Rhein-Kreis Neuss

rhein kreis neuss

N I E D E R S C H R I F T

über die **8.** Sitzung

des Ausschusses für Innovation, Digitalisierung und Standortmarketing

(XVII. Wahlperiode)

Tag der Sitzung:	**04.05.2023**
Ort der Sitzung:	Neuss, ITK Rheinland, Hammfelddamm 4, 5. Etage
Beginn der Sitzung:	16:10 Uhr
Ende der Sitzung:	18:55 Uhr
Den Vorsitz führte:	Simon Kell

Sitzungsteilnehmer:

• CDU-Fraktion

1.	Herr Stefan Arcularius	
2.	Herr Lars Becker	
3.	Herr Jakob Beyen	bis 18.10 Uhr Vertretung für Frau Dilek Haupt
4.	Herr Karl Josef Flüchten	Vertretung für Herrn Norbert Gand
5.	Herr Thomas Kaumanns	Vertretung für Herrn Prof. Dr. Jan-Philipp Büchler
6.	Herr Dominique Ling Lindow	bis 18.40 Uhr

• SPD-Fraktion

7.	Frau Christina Borggräfe	
8.	Herr Justin Kluth	
9.	Herr Leif Eric Lüpertz	
10.	Herr Johannes Strauch	bis 17.20 Uhr Vertretung für Herrn Stefan Schmitz
11.	Herr Ronald Maximilian Voigt	

• Fraktion Bündnis 90/Die Grünen

12.	Frau Ute Leiermann	Vertretung für Herrn Erhard Demmer
13.	Herr Joachim Quass	
14.	Herr Dirk Schimanski	
15.	Frau Jocy Wolff	

• FDP-Fraktion

16.	Herr Simon Kell	

17. Herr Tim Tressel

- **Fraktion UWG-Freie Wählergemeinschaft Rhein-Kreis Neuss/ Deutsche Zentrumspartei**

18. Herr Wolfgang Krause — Vertretung für Herrn Markus Christopher Roß-deutscher

- **AfD-Fraktion**

19. Herr Marko Wiens

- **Die Kreistagsgruppe**

20. Herr Dirk Günter Karl Müller — Vertretung für Herrn Philip Strauss

- **Gäste**

21. Frau Monika Zimmermann
22. Herr Volker Ruff (matrix GmbH) — ab 17.20 Uhr
23. Herr Christian Schoon (Prognos AG) — ab 17.20 Uhr

- **Verwaltung**

24. Frau Hildegard Fuhrmann — ab 17.20 Uhr
25. Herr Frank Meger
26. Herr Dezernent Martin Stiller — von 17.20 Uhr bis 18.45 Uhr
27. Herr Dezernent Harald Vieten
28. Herr Horst Weiner

- **Schriftführerin**

29. Frau Gerlinde Müller
30. Frau Anne Schmitz

I N H A L T S V E R Z E I C H N I S

Öffentlicher Teil:

1. Feststellung der ordnungsgemäß erfolgten Einladung und der Beschlussfähigkeit

Protokoll:

Vorsitzender Simon Kell begrüßte zunächst die Anwesenden und bedankte sich bei den Gastgebern der ITK Rheinland für die Einladung des Ausschusseses für Innovation, Digitalisierung und Standortmarketing in die Räume der ITK Rheinland.

Wolfgang Vits, Geschäftsführer der ITK Rheinland, begrüßte ebenfalls die Anwesenden und stellte die Arbeit ITK Rheinland als kommunaler IT-Dienstleister im Verbandsgebiet vor **(Anlage 1)**. Herr Vits hob die Bedeutung der IT-Sicherheit hervor und stellte dazu Herrn André Thißen vor, der für den Bereich der IT-Sicherheit in der ITK zuständig ist. Herr Thißen ging anschließend in seinem Vortrag auf die aktuell massiv gestiegene Bedrohungslage durch Cyber-Angriffe ein und stellte die wachsende Bedeutung der IT-Sicherheit heraus. So habe es in Deutschland erstmals die Ausrufung eine Katastrophenfalls für einen Kreis nach einem erfolgreichen Cyber-Angriffs gegeben.

Beide Herren beantworteten die Fragen - vor allen Dingen zur IT-Sicherheit - von Leif Lüpertz, Lars Becker und Tim Tressel. Da das umfangreiche Thema IT-Sicherheit und die Zusammenarbeit von ITK Rheinland und Rhein-Kreis Neuss auch im Tagesordnungspunkt 3 zur Sitzung behandelt wurde, schlug Vorsitzender Simon Kell vor, die Diskussion nach dem Vortrag von IT-Sicherheitsbeauftragten Frank Meger fortzuführen.

Es folgte eine Besichtigung des Rechenzentrums der ITK Rheinland.

Im Anschluss an den Rundgang ging Vorsitzender Simon Kell zur Tagesordnung über und stellte die ordnungsgemäß erfolgte Einladung zur Sitzung und Beschlussfähigkeit fest. Hiergegen erhoben sich keine Einwände.

2. Verpflichtung von sachkundigen Bürgerinnen und Bürgern Vorlage: VI/2617/XVII/2023

Protokoll:

Gemäß § 41 Abs. 5 der Kreisordnung Nordrhein-Westfalen (KrO NRW) i.V.m. § 8 Abs. 4 der Hauptsatzung des Rhein-Kreises Neuss können zu Mitgliedern der Ausschüsse neben Kreistagsmitgliedern auch sachkundige Bürgerinnen und Bürger aus den kreisangehörigen Gemeinden bestellt werden. Diese sind vom Ausschussvorsitzenden zu verpflichten.

Die Verpflichtungsformel lautet:
„Ich verpflichte mich, dass ich meine Aufgaben nach bestem Wissen und Können wahrnehmen, das Grundgesetz, die Verfassung des Landes und die Gesetze beachten und meine Pflichten zum Wohle des Kreises erfüllen werde. (So wahr mir Gott helfe.)."

Die sachkundigen Bürger Thomas Kaumanns (CDU), Wolfgang Krause (UWG-FW/Zentrum), Dirk Müller (Die Kreistagsgruppe) und Marco Wiens (AfD) wurden in der Sitzung verpflichtet.

3. IT-Sicherheitsbericht Vorlage: VI/2608/XVII/2023

Protokoll:

Der vierte Jahresbericht des IT-Dezernates zur IT-Sicherheit **(Anlage 2)** lag dem Ausschuss vor.

IT-Sicherheitsbeauftragter Frank Meger stellte anhand einer Präsentation **(Anlage 3**) wichtige Eckpunkte des IT-Sicherheitsberichts 2022 vor. Der Umfang der Sicherheitsaufgaben wachse stetig. Zum Tagesgeschäft gehöre zunehmend potentielle Schwachstellen für Cyber-Angriffe frühzeitig zu lokalisieren und abzustellen, sowie die Beschäftigten der Kreisverwaltung zu schulen und zu sensibilisieren. Meger wies auf die wachsende Zahl von Kommunen hin, die bereits Opfer von Cyberangriffen geworden seien - zum Teil mit gravierenden Auswirkungen. Cyber-Bedrohungen abzuwehren, nehme daher immer mehr Ressourcen in Anspruch.

Dezernent Harald Vieten ergänzte, dass das Thema IT-Sicherheit im beschlossenen Masterplan wegen der hohen Priorität mit einem eigenen Handlungsfeld belegt sei und aus diesem Grunde Frank Meger bereits seit 2019 als Sicherheitsbeauftragter der Kreisverwaltung bestellt sei. Das im vergangenen Jahr bereit gestellte Budget für IT-Sicherheit wurde gut angelegt – IT-Sicherheit verlange auf Grund der wachsenden Bedrohungsszenarien in einer zunehmend digitalen Welt leider auch zunehmend mehr Investitionen und Personalressourcen. Dank des engagierten Einsatzes von Herrn Meger sei es Anfang diesen Jahres möglich geworden, eine Cyberversicherung für die Kreisverwaltung abzuschließen. Um überhaupt versicherungsfähig zu werden, musste dafür viele Hürden genommen und monatelange Arbeit investiert werden.

Dezernent Martin Stiller unterstrich ebenfalls die Wichtigkeit der IT-Sicherheit aus dem Blickwinkel des Katastrophenschutzes, der kritischen Infrastrukturen und der zivilen Verteidigung.

Abgeordneter Stefan Arcularius bat um Informationen, ob es ein Notfallhandbuch zur IT-Sicherheit gebe und ob ausreichend personelle Kapazitäten bei der Kreisverwaltung im Bereich IT-Sicherheit bestehe. IT-Ausfälle könne man sich seiner Meinung nach nicht leisten und müssten definitiv vermieden werden. Frank Meger antwortete, dass IT-Notfallpläne im Rahmen der Energiekrise erstellt wurden, es definitiv aber noch Potential nach oben gebe. Ein Informationssicherheitsmanagementkonzept sei im Aufbau, es fehle aber an der Zeit.

Dezernent Harald Vieten ergänzte, Frank Meger sei vorrangig Abteilungsleiter Zentrale Dienste und zusätzlich IT-Sicherheitsbeauftragter. Der Anteil der Aufgaben zur IT-Sicherheit nehme aber kontinuierlich zu und liege jetzt schon bei 75 Prozent der Arbeitszeit von Herrn Meger.

Auf die Frage von Abgeordnetem Tim Tressel, wieso so wenig Personal bei der Kreisverwaltung für IT-Sicherheit zur Verfügung stehe, antwortete Dezernent Harald Vieten, dass eine zeitliche Ausweitung derzeit mit der Behördenleitung diskutiert werde.

Abgeordneter Joachim Quass stellte fest, dass die personelle Situation bei rd. 1.300 Mitarbeitern für den Bereich IT-Sicherheit bei der Kreisverwaltung erschreckend sei.

Die Fragen von Ute Leiermann, Dirk Müller und Justin Kluth zu Personalstärke bei der IT-Sicherheit beim Kreis und bei der ITK, Awareness-Trainings und Zertifizierung von IT-Prozessen beantworte Frank Meger. Wolfgang Vits fügte an, dass bei der ITK Rheinland aktuell bereits 5 Stellen für die IT-Sicherheit vorgesehen sind.

Auf die Frage von Christina Borggräfe, ob es eine Berechnungsgrundlage für IT-Sicherheitsbeauftragte einer Kreisverwaltung gebe, antwortete Dezernent Vieten, dass lt. eines direkt an die Landrätinnen und Landräte gerichteten Handlungsleitfaden des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und des Deutschen Landkreistages (DLT) in einem Kreis regelmäßig eine Person in Vollzeit als IT-Sicherheitsbeauftrager (CISO) empfohlen werde.

Weitere Wortmeldungen lagen nicht vor.

Beschluss:

Der Ausschuss für Innovation, Digitalisierung und Standortmarketing nimmt den Jahresbericht IT-Sicherheit 2022 des IT-Dezernats zur Kenntnis.

4. Wirtschafts- und Beschäftigungsförderung (März – April 2023) Vorlage: ZS5/2649/XVII/2023

Protokoll:

Es lagen keine Wortmeldungen vor.

Beschluss:

Der Ausschuss für Innovation, Digitalisierung und Standortmarketing nimmt den Bericht zur Wirtschafts- und Beschäftigungsförderung (März - April 2023) zur Kenntnis.

5. Sachstandsbericht zum Wirtschaftsförderungskonzept Vorlage: ZS5/2648/XVII/2023

Protokoll:

Dezernent Martin Stiller führte zunächst aus, dass für das 2022 beschlossene und beauftragte neue Wirtschaftsförderungskonzept derzeit in Erfahrung gebracht werde, wie insbesondere die Bedürfnisse der lokalen Unternehmen/Wirtschaft sind und wie eine Kooperation der Wirtschaftssförderung des Kreises mit anderen Akteuren, wie z.B. IHK, kommunale Wirtschaftsförderer usw. erfolgen könne.

Er stellte die Herren Volker Ruff (matrix GmbH) und Christian Schoon (Prognos AG) vor. Die Herren stellten als Zwischenbilanz erste Ergebnisse der durchgeführten Interviews und Umfragen mit verschiedenen Stakeholder und Akteuren im Rahmen einer Präsentation vor **(Anlage 4)**.

Sie unterstrichen, dass der der Rhein-Kreis Neuss ein vielseitiger und starker Wirtschaftsstandort sei. Dem Ausschuss wurden die nächsten Schritte und der Zeitplan bis zur Fertigstellung des Konzeptes erläutert.
An der anschließenden Diskussion beteiligten sich Christina Borggräfe, Joachim Quass, Wolfgang Krause und Ute Leiermann.

Beschluss:

Der Ausschuss für Innovation, Digitalisierung und Standortmarketing nimmt den Bericht zur Kenntnis.

6. Mitteilungen

Protokoll:

Es lagen keine Mitteilungen vor.

7. Anträge

Protokoll:

Es lagen keine Anträge vor.

8. Anfragen

Protokoll:

Vorsitzender Simon Kell bat die Verwaltung vor dem Hintergrund der Fachkräftebindung um einen Sachstand zur Personalfluktuation in den vergangenen Jahren für die Fachbereiche, die hier im Ausschuss vertreten sind. Er bat die Aufstellung dem Protokoll beizufügen. Dezernent Vieten erkundigte sich, ob die Bereiche IT und Wirtschaftsförderung gemeint seien. Herr Kell bestätigte dies.

Dezernent Vieten sagte dies für die Verwaltung zu.

Weitere Anfragen lagen nicht vor.

Anmerkung der Verwaltung:

*Aufgrund von Urlaub der Amtsleitung Wirtschaftsförderung und des zuständigen Dezernenten Stiller wird die Aufstellung für den Bereich der Wirtschaftsförderung später nachgesendet. Eine Tabelle für die IT liegt als **Anlage 5** bei.*

9. Bericht der Verwaltung/ Beschlusskontrolle

Protokoll:

Es lagen keine Beschlüsse zur Kontrolle vor.

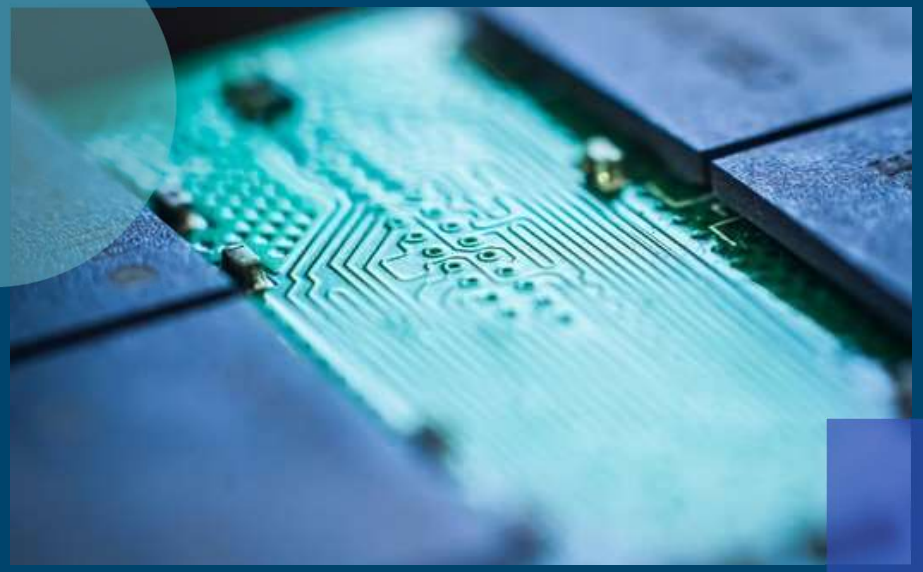
Da keine weiteren Wortmeldungen vorlagen, schloss Simon Kell um 18:55 Uhr die Sitzung.

Simon Kell
Vorsitz

Anne Schmitz
Schriftführung

ITK RHEINLAND
IT für Kommunen

ITK Rheinland Partner der Digitalisierung



Wolfgang Vits
André Thißen

04.05.2023, Neuss

Agenda

Die ITK Rheinland – Ihr kommunaler IT-Dienstleister

IT Sicherheit

Rechenzentrum

Einer der größten kommunalen IT-Dienstleister NRWs

12 Kommunale Mitglieder

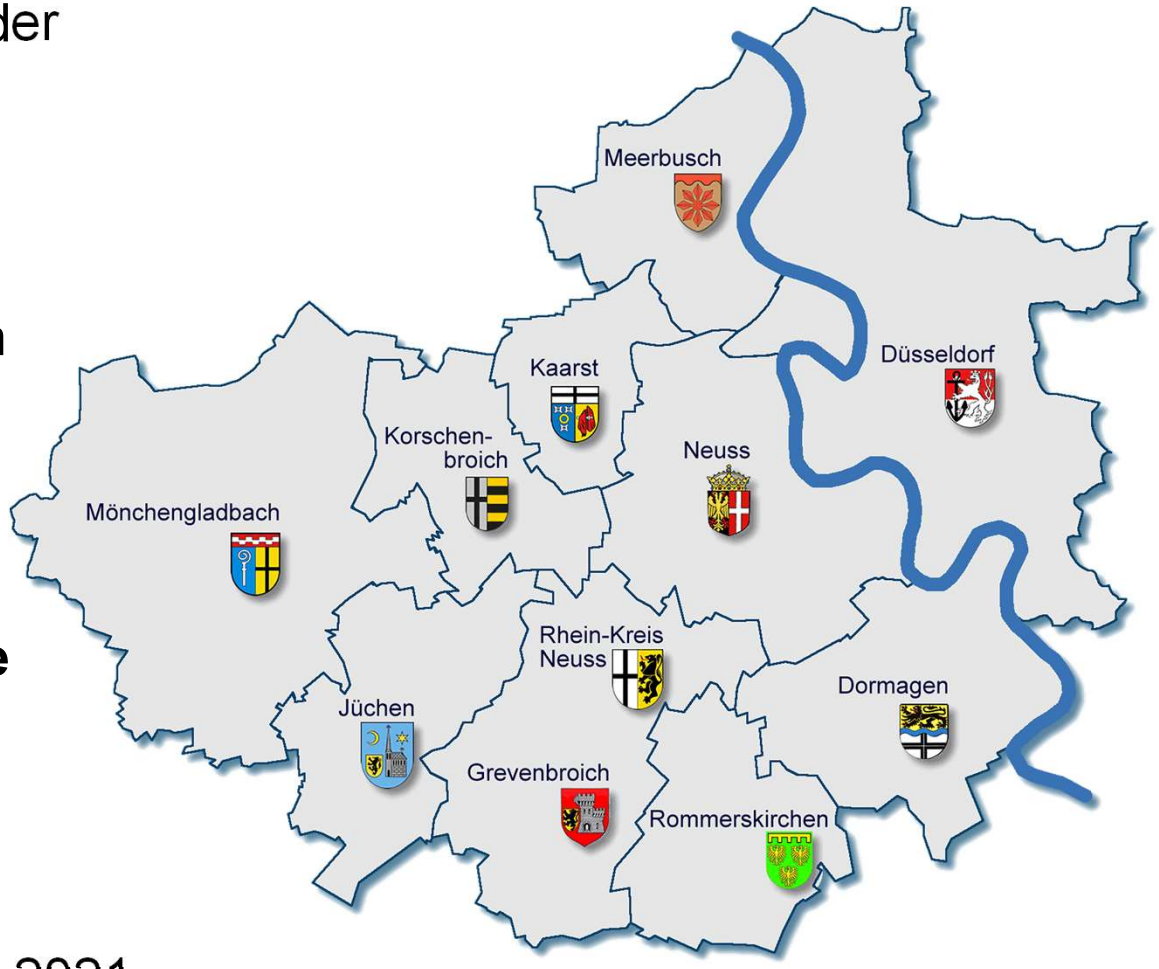
Datenverarbeitung für
1,4 Mio Menschen

15.000 AnwenderInnen

Bereitstellung und
Integration von
kommunaler
Anwendungssoftware
und Verfahren (>500)

320 MitarbeiterInnen

61 Mio EUR Umsatz in 2021



Die Historie

25 Jahre Kommunaler IT-Dienstleister

1998 Gründung Kommunaler Zweckverband

2008 Fusion mit IT-Abteilung der
Stadt Düsseldorf zur ITK Rheinland

2016 Fusion mit IT-Abteilung der
Stadt Mönchengladbach

2019 Beitritt Zweckverband LandFolge Garzweiler

Strukturen im Zweckverband

ORGANE

ARBEITSKREISE

Verbandsversammlung

Verwaltungsrat

Verbandsvorsteher

Geschäftsführer

Rechnungsprüfungsamt
(Kontrollorgan)

Arbeitskreis
Koordinierung

IT-strategische
Aufgaben

Fachliche
Aufgaben

AK IT-Infrastruktur

AK Anwendungen

Unsere Strategie

- ✓ Digitalisierung der Verwaltung ist Kern unserer Strategie
- ✓ Regionaler Verbund zur Sicherung der Zukunftsfähigkeit der Mitgliedskommunen
- ✓ Umfängliche Verantwortlichkeit der ITK Rheinland für die zentrale Produktion (u.a. Vernetzung, Integrität, Stabilität)
- ✓ ITK der 2 Geschwindigkeiten: Bestimmte Prozesse, Produkte sind nicht für alle Verbandsmitglieder gleichermaßen interessant (inhaltlich und/oder zeitlich)
- ✓ Verbandsmitglieder haben in Bezug auf die Erbringung von Leistungen und Kostenvorteilen Vorrang bei der Wachstumsstrategie

Unser Selbstverständnis

- ✓ Ein Großteil unserer Mitarbeitenden war lange Zeit bei den Kommunalverwaltungen im Verbandsgebiet tätig: Bei der **OZG**-Umsetzung sind wir mit **Verwaltungsabläufen** bestens vertraut
- ✓ Wir stellen sichere **IT-Infrastrukturen** bereit
- ✓ Wir sichern die **Verfügbarkeit** von Fachanwendungen
- ✓ Wir setzen auf **Open Source** – „wo es Sinn macht“
- ✓ Wir stärken die **digitale Souveränität** unserer Verbandsmitglieder
- ✓ Wir folgen unserer hauseigenen **Green IT Leitlinie**

Unser Selbstverständnis

Nachhaltig die Zukunft gestalten

- ✓ Zukunftssicherung durch Nachwuchsförderung
- ✓ den demographischen Wandel bewältigen

Zukunftsfähigkeit durch gute Ausbildung
die aktuellen Ausbildungsberufe der ITK:

- Fachinformatiker/-in Fachrichtung Systemintegration
- Fachinformatiker/-in Fachrichtungen Anwendungsentwicklung
- Kauffrau / Kaufmann für IT-Systemmanagement

Unsere Dienstleistungen

Bereitstellung und Betrieb von IuK-Infrastruktur:

- Betrieb Rechenzentrum
- Netzwerk
- Sicherheitssysteme
- Server
- mobile Geräte
- Microsoft-Infrastruktur
- ITK – Cloud

Anwendungsmanagement:

- > 500 kommunale Fachverfahren

Kundenservice:

- ServiceDesk
- Client-Infrastruktur
- Beratung, Vor-Ort-Service (inkl. Schul-IT), Support
- IT-Projektarbeit

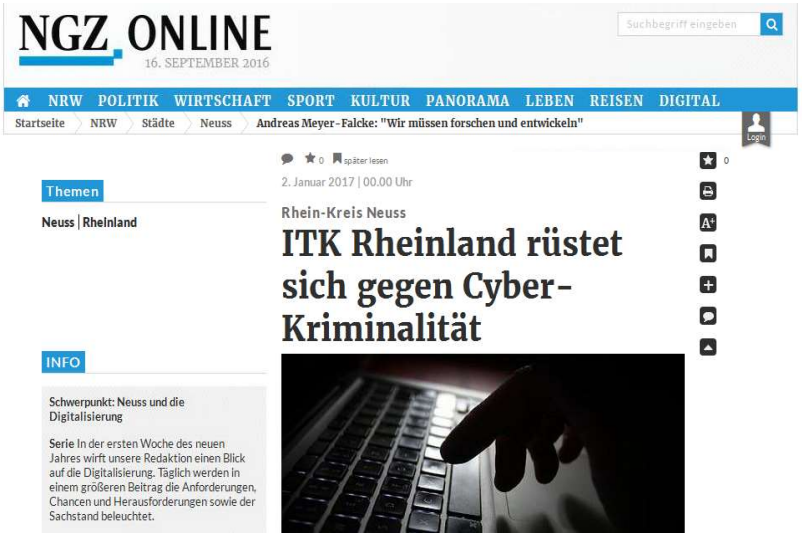
Rechenzentrum und Anwendungsmanagement zertifiziert nach Norm DIN ISO / IEC 27001 DIN ISO / IEC 27701

Qualitätsmanagement zertifiziert nach Norm DIN EN ISO 9001:2015

IT Sicherheit bei der ITK

IT Sicherheit

… wird bei uns groß geschrieben



NGZ ONLINE
16. SEPTEMBER 2016

Suchbegriff eingeben

NRW POLITIK WIRTSCHAFT SPORT KULTUR PANORAMA LEBEN REISEN DIGITAL

Startseite › NRW › Städte › Neuss › Andreas Meyer-Falcke: "Wir müssen forschen und entwickeln"

Login

später lesen

Themen

Neuss | Rheinland

2. Januar 2017 | 00.00 Uhr

Rhein-Kreis Neuss

ITK Rheinland rüstet sich gegen Cyber-Kriminalität

INFO

Schwerpunkt: Neuss und die Digitalisierung

Serie In der ersten Woche des neuen Jahres wirft unsere Redaktion einen Blick auf die Digitalisierung. Täglich werden in einem größeren Beitrag die Anforderungen, Chancen und Herausforderungen sowie der Sachstand beleuchtet.

Allianz für Cyber-Sicherheit

Zertifizierungen:
ISMS = **DIN EN ISO/IEC 27001**
QMS = **DIN EN ISO 9001**
Konformität:
DSMS = **DIN EN ISO/IEC 27701**

IT Sicherheit

BSI – Lagebericht 2022

Die Lage der IT-Sicherheit in Deutschland 2022 - Titelbild
Quelle: BSI

IT Sicherheit

Lagebericht BSI

Quelle BSI

IT Sicherheit

BSI – Lagebericht 2022

Kurzes Fazit aus dem Lagebericht:

Angriffskrieg auf die Ukraine verschärft die Cyber-Sicherheitslage in Deutschland

- Beeinträchtigung der satellitengestützten Kommunikation zur Fernwartung von Windenergieanlagen
- Betreiber Kritischer Infrastrukturen waren Angriffsziele von Hacktivisten
- DDoS-Angriffe (Überlastangriffe) bedrohen weiterhin die Informationssicherheit

Bedrohung durch Cyber-Erpressung steigt weiter

- Dass nicht nur umsatzstarke Unternehmen Ziel von Ransomware-Angriffen werden können, zeigen die Auswirkungen in mehreren betroffenen Kommunen, in denen die Verwaltungsprozesse teils über Monate massiv gestört waren – mit erheblichen Folgen für die Bürgerinnen und Bürger

IT Sicherheit

BSI – Lagebericht 2022

Kurzes Fazit aus dem Lagebericht:

Neue Dimension bei Schwachstellen

- Besonders kritische Schwachstellen traten in weitverbreiteten Produkten wie MS Exchange und Log4j auf, die teilweise von den Herstellern nur zögerlich geschlossen wurden
- Meldungen über Schwachstellen: In den 150 gängigsten Produkten stieg die Anzahl um rund zehn Prozent im Vergleich zum Vorjahr (6190 Meldungen)

Zeitenwende für Cyber-Sicherheit made in Germany

- Schon vor dem Digitalisierungsschub, den die Corona-Pandemie verstärkt hat, und vor der neuen Bedrohungslage in Folge des russischen Angriffskrieges auf die Ukraine, war Cyber-Sicherheit ein wesentlicher Erfolgsfaktor für eine zunehmend digital vernetzte Gesellschaft und Wirtschaft.
- Präventive IT-Sicherheit ist die wirkungsvollste Maßnahme

IT Sicherheit

Beispiel Cyberangriff auf Landkreis Anhalt-Bitterfeld 2021

- **02.06.2021** Tag der eigentlichen Infektion. An diesem Tag wurde ein Mitarbeiter-PC infiziert, der mehrere User-Profile hatte. (Erst durch Forensiker am 12.07.2021 festgestellt)
- **06.07.2021** Start der Verschlüsselung von Daten, erste Meldungen 6:45 Uhr, Lösegeldforderung in Höhe von 500.000 EUR
- **07.07.2021** rund 120 Rechner, Server, sowie Teile der Datensicherung sind betroffen, gesperrt und verschlüsselt worden.
- **09.07.2021** Landkreis Anhalt-Bitterfeld ruft den Katastrophenfall aus – Einsatz der Bundeswehr
- **16.07.2021** Einige Daten werden veröffentlicht
- **21.07.2021** Notinfrastruktur läuft. 80-90% konnten aus den Datensicherungen rekonstruiert werden.
- **März 2022** Nur 40 der 159 Fachanwendungen laufen wieder
- **Juli 2022** ein Jahr nach dem Vorfall, immer noch nicht ganz alles lauffähig

Quelle BSI

DDoS Angriffe / aktuelle Situation

WDR 07.03.2023

Düsseldorfer Rüstungskonzern Rheinmetall von Hackern angegriffen

Der Rüstungskonzern Rheinmetall aus Düsseldorf hat am Dienstag eine Cyberattacke weitgehend abwehren können. Lediglich die Konzernwebseite...

MDR 04.04.2023

Bundesweite Cyberattacken auf Ministerien und Behörden

Durch einen Cyberangriff sind die Internetseiten mehrerer Landesregierungen und Behörden angegriffen worden. In Sachsen-Anhalt waren die...

Behörden Spiegel 06.04.2023

DDoS-Angriffe auf Behörden im ganzen Land

Seit Dienstag griffen Unbekannte die Webseiten deutscher Behörden an. Teilweise waren die Internetauftritte deswegen nicht erreichbar.

Heise
https://www.heise.de › Security 06.04.2023

DDoS-Angriffe auf offizielle Websites: BSI warnt ...

06.04.2023 — Das Bundesamt für Sicherheit in der Informationstechnik (BSI) teilte **heise** online mit, es sei über die Vorgänge informiert. Websites mehrerer ... 24.04.2023

DDoS Angriffe / aktuelle Zahlen

Security-Insider 04.04.2023

Cyberwar mit 436 Petabit (436 Mio. Gigabit Bandbreite)

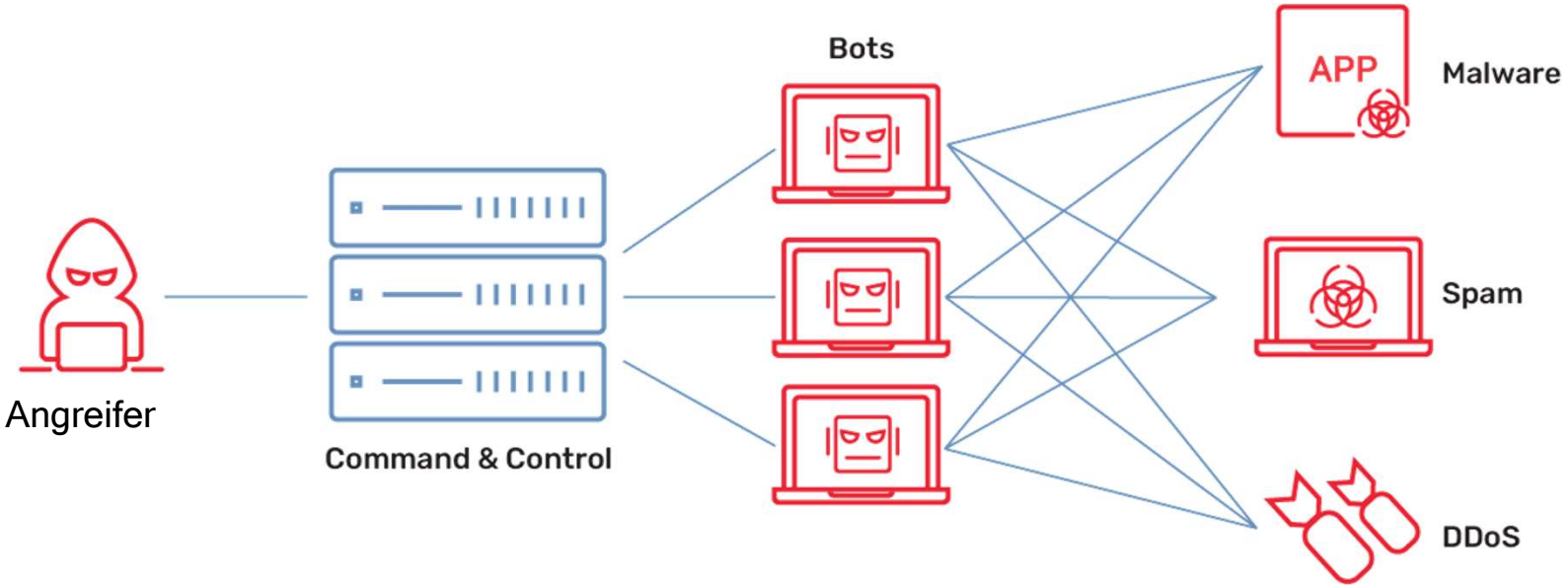
In der zweiten Hälfte des Jahres 2022 haben DDoS-Angriffe auf die HTTP/HTTPS-Anwendungsschicht deutlich zugenommen, was vor allem auf die...

24.04.2023

- Anstieg der DDoS Angriffe von 2019 bis 2022 um 487 Prozent
- >13 Millionen Angriffe in 2022 gezählt => alle 2,5 Sekunden ein Angriff
- Starke Zunahme seit Beginn des Ukraine-Krieges
- Politisch motivierte DDoS Angriffe steigen stark an
- Dauer zwischen mehreren Minuten und mehreren Tagen

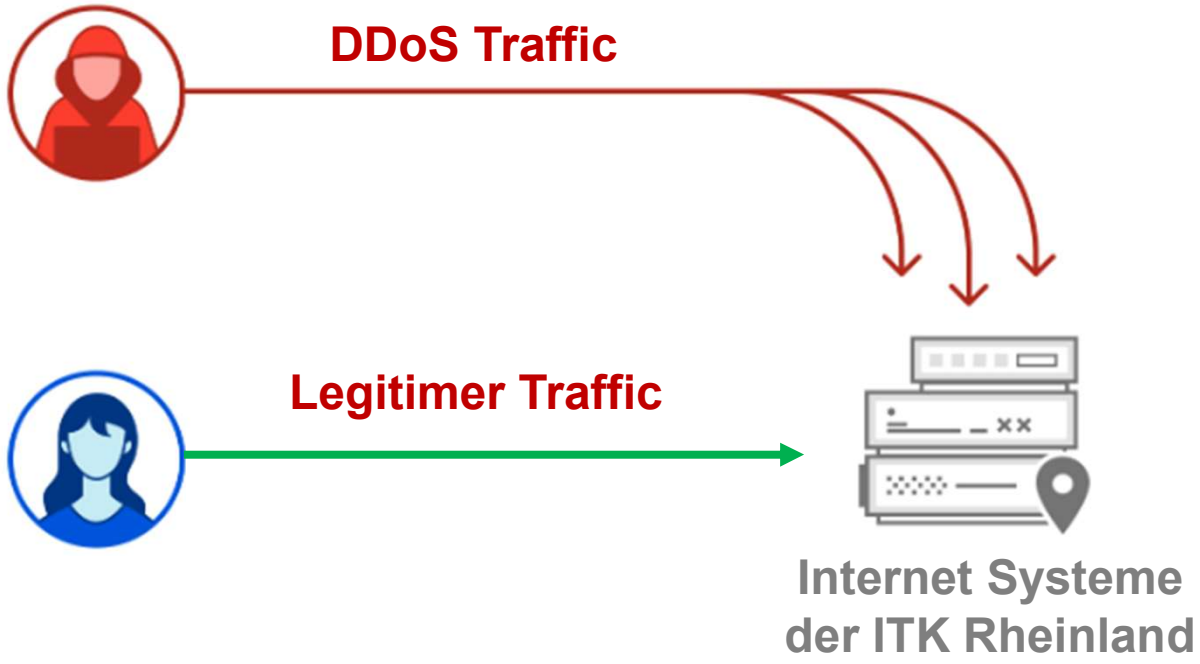
Prinzip DDoS Angriff

Prinzip DDoS Angriff



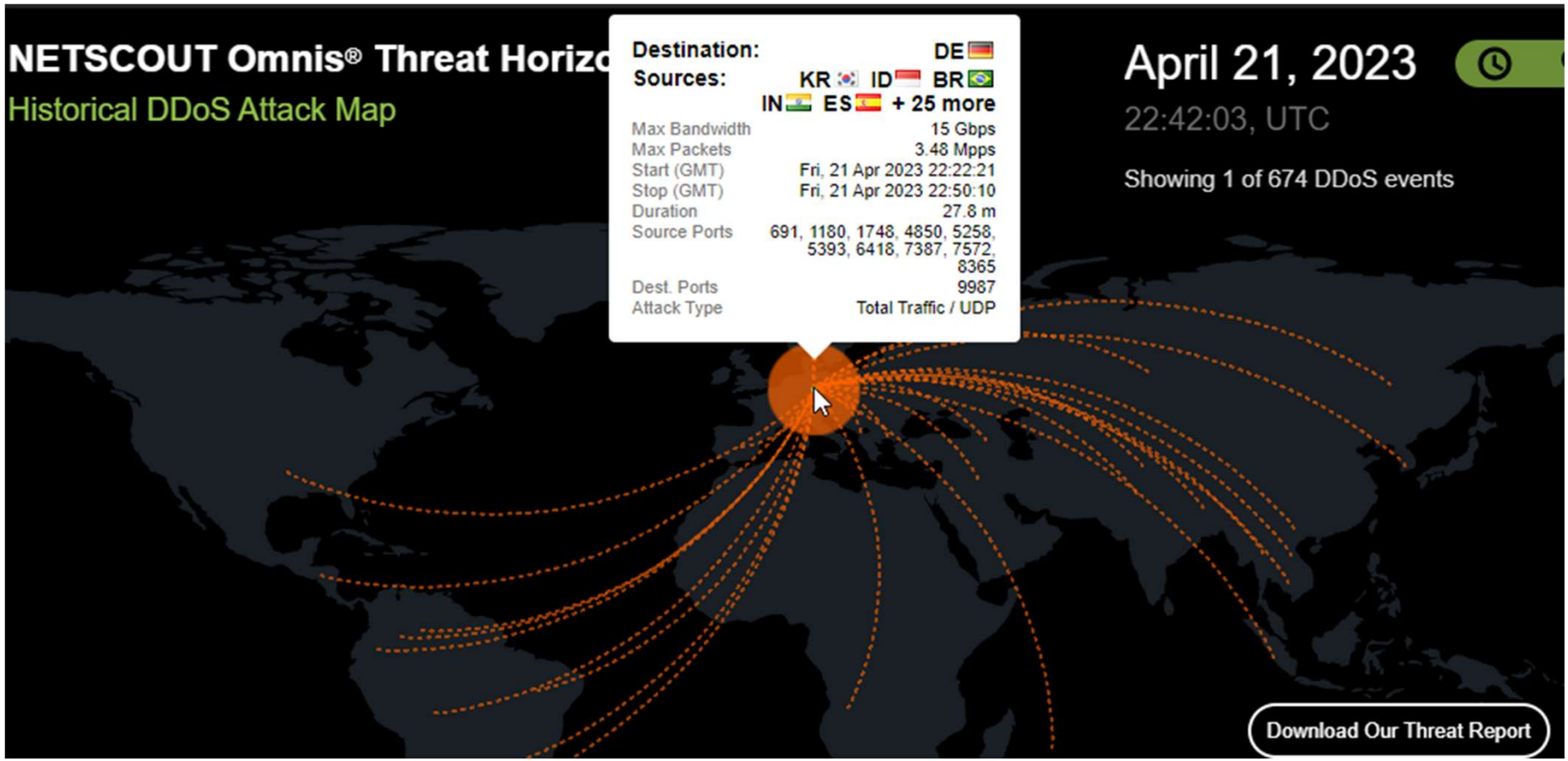
- Der Angreifer hat die Kontrolle über sog. Bots (Roboter)
- Er nutzt die gesammelte Leistung und Internet-Bandbreite aller Bots gegen sein Opfer
- Einsatzzweck ist die massenhafte Verteilung von Malware, Spam oder die Überlastung der Webseite

Herausforderung DDoS Angriff



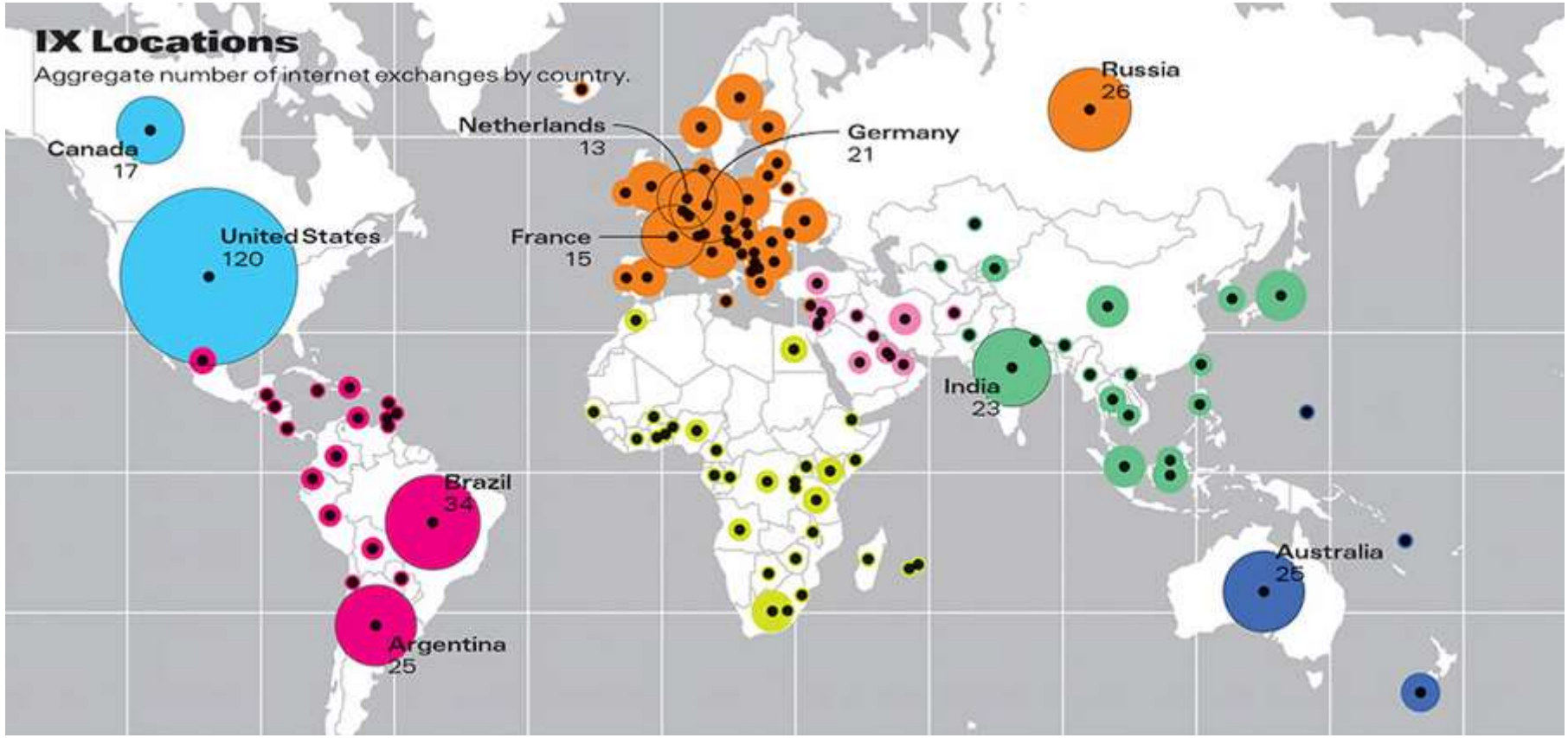
Die Herausforderung ist es, den DDoS Traffic zu erkennen und herauszufiltern,
damit legitimer Traffic weiterhin transportiert wird und
die Internet Dienste aufrecht erhalten bleiben.

Prinzip DDoS Angriff



Beispiel vom 21.04.2023
Angriff aus 30 Ländern auf 1 Ziel in Deutschland

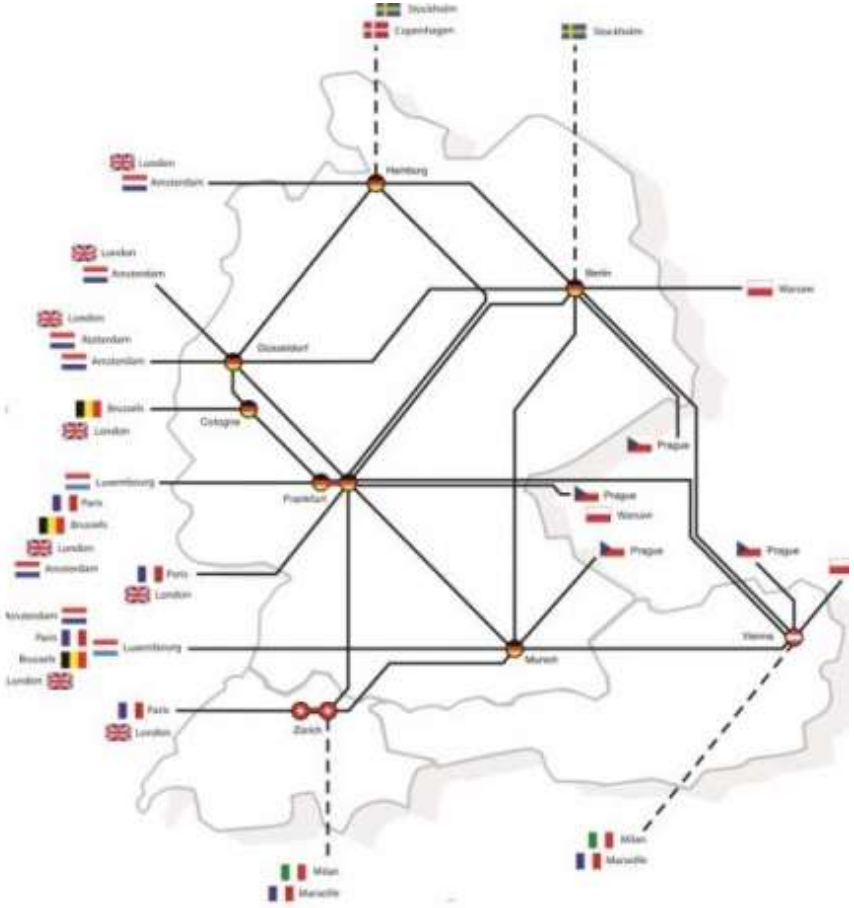
Internet Knotenpunkte Weltweit



Um den DDoS Angriff frühzeitig eingrenzen zu können,
wird der ungewollte Traffic vom Provider an den Landesgrenzen unterbunden

Abwehr eines DDoS Angriffs

- Spätestens an einem der Knotenpunkte in NRW wird der ungewollte DDoS Traffic unterbunden.
- Legitimer Traffic wird während dem DDoS Angriff bevorzugt transportiert, damit die Internet Dienste nicht ausfallen.
- Im Worst Case wird der gesamte, ausländische Traffic unterbunden, damit die Kunden der ITK Rheinland weiterarbeiten können.



Hauptknotenpunkte DACH

IT Sicherheitsmaßnahmen

Digitalisierung – nicht ohne IT Sicherheit

Diskussion / Fragen

Herzstück: Das Rechenzentrum

Microsoft Windows Server → 990 Stck.

Linux → 225 Stck.

Das Rechenzentrum ist offiziell nach DIN ISO / IEC 27001 zertifiziert.

Herzstück: Das Rechenzentrum

- Netzersatzanlage für 8 Tage Autonomiezeit (1000 PS Diesel mit Aggregat)
- Unterbrechungsfreie Stromversorgung
- Klimatechnik mit freier Kühlung
- Gebäudeleittechnik mit 1500 Datenpunkten
- Umweltfreundliche Gaslöschanlage zur Brandbekämpfung
- Einbruchmeldeanlage + Zugangskontrollsystem
- Videoüberwachung

Verbesserung der Energieeffizienz: Rechenzentrum

Das Rechenzentrum ist das technische Herzstück der ITK Rheinland

Maßnahmen im RZ orientieren sich an der Norm Blauer Engel „Energieeffizienter Rechenzentrumsbetrieb“ [DE-UZ 161])

Verbesserung der Energieeffizienz: Rechenzentrum

Nachhaltige Senkung des Stromverbrauchs
im Rechenzentrum in 2021 und 2022

-13%

Durch neue Löschanlage
als Ersatz für die
Brandvermeidungsanlage

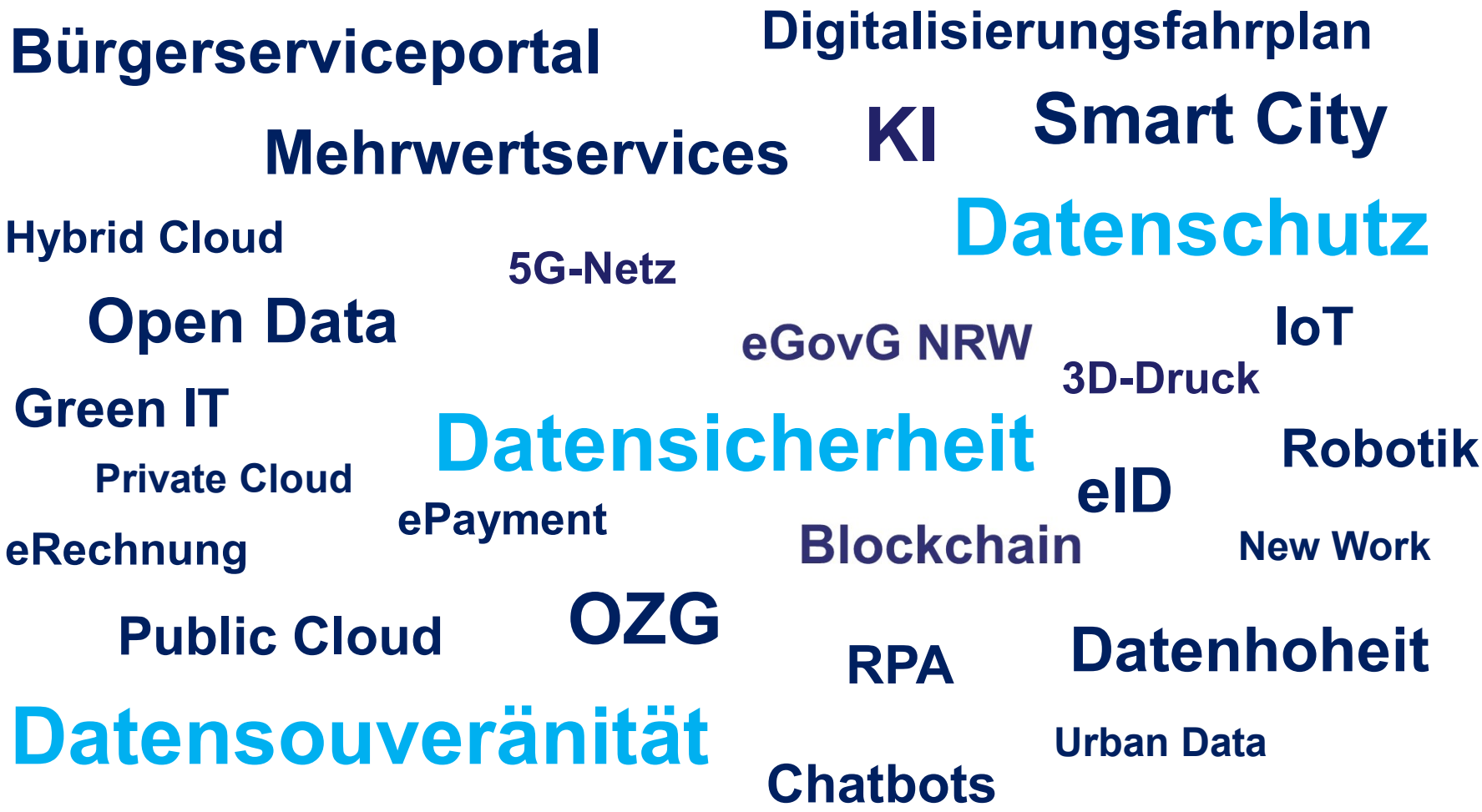
2021

-17%

Durch Inbetriebnahme
einer neuen Klimatechnik

2022

Wir unterstützen auf dem Weg in die digitale Zukunft



Vielen Dank für Ihre Aufmerksamkeit und bleiben Sie mit uns im Austausch

www.itk-rheinland.de

ITK Rheinland

@itkRheinland

@itkRheinland

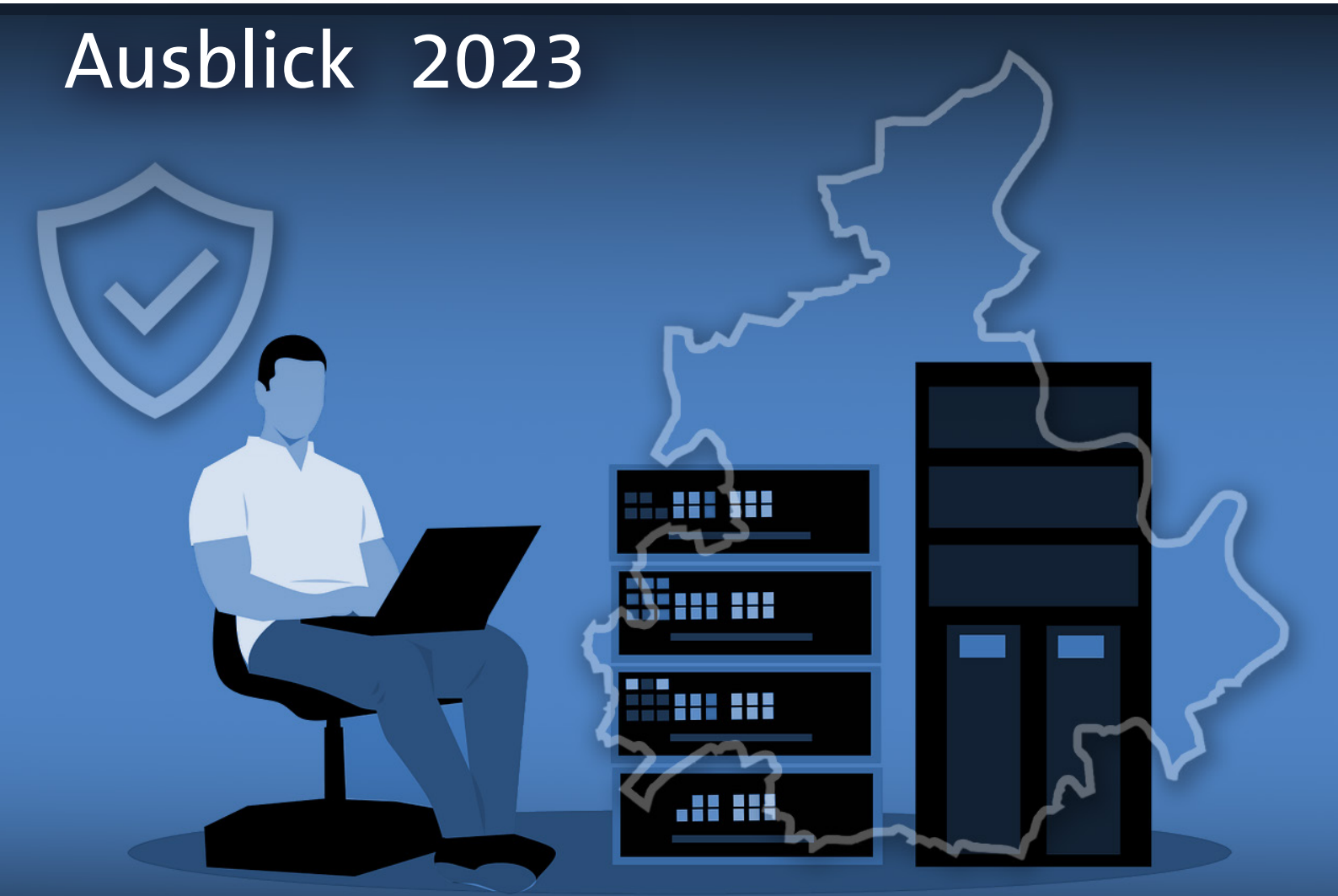
rhein kreis neuss

Jahresbericht

IT-Sicherheit

Rückblick 2022

Ausblick 2023



Vorwort

Die Schäden durch sogenannte Internet-Kriminalität sind hoch. Das BKA verweist auf Zahlen, die der Branchenverband Bitkom veröffentlicht hat. Demnach verursachte Cybercrime im vergangenen Jahr in Deutschland Schäden in Höhe von 223,5 Milliarden Euro. Einen besonders starken Anstieg gab es demnach bei sogenannten Ransomware-Attacken. Dabei verschlüsseln Kriminelle die Computer-Systeme von Privatpersonen, Behörden oder Unternehmen. Diese können dann auf ihre Daten nicht mehr zugreifen. Die Kriminellen versprechen, die Daten für ein Lösegeld wieder zugänglich zu machen.

Das Bundeskriminalamt (BKA) nennt Ransomware „die Bedrohung“ für Unternehmen und öffentliche Einrichtungen. Von Erpressungsversuchen betroffen waren u.a. die Landtage von Sachsen-Anhalt und Mecklenburg-Vorpommern, Schulen, Polizeidienststellen, Landesministerien, Universitäten und Krankenhäuser. Immer wieder trifft es zudem auch Kommunalverwaltungen.

Der kommunale Warndienst CERT NRW informiert den Rhein-Kreis Neuss täglich über bekannte Sicherheitslücken in IT-Systemen und Software. Zum Tagesgeschäft der IT gehört es deshalb zunehmend, solche Schwachstellen zu lokalisieren und abzustellen.

Mit einer weiteren organisatorischen Maßnahme soll der wachsenden Bedrohungslage in unserer IT-Sicherheitsstrategie verstärkt Rechnung getragen werden. Die Aufgaben IT-Sicherheit und die Abwehr von Cyber-Bedrohungen sollen künftig durch einen Chief Information Security Officier (CISO) inkl. Stellvertretung noch mehr Gewicht in der Kreisverwaltung erhalten. Der bisherige IT-Sicherheitsbeauftragte wird dazu aus der Abteilung ZS 4.1 - Zentrale IT herausgelöst. Zusammen mit seiner Stellvertretung, die insbesondere für die IT-Sicherheit an Kreisschulen zuständig ist, wird der CISO mit externer Unterstützung ein Information Security Management System (ISMS) aufbauen, welches hilft, die IT-Sicherheit der Kreisverwaltung nachhaltig, systematisch und workflowgestützt zu steuern, zu kontrollieren und zu verbessern.

Harald Vieten
Dezernent für IT, Digitalisierung und Bauen

Verehrte Leserinnen und Leser,

2022 haben erfolgreiche Ransomeareangriffe bei den Kommunen und zum Teil bei deren Rechenzentren erhebliche Schäden angerichtet. Besonders die kleineren kommunalen Verwaltungen sind zu einem beliebten Ziel geworden. Die IT-Verantwortlichen müssen noch intensiver als bisher vorbereitet sein, damit die Schäden an IT-Systemen durch Hacker vermieden werden. Die Verfügbarkeit und der vertrauensvolle Umgang mit den Daten müssen vor den Attacken von Cyberkriminellen effizient geschützt bleiben.

Im vorliegenden Jahresbericht werden verschiedene Teilmaßnahmen beschrieben, die alle für sich wichtige Bausteine für die gesamte IT-Sicherheitsstrategie beim Rhein-Kreis Neuss sind. Die beschriebenen Themen waren die besonderen Schwerpunkte der Verbesserungsmaßnahmen im Jahr 2022. Sie sind bei Weitem kein abschließendes Bild, welche Maßnahmen insgesamt für einen sicheren IT-Betrieb notwendig sind.

Alle IT-Sicherheitsvorkehrungen unterliegen einem wiederkehrenden Verbesserungsprozess und werden entweder durch zusätzliche technische und organisatorische Maßnahmen ergänzt oder die laufenden Prozesse werden geprüft und aktualisiert. Es gibt in der IT-Sicherheit keinen langlebigen Status Quo, durch den man beruhigt und auf Dauer abgesichert ist.

Der vorliegende Bericht soll ein Querschnitt sein, welche Projekte im letzten Jahr zum sicheren Regelbetrieb überarbeitet oder aufgrund besonderer Relevanz als Arbeitsschwerpunkte umgesetzt wurden.

Nehmen Sie bitte den ein oder anderen Hinweis auch mit, um im privaten Umfeld geschützt zu bleiben. Beachten Sie mit gesundem Misstrauen, inwieweit Sie beim digitalen Austausch Ihrer Daten und Anmeldeinformationen Dritten vertrauen können. Sie finden auf Seite 18 einige Tipps, die Sie beachten sollten, wenn Sie verdächtige Nachrichten im E-Mail Postkorb finden.

Frank Meger
IT-Sicherheitsbeauftragter

Jahresbericht zur IT-Sicherheit

Rückblick 2022 - Ausblick 2023

Inhalt

01 Die Lage der IT-Sicherheit in Deutschland

Bericht des BSI für das Jahr 2022

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im Oktober 2022 seinen jährlichen Lagebericht zur Entwicklung in der IT-Sicherheit veröffentlicht. Der Bericht gibt auf über 100 Seiten einen Rückblick der letzten 12 Monate in der Cyber-Sicherheit. Zu den Bereichen Gesellschaft, Wirtschaft, Staat und Verwaltung werden die wichtigsten Erkenntnisse und Maßnahmen im Lagebericht für Deutschland zusammengefasst.

Ein besonderer Hinweis gilt der Zunahme von bekannten Schwachstellen in Hard- und Softwareprodukten. Solche potentiellen Einfallstore gefährden die Informationssicherheit. Deren Missbrauch muss durch frühzeitige Aktualisierungen vermieden werden.

Auch der russische Angrifsskrieg hat eine weitere Bedrohungslage hervorgerufen. Die Investitionen in die Cybersicherheit sollen bundes- und landesweit noch mehr verstärkt werden, wobei das BSI eine noch wichtigere Rolle als Zentralstelle spielen soll.

Die Erneuerung und der Ausbau von Netzen und IT-Systemen in der Verwaltung, die Stärkung der Sicherheitsbehörden und die Abwehrfähigkeit gegen Cyberangriffe werden als bedeutdende Ziele für mehr IT-Sicherheit in 2023 angestrebt.

Wie verletzlich die IT-Strukturen in Verwaltungen sein können zeigte im Juni 2021 der Cyberangriff auf die Verwaltungs-IT in Anhalt Bitterfeld. Die Kommune hatte nach dem Ausfall der Verwaltungssysteme den Katastrophenfall ausgerufen.

Dem aktuellen Lagebericht zufolge gelten Ransomware-Attacken nach wie vor als eine der größten Bedrohungen, zumal die kriminellen Aktivitäten sehr angespannt, dynamisch und vielfältig sind.

Laden Sie den vollständigen Lagebericht des BSI als PDF-Datei herunter:

Auszug aus dem Lagebericht des BSI

Top 3-Bedrohungen je Zielgruppe:

Gesellschaft	Wirtschaft	Staat und Verwaltung
Identitätsdiebstahl Sextortion Fake-Shops im Internet	Ransomware Schwachstellen IT-Supply-Chain: Abhängig	Ransomware APT Schwachstellen, offene oder falsch konfigurierte Online-Server

Erster digitaler Katastrophenfall in Deutschland

207 Tage Katastrophenfall

Nach Ransomware-Angriff konnten Elterngeld, Arbeitslosen- und Sozialgeld, KfZ-Zulassungen und andere bürger nahe Dienstleistungen nicht erbracht werden.

Die Anzahl der Schadprogramme steigt stetig.

Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund

116,6 Millionen zugenommen.

Hacktivismus im Kontext des russischen Krieges:

Mineralöl-Unternehmen in Deutschland muss kritische Dienstleistung einschränken.

Kollateralschaden

nach Angriff auf Satelliten-kommunikation

20.174

Schwachstellen in Software-Produkten (13% davon kritisch) wurden im Jahr 2021 bekannt. Das entspricht einem **Zuwachs von 10%** gegenüber dem Vorjahr.

69%

aller Spam-Mails im Berichtszeitraum waren Cyber-Angriffe wie z.B. Phishing-Mails und Mail-Erpressung.

90%

des Mail-Betrugs im Berichtszeitraum war Finance Phishing, d.h. die Mails erweckten betrügerisch den Eindruck, von Banken oder Sparkassen geschickt worden zu sein.

Geschäftsmodell Ransomware

Ransomware ist inzwischen ein gut laufendes Geschäftsmodell. Die Angreifer müssen noch nicht einmal selbst besondere IT-Kenntnisse für das Durchführen von Cyber-Angriffen haben. Kriminelle können deartige Schadsoftware inzwischen als Lizenz erwerben und damit anschließend beliebige Netzwerke angreifen.

Behörden sind weiterhin ein beliebtes Ziel für Ransomware-Angriffe. Auch wenn davon abzuraten ist, auf Lösegeldforderungen einzugehen, sind die Verwaltungen aus Sicht der Kriminellen zunächst einmal zahlungsfähige Opfer.

Für Hacker zählen Cyber-Erpressungen als lukratives Geschäft, denn die durchschnittliche Lösegeldzahlung beträgt mehr als 812.000 US-Dollar.

Backups müssen geschützt werden

Die Kriminellen greifen nicht nur den aktiv verwendeten Datenbestand an. In dem Fall könnte der Geschädigte eventuell auf eine unkompromittierte Datensicherung zurückgreifen. Vielmehr ist es das Ziel, auch die Backups der IT-Systeme und damit alle Datenversionen zu verschlüsseln. Deshalb müssen Backups als unveränderbar geschützt werden, damit die Sicherungen gegen Ransomware immunisiert sind. Man spricht von einem „immutable backup“. Hierzu gibt es verschiedene Szenarien, wie eine solche Sicherungsstrategie umgesetzt werden kann.

Der Rhein-Kreis Neuss hat in 2022 seine Backup-Strategie um zusätzliche Schutzmaßnahmen erweitert. Ein Konzept für den Betrieb eines mehrstufigen „Immutable Storage“ wurde in einem mehrwöchigen Projekt erfoglreich umgesetzt.

02 Backups vor Ransomware schützen

”Immutable Storage” wird eingeführt

Voraussetzungen für ein solides Backup

Die Möglichkeit zur Wiederherstellung von Daten erfordert sorgfältige Backups. Dabei spielt es keine Rolle, ob der Verlust auf einen Systemabsturz, eine Malware-Infektion oder einen Ransomware-Angriff zurückzuführen ist. Aus diesem Grund sollte jede IT-Organisation ein System einrichten, das eine Datenwiederherstellung sicherstellt, die vor Kompromittierung geschützt wurde.

Beim Sicherungskonzept ist maßgeblich zu beachten, dass die Konfiguration der Systeme eine eigene Verschlüsselung beinhaltet. Die Unveränderlichkeit und die physische Isolation der Backups muss durch ein angepasstes Sicherungskonzept erreicht werden. Die Backups müssen zudem auf Malware gescannt werden.

Als Ziel muss erreicht werden, eine insgesamt unveränderliche Sicherung vorzuhalten.

Neue Risiken, neue Regeln

Es gibt eine alte „3-2-1“-Regel für den Datenschutz: Bewahren Sie drei Kopien Ihrer Daten auf, eine primäre und zwei Backups. Zwei Kopien werden lokal in zwei Formaten gespeichert (z. B. Network Attached Storage, Band oder ein lokales Laufwerk), wobei eine Kopie extern in der Cloud oder einen sicheren Speicher verlagert wird.

Leider zielen laut Forbes die meisten Ransomware-Angriffe auf Sicherungssysteme ab, indem sie Endpunktdaten verschlüsseln, um eine Wiederherstellung zu verhindern. Aus diesem Grund sollte die „3-2-1-1“-Sicherungsregel eingeführt werden, wobei sich die letzte „1“ auf einen unveränderlichen Speicher bezieht.

Diese letzte „1“ lässt sich mit dem richtigen strategischen Ansatz wiederum doppelt realisieren. Beim Rhein-Kreis Neuss wurden alle notwendigen Maßnahmen dazu inzwischen ungesetzt.

3-2-1-1-0 Strategie

Die 3-2-1 Backupregel muss heutzutage durch zusätzliche Maßnahmen verbessert werden. Die Datensicherung muss auf die Unveränderbarkeit der Daten ausgerichtet werden.

3	2	1	1	0
verschiedene Kopien der Daten	verschiedene Medien	Offsite Speicherung	ist offline	Verifikation erfolgreicher Wiederherstellung

03 Benutzerkonten im Blick
durch Identitäts- und Zugriffsmanagement

Menschliche Zugriffe sind ein Risiko

Auch bei einer Kommunalverwaltung müssen heutzutage hoch komplexe IT-Umgebungen abgesichert werden. Das erfordert auch zu überlegen, welche Sicherheitsanforderungen für die IT-Systeme, die Programmoperationen, die Datenzugriffe und die zugreifenden Benutzer festzulegen sind.

In dem Zusammenhang sind trotz Endpoint-Sicherheit, Datenverschlüsselung und Firewalls gerade die Benutzerkonten ein kritisches Einfallstor. Das Aushebeln der IT-Sicherheit durch Identitätsdiebstahl stellt nach wie vor eine der größten digitalen Gefahren dar.

Benutzerdaten werden gehandelt

Personifizierte Zugangsdaten werden im Darknet als Ware gehandelt. Durch die Ransomware-Angriffe der letzten zwei Jahre und der Veröffentlichung von umfangreichen Anmeldedaten gab es einen regelrechten Boom, sodass weitere Millionen personenbezogener Datensätze angeboten wurden.

Laut Verizon Data Breach Report 2022 resultieren inzwischen 61 Prozent der Datenschutzverletzungen aus gestohlenen Anmeldedaten.

Risikofaktor externe Dienstleister und interne Administratoren

Benutzerkonten sind die bevorzugten Angriffsziele von Cyberkriminellen, um mittels Identitätsdiebstahl einen möglichst hohen Schaden anzurichten. Besonders betroffen sind häufig externe Dienstleister und interne Administratoren. Diese Personen haben oft einen privilegierten Zugang mit Zugriffen auf kritische Anwendungen und Systeme. Es gibt verschiedene Kriterien, um einen solchen Missbrauch zu verhindern. So sollten Zugangsdaten zu kritischen Systemen beispielsweise den Benutzern nicht bekannt sein. Sie sollten an einem sicheren Ort verwahrt und regelmäßig geändert werden.

Zur sicheren Authentifizierung sollte eine Multi-Faktor-Authentifizierung genutzt werden, um den Grundlevel für eine sichere Anmeldung zu erhöhen.

Mehr Sicherheit im Anmeldeprozess

Ein verbessertes Maß an Sicherheit kann auch hier erreicht werden. Dazu muss eine sichere Anmeldemethode eingesetzt werden, ohne dass es unbedingt komplizierter wird. Mittels moderner Authentifizierungsstrategien und integrierter Lösungen ist es möglich, Identitäten und Benutzerkonten besser zu schützen und noch kontrollierbarer zu machen. Dabei muss zwingend beachtet werden, dass alle ausgelagerten Anbieter über den gleichen Sicherheitslevel verfügen und nachweislich als vertrauenswürdig gelten.

Prinzip der geringsten Rechte

Die Grundannahme beim Schutz von Identitäten ist, dass Benutzer*innen, Anwendungen und Daten nicht in einer gemeinsamen vertrauenswürdigen Sicherheitszone sind. Deshalb gilt auf allen Ebenen das Prinzip der geringsten Rechte. Jede Identität soll nach erfolgreicher Authentifizierung einen genau definierten, minimalen Satz von Berechtigungen erhalten. Je nach Bedarf werden die Rechte der Identitäten entweder erweitert oder eingeschränkt. Ihnen fehlen dadurch die Möglichkeiten zu sogenannten Seitenbewegungen, die in der IT-Security besonders gefürchtet sind.

Aufbau eines Privileged-Access-Management (PAM)

Privilegierte Konten ermöglichen den Zugriff auf die sensibelsten und geschäftskritischsten Bereiche der IT der Kreisverwaltung. Ein PAM ermöglicht eine gesteuerte und protokollierte Zugriffsverwaltung von Konten und hilft damit, mehrere Angriffsvektoren auszuschalten.

Der Rhein-Kreis Neuss wird 2023 weitere Maßnahmen zur verstärkten Zugriffskontrolle umsetzen.

Architektur von Privileged Access Management für Cyber Defense

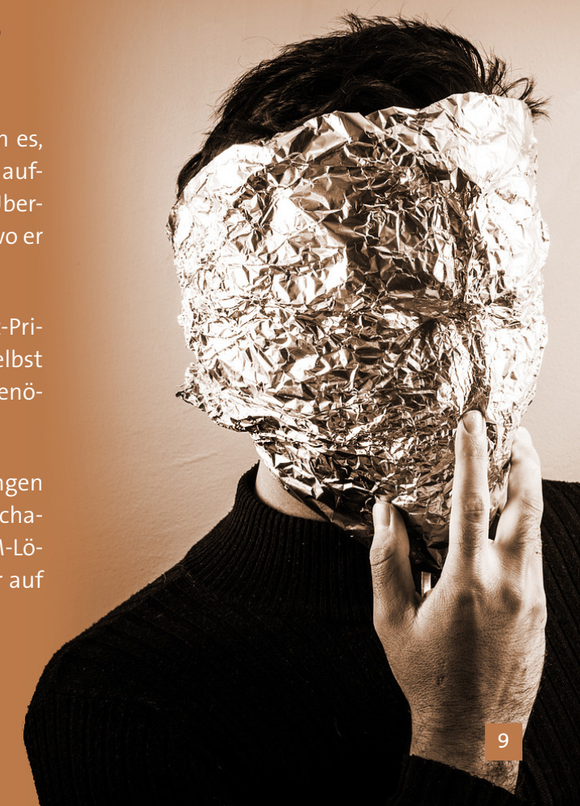
Bedingung	**Anwendungsfälle bestimmen**	**H2M:** • System Admin • Endpoint lokaler Admin • Remote Admin	**M2M:** • Konnektivität – Applikationen und Dienste • Automation – Code, DevOps, RPA	**Cloud Operations:** • Infrastruktur Berechtigungen
Orientierungsrahmen	**Anforderungen definieren**	**Kontrolle und Abdeckung** • Cyber–Sicherheitsrahmen • Plattformen & Umgebungen	**Betriebsmodell:** • User segmentation • Persistent vs. zero standing	**Bereitstellungsmodell:** • Light vs. full PAM
	Architektur entwickeln	**Kernkompetenzen:** • Governance und Verwaltung • Erkennung und Onboarding • Berechtigungsverwaltung • Sitzungsverwaltung • Erhöhungs– und Delegierungsmanagement • Protokollierung, Berichterstattung und Prüfung	**Erweiterte Fähigkeiten:** • Privilegierter Remote–Zugriff • Anwendungen und Dienste • Cloud–Infrastruktur • Privilegierte Aufgabenautomatisierung • Analytik und Reaktion • Robotische Prozessautomatisierung • Betriebstechnik	
Verfizieren	**Resilienz gewährleisten**	**Einfache Bereitstellung**	**Integration**	**Verfügbarkeit**

Wie funktioniert ein Privileged-Access Management (PAM)?

Lösungen für die privilegierte Zugriffsverwaltung ermöglichen es, Aktivitäten von Zugriffen zu überwachen, zu berichten und aufzuzeichnen. Auf diese Weise können Administratoren den Überblick über den privilegierten Zugriff behalten und feststellen, wo er möglicherweise missbraucht wird.

Die privilegierte Zugriffsverwaltung arbeitet nach dem Least-Privilege-Prinzip (Prinzip minimaler Berechtigungen), so dass selbst privilegierte Benutzer nur auf das zugreifen dürfen, was sie benötigen.

Administratoren müssen Anomalien und potenzielle Bedrohungen leicht erkennen können, wenn sie sofort Maßnahmen zur Schadensbegrenzung ergreifen sollen. Im Idealfall verfügt die PAM-Lösung über ein integriertes Warnsystem, um den Administrator auf unerwartete Aktivitäten aufmerksam zu machen.



04 Schwachstellenanalyse
erhöht die IT-Sicherheit

Irgendwo hakt es immer

Die IT-Verantwortlichen beim Rhein-Kreis Neuss kennen das: Nie ist alles auf dem aktuellsten Stand. Ob es um die Firmware-Stände von Hardware, die aktuellste Version von Gerätetreibern oder den Release-Stand der eingesetzten Software geht - bei der Vielzahl an Produkten stehen inzwischen ständig Aktualisierungsaufgaben an. Vieles davon lässt sich durch eine umfassendes Patch Management automatisiert erledigen, oft ist aber auch ein manuelles Handeln für die Umsetzung eines Updates erforderlich. Selbst die möglichen Reste einer Deinstallation von Software müssen womöglich erkannt und durch weitere Eingriffe entfernt werden.

Handlungsfeld für die IT-Sicherheit

Immer häufiger werden Updates erforderlich, um damit Sicherheitslücken zu schließen, die beim Auslassen der Aktualisierung ein Sicherheitsrisiko darstellen. Sicherheitslücken werden dann zum Beispiel zur Gefahr, wenn darüber Malware eingeführt werden kann. Die möglichen Folgen sind Datenklau, Spionage oder Erpressung durch Ransomware bis hin zum kompletten Systemausfall. Die Arbeit der Verwaltung kommt im schlimmsten Fall zum Stillstand.

Kommunaler Warndienst meldet Schwachstellen

Der Rhein-Kreis Neuss ist beim Kommunalen Warn- und Informationsdienst Nordrhein-Westfalen angeschlossen. Der Warn- und Informationsdienst des CERT NRW dient der zielgruppengerechten Aufbereitung und Weiterleitung sicherheitsrelevanter Informationen an die Kommunen in NRW.

Täglich erhält der Rhein-Kreis Neuss über einen sicheren E-Mail-Kanal Informationen zu bekannten Schwachstellen verbunden mit einer Bewertung, wie dringend eine Sicherheitslücke zu beheben ist.

Schwachstellen auffinden

Über eine Schwachstelle informiert zu sein ist die eine Seite der Medaille, aber an welchen Stellen tritt eine Schwachstelle überhaupt auf? Ein gutes Beispiel, in welchen Umfang Maßnahmen erforderlich werden, war in 2022 die „Log4j“ Sicherheitslücke. Für die weltweite IT-Security war die besondere Herausforderung, dass Log4J extrem weit verbreitet ist und sich nicht ohne Weiteres sagen ließ, ob Log4J auf den eigenen Systemen läuft. Das Open-Source-Werkzeug wird von zahlreichen weiteren Anwendungen integriert oder als Abhängigkeit genutzt. Im Internet wurde Listen mit Hiweisen gefüllt, welche Hersteller und Projekte betroffen sind. Diese Listen beinhalten mehrere hundert Einträge.

Mithilfe spezieller Scanvorgänge mussten auch beim Rhein-Kreis Neuss alle Systeme und Programme überprüft werden. Das Entfernen der Schwachstelle hatte für die IT oberste Priorität.

Schwachstellenscan automatisieren

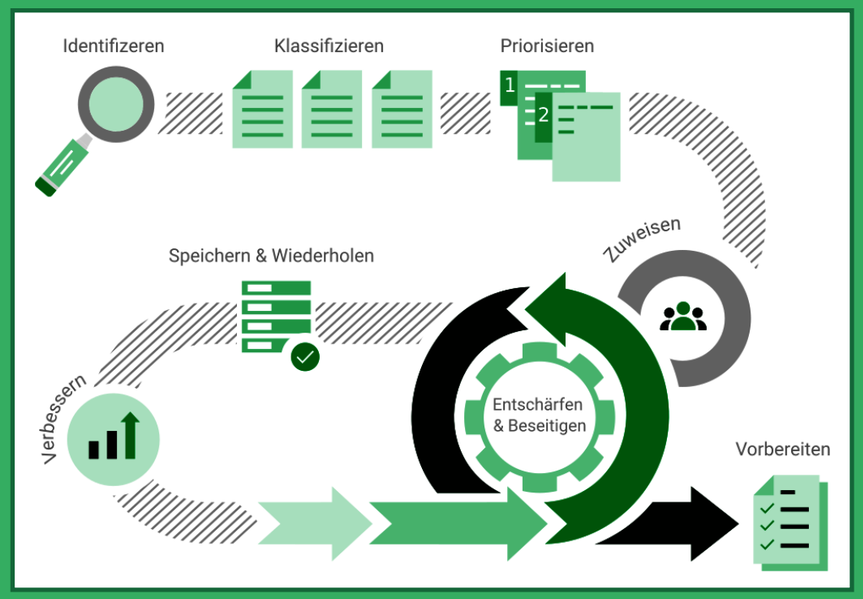
Log4j ist nur ein Beispiel einer Sicherheitslücke, auf die man umgehend reagieren musste. Datenbanken mit Schwachstellen enthalten inzwischen über 100.000 gelistete Schwachstellen verschiedenster Art. Eine kontinuierliche Analyse, ob eine Software oder ein System durch ein Sicherheitsleck angreifbar ist, wäre nicht ohne Automatisierung möglich.

Der Rhein-Kreis Neuss setzt deshalb ab 01/2023 ein „Vulnerability Management“ ein. Über einen automatisieren Prozess werden IP-Adressen mithilfe spezieller Softwaretools auf mögliche Schwachstellen untersucht - unabhängig von Software und Hersteller. Die Analyse zeigt Lücken detailliert auf und liefert Informationen zur Abhilfe. Indirekt kann der Scan beispielsweise auch zeigen, wie verantwortungsbewusst das Patch-Management umgesetzt wird. Die Ergebnisse tragen indirekt zu einem verbesserten Patch-Management bei.

Bereits wenige Tage nach der Veröffentlichung wurde die Log4Shell-Schwachstelle von Kriminellen ausgenutzt.

Kontinuierliche Sicherheit durch Scan Prozess

Von der Erkennung einer Schwachstelle bis zur Behebung und Kontrolle – neben regelmäßigen automatischen Schwachstellenscans sollte auch ein beständiger Kreislauf zur Behebung vorhanden sein. Mit der richtigen Lösung erhalten die IT Verantwortlichen anschließend eine Einstufung der Schwachstellen nach ihrem Schweregrad sowie mögliche Maßnahmen zur Behebung. Dies erlaubt eine Priorisierung und gezielte Behebung der Schwachstellen.



Quelle: Greenbone Networks

05 Managed Detection & Response

Kontinuierliche Ausfallsicherheit

Cyber-Attacken 24/7

Cyberkriminelle agieren nicht dann, wenn wir besonders aufmerksam sind, sondern rund um die Uhr. Sie können ihre Angriffe zu einer beliebigen Zeit starten und nutzen aus, dass eine durchgehende Überwachung durch das IT-Personal nur begrenzt möglich ist.

Auch wenn gute Endpoint-Detection-and-Response-Plattformen (EDR) im Einsatz sind, kann das Potenzial der bereitgestellten Analyse-Tools aus Zeit- oder Personalmangel nicht voll ausgeschöpft werden. Nach der regulären Arbeitszeit muss verstärkt auf Alarmmeldungen gesetzt werden, die wiederum eine personelle Aufmerksamkeit benötigen.

Informationsflut zu Risiken

Die IT-Verantwortlichen erhalten täglich eine Vielzahl an Warnmeldungen, die IT-Sicherheitssysteme ausgeben. Nicht alle Meldungen bedeuten dabei eine aktive Gefahr, aber die Meldungen müssen bewertet und dürfen nicht ignoriert werden. Eine schnellere Reaktion kann die Unterstützung externer Sicherheitsanalysten schaffen. Sie beteiligen sich oder übernehmen die Bewertung der Informationen und Insights von Drittanbietern und nutzen Tools zur Bedrohungsanalyse. Es gilt, aus allen sicherheitsrelevanten Hinweisen die tatsächlichen Bedrohungen durch Cyberkriminelle zu erkennen.

Managed Detection and Response (MDR) etablieren

Die Anbieter von Security-Lösungen bieten professionelle Dienste als „Managed Detection and Response Service“ an. Die Dienstleister stellen Analysten bereit, die nach möglichen Bedrohungen suchen, Warnmeldungen bewerten, individuelle Handlungsempfehlungen geben oder das Problem direkt beheben. Die notwendigen Daten liefert die EDR-Lösung (Endpoint Detection and Response). Zu einer Warnmeldung gibt EDR einen Einblick, woher die Bedrohung kam, wie sie sich ausgebreitet hat, was die Ursache war und wie groß das Ausmaß der Bedrohung ist.

Cyber-Abwehr rund um die Uhr

Die internen IT-Sicherheitskapazitäten wird der Rhein-Kreis Neuss ergänzen, indem die besonders wichtigen Aufgaben wie Erkennung, Threat Hunting und Vorfallsuntersuchungen extern unterstützt werden. Um auf angeleitete Reaktionsszenarien zurückgreifen zu können, bietet MDR einen fortschrittlichen Schutz rund um die Uhr gegen Bedrohungen, die herkömmliche Abwehrmechanismen mittlerweile umgehen können.

Der Rhein-Kreis Neuss wird eine erweiterte Sicherheitsüberwachung etablieren, bei dem ein Team von Cybersicherheitsexperten 24/7 im Einsatz ist.

EDR und MDR kombiniert einsetzen

Mit MDR können sich die firmeninternen Ressourcen gezielt auf weitere kritischen Aufgaben konzentrieren. Fortschrittliche EDR-Systeme sorgen gleichzeitig für eine merkliche Erhöhung des Durchsatzes der Analysen und reduzieren dadurch die mittlere Zeit bis zur Reaktion auf ein Minimum.

Für den Rhein-Kreis Neuss bedeutet ein MDR-Service nicht, dass man sich entspannt zurücklehnen kann. Eine verbesserte Kontrolle und Transparenz der IT-Ereignisse und die Fachexpertise von zusätzlichen IT-Sicherheitskräften sind aber eine hochwertige Ergänzung.

EDR Security Management Dashboard

Analysten erhalten über spezielle Sicherheitskonsolen einen umfassenden Überblick über die gesamte Angriffsfläche. Sobald eine verdächtige Aktivität erkannt wird , reagiert das EDR-System automatisch und/oder alarmiert einen Analysten, der den Vorfall genauer prüft.

Die EDR-Datenbank wird mit weiteren externen Datenbanken hinsichtlich Gefahrenquellen, Warnhinweisen und Schwachstellen fortlaufend kombiniert und verglichen.

Quelle: Bitdefender

06 Darknet Monitoring
deckt Datenlecks auf

Zugangsdaten zu kaufen

Hacker arbeiten hochprofessionalisiert. Es gibt darunter zum Beispiel diejenigen, die Zugangsdaten zu Netzwerken stehlen, aber nicht automatisch auch weitere Straftaten begehen. Diese Aufgabe übernehmen dann meist andere Kriminelle.

Hacker bieten stattdessen diese Datensätze im Darknet zum Verkauf an. An dieser Stelle bietet sich für die IT-Sicherheit die Chance, Schlimmeres zu verhindern. DIe IT-Administratoren können durch Darknet Monitoring, also der Analyse der Marktplätze und der hier angebotenen Datensätze, herausfinden, ob Zugangsdaten illegal veröffentlicht sind.

Analyse des Darknets zur Aufdeckung von Sicherheitslücken

Der Rhein-Kreis Neuss führt ein regelmäßiges Darknet Monitoring aus. Es ist wichtig, bekannt gewordene Passwörter und Zugangsdaten zu ändern, um möglichen Angreifern einen Schritt voraus zu sein. Dafür wird das Darknet nach festgelegten Keywords durchsucht.

Allerdings ist durch die Struktur des Darknets dessen Monitoring alles andere als einfach. Eine zentrale Suchmaschine existiert nicht, eine automatisierte Analyse ist daher unmöglich.

Monitoring as a Service

Die Abdeckung aller relevanten Quellen im Darknet ist komplex. Neben relevanten Foren und illegalen Marktplätzen sowie auf anonymen Netzwerken müssen auch Telegram-Kanäle und Chats, kriminelle Foren und Paste-Seiten im Deep Web und Open Web im Blick behalten und auf sensible Inhalte geprüft werden. Selbst über Suchmaschinen, Social-Media-Kanäle, Mobile App Stores, Code Repositories, Cloud Storage-Datenbanken oder FTP Servern finden sich Informationen, die ein Risiko darstellen.

Ein genaues Bild der Bedrohungslandschaft kann nur eine Lösung bieten, die das ganze Internet mit all seinen Quellen scannt und überwacht. Drei zentrale Schwerpunkte für das Darknet-Monitoring müssen bedacht werden:

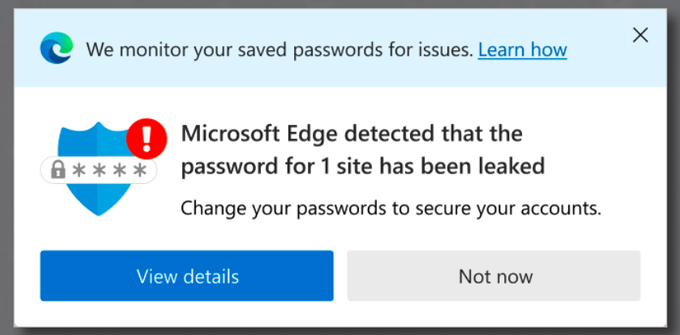
- Bedrohungen aufspüren und verfolgen
- Ungeschützte Login-Daten identifizieren
- Betrugsversuche entdecken

Für den Rhein-Kreis Neus ist auch dieser Service einer von vielen Bausteinen, der Bestandteil einer umfänglichen IT-Sicherheit ist.

Auch privat wichtig:
Anmeldedaten schützen

Moderne Browser haben Funktionen eingebaut, um bei der Verwendung von Anmeldedaten live zu prüfen, ob die eigenen Passwörter bereits im Darknet bekannt sind.

Ändern Sie bei Warnhinweisen die Passwörter, damit die Anmeldedaten nicht von anderen missbraucht werden.



Quelle: Microsoft

07 Cyber-Angriffe im Homeoffice erfolgreich abwehren

Cybergefahren am heimischen Schreibtisch

Das Arbeiten im Homeoffice klingt zunächst einmal nach einer vertrauten, sicheren Umgebung. Hier ist man jedoch in der digitalen Kommunikation den gleichen Gefahren wie in der Büroumgebung ausgesetzt. Hinzu kommt jedoch, dass man ohne den Austausch mit anderen in vielen Entscheidungen des Informationsaustauschs auf sich selbst gestellt ist.

Besondere Vorsicht bei E-Mails

Ist eine harmlos aussehende E-Mail von einer internen Firmenadresse, vielleicht verbunden mit der Bitte, sich doch für einen neuen Verteiler zu registrieren, real? Tatsächlich könnten Cyberkriminelle die Absender der Botschaft sein. Sie wollen auf diese Weise ins Verwaltungsnetzwerk einbrechen - am helllichten Tag. Solche Angriffe nennt man Phishing. Es geht in dem Fall um den Versuch, Nutzer mit gefälschten Nachrichten, Mails oder SMS auf Betrugsseiten zu locken.

Selbst für erfahrene Anwender oder sogar IT-Fachleute ist die Eindeutigkeit solcher Nachrichten nicht immer sofort erkennbar.

Zunahme von Phishing im Homeoffice

Solche Angriffe richteten sich immer öfter gezielt gegen Mitarbeiter im Homeoffice. Der Rhein-Kreis Neuss setzt deshalb im mobilen Arbeiten ausschließlich Geräte ein, die dem kontrollierten Schutz der zentralen IT (u.a. Endpoint Detection & Response, siehe Seite 12) unterliegen.

Zudem müssen die Zugriffsrechte, die Kontrolle von Programm- und Systemänderungen genauso restriktiv reglementiert sein wie bei der IT im Bürogebäude. Dazu zählt auch das Einspielen von Sicherheitsupdates unabhängig davon, an welchem Strandort ein Rechner der Kreisverwaltung verwendet wird.

Der Mensch im Mittelpunkt des Angriffs

Bei allen technischen Möglichkeiten steht bei Cyberangriffen oft die Person vor dem Rechner im Mittelpunkt einer Attacke. Phishing ist eine Form des Social Engineering, also ein Angriff auf die Schwachstelle Mensch. Technische Schutzmaßnahmen sind sinnvoll, können dies Art der Angriffe aber nicht verhindern.

Alle Beschäftigten haben eins gemeinsam: Sie sind mit der Außenwelt über E-Mail-Konten erreichbar. Das macht es den Angreifen im ersten Schritt einfach, einen Informationsaustausch zu versuchen. Während Mail-Angriffe früher noch relativ einfach zu erkennen waren, etwa durch schlechtes Deutsch im Textblock der Mail, ist das mittlerweile deutlich schwieriger. Die Nachrichten sind teilweise sehr professionell und ausführlich recherchiert, bis hin zu den E-Mail-Signaturen der vermeintlichen Absender.

Angriffe auch per Telefon

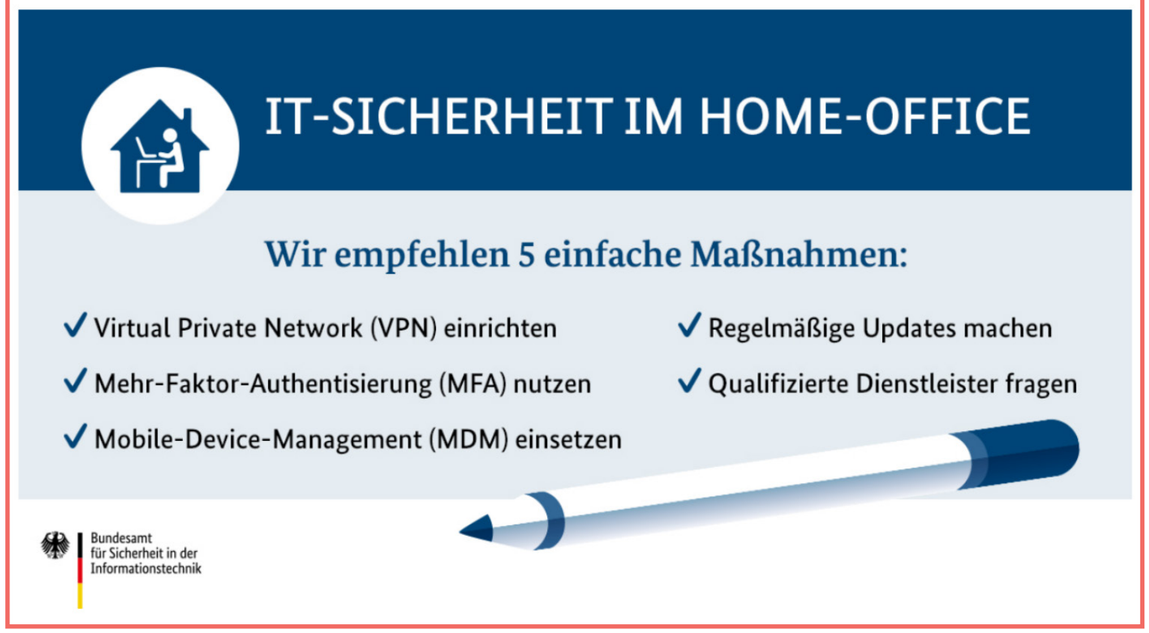
Auch per Telefon versuchen Kriminelle, sich Zugang über die Beschäftigten zu verschaffen. In dem Fall ist von „Vishing“ die Rede, einer Wortschöpfung aus „voice“ (Stimme) und „fishing“. Ein Klassiker: Betrüger geben sich am Telefon als Mitarbeitende von Microsoft aus und schaffen es, Software zur Fernwartung zu installieren. Danach haben sie die volle Kontrolle über den Rechner und einen Zugang zu den Daten.

Bei solchen Anrufen gilt der dringende Rat, sofort aufzulegen. Grundsätzlich verhalten sich die User gut geschützt, wenn sie beonders sensibel und mit einem gesunden Menschenverstand auf Cyber-Attacken und Social Engineering reagieren.

Letztlich ist ein Bündel aus verschiedenenen Sicherheitsmaßnahmen erforderlich, die der Rhein-Kreis Neuss für eine sichere, mobile Arbeitsumgebung vorgegeben hat.

Das BSI gibt Tipps für IT-Sicherheit im mobilen Arbeiten

Wir empfehlen 5 einfache Maßnahmen



Quelle: Bundesamt für Sicherheit in der Informationstechnik

08 Awareness muss trainiert sein

IT-Sicherheits-Training für alle

Der Rhein-Kreis Neuss hat 2021 mit der Einführung eines IT-Sicherheitslernprogramms für alle Beschäftigten begonnen. Seit 2022 wird das verbindliche Awareness-Lernprogramm für alle Beschäftigten in einer neuen Programmumgebung eingesetzt. Begleitet wird die Bereitstellung der Lerninhalte durch einen zertifizierten deutschen Dienstleister für IT-Sicherheitslösungen. Als Teilnehmer der Allianz für Cyber-Sicherheit befasst sich das deusche Unternehmen u.a. mit den Abwehrmaßnahmen gegen Cyberkriminalität.

Das Lernprogramm richtet sich bewusst an alle Beschäftigten. Jeder muss verstehen, welche Angriffsmethoden Hacker verwenden, um IT-Systeme und digitale Daten zu schädigen. Anstelle einmaliger Schulungen setzt man heutzutage „Security Awareness Trainings“ mit kleinen, aber häufigen Lernmodulen ein.

Vielfältige Trainings sind wichtig

Die zentrale Lernplattform bietet eine Auswahl von über 1.000 Trainingseinheiten. Aus der Lernbibliothek werden in Abständen neue Module für den Rhein-Kreis Neuss freigegeben. Zuletzt wurde speziell zu dem Thema „Social Engineering“ informiert.

Social Engineering zu verstehen ist für alle wichtig, denn viele haben bei der Arbeit einen Kontakt mit sonst unbekannten Personen. Hat darunter ein Hacker erst einmal genügend Vertrauen gewonnen, folgen E-Mails mit gefährlichen Inhalten. Die erste Hürde für eine Cyberattacke ist überwunden.

Phishing testen und melden

Alle Mitarbeiter/innen müssen lernen, die Vertraulichkeit einer Nachricht mit Links oder den Anhängen richtig einzuschätzen. Das Lernportal erzeugt deshalb bewusst falsche Phishing-Mails an alle Beschäftigte. Solche Maßnahmen werden als „Phishing Kampagne“ bezeichnet.

Wer gut aufpasst meldet die auffälligen E-Mails über einen Melde-Button im Mailpropgramm. Wichtig ist als Effekt, dass diese Maßnahme die Aufmerksamkeit für alle E-Mails hoch hält.

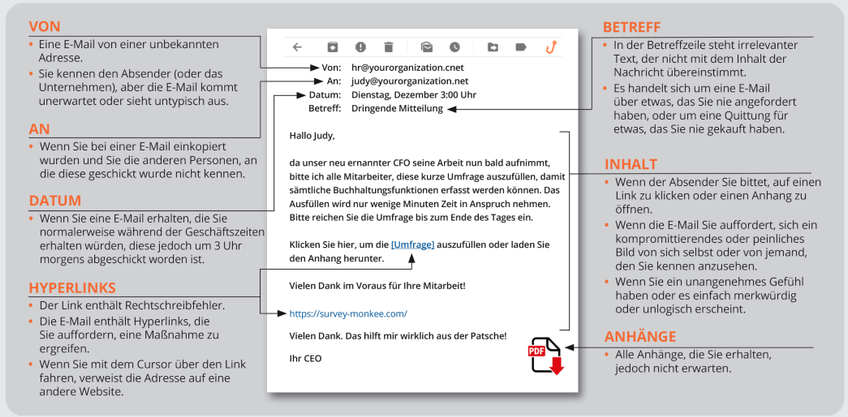
Ein Video informiert über die Meldefunktion von verdächtigen E-Mails

Eine hohe Sensibilität für den richtigen Umgang mit allen E-Mails bleibt eine ganz wichtige Herausforderung, die alle Beschäftigte betrifft und beachten müssen.

SIE sind ein Ziel!

Cyberkriminelle geben nicht auf, bevor Sie bekommen, was sie wollen. Sie wissen, dass der einfachste Zugang zur Verwaltung nicht das Hacken ist, sondern dass die User dazu gebracht werden, sie hereinzulassen. Die Mails sollten deshalb nach bestimmten Anzeichen hinterfragt werden.

Phishing ist die häufigste Form von Social Engineering. Im Folgenden sehen Sie sieben Bereiche in einer E-Mail und die entsprechenden Warnsignale.



Quelle: KnowBe4

Quelle: KnowBe4

Wachsam bleiben
Poster aus dem Security Awareness Training für den Rhein-Kreis Neuss

09 Anwendungssicherheit
auf dem Prüfstand

Bevor es an den Start geht

Für jedes neu geschaffene Programm wünscht sich die Entwicklung, dass die Anwendung den höchsten Qualitätsstandards entspricht. Durch Code-Reviews und ausführliche Tests wird weitestgehend sichergestellt, dass alles wie vorgesehen funktioniert und Fehler entdeckt werden.

Ein wichtiger Bestandteil ist dabei das Prüfen auf Sicherheitslücken. Diese Tests zu vernachlässigen kann im Nachhinein Rollbacks erfordern oder Gefahren für die Anwender und die Systeme mit sich bringen.

Schwachstellen erfordern Updates

Selbst bei best entwickelten Programmcodes werden täglich neue Schwachstellen entdeckt. Anwendungen, die bis heute noch als sicher galten, müssen bei Sicherheitsmängeln neu überarbeitet werden und erfordern neuere Programmversionen. Cyberkriminelle suchen bewusst und oft automatisiert nach solchen Sicherheitslücken.

Programmschwächen derart stellen eine unmittelbare Bedrohung dar und müssen aufgedeckt werden, bevor eine Anwendung freigegeben wird.

Angiffe der Cyberkriminellen verstehen lernen

Angreifer und Entwickler handeln grundsätzlich unterschiedlich. Entwickler haben die „Use Cases“, die Sicht eines Anwendungsszenarios, im Fokus. Angreifer hingegen denken in „Misuse Cases“. Cyberkriminelle wollen eine Anwendungslücke finden und für einen Angriff nutzen.

Oft reicht eine einzige Schwachstelle in einer Anwendung für eine Cyber-Attacke. Daher sind Tools unerlässlich, um die Sicherheit auf der Entwicklungsebene zu verbessern. Developer sollten daher selbst versuchen, mit den Werkzeugen und Techniken potenzieller Angreifer in ihre eigenen Systeme einzudringen.

Penetrationstests sind erforderlich

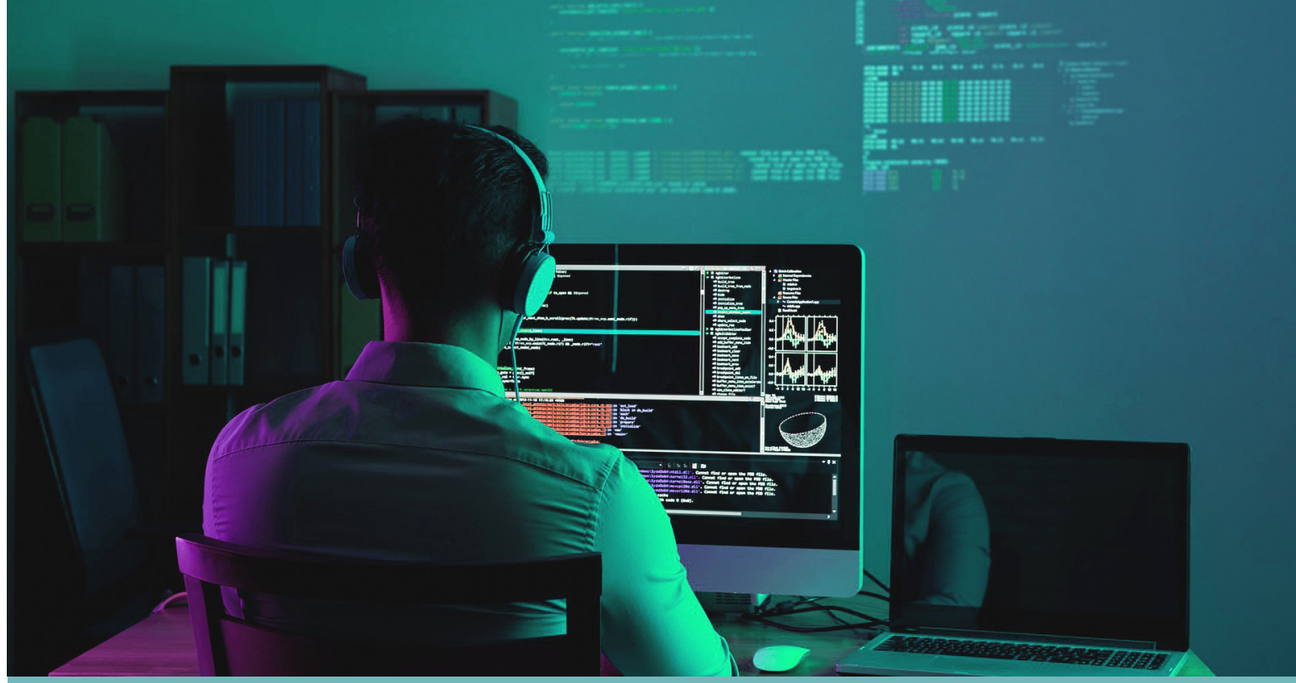
Penetrationstests sind kein Ersatz für Standardtests, Scans oder andere Überprüfungen, die zu den gängigen Sicherheitspraktiken gehören. Sie sind eine notwendige Ergänzung zu diesen Verfahren und können Schwachstellen aufzeigen, die sonst nicht in Betracht gezogen würden. Selbst ein Penetrationstests kann keine dauerhafte Sicherheit bieten. Als Momentaufnahme bestätigen sie jedoch den aktuellen Schutzzustand.

Der Versuch, in die eigenen Anwendungen mit den Tools einzubrechen, die von kriminellen Hackern eingesetzt werden, führt bei Developern zu einem erweiterten Problembewusstsein. Anstatt sich darauf zu konzentrieren, dass die beabsichtigten Verwendungen einer Anwendung möglich sind, konzentrieren sich die Entwickler zusätzlich auch auf eine unbeabsichtigte Ausführung.

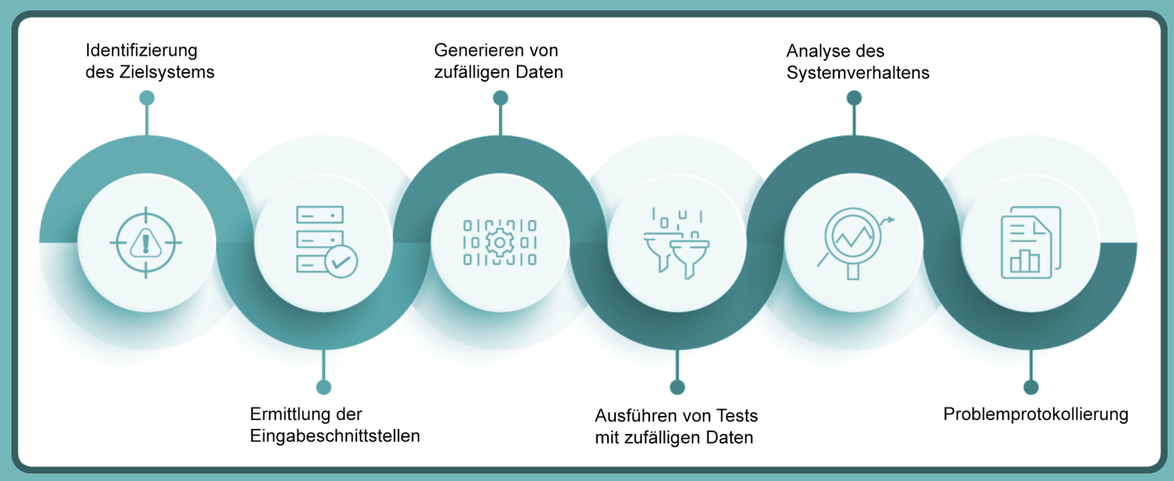
Fehler erkennen und Hacker verstehen

Sehr oft handelt es sich um Fehler im Software- Design oder in der Ablauflogik, die durch dieses Design vorgegeben werden. Der Code ist zwar entsprechend der Spezifikation geschrieben, aber durch die Definition an sich entstehen unvorhergesehene Möglichkeiten für Missbrauch und Verstöße. Diese Schwachstellen sind nicht die Schuld der Entwickler, aber sie sind mit verantwortlich für die Sicherheit der Anwendung.

Das Wissen über die Vorgehensweise von Hackern, vor allem, wenn man ihre Angriffswege und Werkzeuge selbst ausprobiert, schärft das Bewusstsein der Spezialisten für mögliche Schwachstellen in den von ihnen erstellten Codes. Je mehr Probleme bei der Entwicklung von Anwendungen bereits im Vorfeld vermieden werden, desto besser.



Praxisbeispiel
Eigener Anwendungstest mit “Fuzzing”



Quelle: FORTRA Beyond Security

Fuzzing bzw. Fuzz-Testing ist eine vom Wissenschaftler Barton Miller entwickelte Methode, um Software systematisch auf Schwachstellen zu testen. Dabei werden alle möglichen Schnittstellen der Dateneingabe automatisiert aufgerufen und mit Zufallsdaten gespeist. Dieser Prozess kann sich je nach Größe des untersuchten Software-Projekts über Stunden oder Tage hinziehen.

Ziel des Fuzz-Testing ist es, festzustellen, ob für alle möglichen Eingabevarianten die notwendigen Reaktionen im Programm hinterlegt sind. Sinnlose oder fehlerhafte Eingaben sollten möglichst durch Fehlerbehandlungsroutinen aufgefangen werden. Sind diese nämlich für bestimmte Eingaben nicht vorhanden oder funktionieren nicht richtig, kann ein Programmabsturz die Folge sein.

Dies ist eine bewährte Testmethode zum Ermitteln von Schwachstellen in Software. So werden zum Beispiel Webanwendungen per Cross-Browser-Testing auf ihre Funktionsfähigkeit in verschiedenen Webclients bzw. Browserversionen getestet.

Jahresbericht
IT-Sicherheit 2022/2023

Bildinhalte / Quellen

Bundesamt für Sicherheit
in der Informationstechnik (BSI) (S.4,5,11,17)
Bitdefender (S.12,13)
FORTRA (S.21)
Greenbone Networks (S.11)
Knowbe4 (S.18,19)
Microsoft (S.15)
Pixabay.com - CCO Lizenz (S.9,11,13,14,15,16,21W)
Rhein-Kreis Neuss (S.18)

Impressum

Rhein-Kreis Neuss
Der Landrat
Lindenstraße 2-16
41515 Grevenbroich

Frank Meger
IT-Sicherheitsbeauftragter

Telefon: 02181 - 601 1105
E-Mail: frank.meger@rhein-kreis-neuss.de

Bericht zur IT-Sicherheit

beim Rhein-Kreis Neuss

Resilienz in der IT-Sicherheit

Stand: 04.05.2023

Inhalt

Cyberkriminalität zeigt sich kreativ und nutzt modernste technologische Angriffsmethoden.

IT-Verantwortliche und alle Beschäftigten müssen auf die potentiellen Gefahren vorbereitet sein.

01 l Die heutige Bedrohungslandschaft

- Die Angreifer - wer sie sind und was sie tun
- E-Mail- und Multi-Channel Phishing
- Ausnutzen von Schwachstellen

02 l Aufgabenfokus 2022/23

- Schutzniveau der Daten
- Managed Detection & Response
- Schwachstellenanalyse
- Resilienz ausbauen

03 l Ausbau der IT-Sicherheit

- Dokumentation und Leitlinien
- Stärken der Sicherheitskultur
- Maßnahmen auf dem Prüfstand

01

Die heutige Bedrohungslandschaft

„Angreifer müssen oft nur eine Hürde überwinden, um Erfolg zu haben - den Menschen.“

Ulf Baltin, Senior Director, Enterprise Sales DACH bei BlackBerry

Steckbriefe der Angreifer

Cyberkriminelle greifen als einzelne Akteure, im staatlichen Auftrag oder in organisierten Gruppen an. Beim “ Big Game Hunting” konzentrieren sich spezialisierte Teams auf lukrative Angriffsziele.

Bekannte Angreifer

Über 200 Hackergruppen, einzelne Akteure, Hacktivisten etc.

Neu identifiziert

Ca. 20 Prozent Zuwachs im vergangenen Jahr.

Es braucht nicht lange

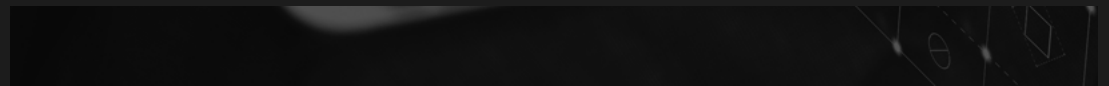
vom Starten des Hackerangriffs bis zur flächen-deckenden Auswirkung einer Cyberattacke.

Oft lange vorbereitet, danach geht es schnell

Im Durchschnitt hat ein Hackerangriff in 84 Minuten sein Schadensziel erreicht. 2021 waren es noch 98 Minuten.

Analyse des Schadens durch IT-Forensik

Eine forensische Analyse setzt eine einwandfreie Beweissicherung der betroffenen Systeme voraus.



Angriffsziele Phishing und Schwachstellen

Angreifer konzentrieren sich auf Schwachstellen - technischer und menschlicher Art.
Das Implementieren von Malware ist im ersten Schritt gar nicht notwendig.

Dauerbrenner Phishing

Cyberkriminelle werden auch 2023 auf die emotionale Manipulation ihrer Opfer setzen. Menschliche Verhaltensmuster lassen sich durch Vertrauen, Dringlichkeit ud Autorität manipulieren.

Durch heutige KI können ausgefeilte Nachrichten automatisch erstellt oder Stimmen simuliert werden.

Multichannel Phishing

Phishing-Angriffe sind inzwischen vielschichtiger.

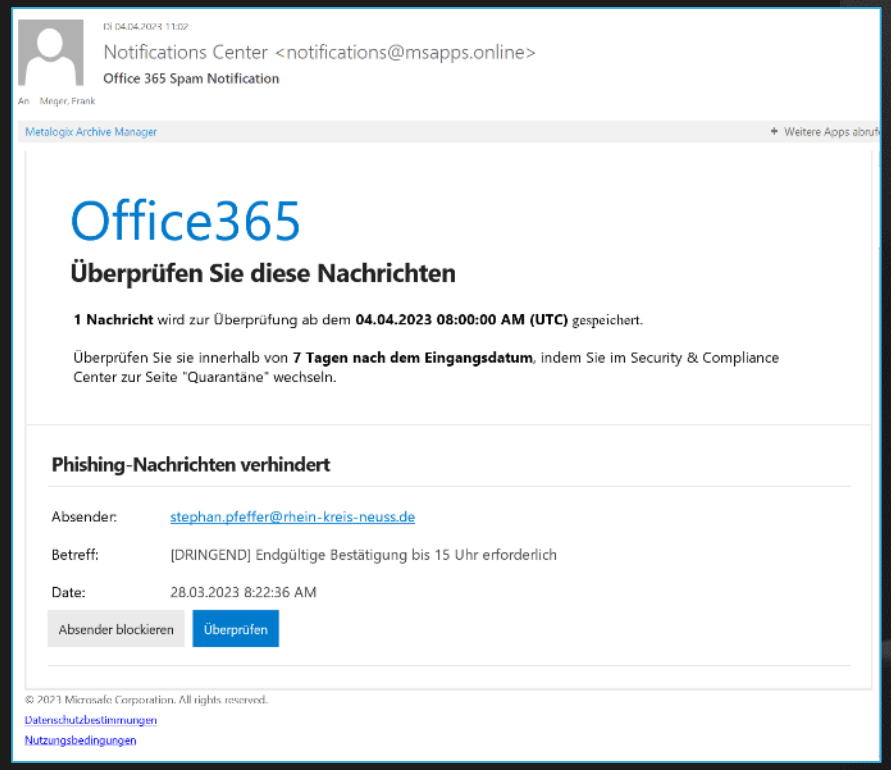
Zur klassischen E-Mail sind soziale Netzwerke, kombinierte Kontaktaufnahmen per Video, Telefon, SMS und professionelle Plattformen wie MS Teams, LinkedIN etc. hinzugkommen.

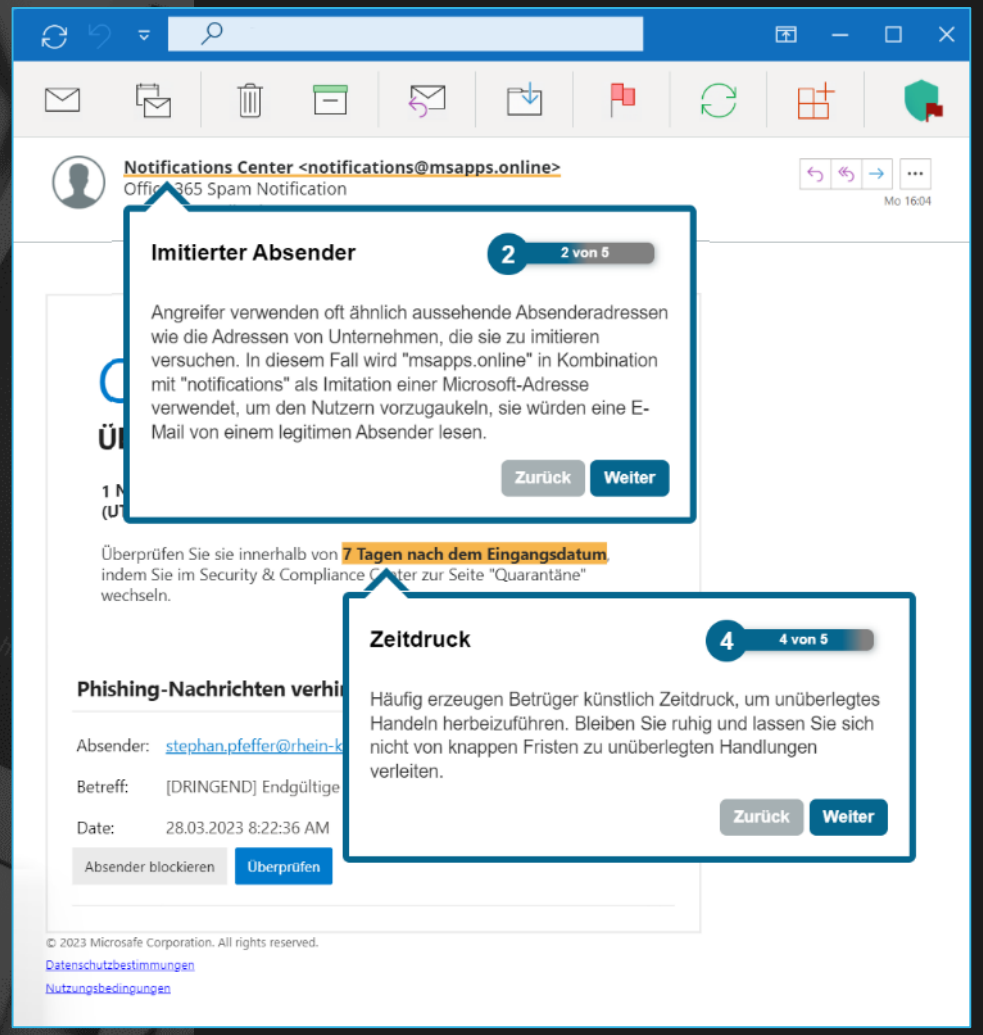
Bekannte Schwachstellen

Über 100.000 Schwachstellen sind in IT-Systemen bekannt. Kommunale Warndienste informieren über neu bekannte Sicherheitslücken.

Zero-Day-Schwachstellen sind Sicherheitsfehler, die der Öffentlichkeit bekannt wurden, bevor ein Patch zur Behebung des Fehlers veröffentlicht ist.

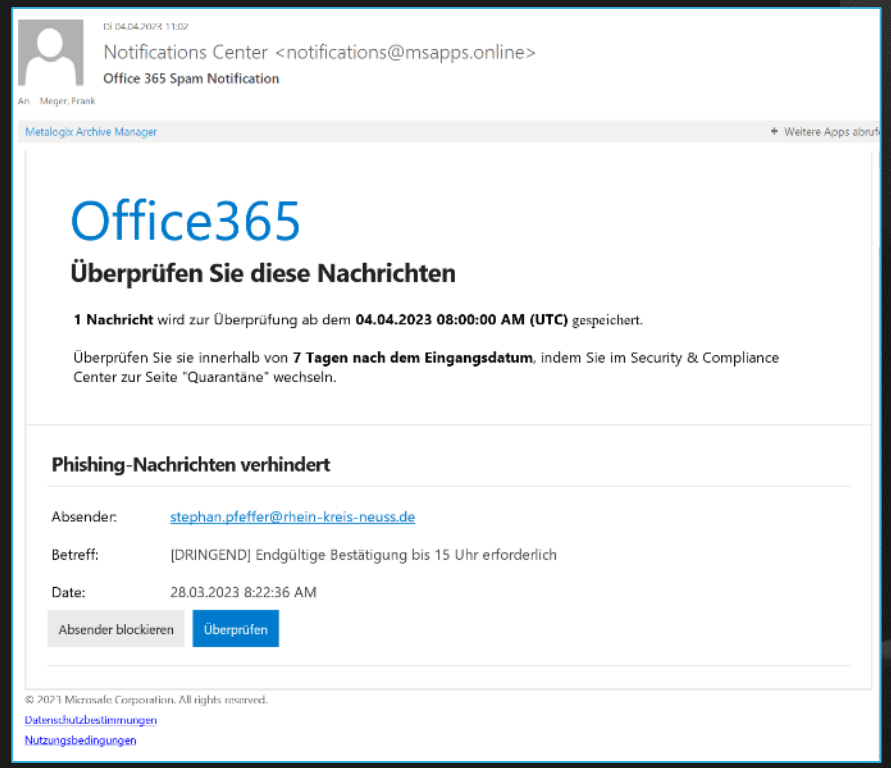
Phishing – jeder ist gefragt

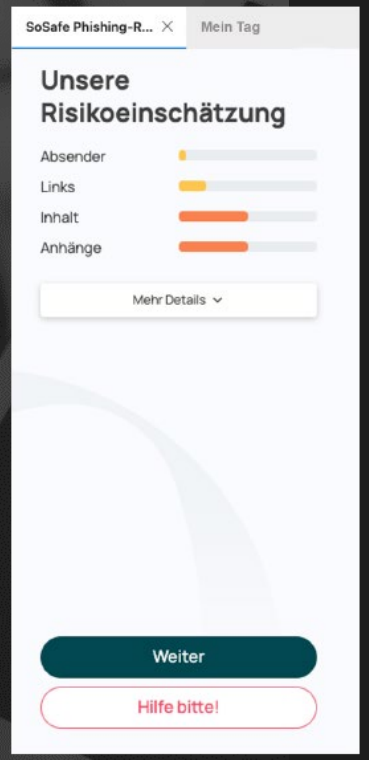


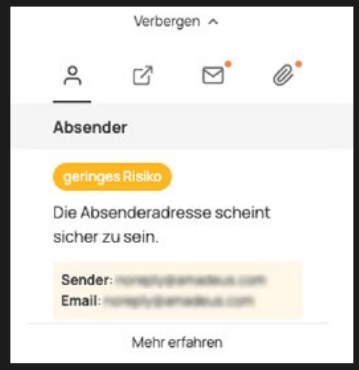


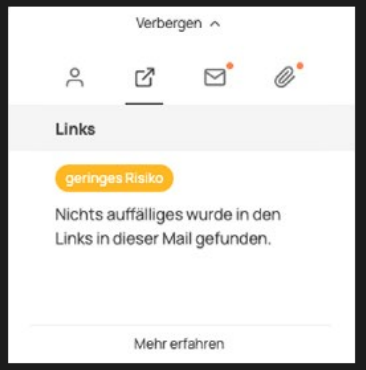
Phishing Mails sind zunehmend sehr professionell und zutreffend vorbereitet. Auch die E-Mail-Signaturen der vermeintlichen Absender werden hochwertig simuliert.

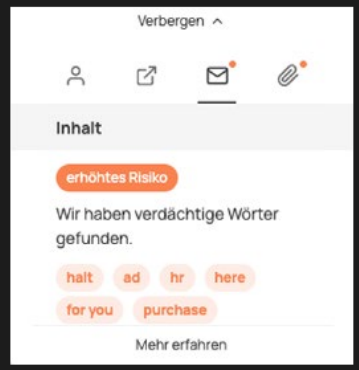
Phishing – jeder ist gefragt

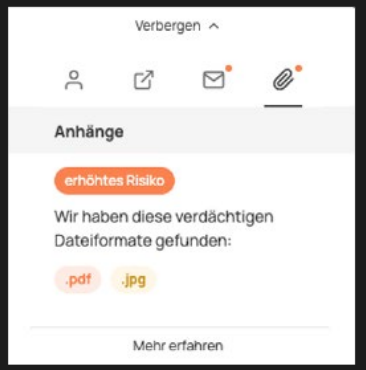












Integrationen im Mail-Programm können helfen, das Risiko einer Nachricht besser einzuschätzen.

Angriffe auf Schwachstellen

Irgendwo hakt es immer, nie ist alles auf dem aktuellsten Stand.

Immer häufiger werden Updates erforderlich, um alle Sicherheits-lücken zu schließen.

Das Auslassen von Aktualisierungen wird zum Sicherheitsrisiko.

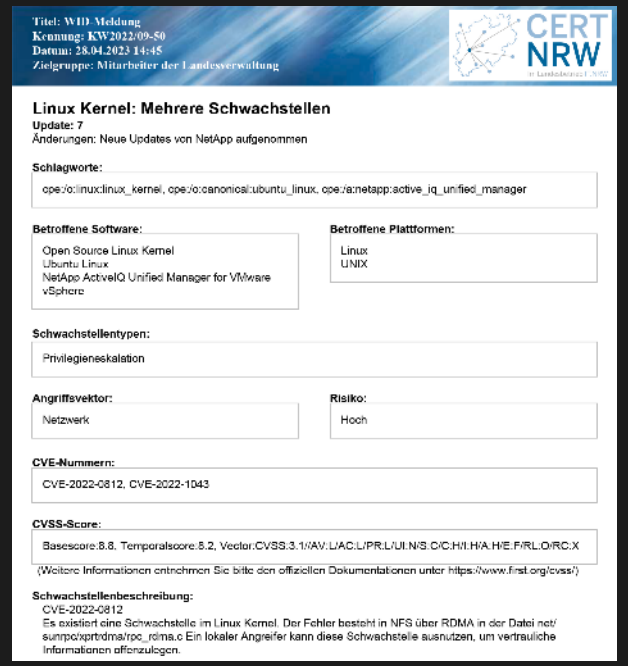
KWID CERT-NRW

Warnungen zu Sicherheitslücken werden als E-Mail gemeldet.

+

Vulnerability Scan

Scanprozesse suchen nach über 100.000 bekannten Schwachstellen.



Titel: WID-Meldung
Kennung: KW2022/09-50
Datum: 28.04.2023 14:45
Zielgruppe: Mitarbeiter der Landesverwaltung

CERT NRW

Linux Kernel: Mehrere Schwachstellen

Update: 7
Änderungen: Neue Updates von NetApp aufgenommen

Schlagworte:
cpe:/o:linux:linux_kernel, cpe:/o:canonical:ubuntu_linux, cpe:/a:netapp:active_iq_unified_manager

Betroffene Software:
Open Source Linux Kernel
Ubuntu Linux
NetApp ActiveIQ Unified Manager for VMware vSphere

Betroffene Plattformen:
Linux
UNIX

Schwachstellentypen:
Privilegieneskalation

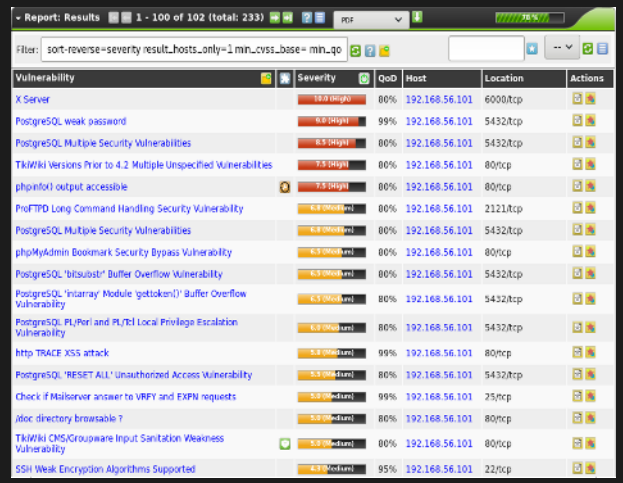
Angriffsvektor:
Netzwerk

Risiko:
Hoch

CVE-Nummern:
CVE-2022-0812, CVE-2022-1043

CVSS-Score:
Basescore:8.8, Temporalscore:8.2, Vector:CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:F/RL:O/RC:X
(Weitere Informationen entnehmen Sie bitte den offiziellen Dokumentationen unter https://www.first.org/cvss/)

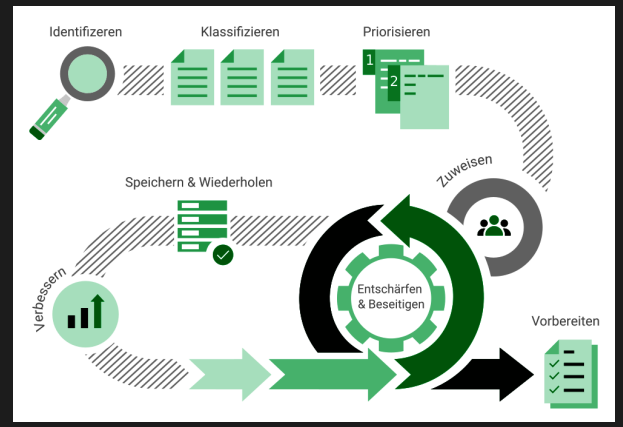
Schwachstellenbeschreibung:
CVE-2022-0812
Es existiert eine Schwachstelle im Linux Kernel. Der Fehler besteht in NFS über RDMA in der Datei net/sunrpc/xprtrdma/rpc_rdma.c Ein lokaler Angreifer kann diese Schwachstelle ausnutzen, um vertrauliche Informationen offenzulegen.



Report: Results 1 - 100 of 102 (total: 233)

Filter: sort-reverse=severity result_hosts_only=1 min_cvss_base= min_qo

Vulnerability	Severity	QoD	Host	Location	Actions
X Server	10.0 (High)	80%	192.168.56.101	6000/tcp	
PostgreSQL weak password	9.0 (High)	99%	192.168.56.101	5432/tcp	
PostgreSQL Multiple Security Vulnerabilities	8.5 (High)	80%	192.168.56.101	5432/tcp	
TikiWiki Versions Prior to 4.2 Multiple Unspecified Vulnerabilities	7.5 (High)	80%	192.168.56.101	80/tcp	
phpinfo() output accessible	7.5 (High)	80%	192.168.56.101	80/tcp	
ProFTPD Long Command Handling Security Vulnerability	6.8 (Medium)	80%	192.168.56.101	2121/tcp	
PostgreSQL Multiple Security Vulnerabilities	6.8 (Medium)	80%	192.168.56.101	5432/tcp	
phpMyAdmin Bookmark Security Bypass Vulnerability	6.5 (Medium)	80%	192.168.56.101	80/tcp	
PostgreSQL 'bitsubstr' Buffer Overflow Vulnerability	6.5 (Medium)	80%	192.168.56.101	5432/tcp	
PostgreSQL 'intarray' Module 'gettoken()' Buffer Overflow Vulnerability	6.5 (Medium)	80%	192.168.56.101	5432/tcp	
PostgreSQL PL/Perl and PL/Tcl Local Privilege Escalation Vulnerability	6.0 (Medium)	80%	192.168.56.101	5432/tcp	
http TRACE XSS attack	5.8 (Medium)	99%	192.168.56.101	80/tcp	
PostgreSQL 'RESET ALL' Unauthorized Access Vulnerability	5.5 (Medium)	80%	192.168.56.101	5432/tcp	
Check if Mailserver answer to VRFY and EXPN requests	5.0 (Medium)	99%	192.168.56.101	25/tcp	
/doc directory browsable ?	5.0 (Medium)	80%	192.168.56.101	80/tcp	
TikiWiki CMS/Groupware Input Sanitation Weakness Vulnerability	5.0 (Medium)	80%	192.168.56.101	80/tcp	
SSH Weak Encryption Algorithms Supported	4.3 (Medium)	95%	192.168.56.101	22/tcp	



02
Aufgabenfokus 2022/23

„IT-Sicherheit ist eine Reise und ein Prozess –
ein permanentes Anpassen.“

Ulrich Irnich, CIO und Modernization Garage Director, Vodafone Deutschland

Managed Detection & Response 24/7

Cyber-Abwehr rund um die Uhr:
MDR-Dienste vereinen Cybersicherheit für Endpoints aller Systeme sowie auch Netzwerk- und Sicherheitsanalysen
Bedrohungen müssen jederzeit und zuverlässig erkannt und im Stile eines SOCs abgewehrt werden.

01
Vorbeugender Schutz

- Präventionstechnologien einsetzen, um Ereignisse und Abläufe zu protokollieren.
- 24x7x365 Bedrohungssuche, Threat Intelligence und Bedrohungsanalysen
- Auf Taktiken, Techniken und Prozeduren der Angreifer vorbereiten.

02
Erweiterte Erkennung

- Ereigniskorrelation über Endpoints und Netzwerke hinweg
- Global Threat Intelligence: Sensoren über die eigene IT hinaus bewerten.
- Proaktive Überwachung, passend zu den eigenen, kritischen IT Prozessen.

03
Reaktion & Berichtswesen

- Meldung von Ereignissen an die IT Verantwortlichen
- Reaktion in Ausnahmemsitationen durch den externen Service
- Bewertung der Lage und notwendige Sicherheitsanpassungen

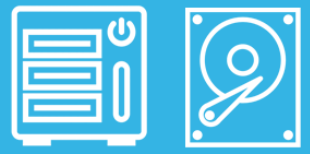
Immutable Storage

Backups müssen geschützt werden.

3-2-1-1-0 Strategie

3
verschiedene Kopien der Daten

2
verschiedene Medien



1
Offsite Speicherung

1
ist offline

0
Verifikation erfolgreicher Wiederherstellung

Cyberresilienz stärken

Die öffentliche Verwaltung besitzt eine essenzielle Verantwortung und muss bedeutende Services für die Bevölkerung unterbrechungsfrei gewährleisten.

Eine cybersicherheitsbewusste Verwaltung ist sich dieser Verantwortung und der Risiken bewusst.

Kernanforderungen

- Cybersicherheit muss 24/7 gewährleistet sein.
- Neue digitale Dienste müssen müssen geprüft werden.
- Eine IT mit maximaler Robustheit ist erforderlich.

Im Fokus: Systeme und Kundendaten

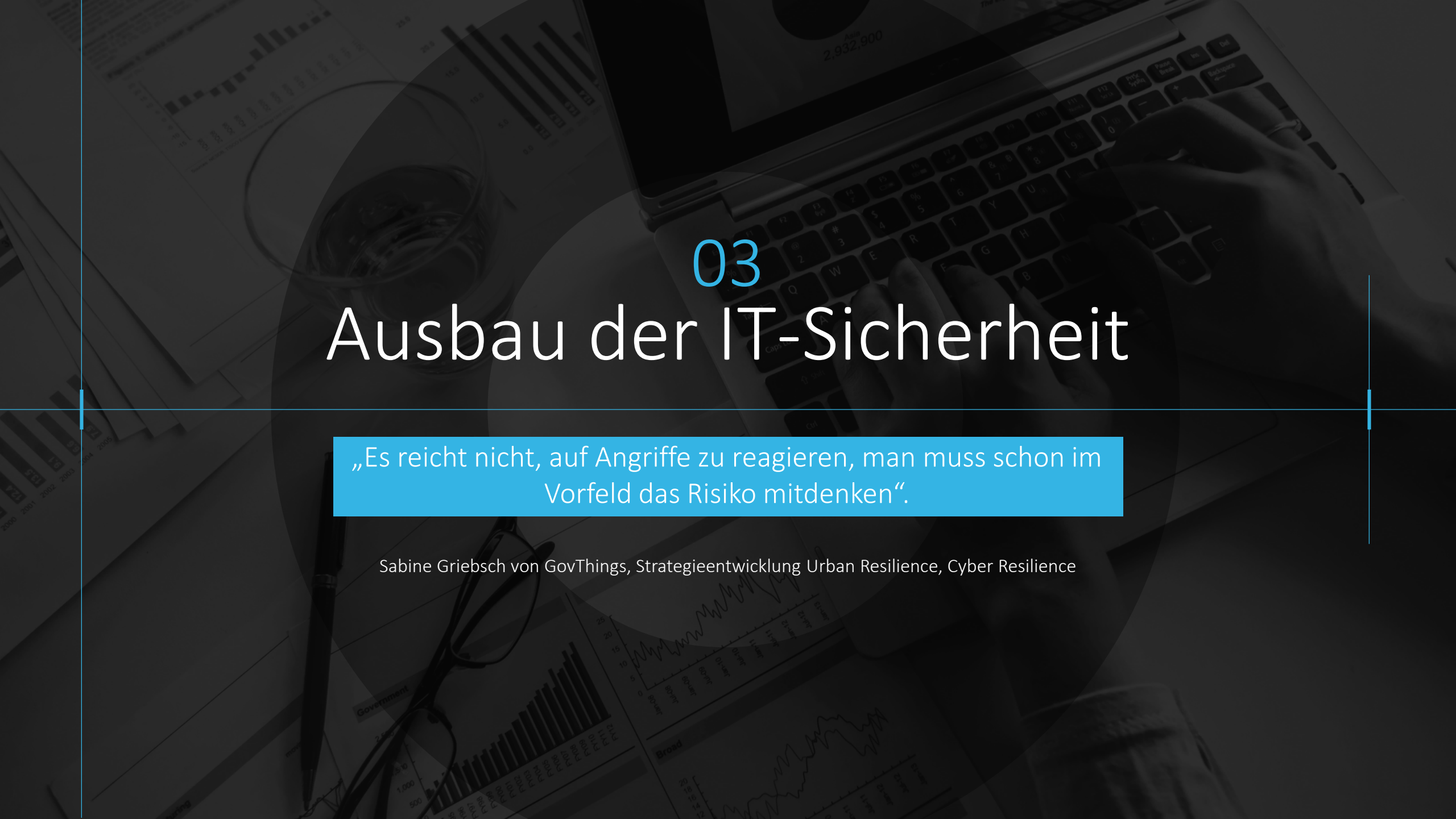
Der Grad der Widerstandsfähigkeit ermisst sich in der Gewährleistung von Vertraulichkeit, Integrität sowie der Verfügbarkeit von Daten und hoheitlichen Diensten.

Den Geschäftsbetrieb sicherstellen

Ergreifen Sie alle Schutzmaßnahmen, um eine beständige, unterbrechungsfreie Geschäftskontinuität zu schaffen.

Verteidigungsstrategie

Dies gelingt durch spezialisierte Kontrollmechanismen und durch generische Maßnahmen, wie z.B. einer starken Verschlüsselung und Authentifizierung.



03
Ausbau der IT-Sicherheit

„Es reicht nicht, auf Angriffe zu reagieren, man muss schon im Vorfeld das Risiko mitdenken“.

Sabine Griebsch von GovThings, Strategieentwicklung Urban Resilience, Cyber Resilience

4 Schritte,
um vorbereitet zu sein.

01

Management der Informationssicherheit

- Ein IT Verbund besteht aus unterschiedlichen Assets wie IT Systemen, IT Prozessen und den schuzbedürftigen Daten. Dazu braucht es zudem verbindliche organisatorische Sicherheits-vorgaben.
- Der Rhein-Kreis Neuss spricht sich für eine vollumfängliche Umsetzung der Vorgaben des BSI (hoher Schutzbedarf) aus.
- Ein vollwertiges Information Security Management System soll die Dokumentationsgrundlage aller Schutzvorgaben und IT-Leitlinien für den Rhein-Kreis Neuss sein.

4 Schritte,
um vorbereitet zu sein.

02 Identitäten müssen geschützt sein.

- Wir müssen den Identitätsschutz priorisieren.
- Die Zunahme von Malware-freien Angriffen und Social Engineering erfordern einen integrierten Identitätsschutz mit enger Korrelation zwischen Endpunkten, Benutzerinformationen und Daten.
- Die IT muss Maßnahmen zur Echtzeit-Verhinderung von verdächtigen Verhalten und dem Missbrauch von Dienstkonten ergreifen.

4 Schritte,
um vorbereitet zu sein.

03

- Auf den Ernstfall vorbereitet sein
- Im Fall einer Cyberattacke trägt eine schnelle und effektive Reaktion entscheidend zur Schadensbegrenzung bei. Für den Rhein-Kreis Neuss soll ein „Incident Response Management“ etabliert werden.
- Ein formeller Notfallplan sollte die Reaktionen definieren, damit im Fall einer Cyberattacke Die Beteiligten ihre Aufgaben kennen.
- Ein Plan zur Aufrechterhaltung des Geschäftsbetriebs erfordert eine Übersicht aller Technologien und physischen Ressourcen sowie eine definierte Strategie von Datenwiederherstellungsprozessen.

4 Schritte,
um vorbereitet zu sein.

04

Übung macht den Meister.

- Das Aufspüren und Stoppen von Angriffen ist ohne Sicherheitsteams und Tests nichts wert.
- Sicherheits- und Pentrationstests müssen intensiviert werden, damit die IT die Wirkung der Schutzmaßnahmen überprüfen kann.
- Alle Beschäftigten müssen gut trainiert werden. Das Erkennen von Phishing Mails liegt als erstes in der Hand der Mitarbeiter:innen.
- Für die Mitarbeiter:innen müssen Awareness Trainings vorbereitet werden.

Danke

für Ihre Zeit und
Ihre Aufmerksamkeit.

Frank Meger, IT-Sicherheitsbeauftragter

frank.meger@rhein-kreis-neuss.de

Erstellung eines Wirtschaftsförderungs-konzepts für den Rhein-Kreis Neuss

Präsentation für den IDS-Ausschuss
im Rhein-Kreis Neuss

Bild: Stocksy – Martí Sans

...

Neuss | 04.05.2023

Agenda

1. Prozess der Konzeptentwicklung
2. Kernergebnisse aus IST- und SOLL-Analyse
3. Empfehlungen aus der Echokammer
4. Empfehlungen: Leitthemen, Handlungsfelder & Struktur

Agenda

1. Prozess der Konzeptentwicklung
2. Kernergebnisse aus IST- und SOLL-Analyse
3. Empfehlungen aus der Echokammer
4. Empfehlungen: Leitthemen, Handlungsfelder & Struktur

Ziele, Erhebungselemente und Ergebnisse

ZIELE

1. Strategischer & kreisweiter Orientierungsrahmen
2. Entwicklungsimpulse für den Wirtschafts- & Innovationsraum RKN
3. Handlungsfelder und Leitprojekte
4. Strategischer Rahmen für die Arbeit und Struktur der Wirtschaftsförderung

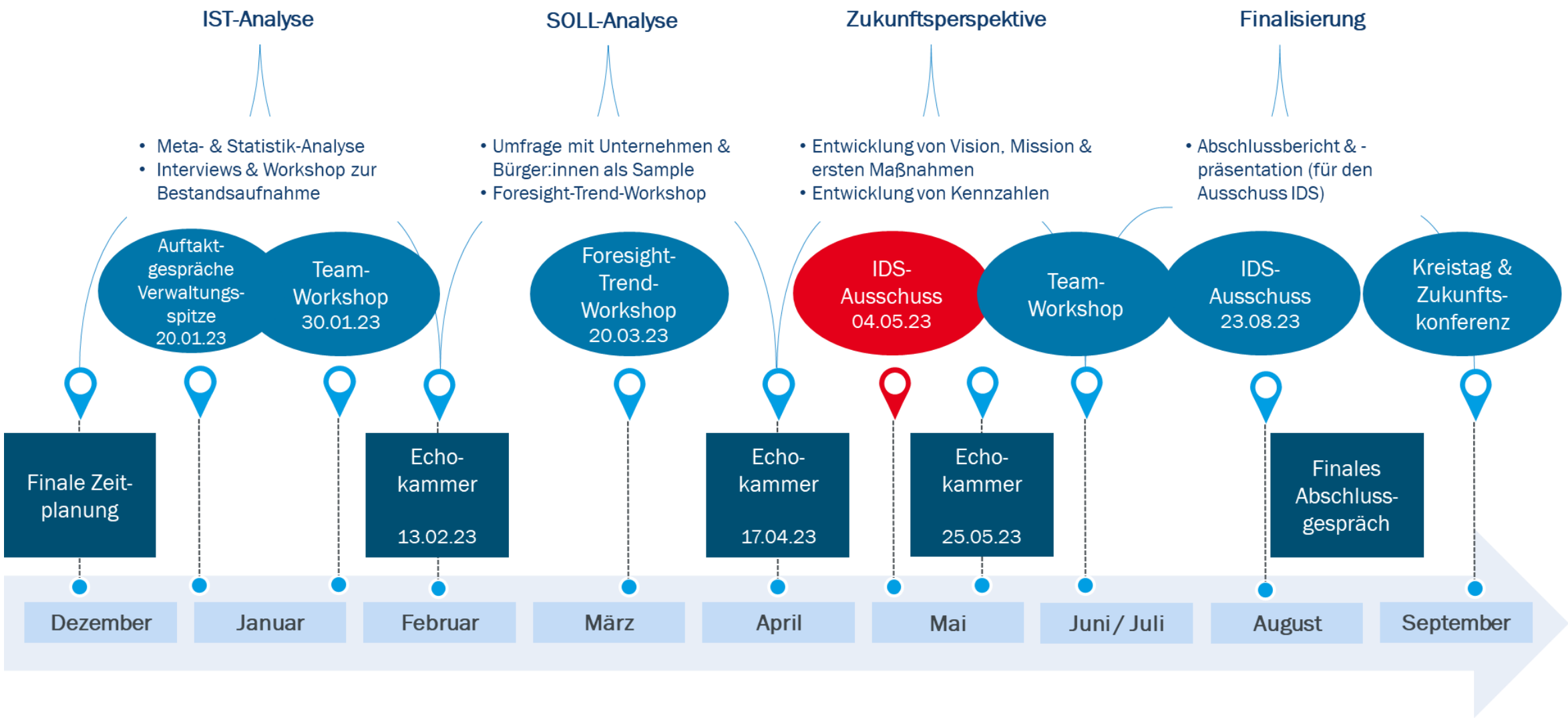
ERHEBUNGSELEMENTE

a. Meta-Analyse
b. Statistische Analyse
c. Benchmark-Analyse
d. Bestandsaufnahme
e. Foresight-Trend-Workshop
f. Online-Umfrage
g. Echokammer

ERGEBNISSE

i. Vision & Mission
ii. Strategische Handlungsfelder
iii. Projektideen
iv. Konkretisierung der Projektideen
v. 6 – 8 Leitprojekte

Prozessübersicht im zeitlichen Verlauf



rhein kreis neuss

matrix prognos

Agenda

1. Prozess der Konzeptentwicklung
2. Kernergebnisse aus IST- und SOLL-Analyse
3. Empfehlungen aus der Echokammer
4. Empfehlungen: Leitthemen, Handlungsfelder & Struktur

Was zeichnet den Rhein-Kreis aus?

Impulse aus Indikatorenanalyse und Benchmark*-Vergleich

Breite Branchenvielfalt, aber besondere Herausforderung in der ökologischen Transformation durch **hohe Lokalisation der Energiewirtschaft und energieintensiver Industrien**

Dynamisches Innovationsgeschehen durch investitionsfreudige Wirtschaft, Zunahme des Gründungsgeschehens und der FuE-Beschäftigung, aber **Fachkräfte- & Nachwuchsmangel**
Investitionsquoten 2020: 15,2% (RKN), ~9,7% (DE, NRW); FuE-Personal in der Wirtschaft 2011-2019: +61% (RKN), +19% (NRW)

Hohe Wirtschaftskraft, aber **abschwächende Entwicklung** in den letzten Jahren, bereits vor Corona Entwicklung der BWS**, 2018-2019: -1,6% (RKN), +1,9% (NRW), +3,1% (DE), 2011-2019: +22,1% (RKN), +24,7% (NRW), + 29,5% (DE)

Eher geringe Impulse für die Digitalisierung der Wirtschaft durch relativ schwaches Wachstum digitaler Impulsgeber und niedrig lokalisierte Digitalwirtschaft
Entwicklung der Beschäftigtengruppe digitale Impulsgeber 2013-2021: +3,1% (RKN), +10,3% (NRW), +14,1% (DE)

Keine **klare Aufgaben- & Ressourcenverteilung sowie Verständigung auf gemeinsame Ziele** im RKN im Sinne einer regional-kooperativen Zusammenarbeit erkennbar
Landkreis Esslingen: Gründung der Wirtschaftsförderung Region Stuttgart GmbH im Jahr 1995

AUFGABEN FÜR DIE FÖRDERUNG DES WIRTSCHAFTSSTANDORTS?

- Transformation der energieintensiven Industrie
- Fachkräfte- & Nachwuchsarbeit adressieren
- Näher an Unternehmen sein, adäquate Dienstleistungen aufbauen und Business Development voranbringen
- Impulse für die Digitalisierung der Wirtschaft setzen
- Interkommunale Zusammenarbeit stärken

*Deutschland, Nordrhein-Westfalen, Rheinisch-Bergischer Kreis, Wetteraukreis, Landkreis Esslingen; ** LQ = *Der Lokalisationsquotient zeigt den branchenspezifischen Beschäftigtenanteil der Region im Bundesvergleich an. Im Bundesvergleich überdurchschnittlich spezialisierte Branchen der Region haben einen Lokalisationsgrad >1.; ***BWS = Bruttowertschöpfung

Foresight-Trend Workshops: Neue Welten, neue Anforderungen, neue Angebote!

AUFGABEN FÜR DIE FÖRDERUNG DES WIRTSCHAFTSSTANDORTS?

- Fachkräfte- und Nachwuchsarbeit adressieren
- Näher an Unternehmen sein, adäquate Dienstleistungen aufbauen und Business Development voranbringen
- Impulsgebung für Digitalisierung & Innovationen / Cross-Innovation
- Kooperative Zusammenarbeit in Netzwerken und fokussierten Formaten stärken

- **Aktive Begleitung von Transformationen** (Digitalisierung, Klimawandel, demogr. Wandel, Technologisierung)
  - Robotik und KI als Unterstützung der menschlichen Arbeitskraft
  - thematisch aktualisierte Fort- und Weiterbildungsangebote
- **Standortstärkung** im Sinne eines attraktiven Wirtschaftsstandorts für AN
  - Austausch zu neuen Aus- und Weiterbildungs- und Recruitingformaten
  - Informationen zu Fördermittelzugängen und Fördermittelberatung
  - Willkommens- und Integrationsinitiativen
  - arbeitnehmerfreundliche Positionierung des Wirtschaftsstandorts
- **Innovationsförderung** durch fokussierte Netzwerke (Cross-Innovation-Communities)
  - Fördermittelzugänge und Austausch zu Zukunftstechnologien
  - zielgerichtete & inhaltlich geprägte Netzwerkformate
  - weiterführende Innovationsinitiativen, vor allem durch Kooperationen zwischen Forschung, Verbänden, Schulen, Verwaltungen, Politik
- **Bürokratiebeschleunigung und Sprachrohr** zwischen Wirtschaft & Politik
  - vereinfachte Bürokratie, z.B. beschleunigte Genehmigungsverfahren
  - One-Stop-Agency zur Vereinfachung bürokratischer Verfahren
  - Interessenvermittlung durch die Wirtschaftsförderung

AUFGABEN FÜR DIE FÖRDERUNG DES WIRTSCHAFTSSTANDORTS?

- Fachkräfte- und Nachwuchsarbeit adressieren
- Erneuerbare Energien als Innovationstreiber verstehen & nutzen
- Näher an Unternehmen sein, adäquate Dienstleistungen aufbauen und Business Development voranbringen
- Impulse bei der Digitalisierung, nicht nur auf KI & Robotik richten, sondern auch auf 3D-Druck und VR

Bild: © iStock - alvarez

Impulse aus der Online-Befragung: Unternehmen

Risiko

Fachkräftemangel im Mittel der befragten Unternehmen eindeutig als **größtes Risiko** eingestuft

Chancen

Neben der Digitalisierung ist auch der zweite Faktor der Twin Transition als Markttreiber erkannt worden: **Erneuerbare Energien werden von den Befragten überwiegend als Chance gesehen**

Bedarfe aus Unternehmen

Die befragten Unternehmen sehen große Mehrwerte und Bedarfe beim **Zugang zu Förderprogrammen und Finanzierungsmöglichkeiten**

Zukunftstechnologien

Die **bedeutendsten Zukunftstechnologien** sind aus Sicht der befragten Unternehmen **KI, 3D-Druck, Robotik und VR**

rhein kreis neuss

matrix prognos

Impulse aus der Online-Befragung:
Bürger:innen

Der Rhein-Kreis Neuss in der Wahrnehmung

Die befragten BürgerInnen nehmen den **Rhein-Kreis als Arbeits- und Wohnort und Industriestandort** wahr. Ein scharfes wirtschaftliches Profil erkennen viele nicht.

Anforderungen an Arbeitgeber

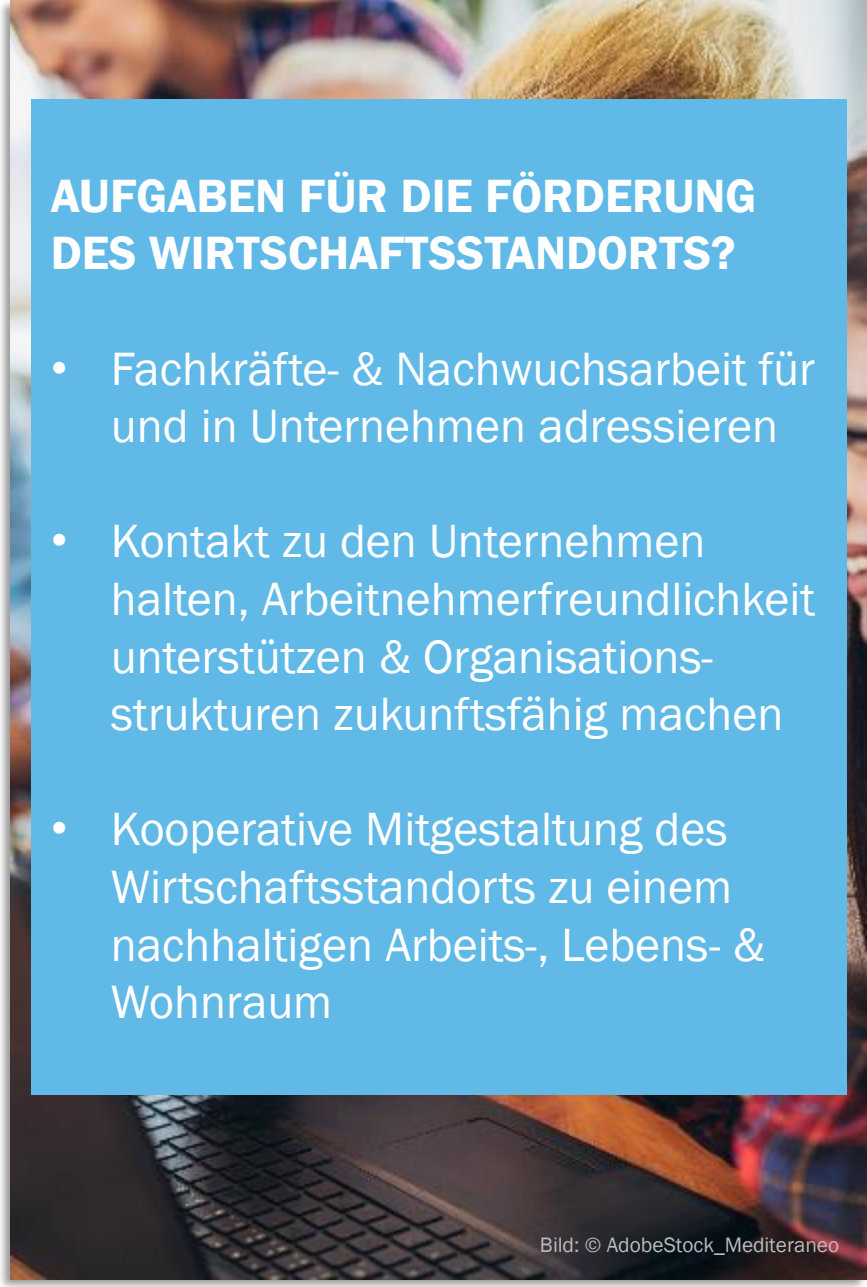
Digitale Arbeitsprozesse und neue Formen der Zusammenarbeit sehen viele Befragte bei Ihrem Arbeitgeber noch nicht gut umgesetzt

Anforderungen an Unternehmensförderung

Bestehende Unternehmen am Standort fördern, **Gründungs- und Start-Up-Kultur** entwickeln und **grüne Industrie** fokussieren.

Fachkräfteförderung in Unternehmen

Der **Zugang zu Weiterbildungsangeboten wird von den Befragten überwiegend sehr positiv eingeschätzt**. Neue Wege der Mitarbeitergewinnung und -bindung werden hingegen noch wenig gegangen.



AUFGABEN FÜR DIE FÖRDERUNG DES WIRTSCHAFTSSTANDORTS?

- Fachkräfte- & Nachwuchsarbeit für und in Unternehmen adressieren
- Kontakt zu den Unternehmen halten, Arbeitnehmerfreundlichkeit unterstützen & Organisations-strukturen zukunftsfähig machen
- Kooperative Mitgestaltung des Wirtschaftsstandorts zu einem nachhaltigen Arbeits-, Lebens- & Wohnraum

Bild: © AdobeStock_Mediteraneo

rhein kreis neuss

matrix prognos

Agenda

1. Prozess der Konzeptentwicklung
2. Kernergebnisse aus IST- und SOLL-Analyse
3. Empfehlungen aus der Echokammer
4. Empfehlungen: Leitthemen, Handlungsfelder & Struktur

Empfehlungen aus der Echokammer: Service- & kundenorientierte Wirtschaftsförderung oder „User-Centered-Design“

Klare und eindeutige Vision und Mission für den Wirtschaftsstandort
Benennung der Branchen und Zukunftsthemen für die zukünftige Arbeit in der Wirtschaftsförderung (Kompetenzen, Kooperationen, Orte und Arbeitsteilungen)

Commitment
Entscheidungsträgerinnen und Entscheidungsträger aus dem RKN stimmen der Strategie zu und akzeptieren die Inhalte als richtungsweisend, auch für das eigene Vorgehen

Vertrauensaufbau, Kooperationen & Ressourcen nutzen
Die zentralen Akteure für die strategische Entwicklung des Wirtschaftsstandort arbeiten zusammen, ziehen an einem Strang und bauen keine doppelten Angebotsstrukturen auf

Fokussierung auf maximal vier zentrale Handlungsfelder
Angebot stärker fokussieren, welches dann mit notwendigen Ressourcenkapazität erfolgreich bearbeitet werden kann.

Thematisch-strategische Innovationsförderung
Die Innovationsförderung geschieht weiterhin an strategisch wichtigen Themen. Netzwerkformate schließen sich hier an. Co-kreation als Leitbild.

AUFGABEN FÜR DIE FÖRDERUNG DES WIRTSCHAFTSSTANDORTS?

- Entwicklung einer zukunftsstabilen Vision und Mission
- Aufbau eines kooperativen Netzwerks für die Entwicklung des Wirtschaftsstandorts
- Wirtschaftsförderungen als Treiber strategischer Innovationsthemen
- Wirtschaftsförderung als Ort einer kontinuierlichen, kooperativen und innovativen Entwicklung eines zukunftsstabilen Wirtschaftsstandort

Besetzung der Echokammer

Peter Hornik	Digital Innovation Hub Düsseldorf/Rheinland GmbH
Patrick Gorzelanczyk	Stadt Korschenbroich – Wirtschaftsförderung
Axel Hebmüller	Hebmüller SRS Technik GmbH
Benjamin Küsters	Gartenhof Küsters GmbH
Marcus Longerich	Sparkasse Neuss
Florian Kriependorf	ScrapBees GmbH
Prof. Dr. Rüdiger Hamm	Hochschule Niederrhein
Jürgen Steinmetz	IHK Mittlerer Niederrhein
Martin Stiller	Rhein-Kreis Neuss, Dezernat III

Agenda

1. Prozess der Konzeptentwicklung
2. Kernergebnisse aus IST- und SOLL-Analyse
3. Empfehlungen aus der Echokammer
4. Empfehlungen: Leitthemen, Handlungsfelder & Struktur

Digitalisierung

Standortmarketing & Internationales

Fachkräfte- & Nachwuchssicherung

Eine Wirtschaftsförderung für den Stand- & Lebensort Rhein-Kreis Neuss: *vernetzt, kooperativ, fokussiert & innovativ*

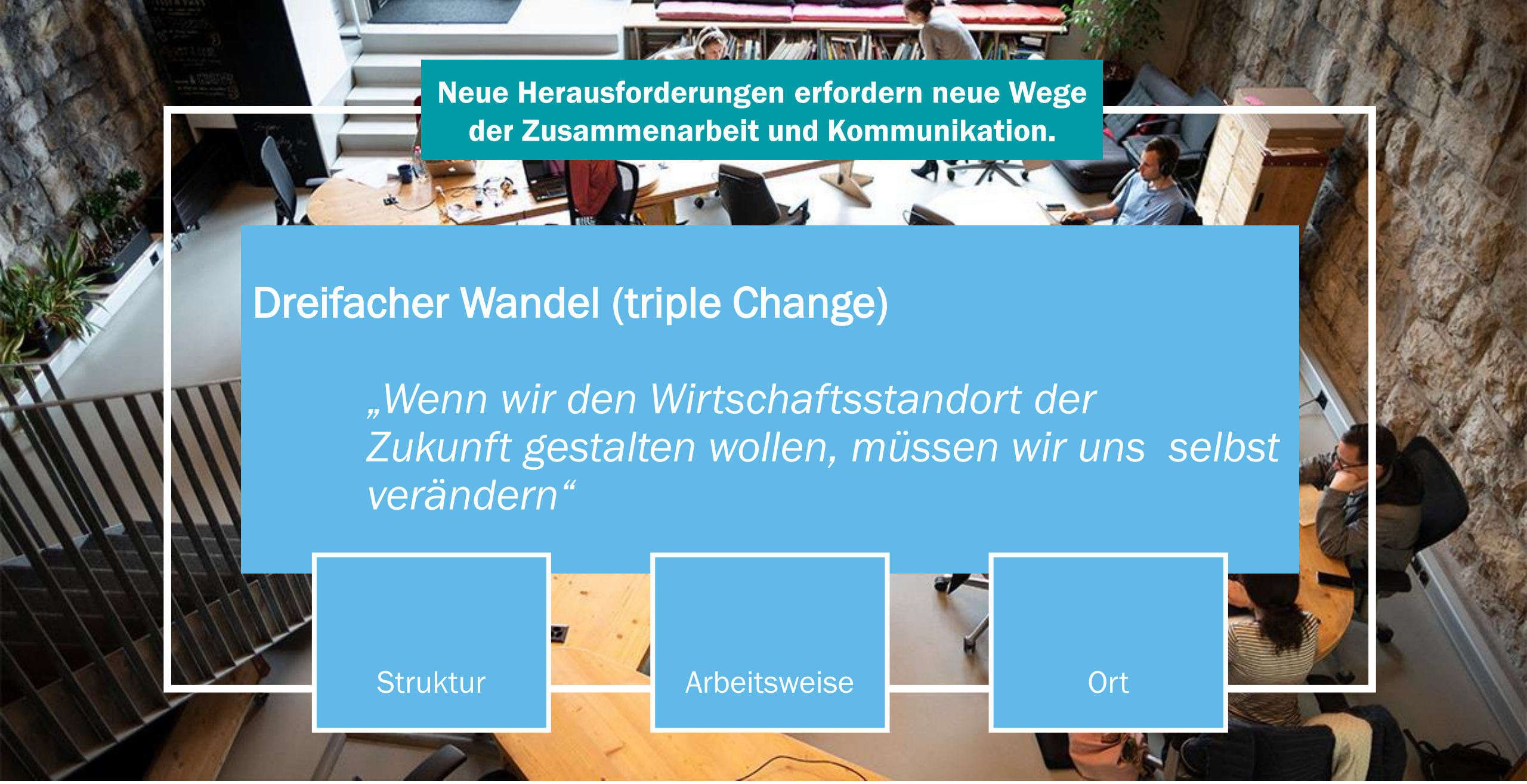
Infrastruktur & Standortqualität

Start-up & Innovationsförderung

Ökologische Wende / Energieversorgung

rhein kreis neuss

matrix prognos



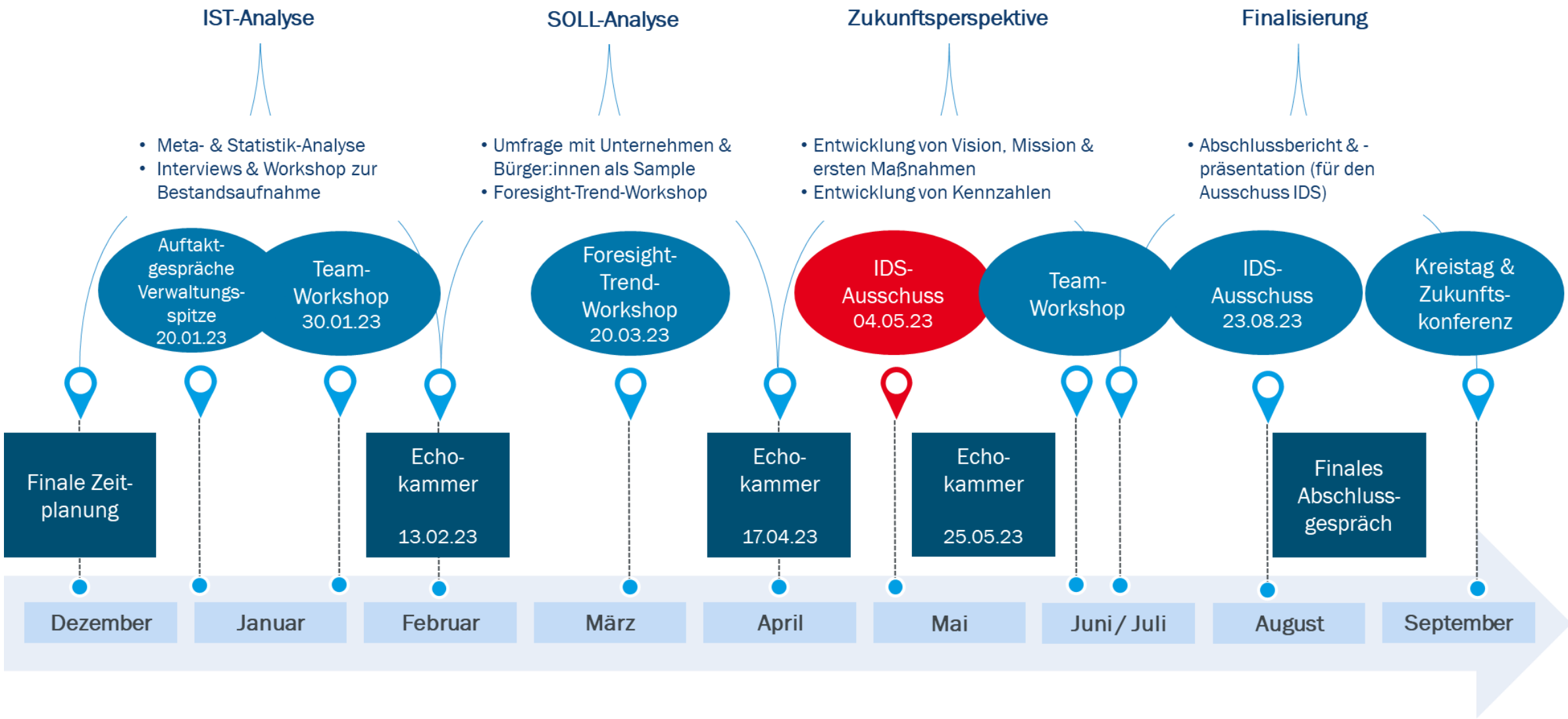
Neue Herausforderungen erfordern neue Wege der Zusammenarbeit und Kommunikation.

Dreifacher Wandel (triple Change)

„Wenn wir den Wirtschaftsstandort der Zukunft gestalten wollen, müssen wir uns selbst verändern“

- Struktur
- Arbeitsweise
- Ort

Prozessübersicht im zeitlichen Verlauf

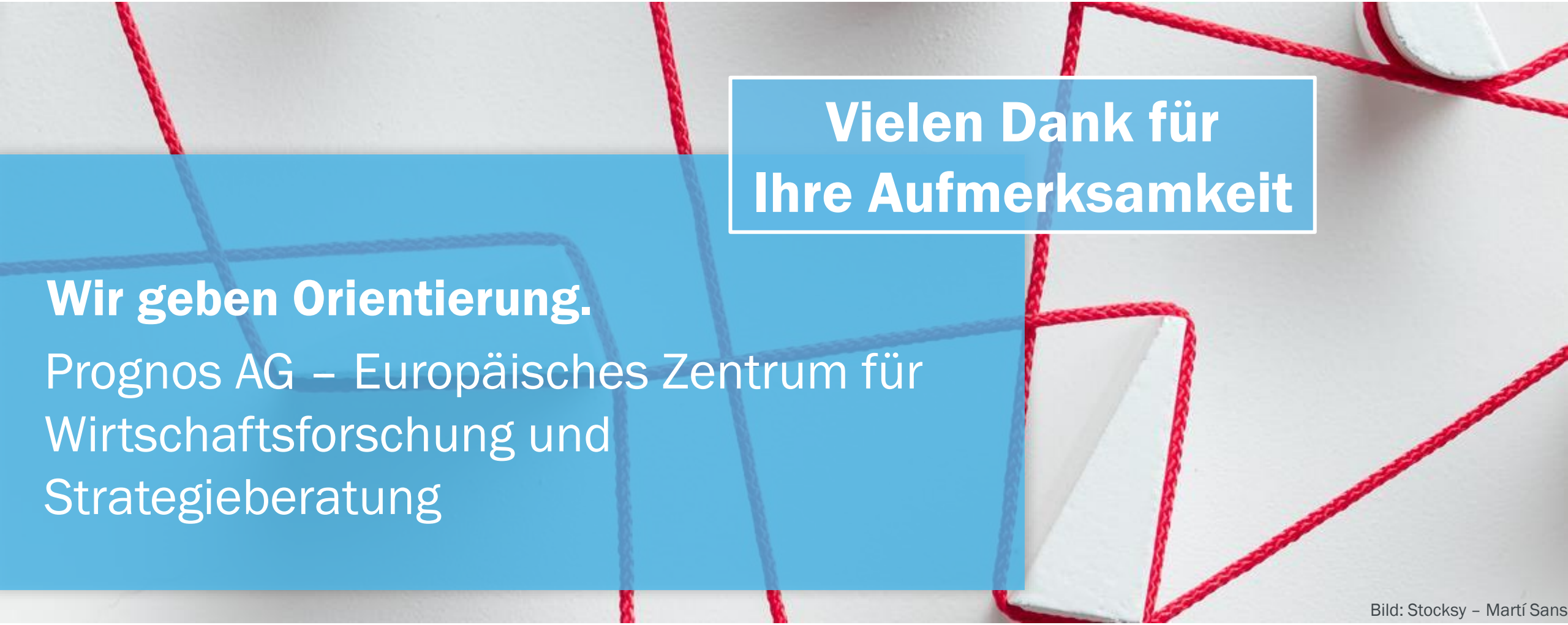


rhein kreis neuss

matrix prognos

rhein kreis neuss

matrix prognos
Wir geben Orientierung.



Vielen Dank für Ihre Aufmerksamkeit

Wir geben Orientierung.

Prognos AG – Europäisches Zentrum für Wirtschaftsforschung und Strategieberatung

Bild: Stocksy – Martí Sans

Unser Projektteam für Sie

Christian Schoon

Region und Standort

Projektleitung Prognos

M.A. Zukunfts-forschung

Volker Ruff

Geschäftsleitung, Leiter creative hubs & labs

Projektleitung matrix

Dipl. Geograph

Julia Schwienbacher

Region und Standort

Stellv. Projektleitung Prognos

M.Sc. Wirtschafts-geographie

Anna Grütering

creative hubs & labs

Stellv. Projektleitung matrix

M.A. Wirtschafts-förderung

Til Ulbrich

Region und Standort

Prognos

M.Sc. Economic Policy Consulting

Anne Spaan

creative hubs & labs

matrix

Hotelfachfrau

Dr. Olaf Arndt

Vizedirektor, Leiter Region und Standort

Supervision und Qualitätskontrolle Prognos

Dipl. Geograph, Dr. rer pol.

rhein kreis neuss

matrix

prognos

Anlage 5 zu TOP 8 der Niederschrift IDS vom 04.05.2023

Anfrage Personalfluktuationen

ZS 4 - IT

Trotz hoher Marktnachfrage nach IT-Personal ist es Dez. VI/ZS 4 in den vergangenen Jahren gut gelungen, das IT-Fachpersonal zu binden. Die Personalfluktuation ist gering, obwohl Stellenangebote und höhere Vergütungen anderenorts möglich wären. Insbesondere die seit einigen Jahren verstärkte eigene Ausbildung von Fachinformatikerinnen und -informatiker zahlt sich hier aus.

Jahr	Anzahl	Beschäftigung	Grund	Anmerkung
2018	2	Fachinformatiker, davon 1 mit Zeitvertrag bis zum 06.07.2018	1x Wechsel in Landesdienst 1 x Ablauf Zeitvertrag	Nachbesetzung durch fertige Ausbildungskraft
2019	1	Beamter	Todesfall	Nachbesetzung
2020	0			
2021	(2)	Fachinformatiker	interner Wechsel zur Stabsstelle Digitalisierung (SSD)	
2022	1	Fachinformatiker	eigene Kündigung	Nachbesetzung soll durch Fachinformatikerin nach Ausbildungsende erfolgen