secuvera:
Cybersicherheit. Nachhaltig.

Go hack yourself

einfache Wege, die größten Einfallstore selbst zu prüfen

COMMERZBANK

Tobias Glemser

Geschäftsbereiche

secuvera:
Cybersicherheit. Nachhaltig.

BSI-Prüfstelle

CRA-Beratung & Prüfung
Common Criteria, BSZ
TR-Prüfungen, Industrial
Security (IEC 62443)

Penetrationstests

u. a. Webanwendungen,
Ransomware-Simulation,
Red-Teaming, AD-Analysen

Sicherheitsberatung

NIS2-Beratung, BSI-
GS/ISO27001/TISAX

CISO as a Service (CaaS)

Schulung und Herstellerberatung

OWASP® Top 10, SSDL,
27001, Cyber für KMU

Zertifizierungen und CRA

secuvera:
Cybersicherheit. Nachhaltig.

- 50 Mitarbeitende
- IT-Sicherheit seit 1988

- BSI-Grundschutz Auditoren, -Berater & -Praktiker
- ISO 27001 Lead Auditoren
- BCM Praktiker
- BSI-zertifizierte Pentester
- Common Criteria Evaluatoren
- Cyber Security Practitioner
- KRITIS-Prüfer
- TR-Prüfer
- ..

whoami

secuvera:
Cybersicherheit. Nachhaltig.

- Tobias Glemser, Geschäftsführer und Gesellschafter
- 25 Jahre in der Branche
- BSI-zertifizierter Penetrationstester
- OWASP German Chapter Lead

Bilderrätsel

Ausgangslage

CHRONIK

Hackerangriff: Mil

Nach dem Cyberangriff auf Salzburg
Produktion am Standort in Salzburg
stehe noch bis mindestens Montag

Salatknappheit: Produktionsausfall in den USA bei Dole nach Ransomware-Attacke

e und Schnittblumen Dole wurde Opfer
e temporär

Traditionsfirma mit über 400 Angestellten in der Insolvenz – nach Cyberattacke

14.10.2024, 16:24 Uhr

Nach Cyb
Tischlere

als 70 Kommunen lahm

Auch gut einen Monat nach dem Cyberangriff auf die Industrie- und Handelskammern (IHK) in Deutschland gibt es dort noch Einschränkungen.

Die Folgen ei
IT-Netzwerk von Tegut. Für Kunden habe dies allerdings

IT des irischen

kenfm.de: Anonymous hackt Website des Aktivisten Ken Jebsen

Nacht von einer
– mit Folgen für das

Das Hackerkollektiv hat Zugriff auf kenfm.de erlangt und von dort nach eigenen Angaben 3 GByte Daten kopiert.

VERSICHERUNG

Asiatische Axa-Partner von Ransomware getroffen

Teile des Versicherungskonzerns Axa in Asien wurden von einem Ransomware-Angriff getroffen, es soll um 3 Terabyte Daten gehen.

Ausgangslage

Landratsamt für Kunden geschlossen

Kreis Ludwigsburg wohl Opfer eines Cyberangriffs

Stand: 11.5.2023, 17:24 Uhr

Von Samantha Ngako

Teilen:

Hacker haben offenbar den Kreis Ludwigsburg angegriffen. Das teilte ein Sprecher des Landratsamts dem SWR mit. Das Landratsamt sei deshalb für den Kundenverkehr geschlossen.

Ausgangslage

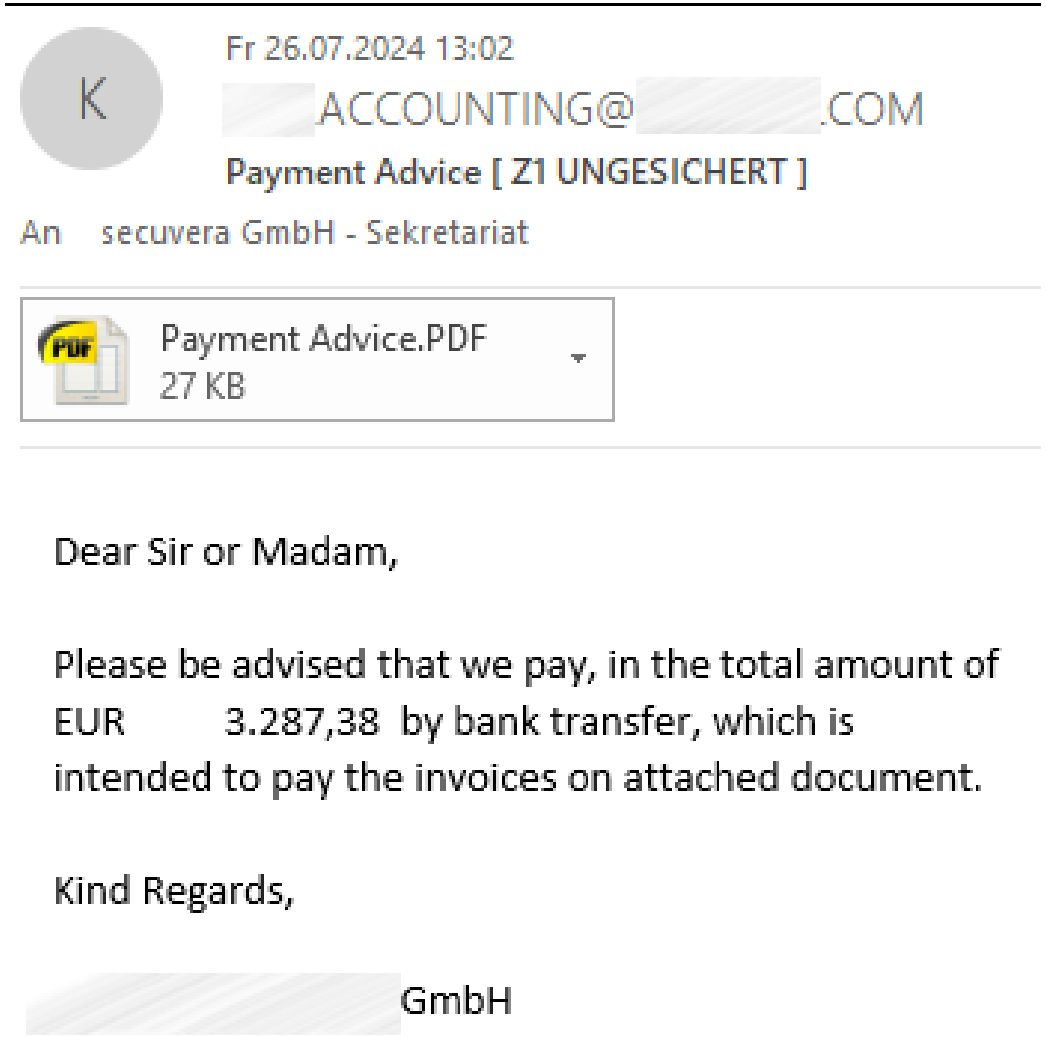
IT-Probleme bei Behörde

Kein Cyberangriff: Schadsoftware legte Landratsamt Ludwigsburg lahm

Das Landratsamt Ludwigsburg sei stattdessen zufällig Opfer einer Schadsoftware geworden, hieß es vom Innenministerium. Ein Mitarbeiter habe eine E-Mail mit infiziertem Anhang geöffnet. Daraufhin sei die IT-Infrastruktur im Landkreis Ludwigsburg heruntergefahren worden. Die betroffenen Computer wurden laut Innenministerium anschließend bereinigt, am IT-System wurde kein Schaden festgestellt.

Ausgangslage

Ausgangslage



K

Fr 26.07.2024 13:02

ACCOUNTING@ .COM

Payment Advice [Z1 UNGESICHERT]

An secuvera GmbH - Sekretariat

Payment Advice.PDF
27 KB

Dear Sir or Madam,

Please be advised that we pay, in the total amount of
EUR 3.287,38 by bank transfer, which is
intended to pay the invoices on attached document.

Kind Regards,

GmbH

Patient Zero

secuvera:
Cybersicherheit. Nachhaltig.

- Kein technischer Schutz vor unbekannter Software
- Schlechte / geleakte Passwörter, kein 2FA
- (Social Engineering)

Go hack yourself – Kritik/FAQ

secuvera:
Cybersicherheit. Nachhaltig.

- Nutzer:innen werden sensibilisiert, nicht auf alles zu klicken. Jetzt sollen sie bei uns klicken?
  - Ja, sollen sie. Wenn Sie sich darauf verlassen, dass Nutzer:innen jede (!) Mail in der Zukunft richtig erkennen und jeden (!) Download korrekt zuordnen und entscheiden können, ob „gut“ oder „böse“, dann werden Sie diese Wette sicher verlieren. Der Klick auf einen Anhang oder der Download einer Datei darf kein Problem sein.
- Soll ich Euch vertrauen?
  - Nein ? Allerdings sollte ein Download oder Klick auf einen Anhang ja nicht zum Problem werden. Oder etwa doch?
- Wer da drauf klickt, ist selbst schuld!
  - Nein. Nutzer:innen werden von Angreifern ja didaktisch in die Falle gelockt zu klicken. Daher muss die Umgebung für Sicherheit in diesem Fall sorgen. Es wird sehr viel Verantwortung auf den IT-Anwender:innen abgeladen. Der technische Schutz funktioniert ordentlich mit Bordmitteln und vergleichsweise wenig Aufwand.

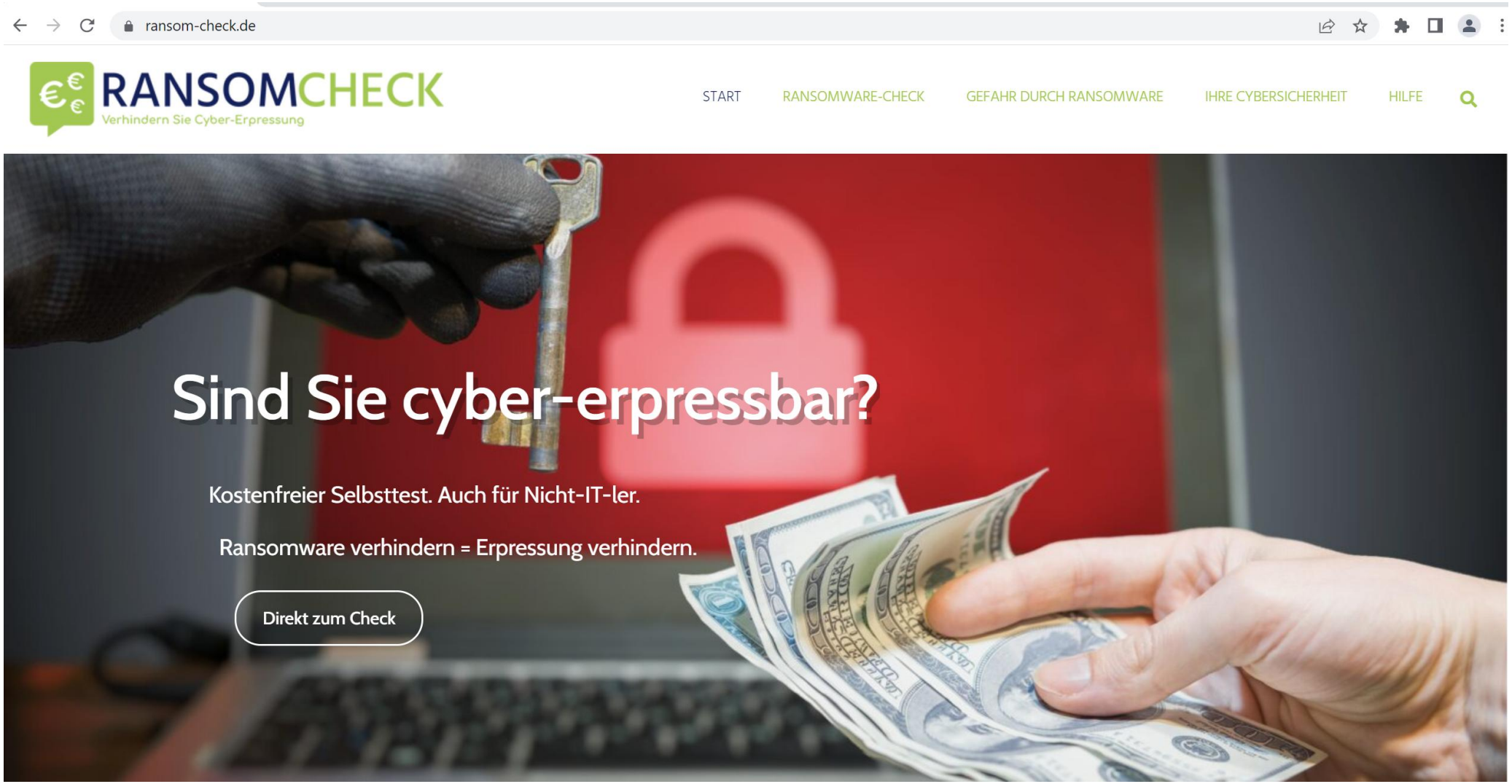
Disclaimer

secuvera:
Cybersicherheit. Nachhaltig.

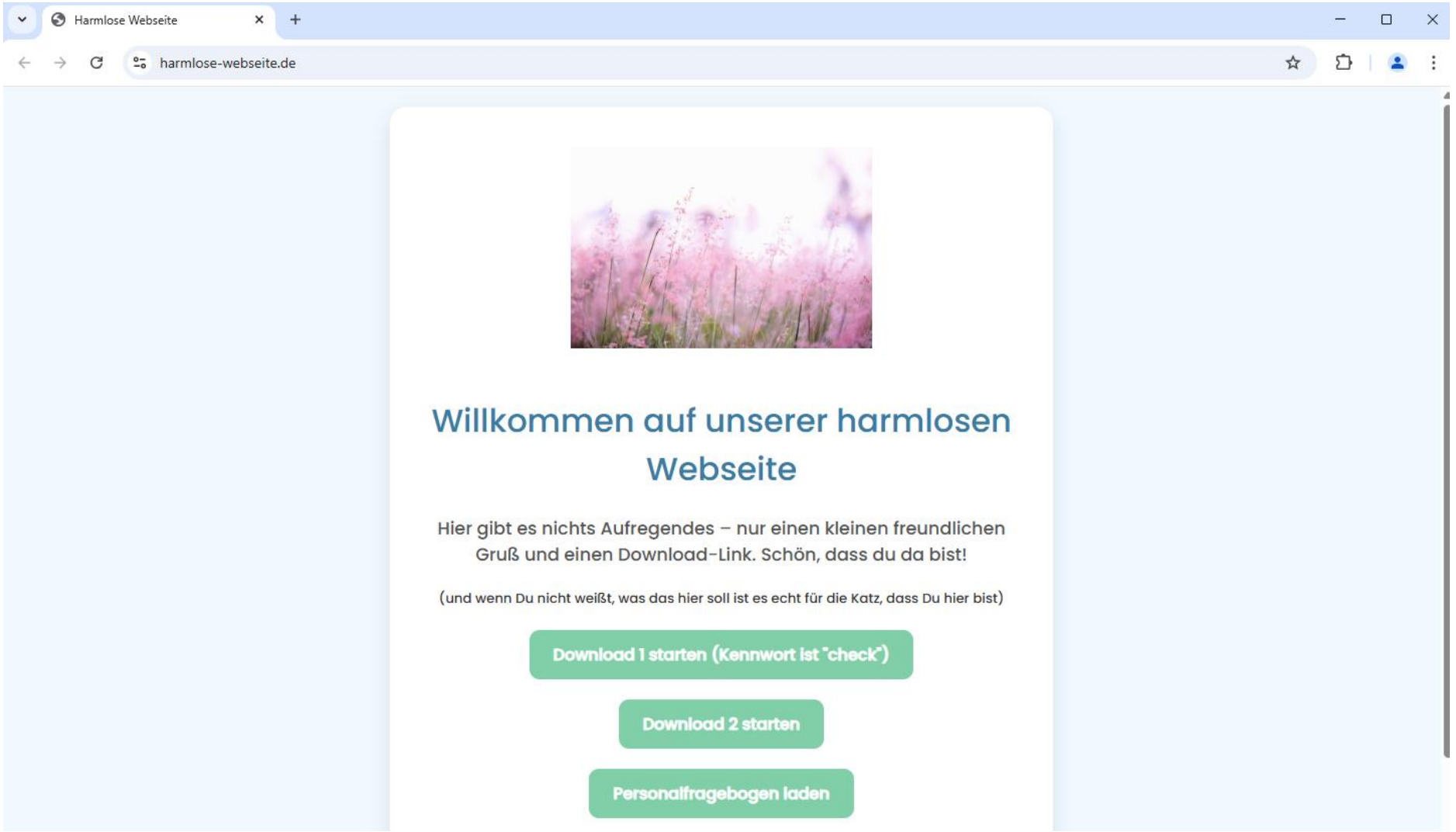
- Bewusster Verstoß gegen Vorgaben möglich
- Unsicher? Reden Sie mit Ihrem CISO/Sicherheitsbeauftragten
- Aber: Sorgen Sie dafür, dass der Check gemacht wird. Bitte.

Go hack yourself

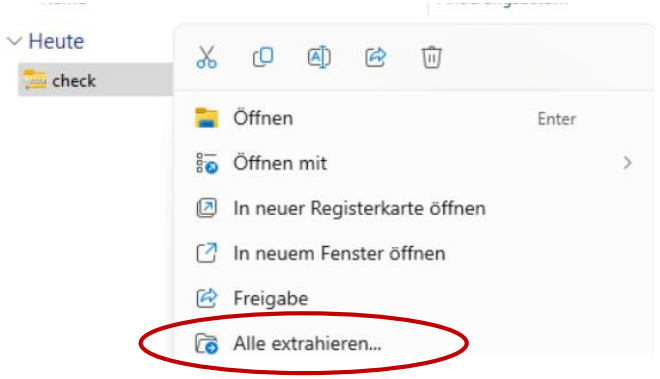
secuvera:
Cybersicherheit. Nachhaltig.

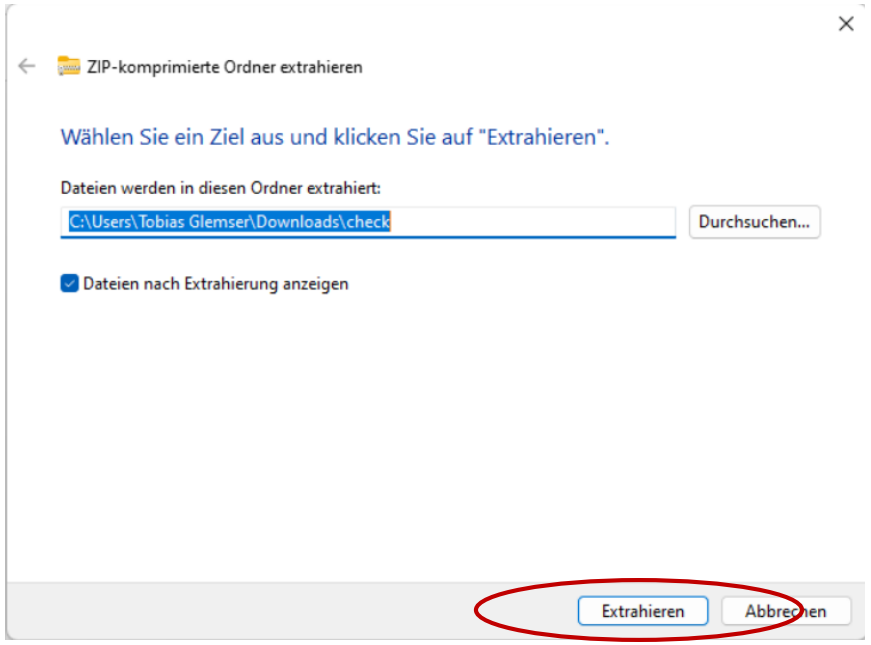


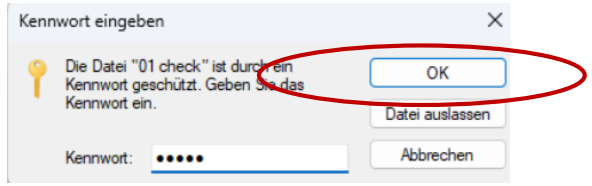
Go hack yourself



Go hack yourself – Vorbereitung

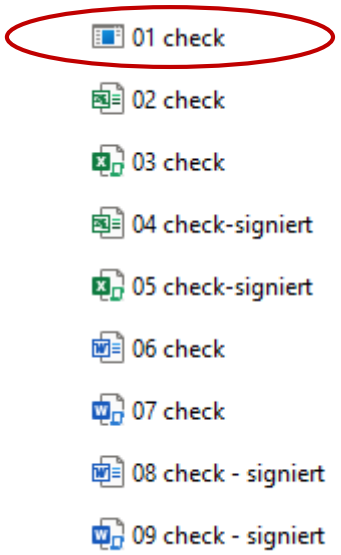


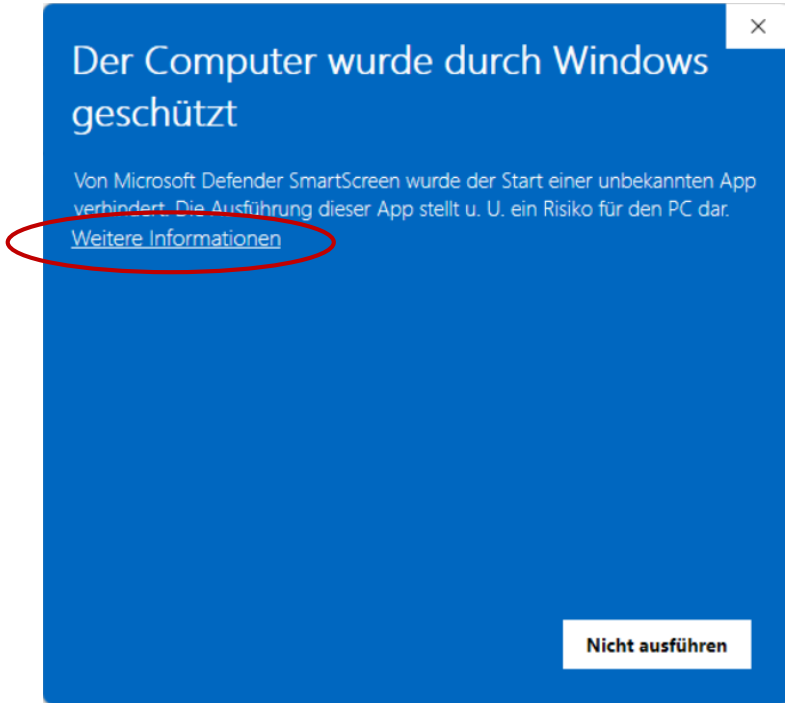




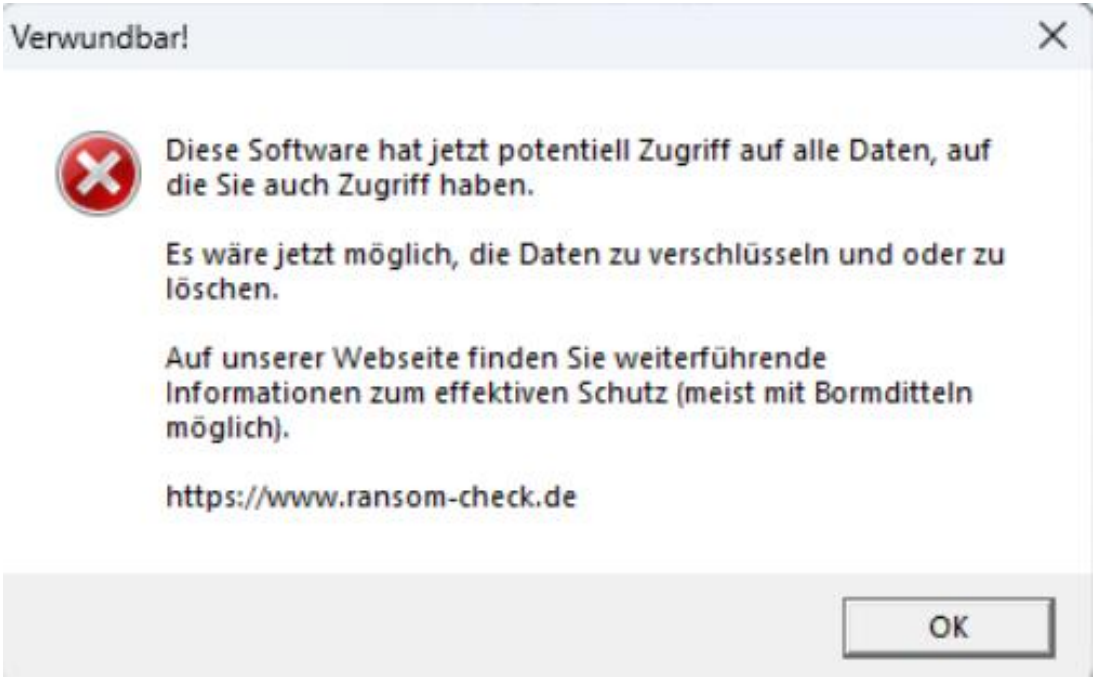
Go hack yourself – Teil 1 – Ausführbare Datei

secuvera:
Cybersicherheit. Nachhaltig.



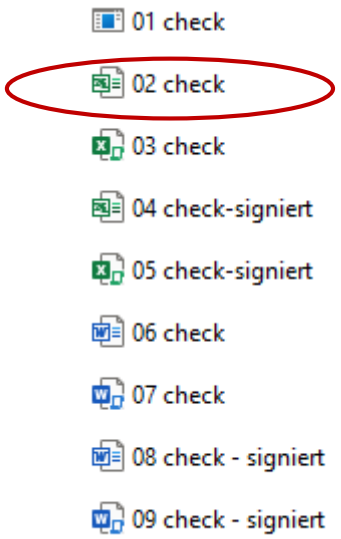


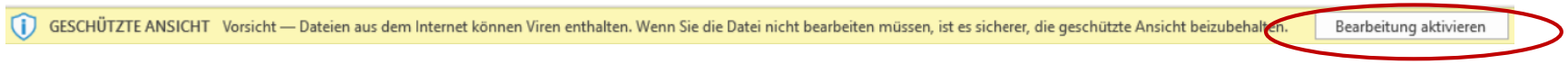
Go hack yourself – Teil 1 – Ausführbare Datei

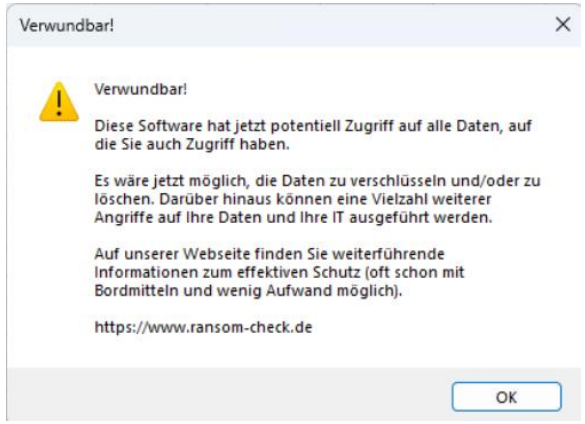


Go hack yourself – Teil 2 – Makro unsigniert

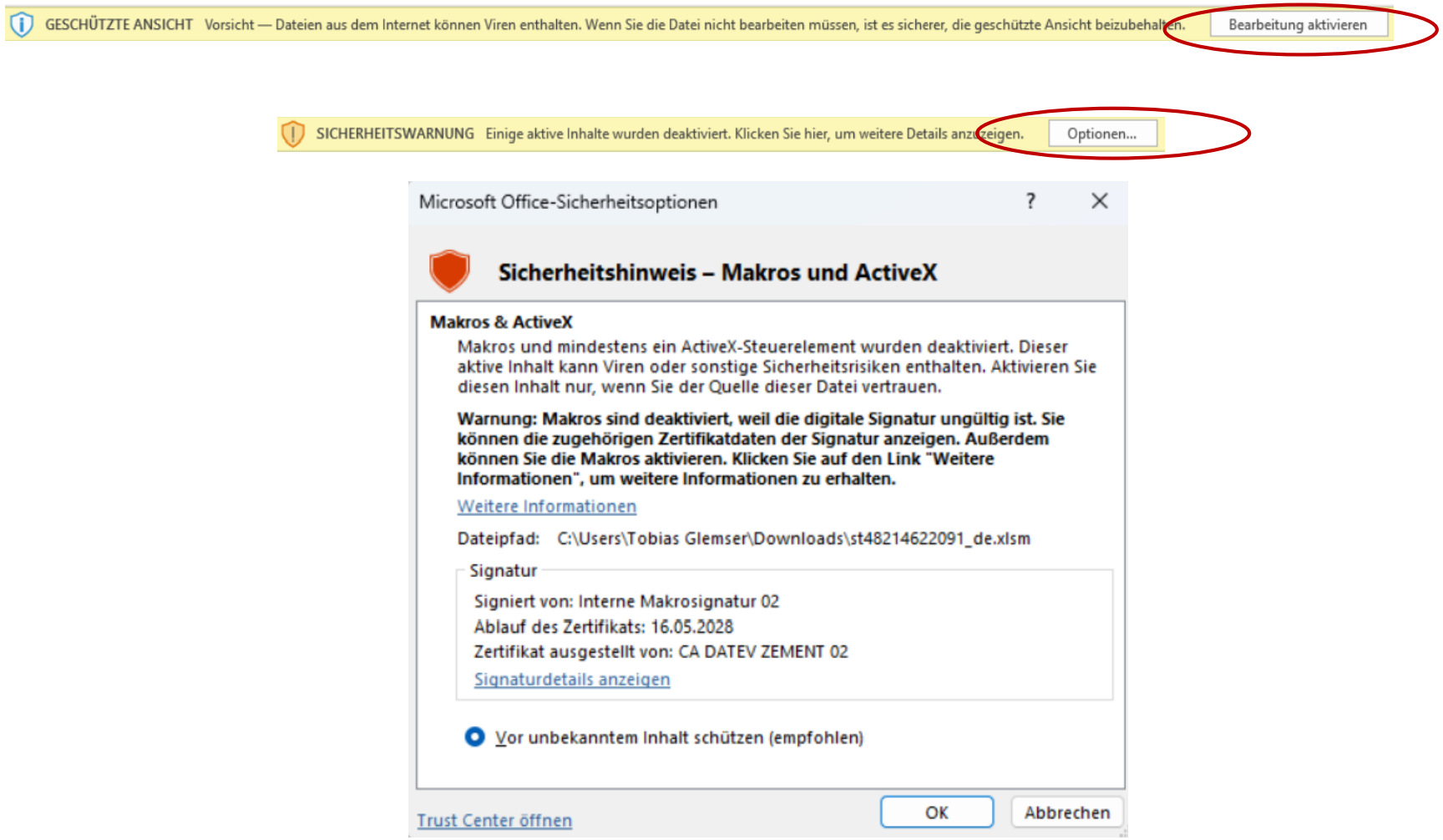
secuvera:
Cybersicherheit. Nachhaltig.







Go hack yourself – Teil 3 – Makro schlecht signiert



Go hack yourself – Teil 4 - Passwortstärke

secuvera:
Cybersicherheit. Nachhaltig.

PASSWORT BRUTEFORCERECHNER

Zeichenauswahl	☑ Großbuchstaben (A, B, C, …) ☑ Kleinbuchstaben (a, b, c, …) ☑ Ziffern (0, 1, 2, …) ☑ Sonderzeichen (&, %, $, …) ☑ Leerzeichen
Weitere Zeichen:	
Passwort-Länge:	8
Versuche pro Sekunde:	10.000.000.000.000.000
Zeichenpool	95
Anzahl möglicher Passwörter	6.634.204.312.890.625
Benötigte Rechenzeit bis zur garantierten Berechnung	0,663 Sekunden

PASSWORT BRUTEFORCERECHNER

Zeichenauswahl	☑ Großbuchstaben (A, B, C, …) ☑ Kleinbuchstaben (a, b, c, …) ☑ Ziffern (0, 1, 2, …) ☐ Sonderzeichen (&, %, $, …) ☐ Leerzeichen
Weitere Zeichen:	
Passwort-Länge:	16
Versuche pro Sekunde:	10.000.000.000.000.000
Zeichenpool	62
Anzahl möglicher Passwörter	4,767 x 10^28
Benötigte Rechenzeit bis zur garantierten Berechnung	151.064,725 Jahre

Checkliste - Technik

secuvera:
Cybersicherheit. Nachhaltig.

- Können Nutzer Programme selbst starten (ransom-check.de)?
- Unsignierte Markos möglich (ransom-check.de)?
- Neue Tastaturen werden erstmal geblockt („Bad-USB“)?
- Zweiter Faktor für alle externen Dienste?
- Gibt es einen „beschulten“ Passwortmanager?
- Werden E-Mails mit eigener Domäne im Absender von außen blockiert/markiert?
- Werden Nutzer regelmäßig, positiv und einfach sensibilisiert?

Checkliste – Organisation und Strategie

secuvera:
Cybersicherheit. Nachhaltig.

- Organisation
  - Ist die Leitung aufgeklärt?
  - Gibt es eine Cyberversicherung mit ausreichender Deckung?
- Strategisch
  - Stand der Dinge erheben lassen (z. B. „Cyber-Sicherheits-Check“, siehe ACS)
  - Maßnahmen technisch prüfen (z. B. Penetrationstest)
  - Managementsystem einführen (z. B. ISO 27001)
  - Hilfe holen (z. B. CISO as a Service/externer IT-Sicherheitsbeauftragter)

Quick-Wins für Ihre Organisation

- Zwei Faktor Authentisierung
  1. Alle externen Anwendungen
  2. Privilegierte Konten
  3. Alle Anwendungen
- Application Allow-Listing
  - Keine „Schatten-IT“ mehr
  - Keine unsignierten Makros
- “Cyberresilienz”..
  1. ... messen (z. B. Cyber - Sicherheits - Check)
  2. ... steuern (ISMS)

Bilderrätsel

secuvera:
Cybersicherheit. Nachhaltig.

Danke sehr!

Weitere Fragen? Beratungsbedarf? Gerne melden.

tglemser@secuvera.de

www.secuvera.de