



Cyber Security Roundtable Liechtenstein

Was tun, wenn die Lösegeldforderung kommt?

malean



«Empathy first: humane security»

David Mantock

Group Director of Information Security and CISO

DocMorris AG



«Cyberangriff: Sprechen wir Klartext»

Andreas Plüer

Leiter Digital Services

EKT AG

Cyberangriff – sprechen wir Klartext!



Erfahrungsbericht Cyberattacke

Sprechen wir Klartext!

- Was ist bei der Cyberattacke passiert?
- Weshalb war der Cyberangriff erfolgreich?
- Welche Vorkehrungen erschweren Cyberangriffe?



Vorgeschichte



Quelle: Meier Tobler AG



Quelle: Meier Tobler AG

Ruhe vor dem Sturm



Quelle: shanemyersphoto



Quelle: LAAX / Danuser

Die SMS, mit der mein Alptraum begann...



Angriff!



EKT: Cyberattacke – sprechen wir Klartext!

Zeitlicher Ablauf Cyberangriff 23./24.07.19



Ungewöhnliches Verhalten IT-Überwachungssysteme festgestellt, unübersichtliche Gesamtlage für IT-Dienstleister, Eskalation innerhalb Piktetorganisation



Befund: Malware-Attacke! Sofortiges Herunterfahren aller Systeme. Alarmierung Kunde (CIO-Stv. , CFO)



Geschäftsleitung durch CFO informiert



Krisenstab einberufen, Information der Führungskräfte, Bezug «War Room»



CIO eingetroffen, erste Krisenstabsitzung zur Lagebeurteilung, Beschluss von Sofortmassnahmen



Schadensbild ermittelt, externe Cyber Security Spezialisten aufgeboden



Priorisierung erstellt, Wiederherstellungsarbeiten gestartet

Beitrag SRF Börse vom 26.07.19



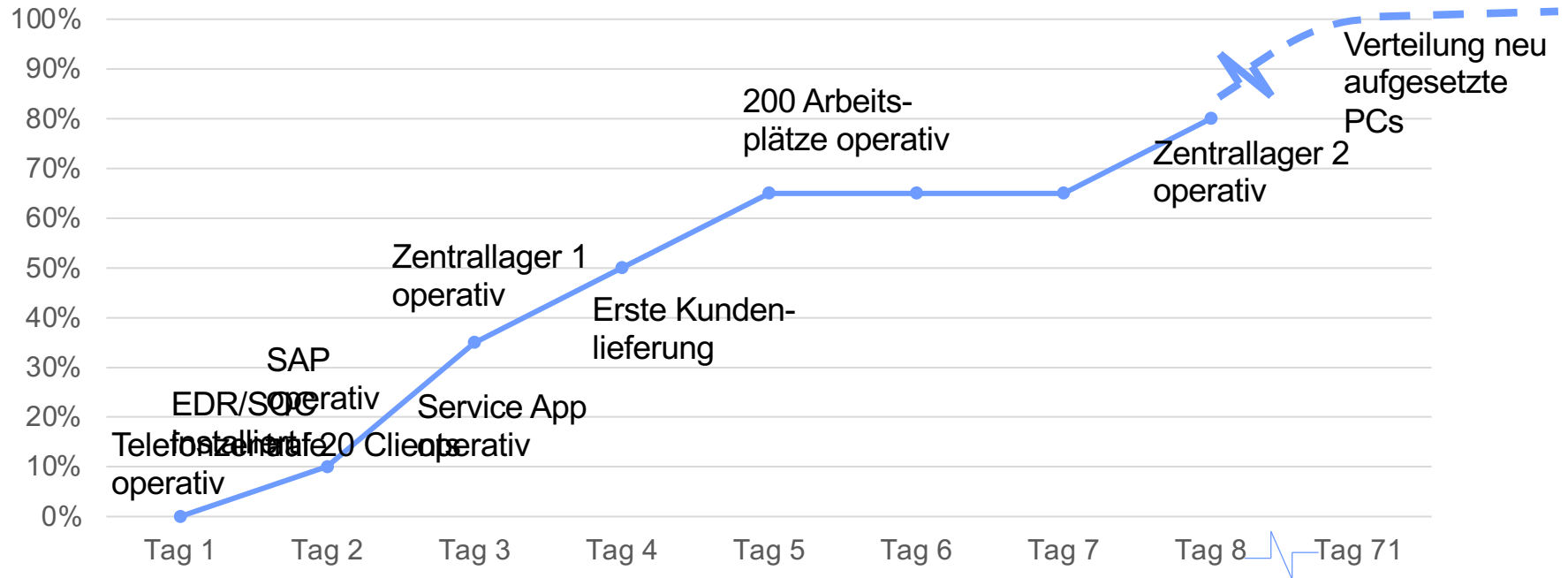
Krisenbewältigung – auf der Zeitachse

Liefer- und Servicebereitschaft in %

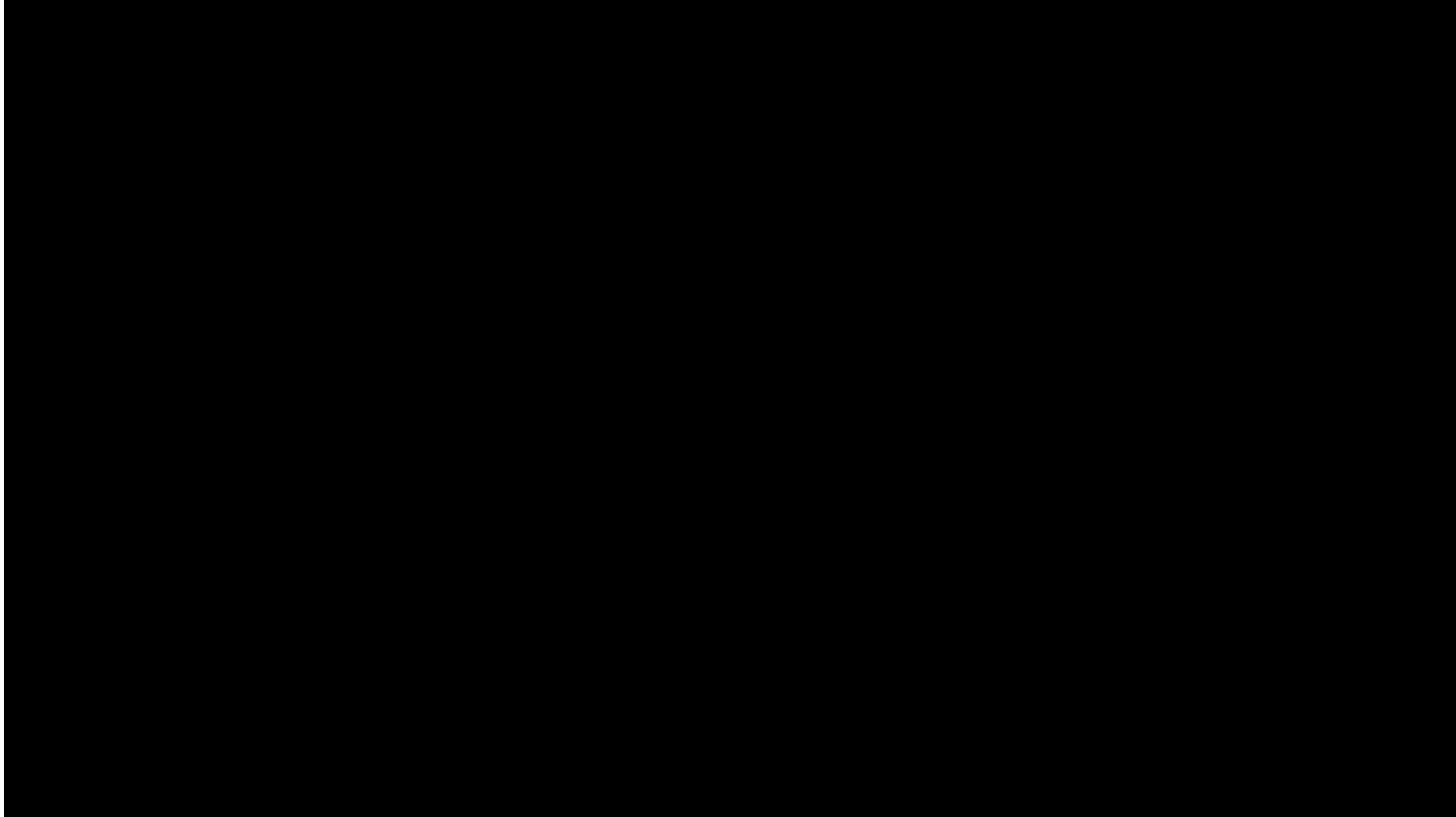


Krisenbewältigung – auf der Zeitachse

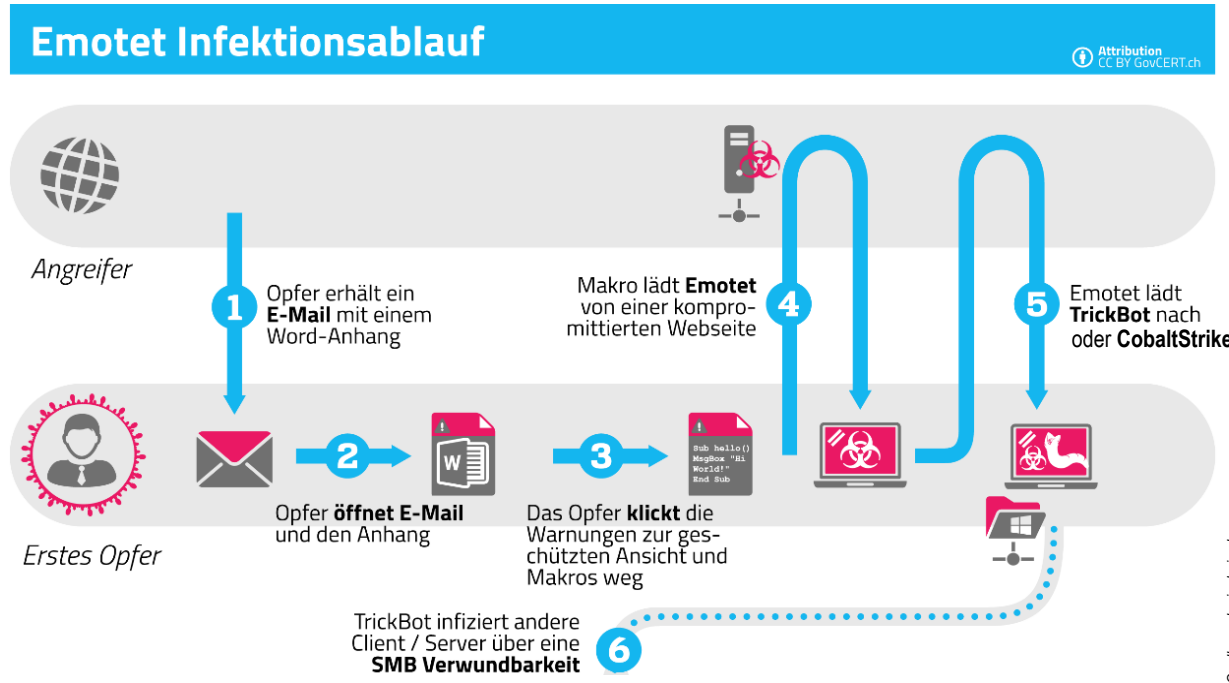
Liefer- und Servicebereitschaft in %



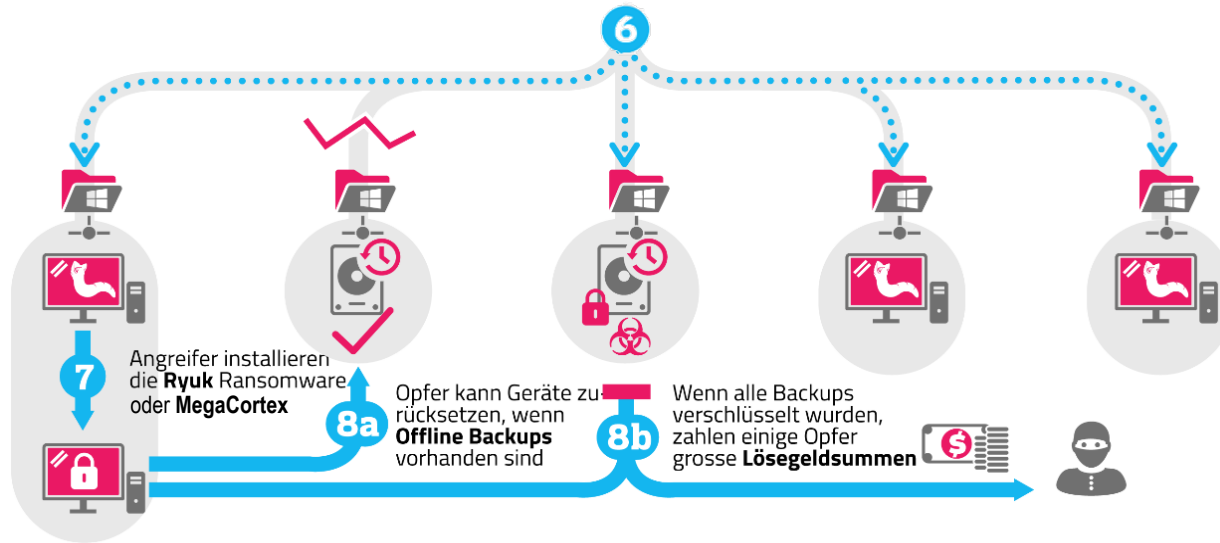
Krisenstab im «War Room»



Das Vorgehen der Angreifer



Das Vorgehen der Angreifer



Erfahrungsbericht Cyberattacke

Sprechen wir Klartext!

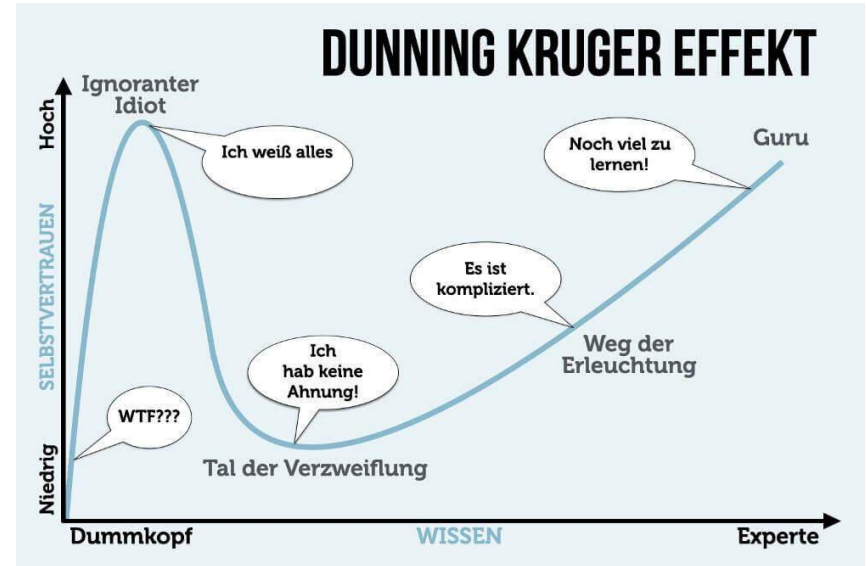
- Was ist bei der Cyberattacke passiert?
- **Weshalb war der Cyberangriff erfolgreich?**
- Welche Vorkehrungen erschweren Cyberangriffe?



Publikumsumfrage

Glauben sie, dass sie zu den
besseren 50% der
Autofahrenden in diesem
Raum gehören?

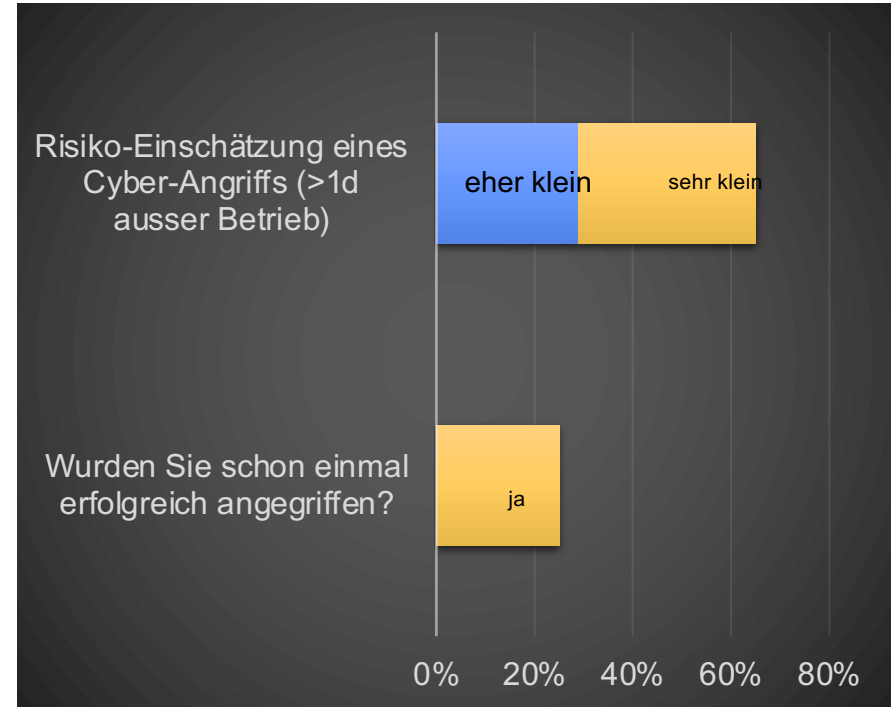
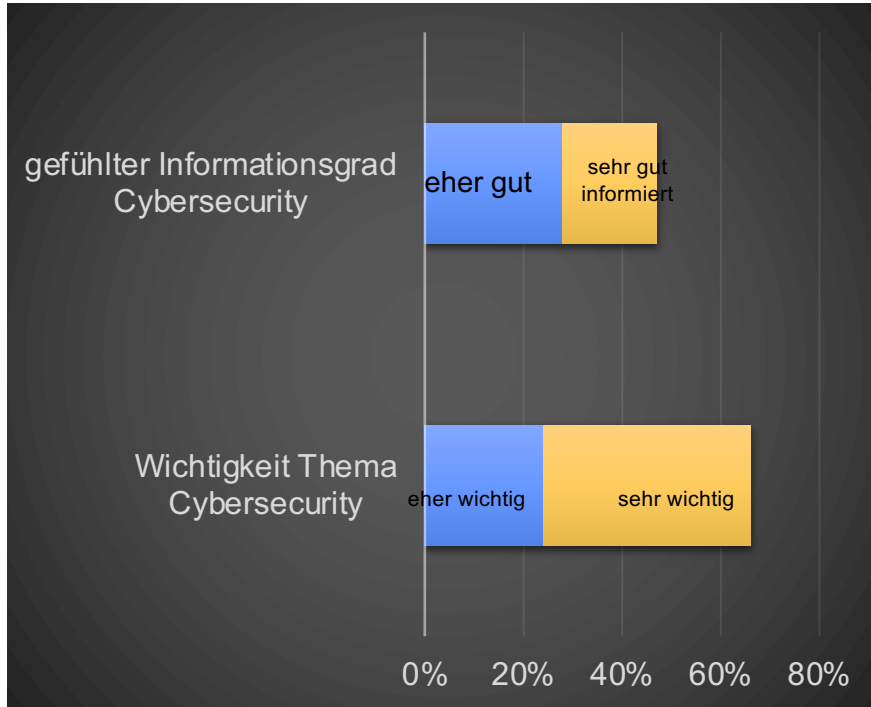
Exkurs zum Thema «Selbstüberschätzung»



Quelle: www.gutefrage.net

Exkurs zum Thema «Selbstüberschätzung»

Studie GFS Zürich (2020, n=503 KMU)



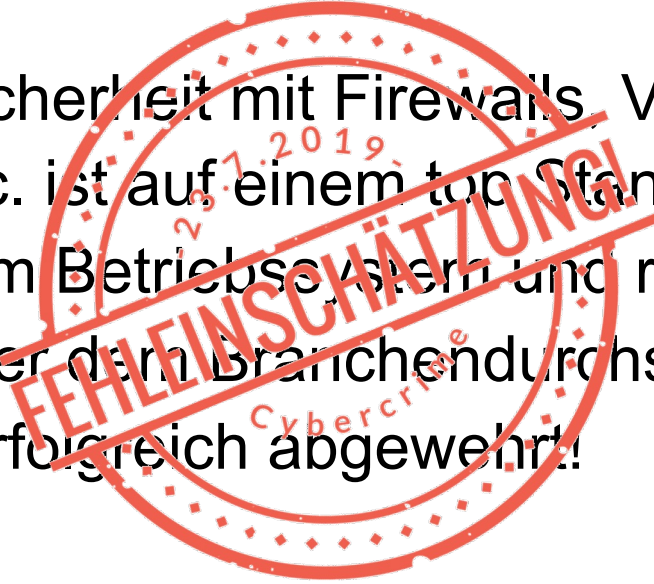
Fehleinschätzungen im Vorfeld – Klartext

Unsere Unternehmung ist in einer traditionellen Branche in der Schweiz tätig. Wir sind keine Bank und stehen nicht im Fokus von Cyberangriffen. Weshalb sollen wir auch ein lukratives Ziel für Hacker sein?



Fehleinschätzungen im Vorfeld – Klartext

Unsere Perimetersicherheit mit Firewalls, Virens Scanner, Anti-Spam-Lösungen etc. ist auf einem top Stand. Server und Clients auf neuestem Betriebssystem und regelmässig gepatched, alles über dem Branchendurchschnitt. Bisher wurde noch jeder Angriff erfolgreich abgewehrt!



Fehleinschätzungen im Vorfeld – Klartext

Wir führten eine 2-monatige Cybercrime Awareness-Kampagne mit allen 1'200 Mitarbeitenden mit simulierten Phishing-Mails durch. Bei uns fällt doch niemand mehr auf Phishing rein!



Fehleinschätzungen im Vorfeld – Klartext

Unsere IT wird im Outsourcing durch absolute Profis betrieben.
Alles sicher, die machen nichts anderes, den ganzen Tag!



Fehleinschätzungen im Vorfeld – Klartext

Ich lese ja regelmässig über diese Cyberangriffe und muss meine Geschäftsleitung immer wieder über meine Lageeinschätzung informieren. Ich kenne mich in diesem Thema Cyberkriminalität doch aus!



Erfahrungsbericht Cyberattacke

Sprechen wir Klartext!

- Was ist bei der Cyberattacke passiert?
- Weshalb war der Cyberangriff erfolgreich?
- Welche Vorkehrungen erschweren Cyberangriffe?

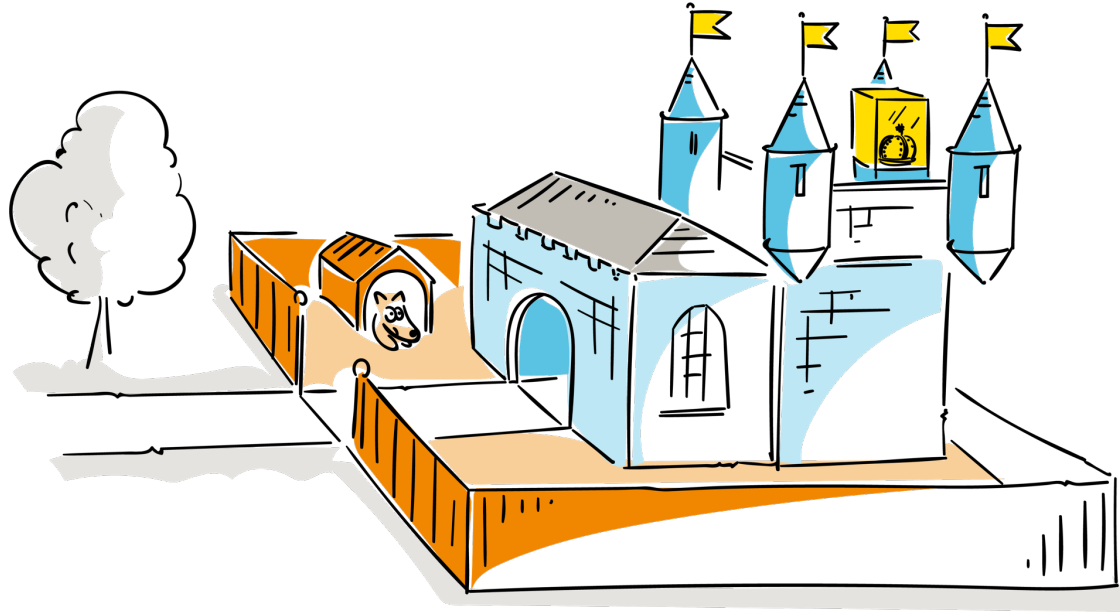


Welche Vorkehrungen erschweren Cyberangriffe?

- Zuständigkeiten festlegen – auf Unternehmensleitung!
- IT-Inventar führen – nur was ich kenne, kann ich schützen!
- Regelmässige Datensicherung durchführen – und testen!
- Updates einspielen – regelmässig und zeitnah!
- Makros deaktivieren – über Gruppenrichtlinien!
- Schutzprogramme verwenden – und bei sicherheitsrelevanten Vorfällen reagieren!
- Richtlinien für Passwörter – und Zwei-Faktor-Authentifizierung für Remote-Anmeldung!
- Mail-Accounts absichern – dies ist das Hauptziel für viele Cyberkriminelle!
- Zonen-Segmentierung des Netzwerks – und keine noch privilegierten User in Benutzerzonen!
- Regelmässige Information und Sensibilisierung der AnwenderInnen – notwendig, aber nicht hinreichend!
- Den Ernstfall vorbereiten – und üben!



Welche Vorkehrungen erschweren Cyberangriffe? Klartext!



Fragen und Antworten



EKT:

Cyberattacke – sprechen wir Klartext

Energie.
Daten.
Zukunft.

EKT AG

Bahnhofstrasse

37

9320 Arbon

T 071 440 61 11

info@ekt.ch

Andreas Plüer

Bereichsleiter Digital Services

D 071 440 63 33

andreas.plueer@ekt.ch

Empathy First

- Humane Security

David Mantock
Group Director of Digital Trust and
Chief Information Security Officer
DocMorris AG



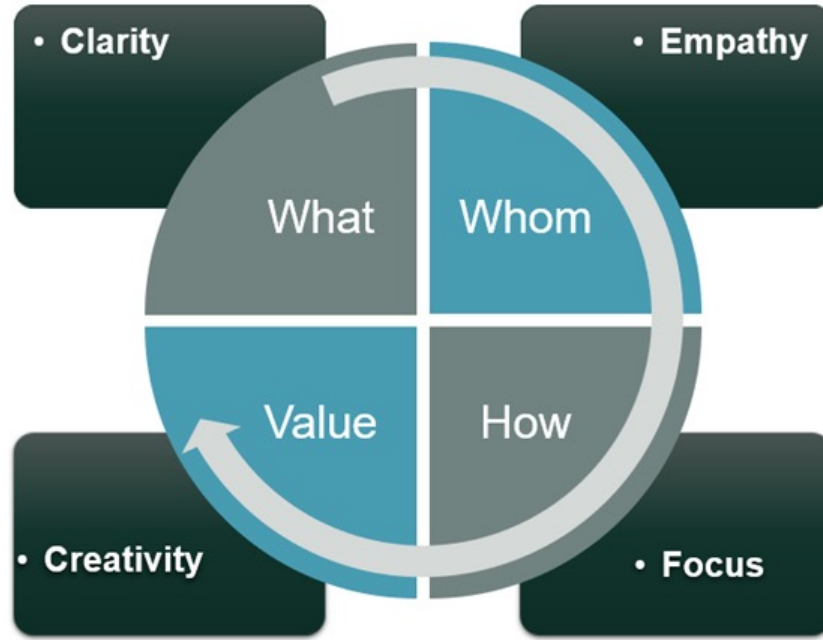
Agenda

- 7 June 2023

1. Why and how empathy first?
 - I. Covid 2020 and NCSC
2. A Strategic Approach
3. Winning components
 - I. Mindfulness
 - II. NVC
4. A Use case
 - I. Security Champions
5. Summary



Empathy First



👉 A Strategic Approach

Mindfulness

- Paying attention, in a particular way: on purpose, in the present moment, and non-judgementally. - Jon Kabat-Zinn



Source: <https://www.joyofmindfulness.com/>

Mindfulness

-
- Getting started: The raisin exercise




Observations

Feelings

Needs

Requests



Want to read the 1 book Microsoft CEO Satya Nadella gave his managers that transformed their culture from cutthroat to creative?

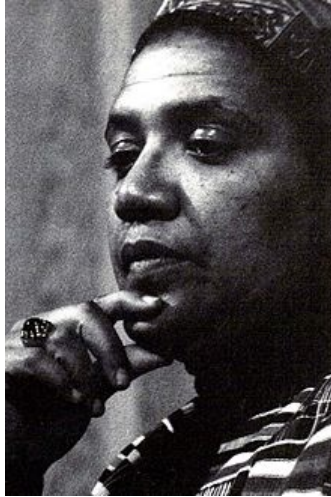
SHOP NVC ABOUT NONVIOLENT COMMUNICATION ABOUT MARSHALL ROSENBERG FREE P



Empathy First!

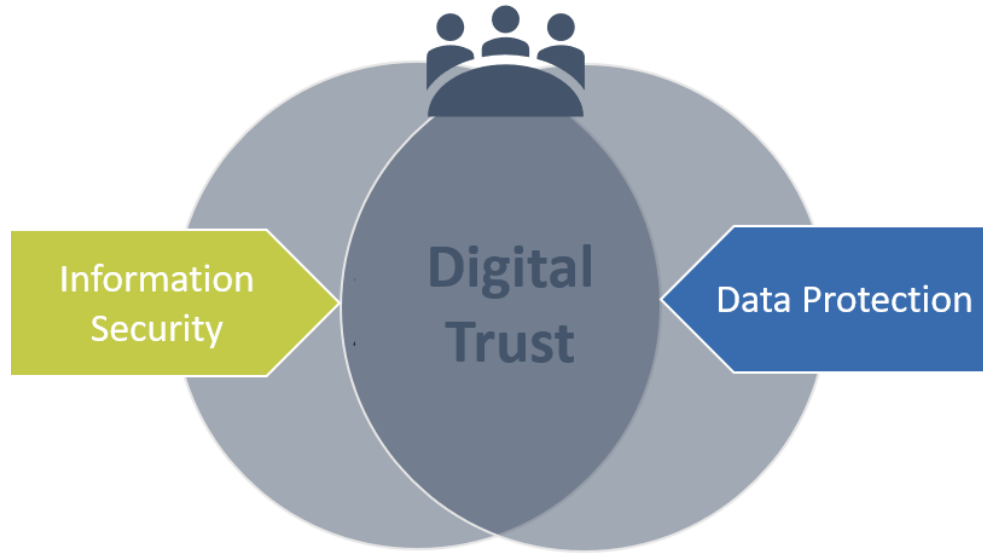


Non-violent Communication



*Our feelings are our most
genuine paths to knowledge –
Audre Lorde*

Non-violent Communication



Digital Trust Champions

Agenda

- How are you round?
- Retrospective →
- Security theme
- Communication theme

Tool: Retrospectives

- What was good?
- What was not so good?
- What have we learnt?
- What still confuses me?



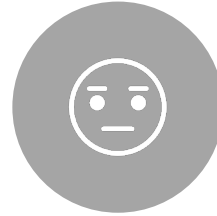
Digital Trust Champions



Summary



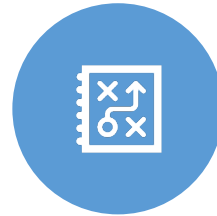
1 . If you want to be heard learn how to listen



2. Feelings are important



3. Transparency builds trust



4. A strategic approach is a must

[1] [Mindfulness](#)

[2] Finding the Space to Lead – Janice Marturano

[3] The Mindfulness Edge – Matt Tenney, Tim Gard

[4] [Nonviolent communication \(NVC\)](#)

[5] Nonviolent Communication: A Language of Life –
Marshall B. Rosenberg



References