Educational Month
Cyber Security

Wenn die Lichter ausgehen!
Aus dem Tagebuch eines gehackten Unternehmens

Presented by
Stefan Würtemberger, Carsten Wallmann und Matthias Magnus

10. November 2023

Herzlich willkommen! Ihre Online-Session startet gleich.

Schön, dass Sie dabei sind. Hören Sie uns einfach per Kopfhörer oder Lautsprecher zu.

Wir schalten die Mikrofone der Teilnehmer:innen stumm. Dann hören Sie alles besser. Auch alle Webcams sind automatisch deaktiviert.

Ihre Fragen können Sie über das Fragen-Fenster stellen. Der Moderator bringt Ihre Fragen entsprechend ein.

Agenda

01 Marabu GmbH - Opfer von Cyberangriffen

02 Vodafone Cyber Security Services

Heute für Sie in der Online-Session:

Stefan Würtemberger

Executive Vice President,
Marabu GmbH & Co. KG

Carsten Wallmann

Go-to-market Lead, Vodafone

Matthias Magnus

Head of Digital Solution Sales Cyber Security, Vodafone

Marabu GmbH - Opfer von Cyberangriffen

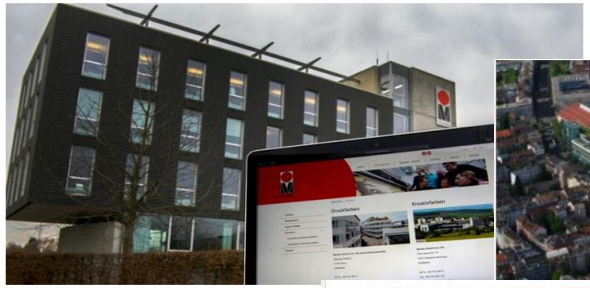
01

Opfer von Cyberangriffen

Cyber-Attacken im Landkreis

Marabu: „100 Prozent Sicherheit gibt es nicht“

Von Frank Ruppert 29.01.2020 - 06:55 Uhr



Marabu wurde Opfer eine Cyber-Angriffs. → *Foto: Martin*

Die Tammer Firma Marabu wurde im vergangene
hat daraus gelernt.

Im November wur
sogenannten Vers
Digitaldruck- und
zahlte nicht und fu
der Internet-Absic
zwischen allen Ni
Eindringling-Detek
Erkennen automat
„Information Tech
jeden einzelnen E-

Technische Hochschule Nü
20.676 Followerinnen
1 Tag •

+++ Cyber-Angriff auf TH Nürnberg

In der Nacht des 1. November kam e

ch Kundendaten betroffen

Nach Hackerangriff: Eberspächer schickt Mitarbeiter in Kurzarbeit

wiwo.de • Lesedauer: 1 Min.

Rental car company **Sixt** confirms **cyber** attack, leaves scores of UK customers in the

Cyber-Attacke auf MediaMarkt und Saturn legt Systeme lahm: Mehr als 3000 Server betroffen

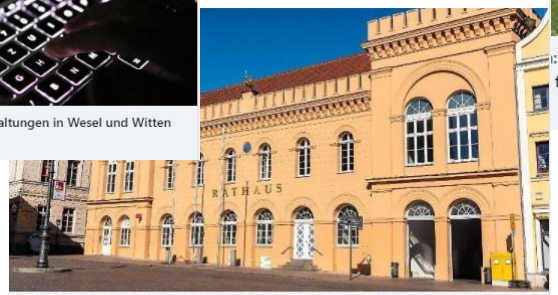
Cyber-Attacke auf Städte: Hackerangriff auf Verwaltungen in Wesel und Witten

rp-online.de • Lesedauer: 3 Min.

: Uni wieder online - Liechtenstein - für Liechtenstein

Rundschau - Gehackt und erpresst: Brutale Cyber-Angriffe auf Schweizer Firmen - Play SRF

srf.ch • Lesedauer: 1 Min.



Attacke auf Dienstleister: Cyber-Angreifer verschlüsseln Daten in Schwerin

amp-n--tv-de.cdn.ampproject.org • Lesedauer: 1 Min.

Black Friday

Am 03.09.2019 drangen die Täter in unser Netzwerk ein und haben bis November sämtliche System Kompromittiert!

Am 29.11.2019 um 4.24Uhr begannen die Hacker mit der Ausführung der Verschlüsselung aller IT Systeme.

Nach knapp über 6 Stunden waren Nahezu alle Systeme Verschlüsselt (auch OT).

Terrabyte an Daten und Systeme waren nicht mehr brauchbar.

Hacker legen Traditionsfirma Marabu lahm

Kriminalität Der Farbenkonzern baut seine Systeme neu auf. Die Attacke könnte für Autobauer Folgen haben. *Von Daniel Gräfe*

Der Hackerangriff auf Marabu begann am 29. November um 4 Uhr und wurde um 6.30 Uhr bemerkt. Etwa fünf Stunden später kappte die Firma zur Sicherheit alle Systeme, nichts ging mehr: kein Rechner, kein Telefon, kein Fax. So könne man sich auch einen Stromausfall vorstellen, sagt der IT-Chef Stefan Würtemberger unserer Zeitung. 15 Landesgesellschaften weltweit waren nicht mehr zu erreichen. Die Hacker hatten die wichtigsten Server und damit praktisch alle Unternehmensdaten verschlüsselt, auf den Bildschirmen erschien nur der Vermerk, wie man die Angreifer über eine anonymisierte Verbindung kontaktieren könne. Dann könne man auch Software kaufen, um die Daten zu entschlüsseln.

„Man muss sich auch mit analogen Mitteln helfen können."
York Boeder, Marabu-Chef

Den Preis wurden Marabu-Chef York Boeder und sein Team nicht mehr erfahren. „Wir wollten den Kriminellen nicht nachgeben – egal wie lange es dauert, wir müssen es durchstehen", sagt Boeder. Das Bundeskriminalamt (BKA) wurde verständigt. Auch um andere zu warnen, habe man sich jetzt an die Öffentlichkeit gewandt. Schließlich könne ein Angriff wie dieser jede Firma treffen.

Tatsächlich machen die Angriffe mit Erpressungssoftware derzeit das Gros von Cyberangriffen aus. Oft fängt es mit einer gefälschten Mail oder einem manipulierten USB-Stick an. Nicht immer sind die Angriffe so gezielt wie bei Marabu, wo der Trojaner BitPaymer zum Einsatz kam. Immerhin handelt es sich bei Marabu um einen weltweit führenden Hersteller von

Cyber-Attacken im Landkreis

Marabu: „100 Prozent Sicherheit gibt es nicht"

Von Frank Ruppert 29.01.2020 - 06:55 Uhr

Marabu wurde Opfer eine Cyber-Angriffs. ⇥ *Foto: Martin Kalb*

Die Tammer Firma Marabu wurde im vergangenen Jahr Opfer einer Cyber-Attacke und hat daraus gelernt.

Im November wurde die Tammer Firma Marabu Opfer einer Cyber-Attacke. Mittels eines sogenannten Verschlüsselungstrojaners sollte Geld von dem Hersteller von Siebdruck-, Digitaldruck- und Tampondruckfarben sowie Kreativfarben erpresst werden. Marabu zahlte nicht und fuhr alle seine Server herunter. Danach sollte eine Neustrukturierung der Internet-Absicherung erfolgen. „Wir haben Firewalls und Ransomware-Filter zwischen allen Niederlassungen aktiviert und verbessert. Zusätzlich laufen sogenannte Eindringling-Detektion- und Prävention-Filter, die den Netzwerkverkehr nach schnellem Erkennen automatisch stoppen", erklärt Stefan Würtemberger, Vize-Präsident „Information Technology" bei dem Unternehmen. Außerdem habe man Systeme, die jeden einzelnen E-Mail-Anhang auf Schadsoftware testen.

„Überlegt euch, wie ihr analog überleben könnt"

Farbenproduzent Marabu von Cyberangriff getroffen - Geschäftsführer Boeder: Wir waren von der Außenwelt abgeschnitten

Staat. „Obwohl unsere Notfallpläne und Sicherheitssysteme funktionierten, konnte nicht aufgehalten werden, dass Teile der Daten auf unseren Servern verschlüsselt und somit zunächst unbrauchbar wurden", betont IT-Leiter Stefan Würtemberger.

Das Landeskriminalamt und das Bundeskriminalamt (BKA) wurden informiert. Deren IT-Experten stehen dem Tammer Unternehmen seither beratend zur Seite. PCs und Server wurden beschlagnahmt, um den Kriminellen auf die Spur zu kommen. „Die Chancen, dass sie gefasst werden, sind sehr klein", so Boeder, der zu den Aufklärungschancen. Die Zielgruppe der Täter ist nach BKA-Informationen der Mittelstand. Nicht wenige Firmen würden bezahlen, um wieder an ihre Daten zu kommen – und schweigen. „Für uns war es eine Grundsatzentscheidung, dass wir auf mögliche Lösegeldforderungen nicht eingehen", sagt Boeder, „sondern die Systeme aus eigener Kraft wiederherstellen." Dafür habe das Unternehmen bewusst in Kauf genommen, dass zur Aufrechterhaltung der Basisproduktion in Tamm in vielen Bereichen von Hand gearbeitet werden musste – wo sonst EDV-Prozesse unterstützen. Mit Papierlisten und Kopien von Lieferscheinen und Bestellungen – ganz wie in alten Zeiten – wusste man sich zu helfen. „Die Bereitschaft der Belegschaft, zu improvisieren und mit anzupacken, war überwältigend", betont Rolf Simon, der Geschäftsführende Gesellschafter.

„Wir haben von anderen Firmen, die an die Öffentlichkeit gegangen sind, gelernt", so Boeder. „Wir wollen unsere Erfahrungen weitergeben." Die Lehren aus dem Vorfall: „Zeit ist ein kritischer Faktor." Und: „Ohne Hilfe von außen geht nichts." Diese kam vom IT-Haus Bechtle. Und von einer speziellen Entschlüsselungssoftware. Seit gestern laufen in Tamm fast alle Systeme wieder reibungslos. Bis Ende der Woche soll dies auch in Bietigheim und bei den Auslandsgesellschaften der Fall sein. Fast alle Daten konnten wiederhergestellt werden. Der Schaden lässt sich bisher schwer beziffern. „Über 100 000 Euro, aber unter einer Million Euro", schätzt der Marabu-Geschäftsführer.

„Überlegt euch einen Plan B, wie ihr analog ohne EDV überleben könnt", lautet Boeders Rat an andere Unternehmen.

„Bei einem erneuten Angriff wären wir jetzt besser gewappnet", sagt Würtemberger, „doch Hacker sind immer schneller als die Sicherheitssoftware. Es gibt keine 100-prozentige Sicherheit."

Der Firmensitz des Farbenherstellers Marabu in Tamm. Fotos: Holm Wollschendorf

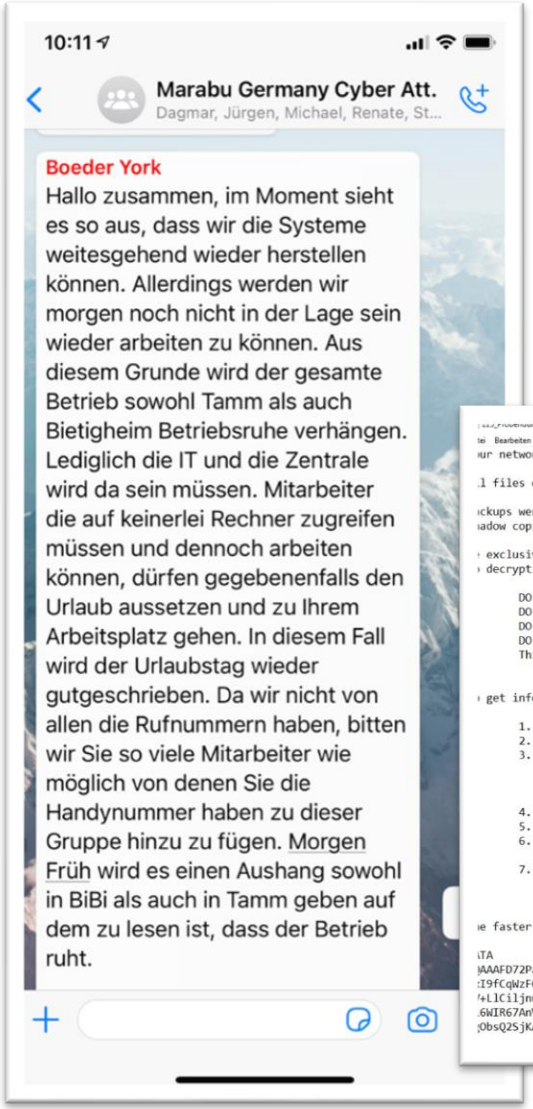
Die Marabu-Chefs Rolf Simon (links), York Boeder (Mitte) und IT-Chef Stefan Würtemberger informieren über den gezielten Erpressungsangriff auf das Unternehmen.

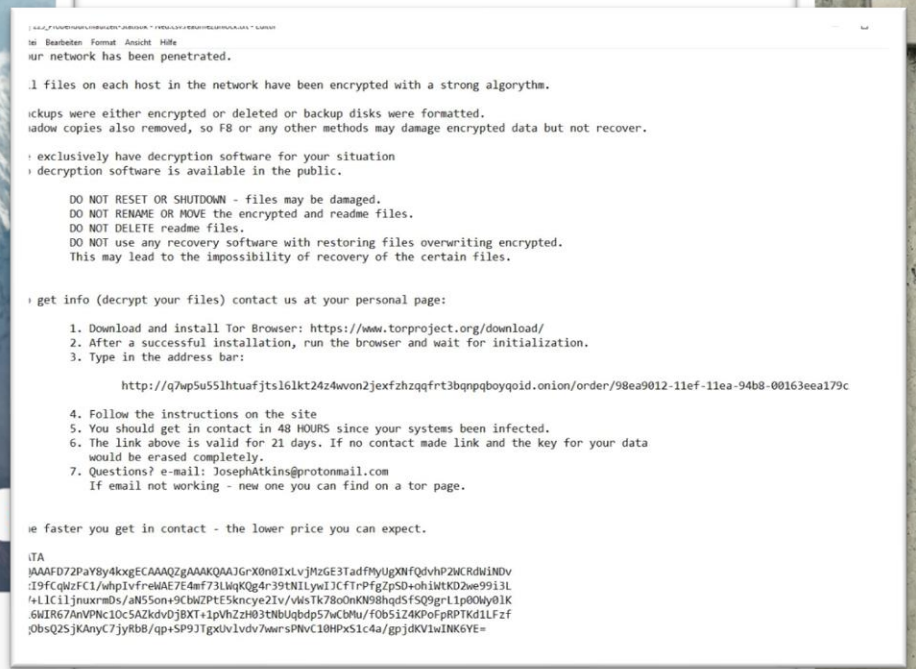
STICHWORT

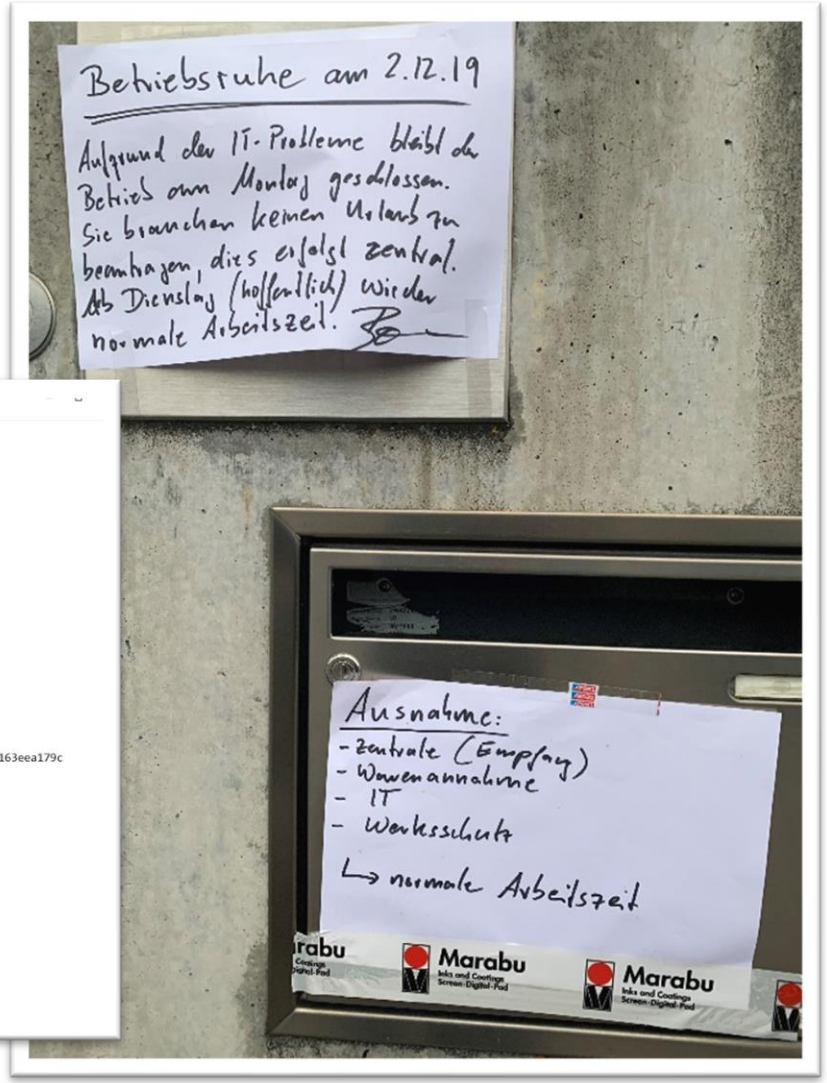
Marabu

Die Marabu Beteiligungs-GmbH in Tamm ist einer der weltweit führenden Hersteller von Sieb-, Digital- und Tampondruckfarben sowie Flüssigkeitsbeschichtungen. Seit der Gründung 1859 entwickelt Marabu Farbserien, die Meilensteine sowohl bei industriellen als auch bei grafischen Anwendungen setzen. Marabu bietet mit 16 Tochtergesellschaften in Russland, Italien, Frankreich, Großbritannien, Schweden, Brasilien, China, USA und Singapur Farbsysteme und Dienstleistungen in über 90 Ländern an. In Tamm werden Druckfarben für die Industrie sowie den industriellen und dekorativen Druck produziert. Im Bietigheimer Werk stellt Marabu vor allem Künstler- und Kreativfarben her. (red)

Black Friday- So sieht's aus!







Agenda

Was sind die wichtigsten Erfahrungen im Umgang mit Cyberangriffen?

Wie begegnet man ihnen und was kann man tun, um sich vorzubereiten?

Wie sieht es aus, wenn es ein zweites Mal passiert und welche Lehren werden daraus gezogen?

Umgang mit einem Cyberangriff

- Der höchste Stresslevel, den man sich vorstellen kan
  - Wie könnte das Problem gelöst werden?
  - Was ist zu tun, was nicht!
- Unbestimmte Situation und kein klarer Ausweg
  - Was kommt zuerst?
  - Was kommt als nächstes?
  - Wie konnte das passieren?

Umgang mit einem Cyberangriff

- Hoher Arbeitsaufwand, um einen Cyberangriff zu überstehen
    - ~5000 Aufgaben mussten geplant und erledigt werden
    - ~1500 TELKOs und Konferenzen

Dauer eines Cyberangriffes

Tag 1- 6: 4. Dezember 2019

- ERP System / Maschinen stehen in Deutschland wieder zur Verfügung
- Erste Produktionsvorgänge laufen wieder über das ERP System
- Vorsichtiges Arbeiten mit den Systemen möglich. Jedoch gibt es immer wieder Unterbrechungen wegen Firmware Updates und Sicherheitspatches

Woche 2- 9: Ende Februar 2020

- ERP Systeme Weltweit wieder Verfügbar
- Alle Maschinen / Server & Computer wieder angebunden
- 95% aller Globalen Services wieder normal verfügbar

Wie kann man ihnen begegnen?

- Krisenmanagement das wichtigste Management-Instrument
    - Trainieren Sie Notfallroutinen
    - Keine Panik, bleiben Sie ruhig und strukturiert

Was können Sie tun, um sich vorzubereiten?

- Fortlaufende Cybersicherheits-Strategie
    - Cybersicherheit hört nicht auf, sobald sie implementiert ist
    - Bleiben Sie am Ball und hinterfragen Sie stets Ihre eigene Strategie
    - Änderungen in der Organisation / Prozesse und Software bedeuten Anpassungen von Cybersicherheit

Wie sieht es aus, wenn es zweimal passiert?

- Bei der Ersten:

  - Am Anfang wussten wir nichts
  - Wir hatten keinen klaren Plan
  - Keine Erfahrung und genaue Verfahren

- Aber bei der Zweiten:

  - Wussten, dass eine Attacke im Gang ist
  - Klare Planung und Strategie
  - Erfahrung in Ablauf und der Strategie

Das bedeutet:
Bei der ersten 9 Wochen, bei der zweiten 48 Stunden

Lessons Learned?

- Organisation
  - Setzen Sie Prioritäten!
  - Klare Struktur!
  - Überblick!
  - Fokus setzen!

- Kommunikation
  - Hört zu!
  - Seien Sie ehrlich!
  - Bleiben Sie objektiv!
  - Erreichbar sein!

- Motivation
  - Sei der Kümmerer!
  - Zeigen Sie Interesse!
  - Anerkennung teilen!
  - Das Wichtigste: Humor!

Lessons Learned?

- Je besser die Cybersicherheitsstrategie, desto besser sind Sie vorbereitet.
- Cybersicherheitsstrategie ist jetzt Aufgabe des Managements / CEO
- Stellen Sie die Cybersicherheit regelmäßig auf den Prüfstand.
- Nicht aufhören, über Cyberangriffe und ihre Auswirkungen zu sprechen

Das Wichtigste: "Es gibt keine 100%ige Sicherheit".

Vodafone Cyber Security Services

02

Safety first!

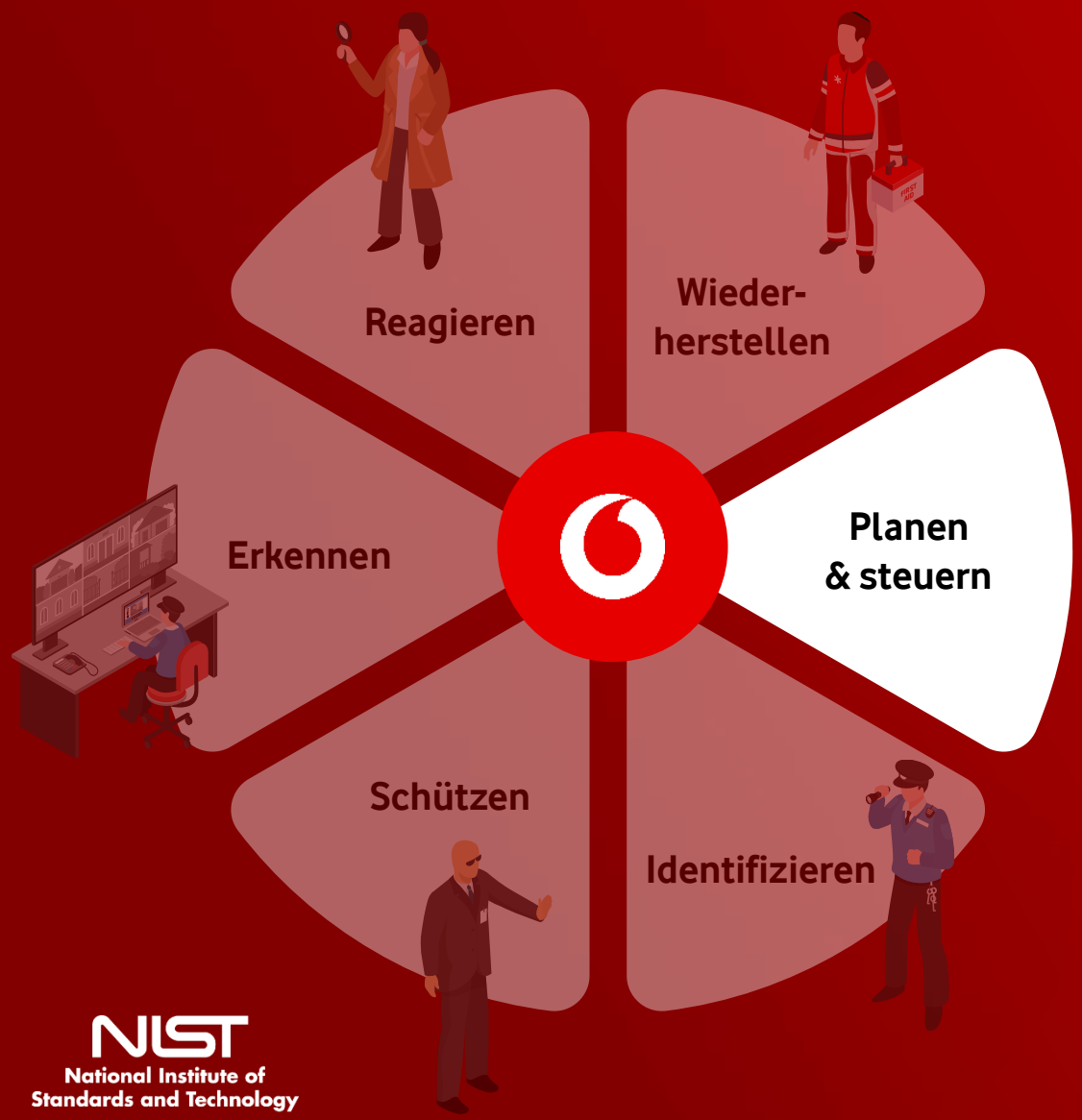
Der digitale Notfallplan gegen Cyber Angriffe

National Institute of Standards and Technology

Security ganzheitlich betrachten ist der Schlüssel zum Erfolg!

NIST
National Institute of
Standards and Technology

Vodafone als Ihr Security-Partner – neutral & unabhängig



Wir planen und steuern mit Ihnen Ihre Sicherheitsorganisation.

- Strategieberatung
- IT Sicherheitskonzept
- Zertifizierungsunterstützung

NIST
National Institute of Standards and Technology

Wir identifizieren Ihre Bedrohungen bevor es Angreifer tun.

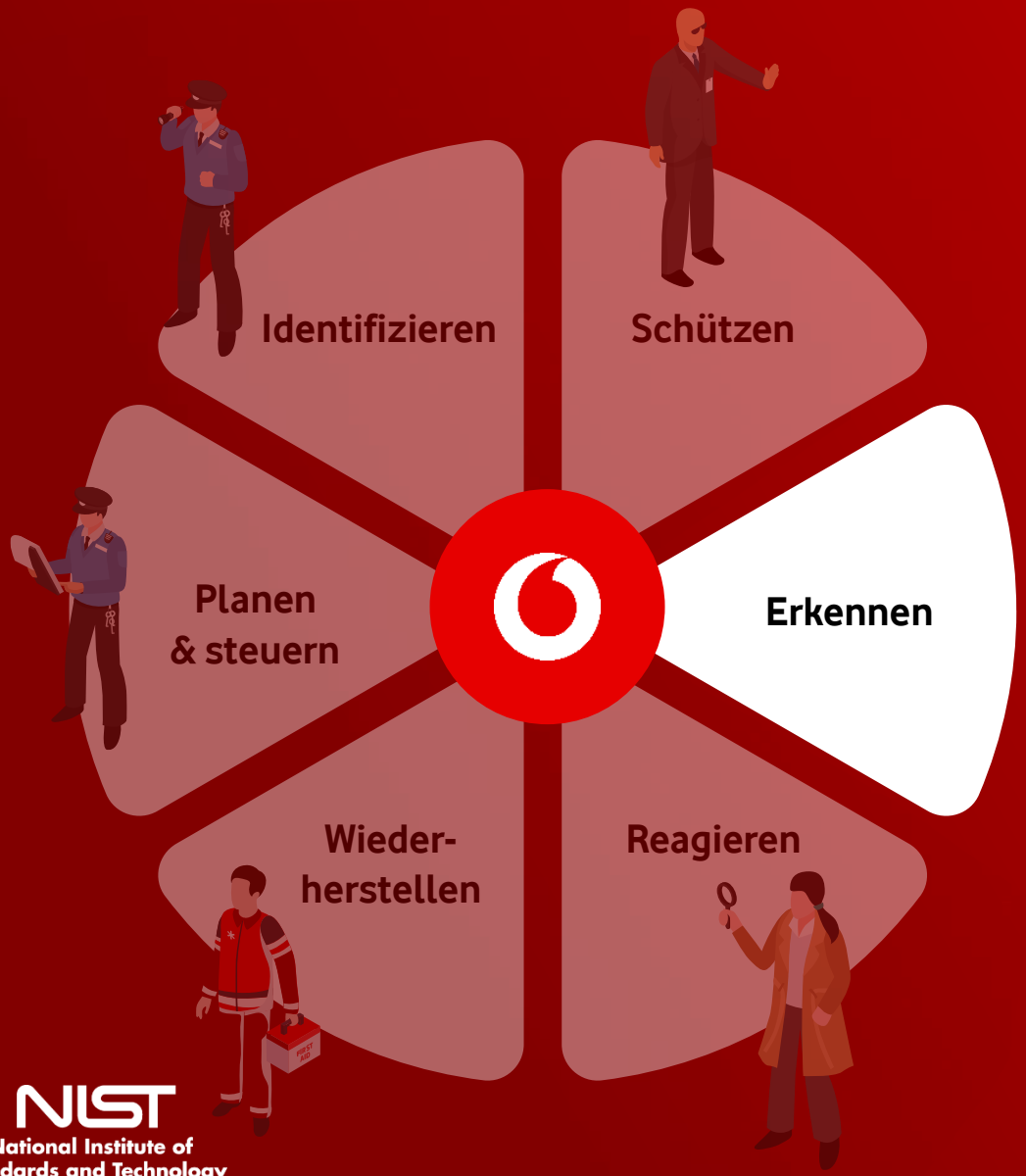
- Risikoanalyse und -bewertung
- Identifikation von Schwachstellen
- Phishing-Kampagnen

NIST
National Institute of Standards and Technology

National Institute of Standards and Technology

Wir verhelfen zu besserem Schutz und machen es Angreifern schwer.

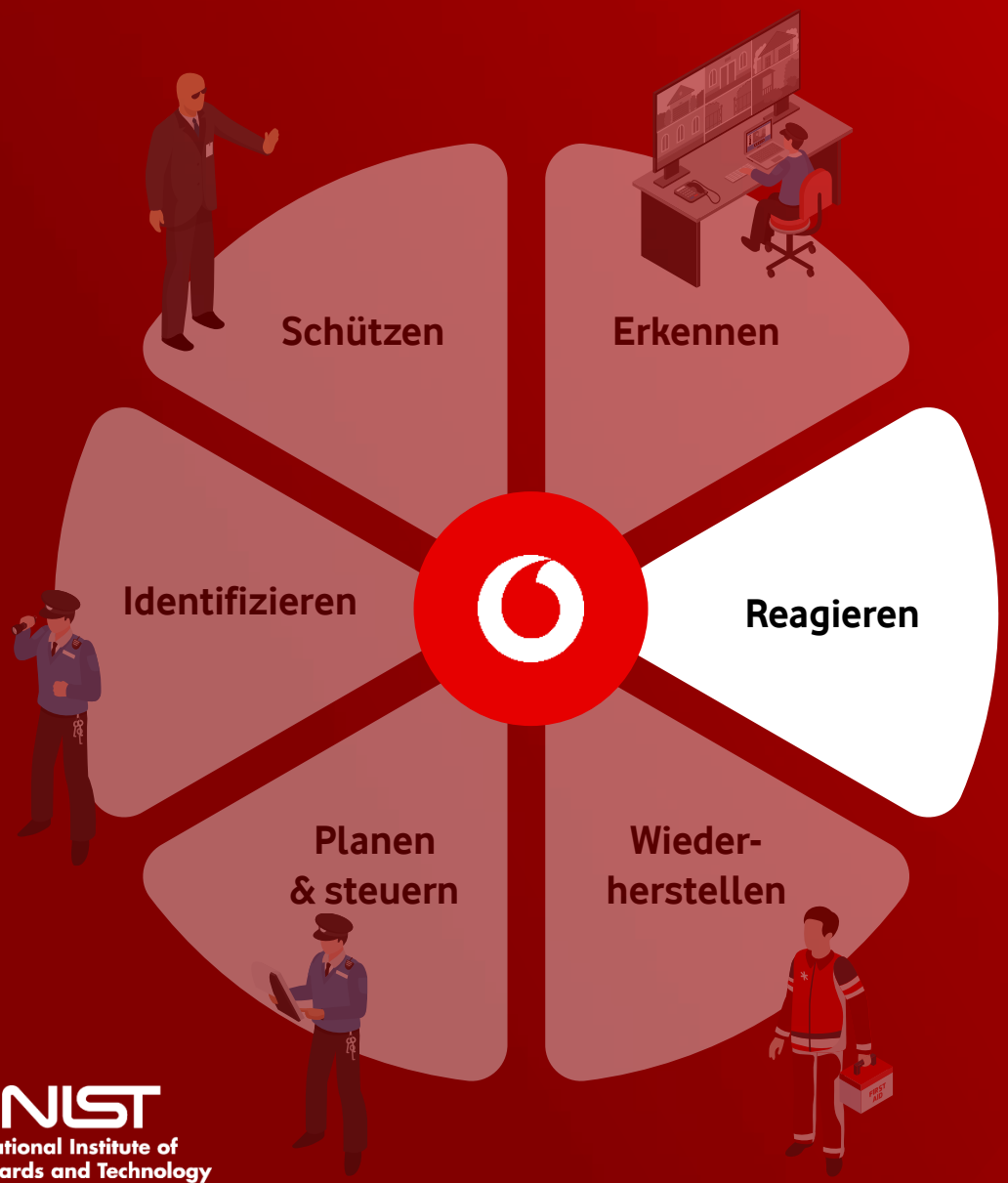
- Systemhärtung
- Netzwerksicherheit
- Endpoint Security
- Zero Trust Lösungen
- Cloud Security
- Security Awareness



NIST
National Institute of Standards and Technology

Wir überwachen 24/7 Ihre gesamte IT, erkennen Angriffe und warnen Sie bevor Schaden ensteht.

- Anomalieerkennung und Log-Monitoring
  - SIEM, NDR, MDR, EDR, XDR (Managed oder unmanaged)



NIST
National Institute of Standards and Technology

Im Ernstfall reagieren wir für Sie, wehren Angriffe ab und übernehmen die Forensik.

- Bewertung und Eindämmung des Angriffs
- Notfallmanagement
- IT-Forensik

NIST
National Institute of
Standards and Technology

**Ihre Daten sind vorhanden,
wenn Sie sie brauchen.
Mit uns geht nichts verloren.**

- Backup-Lösungen
- Disaster Recovery

Ihre Daten sind vorhanden, wenn Sie sie brauchen. Mit uns geht nichts verloren.

- Backup-Lösungen
- Disaster Recovery

Im Ernstfall reagieren wir für Sie, wehren Angriffe ab und übernehmen die Forensik.

- Bewertung und Eindämmung des Angriffs
- Notfallmanagement
- IT-Forensik

Wir überwachen 24/7 Ihre gesamte IT, erkennen Angriffe und warnen Sie bevor Schaden entsteht.

- Anomalie Erkennung und Log-Monitoring
  - SIEM, NDR, MDR, EDR, XDR (Managed oder unmanaged)

Wir planen und steuern mit Ihnen Ihre Sicherheitsorganisation.

- Strategieberatung
- IT-Sicherheitskonzept
- Zertifizierungsunterstützung

Wir identifizieren Ihre Bedrohungen bevor es Angreifer tun.

- Risikoanalyse und -bewertung
- Identifikation von Schwachstellen
- Phishing-Kampagnen

Wir verhelfen zu besserem Schutz und machen es Angreifern schwer.

- Systemhärtung
- Netzwerksicherheit
- Endpoint Security
- Zero Trust Lösungen
- Cloud Security
- Security Awareness

NIST National Institute of Standards and Technology

VODAFONE BUSINESS EDUCATION

Egal ob Blau, Rot, M oder XXL...

Wir haben für Ihren Bedarf die optimale Lösung,
finden diese gemeinsam mit Ihnen und begleiten die Umsetzung.

Partnerprodukte
(Auszug)

dhpg & TÜV AUSTRIA Group SOC
APPVISORY® by mediaTest digital
vmware Carbon Black
ZIMPERIUM
CROWDSTRIKE
paloalto NETWORKS
KALI
pradeo
SOPHOS
ISEC7 SPHERE
cybereason
teamwire.
AGAT
Windows Defender
Lookout
FORTINET

Unsere Partner
(Auszug)

schiffl
isec The Digital Workplace Company
SWISS IT SECURITY GROUP
Sie & 
REPLY
accenture
Microsoft
Systemhaus Compi Power ...the customer company
zscaler
DRACOON
CHECK POINT
BlackBerry CYLANCE
Hypergate

IHRE FRAGEN.

Vielen Dank für Ihre Teilnahme!

Bei Fragen
melden Sie sich gern
bei Ihrem:r Vodafone-
Ansprechpartner:in.

Sie sind neu bei uns?
Schreiben Sie uns an
online.sessions@vodafone.com
eine E-Mail.

Weitere Online-Sessions
aus unserem Educational
Month Cyber Security
finden Sie hier.

TIMETABLE 2023

VODAFONE BUSINESS EDUCATION

Cyber Security Educational Month

KW 42

17.10. | 10:00 **Cyber Security**
Jessica Schäfer (Accenture)
Martin Mausner (Vodafone)

18.10. | 10:00 **Cyberversicherungen**
Sönke Glanz (HDI Versicherung)
Matthias Magnus (Vodafone)

19.10. | 10:00 **Deepfakes**
Dominik Wojcik

KW 43

23.10. | 14:00 **Schutz vor Cyberkriminalität**
Sarah Elßer (Tech Well Told)
Alexander Pessler (Tech Well Told)
Patrick Sulewski (Vodafone)

KW 45

06.11. | 10:00 **KRITIS & NIS 2.0**
Robert Steffen (Vodafone)
Matthias Magnus (Vodafone)

08.11. | 10:00 **Live Hacking**
Lukas Garlik (Accenture) | Emil Stahr (Accenture)
Martin Mausner (Vodafone)

10.11. | 10:00 **Gehacktes Unternehmen**
Stefan Würtemberger (Marabu) | Carsten Wallmann (Vodafone)
Matthias Magnus (Vodafone)

KW 46

16.11. | 10:00 **Cyber-Angriffe abwehren**
Franz Finke (Lookout) | Jasin Mehovic (Lookout)
Mario Bohum (Vodafone)


Together we can
vodafone
business