Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

IT-Sicherheit im HOME-OFFICE

UNTER BESONDERER BERÜCKSICHTIGUNG DER COVID-19 SITUATION

Ergebniskurzbericht einer repräsentativen Umfrage des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

INHALTSVERZEICHNIS

ZIELSETZUNG UND METHODIK

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) führt regelmäßig Umfragen zur Lage der IT-Sicherheit in der deutschen Wirtschaft durch. Das Jahr 2020 hat aufgrund der COVID-19 Pandemie und den damit einhergehenden Schutzmaßnahmen Unternehmen und Organisationen vor komplexe und vielfältige Herausforderungen gestellt. Die Pandemie hat uns nochmals deutlich vor Augen geführt, welche Bedeutung funktionierende und sichere IT-Infrastrukturen haben.

Das Home-Office oder Remote Work kann in diesem Kontext eine spezielle Angriffsfläche bieten. Insbesondere wenn viele Mitarbeitenden kurzfristig als Eindämmungsmaßnahme der Pandemie von zu Hause arbeiten.

Wir haben es uns zum Ziel gemacht, uns ein Bild von der Lage der IT-Sicherheit im Home-Office vor und während der Pandemie zu machen. In einer bundesweiten repräsentativen Umfrage wurden 1000 Unternehmen zur ihrer Home-Office Situation befragt. Befragt wurden explizit nur diejenigen Unternehmen, welche mindestens drei Mitarbeitende beschäftigen und aktuell Mitarbeitende im Home-Office haben. Diese Unternehmen wurden auf der Grundlage eines repräsentativen Screenings aus allen Unternehmen ab 3 Beschäftigten identifiziert. Diese Untersuchung gibt keinen Überblick auf den allgemeinen Stand der IT-Sicherheit in deutschen Unternehmen.

Die Umfrage wurde im zweiten Halbjahr 2020 durch das Umfrageinstitut „INFO GmbH Markt- und Meinungsforschung“ durchgeführt.

DIE ERHEBUNG IM ÜBERBLICK

GRUNDGESAMTHEIT

Unternehmen, Organisationen und Verbände der Wirtschaft aller Branchen mit mindestens 3 Beschäftigten, die Home-Office angeboten haben.

AUSWAHLVERFAHREN

CAWI:
Quotierte Zufallsauswahl aus einem aktiv rekrutierten Online-Accesspanel.
CATI:
Zufallsstichprobe aus Firmenadressen eines Adressanbieters.

GEWICHTUNG

Gewichtung des vollständigen Datensatzes sowie der Kurzinterviews (Firmen, die kein Home-Office angeboten haben) nach den Merkmalen Branche und Unternehmensgröße.

FEHLERSPANNE

Fehlerspanne +/- 3,1 Prozentpunkte bei 1.000 Befragten
(Anteilswert 50 %, Sicherheitswahrscheinlichkeit 95 %).

METHODIK

Mixed Mode: CAWI (Onlineinterviews),
CATI (Computergestützte Telefoninterviews); Interviewdauer: ø 11 Minuten.

FELDZEIT

12.10 – 11.11.2020

BEAUFTRAGTES INSTITUT

INFO GmbH • Markt- und Meinungsforschung

HOME-OFFICE

HOME-OFFICE – DAS MOBILE ARBEITEN WIRD LANGFRISTIG WEITER AUSGEBAUT.

Mit Beginn der COVID-19-Pandemie im Frühjahr 2020 haben viele Unternehmen verstärkt Mitarbeitende als Schutzmaßnahme ins Home-Office geschickt. Im Rahmen dieser Erhebung wurden kleinere und mittlere Unternehmen (KMU) sowie Großunternehmen nach ihrer IT-Situation im Home-Office befragt.

Die befragten Unternehmen gaben an, ihr Home-Office Angebot im Umfragezeitraum stark ausgeweitet zu haben. Die Zahl der angebotenen Home-Office Arbeitsplätze hat sich aufgrund von Corona mehr als verdoppelt. Blickt man auf den Gesamtdurchschnitt, dann sind insgesamt **64 % der Beschäftigten voll oder teilweise im Home-Office.**

Auch perspektivisch planen viele Unternehmen das Arbeiten im Home-Office im gleichen Maße zu erhalten, oder sogar noch auszuweiten. Besonders Großunternehmen planen diesen Schritt.

Bei der derzeitigen Ausstattung des Home-Office wird in rund **42 % der Unternehmen ausschließlich auf unternehmenseigene IT** zurückgegriffen. Ein wichtiger Faktor hierbei ist die Unternehmensgröße: In **kleineren Unternehmen** wird in **rund 13 %** der Fälle überwiegend oder ausschließlich **private IT** im Home-Office eingesetzt.

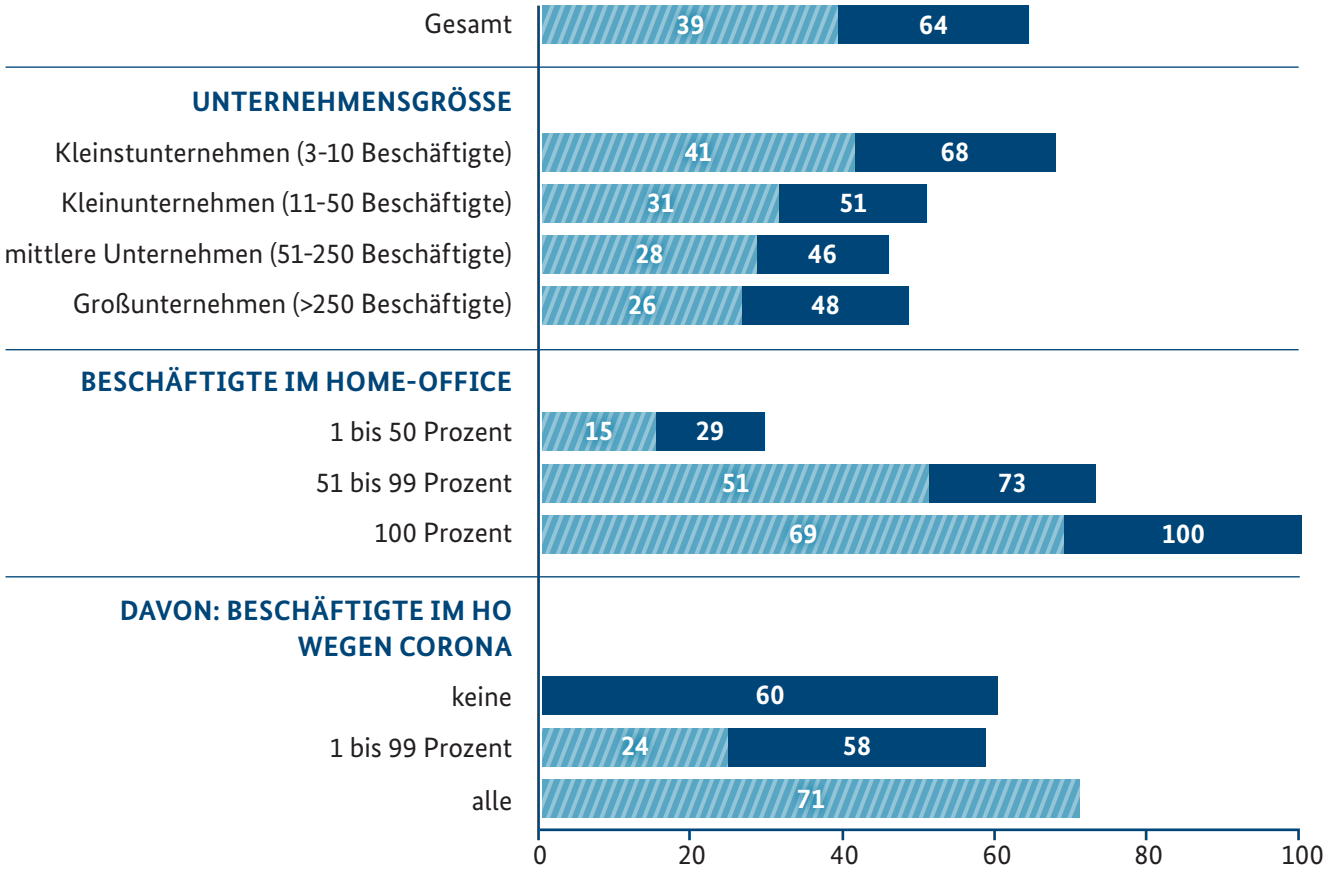
Das BSI empfiehlt, erste ad hoc getroffene Maßnahmen langfristig durch sichere IT-Lösungen zu ersetzen und, wenn möglich, auf den Einsatz von privater IT zu verzichten. Insbesondere die langfristige Perspektive für einen stärkeren Ausbau von Home-Office Plätzen zeigt, wie wichtig passgenaue Sicherheitslösungen an dieser Stelle sind.

HOME-OFFICE

Prozentuale Mittelwerte;
Gesamtwerte für Beschäftigte im HO wegen Corona wurden auf Gesamtbasis prozentuiert
Basis: alle Befragten n = 1.000

ANTEIL DER MITARBEITER*INNEN IM HOME-OFFICE

(Basis: alle Beschäftigten)



- Beschäftigte im HO Gesamt
- Davon: Beschäftigte im HO wegen Corona-Pandemie

Frage: Wie viele Mitarbeiter*innen Ihres Unternehmens sind gegenwärtig oder in den letzten Monaten (also in der Zeit der COVID-19-Pandemie) voll oder teilweise im Home-Office (auch Telearbeit oder mobiles Arbeiten genannt) beschäftigt (gewesen)?

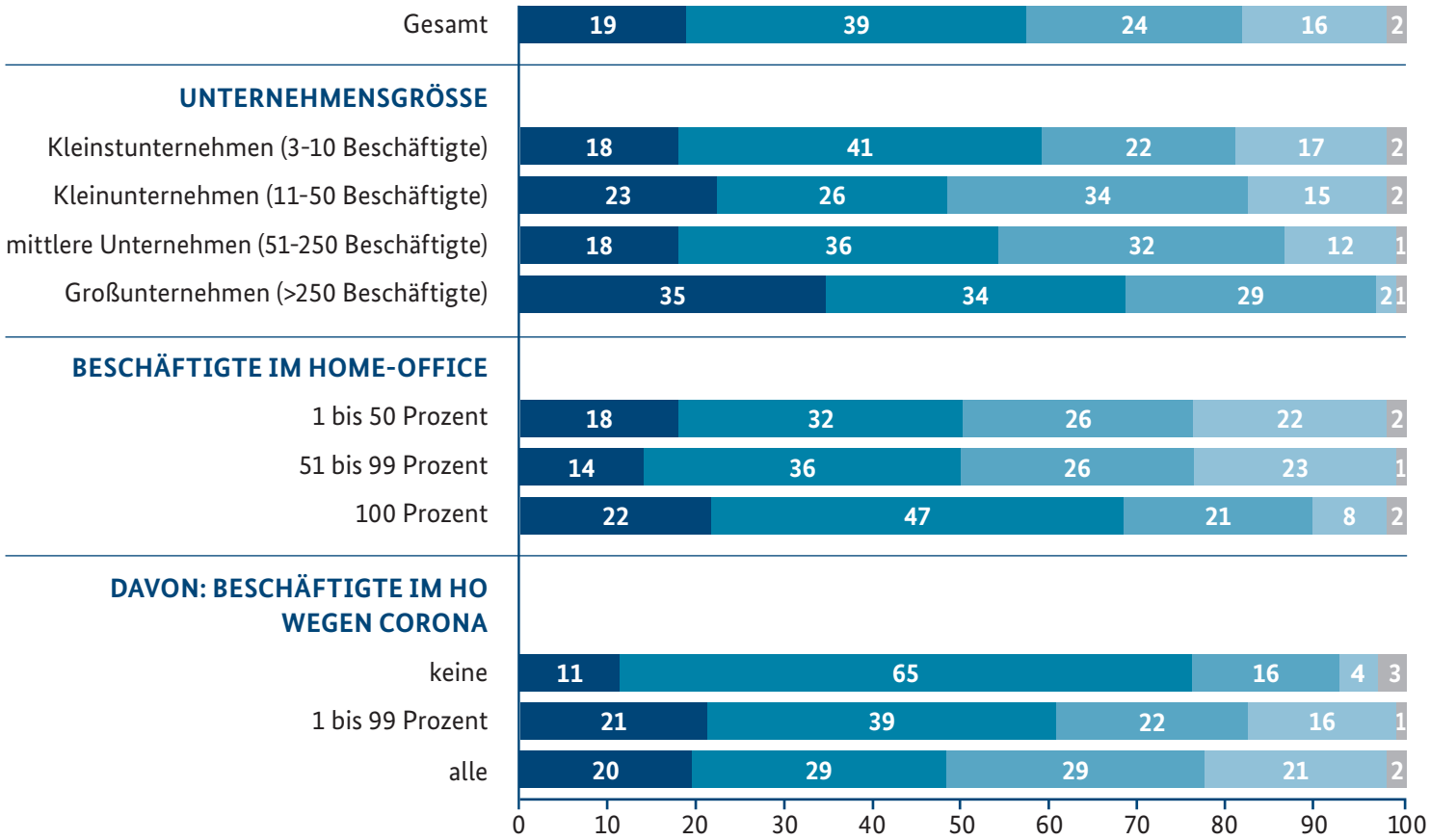
Wieviel Prozent davon waren Corona-bedingt bzw. als Maßnahme zur Eindämmung der COVID-19 Pandemie im HO?

Durch Corona hat sich das Angebot von Home-Office Arbeitsplätzen mehr als verdoppelt.

HOME-OFFICE

Angaben in %
Basis: alle Befragten n = 1.000

PERSPEKTIVE VON HOME-OFFICE, TELEARBEIT UND MOBILEM ARBEITEN



- wird voraussichtlich noch ausgeweitet
- wird voraussichtlich im jetzigen Umfang beibehalten
- wird voraussichtlich in geringerem Umfang beibehalten
- wird voraussichtlich wieder eingestellt
- weiß nicht

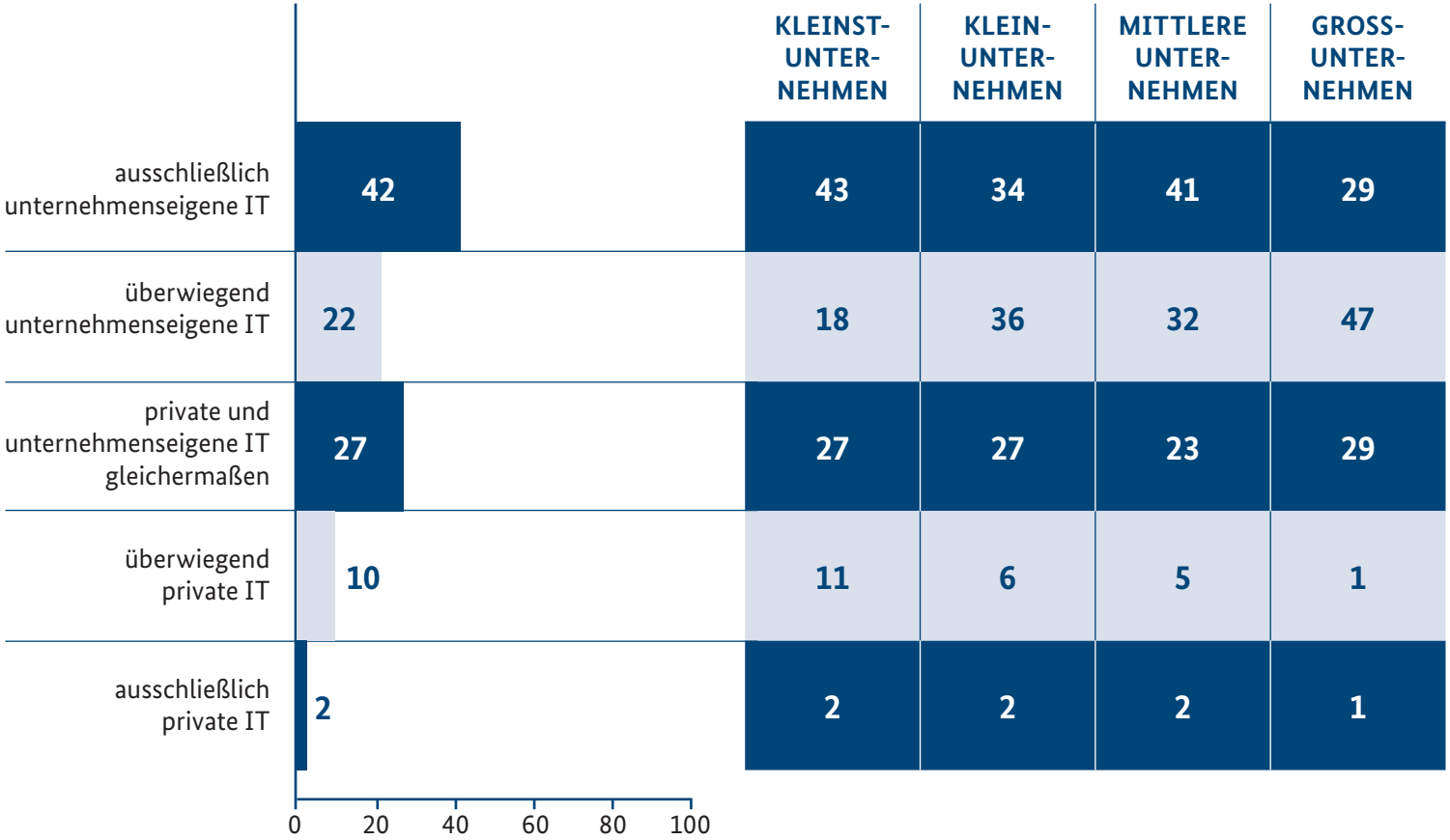
Frage: Welche Perspektive haben Home-Office, Telearbeit oder auch mobiles Arbeiten in Ihrem Unternehmen in der Zeit nach der Corona-Krise voraussichtlich?

58 % der Unternehmen wollen das Home-Office-Angebot nach der Pandemie aufrechterhalten oder sogar ausweiten.

HOME-OFFICE

Angaben in %
Basis: alle Befragten n = 1.000

IT-AUSSTATTUNG IM HOME-OFFICE



Frage: Welche IT-Ausstattung nutzen Ihre Mitarbeiter*innen im Home-Office?

Nur 42 % der Unternehmen nutzen ausschließlich unternehmenseigene IT.

SICHERHEITS-MAßNAHMEN

SICHERHEITSMASSNAHMEN – PRÄVENTION IST DER BESTE SCHUTZ

Das Arbeiten im Home-Office stellt für die Cyber-Sicherheit von Unternehmen eine besondere Herausforderung dar. Zusätzlich zu den IT-Lösungen im Unternehmen vor Ort müssen auch Systeme im Home-Office und die Verbindung der Systeme geschützt werden. Welche technischen und organisatorischen Sicherheitsmaßnahmen haben Unternehmen insgesamt umgesetzt?

Insgesamt zeigt sich bei der Umsetzung von technischen und organisatorischen Maßnahmen ein ungenügendes Bild: **Zu viele Unternehmen vernachlässigen Cyber-Sicherheitsmaßnahmen.** Während einfache Maßnahmen wie der Passwortschutz meist noch umgesetzt werden, werden viele weitere empfohlene Maßnahmen nur von einigen Unternehmen umgesetzt. Deutlich zeigt sich, dass Kleinst- und Kleinunternehmen hier besonderen Nachholbedarf haben.

Die Ergebnisse zeigen zudem, dass nur wenige Unternehmen, trotz erhöhter Angriffsfläche, weitere Schutzmaßnahmen zur Absicherung des Home-Offices planen.

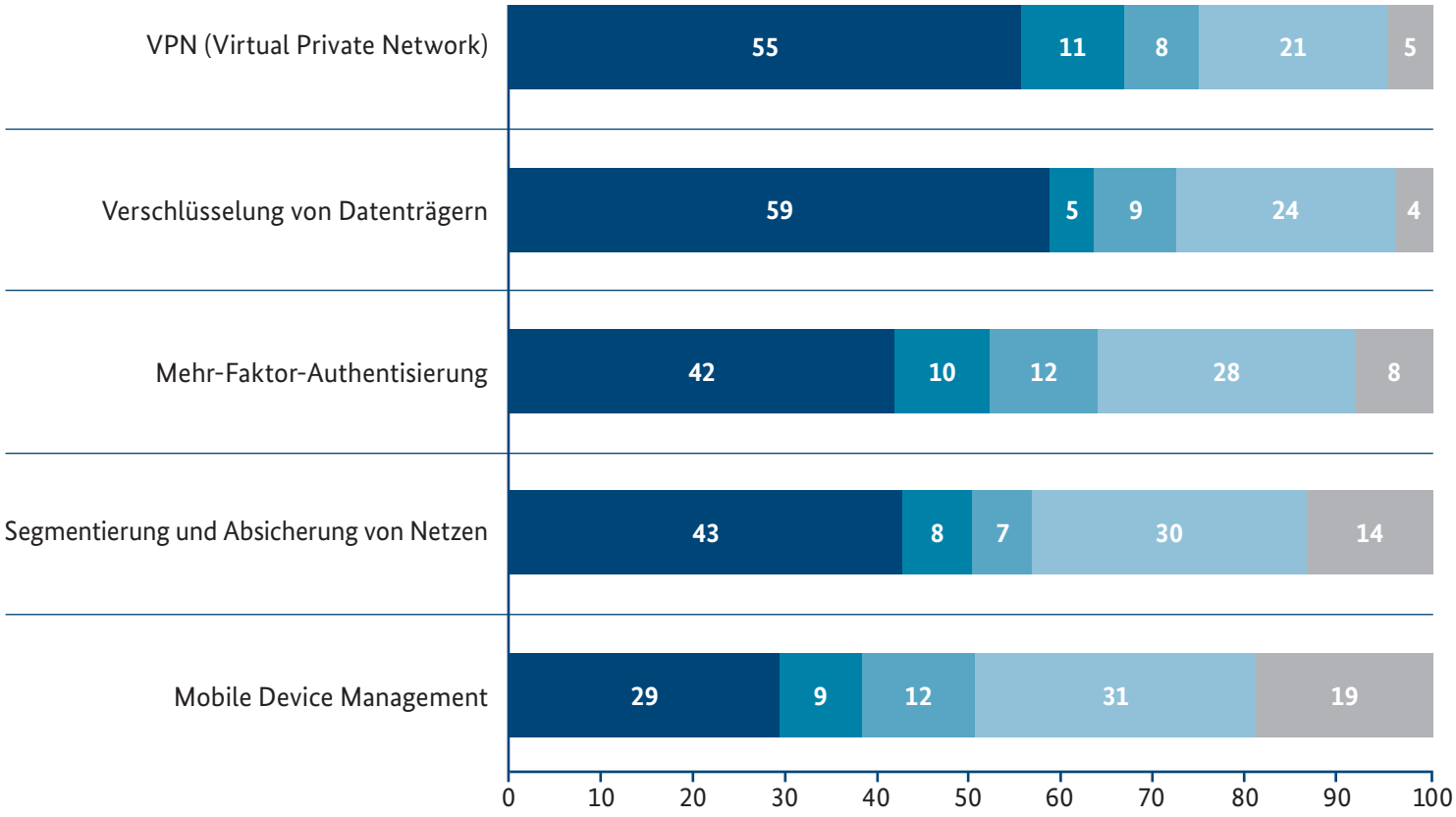
Diese Ergebnisse spiegeln sich auch in den Ausgaben für Cyber-Sicherheit wider: **Über 50 %** der Unternehmen investieren **weniger als 10 %** der **IT-Ausgaben in Cyber-Sicherheit.**

Das BSI empfiehlt, mindestens 20 % der IT-Ausgaben in Cyber-Sicherheit einzuplanen.

SICHERHEITSMAßNAHMEN

Angaben in %;
Basis: alle Befragten n = 1.000

UMSETZUNG TECHNISCHER SICHERHEITSMAßNAHMEN MIT BESONDERER RELEVANZ FÜR DAS HOME-OFFICE



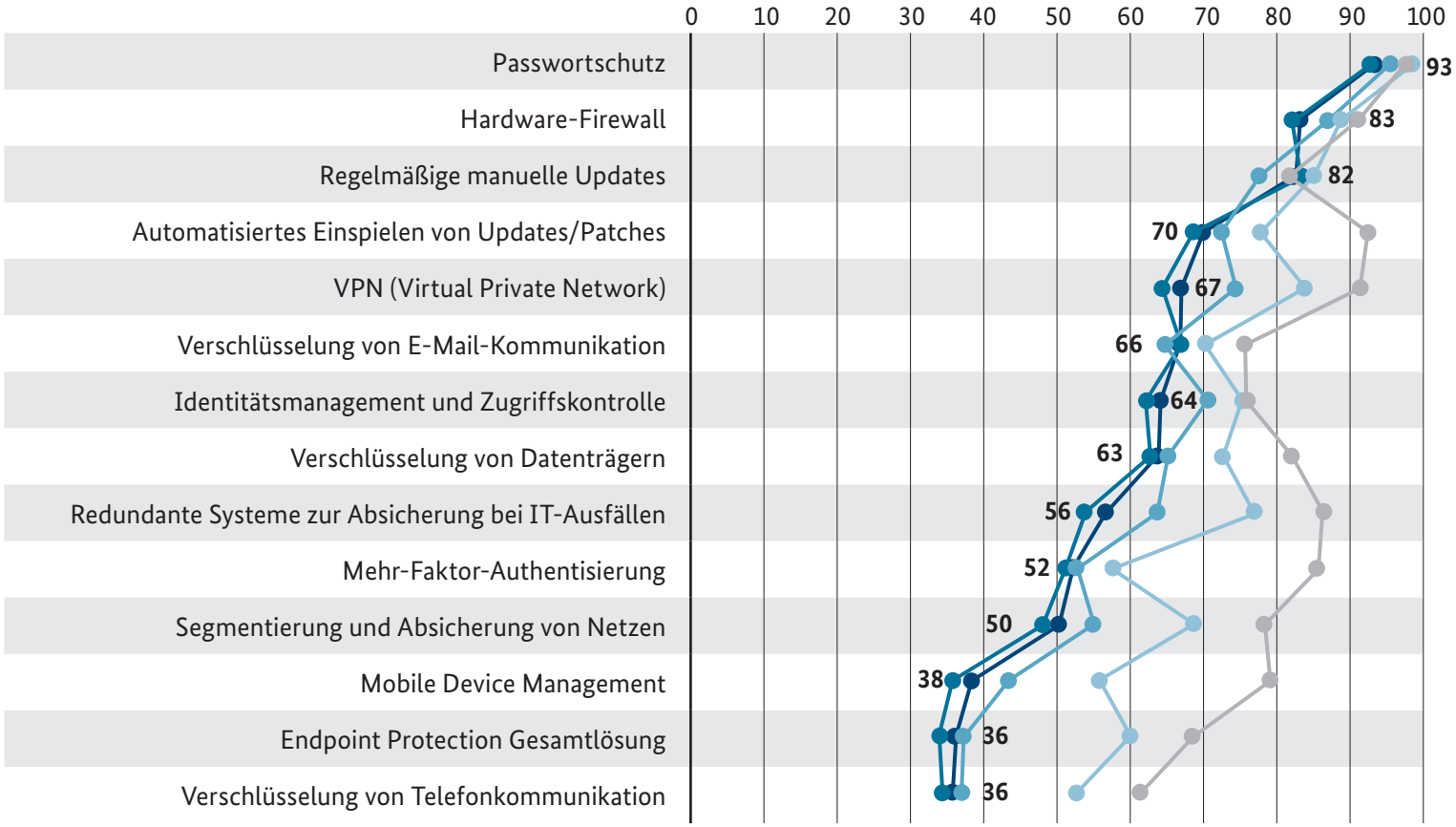
Frage: Welche technischen Sicherheitsmaßnahmen haben Sie in Ihrem Unternehmen bereits umgesetzt? Und seit wann gibt es diese Maßnahmen bzw. wann ist deren Einführung geplant?

Sicherheitslücke Handy: Nur 38 % der Unternehmen managen die Sicherheit von Handys, Laptops, Tablets und weiteren mobile Endgeräte mit Verbindung zum Firmennetzwerk.

SICHERHEITSMAßNAHMEN

Angaben in %;
Basis: alle Befragten n = 1.000

UMSETZUNG TECHNISCHER SICHERHEITSMAßNAHMEN



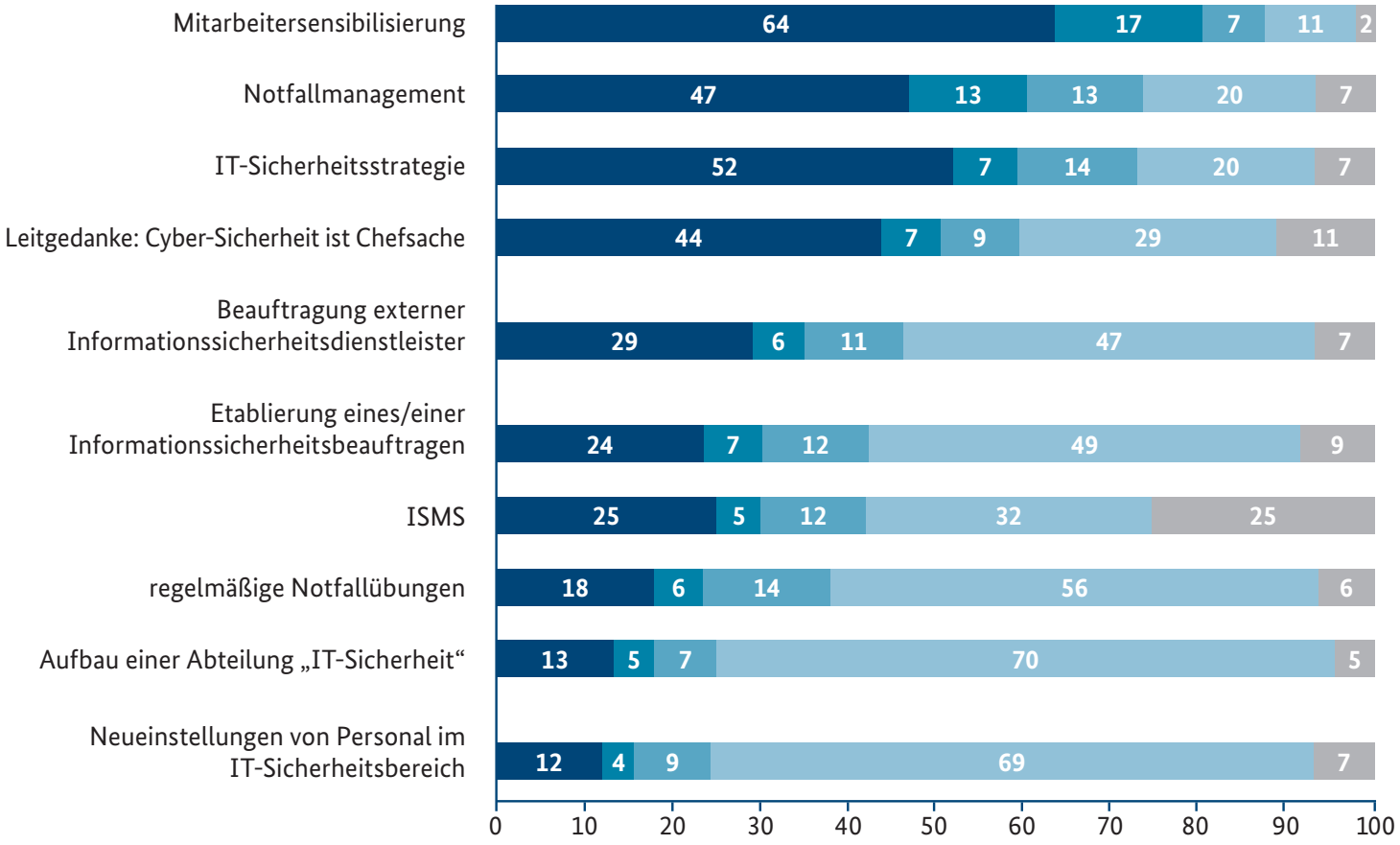
Frage: Welche technischen Sicherheitsmaßnahmen haben Sie in Ihrem Unternehmen bereits umgesetzt? Und seit wann gibt es diese Maßnahmen bzw. wann ist deren Einführung geplant?

Besonders Kleinstunternehmen haben bei der Umsetzung technischer Sicherheitsmaßnahmen Nachholbedarf.

SICHERHEITSMAßNAHMEN

Angaben in %;
Basis: alle Befragten n = 1.000

UMSETZUNG ORGANISATORISCHER SICHERHEITSMAßNAHMEN



- bereits vor der Corona-Krise umgesetzt
- in der Corona-Krise umgesetzt
- Umsetzung ist geplant
- Umsetzung ist bisher nicht geplant
- weiß nicht

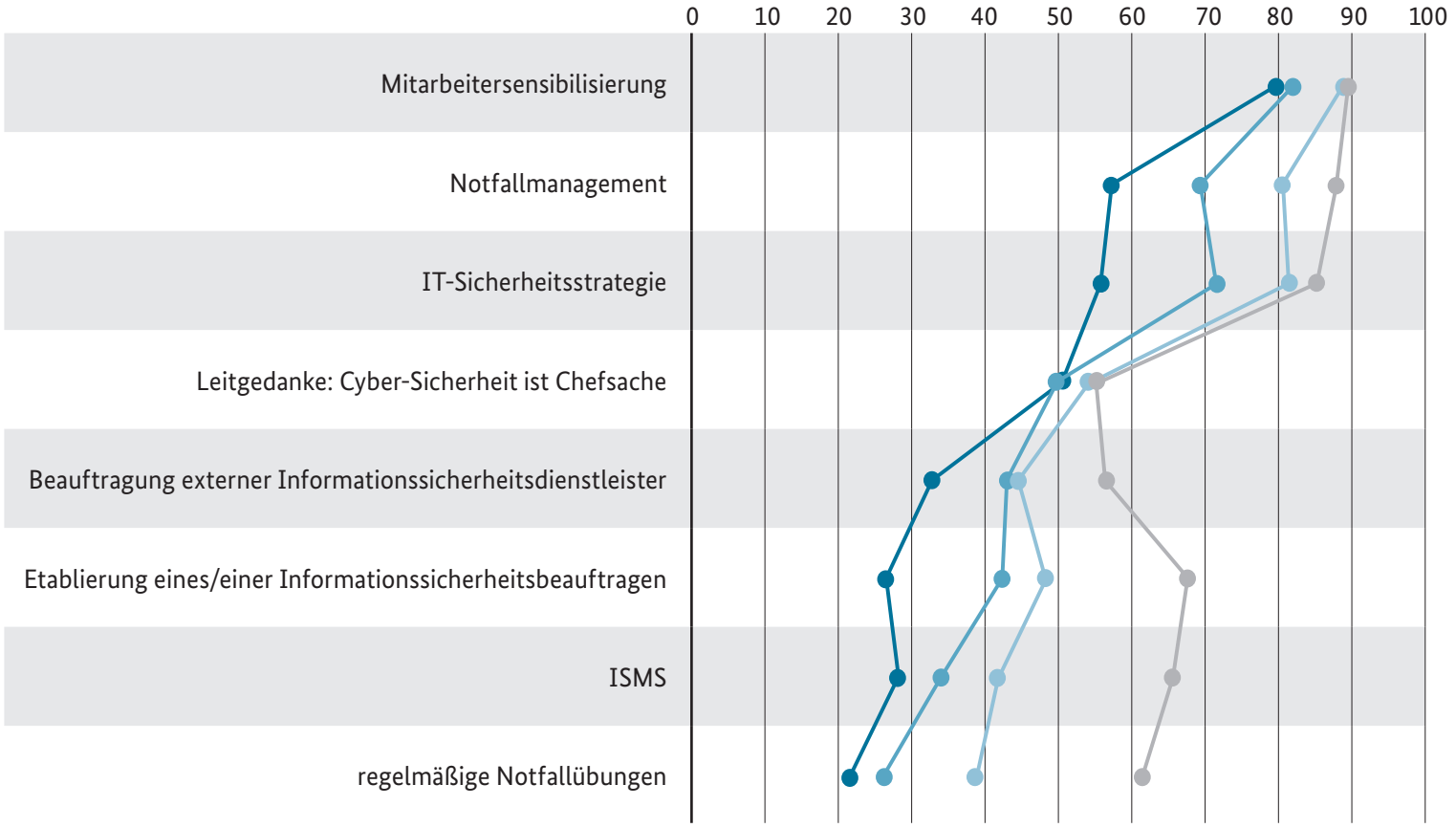
Frage: Und welche organisatorischen Sicherheitsmaßnahmen haben Sie in Ihrem Unternehmen bereits umgesetzt? Und seit wann gibt es diese Maßnahmen bzw. wann ist deren Einführung geplant?

Mitarbeitersensibilisierung wird bereits gut umgesetzt, bei Notfallübung besteht Nachholbedarf: 81 % der Unternehmen schulen ihre Beschäftigten zu Cyber-Sicherheitsrisiken, aber nur 24 % üben regelmäßig, was bei einem Angriff zu tun ist.

SICHERHEITSMAßNAHMEN

Angaben in %;
Basis: alle Befragten n = 1.000

UMSETZUNG ORGANISATORISCHER SICHERHEITSMAßNAHMEN



- Kleinstunternehmen (3-10 Beschäftigte)
- Kleinunternehmen (11-50 Beschäftigte)
- mittlere Unternehmen (51-250 Beschäftigte)
- Großunternehmen (>250 Beschäftigte)

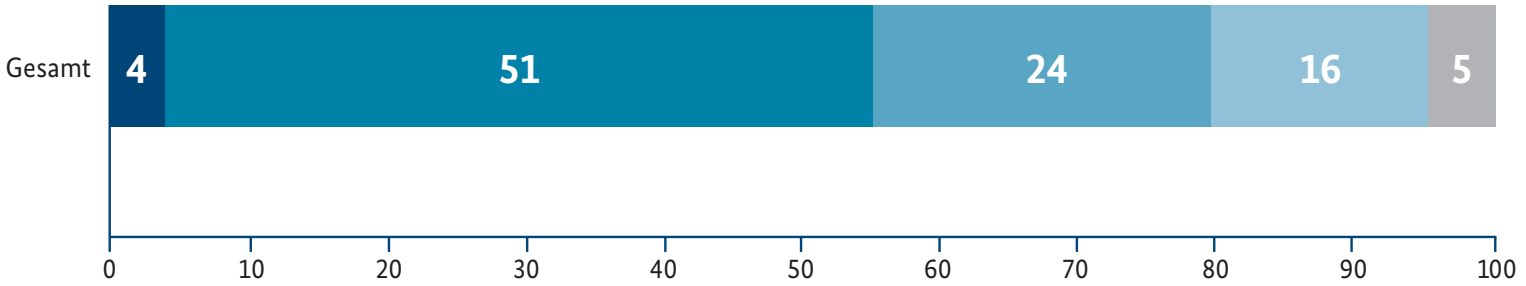
Frage: Und welche organisatorischen Sicherheitsmaßnahmen haben Sie in Ihrem Unternehmen bereits umgesetzt? Und seit wann gibt es diese Maßnahmen bzw. wann ist deren Einführung geplant?

„Cyber-Sicherheit ist Chefsache“ - diesen Leitgedanken setzen Unternehmen aller Größen ungenügend um.

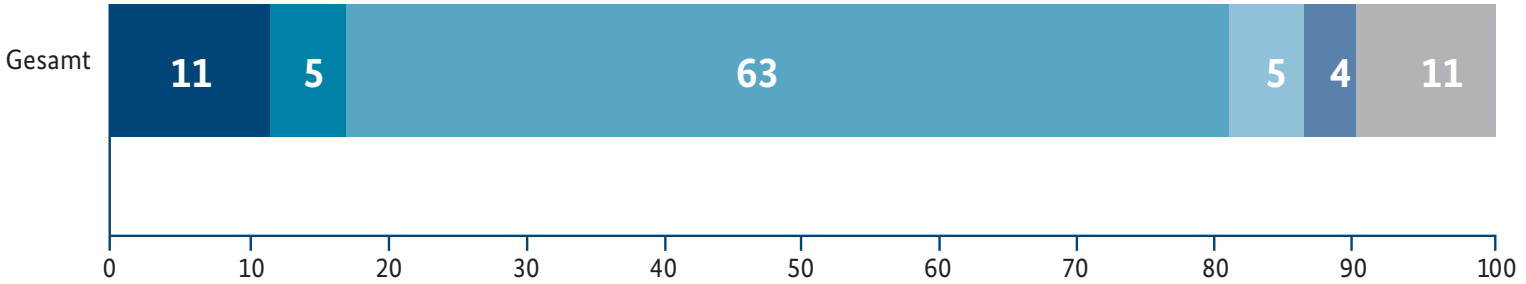
SICHERHEITSMAßNAHMEN

Angaben in %;
Basis: alle Befragten n = 1.000

BUDGET-ANTEIL FÜR CYBER-SICHERHEIT



ERHÖHUNG DES IT-SICHERHEITSBUDGETS WÄHREND DER CORONA-KRISE



Sparen an der Sicherheit: Gut die Hälfte der Unternehmen investiert von ihrem IT-Budget nur zehn Prozent oder weniger in Sicherheit. Nur 16 % der Unternehmen haben während der verstärkten Nutzung von Home-Office ihr IT-Sicherheitsbudget erhöht.

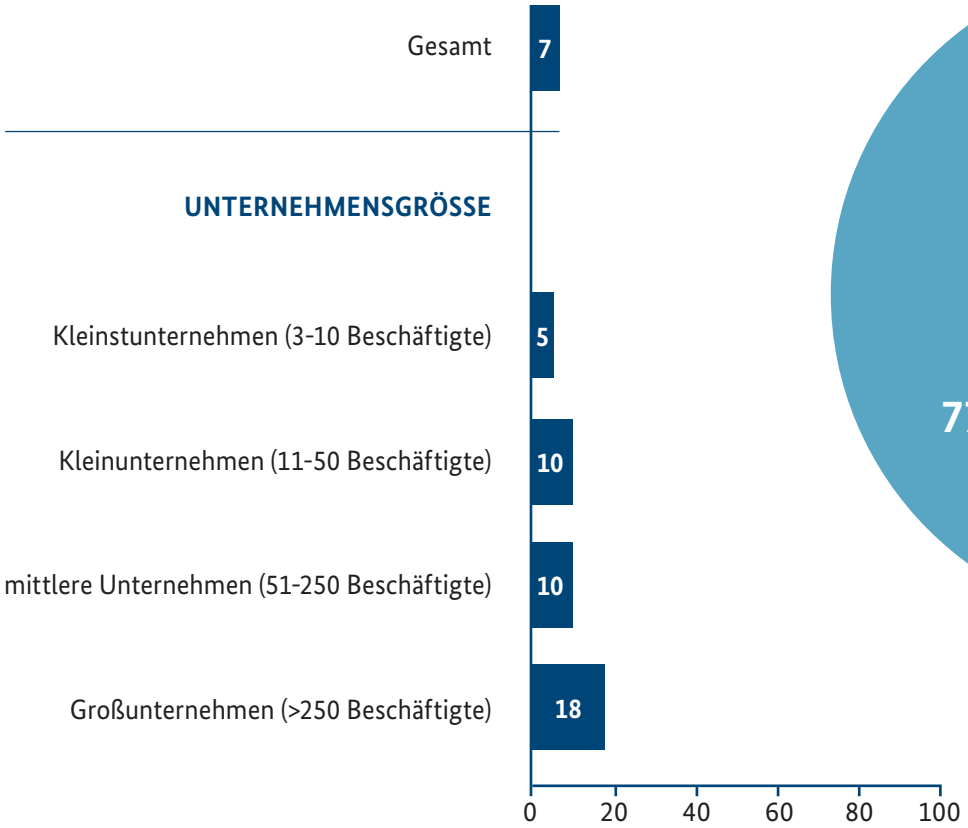
Frage: Wie hoch ist ungefähr der prozentuale Anteil für Cyber-Sicherheit in Ihrem gesamten IT-Budget?

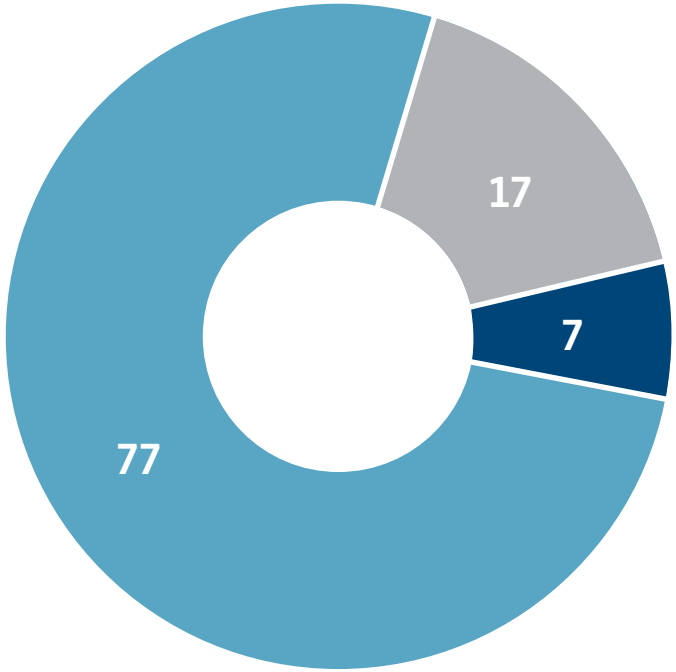
Haben Sie Ihr IT-Sicherheitsbudget aufgrund der Cyber-Sicherheitslage in der Zeit der Corona-Krise erhöht?

SICHERHEITSMAßNAHMEN

Angaben in %;
Basis: alle Befragten n = 1.000

PLANUNG WEITERER HO-SICHERHEITSMASSNAHMEN





ja
nein
weiß nicht

Frage: Sind in Ihrem Unternehmen weitere Maßnahmen geplant, die das Home-Office langfristig IT-sicherer machen?

Nur wenige Unternehmen planen weitere Sicherheitsmaßnahmen speziell für das Home-Office. Kleinste Unternehmen haben zwar offenbar den größten Aufholbedarf, planen aber dennoch am seltensten weitere Maßnahmen.

CYBER-ANGRIFFE
während der Home-Office-Zeit

CYBER-ANGRIFFE - EIN VIERTEL DER ANGEGRIFFENEN UNTERNEHMEN ERLITT EXISTENZBEDROHENDE SCHÄDEN

Das BSI hat im Bericht zur Lage der IT-Sicherheit in Deutschland aufgezeigt, wie schnell Cyber-Kriminelle auf aktuelle Situationen reagieren und ihre Strategien anpassen. So gab es etwa breit gestreute E-Mail-Spamwellen mit vermeintlichen Corona-Informationen. Mussten Unternehmen während der Corona-Krise auf diese oder andere Angriffe aktiv reagieren?

Von den Befragten sagten 8 %, dass sich ihr Unternehmen in der Corona-Krise mit Cyber-Attacken auseinandersetzen musste. Großunternehmen waren besonders häufig von Angriffen betroffen.

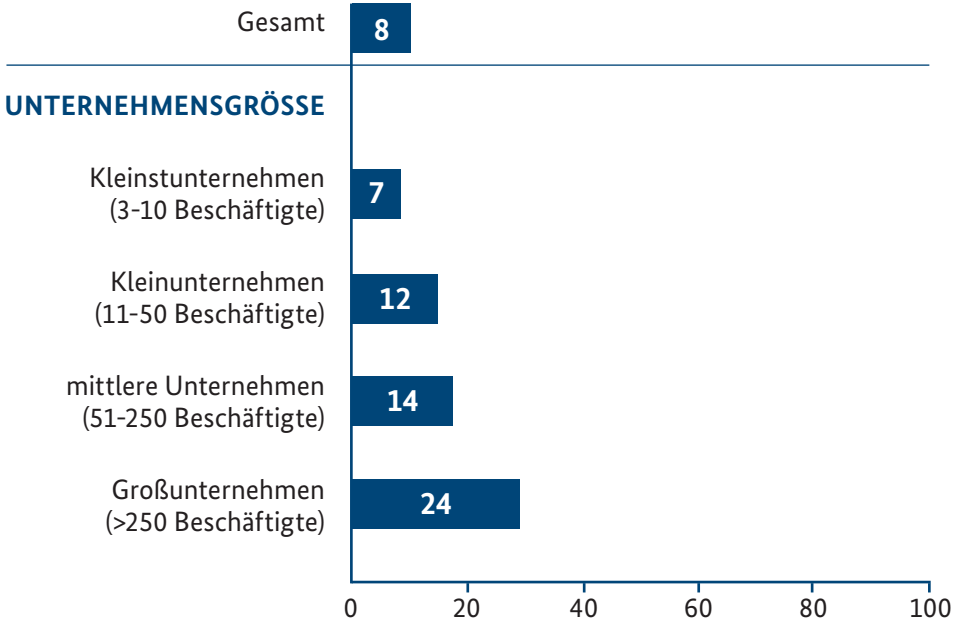
Etwa **ein Viertel** der von Cyber-Angriffe betroffenen Unternehmen erlitten durch diese Angriffe **existenzbedrohende oder sehr schwere Schäden** – besonders Kleinstunternehmen.

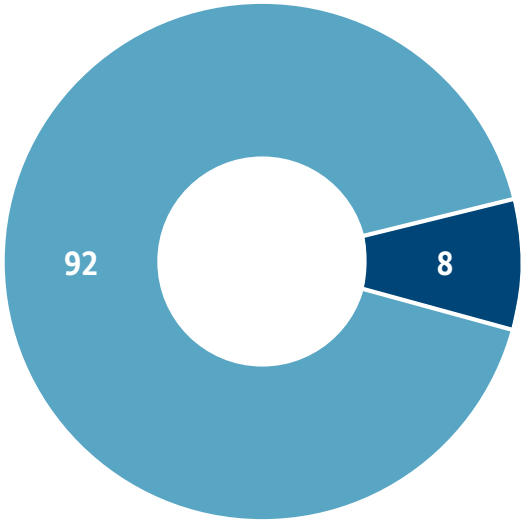
Informationssicherheit und Digitalisierung gehören untrennbar zusammen. Für eine erfolgreiche Digitalisierung ist Prävention ist besser und günstiger als Reaktion! Jedes Unternehmen kann und wird von Cyber-Sicherheitsvorfällen betroffen sein. Unternehmen müssen sich daher für den Notfall vorbereiten und Maßnahmen hierfür vorhalten.

CYBER-ANGRIFFE WÄHREND DER HOME-OFFICE-ZEIT

Angaben in %;
Basis: alle Befragten n = 1.000

NOTWENDIGE REAKTION AUF CYBER-ANGRIFFE





ja
nein

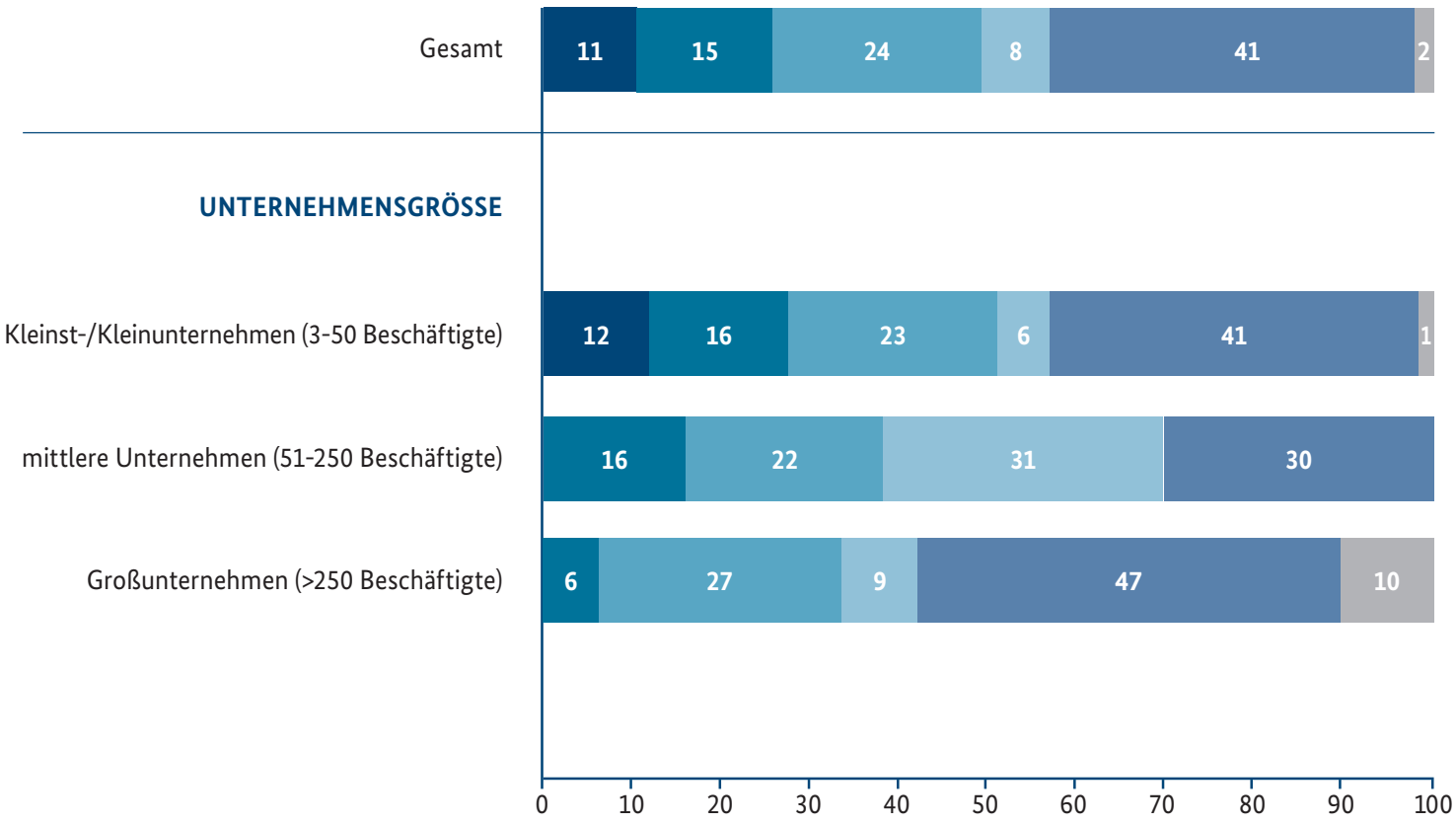
Frage: Musste Ihr Unternehmen während der Zeit des Corona-Home-Offices aktiv auf einen Cyber-Angriff reagieren?

In der Corona-Home-Office-Zeit mussten 8 % der Unternehmen aktiv auf Cyberangriffe reagieren, von den Großunternehmen waren sogar 24 % betroffen.

CYBER-ANGRIFFE WÄHREND DER HOME-OFFICE-ZEIT

Angaben in %;
Basis: Cyberangriff erlitten n = 127

BEWERTUNG DES SCHADENS DURCH CYBER-ANGRIFFE



Frage: Wie würden Sie den materiellen Schaden für Ihr Unternehmen durch diese Cyber-Angriffe bewerten?

Je kleiner die Firma, desto schwerwiegender die Folgen: Für Unternehmen mit weniger als 50 Beschäftigten hat eine von vier Cyberattacken sehr schwere oder sogar existenzbedrohende Folgen.

DIGITALISIERUNG

Die COVID-19-Pandemie hat das Potential, die Arbeitswelt nachhaltig zu verändern. Unternehmen stellten Teile des Arbeitens auf Home-Office um und beschleunigten Digitalisierungsprozesse, um weiterhin arbeits- und wettbewerbsfähig zu bleiben. So gaben **ein Drittel** der Kleinstunternehmen und **zwei Drittel** der Großunternehmen an, die COVID-19-Pandemie als **Digitalisierungsturbo** wahrzunehmen.

Es zeigt sich: Rund ein Drittel der Unternehmen haben aufgrund der Corona-Krise Digitalisierungsprojekte zeitlich vorgezogen oder neu geplant und implementiert. IT-Lösungen mit Home-Office-Bezug wie Video-Konferenz-Systeme wurden dabei häufig neu eingeführt.

Häufig wird bei der Einführung von Geschäftsprozessen Cyber-Sicherheit jedoch nicht von vornherein mitgedacht. Mehr als die Hälfte der Unternehmen berücksichtigen Cyber-Sicherheitsmaßnahmen, wenn überhaupt, erst später. Dies betrifft vor allem Unternehmen, die sich selbst einen schlechten Stand der IT-Entwicklung und Digitalisierung attestieren.

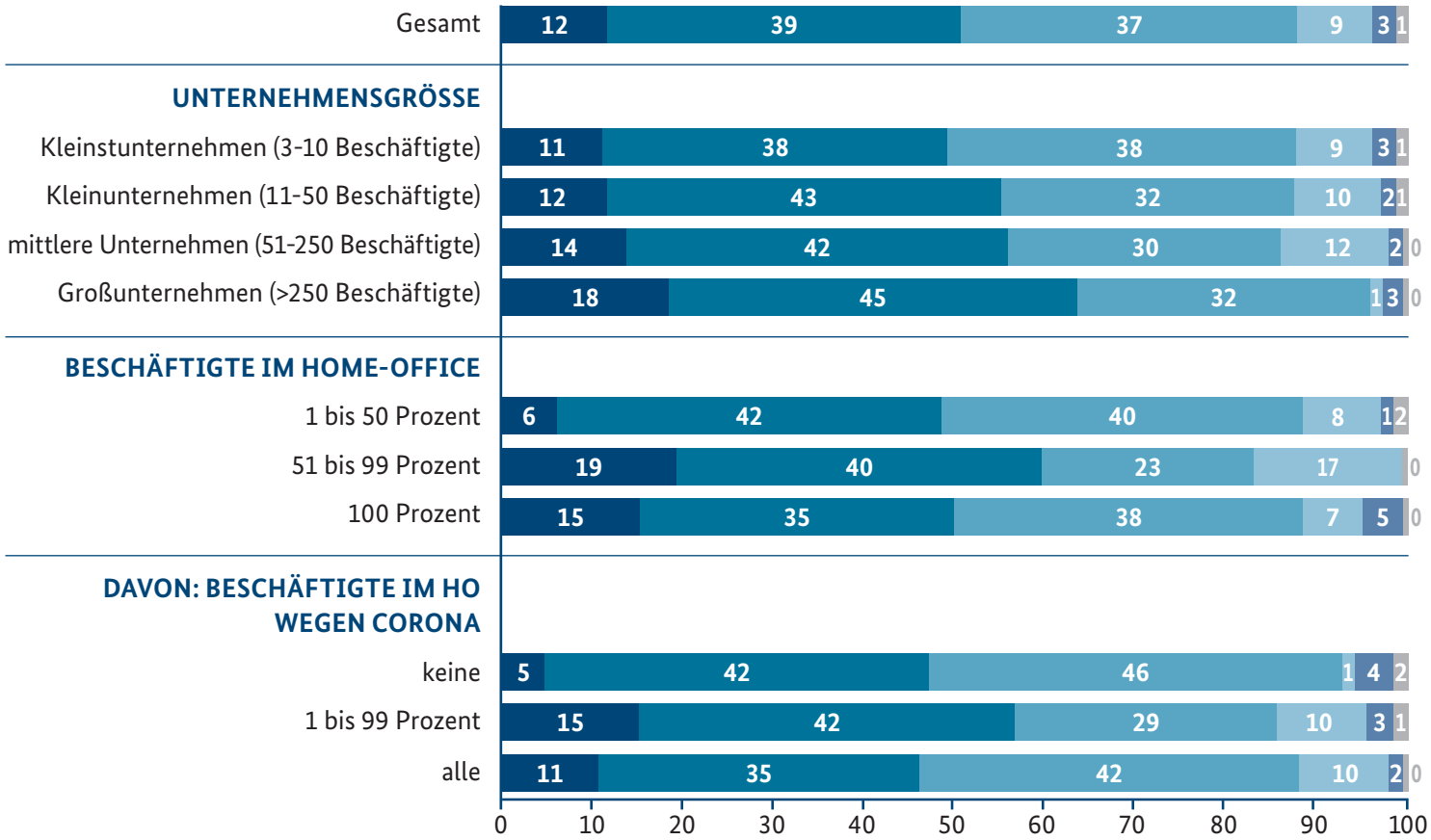
Es zeigt sich zudem, dass es für einen Großteil der Unternehmen wichtig ist, dass ihre genutzten IT-Lösungen und Anlagen in Deutschland oder der EU entwickelt/angefertigt werden.

Bei allen Digitalisierungsvorhaben ist entscheidend, die Cyber-Sicherheit von Anfang an mitzudenken. Eine erfolgreiche Digitalisierung ohne Cyber-Sicherheit kann und wird es nicht geben. Das BSI unterstützt Unternehmen bei der Ausgestaltung von sicheren Digitalisierungsvorhaben, damit Cyber-Sicherheit das neue Qualitätsmerkmal „Made in Germany“ werden kann.

DIGITALISIERUNG

Angaben in %;
Basis: alle Befragten n = 1.000

STAND DER IT-ENTWICKLUNG UND DIGITALISIERUNG



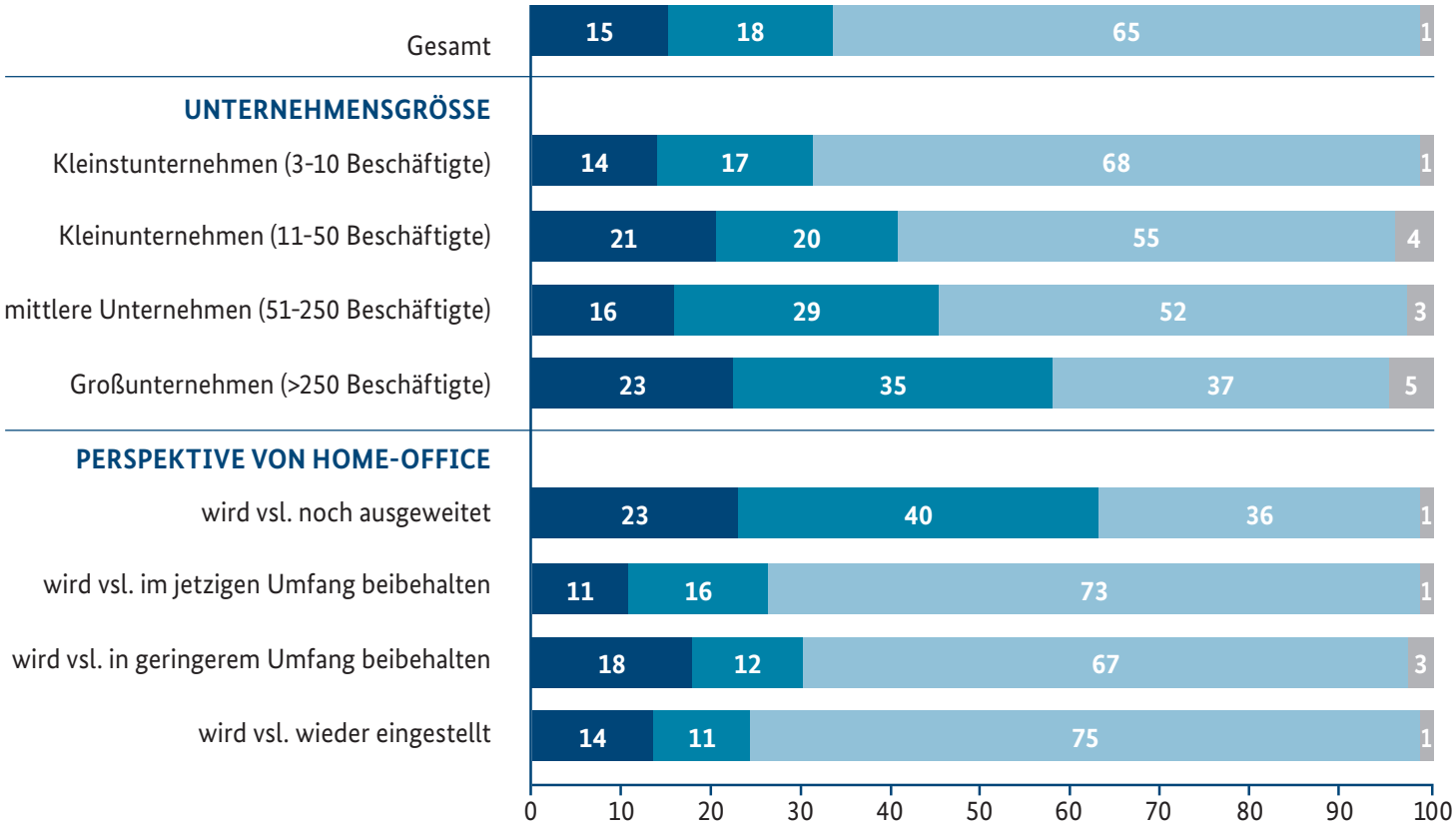
Frage: Wie würden Sie den gegenwärtigen Stand der IT-Entwicklung und Digitalisierung in Ihrem Unternehmen alles in allem bezeichnen?

Das Home Office als Indikator für die Digitalisierung: Je mehr Beschäftigte im Home Office sind, desto besser fallen die Noten für die Digitalisierung des Unternehmens aus.

DIGITALISIERUNG

Angaben in %;
Basis: alle Befragten n = 1.000

UMSETZUNG VON DIGITALISIERUNGSPROJEKTEN WEGEN CORONA



- ja, neu geplant und implementiert
- ja, zeitlich vorgezogen
- nein
- weiß nicht

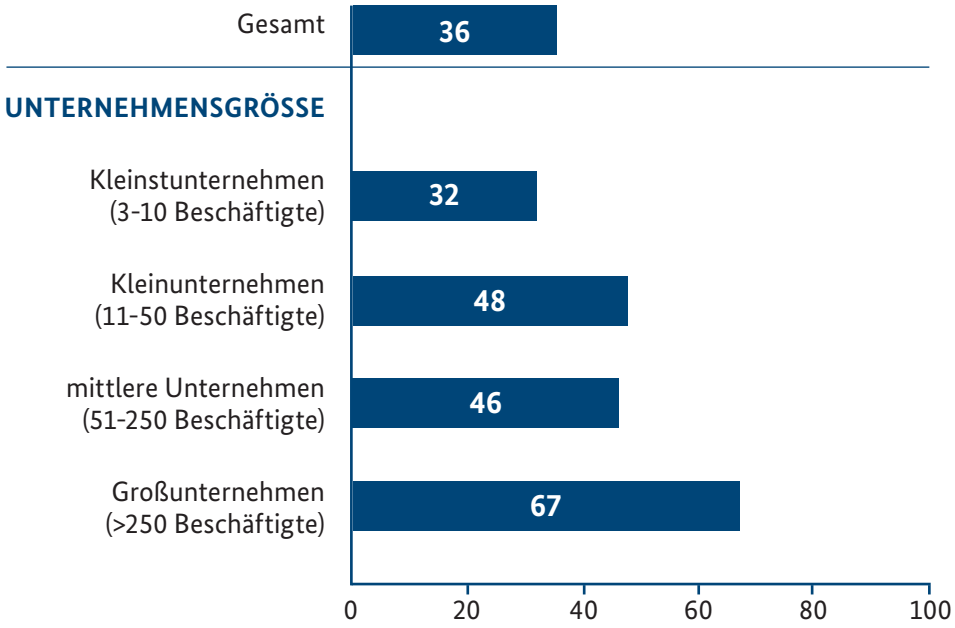
Frage: Wurden aufgrund der COVID-19-Pandemie in Ihrem Unternehmen Digitalisierungsprojekte umgesetzt?

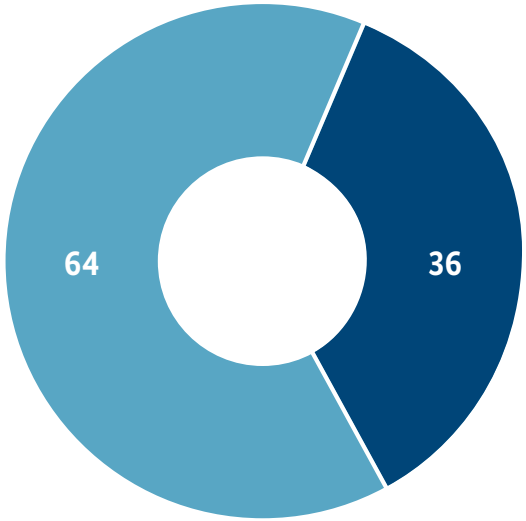
Etwa ein Drittel der Unternehmen hat aufgrund der Corona-Pandemie Digitalisierungsprojekte zeitlich vorgezogen oder neu geplant und implementiert. Wer an das Home-Office glaubt, investiert in die Digitalisierung: Unternehmen, die das Home-Office ausweiten wollen, haben weit überdurchschnittlich Digitalisierungsprojekte beschleunigt oder neu aufgesetzt.

DIGITALISIERUNG

Angaben in %;
Basis: alle Befragten n = 1.000

COVID-19 ALS DIGITALISIERUNGSTURBO





eher ja
eher nein

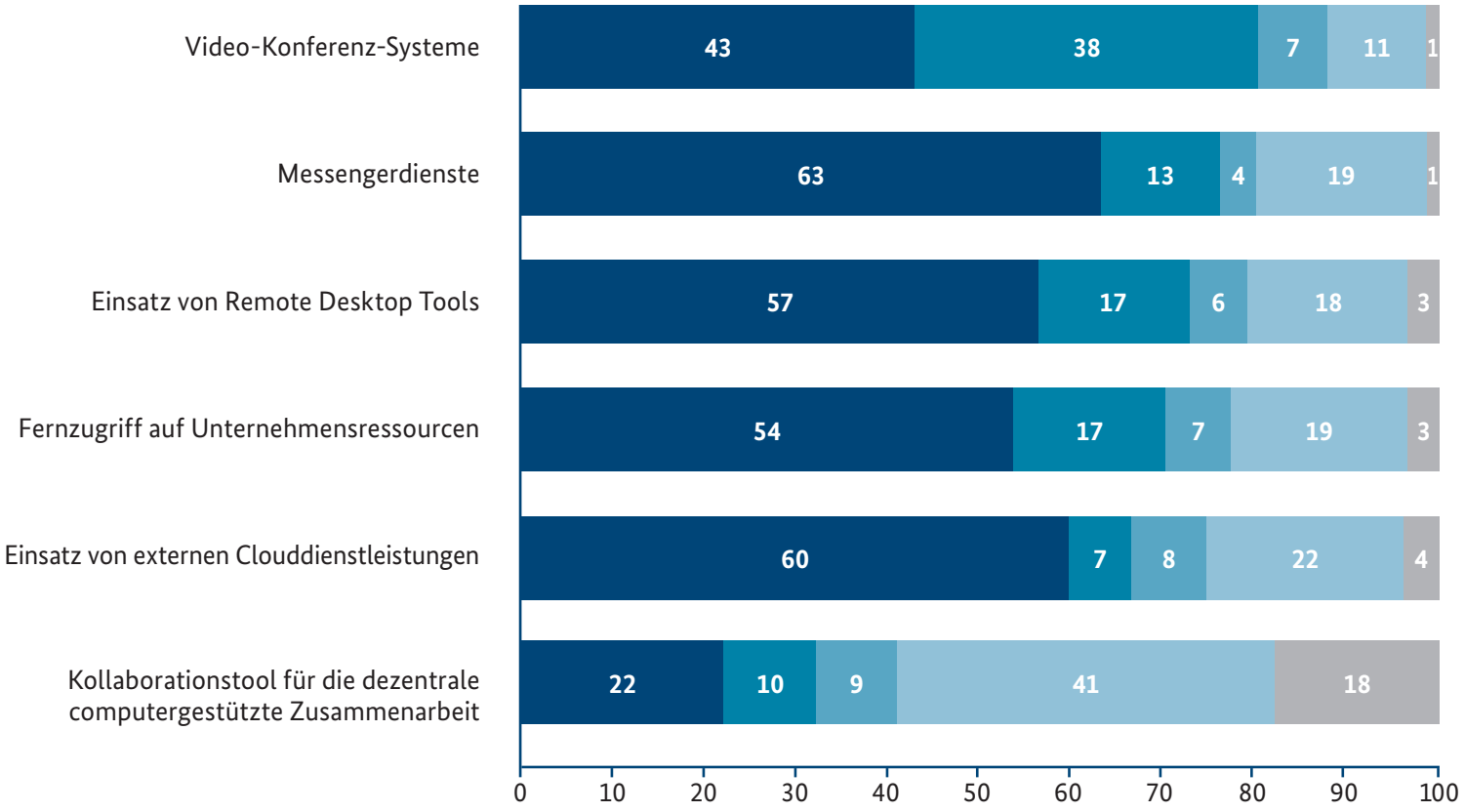
Frage: Stimmen Sie der folgenden Aussage zu: „COVID-19 ist für mein Unternehmen auch ein Digitalisierungsturbo.“?

Ein Drittel der Kleinstunternehmen und zwei Drittel der Großunternehmen nehmen die Corona-Pandemie als Digitalisierungsturbo wahr.

DIGITALISIERUNG

Angaben in %;
Basis: alle Befragten n = 1.000

EINGESETZTE IT-LÖSUNGEN MIT HOME-OFFICE-BEZUG



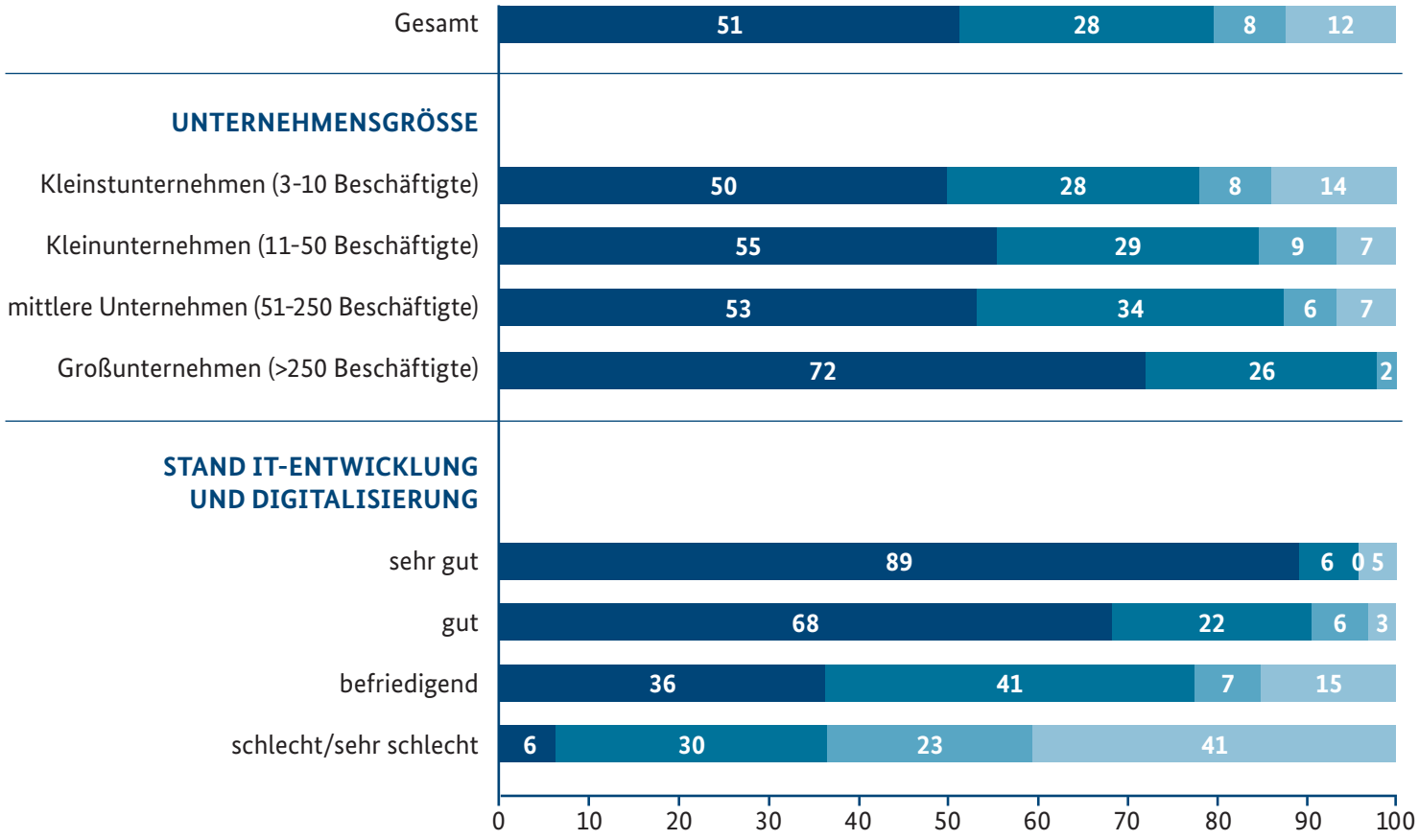
Frage: Welche der folgenden IT-Lösungen mit Home-Office-Bezug werden von Ihrem Unternehmen eingesetzt? Und seit wann werden diese Lösungen genutzt bzw. wann ist deren Einführung geplant?

Während der Corona-Krise ist vor allem die Nutzung von Video-Konferenzsystemen stark angestiegen.

DIGITALISIERUNG

Angaben in %;
Basis: alle Befragten n = 1.000

INFORMATIONSSICHERHEIT IM ZUGE DER DIGITALISIERUNG



- wird von vornherein für alle Prozesse mitgedacht
- wird erst im Laufe der Implementierung berücksichtigt
- spielt erst nach der Implementierung eine Rolle
- spielt bei uns nur eine untergeordnete Rolle

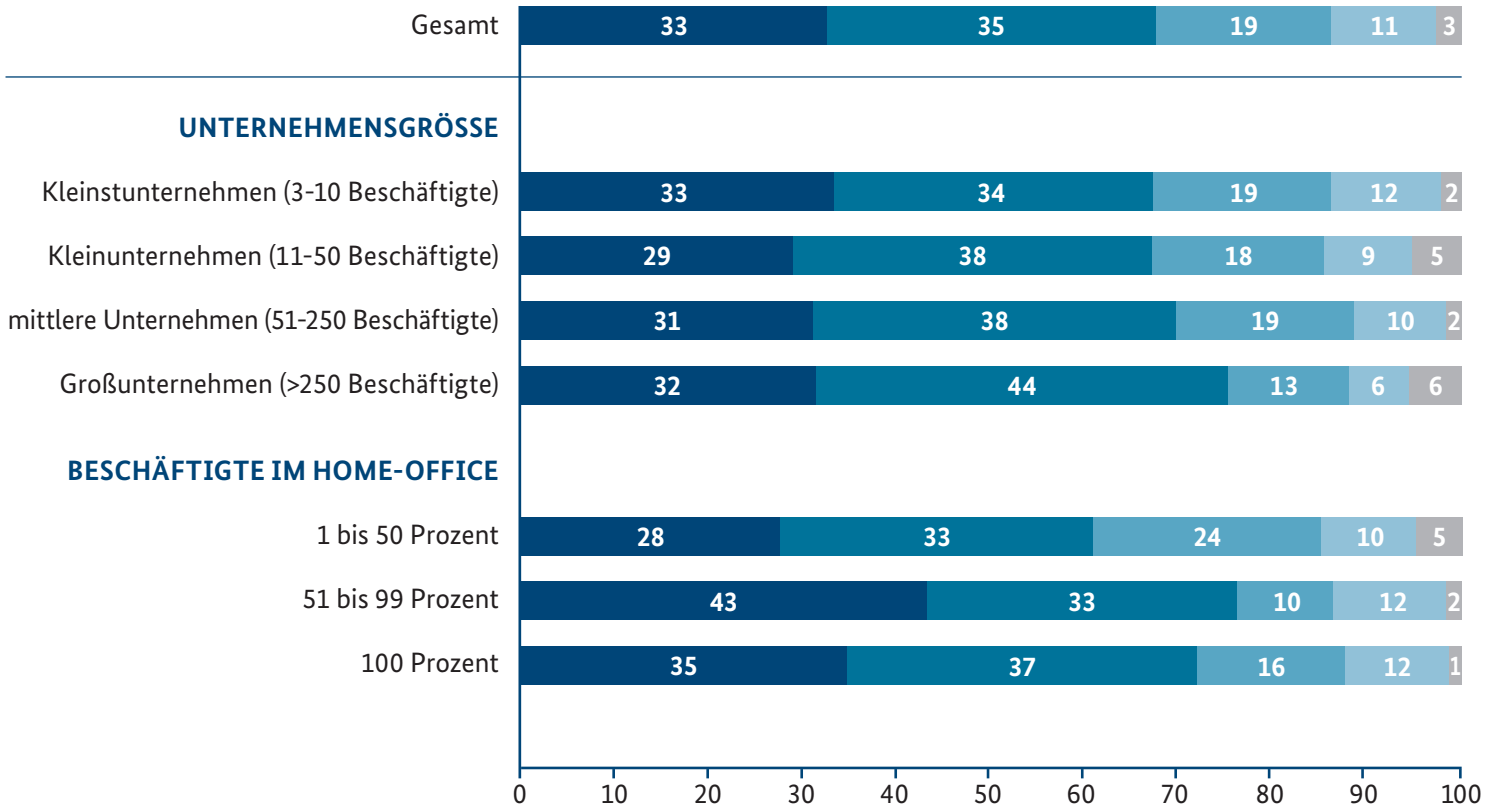
Frage: Welche Rolle spielt denn der Aspekt der „Informationssicherheit“ in Ihrem Unternehmen im Zuge der (weiteren) Digitalisierung von Geschäftsprozessen? Welcher der folgenden Aussagen stimmen Sie am ehesten zu?

Cyber-Sicherheit wird nur von 51 % der Unternehmen von Anfang an mitgedacht.

DIGITALISIERUNG

Angaben in %;
Basis: alle Befragten n = 1.000

WICHTIGKEIT, IN DEUTSCHLAND ODER DER EUROPÄISCHEN UNION HERGESTELLTE IT-LÖSUNGEN ZU NUTZEN



Frage: Wie wichtig ist es für Sie, dass Ihre IT-Lösungen und IT-Anlagen in Deutschland oder der Europäischen Union hergestellt oder entwickelt wurden?

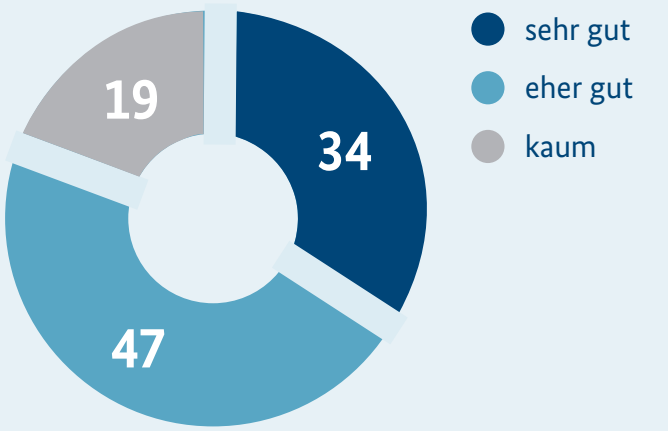
Mehr als zwei Drittel der Unternehmen schätzen es als eher oder sogar sehr wichtig ein, dass ihre IT-Lösungen und Anlagen in Deutschland oder der EU entwickelt/ angefertigt werden.

STATISTIK

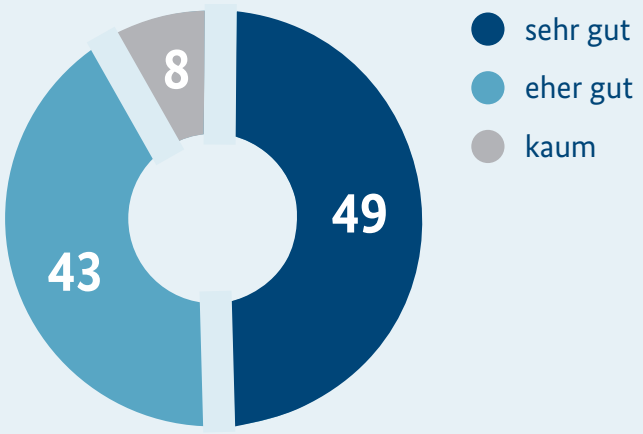
Angaben in %;
Basis: alle Befragten n = 1.000

ÜBERBLICK STATISTIK

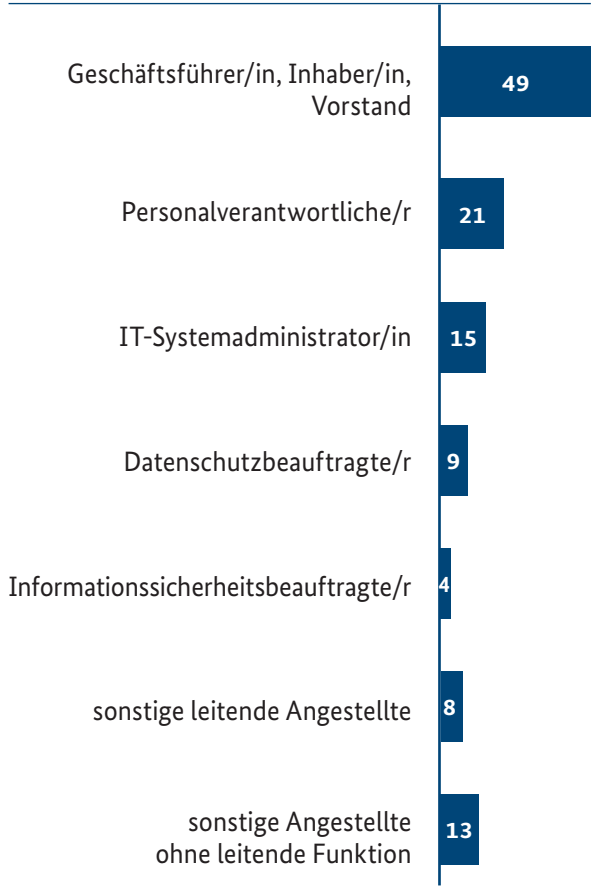
INFORMIERTHEIT ÜBER IT-SICHERHEIT/-STRUKTUR



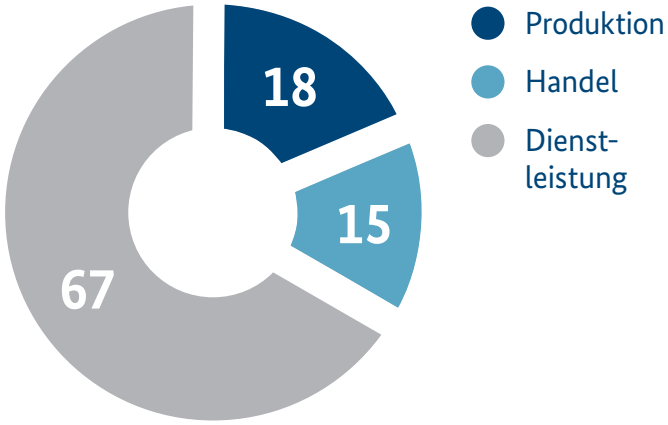
INFORMIERTHEIT ÜBER TECHNISCHE AUSSTATTUNG



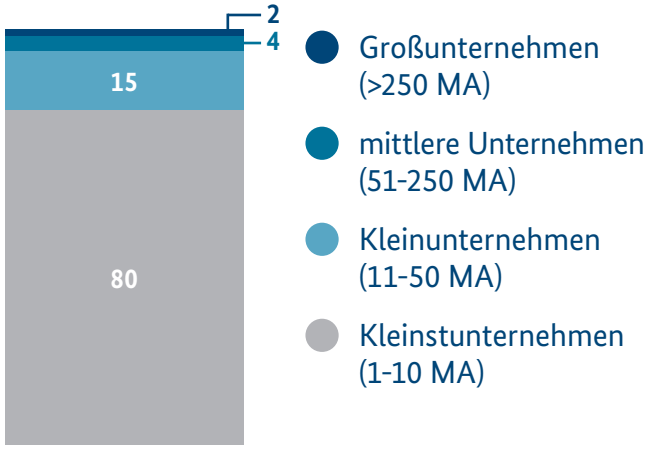
FUNKTION IM UNTERNEHMEN



BRANCHE



ANZAHL DER MITARBEITER*INNEN



PRÄVENTION

Die Ergebnisse der Umfrage zeigen, dass viele Unternehmen vorhaben, auch nach der Corona-Krise ihr Home-Office Angebot im bestehenden Umfang beizubehalten, oder sogar noch ausweiten wollen. Obwohl bereits jetzt die durch das Home-Office **gesteigerte Angriffsfläche** von **Cyber-Kriminellen teilweise erfolgreich ausgenutzt** wird, planen **nur wenige Unternehmen** ihre Cyber-Sicherheitsvorkehrungen diesen strukturellen Veränderungen anzupassen. Insbesondere Kleinst- und Kleinunternehmen **benötigen langfristig Unterstützung** beim grundsätzlichen Vorgehen und bei der Umsetzung von Maßnahmen zur Erhöhung der Cyber-Sicherheit im Unternehmen.

Das Bundesamt für Sicherheit in der Informationstechnik bietet Hilfestellungen und Informationsangebote zur Steigerung der Cyber-Sicherheit in Unternehmen.

Allianz für Cyber-Sicherheit

Die **Allianz für Cyber-Sicherheit (ACS)** ist die Dialog-Plattform des BSI mit der Wirtschaft. Für den erfolgreichen Umgang mit Cyber-Risiken sind aktuelle Informationen, Wissens- und Erfahrungsaustausch sowie der stetige Ausbau von Sicherheitskompetenzen unerlässlich. Werden auch Sie Teil unseres starken Netzwerkes:

https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Ueber-uns/Netzwerke-schuetzen-Netzwerke/netzwerke-schuetzen-netzwerke_node.html

Das BSI und die ACS haben die besonderen infrastrukturellen Bedingungen des mobilen Arbeitens berücksichtigt und **gezielte Empfehlungen** und **Informationsangebote** zur Absicherung des dislozierten Arbeitens für Sie zusammengestellt:

https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Remote/remote_node.html

Sie haben kurzfristig Home-Office Plätze geschaffen? Überprüfen Sie mit unserer **Checkliste** Ihre getroffenen Maßnahmen zur IT-Sicherheit. Die **Checkliste** richtet sich vor allem an kleine und mittelständische Unternehmen und ist als Basismaßnahme zur Umsetzung des Home-Office gedacht. Gleichzeitig können Sie anhand der gestellten Fragen bereits getroffene Vorkehrungen überprüfen. So können Sie die IT-Sicherheits-Schutzziele – Verfügbarkeit, Vertraulichkeit, Integrität – wirksam umzusetzen:

https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Remote/Home-Office/Checkliste-Home-Office/checkhomeoffice_node.html

PRÄVENTION

Mit den nachfolgenden **10 Tipps** zeigen wir Ihnen, wo Sie ansetzen können, um einen umfassenden Schutz aufzubauen. Oder nutzen Sie sie als Checkliste, ob jedem dieser wichtigen Aspekte neben dem Tagesgeschäft auch immer noch die gebührende Aufmerksamkeit zuteil wird:

https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/10-Tipps-zur-Cyber-Sicherheit-fuer-Unternehmen/10-tipps-zur-cyber-sicherheit-fuer-unternehmen_node.html

Sorgen Sie auch im Home-Office für **klare Notfallwege**. Ihren Mitarbeitenden werden wichtige Verhaltenshinweise bei IT-Notfällen aller Art an die Hand gegeben. Die aufgeführten Maßnahmen ermöglichen es Unternehmen und Organisationen, vom ersten Moment an die richtigen Entscheidungen treffen zu können:

https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/it-notfallkarte_node.html

IT-Sicherheit erhöhen, aber wie? Mit dem **Routenplaner** „Cyber-Sicherheit für Handwerksbetriebe“ haben Sie eine praktische Arbeitshilfe an der Hand, die Sie Schritt für Schritt durch den Sicherheitsprozess führt. Expert* innenaus Handwerksorganisationen und dem BSI schlagen Ihnen individuelle Routen gemäß IT-Grundschutz des BSI vor:

https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/Routenplaner/routenplaner_node.html

Cyber-Sicherheit zum Sehen und Hören. In unseren neuen Formaten nehmen wir uns die Zeit, einzelne Themen rund um Cyber-Sicherheit mit Expert* innen zu beleuchten:

Der **Cyber-Sicherheits-Web-Talk** ist ein Online-Seminar-Format der ACS. In den zweistündigen Talks haben Teilnehmende die Möglichkeit, mit Experten in Kontakt zu treten und ihre Kenntnisse zu einem bestimmten Thema zu vertiefen:

https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Netzwerk-Formate/Veranstaltungen-und-Austausch/Cyber-Sicherheits-Web-Talk/cyber-sicherheits-web-talk_node.html

CYBERSNACS ist der ACS-Podcast „to go“ auf die Ohren. Jeden Monat stellen die Moderator*innen Themen rund um Digitalisierung und Cyber-Sicherheit in der Wirtschaft vor:

https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Netzwerk-Formate/Medien/Cyber-Sicherheits-Podcast/cyber-sicherheits-podcast_node.html

Beim **BSI-Podcast „Update verfügbar“** stehen aktuelle Geschehnisse und Tipps zur Cyber-Sicherheit für Privatanwender*innen im Zentrum:

https://www.bsi.bund.de/DE/Service-Navi/Mediathek/Podcast/podcast_node.html

IMPRESSUM

HERAUSGEBER:

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Die Erhebung und Auswertung für die Umfrage
„IT-Sicherheit im Home-Office“ wurde vorgelegt von:
INFO GmbH Markt- und Meinungsforschung
Schönholzer Str. 1A, 13187 Berlin

AUTOREN DER STUDIE:

Agnieszka Pawlowska, Benedikt Scherer

BEZUGSQUELLE:

Bundesamt für Sicherheit in der Informationstechnik (BSI),
Godesberger Allee 185–189, 53175 Bonn
E-Mail: bsi@bsi.bund.de
Telefon: +49 (0) 22899 9582-0
Telefax: +49 (0) 22899 9582-5400
www.bsi.bund.de
www.allianz-fuer-cybersicherheit.de

BILDNACHWEIS:

Titel: GettyImages ©borchee; S. 2: GettyImages ©Westend61

GESTALTUNG:

Faktor 3 AG

Stand: 04/2021