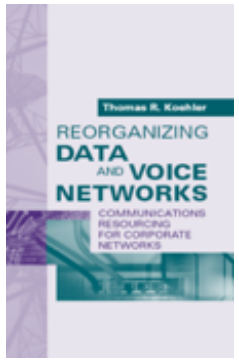

FUTURE CONNECTIONS
IT-SECURITY
& CYBER
CRIME
Summit
West

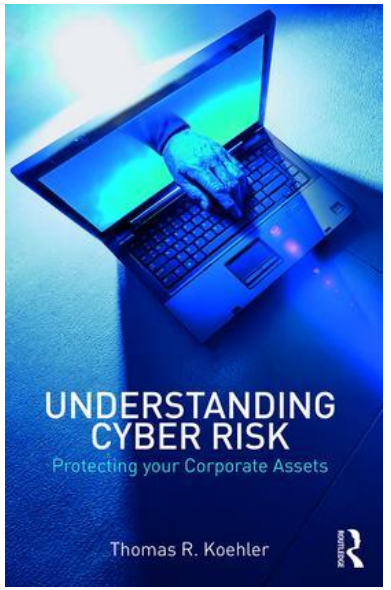
Ransomware:

Zahlen oder nicht zahlen?

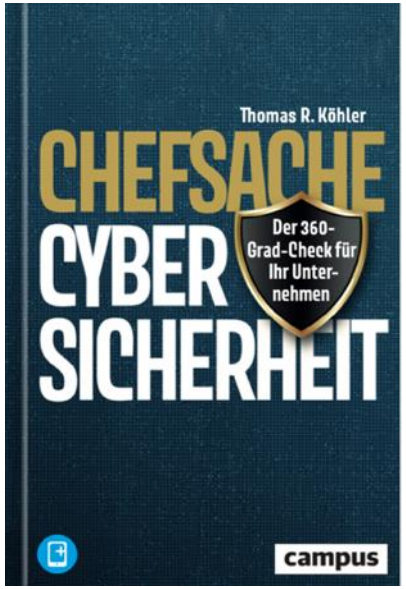
Thomas R. Köhler

Zur Person: Thomas R. Köhler – „Cybersicherheit ist Chefsache“



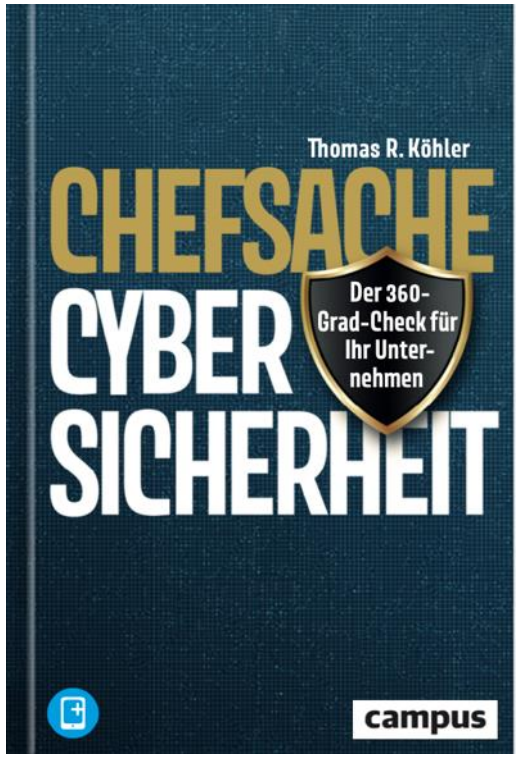


Aktuell



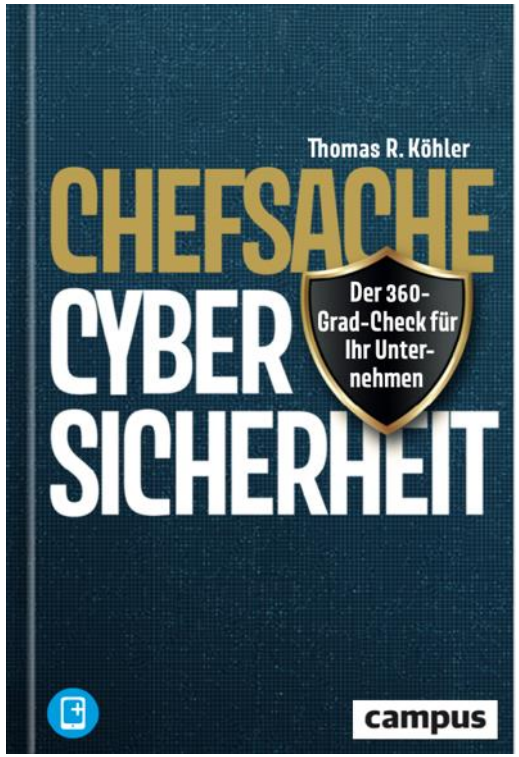
Agenda

- **Ransomware – Ein Lagebericht**
- **Empfehlungen der Behörden (AT/CH/D)**
- **Zahlen oder nicht zahlen?**
- **Lessons Learned**



Agenda

- **Ransomware – Ein Lagebericht**
- **Empfehlungen der Behörden (AT/CH/D)**
- **Zahlen oder nicht zahlen?**
- **Lessons Learned**



Problem Ransomware: WEMPE zahlt 1 Mio (!) Euro an Erpresser

Abonnieren Anmelden

Hamburger Abendblatt

Suche

Home Hamburg Nord Politik Wirtschaft Sport Aus aller Welt Kultur & Medien Wissen Ratgeber Reise Auto Abo Angebote Service

In den Nachrichten: Bürgermeister und Senat | Dieter Hecking | Sylt – das Insel-Special | Luftqualität in Hamburg | Alle Themen

Home – Hamburg – Blaulicht – Ransomware: Wempe zahlt Erpressern mehr als eine Million Euro Lösegeld

RANSOMWARE 02.07.19

Wempe zahlt Erpressern mehr als eine Million Euro Lösegeld

Ulrich Gaßdorf und Daniel Herder

Problem Ransomware: GRAFF zahlt 7,5 Millionen – wenige Jahre später

Bloomberg

Subscribe

Billionaire's Jeweler Pays $7.5 Million Crypto Ransom to Hackers

- Graff is suing Travelers over its refusal to cover the payout
- Ransomware gang threatened to leak high-profile clients' data

By Olivia Fletcher
6. Juli 2022, 11:08 MESZ

Listen to this article

▶ 2:13

Share this article

Follow the authors

@livfletcher

+ Get alerts for Olivia Fletcher

Luxury British jeweler Graff Diamonds Corp. paid $7.5 million ransom in Bitcoin to a Russian hacking gang after it leaked data on the jeweler's high-profile clients, according to a London lawsuit.

Graff, that counts Middle East royalty among its client base, sued its insurer for losses over the extortion saying that the payment should be covered under their policy. The Travelers Companies Inc. is refusing to pay the jeweler's loss caused by the Bitcoin ransom, Graff alleges.

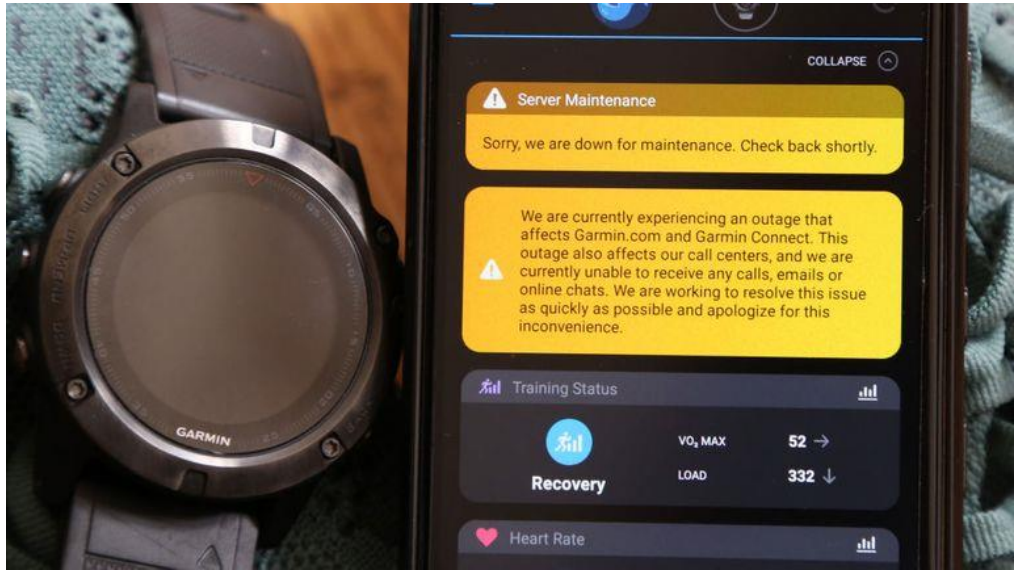
Hotels: Nordic Choice – 200 Hotels haben EIN Problem...

SECURITY & PRIVACY

Hackers demand ransom after stealing hotel guest records – Was your data compromised?

BY KOMANDO STAFF, KOMANDO.COM • AUGUST 15, 2019 SHARE:

Sommer 2020: GARMIN Ransomware – Kundenanwendungen „down“



Kranhersteller Palfinger „Fabrik steht“

Lebensmittelindustrie
Salzburg Milch

„No Milk today“

PROFIL-CRIME 05.02.2022

„You are fucked“: Wie Hacker SalzburgMilch lahmlegten

In der Nacht zum 23. Juni 2021 erhielt die größte Salzburger Molkerei eine unerfreuliche Nachricht. Hacker hatten ihre Computersysteme gekapert und verlangten Lösegeld.

von Sebastian Hofer

Telekommunikation

Vodafone Portugal

„Kein Anschluss unter dieser Nummer...“

Finnland: „Doppelte Erpressung“ mit Psychotherapie Patientendaten

NEWS FROM FINLAND
HELSINKI TIMES

HELSINKI
FINLAND

24°C
clear sky

Sun	Mon	Tue	Wed	Thu
24°C 17°C	23°C 15°C	25°C 17°C	25°C 19°C	26°C 18°C

FINLAND | BUSINESS | COLUMNS | WORLD | CULTURE | LIFESTYLE | EAT AND DRINK | THEMES | CHINA NEWS | 中文

Hacking may have compromised privacy of thousands of psychotherapy clients in Finland

FINLAND / 23 OCTOBER 2020

DOMESTIC

Psychotherapy Centre Vastaamo says a cybercriminal is trying to blackmail it into paying 450,000 euros after allegedly obtaining sensitive information on tens of thousands of its clients. (Markku Ulander – Lehtikuva)

GET OUR LATEST FREE NEWSLETTER

Daily

E-mail

SUBSCRIBE

WEEK'S MOST POPULAR ARTICLES

Supreme court rules to deport Somali man who was born and raised in Finland

Finland puts brakes on travel from high-risk countries

Researcher surprised by high number of births in Finland

ILTA-SANOMAT TUOREIMMAT LUETUIMMAT SÄÄ Kirjaudu Hae Valikko

ETUSIVU UUTISET VIIHDE URHEILU ME NAISET TALOUS AUTOT HYVÄ OLO DIGI RUOKALA ASUMINEN

DIGITODAY

Mobiili Esports Tietoturva Testit

TIETOTURVA

Vastaamon ex-toimitusjohtaja Ville Tapio kiistää tietäneensä vuoden 2018 tietomurrosta: ”Nähtävästi inhimilliset virheet ketjuuntuivat”

Ville Tapion mukaan hänellä on ollut kielto kommentoida asiaa julkisesti.

JAA

Psykoterapiakeskus Vastaamon toimitusjohtajan tehtävistä vapautettu Ville Tapio kiistää tietäneensä aiemmin Vastaamon ensimmäisestä tietomurrosta. KUVA: VESA MOILANEN / LEHTIKUVA, JUKKA GRÖNDAHL

Riika Nykänen
26.10.2020 21:01 | Päivitetty 26.10.2020 21:58

PSYKOTERAPIAKESKUS Vastaamon toimitusjohtajan tehtävistä vapautettu **Ville Tapio** kiistää tietäneensä aiemmin Vastaamon ensimmäisestä tietomurrosta. Tapion mukaan tietomurto, jonka ajankohdaksi epäillään marraskuuta 2018, paljastui hänelle vasta Nixun tutkimuksen pohjalta lokakuussa 2020.

Tapio kommentoi asiaa maanantai-iltana julkaisemassaan julkisessa Facebook-päivityksessä.

LUETUIMMAT

1. THL: Suomessa todettu 138 uutta koronatartuntaa – katso tilanne kunnittain
2. Jyrisevä tauko paahteeseen – näin sunnuntain ukonilmat etenevät
3. Julkkiskokki Hanna Gullichsen kertoo Instagramissa pelottavasta tilanteesta: "Testien jälkeen hän sanoi mun elämäni kauheimmat sanat"
4. Suomalaiset listaavat kauneimmat sukunimet: "Harmi, ettei meistä tullut mitään, nimi olisi ollut täydellinen"
5. Anni, 101, ja Evert, 100, menivät naimisiin 80 vuotta sitten ja vieläkin elämä on ihanaa – paljastavat pitkän liittonsa salaisuuden
6. Aiotko vaihtaa lakanat? Kokeile somehitiksi noussutta nopeaa pussilakananiksiä – "Tämä on jotain taikuutta"
7. Laila Hirvisaari siunattiin hiljaisuudessa – koskettava kuolinilmoitus julkaistiin Helsingin Sanomissa
8. Paahtava helle jatkuu – katso, missä on kuuminta juuri nyt
9. Video ja kuvat paljastavat: näin karmivaan kuntoon Conor McGregorin murtunut nilkka meni

„Der Tod kommt per Mausklick...“

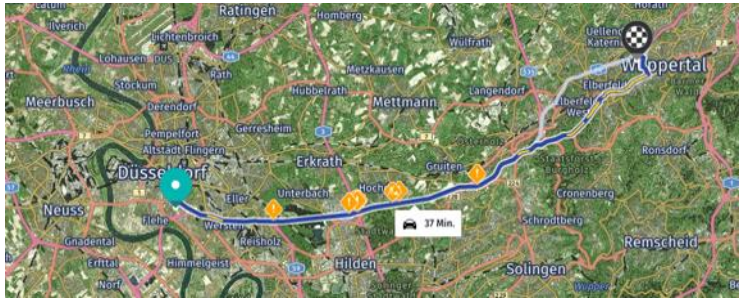
Stand der Ermittlungen

Tödlicher Cyberangriff auf Düsseldorfer Uniklinik

17. September 2020 um 19:34 Uhr | Lesedauer: 2 Minuten

Die Uniklinik in Düsseldorf ist die siebtgrößte Klinik in NRW. Foto: dpa/Roland Weihrauch

Düsseldorf. Weil das IT-System lahmlag, musste ein Notfall in ein anderes Krankenhaus gebracht werden. Die Frau starb. Ermittler rätseln: Wollten Kriminelle die Düsseldorfer Universität treffen?



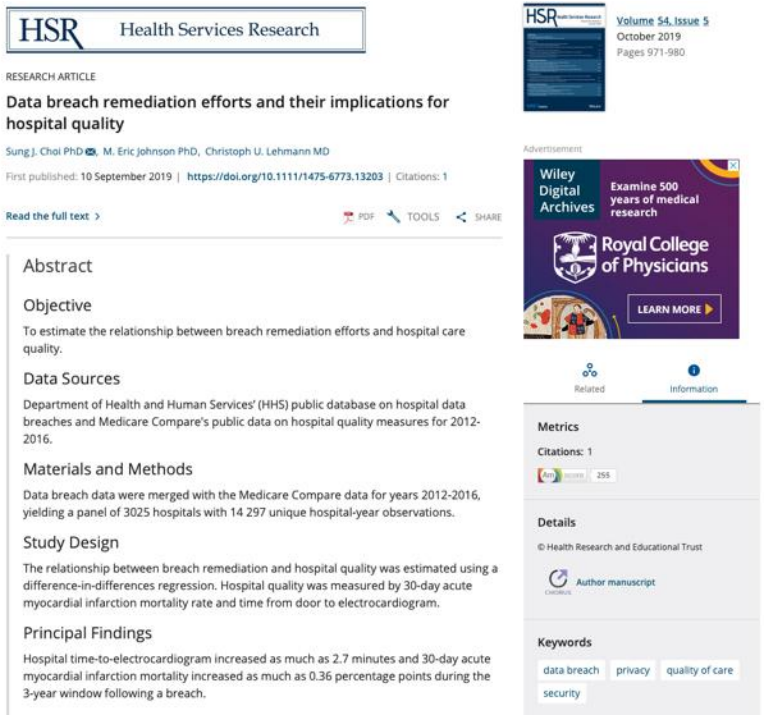
Der erste Todesfall

~~durch~~ nach Cyberangriff?

Cyber-Angriff auf Uniklinik Düsseldorf: BSI warnte vor Schwachstelle

Von Tobias al-Shomer und Britta Kuck

Das Bundesamt für Sicherheit in der Informationstechnik warnte im Januar vor Schwachstellen. Der Angriff auf die Uniklinik Düsseldorf war nicht der erste auf ein NRW-Krankenhaus.



HSR Health Services Research

RESEARCH ARTICLE

Data breach remediation efforts and their implications for hospital quality

Sung J. Choi PhD, M. Eric Johnson PhD, Christoph U. Lehmann MD

First published: 10 September 2019 | https://doi.org/10.1111/1475-6773.13203 | Citations: 1

Read the full text › PDF TOOLS SHARE

Abstract

Objective

To estimate the relationship between breach remediation efforts and hospital care quality.

Data Sources

Department of Health and Human Services' (HHS) public database on hospital data breaches and Medicare Compare's public data on hospital quality measures for 2012-2016.

Materials and Methods

Data breach data were merged with the Medicare Compare data for years 2012-2016, yielding a panel of 3025 hospitals with 14 297 unique hospital-year observations.

Study Design

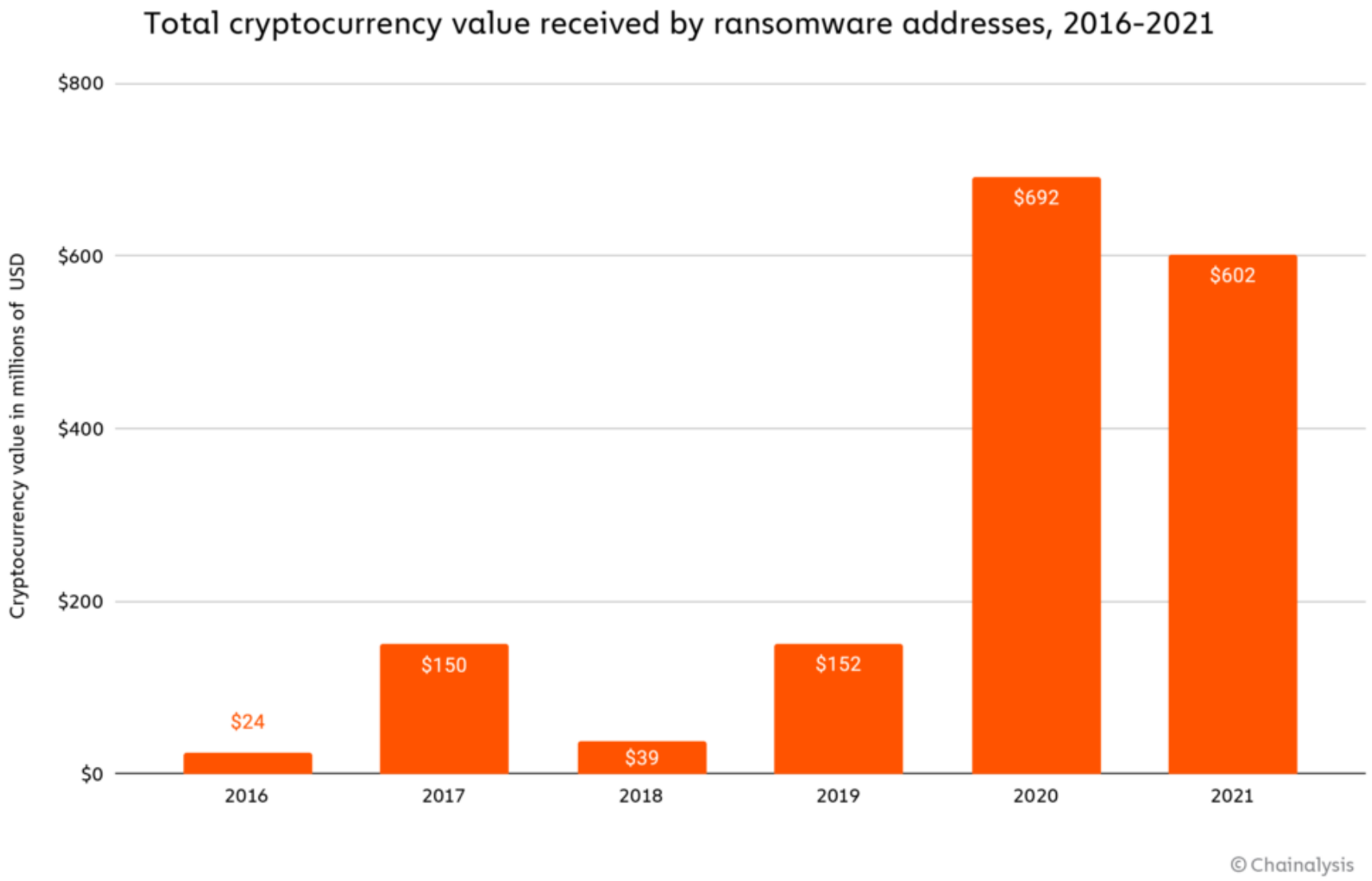
The relationship between breach remediation and hospital quality was estimated using a difference-in-differences regression. Hospital quality was measured by 30-day acute myocardial infarction mortality rate and time from door to electrocardiogram.

Principal Findings

Hospital time-to-electrocardiogram increased as much as 2.7 minutes and 30-day acute myocardial infarction mortality increased as much as 0.36 percentage points during the 3-year window following a breach.

Ransomware

Auch die „Finanzer“ sind aufgewacht bei den Zahlen



Zahlen oder Nicht Zahlen? gefährliche Tendenzen

Ransomware-Fälle die international Schlagzeilen machten:

▪ 2017	Ransom gef./bez.	Wiederherstellungskosten
Maersk	unbekannt	€300Mio
▪ 2018	Ransom gef./bez.	Wiederherstellungskosten
Atlanta	$50.000	$17Mio
▪ 2019	Ransom gef./bez.	Wiederherstellungskosten
Wempe	€1Mio (est.)	$???
▪ 2020	Ransom gef./bez.	Wiederherstellungskosten
Garmin	$9Mio (est.)	$???
▪ 2021	Ransom gef./bez.	Wiederherstellungskosten
PALFINGER	€???	€???
▪ 2021	Ransom gef./bez.	Wiederherstellungskosten
Mediamarkt	€50 Mio ?	€???

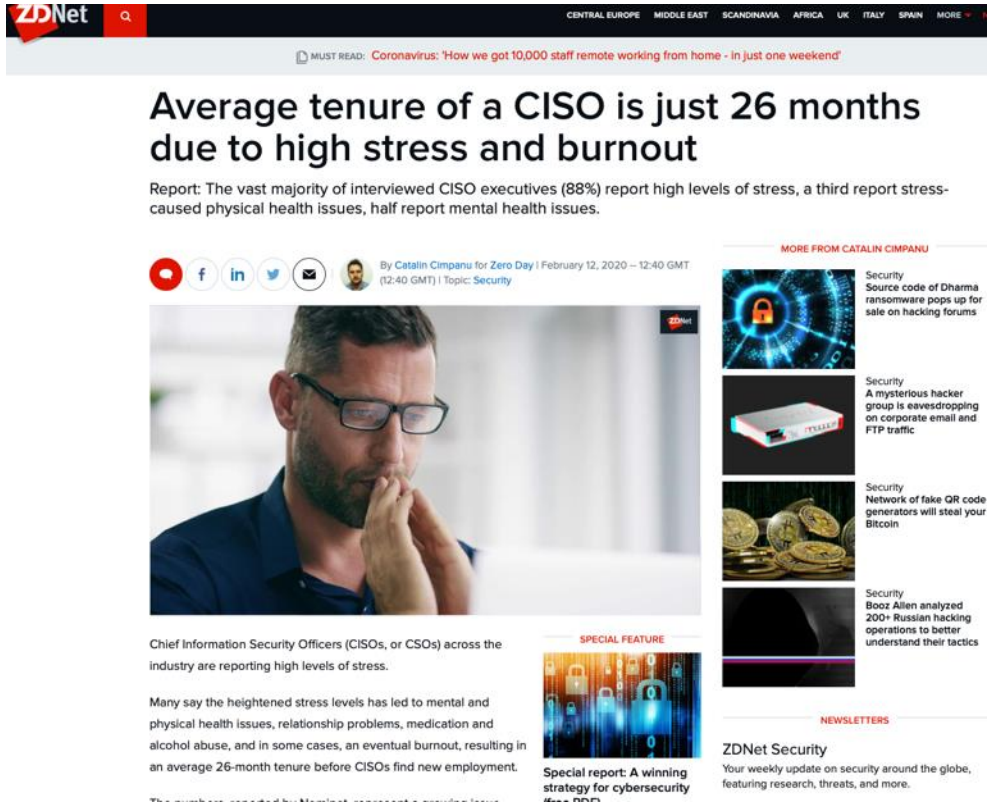
"... The fact is, paying a ransom does not create a market. There already is a market." (Josh Zelonis, Forrester Research)

CISOs unter Druck...

26 Monate durchschnittliche Betriebszugehörigkeit (UK/US-Daten*)

- Ergebnisse der Nominet-Umfrage 2019*:
- 88 % der CISOs gaben an, "mäßig oder enorm gestresst" zu sein
- 48 % der CISOs gaben an, dass sich Arbeitsstress negativ auf ihre psychische Gesundheit ausgewirkt hat
- 40 % der CISOs gaben an, dass ihr Stresslevel die Beziehung zu ihrem Partner oder ihren Kindern beeinträchtigt hat
- 32% gaben an, dass ihr beruflicher Stress Auswirkungen auf ihre Ehe oder romantische Beziehung hatte
- 32% gaben an, dass ihr Stresslevel ihre persönlichen Freundschaften beeinträchtigt hat
- 23 % der CISOs gaben an, dass sie zu Medikamenten oder Alkohol greifen

(*n=800 CISOs UK/US)



Exkurs: Was zahlen Unternehmen für Top-Experten?

- Wenig Expertise am Markt treibt die Preise – in D/A/CH bisher noch nicht so sehr wie in UK/US
- Besetzungsprobleme sind ein wesentlicher Treiber für Outsourcing
- „Missmatch“ in AT/CH/DE zwischen Nachfrage und Preisangebot

Sections

Los Angeles Times

BUSINESS

Cybersecurity pros name their price as data hacking attacks swell

Former Equifax Chief Executive Richard Smith appears before the Senate Banking, Housing and Urban Affairs Committee in 2017. Smith stepped down after hackers broke into the credit reporting agency. (Mark Wilson / Getty Images)

By ANDERS MELIN | BLOOMBERG AUG. 7, 2019 | 11:26 AM

It took a $650,000 salary for Matt Comyns to entice a seasoned cybersecurity expert to join one of America's largest companies as chief information security officer in 2012. At the time, it was among the most lucrative offers out there.

This year, the company had to pay $2.5 million to fill the same role.

"It's a full-on war for cybertalent," said Comyns, a managing partner at executive search firm Caldwell Partners who specializes in information security. "CEOs know that, so they play hardball. Everyone's throwing money at this."

FREE FOR ALL READERS

Live updates on the coronavirus pandemic

5 things you can do to help L.A. restaurants

Was your job affected by coronavirus? Here's how to file for unemployment

Where entertainment industry workers can go for help during the coronavirus crisis

Cases statewide »

5,683 confirmed

121 deaths

Updated March 28, 10:36 p.m. Pacific

ADVERTISEMENT

LATEST BUSINESS

TECHNOLOGY

Delivery workers are keeping California fed. They say no one's keeping them safe

March 28, 2020

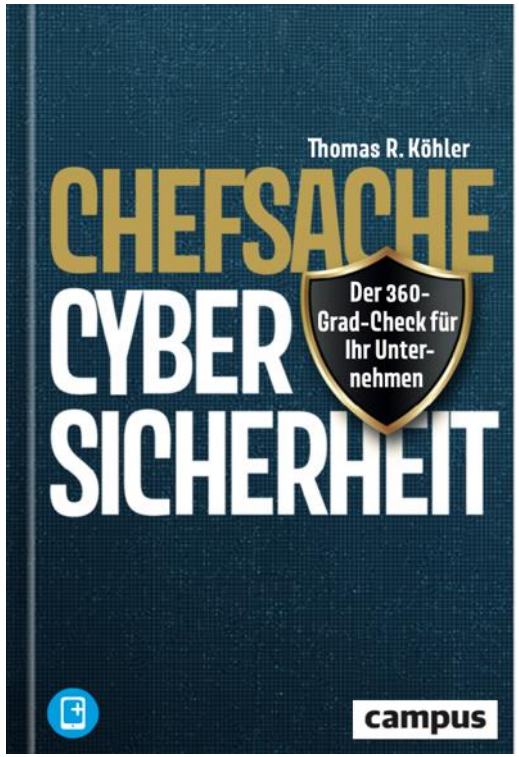
CALIFORNIA

L.A. expands sick leave amid coronavirus — but only for employees at big companies

March 27, 2020

Agenda

- Ransomware – Ein Lagebericht
- Empfehlungen der Behörden (AT/CH/D)
- Zahlen oder nicht zahlen?
- Lessons Learned



Empfehlungen der Behörden (AT)

Empfehlungen zu Ransomware

Soll man auf die Geldforderung eingehen?

Hier gibt es moralische, rechtliche und wirtschaftliche Aspekte. Wir raten, keine voreiligen Entscheidungen zu treffen, sondern nüchtern abzuwägen[13].

Eine Garantie, dass man nach der Bezahlung auch wirklich Zugriff auf seine Daten wiedererlangt, gibt es nicht. Andererseits wissen die Angreifer genau, dass ihr Geschäftsmodell davon abhängt, dass bekannt ist, dass die Entschlüsselung funktioniert[14]. Die Erfolgswahrscheinlichkeit des Zahlens ist daher nicht schlecht.

Empfehlungen der Behörden (CH)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

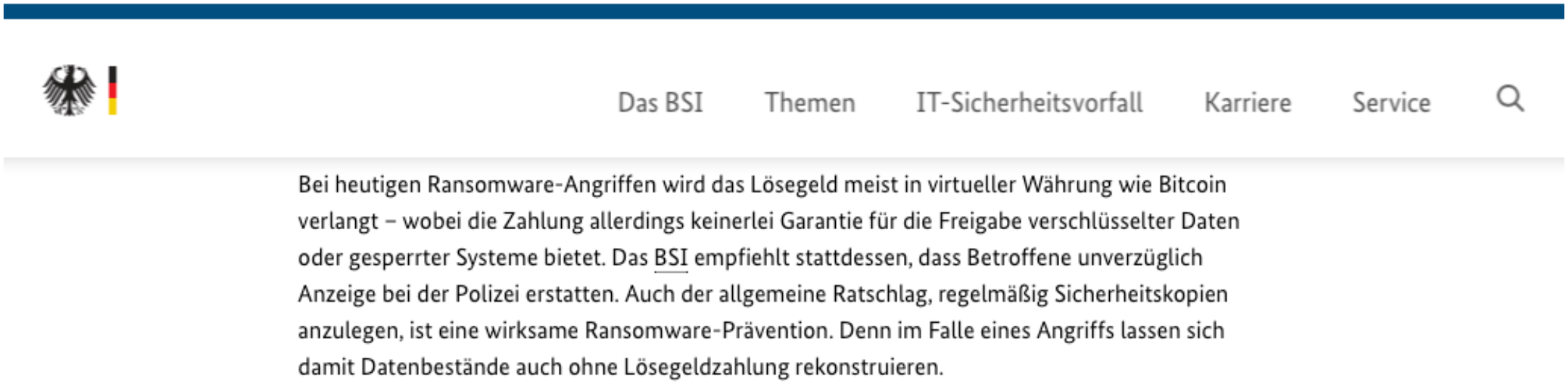
Nationales Zentrum für Cybersicherheit NCSC

Hinweise zur Zahlung von Lösegeldern

NCSC rät von der Zahlung eines Lösegeldes ab. Es gibt keine Garantie, dass die Verbrecher nach der Bezahlung des Lösegelds die Daten nicht doch veröffentlichen oder anderen Profit daraus machen. Zudem motiviert jede erfolgreiche Erpressung die Angreifer zum Weitermachen, finanziert die Weiterentwicklung der Angriffe und fördert deren Verbreitung.

Sollten Sie dennoch das Bezahlen von Lösegeld in Erwägung ziehen, empfiehlt NCSC dringend, diese Schritte mit der Kantonspolizei zu diskutieren.

Empfehlungen der Behörden (DE)



Empfehlungen der Behörden (International)

keine einheitliche Linie!

How to Respond and Report

The FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity.

If you are a victim of ransomware:

- Contact your local FBI field office to request assistance, or submit a tip online.
- File a report with the FBI's Internet Crime Complaint Center (IC3).

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments[1]

Date: October 1, 2020

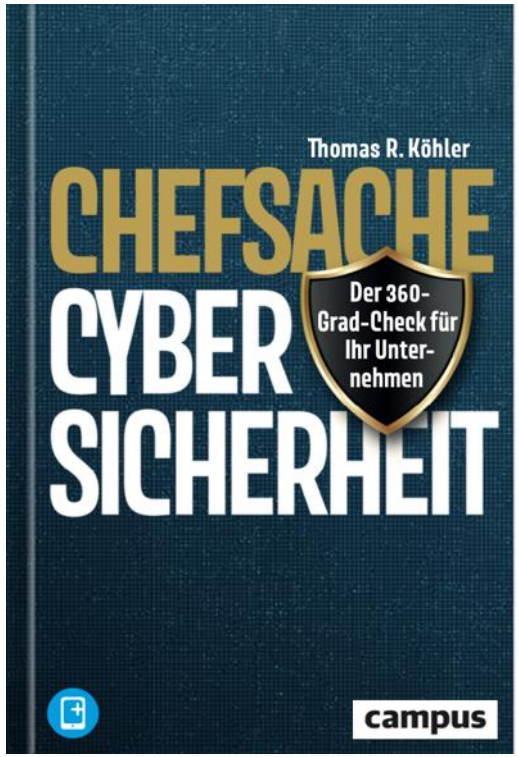
Das Problem liegt in der Funktionsweise von Ransomware...

Einfallstore für Ransomware	Initiale Aktionen	Auswirkungen auf das betroffene Unternehmen
Phising	Command&Control	Verschlüsselung von Daten
(Password Guessing)	Laterale Bewegung im Netz	Zerstörung von Backups
E-Mail mit Payload / Drive By-Download	Privilege Eskalation	Exfiltrierung von Daten
Ausnutzung von Systemschwächen ohne Nutzereingriff		

Zeitdauer: Tage bis Monate (!)

Agenda

- Ransomware – Ein Lagebericht
- Empfehlungen der Behörden (AT/CH/D)
- Zahlen oder nicht zahlen?
- Lessons Learned



Was Analysten raten…

Was in den Medien steht…

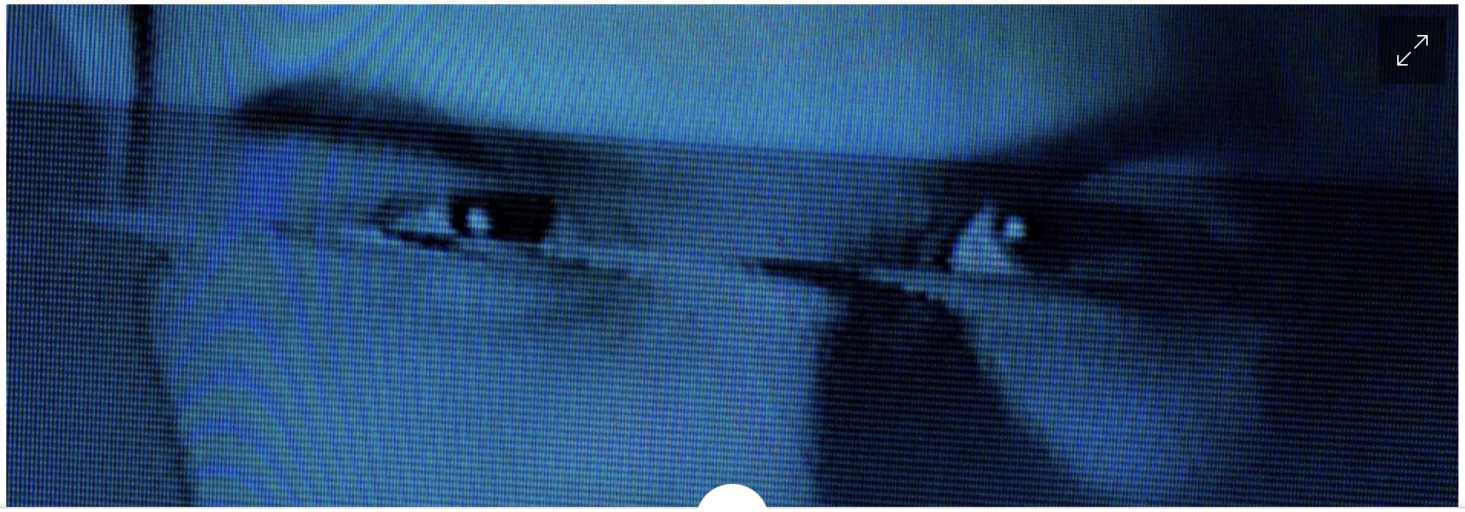
Harvard Business manager

Cybersecurity

Lösegeld zahlen lohnt nicht

Sparen Sie sich das Geld: 82 Prozent der erpressten Unternehmen in Deutschland wurden anschließend noch ein zweites Mal Opfer eines Ransomware-Angriffs.

10.08.2022, 16.57 Uhr • aus **Harvard Business manager 8/2022**



Zahlen oder nicht zahlen? Argumente FÜR Ransom-Zahlung

ZAHLEN

- Zahlung ist (meist, nicht immer) die schnellste Lösung
- Wenn Zahlung die günstigste / die einzige Option ist...
- Wenn im besonderen Interesse von Betroffenen (Krankenhauspatienten / Kritische Infrastruktur etc)
- Durch die Zahlung kann eine Geldstrafe für den Verlust wichtiger Daten vermieden werden;
- Die Veröffentlichung gestohlener Daten stellt für sich betrachtet ein erhebliches Risiko dar.
- Eine Zahlung bedeutet, dass keine streng vertraulichen Informationen verloren gehen;
- Eine Zahlung kann bedeuten, dass die Datenpanne nicht öffentlich gemacht wird;
- Eine Zahlung kann von einer Versicherung gedeckt sein.
- Information der Betroffenen kann (nach Ansicht verschiedener Juristen) vermieden werden.
- Wenn damit „alles unter den Teppich gekehrt werden“ kann

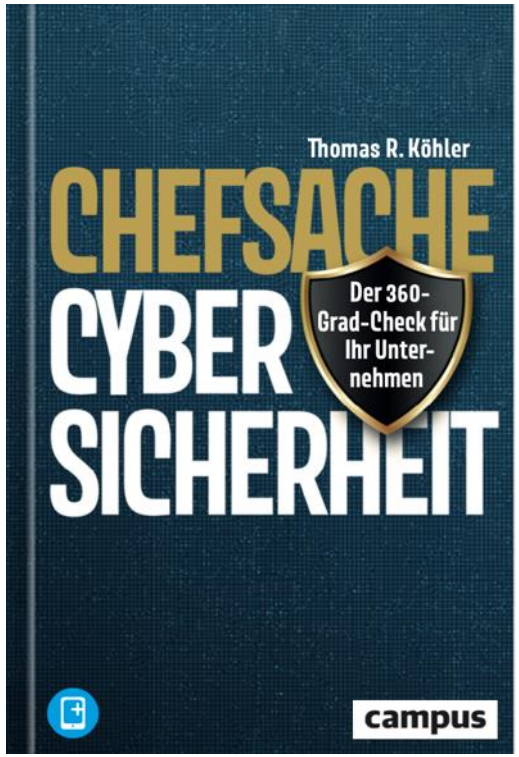
Zahlen oder nicht zahlen? Argumente GEGEN Ransom-Zahlung

NICHT ZAHLEN

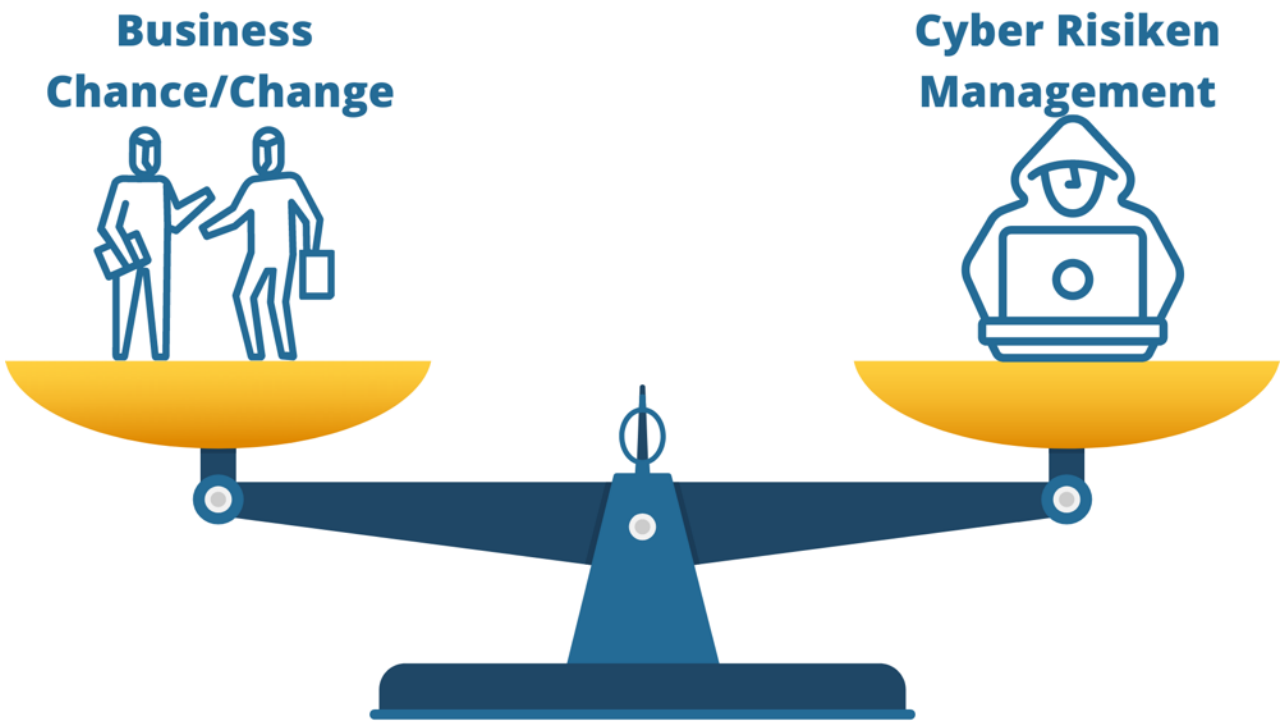
- Funktionsfähiges (und nicht kompromittiertes Backup) vorhanden
- Die Zahlung garantiert nicht, dass der Schlüssel kommt / die Entschlüsselung klappt
- Durch die Zahlung werden weitere kriminelle Aktivitäten finanziert (!)
- Die Zahlung kann der Reputation des Unternehmens schaden;
- Die Zahlung ist eine Einladung an die Angreifer es erneut zu versuchen.
- Die Verwendung von Cryptowährungen zur Zahlung kann Unternehmen in zusätzliche Gefahr bringen.
- Die Zahlung kann rechtliche Konsequenzen haben (falls Unternehmen USA-Bezug hat)
- Eine Zahlung kann ein Vertragsverstoß (Compliance-Regeln? NDAs?) sein.
- Eine Zahlung liefert im Regelfall keine detaillierten Informationen über den Angriff selbst (!)
- Sowas wie Ganovenehre gibt es übrigens nicht ;-)

Agenda

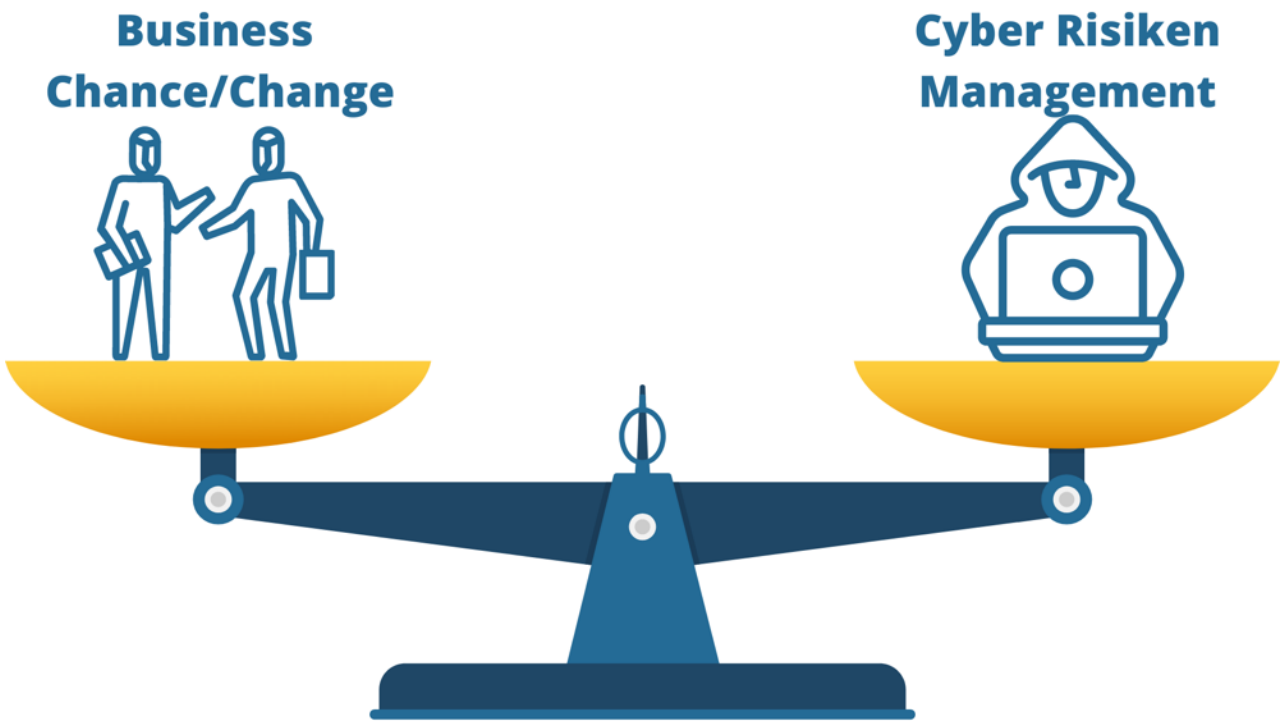
- Ransomware – Ein Lagebericht
- Empfehlungen der Behörden (AT/CH/D)
- Zahlen oder nicht zahlen?
- Lessons Learned



Es kommt auf die “richtige Balance“ an...



Die richtige Balance finden? - Option: „Neuerfindung“ der IT-Infrastruktur



TECH TiMES

Nordic Choice Hotels Changes Windows to Chrome OS After Ransomware Attack

Sophie Webster, Tech Times | 08 January 2022, 01:01 pm

[CE21] Communication Experts

Meine Empfehlungen für Ihr Unternehmen / Ihre Organisation:

(Abb: „The School of Athens“ (Ausschnitt) Fresco, Palazzi Pontifici, Vatican, gemeinfreie Abb.)

Grundlegende Maßnahmen für “mehr“ Cybersicherheit

- Unabhängige Auditierung der eigenen ICT-Infrastruktur
- Laufende automatisierte Überwachung der Infrastruktur
- Notfallplanung (inkl. Einsatzteam / Kommunikationswege etc.)
- Konsequente Policy für Dateizugriffsrechte
- Laufende Schulung / Awareness-Maßnahmen bei Belegschaft
- Selektion von Partnern / Lieferanten / Mitarbeiterinnen und Mitarbeitern
- Etablierung einer dedizierten Verantwortlichkeit (mit eigenem Budget!)
- Identifikation und Schutz der „Kronjuwelen“
- Social Media Policy

Ransomware:

Zahlen oder nicht zahlen?

➡ Q&A

Thomas R. Köhler

Verwendungshinweis:

Dieses Handout ist nur für unmittelbare Teilnehmerinnen und Teilnehmer der Veranstaltung bestimmt und ohne die verbalen Erläuterungen unvollständig. Eine Weitergabe an Dritte ist nicht statthaft.

Kontaktinfo Thomas R. Köhler:

Linktree (alle Links zur Person an einem Ort):
https://linktr.ee/profkoehler

LinkedIn:

https://www.linkedin.com/in/thomasrkoehler/

Meine Firma:
https://www.ce21.de / Thomas.Koehler@ce21.de / +49 175 2914434