Educational Month
Cyber Security

Digitale Resilienz stärken: Sinn und Zweck von Cyberversicherungen in einer vernetzten Welt

Presented by
Matthias Magnus und Sönke Glanz

18. Oktober 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 HDI – Cyberversicherungen in einer vernetzten Welt

02 Vodafone Cyber Security Services

Heute für Sie in der Online-Session:

Matthias Magnus

Head of Digital Solution
Sales Cyber Security

Sönke Glanz

Produktmanagement /
Underwriting Cyber
IT-Sicherheitsbeauftragter

HDI – Cyberversicherungen in einer vernetzten Welt

01

Agenda

1. Die Risiken & Gefahren wahrnehmen
2. Sinn und Zweck einer Cyberversicherung
3. Anforderungen an Unternehmen zur Gewährleistung der IT-Sicherheit

Ihr Referent

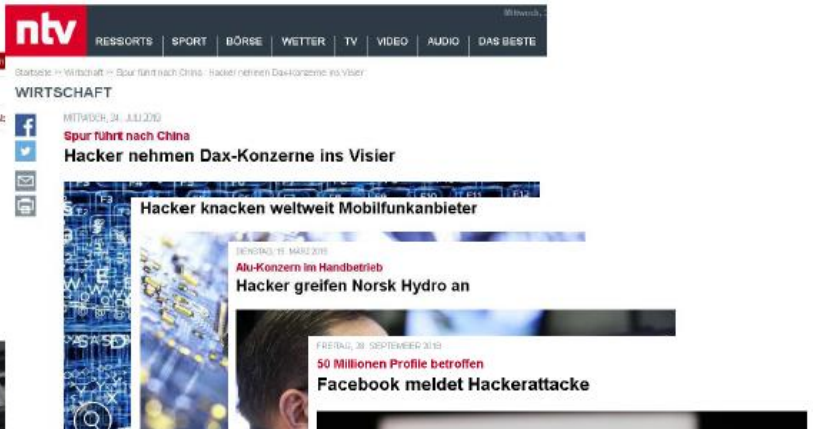
Sönke Glanz

Produktmanagement / Underwriting Cyber
IT-Sicherheitsbeauftragter

1

Die Risiken & Gefahren wahrnehmen

Aktuelle Cyberrisikolage



Bei einem Cyberangriff werden i.d.R. ausschließlich Computersysteme angegriffen – Die Folgen betreffen allerdings die Systeme UND die Menschen!

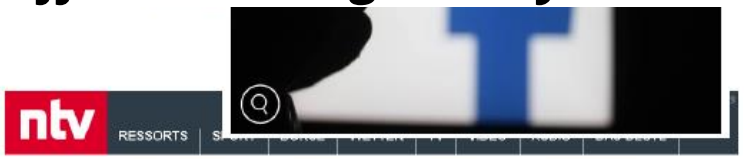
DIENSTAG, 30. APRIL 2019

Daten von Großkunden gestohlen

Hacker erpressen deutsche Online-Firma

Deutscher Mittelstand im Visier

Cyber-Angriffe verursachen 43 Milliarden Euro Schaden



PROPHETE

Hack wohl verantwortlich für Insolvenz von E-Bike-Hersteller

Die Insolvenz des Herstellers Prophete soll einen ungewöhnlichen Grund haben: Neben der Chipkrise sollen Hacker verantwortlich sein, die den Betrieb lahmgelegt haben.

in Pocket speichern | merken

11. Januar 2023, 9:54 Uhr, Sebastian Grüner

Quellen: Spiegel online, NTV

Cybergefahr: Risiko- und Schadenwahrnehmung.

Zielverhalten: Risikowahrnehmung auf Gesamtebene

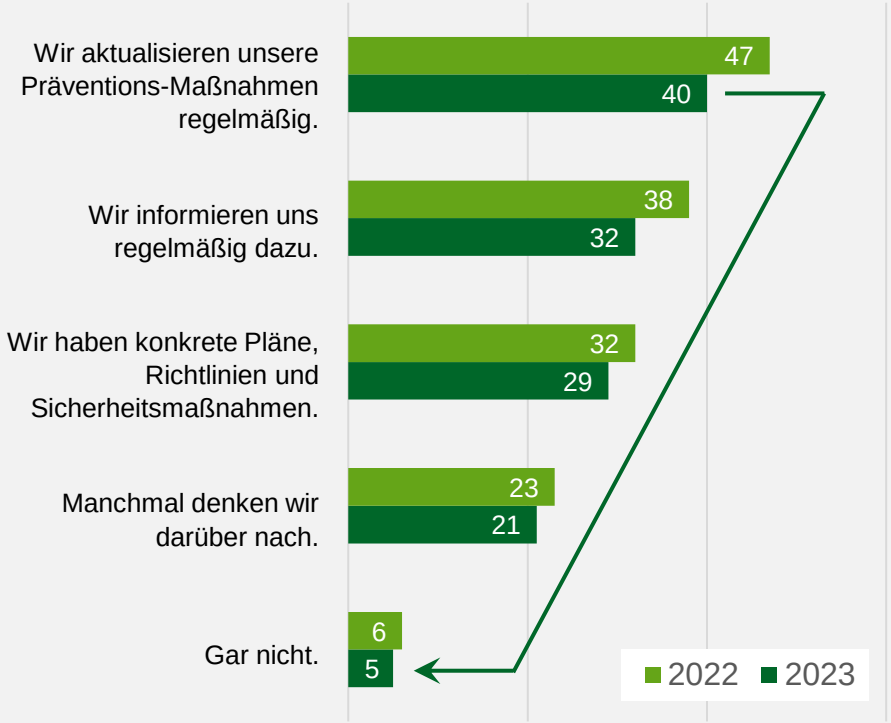
Allgemeine Risikowahrnehmung

Individuelle Risikowahrnehmung

Wahrnehmung Schadenrisiko

Wissensstand und Informationsverhalten

Wie sehr beschäftigt sich Ihr Unternehmen mit dem Thema IT- und Cybersicherheit?



Basis: Online-Befragung, Ranking absteigend nach Gesamt, Angaben in %, Mehrfachantwort möglich.

Grundlagen des Risikomanagements

Welche Zertifizierungsstandards geben Einblick in das Risikomanagement?

ISO 27005	ISRM Information Security Risk Management, Management von Informationssicherheitsrisiken
ISO 31000	Risk Management
BSI 200-3	Risikoanalyse auf Basis IT-Grundschutz
100-4	im Rahmen des Notfallmanagements

Bedrohung

- Eine Bedrohung ist ganz allgemein ein Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann

Schwachstelle

- Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems
- Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird

Gefährdung

- Eine Gefährdung ist eine Bedrohung, die konkret über eine Schwachstelle auf ein Objekt einwirkt.
- Eine Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung

Risiko

- Das Risiko ist die häufig auf Berechnungen beruhende Vorhersage eines möglichen Schadens
- Im Gegensatz zur Gefährdung umfasst das Risiko bereits eine Bewertung

Entwicklung

Beurteilung und Behandlung von Informationssicherheitsrisiken

Risiken vermindern

- Einführung einer strengen(-eren) Passwortrichtlinie

Risiken vermeiden

- Einführung strikter Zugriffskontrollen und die Umsetzung des Prinzips der minimalen Berechtigungen

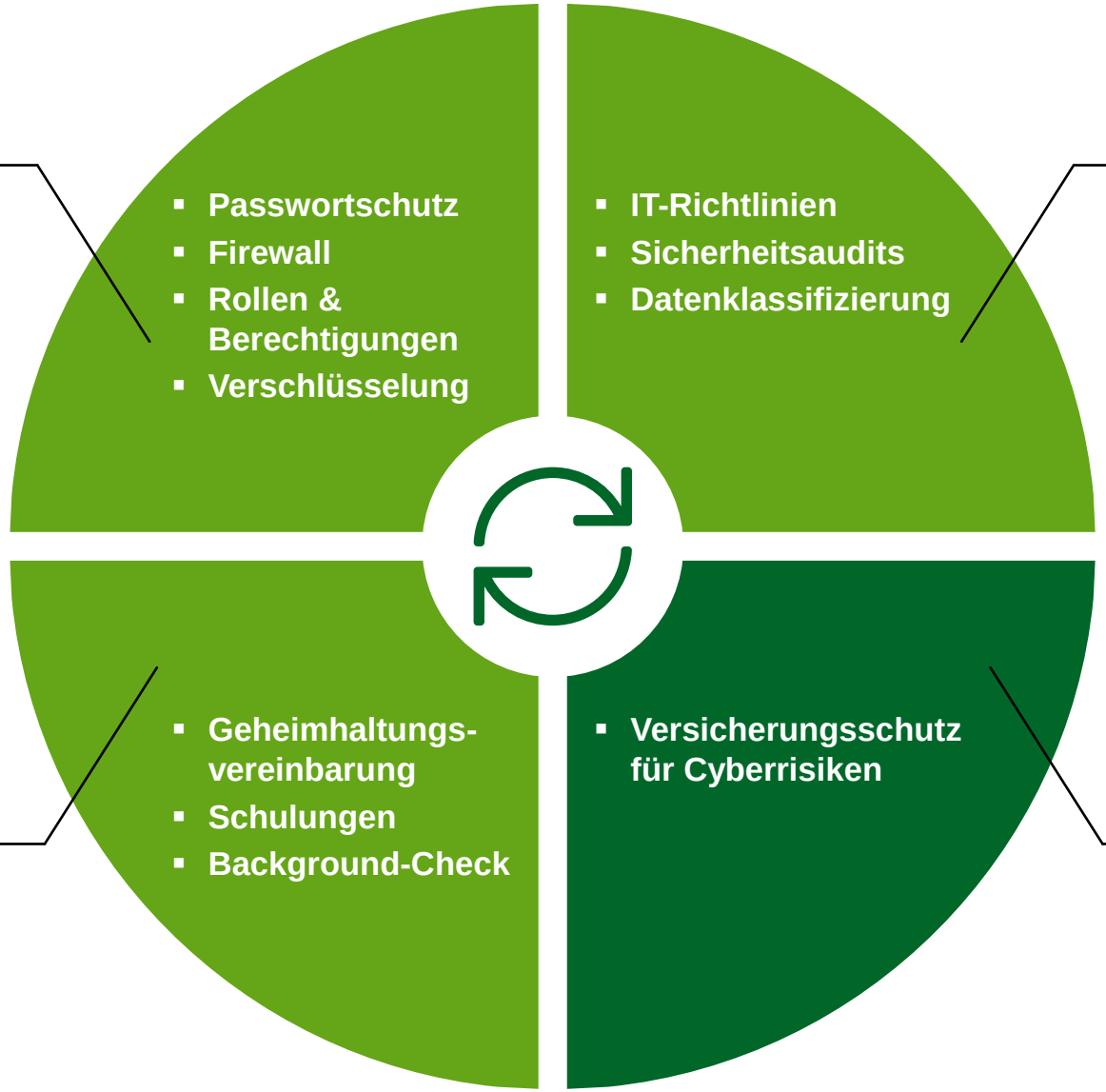
Risiken verlagern

- Auslagerung von IT-Dienstleistungen oder -Ressourcen an einen Drittanbieter, wie Cloud-Service-Provider oder Managed-Service-Anbieter.

Risiken akzeptieren

- Ein Unternehmen akzeptiert bewusst ein Risiko, wie z.B. nur ausgehende E-Mails werden einer E-Mail Verschlüsselung unterzogen. Interner Verkehr bleibt unverschlüsselt.

Gibt es den 100% Schutz vor Cyberrisiken?

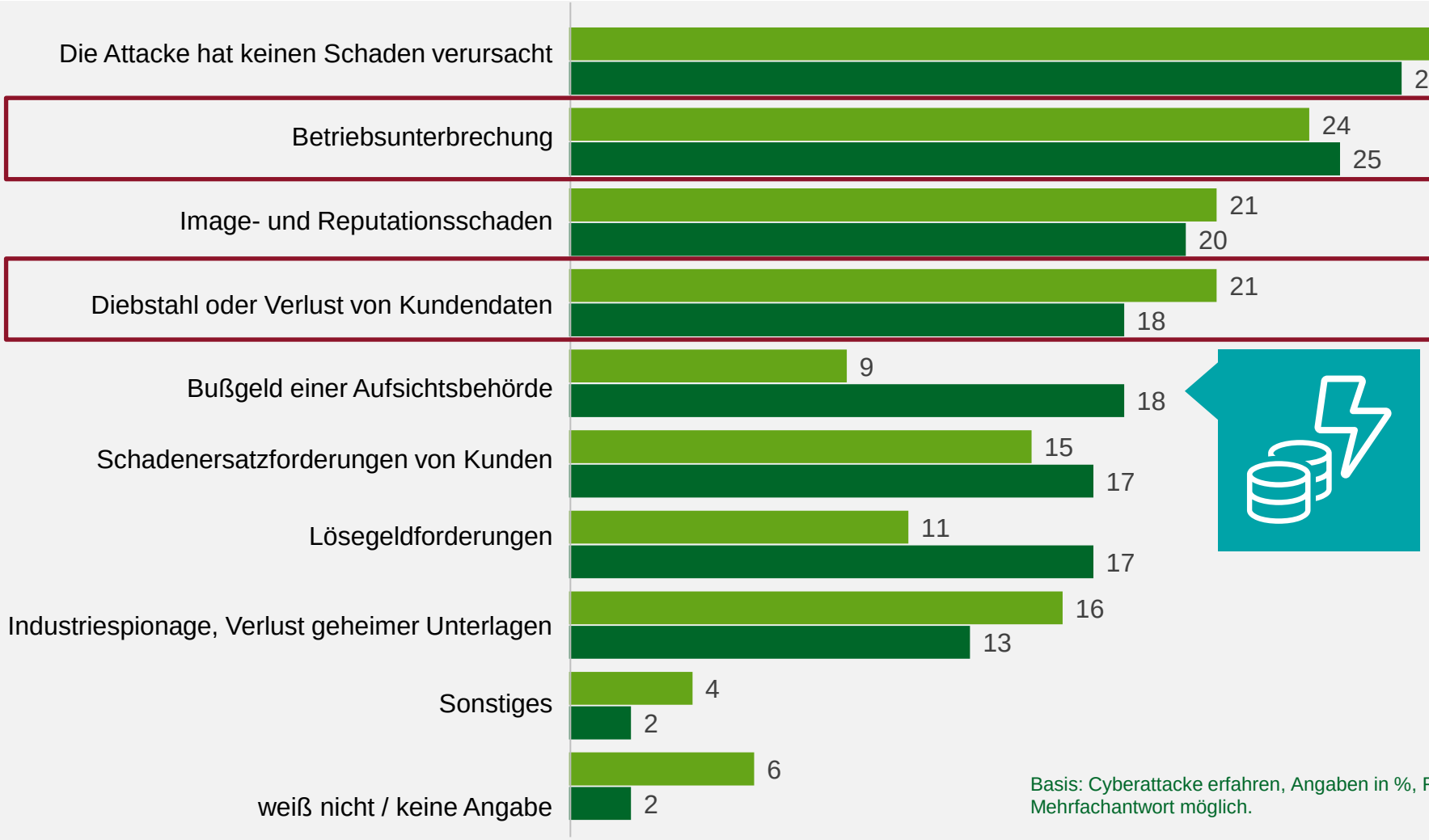


2

Sinn und Zweck einer Cyberversicherung

Welche Schäden sind tatsächlich eingetreten?

Basis: Cyberattacke mit Schaden

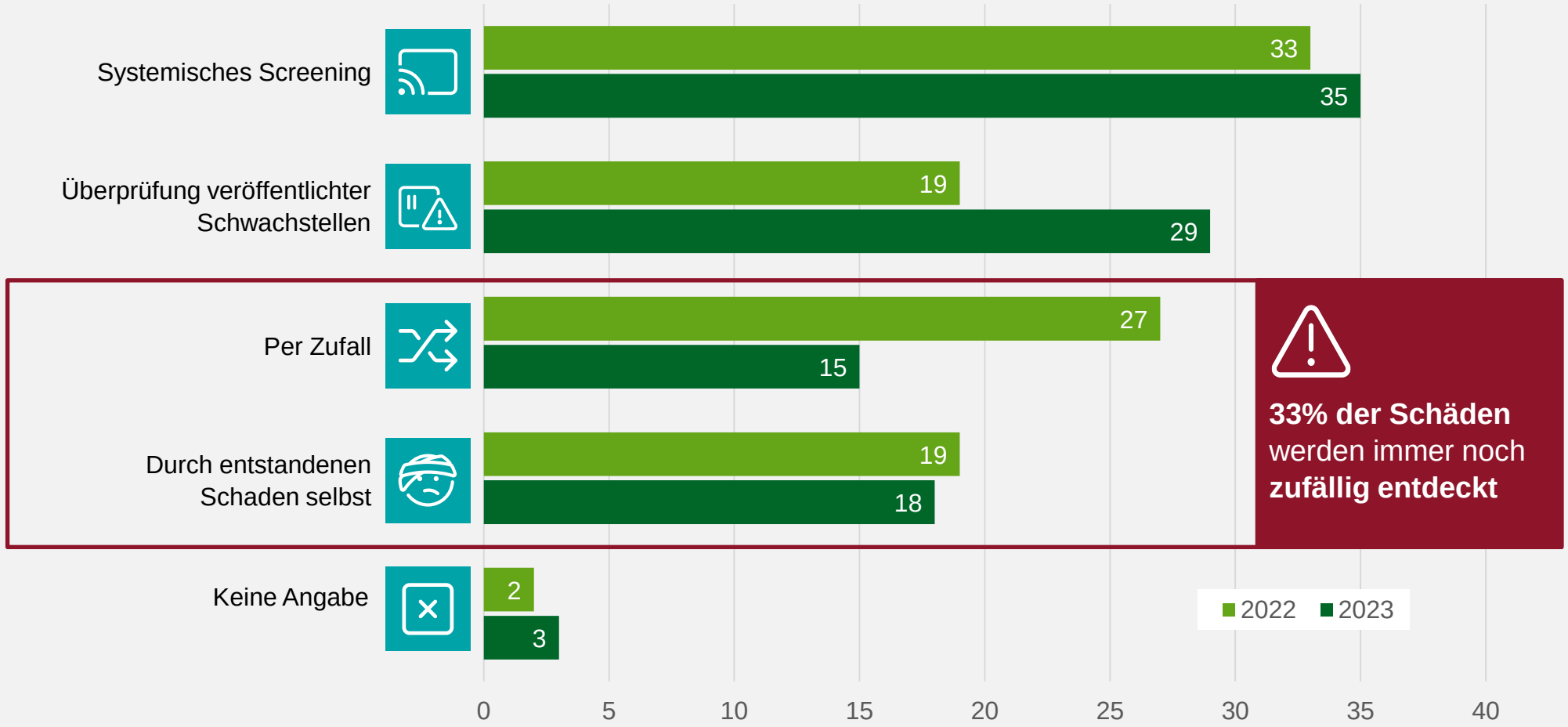


Tatsächlich erleidet ein Viertel der KMU eine BU.

Ein Fünftel erleidet einen Diebstahl von Kundendaten.

Basis: Cyberattacke erfahren, Angaben in %, Ranking absteigend nach Gesamt, Mehrfachantwort möglich.

Detektion von Cybervorfällen.



Definition des Versicherungsfalles

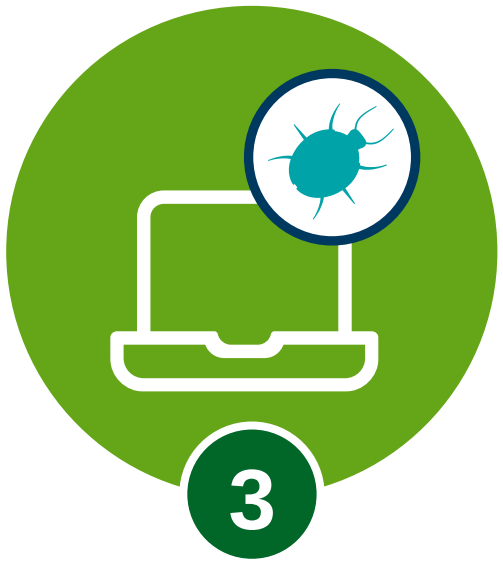
Versicherungsfall: Die Erstmalige Feststellung einer Informationssicherheitsverletzung.
Was ist aber nun eine Informationssicherheitsverletzung?

Datenschutzverletzung

Verletzung von anwendbaren in- und ausländischen gesetzlichen Regelungen zum Datenschutz (z. B. Bundesdatenschutzgesetz) in Bezug auf elektronische Daten Dritter

Datenvertraulichkeits-verletzung

Verletzung der Vertraulichkeit **elektronischer und physischer** Daten Dritter, die sich im Verfügungs-bereich der Versicherten befinden und die durch Versicherte erfolgt



Netzwerkssicherheits-verletzung

- Systemeingriffe
- Zugriffsbeschränkungen
- Datenschaden

Eigenschäden, Drittschäden, Kosten & Service

Eigenschäden

- Forensik und Schaden-feststellungskosten
- Entfernung von Schadsoftware
- Wiederherstellungskosten inkl. betriebsnotweniger Hardware
- Erstattung von Betriebsunterbrechung inkl. fortlaufender Kosten
- Vertrauensschäden

Drittschäden

- Prüfung der Haftpflichtfrage
- Verteidigung in Datenschutzverfahren
- Erstattung von Bußgeldern
- Immaterielle Schäden, z.B. Persönlichkeitsrechts-verletzungen
- Vertragsstrafen wegen Datenvertraulichkeits-verletzungen

Kosten & Services

- Benachrichtigungskosten inkl. Callcenter
- Krisenkommunikation und PR-Maßnahmen
- Rechtliche Beratung
- Kosten für Datenüber-wachungsdienstleistungen
- Abwehr von Cybererpressungen
- Systemverbesserungen

Worauf Sie Acht geben sollten

Schutz bei finanziellen Folgen einer Cyberattacke

- **Eigenschäden** – z.B. Forensik/Wiederherstellung/Betriebsunterbrechung
- **Drittschäden** – Schutz bei Schadensersatzansprüchen
- **Kosten & Service** – PR- und rechtliche Beratung, Benachrichtigungskosten

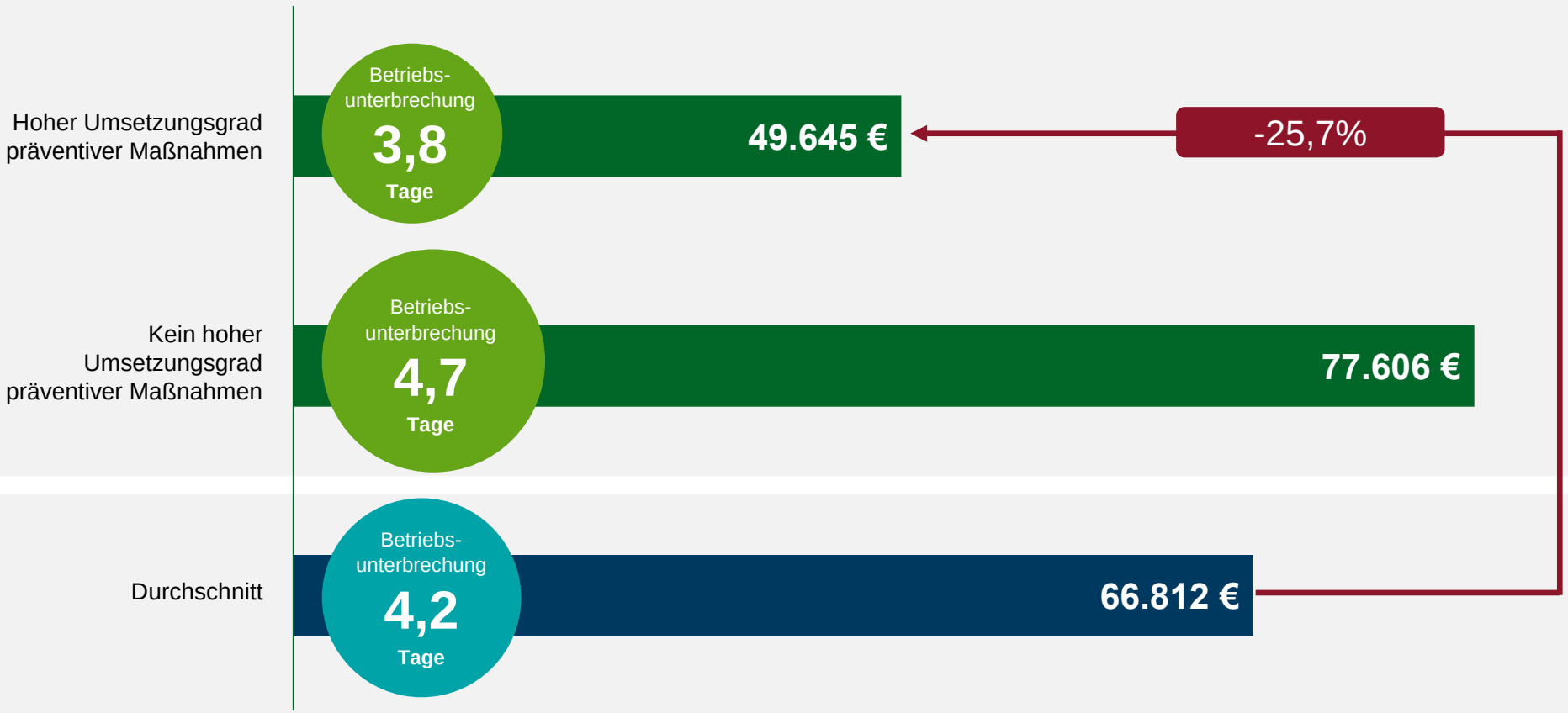
Prävention durch proaktives Mitarbeiter-Training

- **Nachhaltige** – Sensibilisierung aller Mitarbeiter durch Schulungen
- **Praxisnah** – Fingierte Angriffe durch Phishingmails
- **Sichere** – Prozesse mit dem Notfallplan

Notfallhilfe mit Krisenmanagement

- Schadenhotline rund um die Uhr verfügbar
- Soforthilfe auch bei Verdachtsfällen
- Expertennetzwerk für alle Bereiche

Auswirkung von Präventionsmaßnahmen.



Die Wahrscheinlichkeit, dass ein Cyberangriff auf ein Unternehmen mit genutztem **Notfallplan** zu einem Schaden führt, ist um **13 %** niedriger.

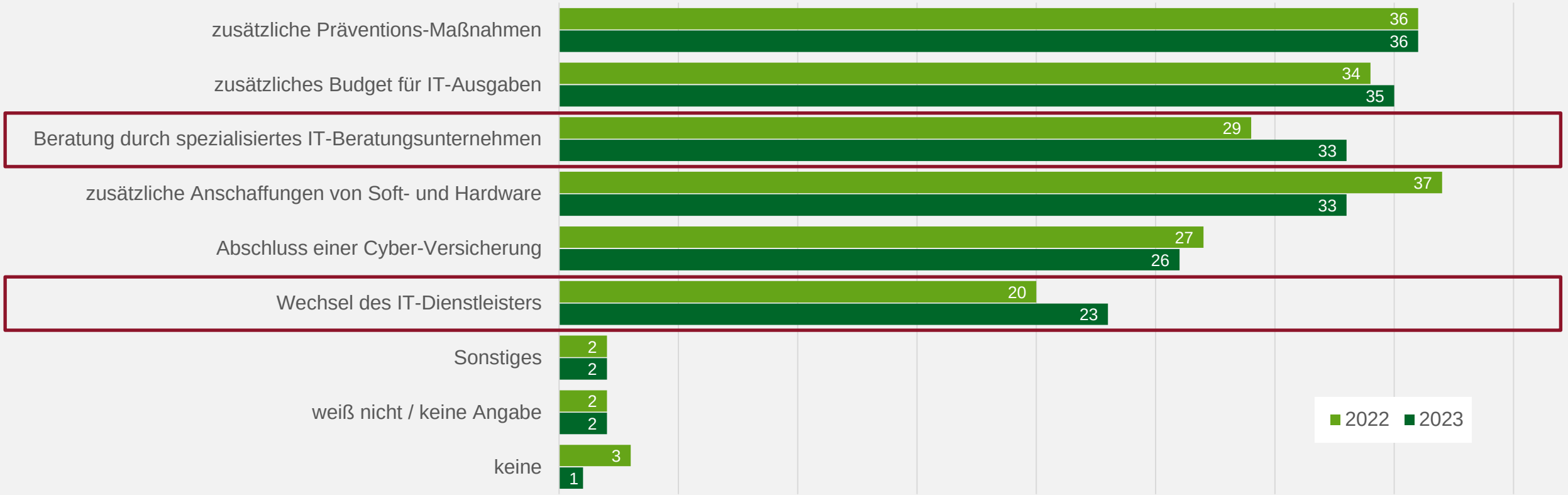
Das gleiche gilt für Unternehmen, die ihre Mitarbeiter **mindestens einmal im Jahr** sensibilisieren.

Ausblick: Maßnahmen nach einem Cyberangriff

Basis: Cyberattacke mit Schaden und Online-Befragung

Erfahrungen mit Cyberattacken: Maßnahmen nach Angriff

Welche Maßnahmen hat Ihr Unternehmen aufgrund des Angriffs vorgenommen?



Basis: Cyberattacke mit Schaden erfahren und Online-Befragung, Angaben in %, Mehrfachantwort möglich.

3

Anforderungen an Unternehmen zur Gewährleistung der IT-Sicherheit

Risikofragen

Betreiben Sie oder Dritte ein Security Operations Center (SOC), dass alle sicherheitsrelevanten Ereignisse dauerhaft überwacht?

Wieviel Benutzerkonten sind Teil der Gruppe der Domain Administratoren?

Verwenden Sie bei der Konfiguration von Dienstkonten die am geringsten erforderlichen Berechtigungen?

Erzwingen Sie Multi-Faktor-Authentifizierung (MFA) für sämtliche Zugriffe zu Ihren IT-Systemen, die für administrative Tätigkeiten genutzt werden (nicht nur bei Fernzugriffen)?

Verwenden Sie für Ihre administrativen Konten einen Password-Safe mit MFA, der nach jeder Nutzung, die Passwörter automatisiert, gemäß einer komplexen Passwortrichtlinie ändert?

Stellen Sie sicher, dass es nicht möglich ist, mit administrativen Berechtigungen ohne gesonderte Authentifizierung und MFA auf die Online Backup Infrastruktur zuzugreifen?

Obliegenheiten vor Eintritt des Versicherungsfalls zur Gewährleistung der IT-Sicherheit

Einzelne Nutzer und Befugnisebenen werden unterschieden. Hierzu sind individuelle und mit einem Passwort gesicherte Zugänge für alle Nutzer erforderlich, soweit technisch möglich;

IT-Systeme sind mit einem zusätzlichen Schutz gegen unberechtigten Zugriff ausgerüstet sind, wenn diese über das Internet erreichbar oder im mobilen Einsatz sind;

IT-Systeme verfügen über einen Schutz gegen Schadsoftware, der automatisch auf dem aktuellen Stand gehalten wird;

durch die vom Hersteller bereitgestellten Updates werden unverzüglich eingespielt. Nicht mehr unterstützte Software muss zeitnah auf einen aktuellen Stand umgestellt werden;

einem mindestens wöchentlichen Sicherungsprozess unterliegen, wobei die Sicherungsdatenträger physisch getrennt und vor dem Zugriff Unberechtigter gesichert aufbewahrt werden.

Die Versicherten sorgen durch regelmäßige Prüfung dafür, dass die Rücksicherung bei Bedarf einwandfrei durchgeführt werden kann.

Vodafone Cyber Security Services

02

Safety first!

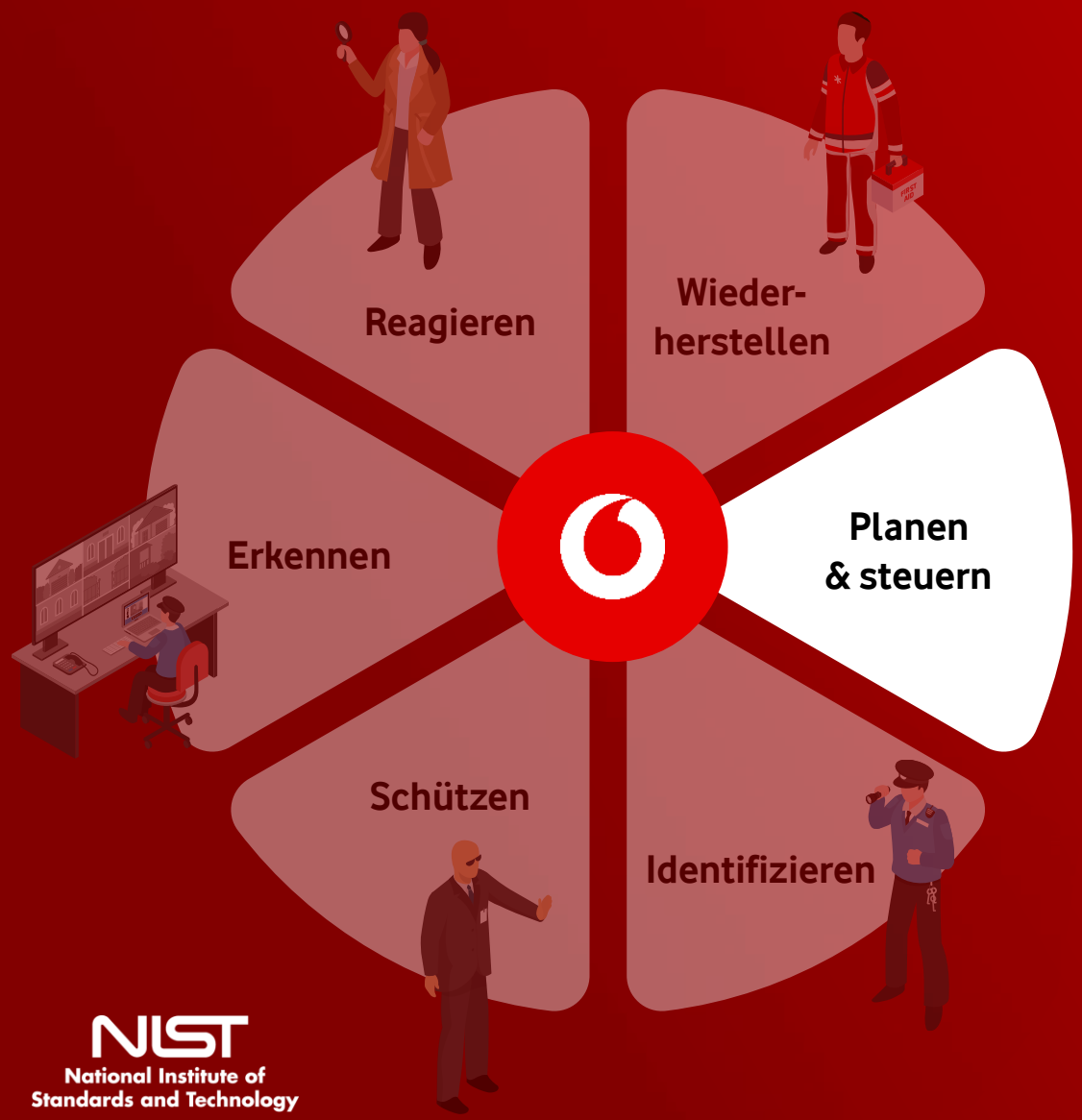
Der digitale Notfallplan gegen Cyber Angriffe

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.

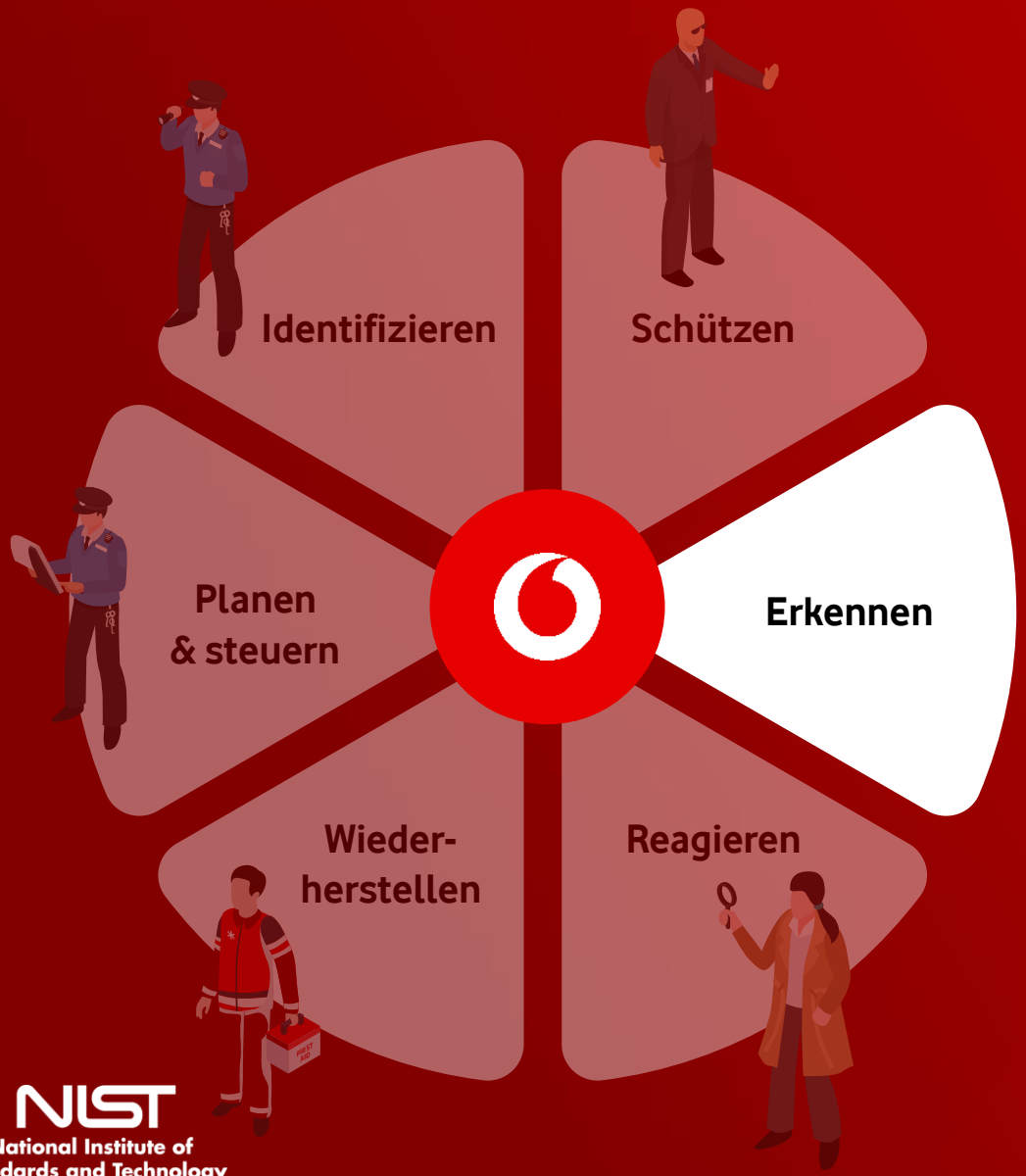
- Risikoanalyse und -bewertung
- Identifikation von Schwachstellen
- Phishing-Kampagnen

NIST
National Institute of Standards and Technology

NIST
National Institute of
Standards and Technology

Wir verhelfen zu besserem Schutz und machen es Angreifern schwer.

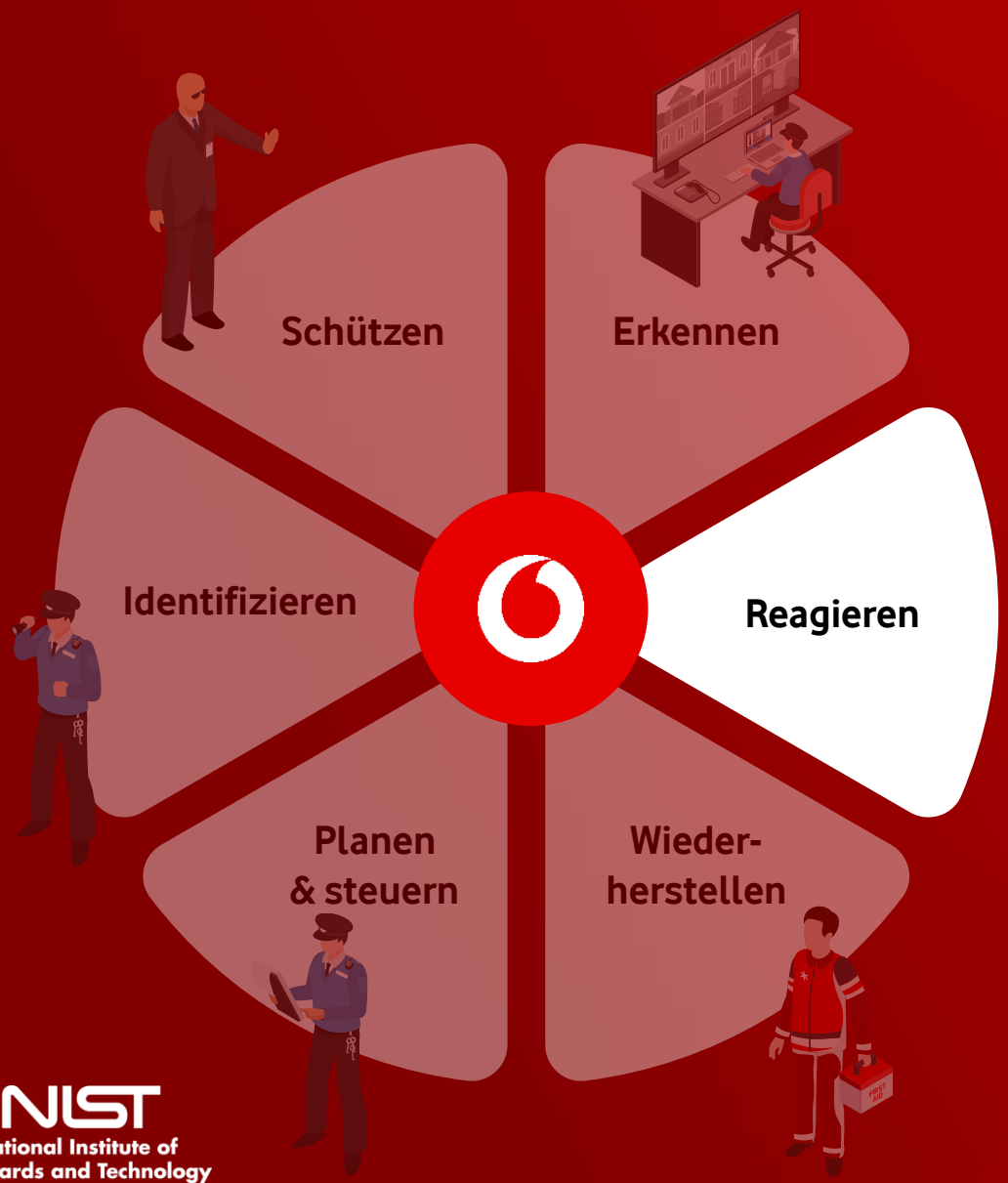
- Systemhärtung
- Netzwerksicherheit
- Endpoint Security
- Zero Trust Lösungen
- Cloud Security
- Security Awareness



NIST
National Institute of Standards and Technology

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

- Anomalie Erkennung 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 ensteht.

- 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