Cyberwar & öff. Betrieb
Mit Sicherheit?
Ohne Organisation!

Fachvortrag Landesgruppenfachtagung VKU 2023

Neunkirchen, 22.09.2023

GE/CON Kommunale Zukunft

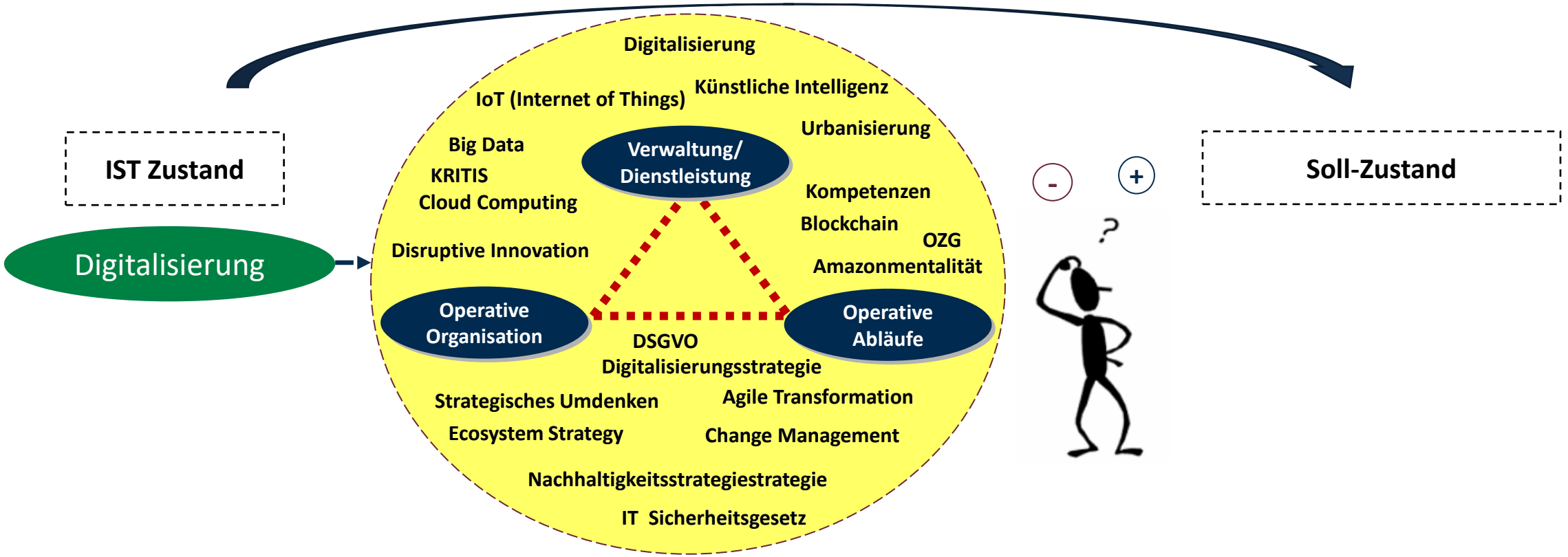
Inhaltsverzeichnis

GE/CON Kommunale Zukunft

Die Rahmenbedingungen kommunalen Handelns ändern sich zeitnah–
Die Digitalisierung ist ein Treiber, nur sicherer wird es auf der Welt nicht

01

Veränderungen lassen sich nicht aufhalten oder verhindern, aber sie lassen sich managen.



2023 zukunftsfähige Organisation - Antworten auf veränderte Rahmenbedingungen **2035**

The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://petya37h5tbhyvki.onion/DAtSQe
   http://petya5koahtsf7sv.onion/DAtSQe

3. Enter your personal decryption code there:

   3bPBup-Rd3Z1r-xrDRS9-XGA1F9-RZTHSB-XyaAmh-b3HWE9-VeYW4i-BemRfv-v1Kk5A-
   DtDLT6-QfdbDF-uehezA-V7b5TP-vcJuRb

If you already purchased your key, please enter it below.

Key: xsC9CAuLWBwjpLt9
Decrypting sector 25178 of 39136 (64%)

Quelle:https://web-assets.esetstatic.com/wls/2016/04/Petya.png

Die digitale Welt wird zunehmend ein Einfallstor für „üble Typen“

Private Nutzung dienstlicher Geräte ist ein zunehmendes Sicherheitsrisiko

01

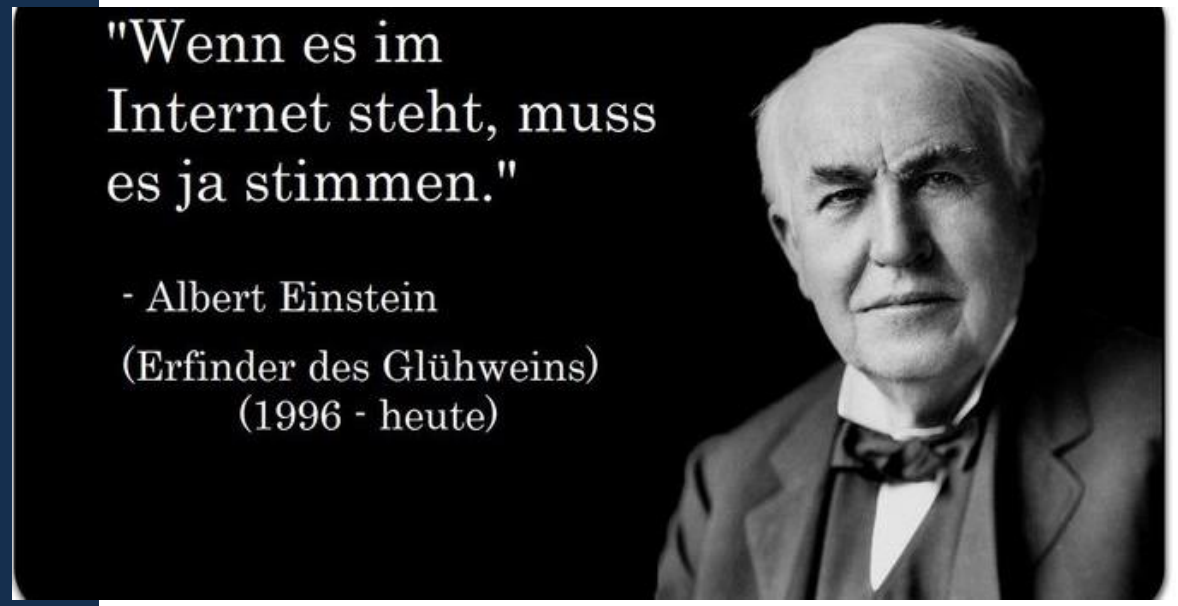
1.Sicherheitsrisiken: Private Apps, Anwendungen und unsichere Internetaktivitäten können Geräte anfälliger für Sicherheitsbedrohungen von außen machen.

2.Datenschutzprobleme: Die Trennung von geschäftlichen und privaten Daten auf denselben Geräten kann schwierig sein.

3.Compliance-Herausforderungen: Die private Nutzung von dienstlichen Geräten kann dazu führen, dass Unternehmen Vorschriften verletzen & rechtlichen Konsequenzen ausgesetzt sind.

4.Erhöhter Verwaltungsaufwand: Die Verwaltung von Geräten und die Durchsetzung von Sicherheitsrichtlinien werden komplexer, wenn private Nutzung erlaubt ist.
Dies erfordert zusätzliche Ressourcen und Technologien, um die Sicherheit zu gewährleisten.

Private Verhaltensweisen haben unmittelbaren Einfluss auf die IT-/ und Cybersicherheit in den kommunalen Betrieben



Kommunale Zukunft

Bildnachweis:
https://twitter.com/rheinfranken/status/810903734423318528/photo/1

Cyber Security was ist das und was müssen wir beachten?
Sechs Schlagwörter zum Einsickern

01

- Netzwerksicherheit
- Programmsicherheit
- Informationssicherheit
- Betriebssicherheit
- Disaster Recovery und Business Continuity
- Endbenutzer-Aufklärung

Unter Cybersicherheit versteht man Maßnahmen, um Computer, Server, Mobilgeräte, elektronische Systeme, Netzwerke und Daten gegen böswillige Angriffe zu verteidigen.

Von der Cyber Security zum Cyber Crime
Thematik ist vielfältig und wird durch verschiedene Täter bespielt

01

Hacking
Unerlaubtes eindringen in fremde Systeme

Spyware
Als Spyware wird üblicherweise Software bezeichnet, die Daten eines Computernutzers ohne dessen Wissen oder Zustimmung an den Hersteller der Software, an Dritte sendet

Phishing
Versand gefälschter E-Mails, die Menschen dazu verleiten sollen, auf einen Betrug hereinzufallen.

Malware
Malware wird mit dem Ziel programmiert, Schaden auf einem eigenständigen Computer oder auf einem vernetzten PC anzurichten.

Denial of Service
Nichtverfügbarkeit eines Internetdienstes, der eigentlich verfügbar sein sollte. Häufigster Grund ist die Überlastung des Datennetzes

Spam-Email
Sammelbegriff für alle Formen von massenhaft versandten, unerwünschten E-Mails, elektronischen Kettenbriefe oder Werbeposts

Cybersicherheit und öffentliche Hand
Drei Thesen die sensibilisieren und aufrütteln sollen

02

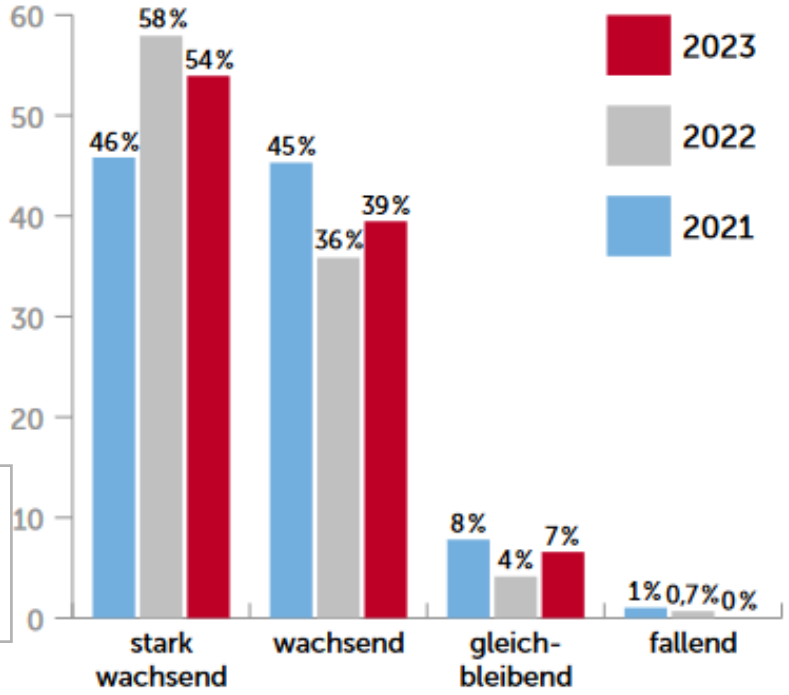
1. Die öffentliche Hand stößt im Bereich Cybersicherheit an die Grenzen Ihrer Fähigkeiten
2. Kommunalen Betrieben fehlen die Ressourcen für eine strategische Befassung mit Cybersicherheit
3. Kommunalen Betriebe fehlt vielfach die organisatorische Power sich den Herausforderungen zu stellen

Herausforderungen

- Kommunen stehen vor einem Cybersicherheits-Knappheitsproblem
- Hacker sind organisatorisch und inhaltlich drei Schritte den „Verteidigern“ in den öffentlichen Betrieben voraus
- Die öffentliche Hand hat eher selten eine Cybersicherheitsstrategie
- Unsere IT-Abteilungen sind nicht auf die Sicherstellung der Cybersicherheit ausgerichtet.
- Die organisatorischen Zusammenhänge zwischen Betrieben und Kommunen verlangsamen viele „Digitalisierungs- und Cyberprozesse
- Der Fokus und der Hauptressourceneinsatz vieler Betriebe liegt auf „der Digitalisierung“ des Unternehmens

Cybersicherheit in Deutschland
Viel Gerede wenig outcome?

Einschätzung der Bedrohungslage bei der IT- Sicherheit*



Quelle: eco e.V.

Lage der IT- Sicherheit in Deutschland 2022 und 2023:

- Phishing bleibt die bevorzugte Angriffsmethode -> 69% aller Spam-Mails waren Cyber- Angriffe
- Professionalität der Angriffe steigt
- Personalmangel gefährden Cybersicherheit
- Geopolitische Krisen als Angriffsvorteil -> Cybercrime (Angriffe auf US-gestützte IT-Infrastruktur)

Conclusio vorweg?:

- „IT-Sicherheit ist eine Reise und ein Prozess – ein permanentes Anpassen“

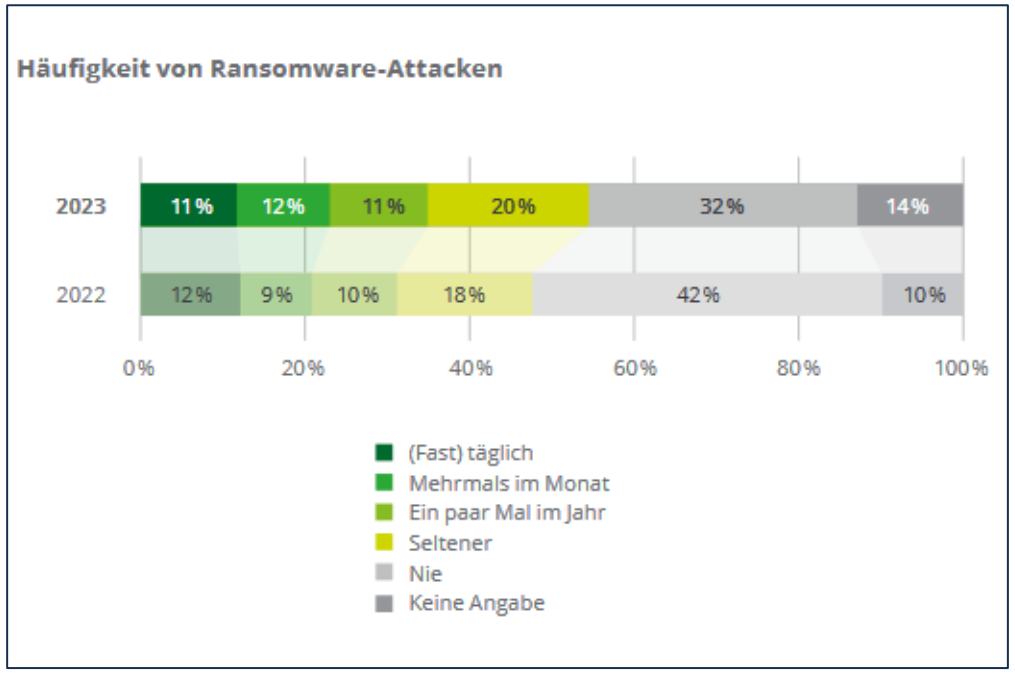
Übergreifende Herausforderungen:

- Vorhandensein digitaler Kompetenzen im Betrieb
- Leistungsfähigkeit der eigenen IT-Abteilung
- Sicherstellung finanzieller Ressourcen zur „Stärkung der Abwehrkraft“

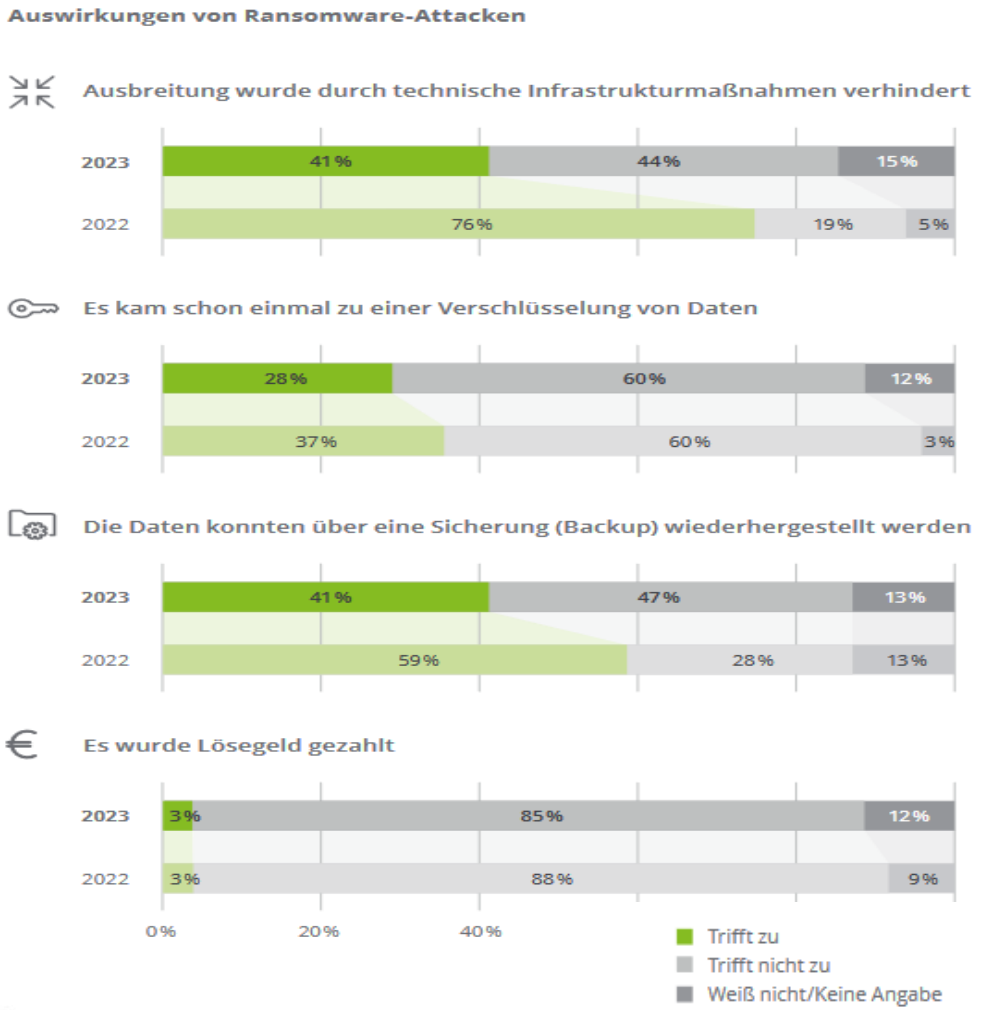
*https://www.eco.de/presse/eco-it-sicherheitsumfrage-2023-viele-unternehmen-unterschaetzen-noch-immer-bedrohungslage/

Geringfügige Zunahme aber Steigerung der Qualität der Cyber-Angriffe

Ransomware-Attacken in ´23 für 1/3 aller Angriffe verantwortlich



Angriffe werden gezielter – Die Abwehr noch nicht effektiver

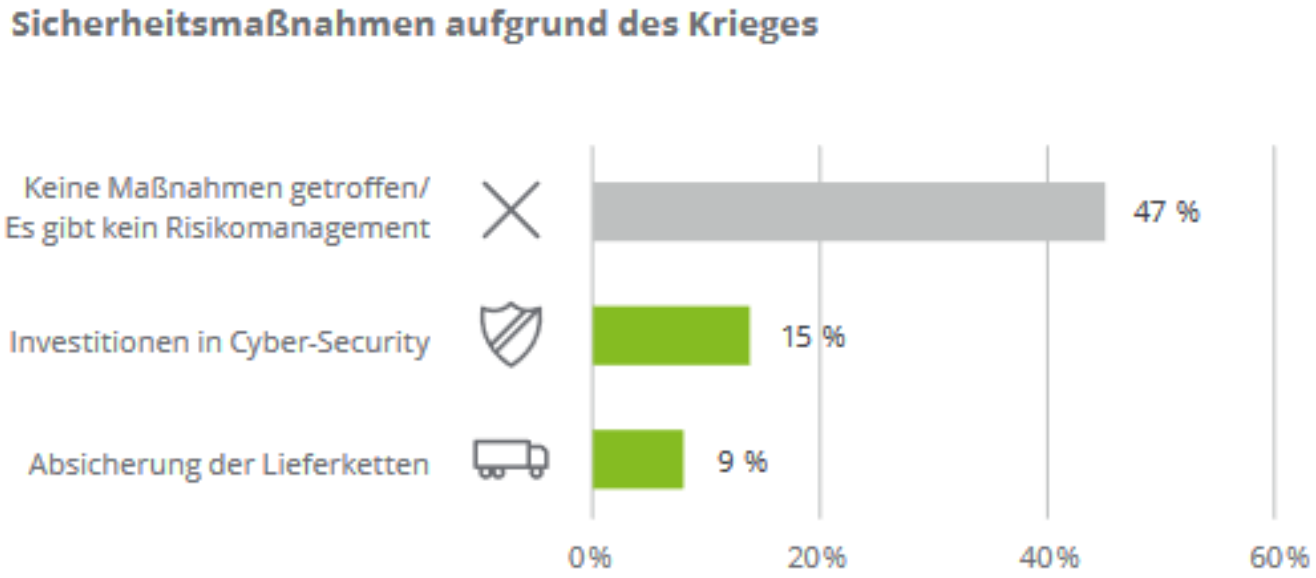


Kommunale Zukunft

Quelle: cyber-security-report-2023; Deloitte

Wie geopolitische Krisen uns zum Handeln zwingen
Oder eben einfach nichts passiert

03

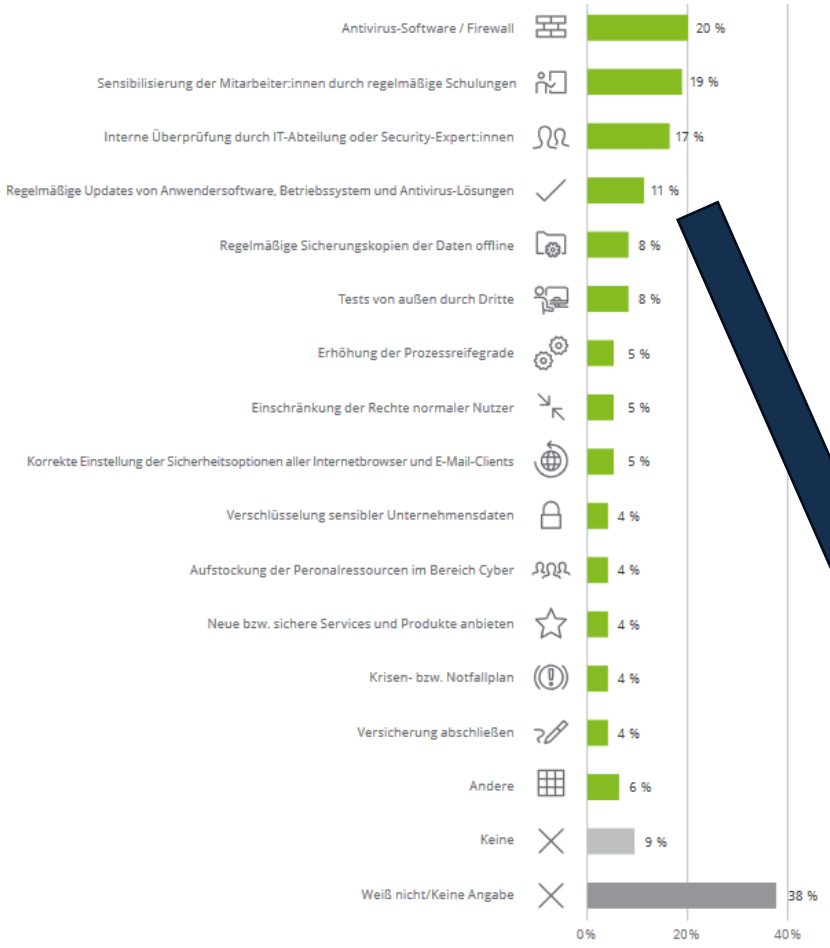


Schutz vor Angriffen aus dem Internet.
Im kommenden Jahr planen 20 % der untersuchten Unternehmen eine Filterung des Traffics mit Antivirus-Software und Firewalls, weitere 19 % fokussieren die Awareness der Mitarbeitenden durch regelmäßige Schulungen. Zudem setzen 17 % der Unternehmen auf Kontrollen ihrer Systeme durch die interne IT-Abteilung oder externe Expertinnen und Experten. Großen Aufholbedarf gibt es bei der Implementierung gezielter technischer Maßnahmen: Lediglich 11 % der Unternehmen wollen derzeit ihre Systeme updaten oder verbessern, 5 % haben vor Zugriffsrechte für Benutzerinnen und Benutzer einzugrenzen.

Quelle: cyber-security-report-2023; Deloitte

Wie gehen Unternehmen mit IT-Sicherheit um?
Was wird eigentlich im Grundsatz überall unternommen?

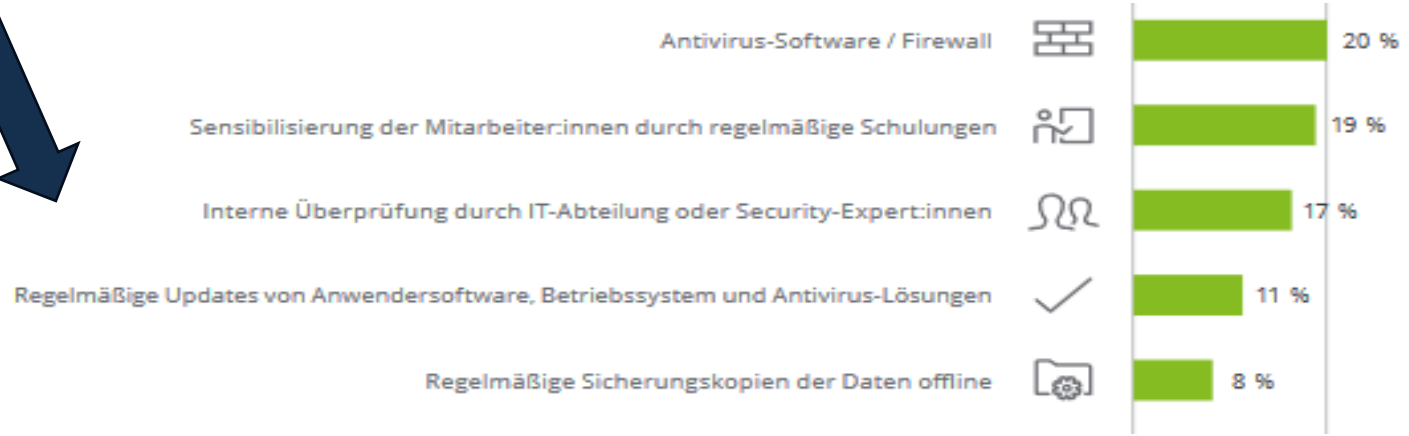
Geplante Maßnahmen zum Schutz vor Cyberattacken



Quo Vadis betriebliche IT-Sicherheit?

- ❑ Cyberbedrohungen kennen keine geografischen Grenzen
- ❑ Cyberbedrohungen kennen keine allgemeingültigen Muster
- ❑ Cyberbedrohungen zielen nicht immer auf Geld

- ➢ Cyberangriffe locken Nachahmer an
- ➢ Cyberangriffe überfordern die Organisation
- ➢ Cyberangriffe kosten Geld (betriebswirtschaftlich)
- ➢ Cyberangriffe führen zu einem Gefühl von & tatsächlichem Kontrollverlust



GE/CON Kommunale Zukunft

Quelle: cyber-security-report-2023; Deloitte

Cybersicherheit und Digitalisierung beginnen im Kopf
Warum handeln wir nicht, wie wir müssten?

04

Zeiteinsatz
Wie viel Zeit in den Bereichen IT, Digi & Cyber erachten wir im Betrieb als Nützlich und Zielunterstützen und vor allem als unsere Aufgabe

Operative Verknüpfung
Verknüpfung zwischen Alltagsgeschäft, „Digitalisierung“, IT-Sicherheit, Weiterbildung.

Welche **Kompetenzen** und **Ressourcen** haben wir über den gesamten Betrieb gedacht beim Thema Digitalisierung, IT und Cyber-Security?

Dokumentation und Prozesse
Zunehmende Digitalisierung führt zu mehr Zeit beim Aufbau und der Betreuung von Abläufen die zu dokumentieren sind

Ressourcen
Der Aufbau von Personalressourcen hat & kostet viel Kraft. -> Der Ausbau von Wissensressourcen über die eigene IT-Abteilung hinaus

GE/CON Kommunale Zukunft

Digitale Kompetenzen werden zunehmend gefragt

Kompetenzen sind für Betriebe von zunehmender Bedeutung

04

1.Kommunikationsfähigkeit: Die Fähigkeit, effektiv mit digitalen Kommunikationstechnologien wie E-Mail, Instant Messaging, Videokonferenzen und sozialen Medien umzugehen, ist in fast allen Arbeitsumgebungen von entscheidender Bedeutung.

2.Flexibilität und Lernbereitschaft: Die Fähigkeit, sich schnell an neue Technologien anzupassen und neue digitale Kompetenzen zu erlernen, ist ebenfalls von grundlegender Bedeutung, da sich die digitale Technologie ständig weiterentwickelt.

3.Anwenderkenntnisse von Office-Software: Die meisten Büroarbeiten erfordern die Verwendung von Office-Software wie Microsoft Word, Excel und PowerPoint, um Dokumente, Tabellen und Präsentationen zu erstellen.

4.Computer-Grundkenntnisse: Zu den grundlegenden digitalen Kompetenzen gehört die Fähigkeit, mit Computern umzugehen, einschließlich grundlegender Computerbedienung, Dateiverwaltung und Netzwerkverbindungen.

5.Datenanalyse und -management: Die Fähigkeit, Daten zu analysieren und zu interpretieren, ist für viele Branchen von Bedeutung. Hierzu gehört auch das Verständnis der Grundlagen von Datenbanken, Datensicherheit und Datenmanagement.

6.Digitale Sicherheit: Angesichts zunehmender Cyber-Angriffe und Datenschutzverletzungen ist ein grundlegendes Verständnis von digitaler Sicherheit, einschließlich Passwortschutz und sicherem Online-Verhalten, unerlässlich.

7.Programmierkenntnisse: In vielen Branchen sind Grundkenntnisse in der Programmierung hilfreich, um Automatisierungsprozesse zu erstellen, Datenanalysen durchzuführen und andere technische Aufgaben zu erledigen.

GE/CON Kommunale Zukunft

Die Organisation als solche wächst durch Ihre Aufgaben
Aber wird in der Organisation in Cyberkategorien gedacht & gehandelt?

04

Verantwortung
You can simply impress your audience and add a unique zing and appeal to your Presentations. Easy to change colors, photos and Text.

Beschreibung
You can simply impress your audience and add a unique zing and appeal to your Presentations. Easy to change colors, photos and Text.

Steuerung
You can simply impress your audience and add a unique zing and appeal to your Presentations. Easy to change colors, photos and Text.

Verknüpfung
You can simply impress your audience and add a unique zing and appeal to your Presentations. Easy to change colors, photos and Text.

Ohne „Organisiertheit“ entsteht in dem Moment des Angriffs Schwäche und Konfusion -> Hierfür kann man sich wappnen

Vier Kategorien in denen die kommunalen Betriebe zu wenig investieren

Cybersicherheit ist nicht ein reines Thema von Gesetzen

Mindset

Digitalisierung & Cybersicherheit sind nicht voneinander zu trennen

Organisation

Handlung wird möglich, wenn organisiert verstanden wird was passiert und wer sich darum kümmert

Ressourcen

Steuerung durch Antizipation menschlichen Verhaltens. Hierauf abgestimmter Ressourceneinsatz

Vorsorge

Cybersicherheit will erlernt werden. Als Idee, Projekt und organisatorische Anlaufstelle

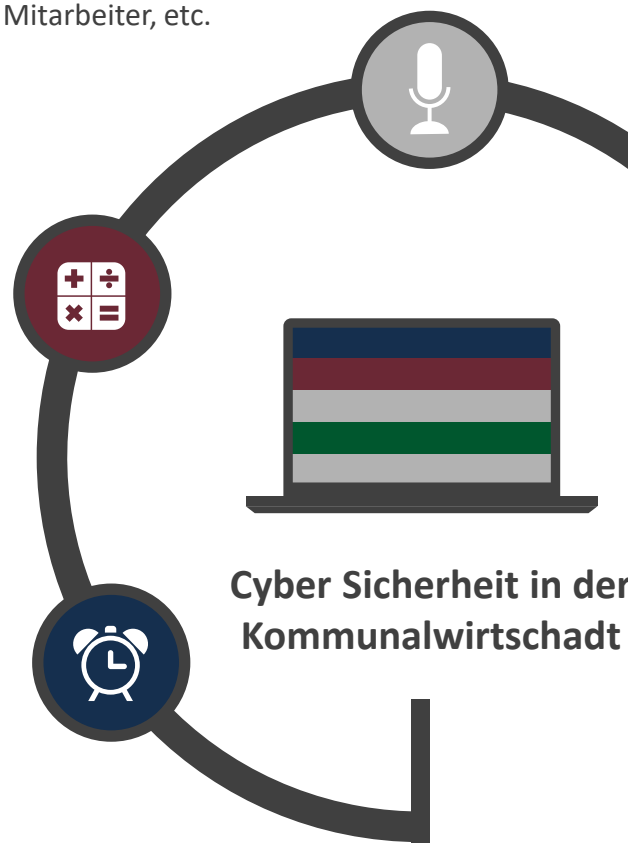
Cyber Security integraler Bestandteil zukunftssicherer Geschäftsmodelle
Auch für die Kommunalwirtschaft?

05

Zunehmender Einsatz von Technik
Benutzung von MDM, Einsatz von LoRa-WAN, Telemetrie auf den Fahrzeugen, Apps für Mitarbeiter, etc.

Digitale Transformation
In Zeiten von Digitalisierung und Disruption ist es für Unternehmen daher unerlässlich, sich mit den Themen Datenschutz und Datensicherheit auseinanderzusetzen.

Datensicherheit
Im Zuge der ordnungsmäßigen Unternehmensführung sind alle Management-Entscheidungen davon gestützt, relevante Informationen zu erzielen.



Was wir uns fragen & gemeinsam diskutieren sollten

- Wie sicher – und wie gefährdet – sind wir? ...
- Wo sollten wir Prioritäten setzen? ...
- Wie können wir die Gefährdung im Laufe der Zeit reduzieren? ...
- Wo stehen wir im Vergleich zu anderen kommunalen Betrieben?

- Was können uns bereits Betroffene mitteilen?
- Befassen wir uns strategisch und organisatorisch mit dem Themenfeld bereits (hinreichend)?
- Haben wir eigene Cybersicherheitsprojekte in der Pipeline?

GE/CON Kommunale Zukunft

Was sind also drei mögliche Handlungsszenarien?
Cybersicherheit selbstbestimmt angehen

05

01

Mindset und Organisation

Wollen/Müssen wir digitaler werden, so wesentlich gefestigter muss unsere Organisation in Sachen Cybersicherheit werden.

02

Ressourceneinsatz überdenken

Bereitstellung/Entwicklung von Ressourcen (Know-how) auch außerhalb der „eigentlichen IT-Abteilung“

03

Starten Sie ein kleines Projekt

Projekte zu diesen Themen steigern die Attraktivität des Unternehmens.

GE/CON Kommunale Zukunft

Projektidee 1: Umsetzung einer CyberGuard-Plattform zur ganzheitlichen Cybersicherheit

05

Um was geht es?

Die Projektidee zielt darauf ab, eine umfassende CyberGuard-Plattform zu entwickeln und umzusetzen, die Unternehmen und Organisationen eine effektive Verteidigung gegen eine breite Palette von Cyberbedrohungen bietet.

Die CyberGuard-Plattform soll eine innovative und integrierte Lösung zur Identifizierung, Analyse und Abwehr von Cyberangriffen bieten. Sie kombiniert modernste Technologien aus den Bereichen künstliche Intelligenz, maschinelles Lernen, Verhaltensanalyse und automatisierte Reaktion, um eine proaktive und reaktive Cybersicherheits-strategie zu ermöglichen.

Projektidee 2: Umsetzung eines ResilienceX-Programms zur Stärkung der unternehmensweiten Resilienz und Widerstandsfähigkeit

05

Um was geht es?

Die Projektidee zielt darauf ab, ein ganzheitliches ResilienceX-Programm in einem Unternehmen zu entwickeln und umzusetzen, um die Widerstandsfähigkeit gegenüber internen und externen Störungen zu erhöhen und sicherzustellen, dass das Unternehmen auch in Zeiten von Unsicherheit und Veränderung erfolgreich agieren kann.

Das ResilienceX-Programm soll eine strategische Initiative sein, die darauf abzielt, das Unternehmen besser auf unvorhersehbare Ereignisse, Risiken und Veränderungen vorzubereiten. Es umfasst die Entwicklung von Strategien, Prozessen und Maßnahmen, um eine umfassende Resilienz in verschiedenen Bereichen des Unternehmens zu erreichen.

Ihre Ansprechpartner:

Erik Schmidtmann

Dipl.-Kfm.

Geschäftsführer

schmidtmann@gecon.gmbh

06201 7100 640

Eric Schramm

Wirtschaftspädagoge

Berater

schramm@gecon.gmbh

06201 7100 640

Sascha Pröhl

Politikwissenschaftler

Senior-Berater

proehl@gecon.gmbh

06201 7100 640

GE/CON Kommunale Zukunft

Werderstrasse 4
69469 Weinheim

Tel.: 06201 7100 640
Fax: 06201 7400 655

www.gecon.gmbh