NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

„Wir weisen darauf hin, dass wir zur Rechts- und Steuerberatung nicht befugt sind. Soweit in unseren Ausführungen zu Rechts- oder Steuerfragen Stellung genommen wird, geben wir damit ausschließlich unsere Meinung wieder,
die wir mit größtmöglicher Sorgfalt auf Grundlage der derzeitigen Rechtslage gebildet haben.“

„Diese Informationen dienen als erste Orientierungshilfe und erheben keinen Anspruch auf Vollständigkeit. Trotz sorgfältiger Recherchen bei der Zusammenstellung der Informationen kann eine Haftung für den Inhalt nicht übernommen werden. Die hier dargestellten Erläuterungen erfolgen vorbehaltlich etwaiger Änderungen durch anstehende verordnungsrechtliche oder gesetzliche Änderungen.“

Ihr Referent

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

Paul Laser

KFZ-Mech.-Meister und KFZ-Betriebswirt
Direktionsbevollmächtigter Vertrieb Autohaus
Vertriebsservice Partnerbetreuung Nord

Neue Postanschrift:

NÜRNBERGER AutoMobil Versicherungsdienst GmbH
Direktion Dortmund AH
Wandweg 1 , 44149 Dortmund
Tel.0231-9053409
Fax. 0231-9053281409
Handy 0151-53840579
paul.laser@nuernberger-automobil.de

Besuchen Sie uns im Internet:

www.nuernberger-automobil.de
www.nuernberger-garanta.de
www.der-sichere-kfz-betrieb.de

NÜRNBERGER SofortHilfe im Schadenfall

Sie erreichen uns kostenfrei unter: **0800 531-6666***

Unbürokratisch, schnell, zuverlässig und rund um die Uhr

Wie sicher ist Ihr Unternehmen?

Referent:
Bjoern Hering

www.netzsicher.net
info@netzsicher.net

Certified Ethical Hacker (CEH 312-50)
Penetration Tester
Red Team Offensive Attacker

offensive IT der Autohaus Trompeter GmbH

kfz-betrieb 17-18 | 2023

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

CYBERSICHERHEIT

Der Hacker Ihres Vertrauens

Christoph Haumann (l.), Geschäftsführer des Autohauses Trompeter, und der zertifizierte Hacker Björn Hering überprüfen auch regelmäßig die Sicherheit des eigenen Betriebs.

Bild: Autohaus Trompeter

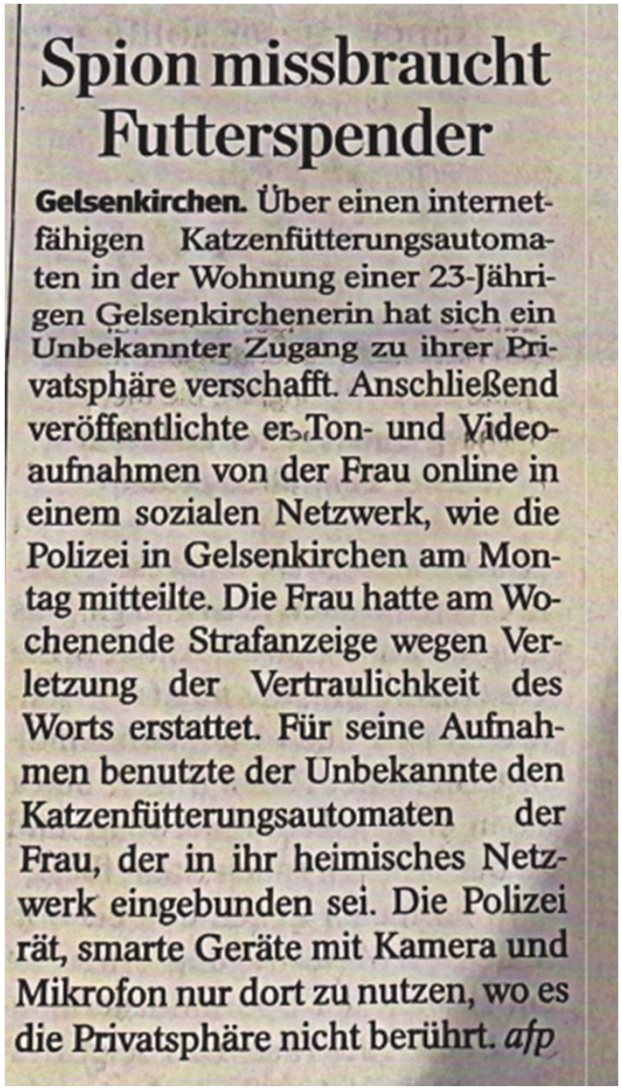
Mit Netzsicher bietet das Autohaus Trompeter Kfz-Betrieben eine besondere Dienstleistung an: Sie können einen professionellen Hacker buchen. Dieser prüft im Rahmen eines ausführlichen Penetrationstests die IT-Sicherheit auf Herz und Nieren.

Von Julia Mauritz

„Bei unseren bisherigen Attacken lag die Erfolgsquote bei 100 Prozent."

Björn Hering, Netzsicher/Autohaus Trompeter

Alexa, Echo und Co



Spion missbraucht Futterspender

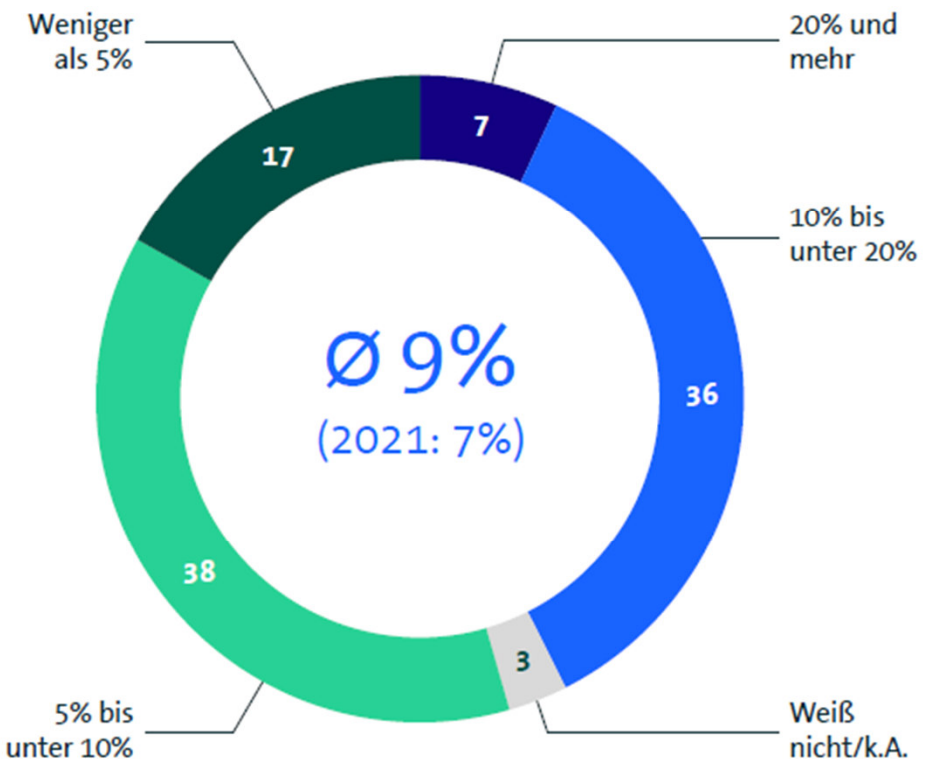
Gelsenkirchen. Über einen internetfähigen Katzenfütterungsautomaten in der Wohnung einer 23-Jährigen Gelsenkirchenerin hat sich ein Unbekannter Zugang zu ihrer Privatsphäre verschafft. Anschließend veröffentlichte er Ton- und Videoaufnahmen von der Frau online in einem sozialen Netzwerk, wie die Polizei in Gelsenkirchen am Montag mitteilte. Die Frau hatte am Wochenende Strafanzeige wegen Verletzung der Vertraulichkeit des Worts erstattet. Für seine Aufnahmen benutzte der Unbekannte den Katzenfütterungsautomaten der Frau, der in ihr heimisches Netzwerk eingebunden sei. Die Polizei rät, smarte Geräte mit Kamera und Mikrofon nur dort zu nutzen, wo es die Privatsphäre nicht berührt. *afp*

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

Cybersicherheit: Anteil der Investitionen wächst – aber zu langsam

Wie hoch ist geschätzt der Anteil des Budgets für IT-Sicherheit am gesamten IT-Budget Ihres Unternehmens?



in Prozent

13 Basis: Alle Unternehmen (n=1.066) | Quelle: Bitkom Research 2022

bitkom

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

"Die Versicherungswirtschaft kann mit Cyberversicherungen das Risiko eines Hackerangriffs absichern – ein solcher Schutz setzt aber ein gewisses Maß an Cybersicherheit voraus. Hier hat gerade die mittelständische Wirtschaft die Potenziale bei weitem noch nicht ausgeschöpft."

Jörg Asmussen, Hauptgeschäftsführer, Geschäftsführendes Mitglied des Präsidiums

Quellen

GDV Gesamtverband der Versicherer

NÜRNBERGER AutoMobil Versicherungsdienst GmbH

KBA

AUTOHAUS

Bundesamt für Sicherheit in der Informationstechnik

bitkom

kfz-betrieb

Polizei - Zentrale Ansprechstellen Cybercrime der Polizeien für Wirtschaftsunternehmen

LKA POLIZEI Nordrhein-Westfalen Landeskriminalamt

Die Justiz des Landes Nordrhein-Westfalen

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

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

Cybercrime – Definition

Cybercrime umfasst die Straftaten, die sich gegen

- das Internet
- Datennetze
- informationstechnische Systeme oder deren Daten

richten (Cybercrime im engeren Sinne), oder die mittels dieser Informationstechnik begangen werden.

Cybercrime – aktuelle Beispiele

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

Die Infektion und Manipulation von Computersystemen um

- persönliche Daten und Zugangsberechtigungen des Nutzers abgreifen und missbräuchlich nutzen zu können
- darauf befindliche Daten/Dateien des Nutzers mittels Ransomware zu verschlüsseln, um Lösegeld zu erpressen
- sie „fernsteuern“ zu können, in Botnetzen zusammen-zuschalten und für weitere kriminelle Handlungen einzusetzen

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

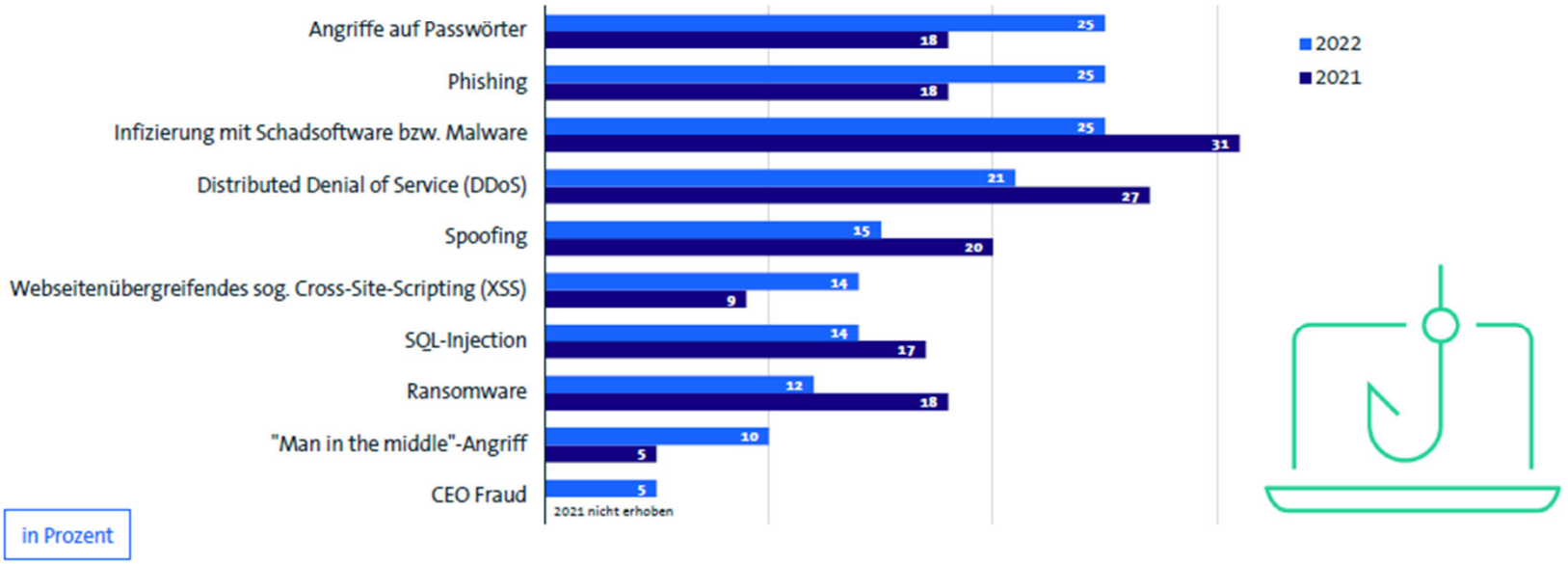
Aktuelle Fälle aus der Presse.

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

Häufigere Schäden durch Phishing & Passwortdiebstahl

Welche der folgenden Arten von Cyberangriffen haben innerhalb der letzten 12 Monaten in Ihrem Unternehmen einen Schaden verursacht?



7 Basis: Alle befragten Unternehmen (n=1.066) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2022

bitkom

Kriminalitätsentwicklung im Überblick

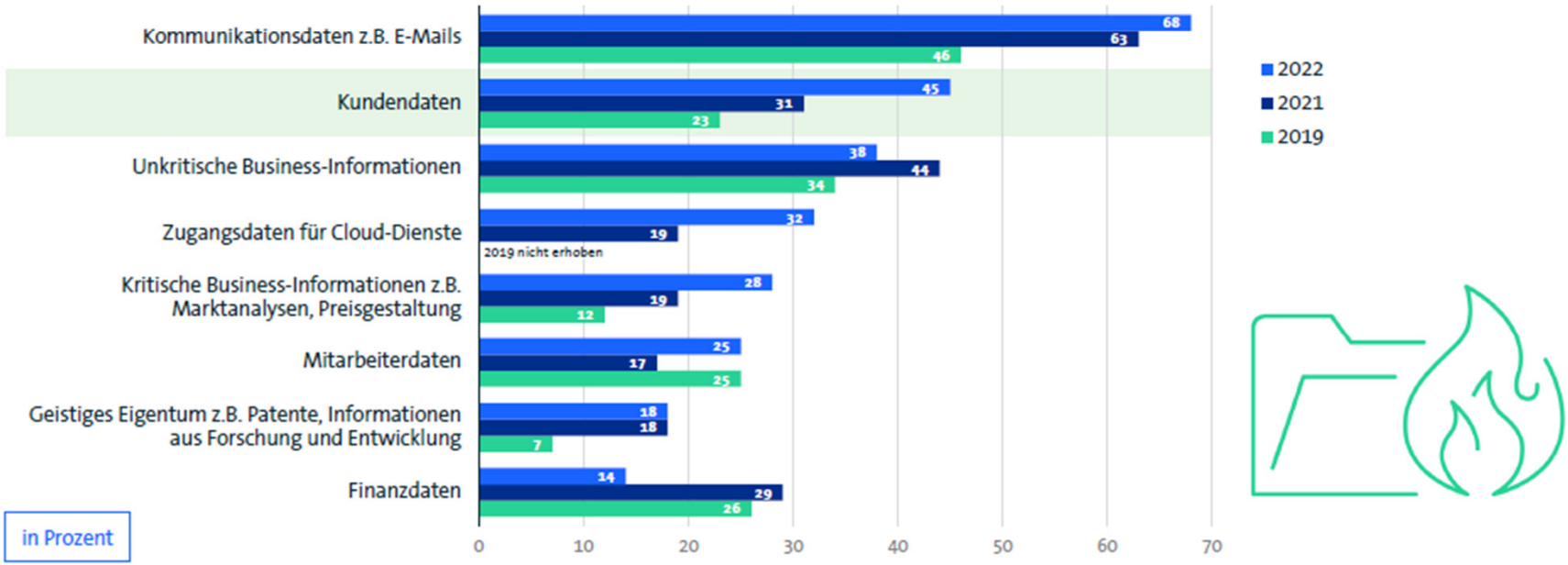
Cybercrime Studie BSI und Bitkom

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

Datendiebstahl: Immer öfter sind Dritte betroffen

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

Welche der folgenden Arten von digitalen Daten wurden in Ihrem Unternehmen gestohlen?



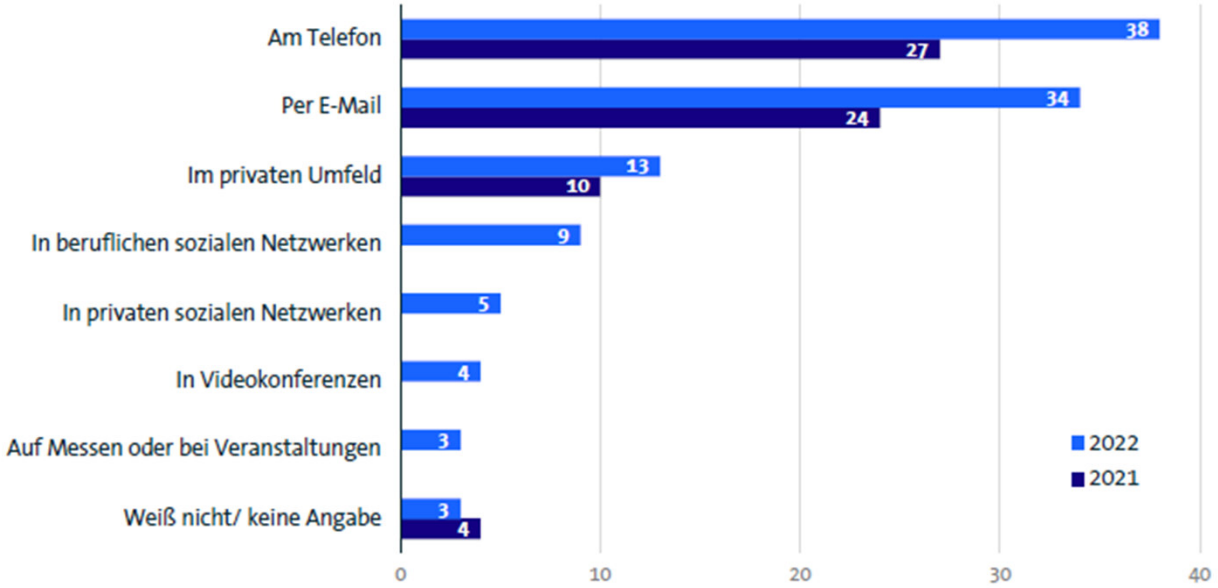
4 Basis: Alle befragten Unternehmen, die in den letzten 12 Monaten (2019: 2 Jahren) von Diebstahl von sensiblen digitalen Daten betroffen waren (2022: n=383; 2021: n=330; 2019: n=229) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2022

bitkom

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

Social Engineering: Jedes zweite Unternehmen im Visier

Von welchen der folgenden Kontexte gab es innerhalb der letzten 12 Monate Versuche, Ihre Mitarbeiter mittels Social Engineering zu beeinflussen?



48%

Es gab **Versuche** von Social Engineering (2021: 41%)

in Prozent

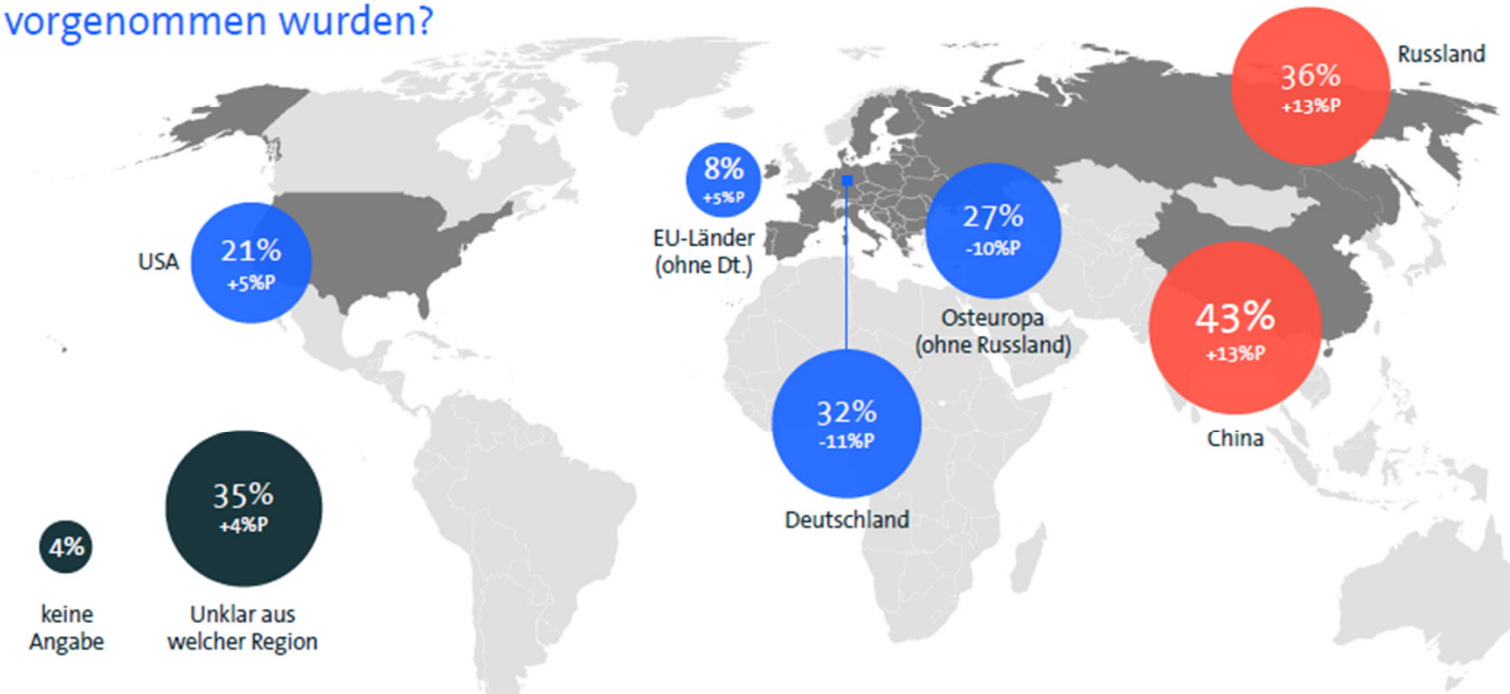
8 Basis: Alle befragten Unternehmen (n=1.066) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2022

bitkom

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

Angriffe auf Deutschland: Der Osten rückt in den Fokus

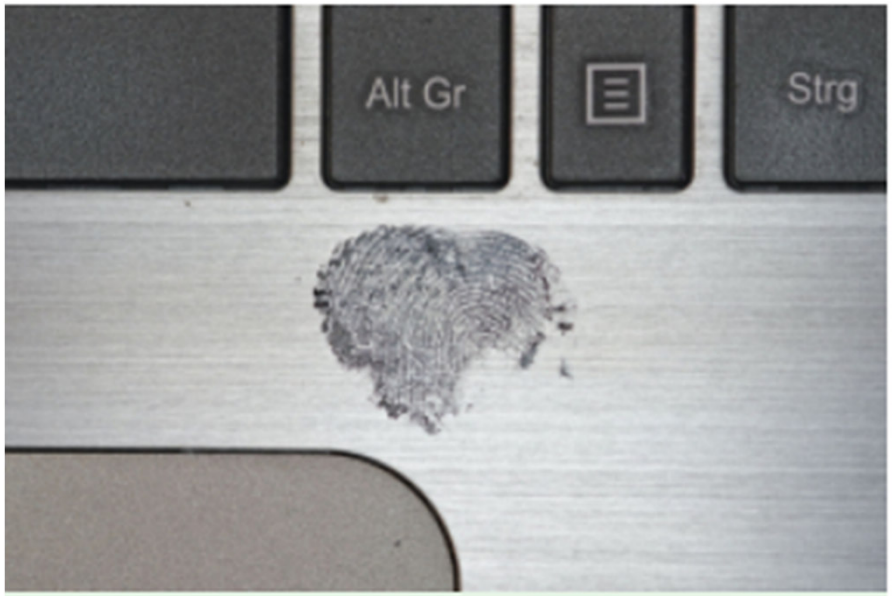
Konnten Sie feststellen, von wo aus bzw. aus welcher Region diese Handlungen vorgenommen wurden?



Prozentpunkte (%P) im Vergleich zu 2021

bitkom

10 Basis: Alle befragten Unternehmen, die in den letzten 12 Monaten von Diebstahl, Industriespionage oder Sabotage betroffen waren (2022: n=899; 2021: n=935) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2022



Sicherheit

Nur jedes zweite Unternehmen hat einen Notfallplan für Cyberattacken

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

So können sich Unternehmen schützen

Absolute Sicherheit im Netz gibt es nicht. Dennoch ist Schutz gegen Cyberangriffe möglich – und lohnt sich! Wer die Gefahren realistisch einschätzt und bei seiner IT-Sicherheit einige Grundlagen beachtet, ist gegen viele Angriffe wirksam geschützt und kann die wirtschaftlichen Folgen eines erfolgreichen Angriffs eindämmen.

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

Management

IT-Sicherheit ist Chefsache! Es braucht ein deutliches Bekenntnis der obersten Führungsebene, klare Verantwortlichkeiten und eine gute Vorbereitung auf den Ernstfall.

Zuletzt aktualisiert: 11.03.2022 • Lesedauer 3min.

1. Verantwortlichen für IT-Sicherheit benennen

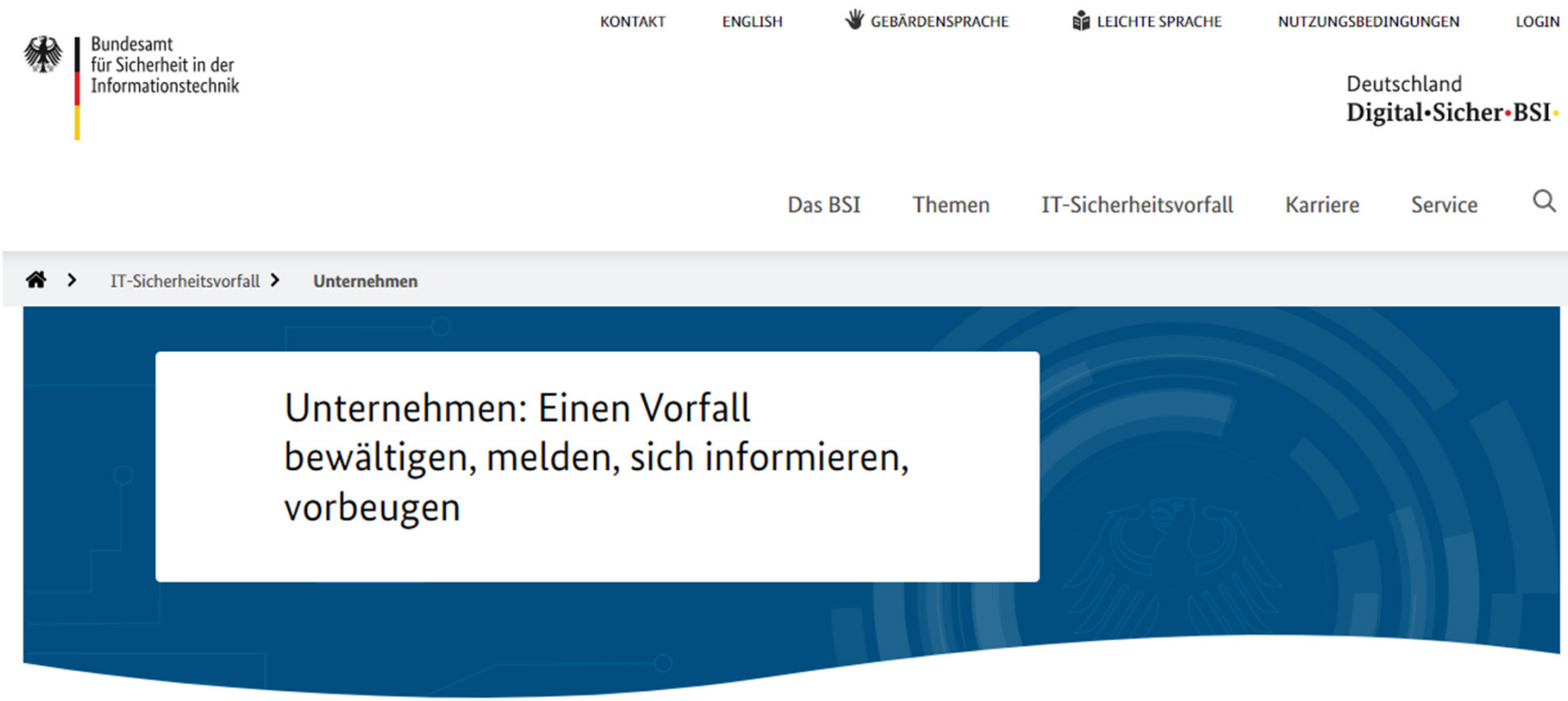
Wo werden welche Daten gespeichert? Wer darf wann auf sie zugreifen? Können Passwörter an Kollegen weitergegeben werden? Dürfen Mitarbeiter das Internet in der Firma auch privat nutzen oder berufliche Dinge am PC zuhause erledigen? In vielen Unternehmen lautet die Antwort auf diese Fragen: „weiß nicht". Sie haben all das nie geklärt. **Im Ergebnis macht im Unternehmen jeder, was er für richtig hält** – mit den entsprechenden Risiken. Besser ist es, wenn die Geschäftsführung eine Person benennt, die für alle Fragen der IT-Sicherheit verantwortlich ist – und alle Regeln schriftlich fixiert sind.

2. Notfallpläne erstellen

Wer sich auf Schwierigkeiten nicht vorbereitet, wird von ihnen schnell überrollt. **Niemand hat einen Plan, Chaos bricht aus.** Dann macht ein Kollege hektisch irgendwas, ein anderer macht gar nichts mehr, der Dritte macht das Gegenteil des ersten. Das zieht den Notfall unnötig in die Länge und vergrößert die negativen Folgen. Gute Vorbereitung und klare Handlungsanweisungen können Probleme hingegen auf ein Minimum beschränken.

3. Worst-Case-Szenario trainieren

Papier ist geduldig und auch der beste Plan nichts wert, wenn er im Ernstfall nicht funktioniert. Notfälle sollten daher nicht nur theoretisch vorbereitet, sondern auch simuliert werden – denn erst **in der praktischen Bewährungssituation fallen Schwachstellen auf**, an die vorher niemand gedacht hat.


Bundesamt
für Sicherheit in der
Informationstechnik
KONTAKT
ENGLISH
GEBÄRDENSPRACHE
LEICHTE SPRACHE
NUTZUNGSBEDINGUNGEN
LOGIN
Deutschland
Digital·Sicher·BSI·
Das BSI
Themen
IT-Sicherheitsvorfall
Karriere
Service
IT-Sicherheitsvorfall
Unternehmen
Unternehmen: Einen Vorfall bewältigen, melden, sich informieren, vorbeugen

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

Ihr Unternehmen ist von einem IT-Sicherheitsvorfall betroffen? Dann gilt es, unverzüglich zu handeln. Die folgenden Seiten geben Ihnen Unterstützung, z. B. über die Digitale Rettungskette des Cyber-Sicherheitsnetzwerks, um die ersten Schritte zur Bewältigung des Vorfalls angehen zu können.

Damit es gar nicht erst zu einem IT-Sicherheitsvorfall kommt, haben wir Ihnen hier zahlreiche Informationen zur Prävention bereitgestellt. Daneben empfehlen wir eine **› kostenlose Teilnahme an der Allianz für Cyber-Sicherheit!**

Ich habe einen Vorfall – Was soll ich tun?

› Mehr

Ich habe einen Vorfall – Checkliste Organisatorisches

› Mehr

Ich habe einen Vorfall – Checkliste Technik

› Mehr

Allianz für Cyber-Sicherheit

TOP 12
MASSNAHMEN BEI CYBER-ANGRIFFEN

Diese Fragen sollten Sie sich stellen!

Die Bewältigung eines Cyber-Angriffs ist stets individuell und Maßnahmen müssen auf die Gegebenheiten der IT-Infrastruktur vor Ort, die Art des Angriffs und die Zielsetzungen der Organisation angepasst werden. Die in den 12 als Fragen formulierten Punkten implizierten Maßnahmen dienen als Impuls und Hilfestellung bei der individuellen Bewältigung.

Das Dokument richtet sich an IT-Verantwortliche und Administratoren, in erster Linie in kleinen und mittelständischen Unternehmen.

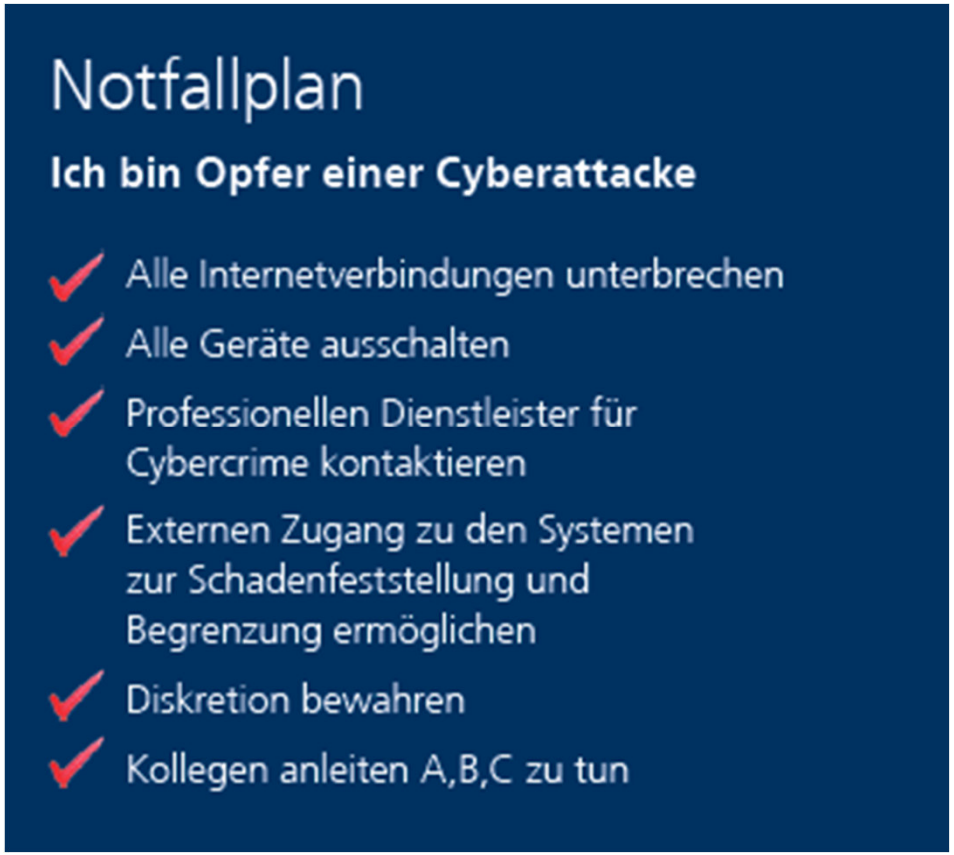
- Wurden erste Bewertungen des Vorfalls durchgeführt, um festzustellen, ob es sich um einen Cyber-Angriff oder lediglich um einen technischen Defekt handelt?
- Haben Sie kontinuierlich Ihre Maßnahmen abgestimmt, dokumentiert und an alle relevanten Personen und Verantwortlichen kommuniziert?
- Wurden System-Protokolle, Log-Dateien, Notizen, Fotos von Bildschirminhalten, Datenträger und andere digitale Informationen forensisch gesichert?
- Haben Sie stets die besonders zeitkritischen und damit vorrangig zu schützenden Geschäftsprozesse im Fokus gehabt?
- Wurden betroffene Systeme vom Netzwerk getrennt? Wurden Internetverbindungen zu den betroffenen Systemen getrennt? Wurden alle unautorisierten Zugriffe unterbunden?
- Wurden Backups gestoppt und vor möglichen weiteren Einwirkungen geschützt?
- Wurden Maßnahmen unternommen, um das gesamte Maß der Ausbreitung festzustellen? Wurden alle angegriffenen Systeme identifiziert?
- Wurden die beim Cyber-Angriff ausgenutzten Schwachstellen in Systemen oder (Geschäfts-) Prozessen durch relevante Maßnahmen adressiert und behoben?
- Wurden, nach Abstimmung, die Polizei oder relevante Behörden (Datenschutz, Meldepflichten, etc.) benachrichtigt?
- Wurden die Zugangsberechtigungen und Authentisierungsmethoden für betroffene (geschäftliche und ggf. private) Accounts überprüft (z.B. neue Passwörter, 2FA)?
- Wird das Netzwerk nach dem Vorfall weiter überwacht, um mögliche erneute Anomalien festzustellen?
- Wurden die betroffenen Daten und Systeme wiederhergestellt oder neu aufgebaut?

Das Dokument ist ein gemeinsames Produkt nachfolgender Organisationen: Bundeskriminalamt, Charter of Trust, Deutscher Industrie- und Handelskammertag e.V., eco – Verband der Internetwirtschaft e.V., Initiative Wirtschaftsschutz, Nationale Initiative für Informations- und Internet-Sicherheit e.V., VOICE - Bundesverband der IT-Anwender e.V., Allianz für Cyber-Sicherheit des Bundesamtes für Sicherheit in der Informationstechnik

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

Wir lassen Sie nicht im Regen stehen - Präventivmaßnahmen und Handlungsempfehlungen

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH



NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

Checkliste **Technische Maßnahmen**

- ☐ Sicherheitsupdates automatisch und zeitnah einspielen und alle Systeme auf dem aktuellen Stand halten
- ☐ Mindestens einmal wöchentlich Sicherungskopien machen
- ☐ Administratoren-Rechte nur an Administratoren vergeben
- ☐ Alle Systeme, die über das Internet erreichbar oder im mobilen Einsatz sind, zusätzlich schützen
- ☐ Manipulationen und unberechtigten Zugriff auf Sicherungskopien verhindern
- ☐ Alle Systeme mit einem Schutz gegen Schadsoftware ausstatten und diesen automatisch aktualisieren lassen
- ☐ Sicherungskopien physisch vom gesicherten System trennen
- ☐ Mindestanforderungen für Passwörter (z. B. Länge, Sonderzeichen) verlangen und technisch erzwingen
- ☐ Jeden Nutzer mit eigener Zugangskennung und individuellem Passwort ausstatten
- ☐ Wiederherstellen der Daten aus der Sicherungskopie regelmäßig testen
- ☐ Öffnen Sie E-Mails nicht automatisch, nur wirklich vertrauenswürdige Mails
- ☐ Vor dem Öffnen von Mails: Prüfen Sie Absender und Betreff
- ☐ Löschen Sie lieber eine Mail zu viel als eine zu wenig

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

Checkliste Maßnahmen gesetzliche Verpflichtungen

1 Datenschutzbeauftragter (DSB)

JA, wenn > 20 Personen im ständigen (arbeitszeitunabhängigem) Umgang mit personenbezogenen Daten sind

2 Verzeichnis von Verarbeitungstätigkeiten

Personenbezogene Daten:
JA, Führung eines Verzeichnisses

3 Datenschutzverpflichtung von Beschäftigten

JA, bei Aufnahme der Beschäftigung und jährliche Wiederholung z. B. über Onlineschulung mit Zertifikat

4 Informations- und Auskunftspflichten

JA, insbesondere im Betrieb durch Flyer, Aushang und auf der Website in der Datenschutzerklärung

5 Löschen von Daten

JA, aber erst nach Ablauf der gesetzlichen Aufbewahrungspflicht (z. B. 10 Jahre)

6 Sicherheit

JA, besondere Sicherung, wenn sensible Daten – weitere Schutzmaßnahmen (siehe technische Maßnahmen)

7 Auftragsverarbeitung

JA, Auftragsdatenverarbeitungsvereinbarung AVV, z. B. mit einem IT-Dienstleister. Eine AVV ist immer dann notwendig, wenn der Kunde nicht selbst, einzeln die Einwilligung zu Verarbeitung seiner Daten unterschreibt.

8 Datenschutzverletzungen

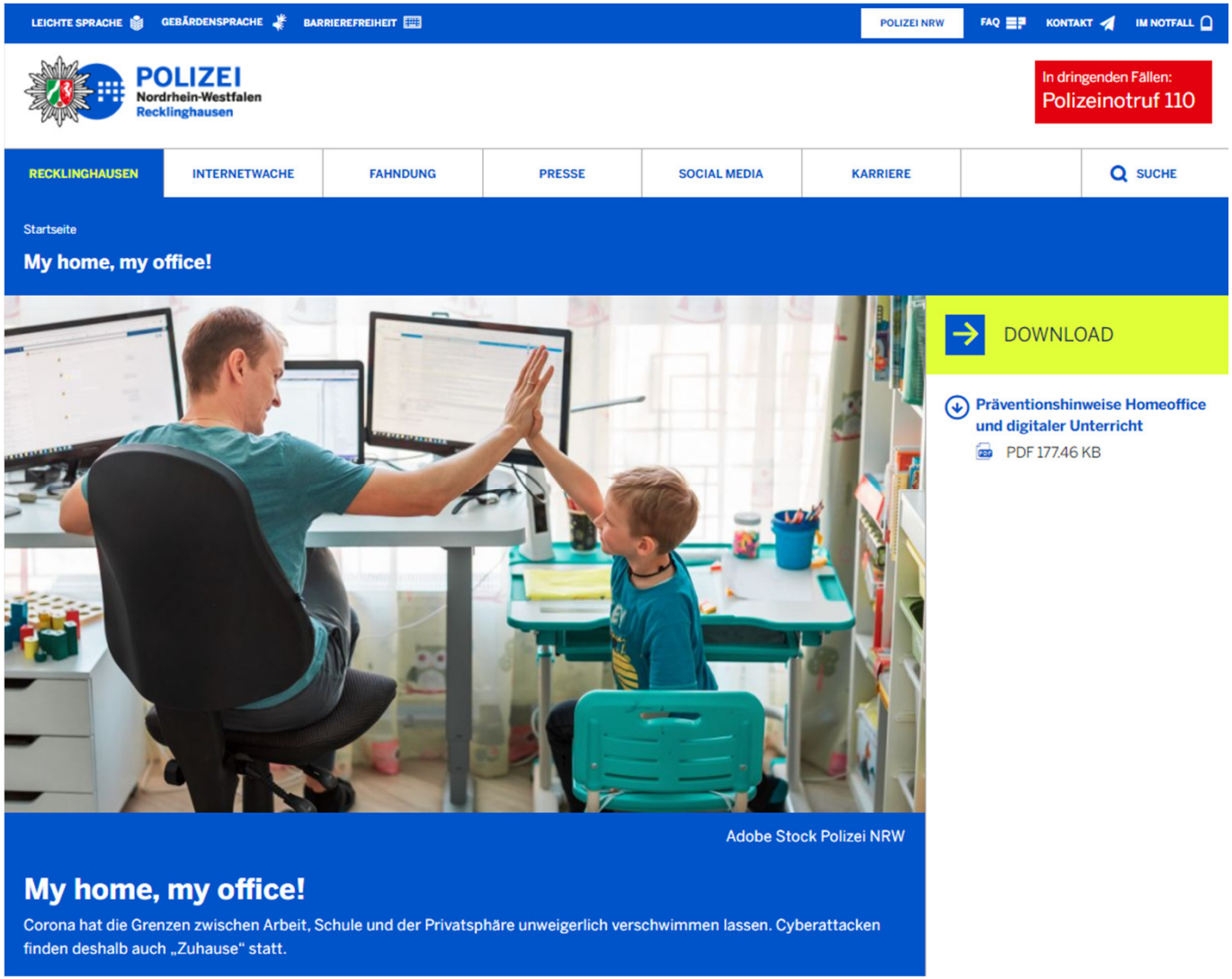
JA, Sicherheitsvorfälle müssen unverzüglich an Aufsichtsbehörde gemeldet werden. Betroffene nur bei hohem Risiko

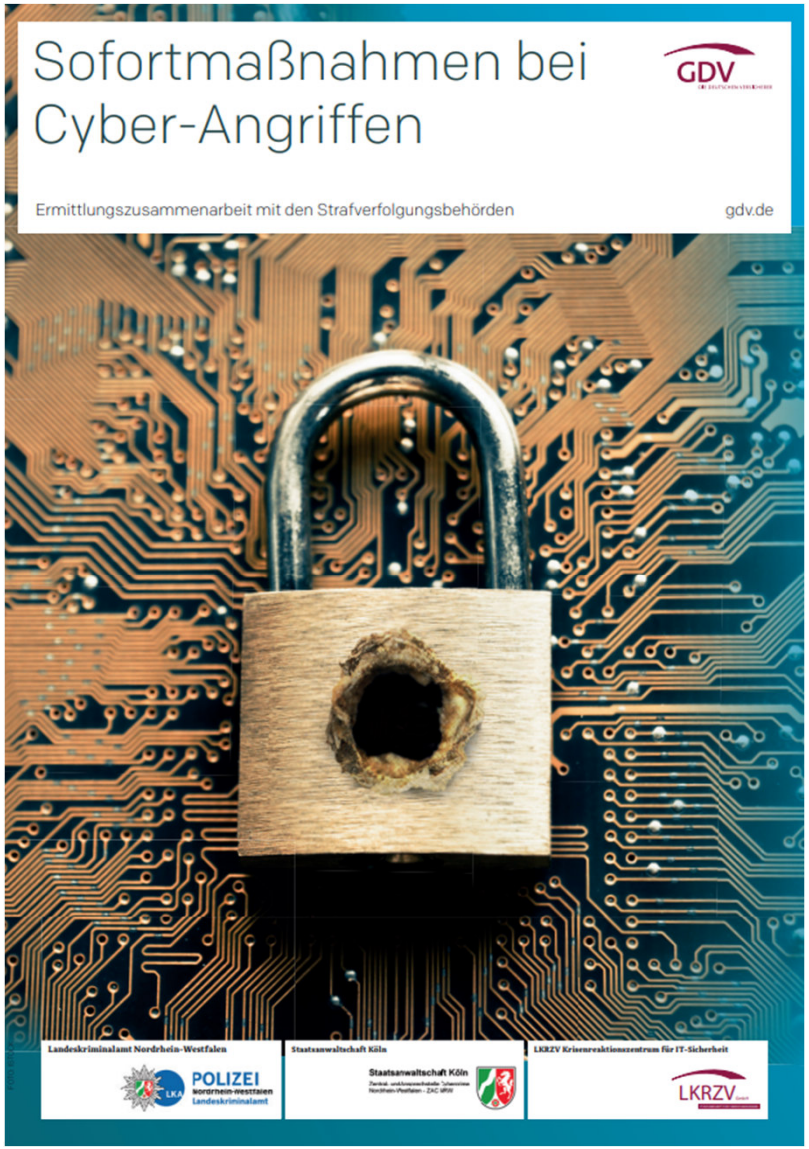
9 Datenschutz-Folgeabschätzung

NEIN, sofern kein hohes Risiko besteht

10 Videoüberwachung

JA, sofern vorhanden gesonderter Hinweis für Mitarbeiter und Kunden


LEICHTE SPRACHE
GEBÄRDENSPRACHE
BARRIEREFREIHEIT
POLIZEI NRW
FAQ
KONTAKT
IM NOTFALL
POLIZEI
Nordrhein-Westfalen
Recklinghausen
In dringenden Fällen:
Polizeinotruf 110
RECKLINGHAUSEN
INTERNETWACHE
FAHNDUNG
PRESSE
SOCIAL MEDIA
KARRIERE
SUCHE
Startseite
My home, my office!
DOWNLOAD
Präventionshinweise Homeoffice und digitaler Unterricht
PDF 177.46 KB
Adobe Stock Polizei NRW
My home, my office!
Corona hat die Grenzen zwischen Arbeit, Schule und der Privatsphäre unweigerlich verschwimmen lassen. Cyberattacken finden deshalb auch „Zuhause" statt.



NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

FOTO: CDU LANDTAG NRW

Der Schutz der Daten der Versicherten genießt ohne Zweifel bei der deutschen Versicherungswirtschaft einen hohen Stellenwert!
Denn Daten sind heutzutage in einigen Branchen wertvoller als Bargeld. Und das gilt bei der Versicherungswirtschaft für geradezu jeden Bereich. Es betrifft nämlich nicht nur Kontoverbindungen und Passwörter für den E-Mailverkehr. Hier geht es um Krankendaten, Schadenunterlagen oder auch um klassische Betriebsgeheimnisse. Virtuelle Angriffe sind daher eine ganz reale Gefahr für eine ganze Branche!

Deswegen ist es wichtig, dass die Versicherungswirtschaft eng und vertrauensvoll mit der Justiz zusammenarbeitet – und zwar nicht erst, wenn die Tat öffentlich geworden ist. Denn je früher wir als Justiz beteiligt werden, umso besser können wir helfen, den Schaden zu begrenzen und natürlich in erster Linie die Tat aufklären. Uns ist dabei bewusst, dass jeder erfolgreiche Cyber-Angriff auch ein Angriff auf den guten Ruf des betroffenen Unternehmens ist. Doch gerade die erfolgreiche Strafverfolgung kann ein wesentlicher Bestandteil Ihrer Krisenkommunikation werden.

Deswegen versteht sich die nordrhein-westfälische Justiz in diesen Fällen auch als Dienstleister, soweit das mit den Aufgaben der Strafverfolgung zu vereinbaren ist. Die ZAC steht Ihnen sieben Tage die Woche rund um die Uhr als kompetenter Ansprechpartner zur Verfügung.

PETER BIESENBACH
Minister der Justiz des Landes Nordrhein-Westfalen

FOTO: GDV

Die Digitalisierung schreitet unaufhaltsam voran und bringt viele Vorteile mit sich:
Prozesse beschleunigen sich, neue Geschäftsmodelle entstehen, die Kommunikation mit den Kunden wird schneller und direkter. Für die Versicherungswirtschaft sind aber auch Sicherheitsaspekte und der unbedingte Schutz der Kundendaten essentiell.

Denn die Digitalisierung birgt auch Risiken. Cyber-Kriminelle versuchen etwa, durch Angriffe oder Erpressung an die Daten der Unternehmen zu gelangen. Dies gilt es zu bekämpfen – vorausschauend ebenso wie bei einem akuten Angriff.

Präventiv hat die deutsche Versicherungswirtschaft in den vergangenen Jahren mit dem Aufbau des Lage-und Krisenreaktionszentrums für IT-Sicherheit (LKRZV) bereits hervorragende Arbeit geleistet. Jetzt möchten wir unsere Kooperation mit den Strafverfolgungsbehörden weiter intensivieren und freuen uns, gemeinsam mit dem Landeskriminalamt und der Zentral- und Ansprechstelle Cybercrime (ZAC NRW) einen Krisenplan vorlegen zu können, der unter der Schirmherrschaft des nordrhein-westfälischen Ministers der Justiz erarbeitet wurde. Es ist unser erklärtes Ziel, diesen Krisenplan fortlaufend weiterzuentwickeln und durch Vernetzung der verantwortlichen Stellen Krisen auf Landes- und Bundesebene effektiv zu bewältigen.

WERNER SCHMIDT
Vorsitzender des Ausschusses Betriebstechnik, Digitalisierung und IT, Gesamtverband der Deutschen Versicherungswirtschaft e.V.

CYBER-SICHERHEIT – EIN KRITISCHER ERFOLGSFAKTOR

Als Teil der Kritischen Infrastrukturen muss die deutsche Versicherungswirtschaft weitreichende Anforderungen an die Sicherheit ihrer IT-Systeme erfüllen. Dazu zählt in erster Linie der präventive Schutz vor externen und internen Angriffen. Im Krisenfall gilt es für Versicherungsunternehmen, schnell geeignete Gegenmaßnahmen zu ergreifen und zeitnah die Strafverfolgung mit dem Ziel einer Täterermittlung einzuleiten. Um dies zu gewährleisten, sollen zukünftig durch einen engeren und schnelleren Informationsaustausch zwischen den betroffenen Versicherungsunternehmen und den Strafverfolgungsbehörden die Ermittlungsarbeiten wirksamer unterstützt werden.

DIESES INFORMATIONSBLATT BIETET HIERFÜR ERSTE HILFESTELLUNGEN:

Unternehmen können Krisensituationen wie einen Cyber-Angriff ohne eine vorausschauende Vorbereitung nicht erfolgreich bewältigen. Anhand prognostischer Szenarien sollten die in einem Unternehmen bei der Krisenbewältigung einzubindenden Personen, die Meldewege und die Entscheidungsbefugnisse in einem Cyber-Notfallplan festgelegt werden. Nur so lässt sich die erforderliche Handlungsschnelligkeit gewährleisten. Die gebotene Handlungssicherheit lässt sich durch die entsprechende Einübung der Abläufe im Krisenfall trainieren.

Wesentlicher Bestandteil der Krisenbewältigungsstrategie sollte die unverzügliche Erstattung einer Strafanzeige sein. Die Strafverfolgungsbehörden sind professionelle Krisenmanager, die betroffene Unternehmen unterstützen können. Die Sicherung von Beweismitteln ermöglicht die Ermittlung des Tathergangs. Sie erfolgt unter Berücksichtigung der Unternehmensinteressen in Abstimmung mit dem geschädigten Unternehmen.

Die Strafverfolgungsbehörden streben eine effektive und vertrauensvolle Kooperation an. Dazu gehört auch ein koordiniertes Reputations- und Öffentlichkeitsmanagement. Interne Ermittlungsressourcen des angegriffenen Unternehmens können in die Ermittlungen einbezogen werden. Hier empfiehlt sich eine frühzeitige Abstimmung des Vorgehens im Einzelfall.

Wirksame Krisenbewältigung und effektive Strafverfolgung sind zwei ineinandergreifende Komponenten. Nur durch das Aufhellen des Dunkelfeldes und die Verurteilung von Tätern lässt sich das Geschäftsmodell der Cyber-Kriminellen nachhaltig bekämpfen. Die Strafanzeige ermöglicht den Rückfluss behördlicher Erkenntnisse aus dem Ermittlungsverfahren zu geschädigten oder gefährdeten Unternehmen. Justiz und Polizei haben spezialisierte Cybercrime-Dienststellen geschaffen, die den Unternehmen als zentrale Ansprechpartner zur Verfügung stehen.

ZUSTÄNDIGKEITEN UND REAKTIONEN IM KRISENFALL

Das Hauptkriterium für eine effektive Strafverfolgung bei Cyber-Angriffen ist schnelles Handeln. Daher sollten bereits vorab Maßnahmen ergriffen und Zuständigkeiten geklärt werden, um im Angriffsfall sicher und schnell handeln zu können.
Hierzu gehört die Erstellung des Krisenplans und entsprechende regelmäßige Übungen.

Unter anderem sind folgende Fragen vor dem Ernstfall zu klären:

1 ZUSTÄNDIGKEITEN KLÄREN

- ☐ Interne Abstimmungsprozesse regeln:
  - Management
  - Rechtsabteilung
  - IT
  - Sicherheitsbeauftragte/r
  - Datenschutzbeauftragte/r
  - Pressestelle
  - Betriebsrat
- ☐ Rechtliche Zuständigkeit für Strafanzeigenerstattung klären.

2 KRISENFALL DARLEGEN

- ☐ Möglichst genaue Vorfallbeschreibung verfassen.
- ☐ Daten sichern und bereitstellen, ggf. in Absprache mit der/dem Datenschutzbeauftragten und dem Betriebsrat.
- ☐ Beweissicherung in Absprache mit den Ermittlungsbehörden vornehmen (*bspw. Logfiles*).

3 REAKTIONEN KOORDINIEREN

- ☐ Verhaltens- und Kommunikationsrichtlinien für Mitarbeiter und Führungskräfte erstellen.
- ☐ Ermittlungsbehörden Zutritt zum Gebäude sowie Zugang und Zugriff zu den betroffenen IT-Systemen gewähren.
- ☐ Strategie für Reputations- und Öffentlichkeitsmanagement erarbeiten, ggf. in Abstimmung mit den Ermittlungsbehörden.


In Nordrhein-Westfalen sind die zuständigen Behörden das Cybercrime-Kompetenzzentrum des Landeskriminalamtes Nordrhein-Westfalen und die bei der Staatsanwaltschaft Köln angesiedelte und landesweit zuständige Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW). Beide sind im Cyber-Krisenfall jederzeit erreichbar.
Landeskriminalamt Nordrhein-Westfalen
Cybercrime-Kompetenzzentrum
Zentrale Ansprechstelle Cybercrime
Single Point of Contact
Völklinger Straße 49 | 40221 Düsseldorf
Tel.: +49 211 939 4040
Fax: +49 211 939 194040
cybercrime.lka@polizei.nrw.de
POLIZEI
Nordrhein-Westfalen
Landeskriminalamt
Staatsanwaltschaft Köln
Zentral- und Ansprechstelle Cybercrime
Nordrhein-Westfalen - ZAC NRW -
Am Justizzentrum 13 | 50939 Köln
Tel.: +49 221 477 4922 (24/7-Hotline)
Fax: +49 221 477 4400
zac@sta-koeln.nrw.de
Staatsanwaltschaft Köln
Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen -ZAC NRW
Bei versicherungsspezifischen Fragen zur IT-Sicherheit wenden Sie sich bitte an:
LKRZV
Krisenreaktionszentrum für IT-Sicherheit der deutschen Versicherungswirtschaft
(Erreichbarkeit 24/7): krisenreaktionszentrum@gdv.de
während der Geschäftszeiten:
Tel.: +49 30 2020 5050
Fax: +49 30 2020 6050
LKRZV

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

Cybersicherheit

Cyberversicherer machen erstmals Verluste – Markt legt weiter zu

Hackerangriffe sind eine wachsende Gefahr für die Wirtschaft, zeigen neue Zahlen der Cyberversicherer. 2021 mussten sie deutlich mehr Schäden regulieren, die Aufwendungen überstiegen gar erstmals die Einnahmen. Der Markt wächst indes weiter.

Angesichts zunehmender Hackerangriffe auf die deutsche Wirtschaft sind die Cyberversicherer 2021 erstmals in die Verlustzone gerutscht. „Unter dem Strich betrug die Schaden-Kostenquote fast 124 Prozent nach 65 Prozent ein Jahr zuvor", sagte Jörg Asmussen, Hauptgeschäftsführer des Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV). Jedem eingenommen Euro in der Sparte standen somit Ausgaben für Schäden und Verwaltung von 1,24 Euro gegenüber.

Insgesamt zählten die Cyberversicherer im vergangenen Geschäftsjahr knapp 3.700 Schäden durch Hackerangriffe (+56 Prozent). Dafür leisteten sie rund 137 Millionen Euro – fast dreimal so viel wie 2020. Dazu kamen Schäden aus den Vorjahren, für die zusätzliche Rückstellungen gebildet werden mussten, sowie Abschluss- und Verwaltungskosten. „Einzelne Cyberattacken hatten besonders schwerwiegende Folgen und führten jeweils zu Kosten im oberen einstelligen Millionenbereich", so Asmussen. An Beiträgen verbuchten die Unternehmen rund 178 Millionen Euro (+49 Prozent).

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

Jahr	Anzahl Versicherungsunternehmen	Beiträge[1]		Leistungen[2]		Schaden-Kosten-Quote[3]
		in Mio. EUR	Veränderung ggü. Vorjahr	in Mio. EUR	Veränderung ggü. Vorjahr	
2020	33	106	39,0%	37	59,0%	64,7%
2021	39	178	49,2%[4]	137	187,6%[4]	123,7%

Wann greift die Cyberversicherung?

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

- Gezielte und ungezielte Angriffe auf das Kundensystem.
- Verstöße gegen gesetzliche Vorschriften des Datenrechts.

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

202 Milliarden Euro Schaden pro Jahr

Wodurch sind Ihrem Unternehmen innerhalb der letzten 12 Monate Schäden im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

Schaden durch…	Schadenssummen in Mrd. Euro (2022)	Schadenssummen in Mrd. Euro (2021)	Schadenssummen in Mrd. Euro (2019)	Schadenssummen in Mrd. Euro (2017)
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	41,5	61,9	13,5	5,3
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	10,7	24,3	5,3	0,7
Datenschutzrechtliche Maßnahmen (z.B. Information von Kunden)	18,3	17,1	4,4	3,2
Patentrechtsverletzungen (auch schon vor der Anmeldung)	18,8	30,5	14,3	7,7
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	41,5	29	11,1	8,6
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	21,1	22,7	11,1	3,5
Imageschaden bei Kunden oder Lieferanten/ Negative Medienberichterstattung	23,6	12,3	9,3	7,7
Kosten für Ermittlungen und Ersatzmaßnahmen	10,1	13,3	18,3	10,6
Kosten für Rechtsstreitigkeiten	16,2	12,4	15,6	5,5
Höhere Mitarbeiterfluktuation/Abwerben von Mitarbeitern	-	-	-	2,2
Sonstige Schäden	0,9	0	<0,1	<0,1
Gesamtschaden pro Jahr	202,7	223,5	102,9	54,8

9 Basis: Alle befragten Unternehmen, die in den letzten 12 Monaten (2019 und 2017: 2 Jahren) von Diebstahl von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (2022: n=899; 2021: n=935; 2019: n=801; 2017: n=571) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2022

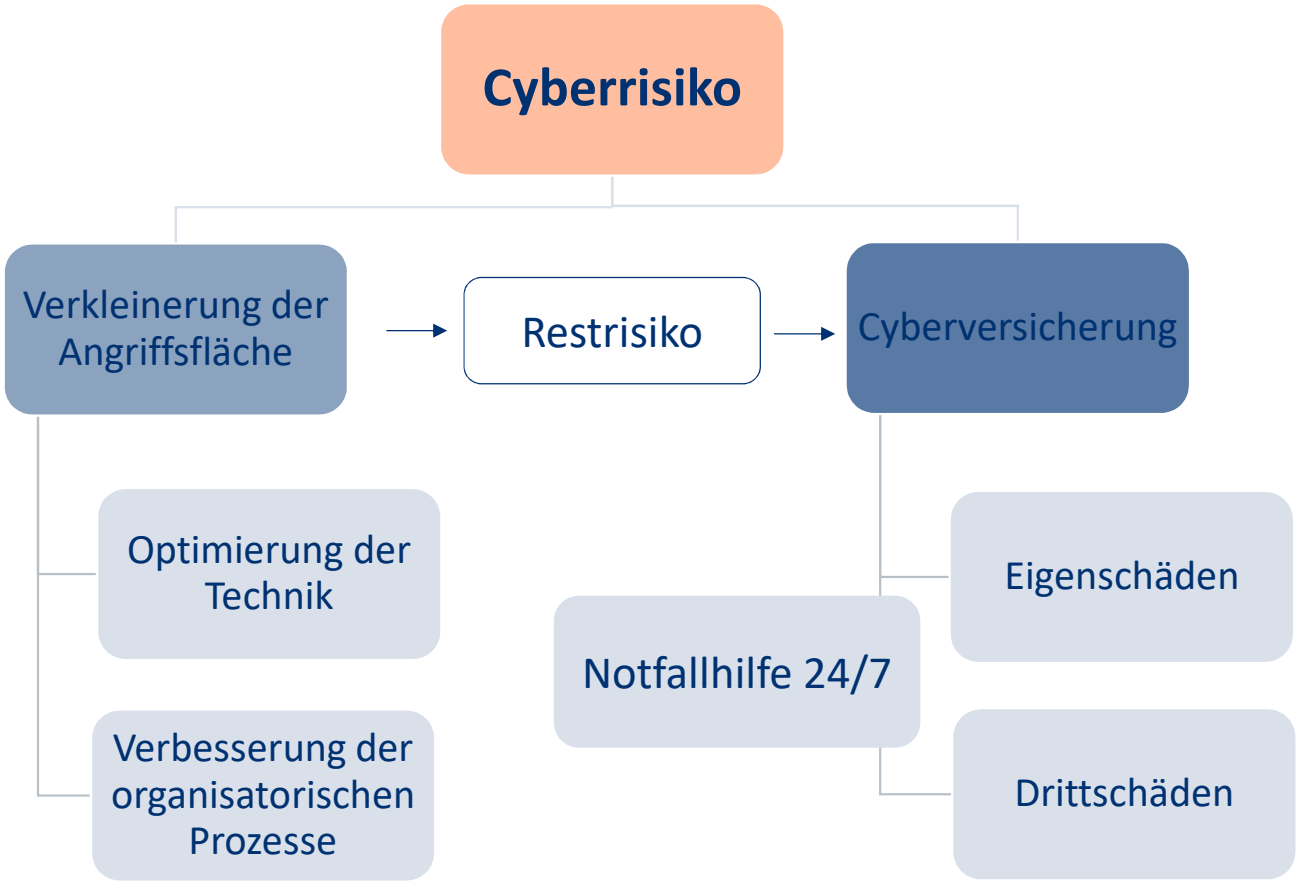
bitkom

Cyberversicherung

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

Das Cyberrisiko kann nur verkleinert, aber nicht verhindert werden.

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH



Produktstruktur der Business Line Cyberversicherung.

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

Prävention	• Sicherheitstrainings & Prävention • optional
Notfallhilfe	• Notfallhilfe 24/7
Eigenschäden	• Betriebsunterbrechung • Datenwiederherstellung • Cyber-Betrug • Cyber-Erpressung
Drittschäden	• Cyber-Haftpflicht • Kreditkarten-Betrug (PCI)

Ihr Betrieb

Betriebsart	**Kfz-Reparaturwerkstatt**
Jahresnettoumsatz	**5.000.000 EUR**
Gesamtversicherungssumme	**1.000.000 EUR** pro Versicherungsfall und -jahr

Versicherungsumfang

Versicherungsschutz	Versicherungssumme	Selbstbeteiligung
Sicherheitstraining & Prävention		keine
Notfall-Hotline und -hilfe 24/7	1.000.000 EUR	5.000 EUR
Betriebsunterbrechung	1.000.000 EUR	5.000 EUR
Datenwiederherstellung	500.000 EUR	5.000 EUR
Cyber-Erpressung	50.000 EUR	5.000 EUR
Cyber-Betrug	50.000 EUR	5.000 EUR
Cyber-Haftpflicht	1.000.000 EUR	5.000 EUR
Kreditkarten-Betrug (PCI)	50.000 EUR	5.000 EUR
Ihr Beitrag		**2.782,05 EUR**

Darin enthalten ist die Versicherungssteuer

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

Diese Hinweise und Voraussetzungen sind wichtig für Ihren Versicherungsschutz

Backups
Sie sichern Ihre Daten mindestens einmal pro Woche. Wir empfehlen Ihnen außerdem einmal jährlich einen Test zur Wiederherstellung der Daten durchzuführen. Dieser Test ist aber nicht verpflichtend für den Versicherungsschutz.

Antiviren-Software
Alle Mitarbeiter haben einen Viren-/Malwareschutz auf ihren Arbeitsplatzrechnern (Desktops, Laptops) installiert.

Software-Patching
Software-Patches (Updates) werden spätestens 3 Monate nach Erhalt einer Benachrichtigung durch das Softwareunternehmen installiert.

Cyber-Betrug
Geänderte Zahlungsdaten von Geschäftspartnern, die per Mail oder Telefon eingehen werden immer auf ihre Echtheit überprüft. Dafür wird der Geschäftspartner über die bisher gespeicherten Kontaktdaten kontaktiert und eine Rückbestätigung eingeholt.

Verantwortliche Personen
Für die IT-Sicherheit im Unternehmen ist eine der folgenden Personen verantwortlich:
- Leiter der IT-Abteilung
- Leiter des Betriebs
- Leiter für interne Sicherheit
- Ausgelagerter Anbieter (z. B. externe IT-Beratung)

• IT-Administrator (z. B. IT-Supporter, der sich um alle IT-Angelegenheiten kümmert)

Prävention
Ihre Mitarbeiter werden über Bedrohungen der Cybersicherheit informiert:
• Diskussionen in Teamsitzungen über Cybersicherheit oder
• Informeller Austausch von Informationen, Artikeln oder Newslettern zur Cybersicherheit oder
• Regelmäßige Pflichtschulungen (mindestens einmal pro Jahr) oder
• Simulationsübungen (z. B. Phishing E-Mails)

Netzwerkschutz
Sie haben eine Firewall, die von einer qualifizierten Person, z. B. einem internen oder externen IT-Experten eingerichtet und konfiguriert wurde.

Daten-Kopien
Backup-Kopien Ihrer Daten werden aufbewahrt
• bei einem Cloud-Anbieter oder
• auf einem externen Festplattenlaufwerk oder
• auf Datensicherungs-Bändern oder
• auf einem Speichergerät im eigenen Netzwerk

Zugriffsrechte
Ihre Mitarbeiter haben nur Zugang zu den für sie wichtigen Geschäftsanwendungen, z. B. Auftragssystem, Zahlungssystem, Buchungssystem, Produktionssteuerungssystem. Anwendungen, die für einzelne Mitarbeiter nicht relevant sind, sind für sie gesperrt.

Tipp des Tages:

Auf einen Blick

- Analysen, Schulungen und Software für eine resiliente IT-Sicherheit
- drei miteinander kombinierbare Schwerpunkte:

Aktuelle Förderbekanntmachung

Bekanntmachung des Ministeriums für Wirtschaft, Industrie, Klimaschutz und Energie des Landes Nordrhein-Westfalen (MWIKE) zur Durchführung des Förderprogramms

„Mittelstand Innovativ & Digital“ (MID) Gutscheine

MID-Digitalisierung
MID-Analyse
MID-Innovation

vom 01. Januar 2023

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

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

ZUWENDUNGSBESCHEID

(Projektförderung)

Zuwendung des Landes Nordrhein-Westfalen auf Grundlage der Förderbekanntmachung „Mittelstand Innovativ & Digital (MID)" des Ministeriums für Wirtschaft, Industrie, Klimaschutz und Energie des Landes Nordrhein Westfalen" Programmteil MID Digitale Sicherheit

Förderkennzeichen: 005-2212-9055_0420
PtJ-Aktenzeichen: 2212ms030
Vorhaben: „Mittelstand Innovativ & Digital (MID)"

Bezug: Ihr Vorhaben zum Programmteil Mittelstand Innovativ & Digital (MID) - MID-Digitale Sicherheit
Ihr Antrag vom 07.12.2022 mit Ergänzung vom 09.12.2022

Anlagen:

- **Allgemeine Nebenbestimmungen für Zuwendungen zur Projektförderung (ANBest-P, Stand 02.06.2020)**
- **Projektüberwachung**

Den Durchführungszeitraum für die Projektarbeiten legen wir wie folgt fest:

2.1	Projektstart	**15.01.2023**
	Projektende	**14.07.2023**

Die Zuwendung darf nur für die in diesem Zeitraum durch das Vorhaben verursachten Ausgaben abgerechnet werden.

Wird MID-Digitale Sicherheit nicht innerhalb des o.g. Durchführungszeitraums in Anspruch genommen und nicht innerhalb des o.g. Bewilligungszeitraums mit der bewilligenden Stelle abgerechnet, **verliert MID-Digitale Sicherheit mit Ablauf des Bewilligungszeitraums 31.12.2023 die Gültigkeit.**

3. *Finanzierungsart/-höhe*

Die Zuwendung wird in der Form eines nicht rückzahlbaren Zuschusses in Höhe der nachfolgenden Förderquote zu den geplanten Gesamtausgaben gewährt. **Umsatzsteuer, die nach § 15 Umsatzsteuergesetz (UStG) als Vorsteuer abziehbar ist, ist nicht zuwendungsfähig.**

3.1	Gesamtausgaben in Höhe von	**5.550,16 €**
	Förderquote	**80 %**
	Zuwendung in Höhe von	**4.440,12 €**

4. *Bewilligungsrahmen*

Die Bereitstellung des Zuwendungsbetrages ist wie folgt vorgesehen:

im Haushaltsjahr 2023	**4.440,12 €**

Kostenvoranschlag

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

ANGEBOT ZUR DURCHFÜHRUNG EINES PENETRATION TESTS
DURCH UNSERE OFFENSIVE IT "NETZSICHER".

SCOPE:
ES ERFOLGT EIN "BLACK-BOX" ANGRIFF AUF 8
STANDORTE DES UNTERNEHMENS OHNE VORWISSEN
ÜBER DIE IT-STRUKTUR (EXTERNER HACKER ANGRIFF).
DABEI WIRD EIN SOCIAL ENGINEERING (TEST DER
MITARBEITER) AUSDRÜCKLICH MIT EINBEZOGEN. ZIEL IST
ES, EINEN WEG ZU FINDEN, UM EINE BACKDOOR IM
UNTERNEHMEN ZU INSTALLIEREN. DESWEITEREN WIRD EINE
PHYSISCHE BEGEHUNG DES OBJEKTS MIT EINBEZOGEN. IM
ANSCHLUSS AN DEN ERFOLGTEN ANGRIFF (POSITIV ODER
NICHT) WIRD DURCH UNS EINE AWARENESS-SCHULUNG
ALLER RELEVANTEN MITARBEITER DURCHGEFÜHRT. DER
PENETRATION TEST IST ZU JEDER ZEIT TRANSPARENT UND
ERFOLGT INNERHALB WIE AUCH AUßERHALB DER ÜBLICHEN
GESCHÄFTSZEITEN (AUCH ZU ABEND/NACHTZEITEN SOWIE
AN WOCHENENDEN UND FEIERTAGEN).

PEN01-OSINT	VORARBEIT EXTERNER ANGRIFF, OSINT, EXTERNE SCANS, CVE BEGUTACHTUNG, PRÜFUNG DER MITARBEITER AUF DATEN-LEAKS	1.675,52
PEN02-AKTIV	DURCHFÜHRUNG PENETRATION TEST (AKTIVER ANGRIFF) INKLUSIVE STRESSTEST DER MITARBEITER	1.675,52
PEN03-PHISH	ERSTELLUNG PHISHING MAIL, MAILVERTEILER, "MALICIOUS PDF", SPEAR PHISHING ATTACKE,TELEFON-SCAMS	314,16
PEN05-INTERN	BEGEHUNG DER OBJEKTE, INTERNER SCAN INKL. PRÜFUNG	1.047,20
	******* ZWISCHENSUMME ********	***4.712,40

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

Artikel-Nr.	Bezeichnung	Menge	Einzelpreis	Gesamt
	********* ÜBERTRAG **********			***4.712,40
	DER ACTIVE DIRECTORY AUF SCHWACHSTELLEN, PASSWÖRTER UND SENSIBLE DATEN, ANGRIFFE MITTELS WINDOWS-NETZWERK MECHANISMEN (NTLM RELAY, PASS-THE-HASH, KERBEROASTING) PRÜFUNG DES WLAN SYSTEMS AUF VERWUNDBARKEITEN			
PEN04-SCHULUNG	SCHULUNG ALLER RELEVANTEN MITARBEITER, IN BLÖCKEN VON CA 10 MAS PRO SITZUNG			837,76

Es bediente Sie: Hering, Bjoern

Arbeitspreis	Material/Fahrzeug	USt. 19,00%	Austausch-Altwert	USt. auf Altwert	Auslagen*	Gesamtbetrag
5.550,16 €	0,00 €	1.054,53 €	0,00 €	0,00 €	0.00 €	**6.604,69 €**

Netto 5.550,16 €


Ref. Ares(2016)956541 - 24/02/2016
Europäische
Kommission
Benutzerleitfaden
zur Definition von KMU
A
B
C
1
2
3
STEP.1
STEP.2
STEP.3
Binnenmarkt,
Industrie,
Unternehmertum
und KMU

2. Ihre Fragen und Anliegen
paul.laser@nuernberger-automobil.de

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

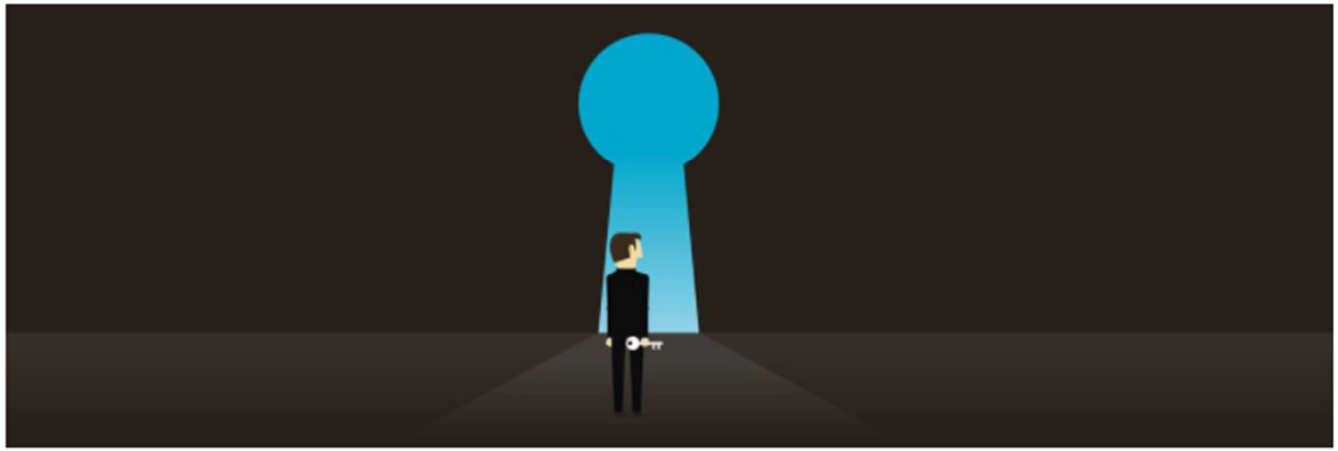
Prävention

NÜRNBERGER
AutoMobil
Versicherungsdienst GmbH

— White-Hat-Hacker

Mehr Cybersicherheit durch geplante Hackerangriffe

Manager, die in Sachen Cybersecurity schon alles zu wissen glauben, haben vermutlich noch nie White-Hat-Hacker engagiert. Die bezahlten Angreifer knacken IT-Systeme bevor Kriminelle es tun – und decken oft erschreckende Schwachstellen auf.



Attacken aus dem Cyberspace richten immer gravierendere Schäden an: Nach Berechnungen des Branchenverbands Bitkom verursachte Internetkriminalität in Deutschland 2019 Schäden von knapp 103 Milliarden Euro – fast doppelt so viel wie im vorherigen Erhebungszeitraum 2017/18.

© twotype design

Wie sicher ist Ihr Unternehmen?

Referent:
Bjoern Hering

www.netzsicher.net
info@netzsicher.net

Certified Ethical Hacker (CEH 312-50)
Penetration Tester
Red Team Offensive Attacker

offensive IT der Autohaus Trompeter GmbH