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

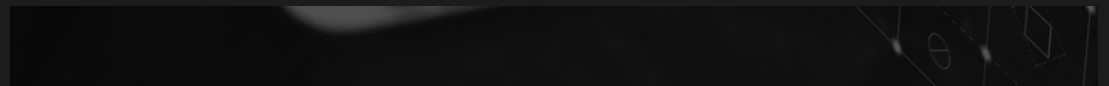
vom Starten des Hackerangriffs bis zur flächen-deckenden Auswirkung einer Cyberattacke.

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.

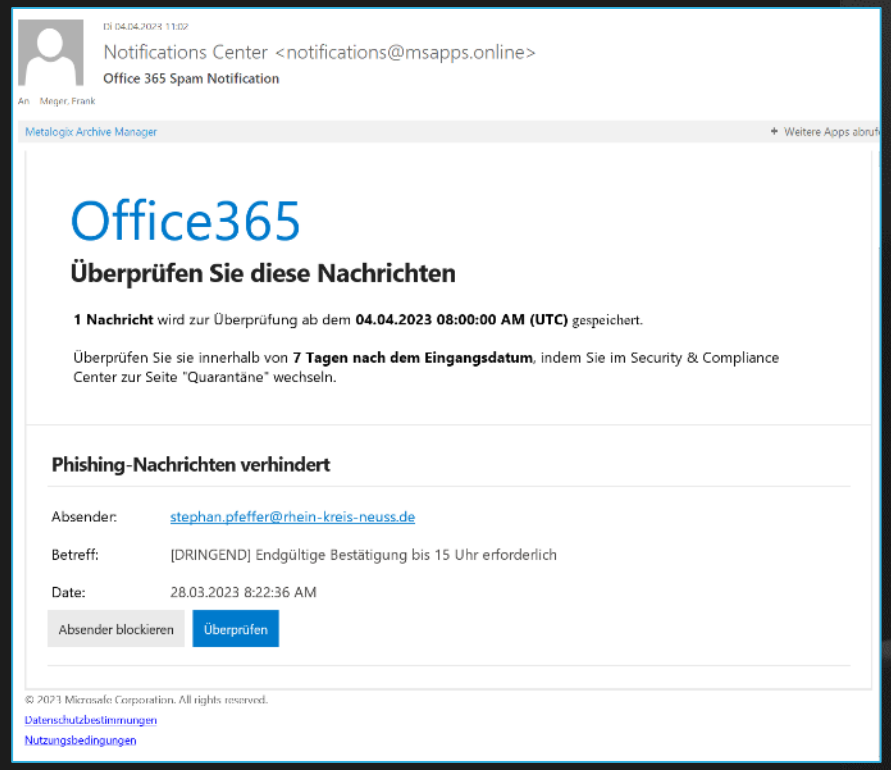
Zur klassischen E-Mail sind soziale Netzwerke, kombinierte Kontaktaufnahmen per Video, Telefon, SMS und professionelle Plattformen wie MS Teams, LinkedIN etc. hinzugkommen.

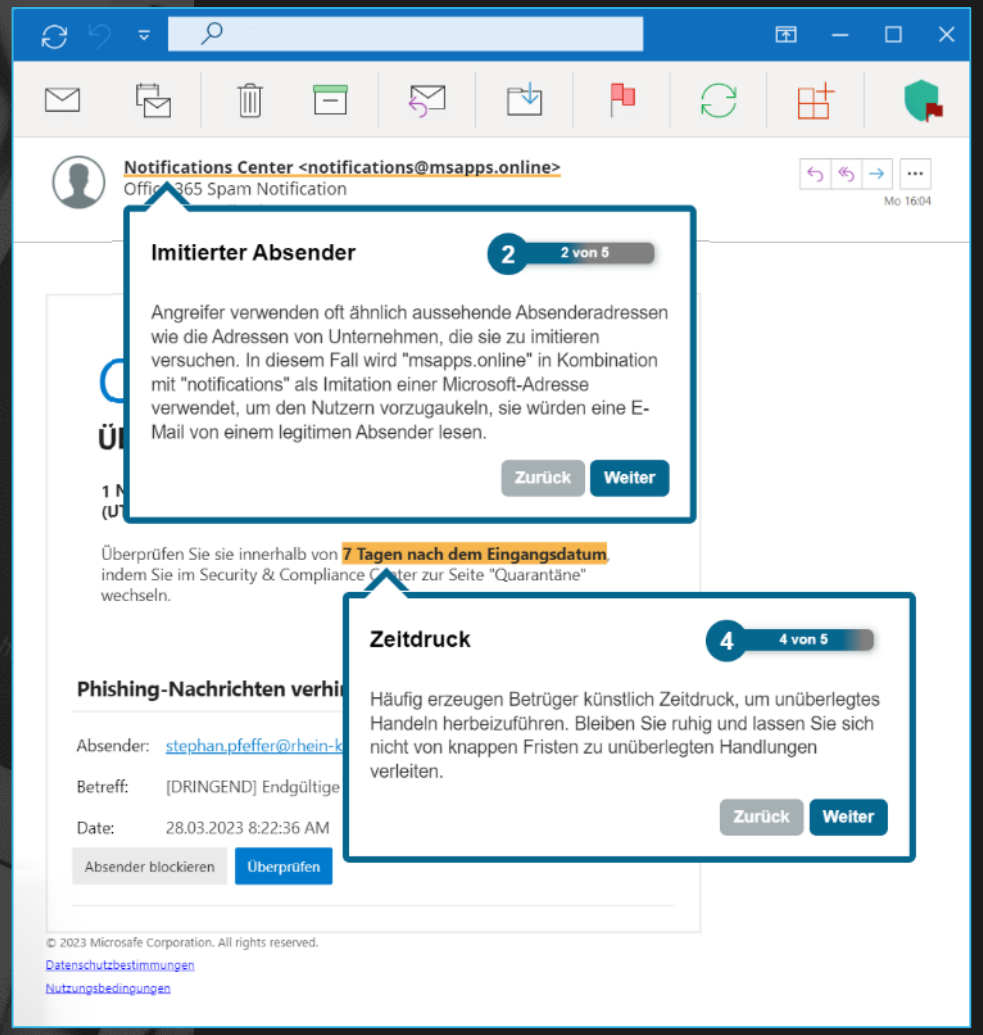
Bekannte Schwachstellen

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.

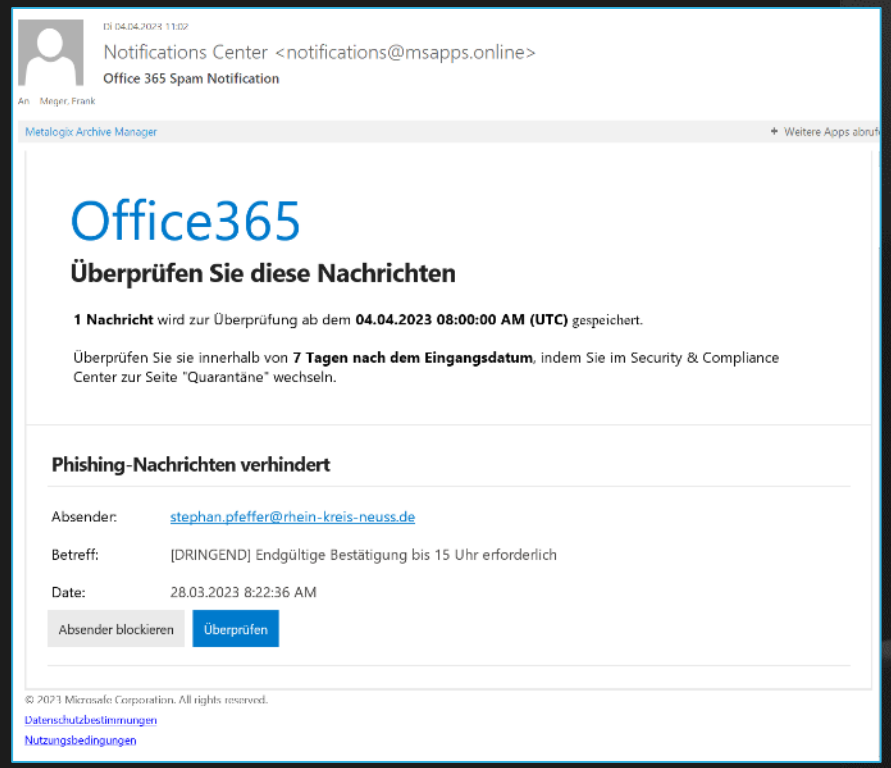
Phishing – jeder ist gefragt

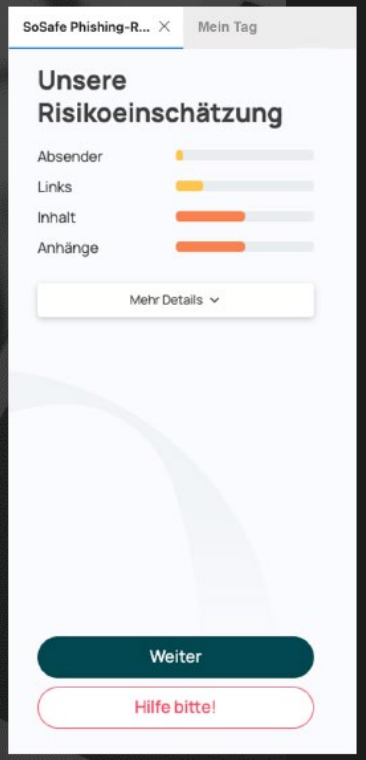


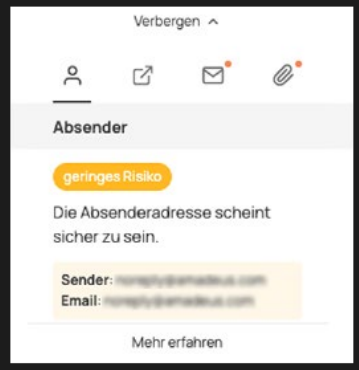


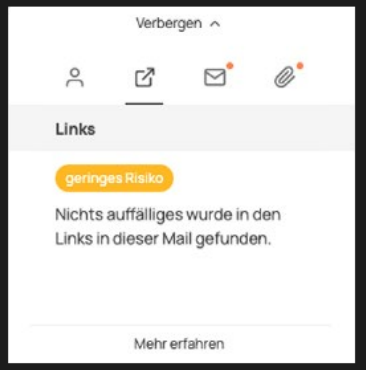
Phishing Mails sind zunehmend sehr professionell und zutreffend vorbereitet. Auch die E-Mail-Signaturen der vermeintlichen Absender werden hochwertig simuliert.

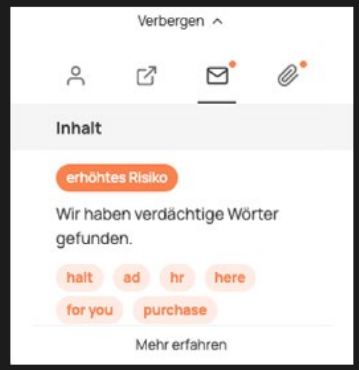
Phishing – jeder ist gefragt

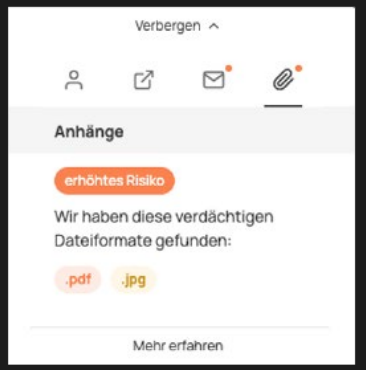












Integrationen im Mail-Programm können helfen, das Risiko einer Nachricht besser einzuschätzen.

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.

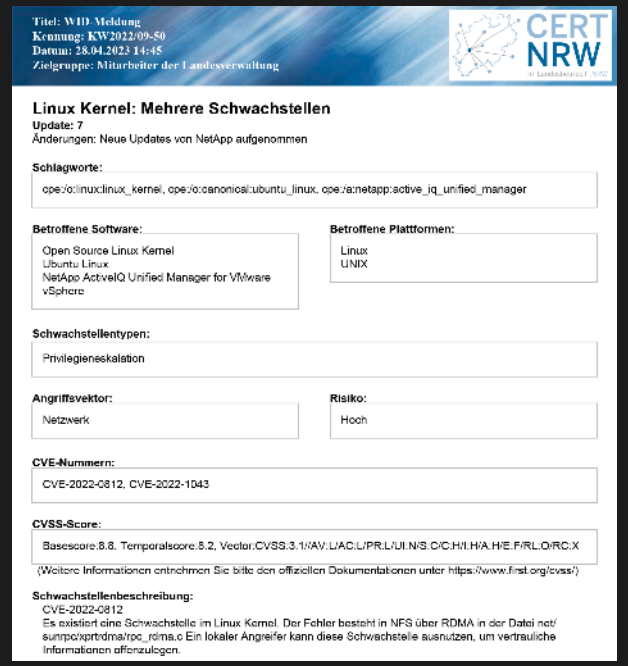
KWID CERT-NRW

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

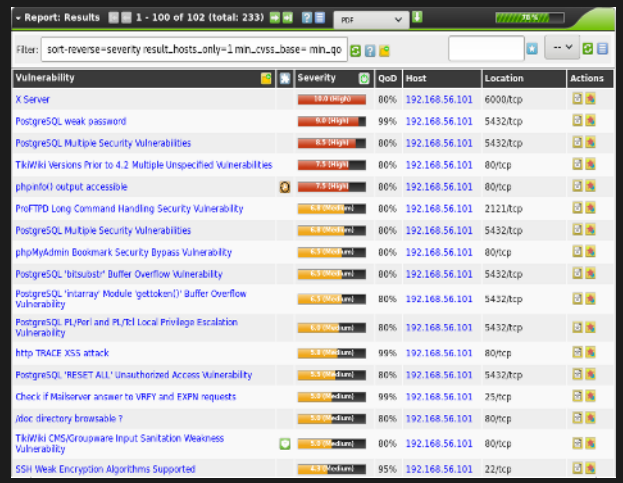
Angriffsvektor:
Netzwerk

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/)

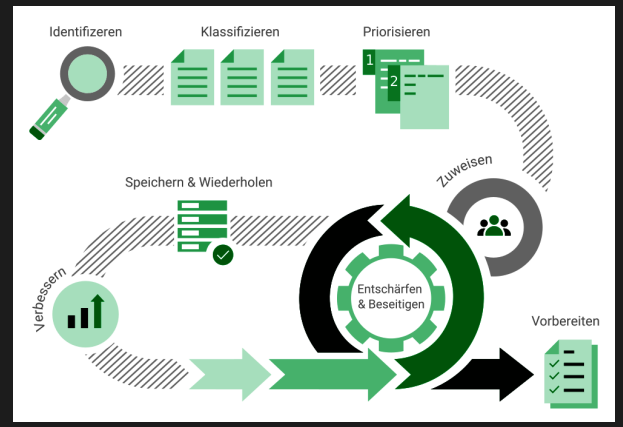
Schwachstellenbeschreibung:
CVE-2022-0812
Es existiert eine Schwachstelle im Linux Kernel. Der Fehler besteht in NFS über RDMA in der Datei net/sunrpc/xprtrdma/rpc_rdma.c Ein lokaler Angreifer kann diese Schwachstelle ausnutzen, um vertrauliche Informationen offenzulegen.



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

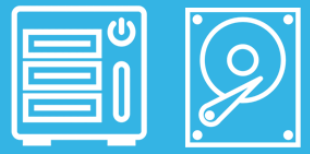
Immutable Storage

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

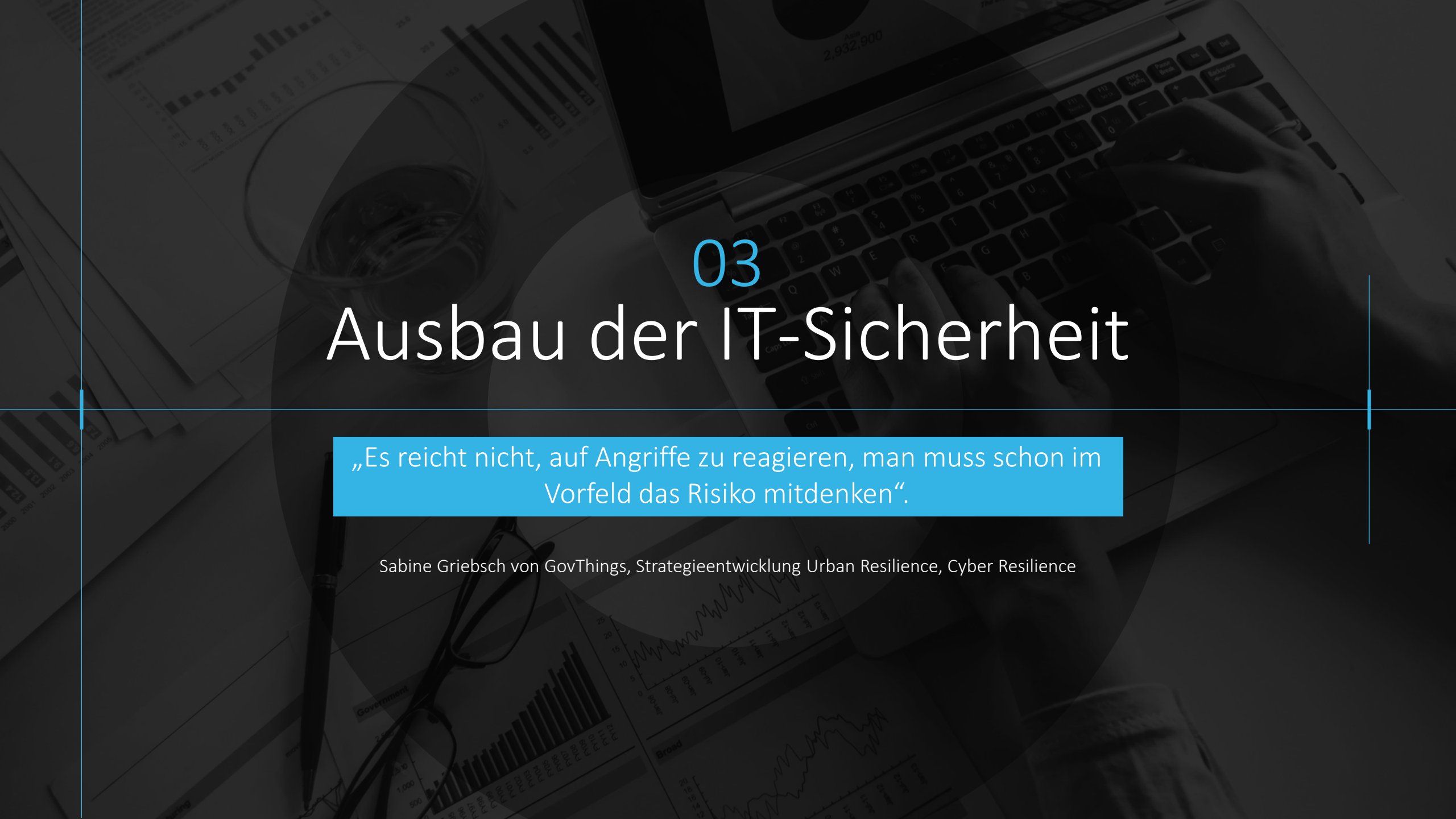
Der Grad der Widerstandsfähigkeit ermisst sich in der Gewährleistung von Vertraulichkeit, Integrität sowie der Verfügbarkeit von Daten und hoheitlichen Diensten.

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