



**DIGITAL
SICHER
NRW**

Kompetenzzentrum für
Cybersicherheit in der Wirtschaft

Cybersicherheit ist Chefsache

DIGI DAY Hagen

05.06.2024

Peter Meyer

Mitglied der Geschäftsführung bei DIGITAL.SICHER.NRW

Beauftragt vom

Ministerium für Wirtschaft,
Industrie, Klimaschutz und Energie
des Landes Nordrhein-Westfalen



DIGITAL.SICHER.NRW

Kompetenzzentrum für Cybersicherheit in der Wirtschaft in Nordrhein-Westfalen

- **Gegründet:** März 2021
- **Standorte:** Bochum & Bonn
- **Rechtsform:** gGmbH (CyberSEC NRW gGmbH)
- **Trägervereine:** eurobits e.V.
Cyber Security Cluster Bonn e.V.
- **Auftraggeber:** *Ministerium für Wirtschaft, Industrie,
Klimaschutz und Energie des Landes
Nordrhein-Westfalen (MWIKE)*

Auftrag:
**Mehr Bewusstsein für digitale Sicherheit
an kleine und mittlere Unternehmen in NRW herantragen**



DIGITAL SICHER NRW

Kompetenzzentrum für
Cybersicherheit in der Wirtschaft



**Alle Angebote sind kostenlos
und herstellerneutral!**

WARUM IST CYBERSICHERHEIT ELEMENTAR?

206 Mrd. €

Bitkom Studie Wirtschaftsschutz 2023

35 Mrd. €



Durch Cyberattacken entsteht der deutschen Wirtschaft jährlich ein Gesamtschaden von 205,9 Milliarden Euro.

Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen

88%

**Fast 9 von 10 Unternehmen
von Angriffen betroffen
(2020/2021)**

52%

**Jedes zweite Unternehmen
sieht seine geschäftliche Existenz
durch Cyberattacken bedroht**

KMU IN NRW



755 290

KMU* in NRW (99,5% aller Unternehmen sind KMU)

20 945

Mittlere Unternehmen (zwischen 50-249 MA)

Handwerk

Größter Arbeitgeber (ca. 15% aller Beschäftigten)

40,5%

Anteil der Arbeitnehmer bei Unternehmen mit unter 25 Beschäftigten

10,1

Durchschnittliche Mitarbeiterzahl in Unternehmen

68%

Alle Angestellten in NRW arbeiten in KMU (Unternehmen unter 250 Beschäftigte)

85%

Der Arbeitnehmer in NRW arbeiten in Unternehmen mit < 10 Angestellten



PETER MEYER

**Mitglied der Geschäftsführung DIGITAL.SICHER.NRW
Kompetenzzentrum für Cybersicherheit
in der Wirtschaft in NRW**

- seit 2022** **DIGITAL.SICHER.NRW (Standort Bonn)**
- 2021-2022** **Cyber Security Cluster Bonn e.V.**
- 2019-2021** **eyeo GmbH (Köln)**
- 2019-2021* *Beirat SoSafe GmbH (Köln) & cyberwiser.eu*
- 2013-2018** **eco - Verband der Internetwirtschaft (Köln)**
- 2000-2012** **Webwasher AG / McAfee / Intel Security (Paderborn)**

Schwerpunkte:

**Awareness | Phishing | Spam | Botnetze | Malicious Advertising |
Ad- und Content-Blocker | Rechtswidrige Inhalte | Cybercrime |
Online-Betrug | Datensicherheit | Webseiten-Sicherheit | Allrounder**

KEIN UNTERNEHMEN IST

- zu jung
- zu klein
- zu unbedeutend
- zu unattraktiv

um nicht angegriffen zu werden.



DIE CYBERCRIME ÖKONOMIE

– WER SIND DIE TÄTER?



**DIGITAL
SICHER
NRW**

Kompetenzzentrum für
Cybersicherheit in der Wirtschaft

CYBERCRIME AS A SERVICE

Das Vorurteil:

- Warum sollte ausgerechnet mein Unternehmen für Hacker interessant sein?

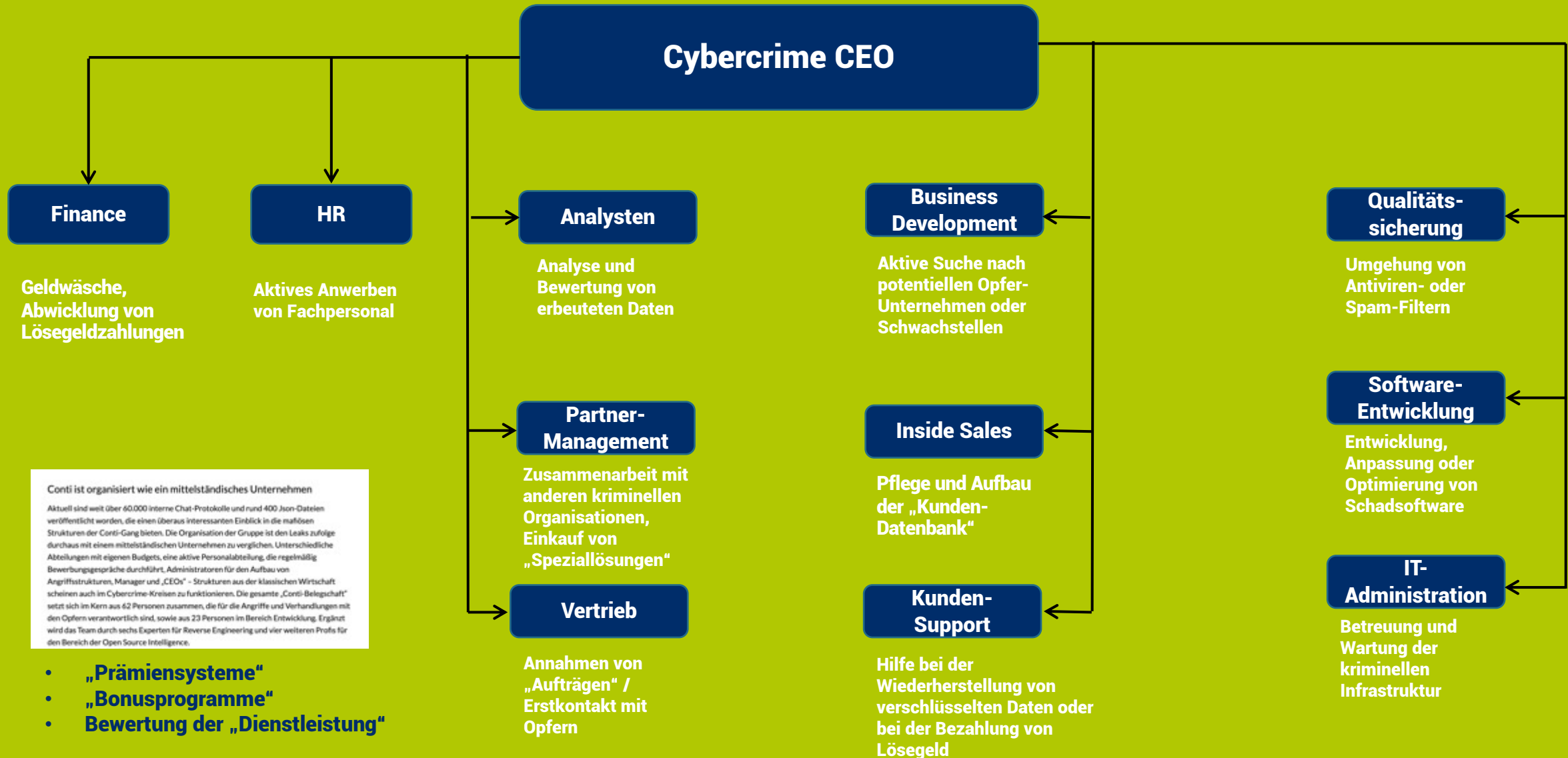
Die Realität:

- Es geht (primär) nicht um Spionage, sondern um „normale“ Kriminalität. Oft werden Daten einfach verschlüsselt und es wird ein Lösegeld erpresst
- Nur ein Bruchteil der „Hackerangriffe“ auf Unternehmen erfolgt gezielt.
- Die Täter gehen nach dem „Gießkannenprinzip“ vor und schauen, wer ihnen beim Phishing an den Haken geht.

Cyberkriminelle sind selten Einzeltäter, sondern professionell-organisierte „mittelständische IT-Unternehmen“



„THIEVERY CORPORATION“



Conti ist organisiert wie ein mittelständisches Unternehmen
 Aktuell sind weit über 60.000 interne Chat-Protokolle und rund 400 Json-Dateien veröffentlicht worden, die einen überaus interessanten Einblick in die mafiosen Strukturen der Conti-Gang bieten. Die Organisation der Gruppe ist den Leaks zufolge durchaus mit einem mittelständischen Unternehmen zu vergleichen. Unterschiedliche Abteilungen mit eigenen Budgets, eine aktive Personalabteilung, die regelmäßig Bewerbungsgespräche durchführt, Administratoren für den Aufbau von Angriffsstrukturen, Manager und „CEOs“ - Strukturen aus der klassischen Wirtschaft scheinen auch im Cybercrime-Kreislauf zu funktionieren. Die gesamte „Conti-Belegschaft“ setzt sich im Kern aus 62 Personen zusammen, die für die Angriffe und Verhandlungen mit den Opfern verantwortlich sind, sowie aus 23 Personen im Bereich Entwicklung. Ergänzt wird das Team durch sechs Experten für Reverse Engineering und vier weiteren Profis für den Bereich der Open Source Intelligence.

- „Prämiensysteme“
- „Bonusprogramme“
- Bewertung der „Dienstleistung“

Phishing-as-a-Service: LabHost

Portfolio:

- **Monatliche Abos für Phishing-Kits: ab 249 US-Dollar**
 - **2.000 registrierte Nutzer**
- **Infrastruktur zum Hosten von Webseiten (40.000 Seiten)**
- **Funktionen zur direkten Interaktion mit Opfern**
- **„Kunden“ konnten aus 170 verschiedenen „Marken“ auswählen (und neue Marken in Auftrag geben)**
 - **Finanzinstitutionen, Post-Dienste oder Telekommunikationsanbietern.**

„Verwaltungswerkzeug“ Labrat:

- **Starten und Überwachen von Angriffen in Echtzeit**
- **Abfangen von Zwei-Faktor-Authentifizierung**
- **Abfangen von Zugangsdaten abfangen**

Datenfundus:

- **480.000 Kreditkartennummern / 64.000 PINs**
- **Mehr als eine Million Passwörter**

Ransomware, auch Erpressungstrojaner, Erpressungssoftware, Kryptotrojaner oder Verschlüsselungstrojaner, sind Schadprogramme, mit deren Hilfe ein Eindringling den Zugriff des Computerinhabers auf Daten, deren Nutzung oder auf das ganze Computersystem verhindern kann.

Dabei werden private Daten auf dem fremden Computer verschlüsselt oder der Zugriff auf sie verhindert, um für die Entschlüsselung oder Freigabe ein Lösegeld zu fordern.



Kein Lösegeld zahlen!*
Nicht mit den Kriminellen verhandeln!

**Acht von zehn Unternehmen und Organisationen, die sich einmal für die Zahlung des Lösegelds entschieden haben, wurden erneut angegriffen – in vielen Fällen sogar von denselben Tätern.*

[Cyberreason](#)

Schön, wenn
TROJANER
nur noch eine Legende sind.

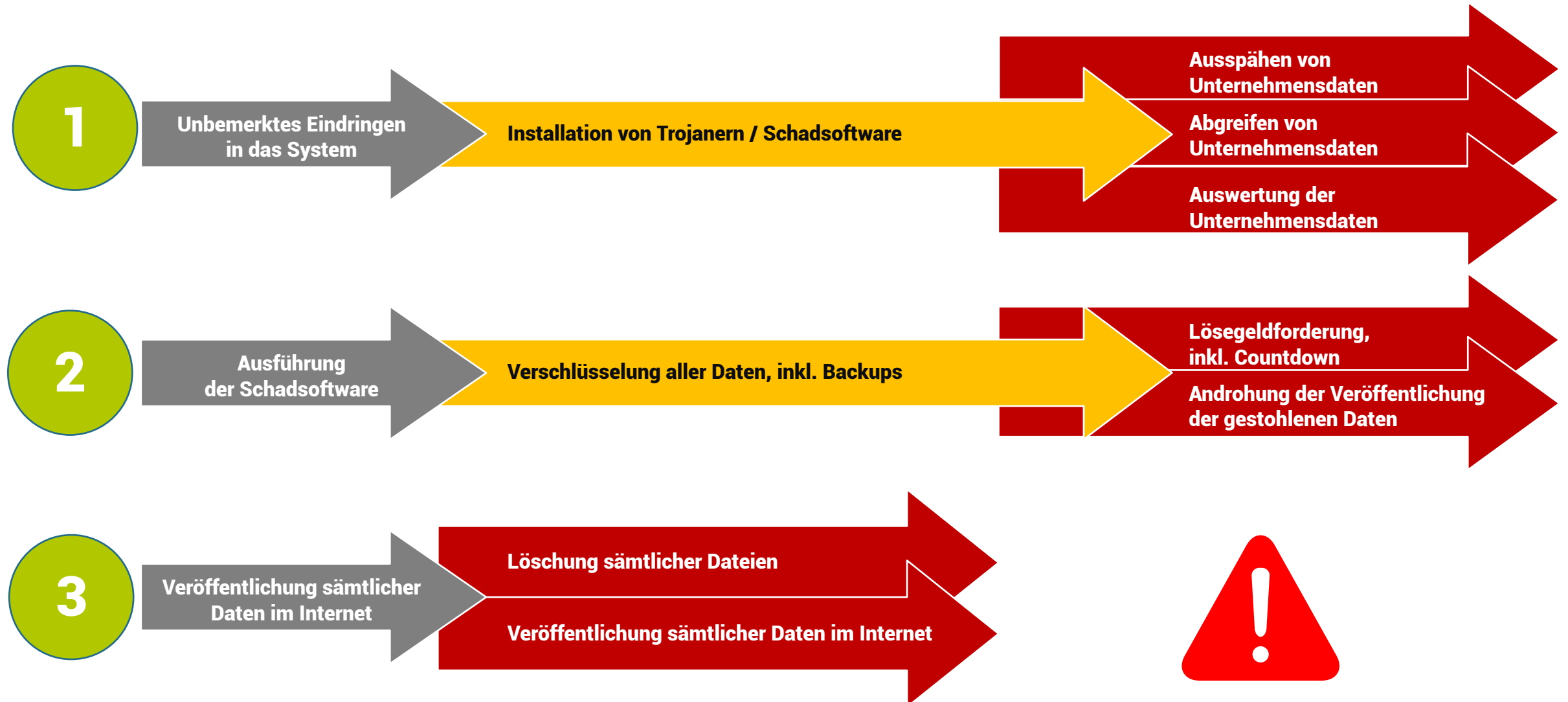
Bis zu **15.000 €**
staatliche
Förderung für
deinen Betrieb

**TÜR ZU
IM NETZ**

Digitale Sicherheit ist wichtig für jedes Unternehmen. Auch du kannst etwas dafür tun, dass dein Betrieb sicher bleibt. Wir helfen dir dabei!
www.tuer-zu-im-netz.nrw

Eine Initiative von:
**DIGITAL
SICHER
NRW**

ABLAUF EINES TYPISCHEN RANSOMWARE-ANGRIFFS



GERÄTE IM INTERNET



WLAN-Router



PCs



Drucker & Scanner



Laptops



Backups



Alarmanlage /
Überwachungskamera



Industrie /
Maschinen



Webseite



Online-Shop



Telefonanlage



Smartphones /
Tablets



Kartenleseterminal

Bei vielen Unternehmen überschreitet inzwischen die Anzahl der Geräte im Netzwerk und mit Internetanschluss die Anzahl der Mitarbeitenden.

Sind bei Ihnen alle diese Geräte vor Fremdzugriff geschützt?
Wer updatet diese Geräte? Wie? Und wann?

IT-NUTZUNG IN UNTERNEHMEN



E-Mails



Office Programme



Social Media



Spezial-Software



Warenwirtschafts-
systeme



Lohnbuchhaltung



Photoshop /
Bildbearbeitung



WhatsApp /
Messenger

DIE KOSTEN EINES CYBERANGRIFFS

Wirtschaft

Nach Hackerangriff: Weseler Traditionsunternehmen meldet nach 150 Jahren Insolvenz an

Der Hackerangriff führte nun dazu, dass das Weseler **Traditionsunternehmen** nach über 150 Jahren die Tore endgültig schließen muss. Über 80 Mitarbeiter droht nun die Arbeitslosigkeit.

Gütersloh

Cyberangriff: Küche bleibt in Kitas, Schulen und Seniorenheime weiterhin kalt

Auch eine Woche nach dem Cyberangriff auf den Gütersloher **Essenslieferanten können Kitas, Schulen und Seniorenheime weiterhin nicht beliefert werden.**

Logistik

Gesamter Fuhrpark steht still: **Spedition in Rheine nach Hackerangriff kann keine Waren ausliefern.**

Castrop-Rauxel: Hackerangriff während Wurzelbehandlung – Patientin erlebt Albtraum!

Während einer Wurzelbehandlung fiel plötzlich die gesamte Technik in einer Zahnarztpraxis in Castrop-Rauxel aus, der behandelnde **Zahnarzt muss die Wurzelbehandlung abbrechen.**

Freizeit:

Kino in Hagen bleibt nach Cyberangriff noch bis zum Wochenende geschlossen

Das beliebte Hagener **Kino** leidet weiterhin unter den Folgen eines Hackerangriffs, bei dem u.a. die Filmprojektoren in den Sälen durch sogenannte Erpressungstrojaner weiterhin keine Filme abspielen können.

CYBERCRIME:

ANLAGENBAUER AUS HÖXTER MUSS DIE HÄLFTE SEINER MITARBEITER ENTLASSEN
ÜBER DREI WOCHEN STANDEN DIE ANLAGEN DES **ANLAGENBAUERS** STILL. DER ENTSTANDENE SCHADEN FÜHRT NUN DAZU, DASS DAS UNTERNEHMEN ETWA DIE HÄLFTE SEINER MITARBEITENDEN ENTLASSEN MUSS.

Lokale Wirtschaft

Tischlermeister berichtet von den Folgen des Cyberangriffs: „Ich hätte nicht gedacht, dass mein Betrieb so abhängig von der EDV ist“

Euskirchen: „Alle Kundendaten und Rechnungen waren plötzlich weg, wir hatten keine Übersicht mehr über unseren Lagerbestand, nicht mal die Telefonanlagen funktionierte noch“, berichtet der 48 jährige Tischlermeister noch immer schockiert.

Internet:

Kundendaten veröffentlicht: Arnsberger **Steuerkanzlei** muss nach Hackerangriff 23.000 EUR Strafe zahlen

Nach einem Hackerangriff stellten Kriminelle sensible Kundendaten der Arnsberger Steuerkanzlei ins Internet. Aufsichtsbehörde sieht in dem Vorfall ein fahrlässiges Verhalten der Kanzlei.

Hinweis: Die folgenden Meldungen sind „konstruiert“, basieren auf tatsächlichen Vorfällen

WENIG AUFWAND

80 / 20

GROSSE WIRKUNG



RISIKOFAKTOR Nr.1: E-MAIL

Phishing & Co.



**DIGITAL
SICHER
NRW**

Kompetenzzentrum für
Cybersicherheit in der Wirtschaft

E-MAILS

90%

90% aller erfolgreichen Cyber-Angriffe beginnen mit einer E-Mail

- Abgreifen von Zugangsdaten
- Manuelles Starten der Schadsoftware
- Falsche Identitäten

Schön, wenn beim
PHISHING
niemand anbeißt.

Bis zu
15.000 €
staatliche
Förderung für
deinen Betrieb

**TÜR ZU
IM NETZ**

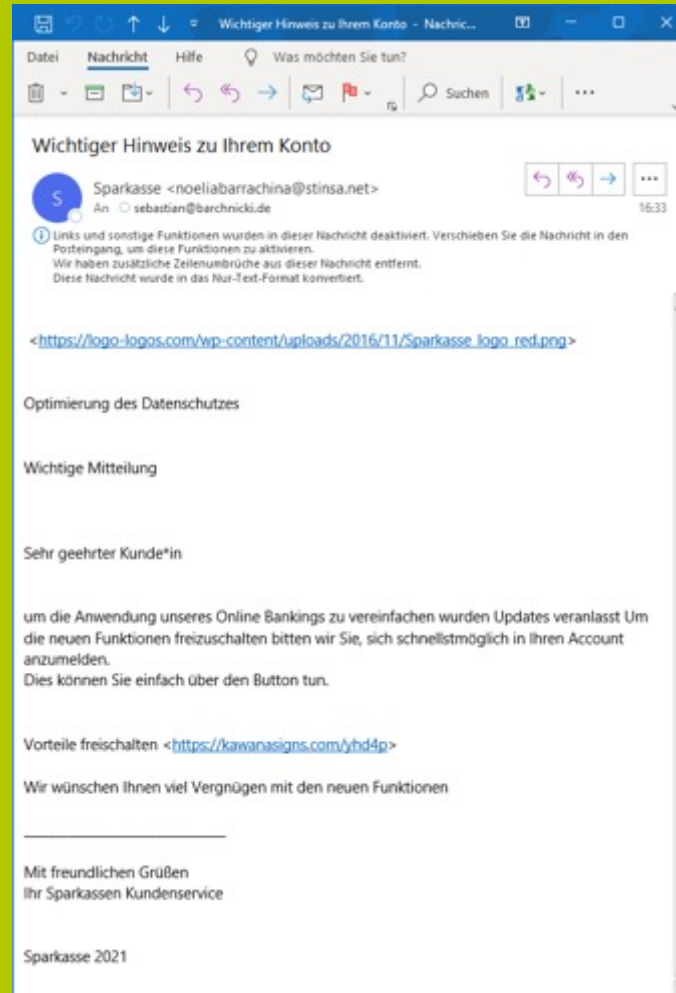
Digitale Sicherheit ist wichtig für jedes Unternehmen. Auch du kannst etwas dafür tun, dass dein Betrieb sicher bleibt. Wir helfen dir dabei!
www.tuer-zu-im-netz.nrw

Eine Initiative von:
**DIGITAL SICHER
NRW**

HTML vs. Text



„HTML sieht
doch toll aus!“



Wichtiger Hinweis zu Ihrem Konto

Sparkasse <noeliabarrachina@stinsa.net>
An: sebastian@barchnicki.de

Links und sonstige Funktionen wurden in dieser Nachricht deaktiviert. Verschieben Sie die Nachricht in den Posteingang, um diese Funktionen zu aktivieren.
Wir haben zusätzliche Zeilenumbrüche aus dieser Nachricht entfernt.
Diese Nachricht wurde in das Nur-Text-Format konvertiert.

<https://logo-logos.com/wp-content/uploads/2016/11/Sparkasse_logo_red.png>

Optimierung des Datenschutzes

Wichtige Mitteilung

Sehr geehrter Kunde*in

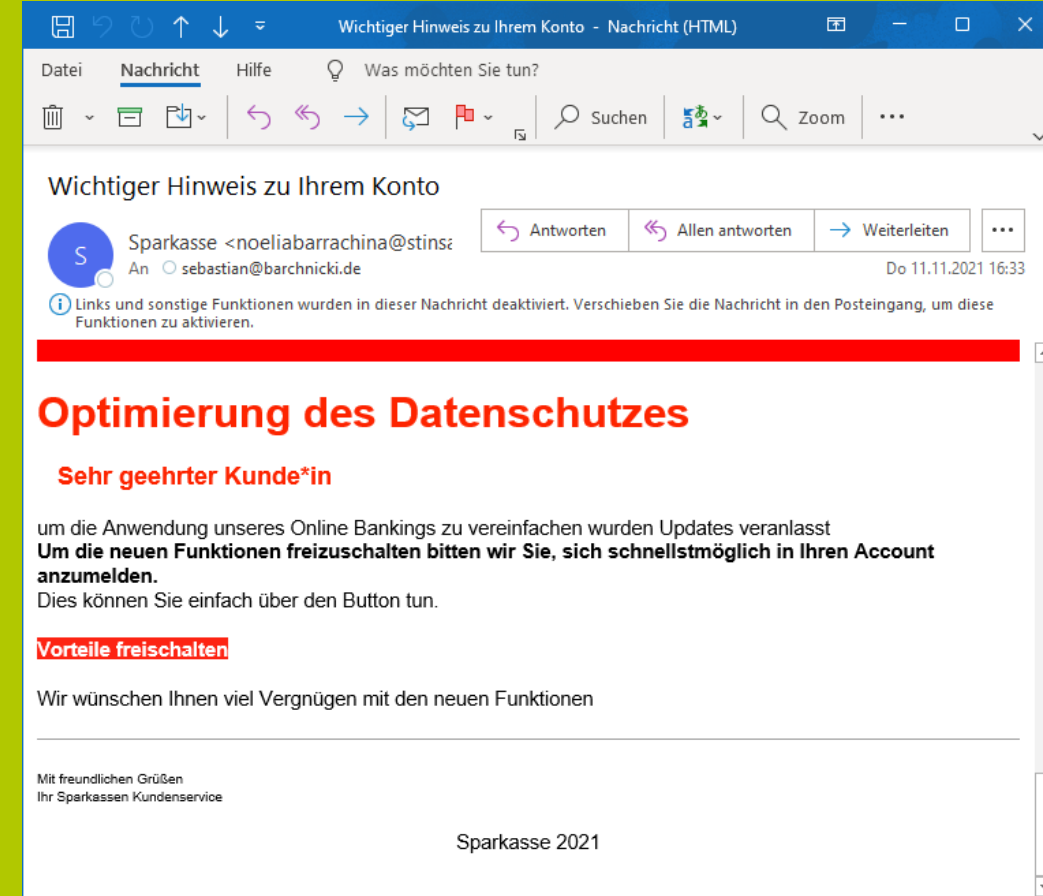
um die Anwendung unseres Online Bankings zu vereinfachen wurden Updates veranlasst Um die neuen Funktionen freizuschalten bitten wir Sie, sich schnellstmöglich in Ihren Account anzumelden.
Dies können Sie einfach über den Button tun.

Vorteile freischalten <<https://kawanasigns.com/yhd4p>>

Wir wünschen Ihnen viel Vergnügen mit den neuen Funktionen

Mit freundlichen Grüßen
Ihr Sparkassen Kundenservice

Sparkasse 2021



Wichtiger Hinweis zu Ihrem Konto (HTML)

Sparkasse <noeliabarrachina@stins: >
An: sebastian@barchnicki.de

Do 11.11.2021 16:33

Links und sonstige Funktionen wurden in dieser Nachricht deaktiviert. Verschieben Sie die Nachricht in den Posteingang, um diese Funktionen zu aktivieren.

Optimierung des Datenschutzes

Sehr geehrter Kunde*in

um die Anwendung unseres Online Bankings zu vereinfachen wurden Updates veranlasst
Um die neuen Funktionen freizuschalten bitten wir Sie, sich schnellstmöglich in Ihren Account anzumelden.
Dies können Sie einfach über den Button tun.

Vorteile freischalten

Wir wünschen Ihnen viel Vergnügen mit den neuen Funktionen

Mit freundlichen Grüßen
Ihr Sparkassen Kundenservice

Sparkasse 2021

Phishing – ein alter Hut!

- Erste bekannte Phishing-Mail: 02.01.1996
- Wo: alt.online-service.america-online (USENET)

Seitdem hat sich an der Methodik wenig geändert:

- Die E-Mail enthält einen Link
- „Die E-Mail“ bittet darum, die Zugangsdaten auf einer Webseite zu aktualisieren
- E-Mail erzählt „irgendeine“ Geschichte
- Die verlinkte Webseite ist manipuliert
- Die Webseite sieht fast aus wie die „echte“ Seite

ABGREIFEN VON ZUGANGSDATEN

- E-Mail erzählt „irgendeine“ Geschichte
 - „Fehler“
 - „Zugang gesperrt“
 - „Lieferung / Paket konnte nicht zugestellt“
 - „Buchungsfehler“
 - „Gutschrift“ / Auszahlung
 - „Offener Posten“
 - „Update von AGBs“
 - „Unberechtigter Zugang“
 - usw.
- „Call to action“
 - „Schnell, sonst passiert etwas“

Credential Stuffing

- Was wollen Kriminelle mit Ihren Netflix-Zugangsdaten?
 - 81 % der Nutzer haben ein Passwort für zwei oder mehr Websites wiederverwendet (https://en.wikipedia.org/wiki/Credential_stuffing)
 - 25 % der Nutzer verwenden dieselben Passwörter für die Mehrzahl ihrer Konten.
 - Ein Drittel der weltweiten Anmeldeversuche erfolgt mit erbeuteten Login-Daten (Okta, 2022)

| Schließung Ihres Kontos |

NETFLIX

Sehr geehrter Kunde

Bitte beachten Sie, dass Ihr Abonnement erneut ausgesetzt wurde. Bei unserem letzten Versuch, Ihr Abonnement zu verlängern, wurde Ihre Zahlung von Ihrer Bank abgelehnt oder der Vorgang wurde nicht abgeschlossen.

Es ist jedoch unbedingt erforderlich, dass Sie die Dringlichkeit der Situation verstehen. Dies ist die letzte Erinnerung vor der endgültigen Schließung Ihres Kontos. Wenn Ihre Rechnungsinformationen nicht sofort aktualisiert werden, wird der Zugang zu Ihrem Konto und allen seinen Vorteilen gesperrt. Wir möchten nicht, dass Sie den Zugang zu den mit Ihrem Abonnement verbundenen Diensten und Funktionen verlieren.

Um die endgültige Schließung Ihres Kontos zu verhindern und weiterhin alle Vorteile unseres Dienstes nutzen zu können, bitten wir Sie, Ihre Rechnungsinformationen umgehend zu aktualisieren.

Aktualisieren

ABGREIFEN VON ZUGANGSDATEN

Tipps:

- Kein Provider / Bank usw. wird Sie normalerweise per E-Mail auffordern, Ihre Zugangsdaten zu aktualisieren.
- Niemals über einen Link in einer E-Mail seine Zugangsdaten auf einer Webseite eingeben
- Rufen Sie die echte Webseite manuell auf (Suchmaschine / Bookmark / App)
- Misstrauen Sie jeder E-Mail, die darum bittet, Passwörter zu ändern.
- Fragen Sie bei Zweifeln direkt beim Anbieter/Absender nach
- Nutzen Sie jedes Passwort nur einmal!

Schön, wenn man das

PASSWORT

auch zum Fluchen verwenden kann

Bis zu **15.000 €** staatliche Förderung für deinen Betrieb

#\$_*!?

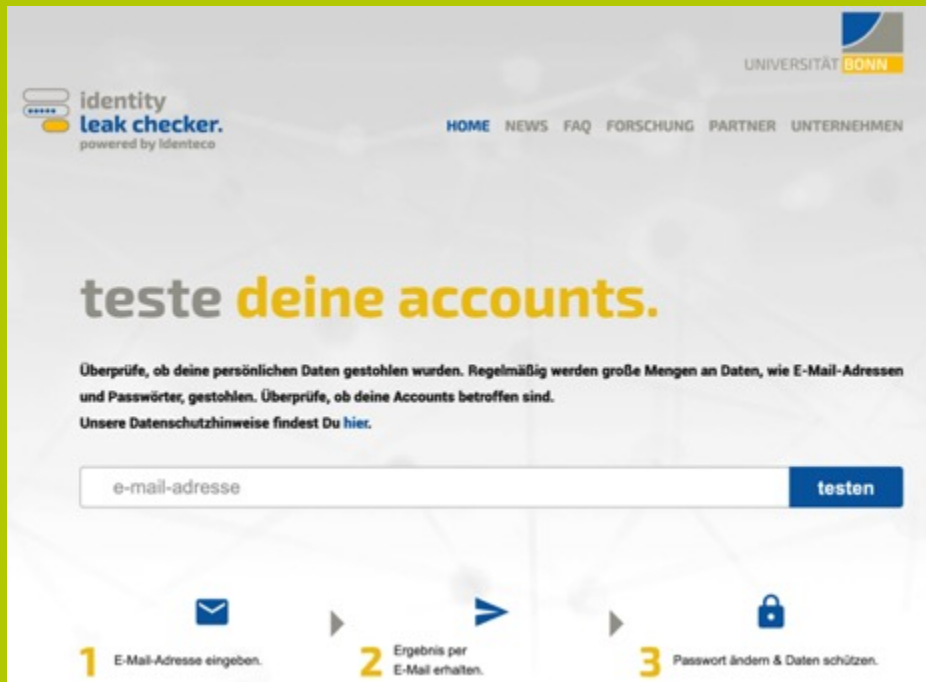
TÜR ZU IM NETZ

Digitale Sicherheit ist wichtig für jedes Unternehmen. Auch du kannst etwas dafür tun, dass dein Betrieb sicher bleibt. Wir helfen dir dabei
www.tuer-zu-im-netz.nrw

Eine Initiative von:

DIGITAL SICHER NRW

ACCOUNT-SICHERHEIT



identity leak checker.
powered by Identico

UNIVERSITÄT BONN

HOME NEWS FAQ FORSCHUNG PARTNER UNTERNEHMEN

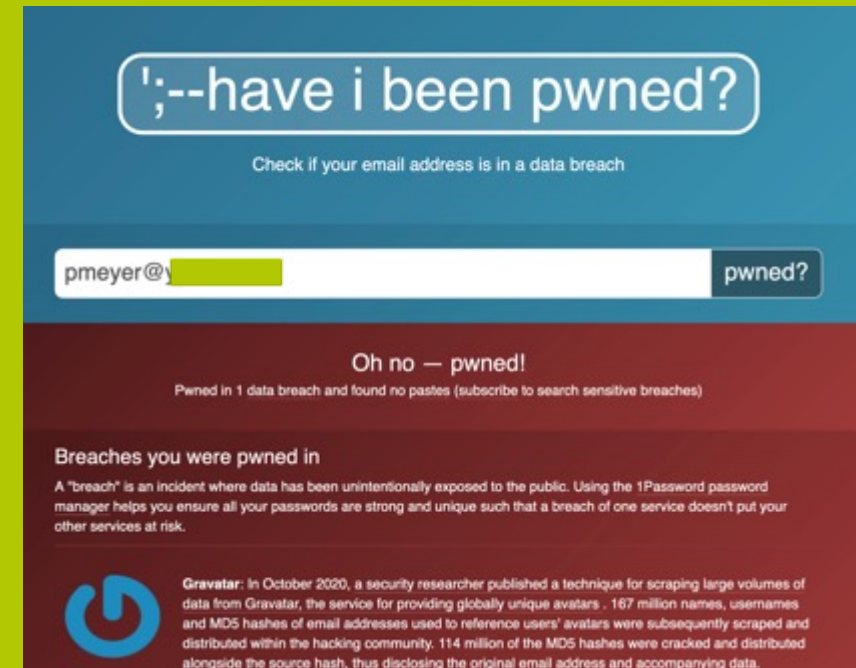
teste deine accounts.

Überprüfe, ob deine persönlichen Daten gestohlen wurden. Regelmäßig werden große Mengen an Daten, wie E-Mail-Adressen und Passwörter, gestohlen. Überprüfe, ob deine Accounts betroffen sind. Unsere Datenschutzhinweise findest Du hier.

e-mail-adresse **testen**

- 1 E-Mail-Adresse eingeben.
- 2 Ergebnis per E-Mail erhalten.
- 3 Passwort ändern & Daten schützen.

<https://leakchecker.uni-bonn.de>



;-have i been pwned?

Check if your email address is in a data breach

pmeyer@[redacted] **pwned?**

Oh no — pwned!
Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Gravatar: In October 2020, a security researcher published a technique for scraping large volumes of data from Gravatar, the service for providing globally unique avatars. 167 million names, usernames and MD5 hashes of email addresses used to reference users' avatars were subsequently scraped and distributed within the hacking community. 114 million of the MD5 hashes were cracked and distributed alongside the source hash, thus disclosing the original email address and accompanying data.

<https://haveibeenpwned.com>

Phishing Methode 2:

SCHADSOFTWARE IM ANHANG

E-Mails mit Schadsoftware im Anhang, die ein User selbst aktiviert



**DIGITAL
SICHER
NRW**

Kompetenzzentrum für
Cybersicherheit in der Wirtschaft

MANUELLES STARTEN DER SCHADSOFTWARE

- E-Mail erzählt „irgendeine“ Geschichte
 - Bewerbung oder Rechnung
 - Update einer Software / Treiber
 - Inkompatibilität einer Datei
 - Wichtige Information
- Die E-Mail enthält einen Anhang, den Sie öffnen sollen und ggf. ein „Makro“ o.ä. starten müssen.
- Die E-Mail bittet Sie „etwas“ von einer Webseite / einem App Store „etwas“ zu installieren
- Der Link führt Sie auf eine manipulierte Webseite, wo automatisch ein Download erfolgt

Schön, wenn
SPY-WARE
nur von James Bond
angezogen wird.

Bis zu
15.000 €
staatliche
Förderung für
deinen Betrieb

**TÜR ZU
IM NETZ**

Digitale Sicherheit ist wichtig für jedes Unternehmen. Auch du kannst etwas dafür tun, dass dein Betrieb sicher bleibt. Wir helfen dir dabei!
www.tuer-zu-im-netz.nrw

Eine Initiative von:
**DIGITAL SICHER
NRW**

Phishing Methode 3:

Spear Phishing

Gezielt und personalisiert gesendete E-Mails an Mitarbeitende im Unternehmen oder Privatpersonen



**DIGITAL
SICHER
NRW**

Kompetenzzentrum für
Cybersicherheit in der Wirtschaft

CEO-FRAUD

- E-Mail-Absender gibt sich als vertraute Person aus
- Direkte Anrede
- Person bittet etwas zu erledigen
 - Schnell
 - Vertraulich / Diskret
- Empfänger soll:
 - Etwas überweisen
 - Gutscheine kaufen
 - Dokumente teilen
 - Zugangsdaten weitergeben
 - Etwas installieren (Teamviewer o.ä.)
- Absender reagiert schnell, übt Druck aus und schmeichelt

CEO-FRAUD

- Absender-Adresse genau kontrollieren
- Immer misstrauisch sein / a-typisches Verhalten hinterfragen
- Auf einen zweiten "Kanal" nachfragen & eine Bestätigung einholen
 - Messenger / Telefon / Chat
- Interne Prozesse etablieren
- Firmenkultur anpassen



<https://botfrei.de/safer-internet-day-christina-und-der-vermeintliche-ceo>

ACCOUNT-SICHERHEIT

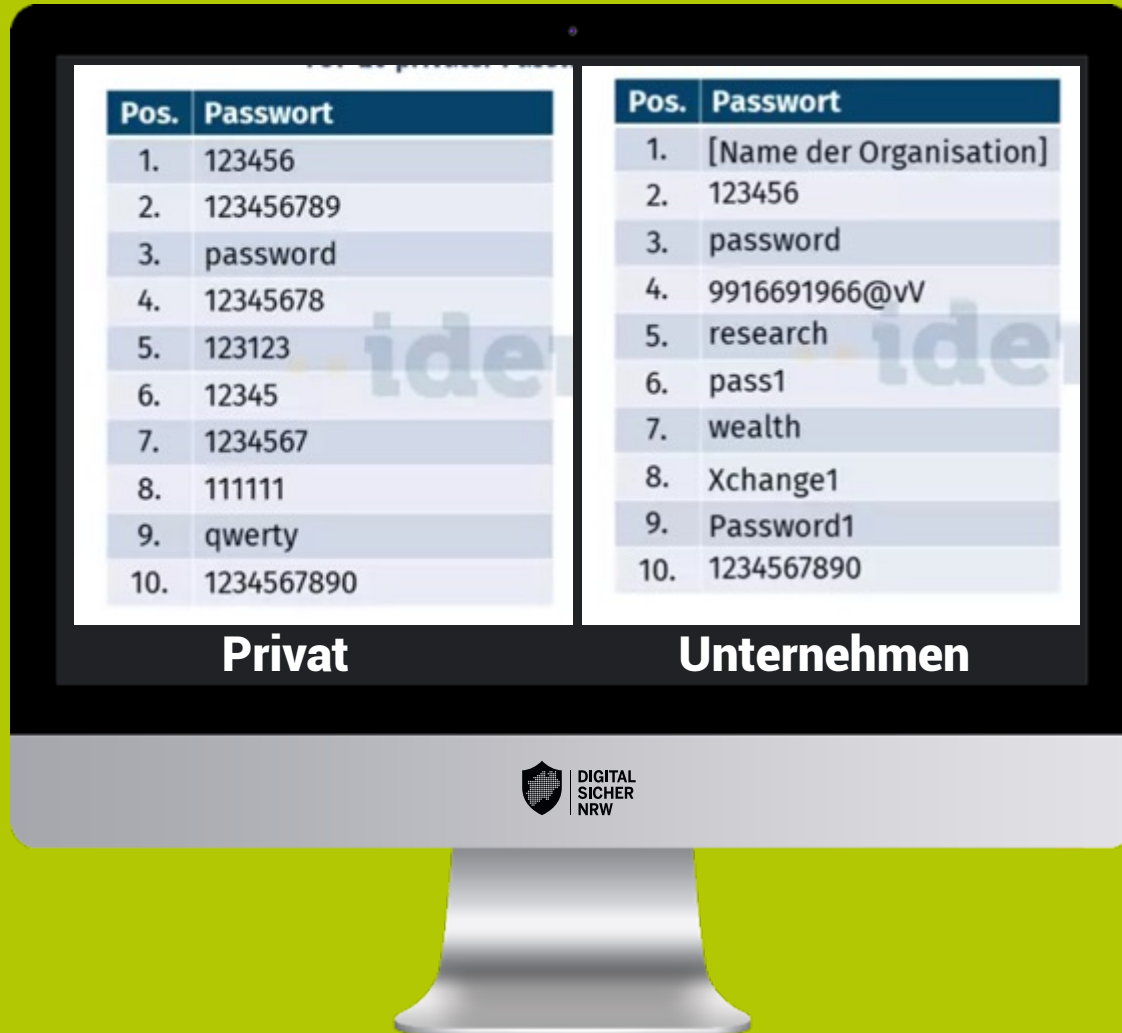
Passwörter & Co.



**DIGITAL
SICHER
NRW**

Kompetenzzentrum für
Cybersicherheit in der Wirtschaft

TOP 10 DEUTSCHER PASSWÖRTER 2023



- **Länge:** Mindestens zwölf Zeichen
- **Vollen ASCII-Zeichensatz nutzen**
 - **Groß- und Kleinschreibung**
 - **Zahlen / Sonderzeichen**
- **Komplex:** Keine Begriffe aus dem Wörterbuch verwenden
- **Jedes Passwort nur 1x nutzen**
- **Keine regelmäßigen Änderungen notwendig**
- **Passwort Manager unternehmensweit nutzen**
- **Passwort-Richtlinien festlegen & technisch umsetzen**

Passwörter & Brute Force

Zeichenanzahl	Nur numerisch	Nur Kleinbuchstaben	Groß- und Kleinbuchstaben	Ziffern, Groß- und Kleinbuchstaben	Ziffern, Groß- und Kleinbuchstaben, Symbole
8	sofort	sofort	2 Minuten	7 Minuten	39 Minuten
12	2 Sekunden	2 Tage	24 Jahre	200 Jahre	3000 Jahre
13	19 Sekunden	2 Monate	1.000 Jahre	12.000 Jahre	202.000 Jahre
14	3 Minuten	4 Jahre	64.000 Jahre	750.000 Jahre	16 Mio. Jahre
15	35 Minuten	100 Jahre	3 Mio. Jahre	46 Mio. Jahre	1 Mrd. Jahre
16	5 Stunden	3.000 Jahre	173 Mio. Jahre	3 Milliarden Jahre	92 Mrd. Jahre
17	2 Tage	69.000 Jahre	9 Mrd. Jahre	179 Mrd. Jahre	7 Bill. Jahre
18	3 Wochen	2 Mio. Jahre	467 Mrd. Jahre	11 Bill. Jahre	438 Bill. Jahre

Multi-Faktor Authentifizierung

- Zwei-Faktor Authentifizierung
 - TAN-Nummer beim Online-Banking
- Multi-Faktor Authentifizierung
 - Authentifizierung per SMS
 - Authentifikations-App
 - Biometrie (Gesichtserkennung, Fingerabdruck Sprache)
 - Anruf / Passcode
 - QR-Code



Eine Multi-Faktor-Authentifizierung ist der heutige „Stand der Technik“

Nutzen Sie eine Multi-Faktor Authentifizierung, wo immer es möglich ist!

Zugriffsrechte

- Admin-Rechte / Zugriffsrechte behutsam vergeben
- Als Admin nur anmelden (und angemeldet bleiben), wenn erforderlich
- Active Directory (Nutzerverwaltung) besonders schützen
- Zugriffe / Zugriffsrechte protokollieren (Datenschutz beachten!)
- Zugriffsrechte regelmäßig prüfen
- Bei Personalwechsel (Kündigung, Austritt) Zugriffsrechte rechtzeitig entziehen
- Nutzung gemeinsamer Accounts vermeiden
- Redundanzen schaffen

Admin-Accounts / Admin-Rechte nur zum Administrieren nutzen!



TECHNISCHE MASSNAHMEN

Backups & Updates



**DIGITAL
SICHER
NRW**

Kompetenzzentrum für
Cybersicherheit in der Wirtschaft

WARUM SIND BACKUPS WICHTIG?

RANSOMWARE

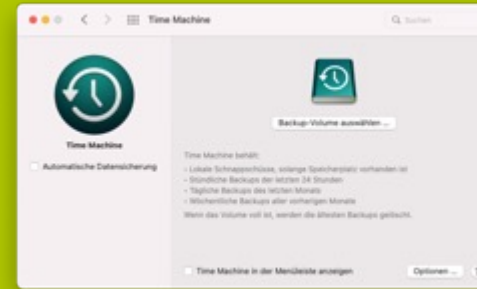
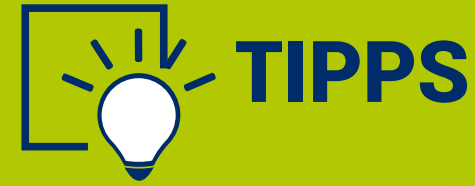
- Schadprogramm, das den Zugriff auf Systeme einschränken oder unterbinden kann (Erpressung)
- Für die Freigabe wird von Kriminellen ein Lösegeld gefordert
- Häufigkeit und Erfolg von Ransomware-Attacken nehmen immer weiter zu



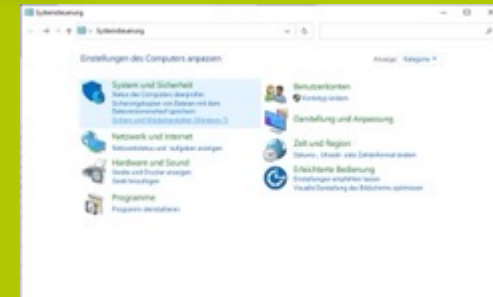
Backups können Angriffe selbst zwar nicht verhindern, stellen aber sicher, dass Ihr Unternehmen danach schnellstmöglich wieder betriebsbereit ist.

BACKUPS

- Haben Sie schon mal geprüft, wie und ob sich die Backups wieder einspielen lassen?
- Sind die Backups so redundant, dass Sie nach einem Ransomware-Angriff nicht mit verschlüsselt wurden?
- Enthält das Backup alles notwendige?
- Wer ist im Notfall bei Ihnen dafür zuständig?
- Und wie und wann ist die Person erreichbar?
- Sind die Backups alt genug, um eine vorherige Infektion auszuschließen?



Vorinstallierte Backup-Tools bei Windows und MacOS



Webinar:
Effektive Backups für KMU

UPDATES

- Wer ist wann für welche Updates verantwortlich?
 - User vs. IT-Abteilung vs. IT-Verantwortlicher
- Updates möglichst automatisieren
 - Netzwerkgeräte (Drucker, Telefonanlage, Router, Firewall etc.)
 - Clients / Mobilgeräte
 - IoT / OT-Geräte
- Mitarbeitende sollten regelmäßig Browser oder Geräte neu starten
- Sicherheitsupdates an Mitarbeitende kommunizieren
- Sicherheitshinweise z.B. vom Hersteller oder BSI beachten
- „Patch-Gap“



Einsatz veralteter Software

- Mehr als 1,8 Millionen Windows-Computer in Deutschland mit veralteten Betriebssystemen im Internet
 - Rund 1,5 Millionen Geräte mit Windows 7 (Supportende: 14. Januar 2020)
 - 90.000 Systeme mit Windows XP (Supportende: 8. April 2014)
- Support-Ende für Windows 10: 14. Oktober 2025
- Keine Updates von Microsoft (außer: spezieller Supportvertrag für Sicherheitsupdates)
- Keine Sicherheitsupdates

Nicht mehr updatebare Geräte vom Netzwerk isolieren (z.B. in der Industrie / Gesundheitswesen)

NOTFALL &

NOTFALLPLANUNG



**DIGITAL
SICHER
NRW**

Kompetenzzentrum für
Cybersicherheit in der Wirtschaft

NOTFALLMANAGEMENT

- Wen müssen Sie kontaktieren? Sind die Personen erreichbar?
- Wer ist Teil Ihres „Krisenstabs“?
- Wie benachrichtigen Sie Ihre Kunden und Geschäftspartner?
- Wie benachrichtigen Sie Ihre Mitarbeiter?
- Wann und wie schalten Sie die Polizei ein?
- Wie stellen Sie einen ersten Notfallbetrieb her?
- Wie stellen Sie z.B. die Gehaltszahlungen sicher?

Über die Hälfte der Beschäftigten weiß nicht, was im Fall eines IT-Sicherheitsvorfalls zu tun wäre.

- In kleinen und mittleren Unternehmen in NRW sind dies weniger (42%) (G DATA GmbH 2022).

VERHALTEN BEI IT-NOTFÄLLEN



Ruhe bewahren & IT-Notfall melden

Lieber einmal mehr als einmal zu wenig anrufen!



IT-Notfallrufnummer:



Wer meldet?



Welches IT-System ist betroffen?



Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?



Wann ist das Ereignis eingetreten?



Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

Weitere Arbeit
am IT-System
einstellen

Beobachtungen
dokumentieren

Maßnahmen nur
nach Anweisung
einleiten

WAS TUN NACH EINEN RAMSOMWARE-ANGRIFF?

- Polizei einschalten – Strafanzeige stellen
- IT-Dienstleister informieren
- Beweise sichern
- Leistungen in Ihrer Cyberversicherung prüfen
- Internen Krisenstab einrichten
- Kommunikation (Intern / extern)
- Notfall-Infrastruktur aufsetzen



Kein Lösegeld zahlen!*

Nicht mit den Kriminellen verhandeln!

**Acht von zehn Unternehmen und Organisationen, die sich einmal für die Zahlung des Lösegelds entschieden haben, wurden erneut angegriffen – in vielen Fällen sogar von denselben Tätern. [Cyberreason](#)*



KONTAKT FÜR
FIRMEN,
INSTITUTIONEN UND
BEHÖRDEN



**Cybercrime-Kompetenzzentrum
Single Point of Contact (SPoC)**

Tel.: +49 211 939-4040

Fax: +49 211 939-194040

E-Mail: cybercrime.lka@polizei.nrw.de

Adresse:

Völklinger Straße 49

40221 Düsseldorf

DIGITALE SICHERHEIT IST CHEFSACHE!



**Investieren Sie 20% Ihres
IT-Budgets
in digitale Sicherheit!**

Sonst wird es richtig teuer!



SCHULEN SIE IHRE MITARBEITER!

- Digitale Sicherheit ist immer ein Zusammenspiel von Mensch und Technik
- Digitale Sicherheit erfordert die Aufmerksamkeit aller Mitarbeitenden – von Updates bis zum Phishing E-Mails.
- Jeder Mitarbeitende sollte über die Risiken und Folgen von Cyberangriffen sensibilisiert werden.
- Informieren Sie Ihre Mitarbeiter und Kollegen regelmäßig über aktuelle Gefahren
- Installieren Sie interne Prozesse



CYBERSPRACHE UND SIE!

- **Niemand erwartet, dass Sie alles Digitale verstehen, lösen oder regeln müssen**
- **Tauschen Sie Sich im Freundeskreis / bei anderen Unternehmen zur Digitalen Sicherheit aus.**
- **Lassen Sie sich einen vertrauensvollen Dienstleister empfehlen**
- **Fragen Sie uns bei DIGITAL.SICHER.NRW!**

Cybersecurity Buzzword Bingo

SSO	XDR	Resilienz	Crypto	0-Day	APT	IoT
Industrie 4.0	SSL	SDK	Cyber	DKIM	Smart	Machine Learning
PKI	Endpoint Security	CVE	ZeroTrust	DDoS	Human Risk Management	Cloud
2FA	Künstliche Intelligenz	VPN	NextGen	Quanten-computing	TISAX	MFA
Threat Intel	TLS	BSI	Supply-Chain	ChatGTP	DSGVO	BYOD
OpenID	SaaS	ISO 27001	DSNRW	Compliance	KRITIS	Blockchain
Hyperscaler	RPKI	Edge Computing	Quanten-cryptographie	Fuzzing	BCM	Managed Services

**FÖRDERMÖGLICHKEITEN
FÜR KLEINE
UND MITTLERE
UNTERNEHMEN**



MID-DIGITALE SICHERHEIT



5 Gründe, jetzt die Förderung zu beantragen!

Bis zu 15.000 €
Förderprämie

1

Bis zu 70 %
Förderquote

2

Verbesserung
der digitalen Sicherheit

3



**MID-Digitale
Sicherheit**

4

Für kleine und mittelgroße
Unternehmen aus NRW

5

Wir unterstützen Sie bei
der Auswahl Ihrer
Förderschwerpunkte

Jetzt digitale
Erstberatung buchen:



**DIGITAL
SICHER
NRW**



**DIGITAL
SICHER
NRW**

Kompetenzzentrum für
Cybersicherheit in der Wirtschaft

FÖRDERSCHWERPUNKTE



DIGITAL
SICHER
NRW

Schwerpunkt A: Analyse des Ist-Zustandes

Analyse ihrer
IT-Sicherheits-Infrastruktur und
Behebung erkannter
Schwachstellen

Durchführung von
Penetrationstests

Erarbeitung von Notfallplänen /
Notfallmanagement

Schwerpunkt B: Faktor Mensch

Sensibilisierung und Schulung
der Mitarbeitenden

Fortbildung von Mitarbeitenden
zur/zum
IT-Sicherheitsbeauftragten

Das Land NRW
unterstützt Ihre
Schritte zu einem
digital sicheren
Betrieb – und das
mit bis zu
15.000 Euro



Schwerpunkt C: Software / Hardware

Software*
Antiviren-Software
Ransomware-Schutz
DDoS-Schutz
Back-Up-Software

Schlüsselfertige Firewalls
(Soft- und Hardware)

*Installation, Erwerb von Lizenzen
sowie die Wartung



DIGITAL
SICHER
NRW

Kompetenzzentrum für
Cybersicherheit in der Wirtschaft

DIGITALE ERSTBERATUNG

Schauen Sie unbedingt auf
unserer Webseite vorbei oder
sprechen Sie uns an!

Unsere Beratung ist für nordrhein-westfälische Betriebe **kostenfrei**. Scheuen Sie sich nicht und vereinbaren noch heute einen Termin, um Ihre digitale Selbstverteidigung zu stärken.

BERATUNGSTERMIN VEREINBAREN

Ihr/e DIGITAL.SICHER.NRW-Ansprechpartner/in zu allen Fragen rund um digitale Sicherheit:



Arbnor Memeti

„Jeder, der denkt, er sei nicht digitalisiert, sollte sich fragen: Habe ich einen PC, eine Webseite oder ein Kassensystem? Dann muss auch digitale Sicherheit eine Rolle im Betrieb spielen.“



Lena Nienstedt

"Technische Maßnahmen helfen bei Ihrer digitalen Sicherheit. Der beste Schutz gegen Cyberangriffe sind aber Sie."



Sebastian Barchnicki

"Eine gute Vorbereitung ist günstiger als eine teure Nachsorge. Mit wenig Aufwand können Sie bereits einen wirksamen digitalen Schutz aufbauen – packen Sie's an!"

www.digital-sicher.nrw

IT-SICHERHEITSKOMPASS

Grundregeln der IT-Sicherheit

Fast alle mittelständischen Unternehmen in Nordrhein-Westfalen haben sich in den letzten Jahren zunehmend digitalisiert. Das hat einerseits viele Arbeiten enorm erleichtert. Andererseits wurden so neue Angriffsflächen innerhalb von Unternehmen geschaffen. Diese zu schließen und sich vor einem Großteil digitaler Kriminalität zu schützen, ist für kleine und mittlere Unternehmen ein zentrales Zukunftsthema.

Passwörter



Smartphones und Tablets



Internet und Browser



Spam und Anti-Virus



Backups (Sicherheitskopien)



Löschen und Zerstören



Home-Office und mobiles Arbeiten



Online-Shops



Verschlüsselung



Schauen Sie unbedingt auf
unserer Webseite vorbei oder
sprechen Sie uns an!

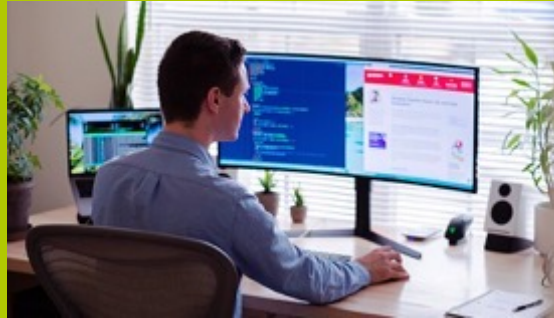
www.digital-sicher.nrw



KOSTENLOSE WEBINARE – GRUNDLAGEN & VERTIEFUNG



Webinar:
Rundflug durch die Cybersicherheit
im Unternehmen



Webinar:
Sicher im Home-Office



Webinar:
Smartphones, Tablets und Laptops in
der Firma



Webinar:
Gefahren im Internet – So schützen
Sie sich und Ihr Unternehmen



Webinar:
Geschäftsgeheimnisse schützen –
Verschlüsselung im Unternehmen



Webinar:
Effektive Backups für KMU

BESUCHEN SIE UNSERE WEBSITEN



[WWW.DIGITAL-SICHER.NRW](http://www.digital-sicher.nrw)



[WWW.TUER-ZU-IM-NETZ.NRW](http://www.tuer-zu-im-netz.nrw)



**DIGITAL
SICHER
NRW**

**Kompetenzzentrum für Cybersicherheit in
der Wirtschaft in NRW**

VIELEN DANK!

Adresse

**Standort Bochum
Lise-Meitner-Allee 4
44801 Bochum**

**Standort Bonn
Rheinwerkallee 6
53227 Bonn**

Kontakt

 **+49 234 - 5200 7334**

 **info@digital-sicher.nrw**



**Peter Meyer
Mitglied der Geschäftsführung**

**E-Mail: meyer@digital-sicher.nrw
Mobil: +49 151 50805500**

**Rheinwerkallee 6
53227 Bonn**