schulungen & Tests
  - Auch für Vorstände und Aufsichtsräte
  - Nach Angriffen ist plötzlich Geld kein Thema mehr…
  - Beispielhafte Anbieter: SoSafe, KnowBe4, G-Data, …
- Identity & Access-Management ernst nehmen
  - Prozesse, Active Directory, …
- Passwort-Manager & MFA verpflichtend, keine Gruppen-Accounts
- Zugriffe beschränken
  - IP-Adressbereiche/Länder, Need-to-Know-Prinzip, etc.

caritas Netzwerk IT

Was kann (und muss!) jede Organisation tun? Angriff unwahrscheinlicher machen



- Software aktuell halten
- Möglichst wenig eigene IT betreiben
  - Cloud / Rechenzentrum, MS365 oder ähnlich
- Gute Dienstleister nutzen
- Eigene Expertise aufbauen & halten

caritas Netzwerk IT

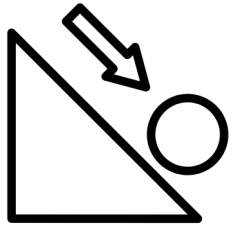
Was kann (und muss!) jede Organisation tun? Folgen eines erfolgreichen Angriffs reduzieren

- Angriffe schnell erkennen & eingrenzen
  - XDR-Systeme, Microsoft Defender
  - 7x24-Überwachrungen: Dienstleister, teuer
  - melden für MA leicht machen
- Ordentliche Backups, Air Gap
  - regelmäßig prüfen!

caritas Netzwerk IT

Was kann (und muss!) jede Organisation tun? Folgen eines erfolgreichen Angriffs reduzieren

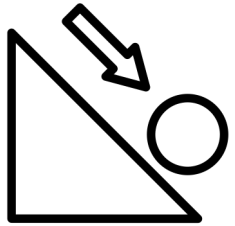
- Zero-Trust-Konzepte einführen/nutzen
- Gut administrierte Systeme
  - Alles immer aktuell halten (wird zunehmend eine Herausforderung…)
  - Active Directory professionell managen
  - Jedes System eigenes Passwort
  - Patch-Management



caritas Netzwerk IT

Was kann (und muss!) jede Organisation tun? Folgen eines erfolgreichen Angriffs reduzieren

- Notfall-Konzept/Handbücher/Vorbereitung gemacht haben (wie im Brandschutz!)
  - Kommunikation
  - Assets / Netzwerke
  - Krisenstab
  - Kontakte Dienstleister / Kunden / Lieferanten
  - Notfälle üben
  - …

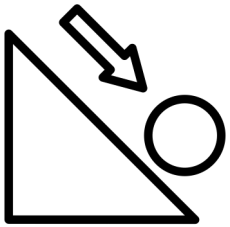


caritas Netzwerk IT

Was kann (und muss!) jede Organisation tun? Folgen eines erfolgreichen Angriffs reduzieren

- Dienstleister-Vertrag haben, Incident & Response
  → siehe später
- Netz-Segmentierung / unterschiedliche Systeme („Brandschutz-Mauern“)
  - Buchhaltung
  - Personalmanagement
  - „Office“
- Eigene Kronjuwelen & Kern-Prozesse kennen und besonders behandeln

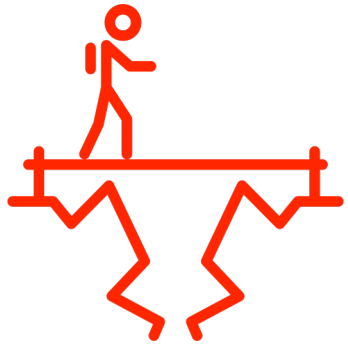
→ bewusstes Risiko-Management machen!



caritas
Netzwerk IT

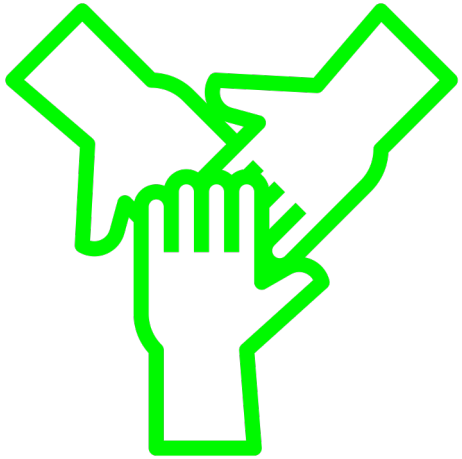
Die Caritas-Welt hat besondere Herausforderungen

- IT / Digitalisierung war kein Kern-Thema
- Keine ordentliche Re-Finanzierung von IT
  - Nicht genügend IT-Expertise & Geld
- Bisherige Investitionen stehen in Frage
  - Rechenzentrum…
  - Eigenes Know-How & eigene Strukturen
- Besonders schützenswerte Daten
- Angst vor Datenschutz, deswegen „nix“ machen
  - Angst vor Einsatz MS365…
- Dezentrale Strukturen



caritas Netzwerk IT

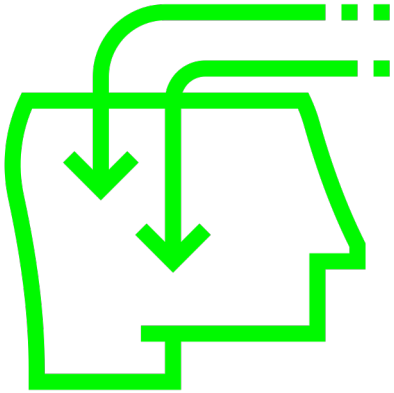
Was können wir gemeinsam tun? Zusammenarbeiten!



- Fähigkeiten schaffen, zusammenzuarbeiten
- Caritas-Netzwerk IT e. V.
  - Gemeinsamer Incident & Response-Dienstleister
  - Austausch Erfahrungen
  - Standardisierung
- Allianz für Cyber-Sicherheit
  - https://www.allianz-fuer-cybersicherheit.de/
- Infos vom BSI anschauen & nutzen

caritas Netzwerk IT

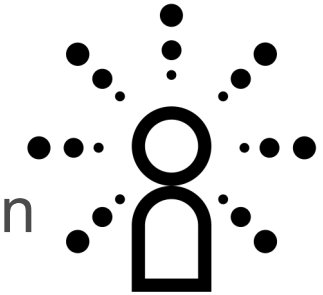
Was können wir gemeinsam tun? Lernen!



- Informell & formell
- Gemeinsame Schulungen, Workshops, etc.
- Analog und digital
- Pro Zielgruppe
  - Auch für Vorstände, Aufsichtsräte & Co.!
- Voneinander aus verschiedenen Perspektiven

caritas Netzwerk IT

Was können wir gemeinsam tun?
Bewusstsein schaffen!

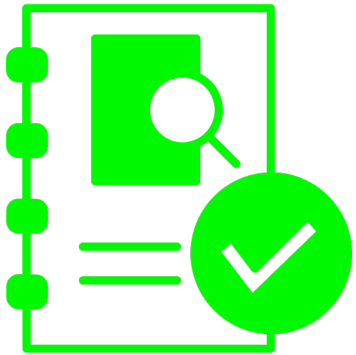


- Jede Gruppe über die Auswirkungen den anderen
- Z.B. Wirtschaftsprüfer ←→ Vorständ:innen/Geschäftsführungen
- Gegenseitig über erfolgreiche Angriffe und deren Konsequenzen informieren
- Was funktioniert besonders gut?
- …?

caritas Netzwerk IT

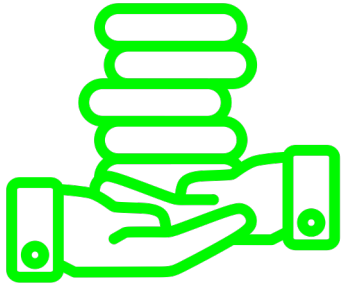
Was können wir gemeinsam tun?
Standards setzen & Good Practice einfordern

- Was muss eingesetzt werden (PW-Manager etc.)
- Gute Lösungen leichter skaliert nutzbar machen
  - egal ob eigene oder fremde
  - gemeinsame DSFA-Templates etc.
- Kostenstruktur IT-Kosten verständlich & erklärbar machen
- Gemeinsame Organisationsprozesse & Tooling entwickeln



caritas Netzwerk IT

Was können wir gemeinsam tun? Übergreifend…



- Übergreifende Tests durchführen
  - Vgl. EZB-Stresstest zu IT-Sicherheit in Banken
- Übergreifende IT- und Organisationsstandards entwickeln
- Gemeinsames Alarming / Notfallplanung / Not-Kommunikation
- Politisch: gemeinsam mit anderen (BAGFW?) über IT-Refinanzierung sprechen

caritas Netzwerk IT

Zusammenarbeit im Caritas-Netzwerk IT: Konkrete Ergebnisse

- Gemeinsamer Incident & Response-Dienstleistungsvertrag
  - 34 Organisationen (von den ca. 140 Mitgliedern) sind in der ersten Welle dabei, auch der Deutsche Caritasverband e. V.
  - Bei erstem Angriff Wichtigkeit schon unter Beweis gestellt: Caritasverband für den Rhein-Erft-Kreis e. V.
  - Gemeinsame Unterlagen, Onboarding, Erfahrungsaustausch, Workshops
  - Welle 2 geplant für Mitglieder (oder welche mit Mitgliedsantrag) Ende Q1/2024, Welle 3 Q4/2024 offen für alle Caritas-Organisationen
- Vorteil zu Versicherungen: „Die Feuerwehr hat schon eine Begehung gemacht“, keine falsche Sicherheit

caritas Netzwerk IT

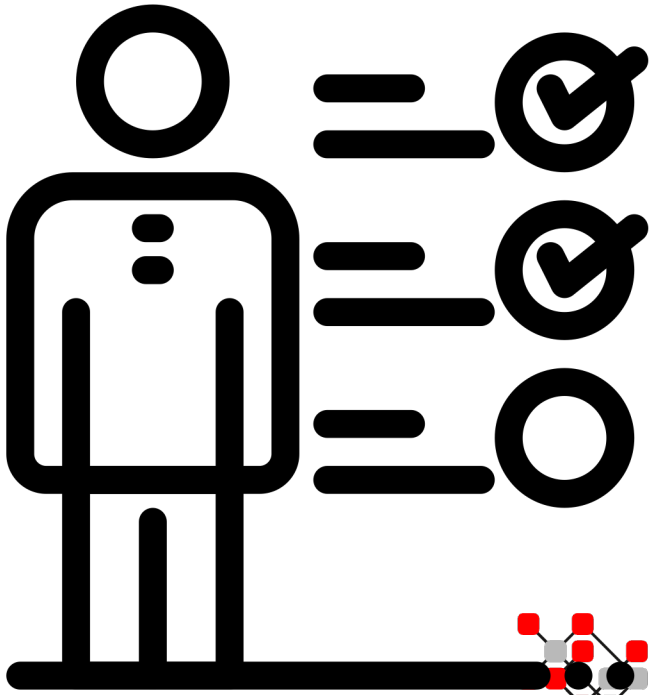
Zusammenarbeit im Caritas-Netzwerk IT: Erfahrungsaustauschgruppen

- Regelmäßiger Erfahrungsaustausch zu Themen wie:
  - Notfallmanagement
    - Incident & Response
    - In Planung: Auf der Basis von BSI-200-4 Notfallplanung
  - Einsatz von Micrsosoft 365
    - Aktuell in Arbeit: Beispiel für Datenschutzfolgeabschätzung, auf der Basis vom Open-Source-Curacon-Excel

caritas Netzwerk IT

Krise als Chance!

- Cyber-Themen zwingen uns zur Professionalisierung & Standardisierung
- Das sollten wir aktiv nutzen!



caritas
Netzwerk IT

Fazit

- Wir alle (individuell und Organisationen/Gesellschaft) müssen Cybersicherheit ernster nehmen als bisher, und viel lernen & tun
- Alleine ist jeder einzelne & jede Organisation überfordert, Zusammenarbeit ist sinnvoll und lohnt sich
  - Trotzdem kann & muss jeder lokal starten und so viel wie möglich tun
- Freie Wohlfahrt: Druck auf politische, rechtliche & finanzielle Rahmenbedingungen (insbesondere IT-Refinanzierung) notwendig, sonst keine nachhaltigen Erfolge möglich

caritas
Netzwerk IT

Buchtipp:
Ransomware und Cyber-Erpressung

https://dpunkt.de/produkt/ransomware-und-cyber-erpressung/

caritas Netzwerk IT

Weitere Referenzen

- https://www.bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf
- https://hub.kpmg.de/hubfs/LandingPages-PDF/eCrimeStudie2022_BF_sec.pdf
- https://www.ibm.com/downloads/cas/YXRVGPLD
- https://www.gdata.de/fileadmin/web/de/documents/Studies/G_DATA_Cybersicherheit_in_Zahlen_2023.pdf

caritas Netzwerk IT

IT-Notfallkarte

Quelle:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/IT-Notfallkarte/it-notfallkarte.html

Bzw. https://www.allianz-fuer-cybersicherheit.de/ACS/IT-Notfallkarte

VERHALTEN BEI IT-NOTFÄLLEN

Ruhe bewahren & IT-Notfall melden
Lieber einmal mehr als einmal zu wenig anrufen!

IT-Notfallrufnummer:

Wer meldet?

Welches IT-System ist betroffen?

Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?

Wann ist das Ereignis eingetreten?

Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

Weitere Arbeit am IT-System einstellen | Beobachtungen dokumentieren | Maßnahmen nur nach Anweisung einleiten

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

Ausgewählte empfehlenswerte Newsletter

- https://www.heise.de/security/
- Newsletter der Allianz für Cybersicherheit (Mitgliedschaft erforderlich)
- Newsletter des BSIs / https://www.bsi.bund.de/DE/Service-Navi/Abonnements/Newsletter/newsletter_node.html
- https://www.security-insider.de/

caritas
Netzwerk IT

Ausgewählte empfehlenswerte Webseiten

- Bundesamt für Sicherheit in der Informationstechnik
  - https://www.bsi.bund.de/
- Allianz für Cyber-Sicherheit
  - https://www.allianz-fuer-cybersicherheit.de/
- BSI Cyber-Sicherheitsnetzwerk
  - https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/cyber-sicherheitsnetzwerk_node.html
- IHK München und Oberbayern:
  - https://www.ihk-muenchen.de/informationssicherheit/
- Stiftung Neue Verantwortung / Deutschlands staatliche Cybersicherheitsarchitektur
  - https://www.stiftung-nv.de/de/publikation/deutschlands-staatliche-cybersicherheitsarchitektur

caritas Netzwerk IT

Ausgewählte empfehlenswerte Podcasts

- IT IST ALLES.
  - https://open.spotify.com/show/46EUTeJsHSfscbkrI38f6p
- CYBERSNACS
  - https://open.spotify.com/show/5TkXmDyddtuomgWBaDreLB
- Update verfügbar
  - https://open.spotify.com/show/1g5qr33CFc2sgxLVvMlbBp
- Security-Insider
  - https://open.spotify.com/show/6gYlq4yncMGiiuMycqUkNK
- You are fucked – Deutschlands erste Cyberkatastrophe
  - https://open.spotify.com/show/6X46fiv5CtByierNT3nFYV

caritas
Netzwerk IT

Folien:
https://www.dropbox.com/scl/fi/94xspx8z5ix7pcy3i9a77/2024-01-15-Cybersicherheit-CNIT-GerhardMueller.pdf?rlkey=d2celsnhmynsc8mm8z7i06gxs&dl=0

Kontakt

Ansprechpartner:
Gerhard Müller, Community Manager

Mobil: +49-179-1338060
gerhard.mueller@caritas-netzwerk-it.de

caritas Netzwerk IT