DIGITAL SICHER NRW

Kompetenzzentrum für Cybersicherheit in der Wirtschaft

Willkommen zum Spitzengespräch „Cybersicherheit in der Wirtschaft NRW“

Düsseldorf, 06.03.2024

Beauftragt vom

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

UNSERE GEMEINSAME HEUTIGE AGENDA

Gemeinsames Foto | Alle

Begrüßung | Ministerin Mona Neubaur

Stand der Initiative Wirtschaft.Digital.Sicher.NRW | Sebastian Barchnicki

Bericht zu den Cyberangriffen im Bergischen Städtedreick und Vorstellung des Vorhabens „Modellregion Bergisches Land“| Stephan Vogelskamp

Vorstellung des Vorhabens „NIS2-Beratung für KMU“| Christine Skropke

Gemeinsame Diskussion | Alle

Fazit und Ausblick | Ministerin Mona Neubaur

TÜR ZU
IM NETZ

BEGRÜßUNG

Mona Neubaur, Wirtschaftsministerin sowie stellvertretende Ministerpräsidentin des Landes Nordrhein-Westfalen

STAND DER DINGE BEI „WDS“

Update zum Stand unserer

INITIATIVE
WIRTSCHAFT.DIGITAL.SICHER
NORDRHEIN-WESTFALEN

ROADMAP Initiative "Wirtschaft.Digital.Sicher NRW"

2024 | 2025 - 2026 | Begonnen | In Vorbereitung | Nachfolgende

#1 Förderprogramm MID-Digitale Sicherheit

#2 ewa – eurobits women academy

#3 Digitale Sicherheit für Gründer:innen

#4 Durchführung einer landesweiten Sichtbarkeitskampagne „Tür zu im Netz!“

#5 Roadshow zur Digitalen Sicherheit - eine Initiative von DIGITAL.SICHER.NRW - auch in Ihrer Stadt, Gemeinde oder Region

#8 Erarbeitung eines Frameworks („Rahmenstruktur“) für ein „NRW Basispaket Digitale Sicherheit für KMU“

#6 CISO (Chief Information Security Officer) Netzwerk NRW

#9 Regionale Cybersicherheitsberatung, Regionale Anlaufstellen & Multiplikatoren-Schulung

#10 Informationsoffensive zur bevorstehenden NIS2-Richtlinie

#7 Erarbeitung und Bereitstellung kostenfreier Vorlagen für die Notfallplanung & Notfallkarten in Kleinst-/Kleinunternehmen

#12 Checkliste Digitale Sicherheit für Chefinnen und Chefs

#13 Risiko-Folgeabschätzung „Cyberangriff“ für KMU

#11 CYBERWEHR NRW

Bericht zu den Cyberangriffen im Bergischen Städtedreieck

Stephan Vogelskamp

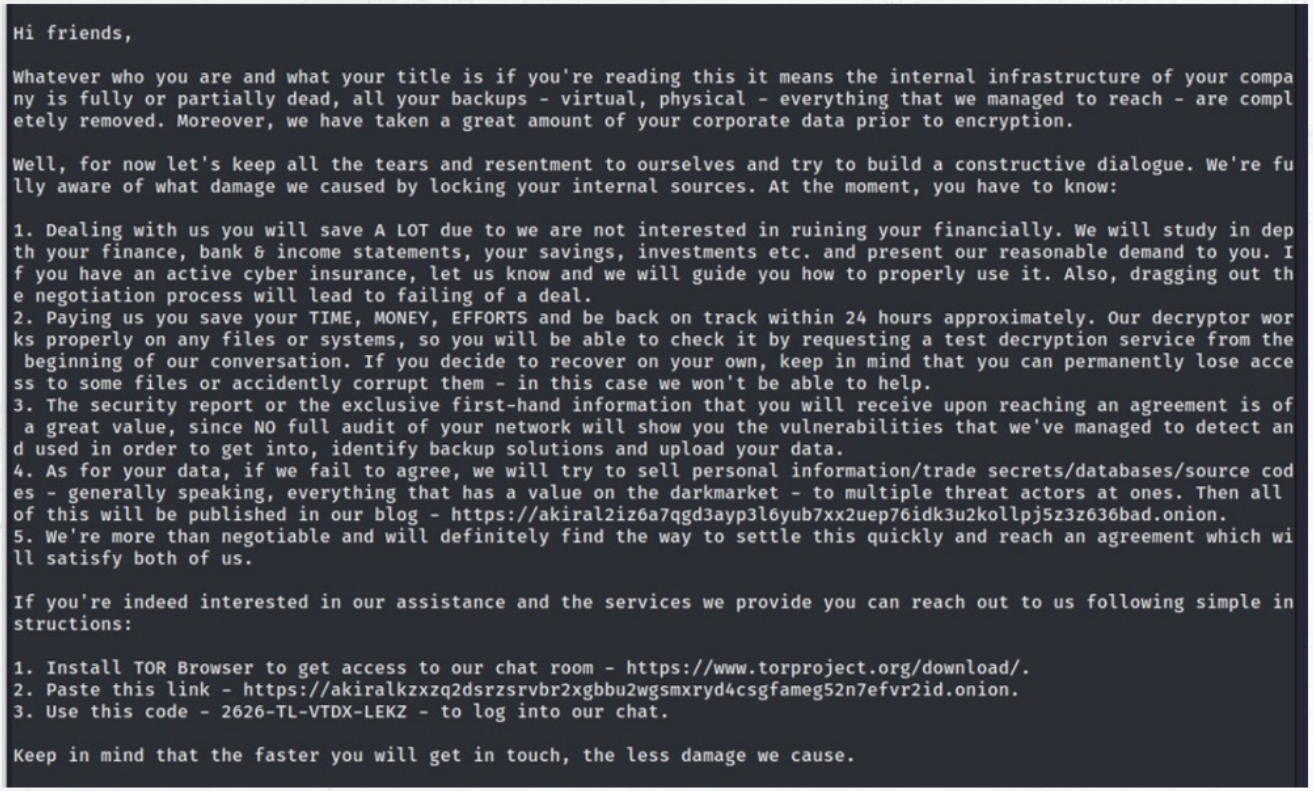
Kurzbericht zur Cyber-Attacke auf die Bergische Struktur- und Wirtschaftsförderungsgesellschaft mbH

BERGISCHE
STRUKTUR- UND
WIRTSCHAFTS-
FÖRDERUNGS-
GESELLSCHAFT

Stephan A. Vogelskamp

Was passierte am 22.12.2023?

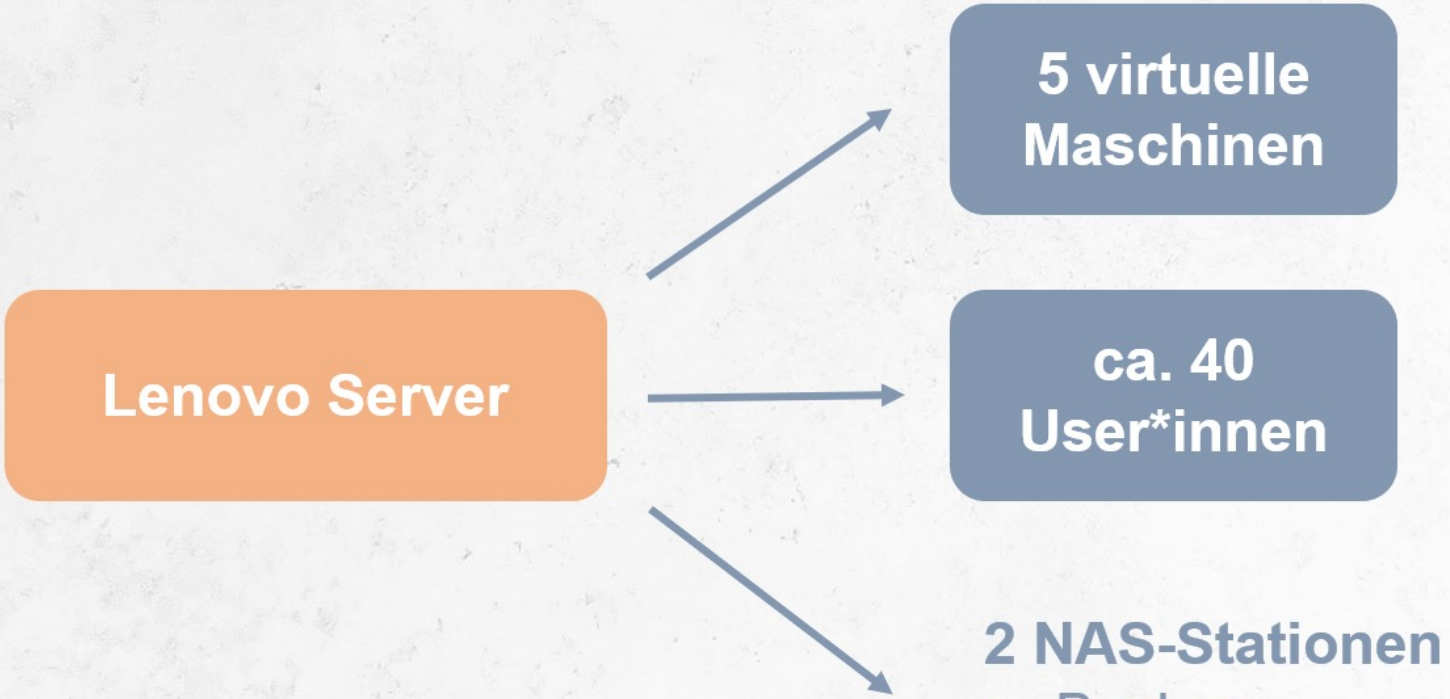
- Verschlüsselung aller Datenzugänge
- Erpresser-Schreiben auf dem Server



```
Hi friends,

Whatever who you are and what your title is if you're reading this it means the internal infrastructure of your compa
ny is fully or partially dead, all your backups - virtual, physical - everything that we managed to reach - are compl
etely removed. Moreover, we have taken a great amount of your corporate data prior to encryption.

Well, for now let's keep all the tears and resentment to ourselves and try to build a constructive dialogue. We're fu
lly aware of what damage we caused by locking your internal sources. At the moment, you have to know:

1. Dealing with us you will save A LOT due to we are not interested in ruining your financially. We will study in dep
th your finance, bank & income statements, your savings, investments etc. and present our reasonable demand to you. I
f you have an active cyber insurance, let us know and we will guide you how to properly use it. Also, dragging out th
e negotiation process will lead to failing of a deal.
2. Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24 hours approximately. Our decryptor wor
ks properly on any files or systems, so you will be able to check it by requesting a test decryption service from the
 beginning of our conversation. If you decide to recover on your own, keep in mind that you can permanently lose acce
ss to some files or accidently corrupt them - in this case we won't be able to help.
3. The security report or the exclusive first-hand information that you will receive upon reaching an agreement is of
 a great value, since NO full audit of your network will show you the vulnerabilities that we've managed to detect an
d used in order to get into, identify backup solutions and upload your data.
4. As for your data, if we fail to agree, we will try to sell personal information/trade secrets/databases/source cod
es - generally speaking, everything that has a value on the darkmarket - to multiple threat actors at ones. Then all
of this will be published in our blog - https://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion.
5. We're more than negotiable and will definitely find the way to settle this quickly and reach an agreement which wi
ll satisfy both of us.

If you're indeed interested in our assistance and the services we provide you can reach out to us following simple in
structions:

1. Install TOR Browser to get access to our chat room - https://www.torproject.org/download/.
2. Paste this link - https://akiralkzxzq2dsrzsrvbr2xgbbu2wgsmxryd4csgfameg52n7efvr2id.onion.
3. Use this code - 2626-TL-VTDX-LEKZ - to log into our chat.

Keep in mind that the faster you will get in touch, the less damage we cause.
```


[AKIRA]
AKIRA
Well, you are here. It means that you're suffering from cyber incident right now. Think of our actio
ns as an unscheduled forced audit of your network for vulnerabilities. Keep in mind that there is a
fair price to make it all go away.
Do not rush to assess what is happening - we did it to you. The best thing you can do is to follow o
ur instructions to get back to your daily routine, by cooperating with us you will minimize the dama
ge that might be done.
Those who choose different path will be shamed here publicly. The functionality of this blog is extr
emely simple - enter the desired command in the input line and enjoy the juiciest information that c
orporations around the world wanted to stay confidential.
Remember. You are unable to recover without our help. Your data is already gone and cannot be traced
to the place of final storage nor deleted by anyone besides us.
guest@akira:~$ help
List of all commands:
leaks — hacked companies
news — news about upcoming data releases
contact — send us a message and we will contact you
help — available commands
clear — clear screen
guest@akira:~$

Was wurde getroffen?



Was haben wir unternommen?

Tag 1

09:30	Vorfall
09:45	Anordnung: „Sofortiges Einfrieren!“
10:00	Telefonat LKA
10:15	Telefonate @yet & IT-Dienstleister
10:30	1. Information an die Gesellschafter
11:00	Austausch Datenschutzbeauftragter
12:00	Erste Videokonferenz @yet und IT-Dienstleister
12:30	Anordnung: „Bring in the devices!“
13:00	KriPo vor Ort / Anzeigenerstellung
15:00	Abstimmung KVA‘s
17:00	Abstimmung Prioritäten und Handlungsplan Forensik und IT-Dienstleister
19:00	2. Information an die Gesellschafter
21:00	Abstimmung und Meldung LDI

Was haben wir unternommen?

Tag 4 bis 34

- Forensik
- Aufsetzen der neuen IT-Struktur
- Wiederherstellung der Datenbestände
- Sukzessive Wieder-Inbetriebnahme der Arbeitsplätze gemäß Prioritätenliste
- Austausch mit Ermittlungsbehörde
- Kommunikation mit LDI
- Kommunikation mit gesamten Netzwerk

Ergebnisse der Forensik

- 3 Angriffswellen (Mai, Oktober, Dezember)
- Datenverlust: 18 GB
- Wahrscheinliche Ursache: Schwachstelle in der Cisco-ASA-Firewall
- Zugang: 4 kompromittierte User*innen (Brute-Force-Angriff)
- Keine geleakten Daten auffindbar
- Nach Rücksprache mit LDI kein melde- aber dokumentationspflichtiger Vorfall
- Einschätzung Ermittlungsbehörde: Wirtschaftskrieg

BERGISCHE
STRUKTUR- UND
WIRTSCHAFTS-
FÖRDERUNGS-
GESELLSCHAFT

Learnings

- Bergische Gesellschaft hatte kein aktives Sicherheitsleck in der Systemlandschaft
- 100%-Schutz gegen systemimmanente Schwachstellen einzelner Komponenten / Codes nicht möglich
- Hohe Reaktionsgeschwindigkeit hat schlimmere Schäden verhindert. Zentraler Moment: Tag 1
- Unternehmenskultur ist im Ernstfall entscheidend!
- Wissen über und Kontakt zu Ermittlungsbehörden, Forensikern und Landesbeauftragte für Datenschutz und Informationsfreiheit ist **existenziell**.
- Budgetierung von „Notfall-Plan“ muss vorhanden sein
- „Hardcopy“ von relevanten Adressverteilern notwendig!

Vorstellung des Vorhabens „Modellregion Bergisches Land“

Stephan Vogelskamp

Modellregion Cybersicherheit Bergisches Städtedreieck

Kurz-Portrait

BERGISCHE
STRUKTUR- UND
WIRTSCHAFTS-
FÖRDERUNGS-
GESELLSCHAFT

Stephan A. Vogelskamp

Zielsetzung

- Erprobung und Praxis-Evaluation des Maßnahmenpaketes der Initiative „Wirtschaft.Digital.Sicher NRW“
- Steigerung der Cybersicherheit und Resilienz in der Wirtschaft in Nordrhein-Westfalen
- Starker Fokus auf die Involvierung der innovationsstarken KMU-Landschaft

DIGITAL SICHER NRW

Modellregion

- Überschaubar
- Unternehmerregion: KMU / Hidden Champions
- Ausgeprägte Unternehmensnetzwerke

Besonders geeignet für eine „Blaupause“

BERGISCHE
STRUKTUR- UND
WIRTSCHAFTS-
FÖRDERUNGS-
GESELLSCHAFT

Regionale Akteure

- KMU‘s
- Start-Up Szene
- Konzernrepräsentanzen
- Bergische Universität und weitere Hochschulen
- Weitere Bildungsträger
- Verbände
- Großprojekte z.B. TRAIBER
- Lokale Wirtschaftsförderungen
- Ermittlungsbehörden
- Medienpartner

Involvierung relevanter Bezugsgruppen gewährleistet

Bausteine

Sensibilisierung / Aufklärung

Kampagnen / Vorträge / Roadshows

Transferstelle

NRW / Bundesweit / International

„Markt“-Beobachtung

Dienstleister / Produkte / „Attack“-Arten

Forschung

IT-Security / Partizipation

Verstetigung

Cyberabwehr / Trägerentwicklung

Förderberatung

MID

Qualifizierung

Alle Ebenen / Alle Bereiche

Coaching / Beratung

Vorträge / Workshops / Erfahrungsaustausch

Austausch-Plattform CISO

Tool-Entwicklung

Notfall-Pläne / Checklisten

BERGISCHE
STRUKTUR- UND
WIRTSCHAFTS-
FÖRDERUNGS-
GESELLSCHAFT

Vielen Dank für Ihre Aufmerksamkeit.

Vorstellung des Vorhabens „NIS2-Beratung für KMU“

Christine Skropke

eurobits

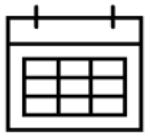
NIS2-Anlaufstelle NRW

6. März 2024

www.eurobits.de

Überblick: NIS2-Richtlinie

- Die Umsetzung der NIS2-Richtlinie der Europäischen Union erfolgt über das Bundesgesetz (NIS2UmsuCG).



- Die Umsetzungsfrist endet am 17. Oktober 2024.
  Das BMI rechnet mit einer Verspätung um mindestens zwei Monate.

- Die Richtlinie fordert von Unternehmen in kritischen Branchen, dass angemessene Risikomanagement-maßnahmen ergriffen und IT-Sicherheits-vorfälle gemeldet werden.

- Die Umsetzung betrifft in Deutschland über 30.000 Unternehmen sowie Zentral- und Regionalregierungen.
- In NRW werden mehrere tausend Unternehmen betroffen sein.

Wer ist betroffen? gem. NIS-2-Richtlinie (EU) 2022/2555

- Öffentliche und private Einrichtungen in 18 Sektoren mit mindestens 50 Beschäftigten oder mindestens 10 Mio. EUR Jahresumsatz und Jahresbilanz
  - Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, Digitale Infrastruktur, Verwaltung von IKT-Diensten (B2B), öffentliche Verwaltung, Weltraum (Annex I)
- Einige unabhängig von ihrer Größe (z.B. Teile der digitalen Infrastruktur und öffentlichen Verwaltung, alleinige Anbieter, KRITIS)
  - Post- und Kurierdienste; Abfallbewirtschaftung; Produktion, Herstellung und Handel mit chemischen Stoffen sowie mit Lebensmitteln; verarbeitendes Gewerbe / Herstellung von Waren; Anbieter digitaler Dienste; Forschung (Annex II)
- Nationale Gesetzgebung weicht z.T. von EU-Betreiber- und Sektor-Definitionen ab; z.B.: deutsches NIS2UmsuCG

Informationsoffensive zur NIS2-Richtlinie (basierende auf der Initiative Wirtschaft.Digital.Sicher.NRW)

Projekt: NIS2-Anlaufstelle Mittelstand NRW

Unser Ziel ist es, Unternehmen ohne bzw. mit unzureichendem Cybersicherheitsressourcen/-Kenntnissen einen Zugang zu NIS2-Beratung zu ermöglichen:

NIS2-Anlaufstelle in der eurobits Geschäftsstelle in Bochum

- NIS2-betroffene Unternehmen werden bei der Prüfung/Feststellung der NIS2-Relevanz unterstützt.
- Aufgrund der hohen Beratungsexpertise ist eurobits in der Lage, für jedes auch mittelständische Unternehmen in NRW, das sich zukünftig den Herausforderungen der NIS2-Umsetzung stellen muss, eine geeignete Erstberatung anzubieten.

NIS2-Erstberatung durch Projektpartner

- Daraus resultiert eine Empfehlung von Maßnahmen, die umgesetzt werden müssen um NIS2-compliant zu werden.
- Im Rahmen der Erstberatung wird über verfügbare Fördermittel für die Umsetzung der Maßnahmen informiert (bspw. MID).

Mehr Cybersicherheit für mehr NRW-Unternehmen

- Ziel ist es, dass KMUs in NRW mit kleinerer IT-Ausstattung (Personal + Budget) zukünftig nicht mehr auf eine kompetente Beratung verzichten müssen. Das Projektteam wird dazu moderne digitale Analysetools zum Einsatz bringen.

eurobits

Ansprechpartner:

Christine Skropke, Vorstandsvorsitzende
Alpha Barry, Vorstandsmitglied

kontakt@eurobits.de

www.eurobits.de

GEMEINSAME DISKUSSION

Wir freuen uns auf Ihre Meinung!

Schlusswort: FAZIT, AUSBLICK & „one more thing“

Mona Neubaur,
Wirtschaftsministerin sowie stellvertretende Ministerpräsidentin des Landes Nordrhein-Westfalen

TÜR ZU IM NETZ! EIGENE MOTIVE FÜR IHRE BRANCHE

Schön, wenn du

GESCHÄFTS-DATEN

nicht auf dem Silbertablett servierst.

Lass dich nicht erpressen.
Schütz dich vor Datenklau!

Digitale Sicherheit ist wichtig für jede Gastwirtin und jeden Gastwirt.
Auch du kannst etwas dafür tun, dass dein Gastronomie- oder Hotelbetrieb sicher bleibt.

Wir helfen dir dabei!

verbandsname.tuer-zu-im-netz.nrw

Eine Aktion von:

DIGITAL SICHER NRW | IHR LOGO | TÜR ZU IM NETZ

Schön, wenn die Rezeption für

HACKER

geschlossen bleibt.

Lass dich nicht erpressen.
Schütz dich vor Datenklau!

Digitale Sicherheit ist wichtig für jede Gastwirtin und jeden Gastwirt.
Auch du kannst etwas dafür tun, dass dein Gastronomie- oder Hotelbetrieb sicher bleibt.

Wir helfen dir dabei!

verbandsname.tuer-zu-im-netz.nrw

Eine Aktion von:

DIGITAL SICHER NRW | IHR LOGO | TÜR ZU IM NETZ

Schön, wenn

DIGITALE SICHERHEIT

zum Routineeingriff wird.

Lass dich nicht infizieren.
Schütz dich vor Cyberangriffen!

Digitale Sicherheit ist wichtig für jede medizinische Einrichtung. Auch du kannst etwas dafür tun, dass deine Praxis sicher bleibt.

Wir helfen dir dabei!

verbandsname.tuer-zu-im-netz.nrw

Eine Aktion von:

DIGITAL SICHER NRW | IHR LOGO | TÜR ZU IM NETZ

TÜR ZU IM NETZ! EIGENE MOTIVE FÜR IHRE BRANCHE

Schön, wenn

HACKER

draußen bleiben müssen.

Lass dich nicht beklauen. Schieb Cyberkriminellen einen Riegel vor!

Digitale Sicherheit ist wichtig für jede Einzelhändlerin und jeden Einzelhänder. Auch du kannst etwas dafür tun, dass dein Laden sicher bleibt.

Wir helfen dir dabei!

verbandsname.tuer-zu-im-netz.nrw

Eine Aktion von:

DIGITAL SICHER NRW | IHR LOGO | TÜR ZU IM NETZ

Schön, wenn

DATEN-DIEBE

von dir die Quittung bekommen.

Lass dich nicht beklauen. Schieb Cyberkriminellen einen Riegel vor!

Digitale Sicherheit ist wichtig für jede Einzelhändlerin und jeden Einzelhänder. Auch du kannst etwas dafür tun, dass dein Laden sicher bleibt.

Wir helfen dir dabei!

verbandsname.tuer-zu-im-netz.nrw

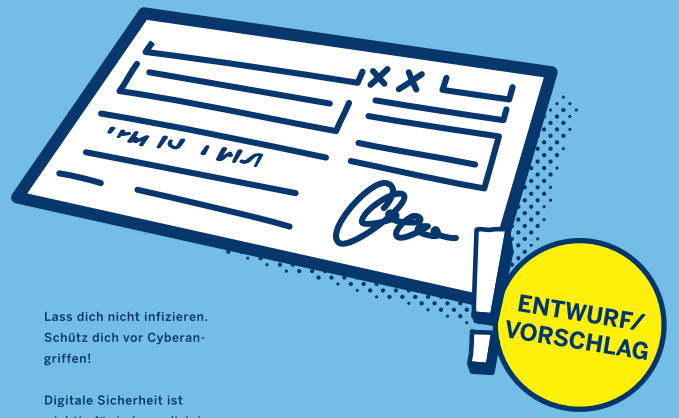
Eine Aktion von:

DIGITAL SICHER NRW | IHR LOGO | TÜR ZU IM NETZ

Schön, wenn du sichere

PASSWÖRTER

so routiniert wie Rezepte vergibst.



Lass dich nicht infizieren. Schütz dich vor Cyberangriffen!

Digitale Sicherheit ist wichtig für jede medizinische Einrichtung. Auch du kannst etwas dafür tun, dass deine Praxis sicher bleibt.

Wir helfen dir dabei!

verbandsname.tuer-zu-im-netz.nrw

Eine Aktion von:

DIGITAL SICHER NRW | IHR LOGO | TÜR ZU IM NETZ

TÜR ZU IM NETZ! EIGENE LANDING-PAGE FÜR IHRE BRANCHE

IHR-VERBAND.tuer-zu-im-netz.nrw

MACHEN WIR GEMEINSAM DIE „TÜR ZU IM NETZ“

Wir stehen gerne jederzeit für einen persönlichen Austausch mit Ihnen zur Verfügung. **Sprechen Sie uns an!**

Website: www.digital-sicher.nrw

Das Team hinter DIGITAL.SICHER.NRW:

Adresse

Standort Bochum
Lise-Meitner-Allee 4
44801 Bochum

Standort Bonn
Rheinwerkallee 6
53227 Bonn

Kontakt

+49 234 - 52007334

info@digital-sicher.nrw

CYBER SECURITY CLUSTER BONN

eurobits

Beauftragt durch

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