CANCOM CYBER SECURITY

# 7 FRAGEN – 7 ANTWORTEN

CANCOM Lösungen für die aktuell dringendsten Fragen im Bereich IT-Security

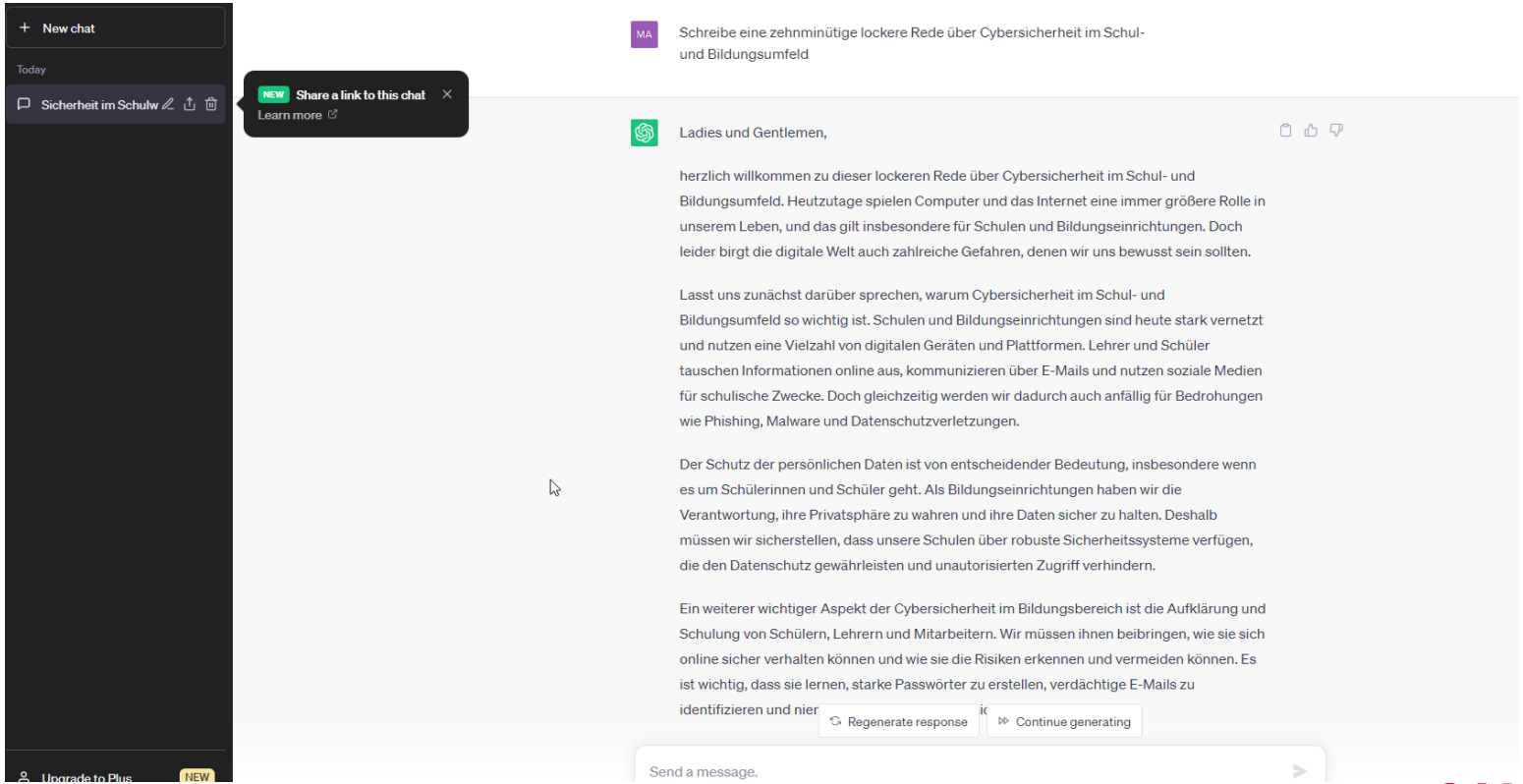
Sprecher: Marc Eilert

CANCOM

PLAN.
BUILD.
PERFORM.

Autor: Holger Müller, Jesper Schulz, Alexander Ernst

# HELLO WORLD


New chat
Today
Sicherheit im Schulw
NEW
Share a link to this chat
Learn more
Upgrade to Plus
NEW
MA
Schreibe eine zehnminütige lockere Rede über Cybersicherheit im Schul- und Bildungsumfeld
Ladies und Gentlemen,
herzlich willkommen zu dieser lockeren Rede über Cybersicherheit im Schul- und Bildungsumfeld. Heutzutage spielen Computer und das Internet eine immer größere Rolle in unserem Leben, und das gilt insbesondere für Schulen und Bildungseinrichtungen. Doch leider birgt die digitale Welt auch zahlreiche Gefahren, denen wir uns bewusst sein sollten.
Lasst uns zunächst darüber sprechen, warum Cybersicherheit im Schul- und Bildungsumfeld so wichtig ist. Schulen und Bildungseinrichtungen sind heute stark vernetzt und nutzen eine Vielzahl von digitalen Geräten und Plattformen. Lehrer und Schüler tauschen Informationen online aus, kommunizieren über E-Mails und nutzen soziale Medien für schulische Zwecke. Doch gleichzeitig werden wir dadurch auch anfällig für Bedrohungen wie Phishing, Malware und Datenschutzverletzungen.
Der Schutz der persönlichen Daten ist von entscheidender Bedeutung, insbesondere wenn es um Schülerinnen und Schüler geht. Als Bildungseinrichtungen haben wir die Verantwortung, ihre Privatsphäre zu wahren und ihre Daten sicher zu halten. Deshalb müssen wir sicherstellen, dass unsere Schulen über robuste Sicherheitssysteme verfügen, die den Datenschutz gewährleisten und unautorisierten Zugriff verhindern.
Ein weiterer wichtiger Aspekt der Cybersicherheit im Bildungsbereich ist die Aufklärung und Schulung von Schülern, Lehrern und Mitarbeitern. Wir müssen ihnen beibringen, wie sie sich online sicher verhalten können und wie sie die Risiken erkennen und vermeiden können. Es ist wichtig, dass sie lernen, starke Passwörter zu erstellen, verdächtige E-Mails zu identifizieren und nier
Regenerate response
Continue generating
Send a message.

# LERNWOLKE MIT KI

## Reaktion auf ChatGPT: Acht Bundesländer planen Lernwolke mit KI

Die neue Schulcloud soll den Leistungsstand von Schülern in einer Lerneinheit automatisiert messen und ihnen individuell Aufgaben zuweisen. Ein Test lief schon.

Lesezeit: 3 Min. In Pocket speichern 22


(Bild: metamorworks/Shutterstock.com)

**06:33 Uhr**

*Von Stefan Krempl*

Künstliche Intelligenz (KI) mit den eigenen Waffen schlagen, lautet offenbar der

## "Zugeschnitten auf die individuellen Bedürfnisse"

Zum Einsatz gekommen sei eine Lösung des Anbieters Area 9 Lyceum, der seine Hauptsitze auf Kopenhagen und Boston verteilt hat und eine deutsche Niederlassung in Leipzig betreibt. Die Firma bezeichnet sich selbst als "Marktführer für adaptive Lernsysteme". Die eigene Lernplattform ermögliche den Wissenserwerb "zugeschnitten auf die individuellen Bedürfnisse jedes Einzelnen". Dem Bericht zufolge setzt das Unternehmen für das Erstellen von Lerneinheiten inzwischen auch das generative Sprachmodell ChatGPT ein. Im Rahmen der unmittelbar bevorstehenden Ausschreibung für die KI-Lernwolke müsse es sich aber neu bewerben. Insgesamt sollen 55 Millionen Euro aus dem Etat für länderübergreifende Projekte in die Entwicklung des Systems fließen, heißt es bei Table.Media. Unter Federführung Sachsens beteiligten sich Brandenburg, Hessen, Mecklenburg-Vorpommern, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen-Anhalt und das Saarland.

CANCOM

# .. UND DANN AUCH NOCH DAS

## Software Probleme, kann man nichts machen

### Vermutlich KI-Training: Massenhafte Zugriffe kicken Internet Archive offline

Übers verlängerte Wochenende war das Internet Archive Ziel von vermutlich unabsichtlichen DDoS-Attacken. Der Verdacht fällt auf ein unbedachtes KI-Training.

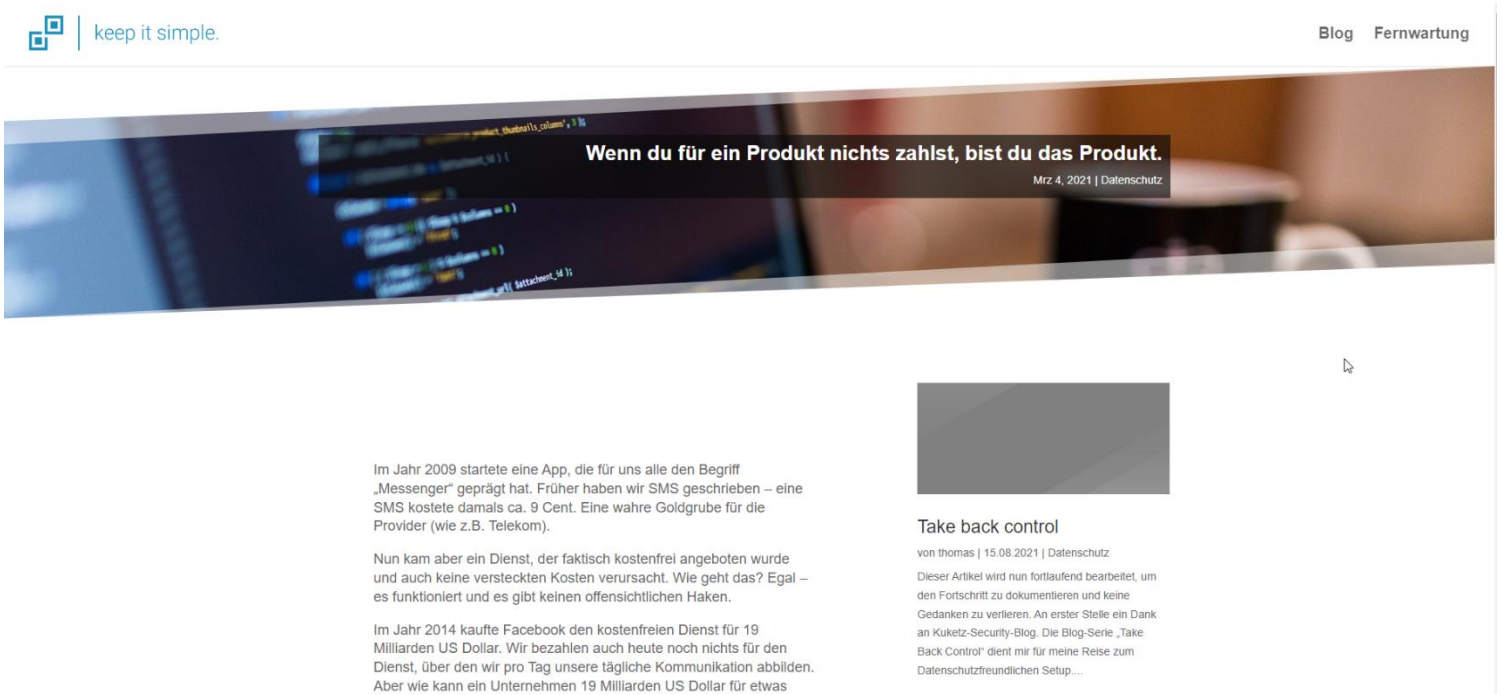
Lesezeit: **3 Min.** In Pocket speichern 15

(Bild: Timofeev Vladimir/Shutterstock.com)

**30.05.2023 08:44 Uhr**

*Von Martin Holland*

# FREE, AT LAST




CANCOM

# MULTIFAKTOR


CANCOM

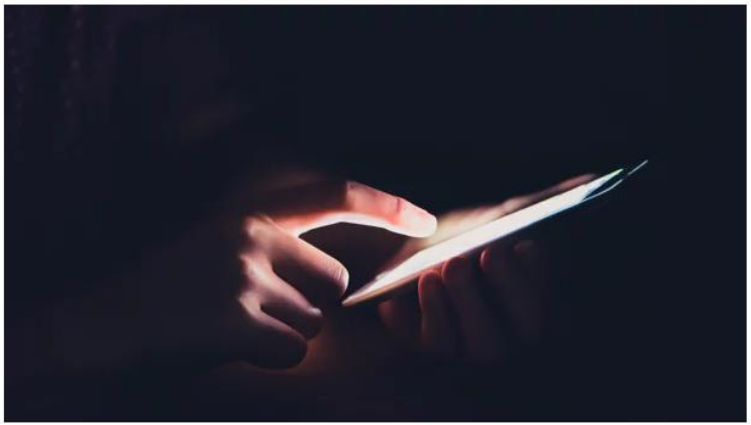
# VERSCHLÜSSELUNG IST EHER NICHT SO MEIN DING

heise online > Überwachung > **Chatkontrolle: Spanien plädiert für EU-Verbot von Ende-zu-Ende-Verschlüsselung**

## Chatkontrolle: Spanien plädiert für EU-Verbot von Ende-zu-Ende-Verschlüsselung

Die EU-Staaten diskutieren über die Pläne zur sogenannten Chatkontrolle. Ein geleaktes Dokument macht jetzt deutlich, wie extrem die Positionen teilweise sind.

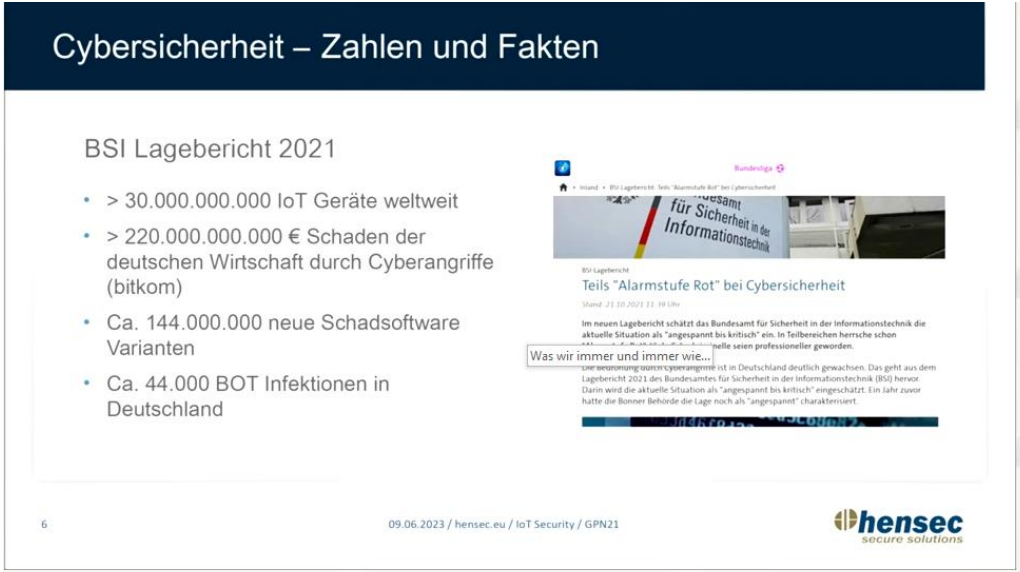
Lesezeit: **3 Min.** In Pocket speichern 358

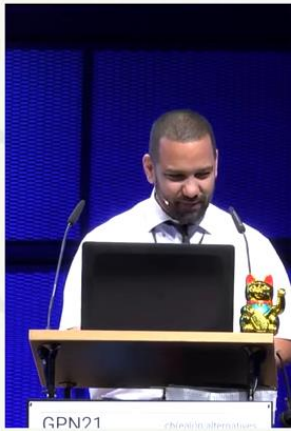


CANCOM

# HEUTE DANN MAL IOT

**ETSI EN 303 645**




Kevin Heneka: IoT Cybersecurity - EU Normenupdate

media.ccc.de

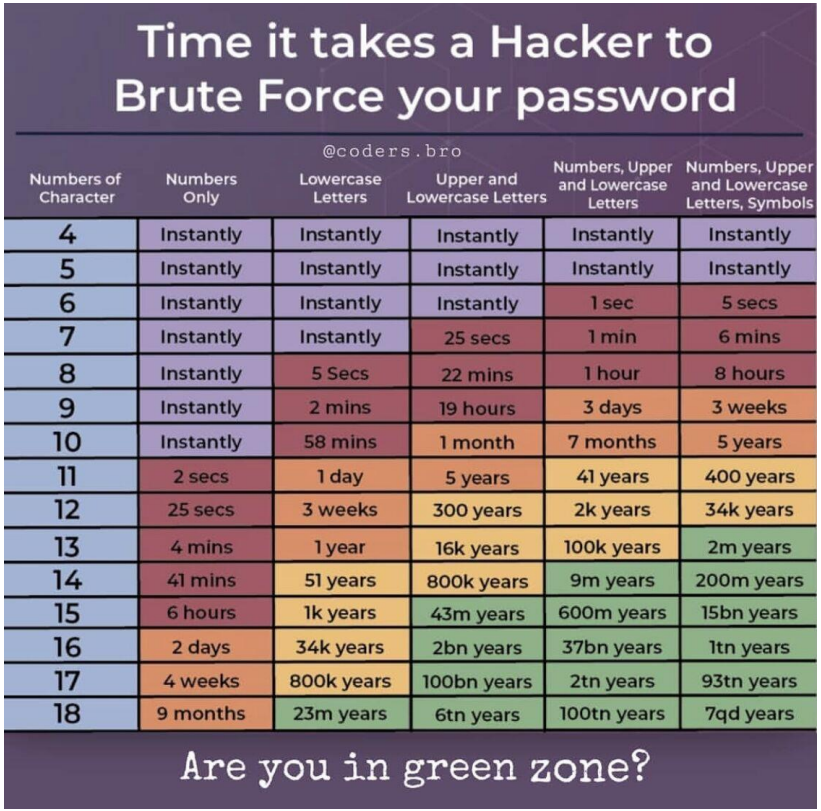
CANCOM

# WAS WIR IMMER UND IMMER WIEDER VON KUNDEN HÖREN

**Security Bull-Shit Bingo überfordert uns**

Zu viele gleichzeitige Security Projekte ohne Priorisierung

**Zu wenig Fachkräfte und Know-How**




| Numbers of Character | Numbers Only | Lowercase Letters | Upper and Lowercase Letters | Numbers, Upper and Lowercase Letters | Numbers, Upper and Lowercase Letters, Symbols |
|---|---|---|---|---|---|
| 4 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 5 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 6 | Instantly | Instantly | Instantly | 1 sec | 5 secs |
| 7 | Instantly | Instantly | 25 secs | 1 min | 6 mins |
| 8 | Instantly | 5 Secs | 22 mins | 1 hour | 8 hours |
| 9 | Instantly | 2 mins | 19 hours | 3 days | 3 weeks |
| 10 | Instantly | 58 mins | 1 month | 7 months | 5 years |
| 11 | 2 secs | 1 day | 5 years | 41 years | 400 years |
| 12 | 25 secs | 3 weeks | 300 years | 2k years | 34k years |
| 13 | 4 mins | 1 year | 16k years | 100k years | 2m years |
| 14 | 41 mins | 51 years | 800k years | 9m years | 200m years |
| 15 | 6 hours | 1k years | 43m years | 600m years | 15bn years |
| 16 | 2 days | 34k years | 2bn years | 37bn years | 1tn years |
| 17 | 4 weeks | 800k years | 100bn years | 2tn years | 93tn years |
| 18 | 9 months | 23m years | 6tn years | 100tn years | 7qd years |

Fehlende Angriffs-zentrische Betrachtung

Operative Komplexität lähmt zunehmend

**Fähigkeiten bzgl. dem Vermeiden und Entgegenwirken von Attacken nicht ausreichend vorhanden**

Zu kleinteiliges und produkt-zentrisches Denken und Arbeiten

CANCOM

# ÖFFENTL. BEKANNTE CYBER ATTACKEN IN DEUTSCHLAND AUF EINEN BLICK

## Von Januar 2022 bis 6. April 2023 aus **Verwaltung**, **Bildung** und **Gesundheit** in Deutschland


Quelle:
https://konbriefing.com/en-topics/hacker-attacks-germany.html#/

- Unfallkasse Thüringen
- Ev. Schule St. Marien Neubrandenburg
- Medizin Campus Bodensee
- Pfarrei Heilig Kreuz Winnweiler
- FH Münster
- Kunstmuseum Stuttgart
- Museum Ulm
- Hochschule Anhalt
- BBS Goslar
- Stadtverwaltung Bochum
- Stadt Suhl in Thüringen
- BBS Cloppenburg
- Stadt Dingolfing
- TH Aschaffenburg
- Fraunhofer Institut Halle
- Donau-Stadtwerke Dillingen
- Stadt Schriesheim
- Uni-Bibliothek Leipzig
- Hochschule für Technik und Wirtschaft in Berlin
- Bundespolizei und Bundestag
- Stadt Murnau
- Stadt Bissingen
- Stadtreinigung Kassel
- Päd. Hochschule Freiburg
- FH Münster
- Komm DL. Hessen
- Stadt Burladingen
- Uni Wuppertal
- AMEOS Klinikum Neuburg
- Gymnasium Gunzenhausen
- IHK Verbände
- Stadt Stockach
- Stadt Egelsbach
- Gemeinde Dorn-Dürkheim
- Caritasverband
- Kath. Sozialdienstleister SKM
- Leibniz Institut Frankfurt/Main
- Landtag NRW
- Verwaltung Rhein-Pfalz Kreis
- Hochschule Ansbach
- Schulverwaltung München
- Enercity Stadtwerke Hannover
- Reha Klinik Bad Säckingen
- Hochschule Heilbronn
- Richard Wolf Medizingeräte GmbH
- Klinikum Lippe
- Die Zieglerschen
- TH Ulm
- Goetheschule Hannover
- Universität Duisburg – Essen
- Stadtverwaltung Drensteinfurt NRW
- Stadtwerke Wedel
- Stadt Karlstadt in Bayern
- Westsächische HS Zwickau
- Stadtverwaltung Potsdam
- HAW Hamburg
- FH Westküste
- HS Zwickau
- TU Freiberg
- Bitmarck
- HS Ruhr-West
- Polizei Baden-Württemberg
- Hochschule Harz
- Klinik Gerolzhofen und Schwabach
- Gemeinde Gerstetten
- FH Brühl
- Europäische FH Rhein/Erft
- 8 Schulen in Karlsruhe
- TU Illmenau
- Landratsamt Böblingen
- Heinrich-Heine Universität Düsseldorf
- Stadt Rodgau
- Stadt Raststatt
- Stadtverwaltung Bad Kreuznach
- Feuerwehr Hamburg
- Stadtwerke Karlsruhe
- Helmholtz Institut München
- ZBW Kiel – Leibniz Institut
- Polizei- und Landesverwaltungen vieler Bundesländer (DDoS)

CANCOM

# 7 FRAGEN – 7 ANTWORTEN

- Story Telling

# WIR VERSUCHEN  ANTWORTEN AUF DIE FOLGENDEN FRAGEN ZU GEBEN

- Was gilt es **JETZT** anhand der aktuellen Vorfällen und der aktuellen Bedrohungslage zu bewerten?
- Was sind überhaupt die größten Cyber-Risiken und was sollte ich dazu wissen?
- Wie kann ich **MEIN** Risiko und MEINE Eintrittswahrscheinlichkeit dementsprechend besser bewerten?
- Wo haben WIR dringenden Handlungsbedarf anhand großer Defizite bei elementaren Sicherheitsmaßnahmen?
- Wie sehen mögliche Gegemaßnahmen und Lösungsansätze aus?

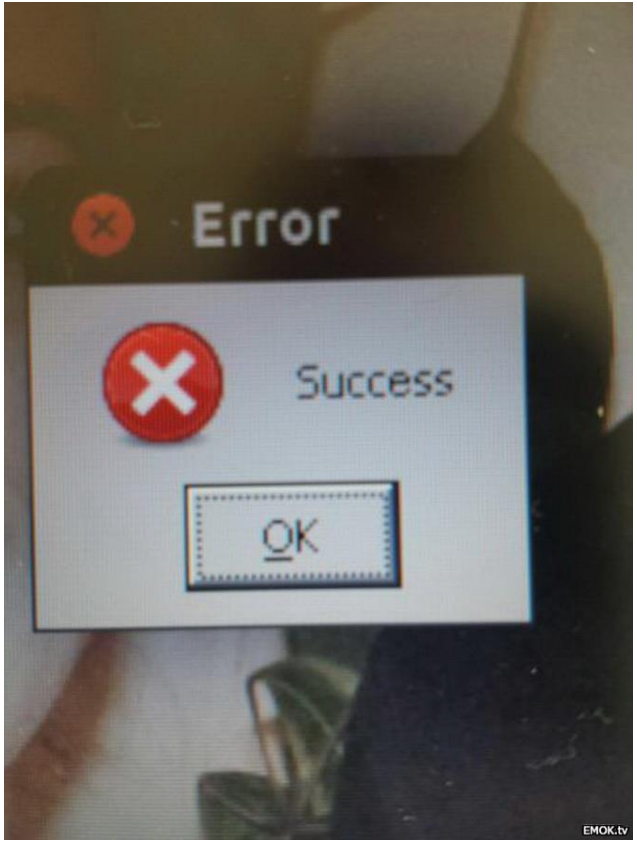
CANCOM

# UNSERE DATEN

„Unsere Daten sind sehr sicher, wir kommen ja selbst nicht mal richtig dran.“

„Kuratierte Daten!!“

„Bedrohungsszenario aufbauen.. Bla bla bla… alles ist schlimm, dann ist DAS die Lösung und ich mach ich Dir gute Preise.“



# HOW TO FIX IT




CANCOM

# 7 FRAGEN – 7 ANTWORTEN

**Details – Warum, Was... Darum**

# WICHTIGE FRAGEN...

... die es **jetzt** zu bewerten und bei Bedarf schnellstmöglich umzusetzen gilt

**Admin Accounts geschützt?**

Sind meine privilegierten Admin-Accounts vor unberechtigtem Zugriff geschützt durch eine starke Authentifizierung und Autorisierung?

**Ist unser Backup geschützt und leistet schnelle Wiederherstellung?**

Ist unser Backup selbst ausreichend geschützt, aktualisiert und ist eine schnelle Wiederherstellung ohne Datenverlust gewährleistet?

**Haben wir ein Notfallkonzept?**

Gibt es ein Notfallkonzept und ist für den Eintritt eines Vorfalls die Verfügbarkeit von Incident & Response Spezialisten gegeben?

**Erkennen wir Anomalien?**

Haben wir im eigenen Netzwerk eine Anomalie-Erkennung anhand der Netflow Daten etabliert?


**Remote Zugriffe geschützt?**

Sind alle VPN Zugänge in das eigene Netzwerk durch eine starke Authentifizierung und Autorisierung geschützt?

**Kennen wir unsere Schwachstellen?**

Haben wir eine Übersicht über aktuelle Schwachstellen in unserer IT-Landschaft und die Höhe der Eintrittswahrscheinlichkeit?

**Schutzschirm nach außen?**

Haben wir einen Schutzschirm zum Internet etabliert, um Anomalien und Angriffsversuche frühzeitig zu erkennen und zu blocken?



CANCOM

# FRAGE #1

... die es **jetzt** zu bewerten und bei Bedarf schnellstmöglich umzusetzen gilt

Hersteller

## Warum ist dies wichtig?

- Primäres Ziel beim Eindringen in ein System ist das Erlangen von Admin Rechten für kritische Systeme.
- User & Password ist kein ausreichender Schutz.


## Was kann ich tun?

- Multi-Faktor Authentifizierung und Autorisierung, insbesondere von privilegierten Accounts zur absoluten Pflicht machen.
- Kontinuierliche Überprüfung des Kontextes von Zugriffen.

**PSO Dienstleistungspakete**

Produkt/ Lösung

CANCOM

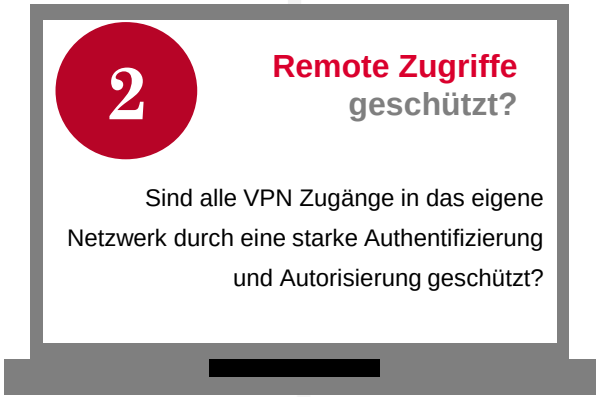
# FRAGE #2

... die es **jetzt** zu bewerten und bei Bedarf schnellstmöglich umzusetzen gilt

Hersteller

## Warum ist dies wichtig?

- Nutzung von VPN Zugängen sind ein Hauptangriffsvektor, wenn Angreifer sich Zugang zu persönlichen Anmeldedaten verschafft haben.
- Ist ein Angreifer so erst einmal ins Netz eingedrungen, kann er sich frei bewegen, da er erst einmal nicht als Angreifer war genommen wird.




## Was kann ich tun?

- Multi-Faktor Authentifizierung und Autorisierung, aller VPN Zugänge
- Idealerweise inkl. Überprüfung des Kontext eines Zugriffs.
- Einrichtung sollte einfach, schnell und für ein große Anzahl an Systemen möglich sein.
- Nutzer sollte im besten Fall wählen können was der zweite Faktor ist. (Nutzerzufriedenheit essentiell)

**PSO Dienstleistungspakete**

Produkt/ Lösung

CANCOM

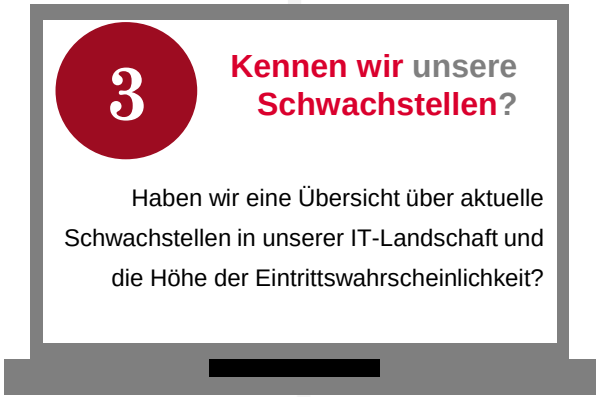
# FRAGE #3

... die es **jetzt** zu bewerten und bei Bedarf schnellstmöglich umzusetzen gilt

Hersteller CANCOM

## Warum ist dies wichtig?

- Neben dem Faktor Mensch, stellen auch technische Schwachstellen eine erhebliche Gefahr da.
- Allerdings sind nicht alle Schwach-stellen kritisch, hier gilt es also fokussiert und schnell vorzugehen.




## Was kann ich tun?

- Interne und externe Schwachstellen kontinuierlichen scannen, bewerten und erkannte, kritische Schwachstellen schnellstmöglich schließen.
- Penetration Test zur Überprüfung der eigenen Angreifbarkeit
- Kontinuierliche Überprüfung externer Quellen, z.B. Darknet.

**CANCOM #RedTeam Dienstleistungen**

Produkt/ Lösung

CANCOM

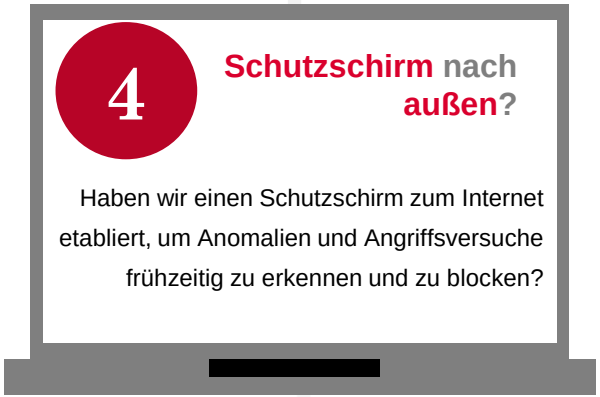
# FRAGE #4

... die es **jetzt** zu bewerten und bei Bedarf schnellstmöglich umzusetzen gilt

Hersteller CANCOM Cisco Umbrella

## Warum ist dies wichtig?

- Eine Firewall ist ein guter aber kein ausreichender Schutz vom und ins Internet.
- Stiehlt ein Angreifer z.B. häppchen-weise Informationen eines AD, kann der DNS Schutzschirm dies erkennen und verhindert den Transfer der Daten.




## Was kann ich tun?

- Konsequenter Einsatz eines DNS-Security Resolvers.
- Umstieg auf externen DNS-Schutzschirm binnen weniger Minuten möglich. Kein Eingriff in die System notwendig.
- Auch Geräte außerhalb des lokalen Netzwerks können geschützt werden.

**CANCOM**
**Internet Security aaS**

Produkt/ Lösung

CANCOM

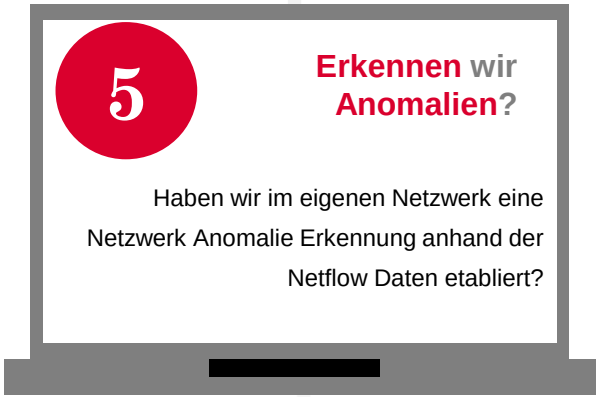
# FRAGE #5

... die es **jetzt** zu bewerten und bei Bedarf schnellstmöglich umzusetzen gilt

Hersteller CANCOM

## Warum ist dies wichtig?

- Angreifer bewegen sich oft Wochen und Monate als “legitime User” im System und spähen weitere Informationen aus.
- Je schneller Netzwerk Anomalien z.B. Lateral Movement erkannt werden um so Schneller können Maßnahmen eingeleitet werden.
- Im Nachgang lassen sich nützliche Infos zu einem Angriff rekonstruieren.




## Was kann ich tun?

- Kontinuierliche Auswertung von Netflowdaten von Switchen und Routern inkl. Ergänzung durch Datenquellen wie Webproxy.
- Eine Startup Phase (nur Monitoring) schafft mehr Visibilität mit direktem Schutz vor bekannten Gefahren.

**CANCOM SOC aaS/**
**Cisco Sec. Network Analytics** Produkt/ Lösung

CANCOM

# FRAGE #6

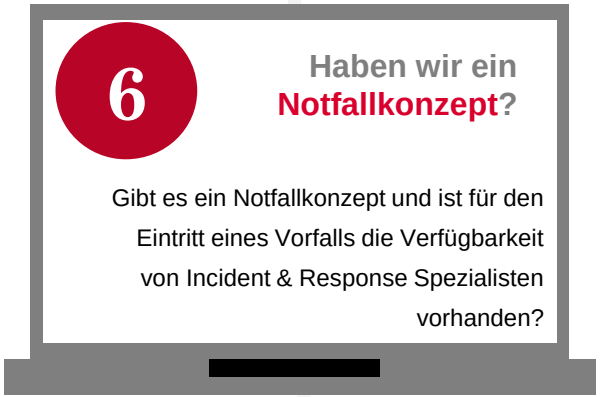
... die es **jetzt** zu bewerten und bei Bedarf schnellstmöglich umzusetzen gilt

Hersteller

CANCOM TALOS INCIDENT RESPONSE

## Warum ist dies wichtig?

- Die Frage ist nicht ob, sondern wann man Angegriffen wird. Einen 100% Schutz gibt es nicht.
- Kam es erstmal zu einem Vorfall ist Zeit der entscheidende Faktor um Schäden so gering wie möglich zu halten.
- Die Zahl von Cyber Angriffen steigt stetig und IR Spezialisten sind rar.




## Was kann ich tun?

- BSI-verifizierten IR Service einkaufen
- IR Service sollte Teil eines größeren Notfallplans sein
- Ein guter IR Service sollte folgende Merkmale aufweisen
  - hohe Anzahl Spezialisten, mit 24x7x365 Verfügbarkeit
  - Globale Threat Intelligenz
  - Pro-aktive Unterstützungsleistung

**Rapid Response Team**

Produkt/ Lösung

CANCOM

# FRAGE #7

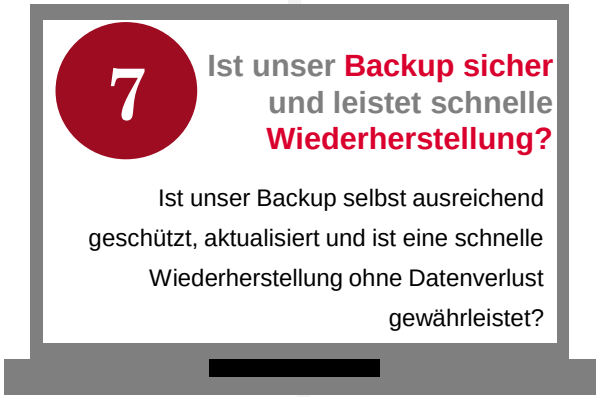
... die es **jetzt** zu bewerten und bei Bedarf schnellstmöglich umzusetzen gilt

Hersteller

CANCOM VEEAM

## Warum ist dies wichtig?

- Angreifer versuchen fast immer Admin Zugriff auf Backups zu bekommen, um dieses zu verschlüsseln.
- Werden auch existierenden Backups verschlüsselt, ist eine Wiederherstellung von Systemen unmöglich.




## Was kann ich tun?

- Backups sollten sich in einem durch eine Firewall geschützten Bereich des Netzwerks befinden das nur berechtigten Datenverkehr zulässt.
- Zugriffsrechte auf Backups grundsätzlich mit MFA sichern (F. #1)

**CANCOM Backup aaS**

Produkt/ Lösung

CANCOM

# 7 FRAGEN – 7 ANTWORTEN

## Summary

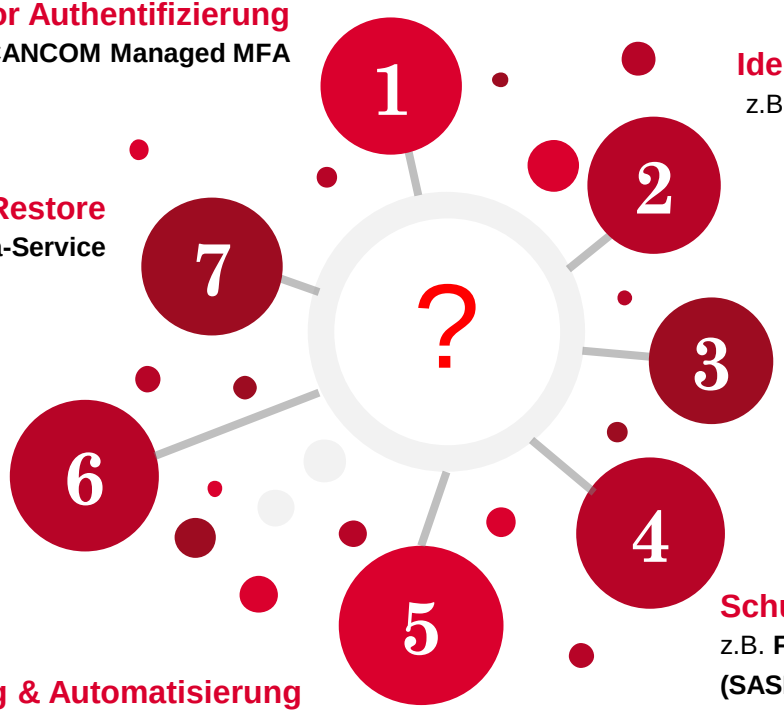
# KENNT IHR UNSERE ANTWORTEN?

## Summary

**Multi-Faktor Authentifizierung**
z.B. **CANCOM Managed MFA**

**Identity & Access Control**
z.B. **CANCOM Managed NAC**

**Backup & Restore**
z.B. **CANCOM Backup as-a-Service**




**PenTest & Analysen**
**CANCOM #RedTeam** Pakete & weitere standardisierte DL Pakete

**Vorbereitende Maßnahmen & Verträge**
z.B. **CANCOM Security Operation Center aaS** & Incident Response

**Schutzschirm nach außen?**
z.B. **Firewall aaS** und **Internet Security aaS (SASE)**

**Monitoring & Automatisierung**
SIEM & SOAR und EDR/MDR, z.B. **CANCOM Endpoint Protection aaS**, *sowie künftig* ***CANCOM Managed SOAR***



CANCOM

# SUMMARY

## CANCOM - Partner für den Security Lifecycle

- **Cyberbedrohungen** steigen stetig und betreffen **alle unsere Kunden**
- **Nicht jeder** Security **Lösung** hinterherlaufen
  - Fokussierung, Plattformen
- **Einstiegspunkte** mit klaren Angeboten
  - 7 Fragen und 7 Antworten!
- Es braucht einen **gesamtheitlichen Ansatz**
  - z.B. CANCOM Cyber Security Architektur

CANCOM

# FINAL STATEMENT




CANCOM

# CHATGPT SAGT "AUF WIEDERSEHEN"

Abschließend möchte ich betonen, dass Cybersicherheit im Schul- und Bildungsumfeld ein kontinuierlicher Prozess ist. Technologie und Bedrohungen entwickeln sich ständig weiter, und wir müssen unsere Strategien und Maßnahmen entsprechend anpassen. Nur durch eine umfassende Sicherheitskultur, die Zusammenarbeit zwischen Lehrern, Schülern, Eltern und Schulverwaltung, können wir eine sichere Lernumgebung schaffen, in der Schülerinnen und Schüler ihr volles Potenzial entfalten können.

Ich danke Ihnen für Ihre Aufmerksamkeit und hoffe, dass Sie aus dieser Rede einige wichtige Erkenntnisse mitnehmen konnten. Lassen Sie uns gemeinsam daran arbeiten, die Cybersicherheit im Schul- und Bildungsumfeld zu stärken und unsere Kinder und Jugendlichen vor den Gefahren des digitalen Zeitalters zu schützen. Vielen Dank!

CANCOM


# FRAGEN?! ☺