DIGITAL SICHER NRW

Kompetenzzentrum für Cybersicherheit in der Wirtschaft

Machen wir gemeinsam die „Tür zu im Netz“: Wie Sie das digitale Dauerlüften in Ihrem Betrieb beenden.

Düsseldorf, 12.03.2025

Beauftragt vom

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

KURZE VORSTELLUNG

Sebastian Barchnicki

Bachelor of Science Praktische Informatik
Master of Science Internet-Sicherheit

IT-Sicherheitsforschung im Bereich Frühwarnsysteme, Mobile Security und Strategieentwicklung

Leiter Unternehmensstrategie bei einem der führenden IT-Sicherheitsunternehmen in Deutschland (Geschäftsbereiche: eHealth, Innere Sicherheit, Industrie, Öffentliche Auftraggeber, Verteidigung & Raumfahrt)

Sprecher der Geschäftsführung bei DIGITAL.SICHER.NRW

„Überzeugter Anwender“

Digitale Sicherheit von Anfang an mitdenken

vs.

TÜR ZU

IM NETZ

ICH BIN JA GAR NICHT „DIGITALISIERT“ ▶ IST DAS SO?

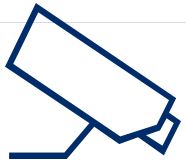
WLAN-Router

PCs

Drucker & Scanner

Laptops

Backups



Alarmanlage/Überwachungskamera

Industrie/Maschinen

Webseite

Online-Shop

Telefonanlage

Smartphones/Tablets

Kartenleseterminal

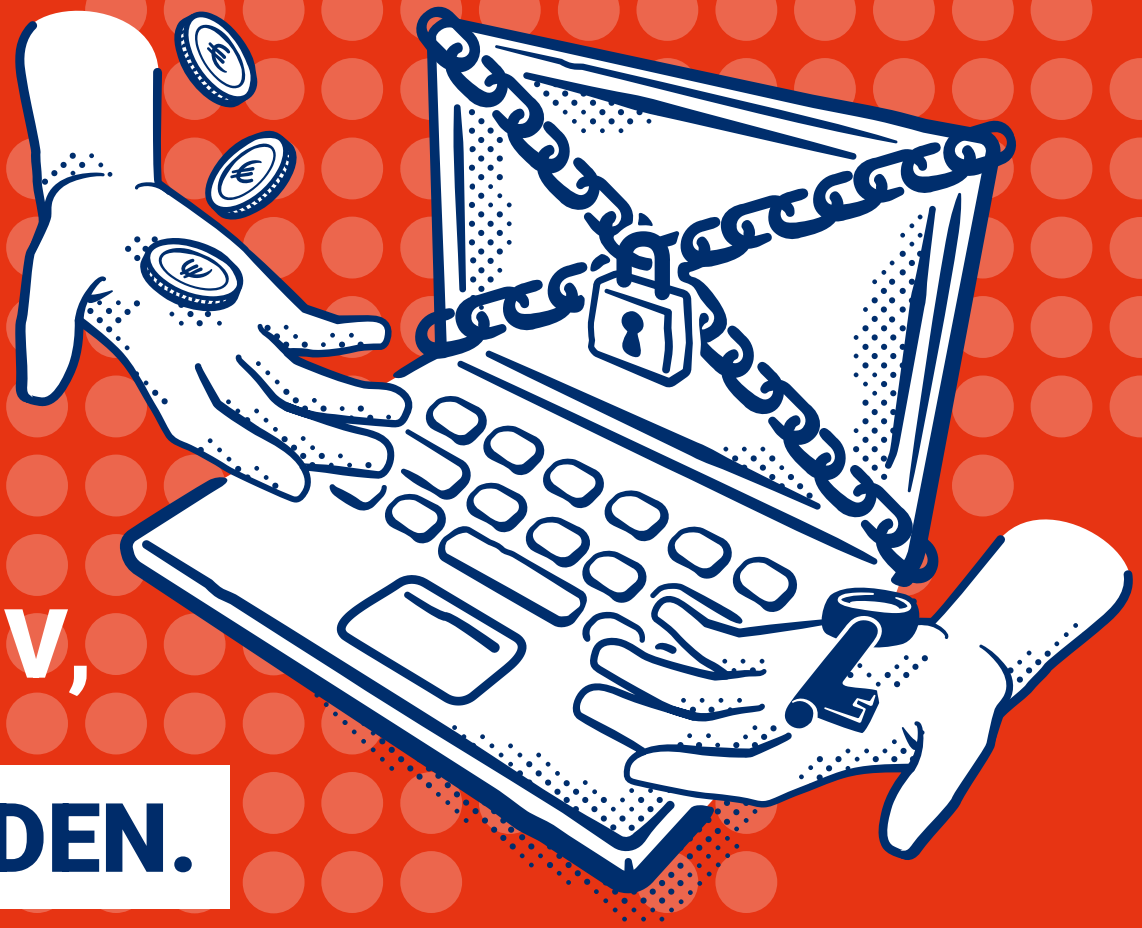
Bei vielen Unternehmen:
Anzahl der Geräte im Netzwerk und mit Internetanschluss übersteigt die Anzahl der Mitarbeitenden

- **Sind bei Ihnen alle diese Geräte vor Fremdzugriff geschützt?**
- **Wer updatet diese Geräte? Wie? Und wann?**
- **Muss jedes Gerät 24/7 mit dem Internet verbunden sein?**

KEIN UNTERNEHMEN IST

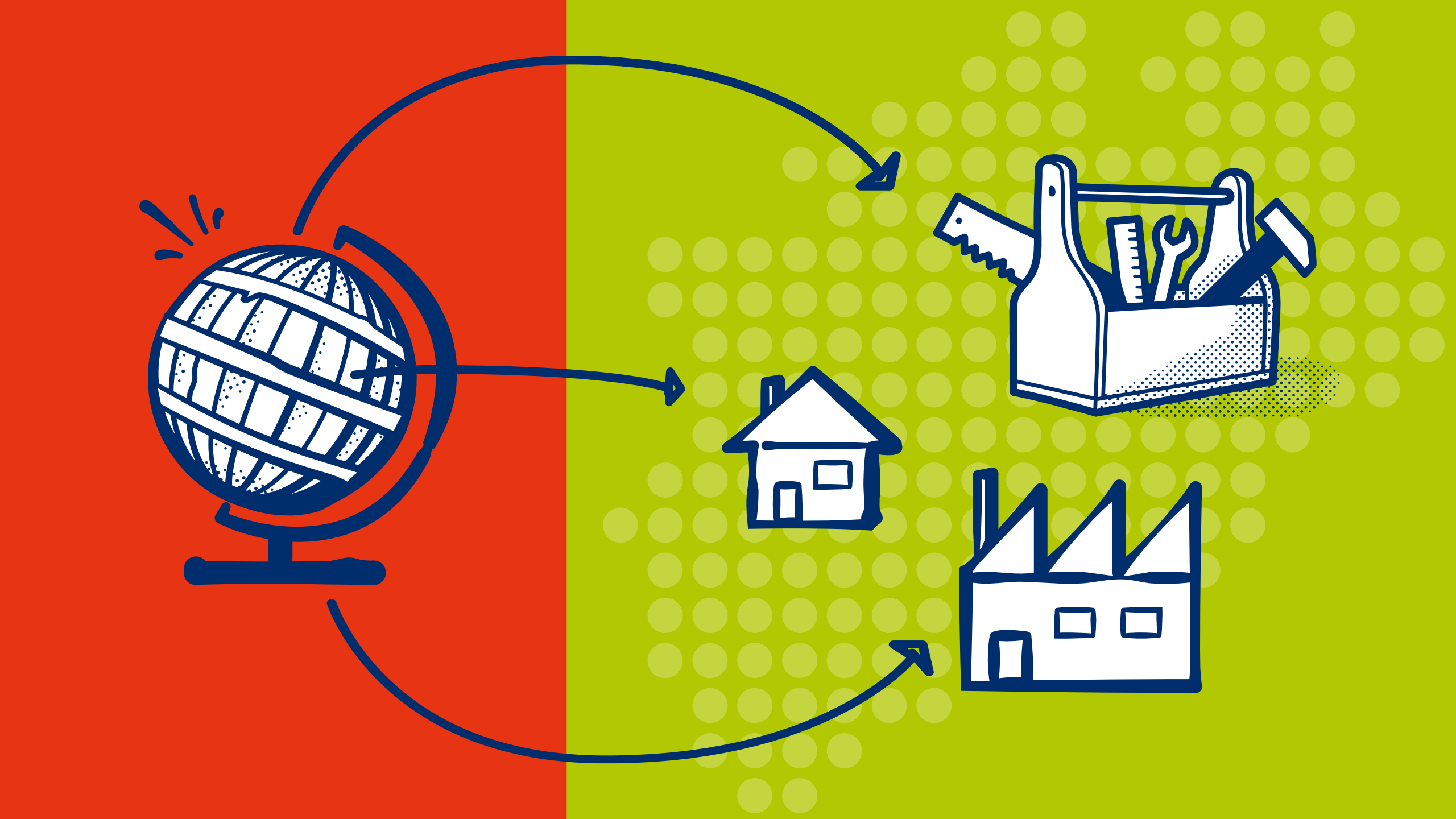
ZU JUNG,
ZU KLEIN,
ZU UNBEDEUTEND,
ZU UNATTRAKTIV,

UM ANGEGRIFFEN ZU WERDEN.



REALITÄT

DIGITAL



WAS IST RANSOMWARE?

- Nach erfolgreicher Infektion eines Systems folgt die vollständige Verschlüsselung dessen und zieht eine Erpressung des Betroffenen nach sich.
- verschiedene Wege der Ausbringung:
  - Phishing-E-Mails
  - Trojaner
- Angriff kann vielschichtig sein:
  - Daten und Systeme verschlüsseln
  - Daten veröffentlichen

„WIR HACKEN JEDEN GmbH“ – Ransomware as a Service

Cybercrime „CEO“

Finance

Geldwäsche, Abwicklung von Lösegeldzahlungen

HR

Aktives Anwerben von Fachpersonal

Analysten

Analyse und Bewertung von erbeuteten Daten

Business Development

Aktive Suche nach potenziellen Opfer-Unternehmen oder Schwachstellen

Qualitätssicherung

Umgehung von Antiviren- oder Spam-Filtern

Partner-Management

Zusammenarbeit mit anderen kriminellen Organisationen, Einkauf von „Speziallösungen“

Inside Sales

Pflege und Aufbau der „Kunden-Datenbank“

Software-Entwicklung

Entwicklung, Anpassung oder Optimierung von Schadsoftware

Vertrieb

Annahmen von „Aufträgen“ / Erstkontakt mit Opfern

Kunden-Support

Hilfe bei der Wiederherstellung von verschlüsselten Daten oder bei der Bezahlung von Lösegeld

IT-Administration

Betreuung und Wartung der kriminellen Infrastruktur

Nach allem, was wir wissen, leidet auch diese Branche unter einem Mangel an Fachkräften …

Beispiel-Organigramm

ZIELE VON CYBERCRIME AS A SERVICE

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 Täterinnen und Tätern. *Cyberreason*

DIE NOTFALLNUMMER DES LKA NRW

0211/939-4040

LKA Cybercrime-Kompetenzzentrum Single Point of Contact (SPoC)

Diese Hotline steht allen Unternehmen und Organisationen **rund um die Uhr** in Nordrhein-Westfalen kostenfrei zur Verfügung.
Sie dient als erste Ansprechstelle im Falle eines Cyberangriffs.

CYBERCRIME AS A SERVICE

Phishing-Kampagne

Preis inklusive Hosting und entsprechendem Toolkit:

494 $ pro Monat

Einstiegspreis:
28 Dollar pro Monat

Quelle: us-risk-black-market-ecosystem.pdf (deloitte.com)

Keylogging-Kampagne

Preis inklusive angepasster Malware, Versand, Hosting und entsprechendem Toolkit:

723 $ pro Monat

Einstiegspreis:
183 Dollar pro Monat

Quelle: us-risk-black-market-ecosystem.pdf (deloitte.com)

160 Mio. E-Mail-Adressen

Gesamter Datensatz von E-Mail-Adressen und Passwörtern von z.B. Dubsmash:

2.000 $

Durchschnittlich 30.000 Accounts: **für 1 $**

Quelle: https://www.theregister.com/2019/02/11/620_million_hacked_accounts_dark_web/

DUNKELZIFFER: BETROFFENE UNTERNEHMEN

BETROFFENE UNTERNEHMEN IN NRW 2024 (Auszug)

Anzahl der Mitarbeitenden / Betriebsgröße

Verkehrsdienstleister	Düsseldorf	15.01.2024	810
Gesundheitswesen	Essen	16.02.2024	11-50
Schneid- und Wickeltechnik	Wiehl	24.02.2024	650
Heizungs- und Klimatechnikbetrieb	Köln	12.03.2024	930
IT-Unternehmen	Bonn	14.03.2024	50-200
Planungsunternehmen	Krefeld	01.04.2024	60
Schuhhandelsunternehmen	Wuppertal	01.04.2024	2.000
Wohlfahrtsverband	Herten	01.04.2024	3.000
Schließsysteme	Halver	02.04.2024	700
Beratung und Planung von Krankenhäusern	Krefeld	18.04.2024	60
Süßwarenhersteller	Aachen	01.05.2024	4.000
Elektronikhersteller	Rheinbach	06.05.2024	250
Floristik	Kevelaer	07.05.2024	30-50

Branche / Tätigkeitsbereich

Kunststoffunternehmen	Köln	09.05.2024	189
Landmaschinenhersteller	Alpen	11.05.2024	1.773
Sicherheitsdienstleister	Köln	13.05.2024	4.000
Verbindungstechnik	Münster	17.05.2024	201-500
Transportunternehmen	Remscheid	04.06.2024	10-20
Stahlunternehmen	Plettenberg	09.06.2024	300
Automobilzulieferer	Rheda-Wiedenbrück	24.06.2024	4.200
Autohaus	Viersen	27.06.2024	2-10
Prüfdienstleister	Köln	01.07.2024	20.870
Bauunternehmen	Siegen	10.07.2024	350
Antriebsriemenhersteller	Höxter	25.08.2024	2.300
Industrieservice	Dormagen	26.08.2024	18.000
Elektrohandel	Kempen	29.08.2024	180

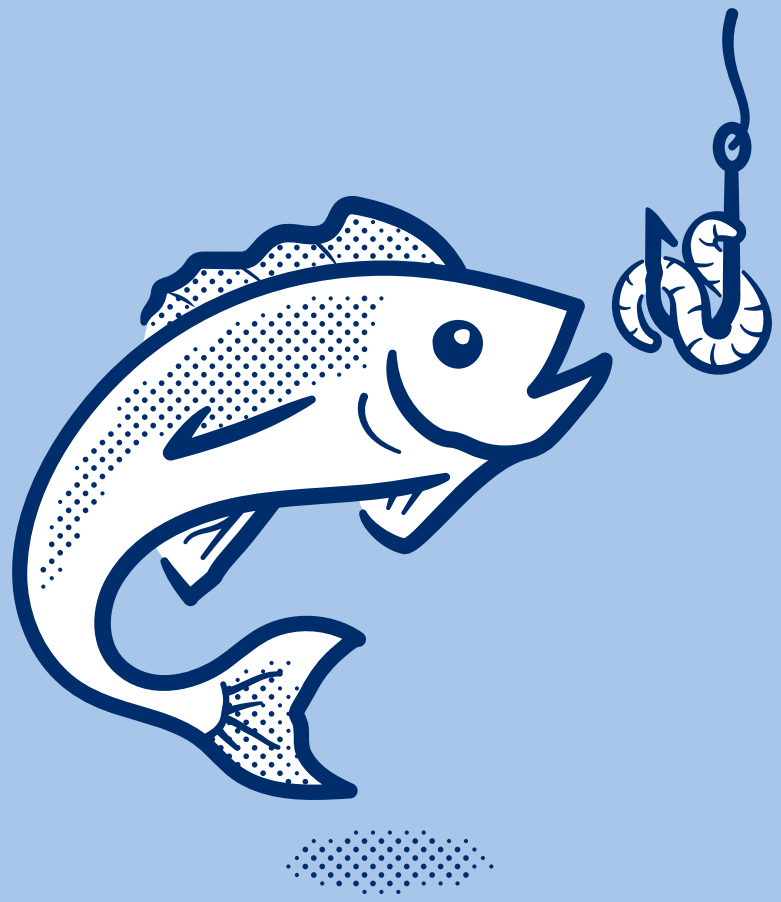
ZEIT FÜR DIGITALE SELBSTVERTEIDIGUNG

AUS DER PRAXIS HEUTE FÜR SIE ZUM MITNEHMEN

DIGITAL SICHER NRW
Kompetenzzentrum für Cybersicherheit in der Wirtschaft

E-Mail-Sicherheit

- **90%** aller erfolgreichen Angriffe beginnen mit einer E-Mail.
- Misstrauen Sie jeder E-Mail!
- Verstecken von schadhaften Inhalten ist leicht, alles ist super automatisierbar.
- Ergaunern sensibler Informationen für Angriffsvorbereitung.
- Wachsamkeit und technische Maßnahmen notwendig.

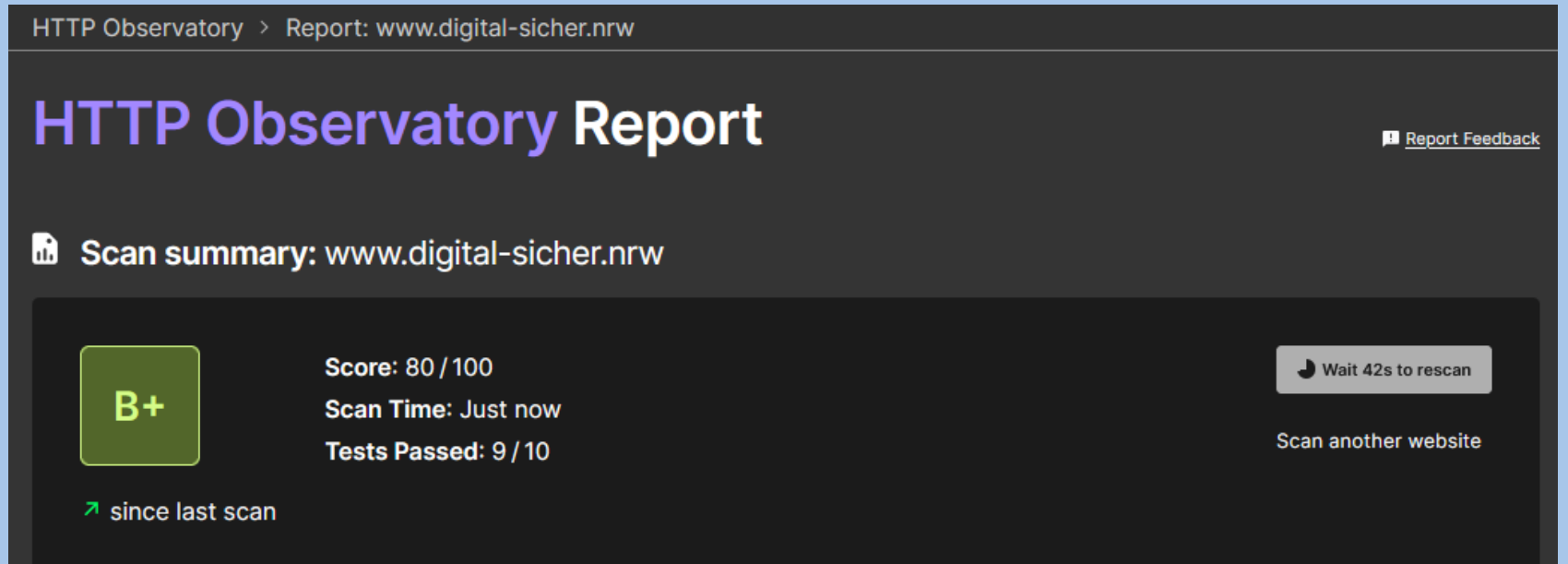


Basissicherheit herstellen

- Wartungsfreie Software existiert nicht: Updates – stets zeitnah.
- Datensicherungen sind lebensnotwendig, Wiederherstellungstests wichtig.
- Betrieb und Einsatz von IT bedeuten Verantwortung.
- Zugriffsrechte bewusst und richtig wählen.
- Mitarbeiter verlassen ein Unternehmen? Offboarding beachten!

Webseite oder Onlineshop absichern

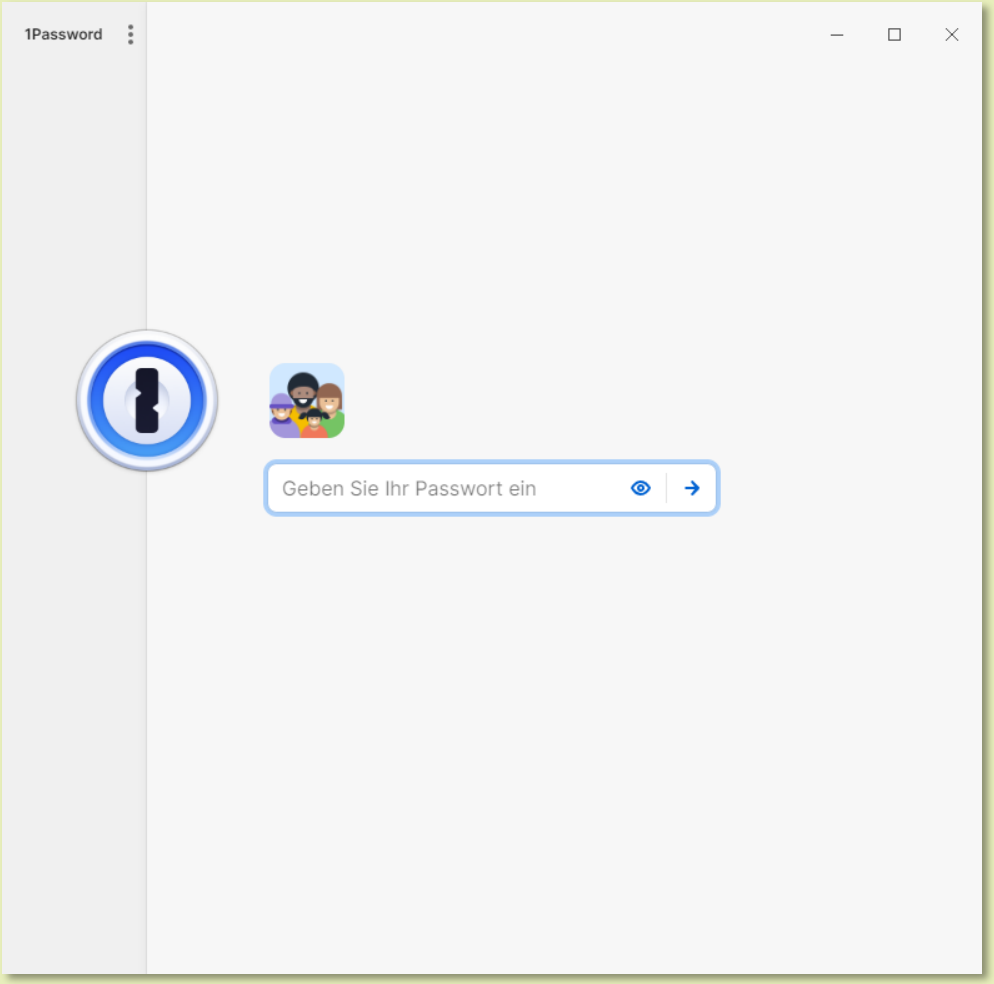
- Ihr Onlineauftritt ist weltweit erreichbar – mit allen Vor- und Nachteilen!
- Webseiten und Onlineshops bestehen aus „Software“
- Betreuung durch Dritte notwendig. Erfordert klare Vereinbarungen für korrekte Sicherheitseinstellungen, Wartung und Sicherheitsupdates.



Kostenfrei nutzbar unter:
https://developer.mozilla.org/de/observatory

Sichere Passwörter + 2FA

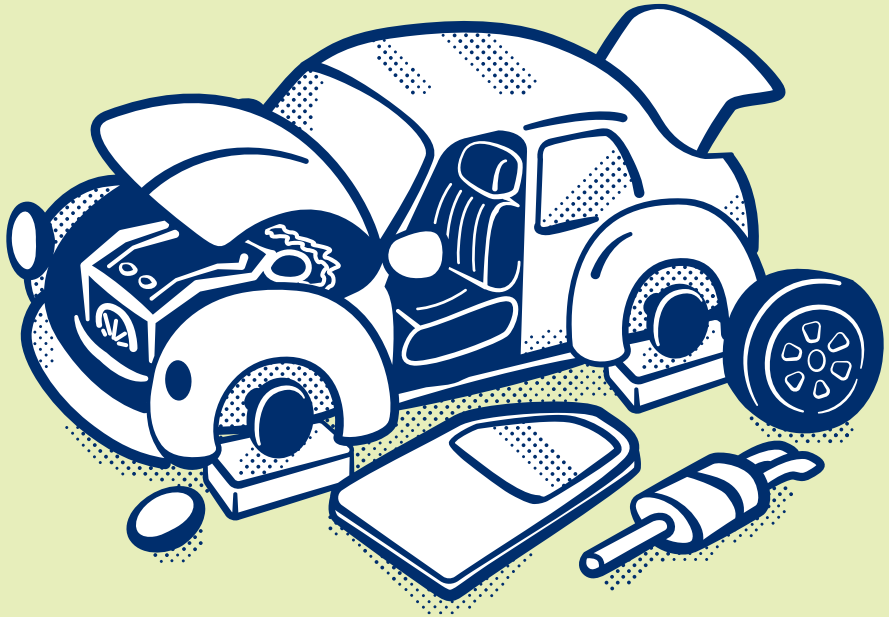
- Komplexität und Länge sind Ihre Freunde.
- Einzigartigkeit ist nicht nur eine großartige Idee.
- Warum nicht alle Passwörter 50 Zeichen lang machen oder direkt Passkeys einsetzen?
- Ein zweiter Faktor mit automatischem Backup ist super.
- Setzen Sie auf Passwortmanager und behalten Sie den Überblick.

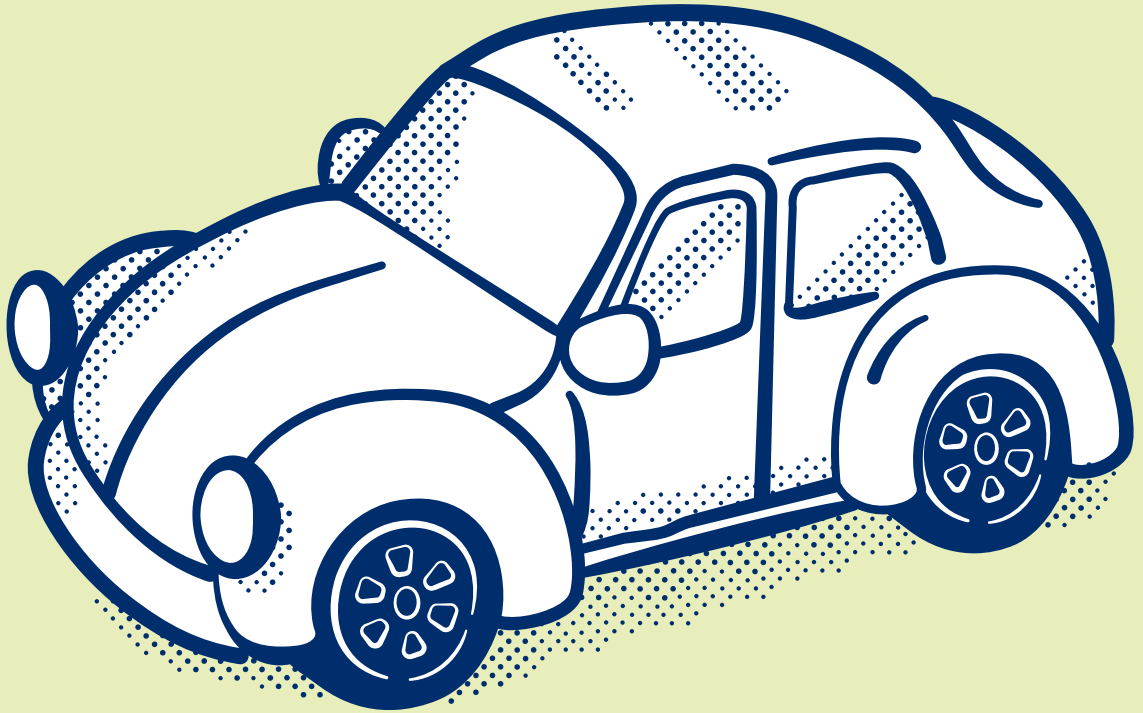


1Password Passwortmanager Login - Beispielbild, keine Empfehlung.

Digitale Dienste sichern

- Kartenlesegeräte / Bezahlsysteme sicher betreiben.
- Bankzugänge absichern.
- Google-Dienste absichern (Sicheres Passwort & 2FA).
- Instagram, Facebook & Co.: Vor Übernahmen schützen.
- Leakchecker-Dienste nutzen.





Leakchecker-TOOLTIP zum Nachlesen: https://www.digital-sicher.nrw/infomaterial/aktuelle-themen-und-ratgeber/tooltip-leak-checker

FRAGEN, DIE SIE SICH STELLEN SOLLTEN

Wie sieht meine IT-Infrastruktur aus?

Was habe ich alles in meinem Betrieb?

- Anzahl und Art der Geräte
- Geräte- und Maschinentypen
- Eingesetzte Software

Was benötige ich, um betriebsfähig zu bleiben?

Was sind meine Kronjuwelen und damit besonders schützenswert?

Wie sehen meine aktuellen Schutzmaßnahmen aus und wer ist dafür verantwortlich?

- Datensicherungen
- Updates von Geräten und Software
- Schnittstellen für Fernwartung?

Wenn Sie einen IT-Dienstleister haben:

- Was wird extern betreut?
- Was wird NICHT betreut?
- Wer ist mein Ansprechpartner?

CYBERSICHERHEIT IST CHEFINNEN- UND CHEFSACHE

WAS BEDEUTET DAS?

Sich der **Bedeutung** bewusst werden und **Verantwortung** für die Cybersicherheit der eigenen Organisation übernehmen.

ZIELE

Schäden vermeiden und **Risiken senken** für:

- Die eigene Organisation, Mitglieder, Partner und Mitarbeiter.

DAS WICHTIGSTE FÜR DEN EINSTIEG

- **Cybersicherheitsstrategie festlegen**
  Sollte die wichtigsten Risiken für das Unternehmen identifizieren und Maßnahmen festlegen.
- **Regelmäßige Sicherheitsaudits und –tests durchführen**
  Helfen dabei, Schwachstellen in den IT-Systemen und -Infrastruktur zu identifizieren und zu beheben.
- **Mitarbeiter & Führungskräfte schulen**
  Bewusstsein für die wichtigsten Bedrohungen und deren Konsequenzen schaffen.
- **Notfallplanung für den Ernstfall erstellen**
  Reaktion & Vorgehen im Fall eines Vorfalls planen, externe Hilfe klären, Verantwortlichkeiten festlegen und gewappnet sein.

Die Top 14 der wichtigsten Fragen an Ihr heutiges Ich ;)

Frage 1: Wer ist verantwortlich?

Frage 2: Wie gut kennen Sie Ihre IT-Systeme?

Frage 3: Führen Sie regelmäßig eine Datensicherung durch?

Frage 4: Spielen Sie regelmäßig Updates ein?

Frage 5: Verwenden Sie Virenschutzprogramme?

Frage 6: Haben Sie eine Firewall eingerichtet?

Frage 7: Haben Sie Makros deaktiviert?

Frage 8: Haben Sie Regelungen für sichere Passwörter getroffen?

Frage 9: Wie sichern Sie Ihre Mailaccounts ab?

Frage 10: Wie trennen Sie unterschiedliche IT-Bereiche?

Frage 11: Haben Sie IT-Risiken im Homeoffice und bei Geschäftsreisen im Griff?

Frage 12: Wie informieren Sie sich? Wie sensibilisieren Sie Ihre Mitarbeiter?

Frage 13: Deckt Ihre Versicherungspolice auch Cyberrisiken ab?

Frage 14: Wissen Sie, wie Sie bei einem Cyberangriff reagieren müssen?

Zusatzfrage: Haben Sie schon den CyberRisikoCheck gemacht?

TÜR ZU
IM NETZ

Direkt zur PDF-Datei:

TÜR ZU IM NETZ

Neue, 3. Auflage von Juli 2024

Weitere Informationen & Download:
https://www.digital-sicher.nrw/news/news-zum-thema-digitale-selbstverteidigung/neue-bsi-broschuere-fuer-kmu-zur-digitalen-sicherheit

Die neue Broschüre vom BSI zur Cybersicherheit für KMU

Bundesamt
für Sicherheit in der
Informationstechnik

DIGITAL SICHER NRW

Kompetenzzentrum für Cybersicherheit in der Wirtschaft

AUS BOCHUM & BONN FÜR GANZ NRW

kostenfrei & produktneutral

Beauftragt vom

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

PORTFOLIO: UNSERE ANGEBOTE

DIGITAL SICHER NRW

- Erstberatung
- IT-Sicherheitskompass
- Wissen
- Veranstaltungen
- Webinare
- Kooperationen

kostenfrei & produktneutral

www.digital-sicher.nrw

Newsletter,

Infos rund ums Thema digitale Sicherheit stellen wir Ihnen regelmäßig in unserem Newsletter zusammen.

Melden Sie sich an, um nichts mehr zu verpassen.

DIGITAL SICHER NRW

- **Ratgeber mit hilfreichen Tipps**
- **Aktuelle Veranstaltungen**
- **Neues aus unserem Kompetenzzentrum**

1 x Monatlich

DIGITALE SICHERHEIT

ANPACKEN

Im Fokus steht nicht das WAS, sondern das WIE.

#umsetzungstag

26. Juni 2025 | 9:00 - 13:45 Uhr

Jetzt anmelden:

Packen Sie's an und lernen Sie in kostenfreien Online-Workshops, wie digitale Sicherheit ganz einfach klappt.

DIGITAL SICHER NRW

Kompetenzzentrum für Cybersicherheit in der Wirtschaft in NRW

DIGITAL.SICHER.NRW unterstützt die Wirtschaft in NRW bei der präventiven Cybersicherheit.
Ausnahmslos kostenfrei und anwenderorientiert.

Hilfreiches Wissen und aktuelles finden Sie unter www.digital-sicher.nrw

Adresse

Standort Bochum
Lise-Meitner-Allee 4
44801 Bochum

Standort Bonn
Rheinwerkallee 6
53227 Bonn

Kontakt

+49 234 - 5200 7334

info@digital-sicher.nrw

Social Media

DIGITAL SICHER NRW

CYBER SECURITY CLUSTER BONN

eurobits

Beauftragt durch

Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen