INFO GmbH
Markt- und Meinungsforschung

Schönholzer Straße 1A,
D-13187 Berlin

Geschäftsführer: Dr. Holger Liljeberg

Tel. +49-30/49001-0
Fax +49-30/49001-499

mail@infogmbh.de
www.infogmbh.de

Ein Unternehmen der INFO Research Group

Ergebnisbericht

IT-Sicherheit im Home-Office

unter besonderer Berücksichtigung der Covid-19 Situation

für

Bundesamt
für Sicherheit in der
Informationstechnik

Berlin, August 2021

Inhalt

1. Zusammenfassung

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. Bei den befragten Firmen hat sich die Zahl der angebotenen Home-Office Arbeitsplätze aufgrund von Corona mehr als verdoppelt. Vor allem kleine Unternehmen nutzten diese Möglichkeit.

Auch perspektivisch wollen viele Unternehmen das Arbeiten im Home-Office im gleichen Maße erhalten oder sogar ausweiten. Insbesondere Großunternehmen planen diesen Schritt.

Die IT-Ausstattung hinkt allerdings noch hinterher: In vielen, vor allem kleineren Firmen verwenden Beschäftigte im Home-Office auch oder überwiegend ihre privaten Geräte.

Zu viele Unternehmen vernachlässigen die Cyber-Sicherheit

Bei der Umsetzung technischer und organisatorischer Sicherheitsmaßnahmen ergibt sich ein mangelhaftes Bild.

Abgesehen von einfachen technischen Maßnahmen wie Passwortschutz, Hardware-Firewall und regelmäßige manuelle Updates werden viele weitere empfohlene Schritte nur von einigen Unternehmen umgesetzt. Zu kurz kommt vor allem die Endgerätesicherheit, insbesondere von mobilen Geräten.

Außer einer Mitarbeitersensibilisierung nehmen organisatorische Maßnahmen wenig Raum ein. Besonders kurz kommen regelmäßige Notfallübungen, der Aufbau einer eigenen IT-Sicherheitsabteilung und Neueinstellungen in diesem Bereich.

Der zum Teil erhebliche Nachholbedarf betrifft insbesondere Klein- und vor allem Kleinst-unternehmen.

Trotz erhöhter Angriffsfläche sparen die Unternehmen an der Sicherheit: Über die Hälfte investiert weniger als 10 Prozent seines IT-Budgets in Cyber-Sicherheit, nur jedes sechste Unternehmen hat sein Budget währen der Corona-Krise erhöht.

Mit ihrem Status Quo scheinen sich die meisten zufrieden zu geben: Nur wenige Firmen planen eine Erhöhung des Budgets und weitere Schutzmaßnahmen zur Absicherung des mobilen Arbeitens.

Auch hier sind es eher Großunternehmen, die langfristiger investieren wollen. Ausgerechnet die kleinen Unternehmen, die den größten Nachholbedarf haben, äußern diesen Plan nur selten.

Cyber-Angriffe betreffen vor allem Großunternehmen

8 Prozent der befragten Unternehmen mussten während der Corona-Krise auf eine Cyber-Attacke reagieren. Besonders stark betroffen waren Großunternehmen: Hier war jedes vierte Ziel eines solchen Angriffs. Kleine Firmen erlebten dies zwar deutlich seltener, erlitten aber größere, zum Teil sogar existenzbedrohende Schäden.

COVID-19-Krise insbesondere für größere Unternehmen ein Digitalisierungsturbo

Rund ein Drittel der Unternehmen hat aufgrund der Corona-Krise Digitalisierungsprojekte zeitlich vorgezogen oder neu geplant und implementiert.

Zwei Drittel der Großunternehmen erlebten die Corona-Krise als „Digitalisierungsturbo“, bei den mittleren Firmen war es knapp die Hälfte, bei Kleinstunternehmen nur jedes dritte.

Während der Corona-Krise ist vor allem die Nutzung von Video-Konferenz-Systemen stark angestiegen. Die meisten der abgefragten IT-Lösungen mit Home-Office-Bezug wurden jedoch schon zuvor genutzt. Nur wenige Unternehmen planen einen weiteren Ausbau von unterstützenden IT-Lösungen.

Vor allem schlecht ausgestattete Unternehmen vernachlässigen die Cyber-Sicherheit

Bei der Einführung von Geschäftsprozessen wird Cyber-Sicherheit häufig nicht von vornherein mitgedacht. Etwa die Hälfte der Unternehmen berücksichtigen Cyber-Sicherheitsmaßnahmen, wenn überhaupt, erst während der Implementierung oder später.

Dies betrifft vor allem Unternehmen, die sich selbst einen schlechten Stand der IT-Entwicklung und Digitalisierung attestieren.

IT-Lösungen aus Deutschland oder der EU gewünscht

Zwei Drittel der Unternehmen ist es wichtig, dass ihre IT-Lösungen und Anlagen in Deutschland oder der EU entwickelt bzw. angefertigt werden. Dieser Wunsch wird besonders häufig von Großunternehmen und Firmen mit hohem Home-Office-Anteil geäußert.

2. Zielsetzung der Erhebung

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 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. Ziel der Befragung war, die Lage der IT-Sicherheit im Home-Office vor und während der Pandemie abzubilden.

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 drei Beschäftigten identifiziert. Diese Untersuchung gibt keinen Überblick auf den allgemeinen Stand der IT-Sicherheit in deutschen Unternehmen.

3. Erhebungsdesign

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

Grundgesamtheit der Erhebung waren Unternehmen, Organisationen und Verbände der Wirtschaft aller Branchen mit mindestens drei Beschäftigten, die Home-Office angeboten haben. Befragt wurden insgesamt 1000 kleinere und mittlere Unternehmen (KMU) sowie Großunternehmen.

Die Befragung fand zwischen dem 12. Oktober und 11. November 2020 statt und wurde in Form von Online-Interviews (CAWI) und computergestützten Telefoninterviews (CATI) realisiert. Die CAWI-Befragten wurden per quotierter Zufallsauswahl aus einem aktiv rekrutierten Online-Accesspanel gewonnen, die CATI-Befragten per Zufallsstichprobe aus Firmenadressen eines Adressanbieters ausgewählt.

Um repräsentative Gesamtergebnisse zu erzielen, wurden der vollständige Datensatz und die Kurzinterviews (Firmen, die kein Home-Office angeboten haben) nach den Merkmalen Branche und Unternehmensgröße gewichtet.

4. Home-Office während der COVID 19-Pandemie

4.1. Anteil der Beschäftigten im Home-Office

Im vergangenen Jahr war bei den Unternehmen der Anteil der Beschäftigten im Home-Office hoch: Im Durchschnitt arbeiteten **64 Prozent der Beschäftigten** voll oder teilweise von zu Hause, zwar nicht alle im Zusammenhang mit Corona, aber die Zahl der Heim-Arbeitsplätze hat sich aufgrund der Pandemie-Situation **mehr als verdoppelt**. Während zuvor bzw. unabhängig von der Corona-Krise im Durchschnitt 25 Prozent der Belegschaft das Home-Office nutzten, kamen wegen der Pandemie 39 Prozent hinzu.

Vor allem kleine Unternehmen ermöglichen das Home-Office: In Kleinstunternehmen arbeiteten im letzten Jahr etwas mehr als zwei Drittel der Mitarbeitenden zumindest zeitweise im Home-Office, 41 Prozent wegen Corona. In Kleinunternehmen war es rund die Hälfte der Belegschaft, darunter ein Drittel Pandemie-bedingt. In mittleren und großen Firmen lag der Home-Office-Anteil bei knapp unter 50 Prozent, ein gutes Viertel der Belegschaft arbeitete aus Corona-Schutzgründen zu Hause.

Je mehr Beschäftigte zu Hause arbeiteten, desto höher war der prozentuale Anteil der Home-Office-Arbeitsplätze in Zusammenhang mit Corona: Unternehmen, die mindestens die Hälfte oder sogar alle Mitarbeitenden ins Home-Office schickten, begründeten über zwei Drittel der Fälle mit „einer Maßnahme der Eindämmung der COVID-19-Pandemie“. Waren 50 Prozent oder weniger im Home-Office, galt das nur für etwa die Hälfte.

In Unternehmen, die wegen Corona ihrer kompletten Belegschaft Home-Office ermöglichten, arbeiteten im Durchschnitt 71 Prozent zu Hause. Aber auch in Firmen, in denen Corona seltener oder gar nicht die Begründung war, nutzten rund sechs von zehn Beschäftigten einen mobilen Arbeitsplatz.

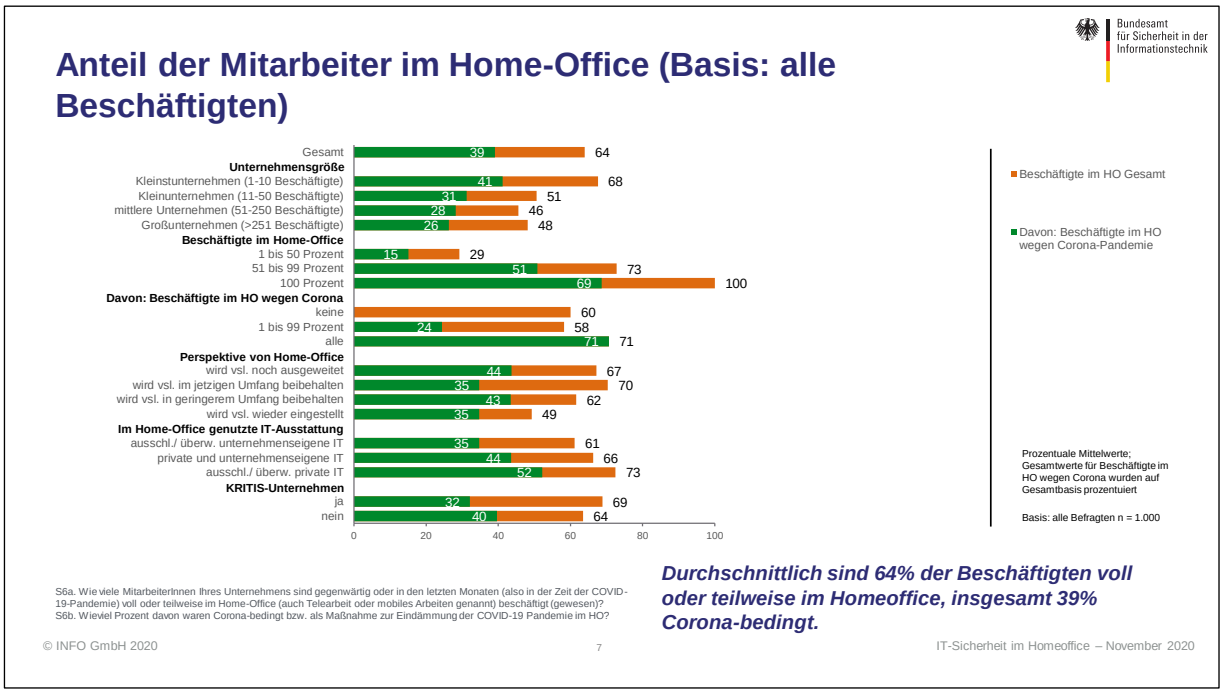

Abbildung 1 - Anteil der Mitarbeiter im Home-Office.

4.2. Perspektive von Home-Office, Telearbeit und mobilem Arbeiten

Die meisten Unternehmen **möchten am mobilen Arbeiten festhalten**. 58 Prozent planen, ihr Home-Office-Angebot nach der Corona-Krise entweder im gleichen Umfang aufrechtzuerhalten (39 Prozent) oder sogar auszuweiten (19 Prozent). Jedes vierte Unternehmen will das Angebot in geringerem Umfang beibehalten, und nur 16 Prozent wollen es voraussichtlich einstellen.

Besonders Firmen, die alle Mitarbeitenden ins Home-Office schickten, wollen auch künftig an der Möglichkeit festhalten: 69 Prozent planen, das Angebot mindestens im gleichem Umfang beizubehalten (47 Prozent) oder zu vergrößern (22 Prozent).

Die Offenheit für Home-Office hat nicht zwingend mit der Pandemie zu tun: Auch drei Viertel der Firmen, deren Beschäftigte im letzten Jahr aus anderen Gründen als Corona zu Hause arbeiteten, wollen dies künftig fortführen.

Insbesondere **Großunternehmen setzen perspektivisch auf das Home-Office**: 35 Prozent wollen das mobile Arbeiten weiter ausbauen, weitere 34 Prozent beibehalten, und nur 2 Prozent werden diese Möglichkeit voraussichtlich wieder einstellen.

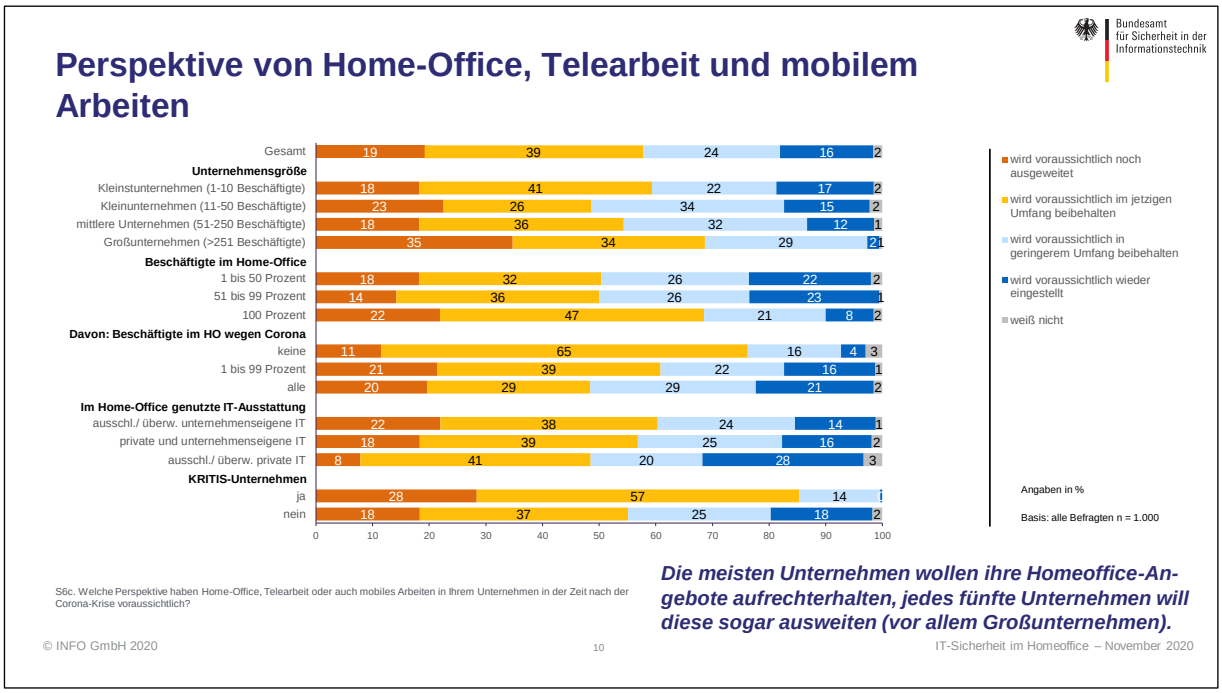

Abbildung 2 - Perspektive von Home-Office, Telearbeit und mobilem Arbeiten.

4.3. IT-Ausstattung im Home-Office

In nur rund **42 Prozent der Unternehmen** wird im Home-Office **ausschließlich unternehmenseigene IT** genutzt, in allen anderen ist zumindest teilweise auch private IT-Ausstattung im Einsatz.

Ein **wichtiger Faktor ist hierbei die Unternehmensgröße**: 13 Prozent der Kleinstunternehmen nutzen zu Hause überwiegend oder ausschließlich private Geräte, während dies nur in 2 Prozent der Großunternehmen der Fall ist.

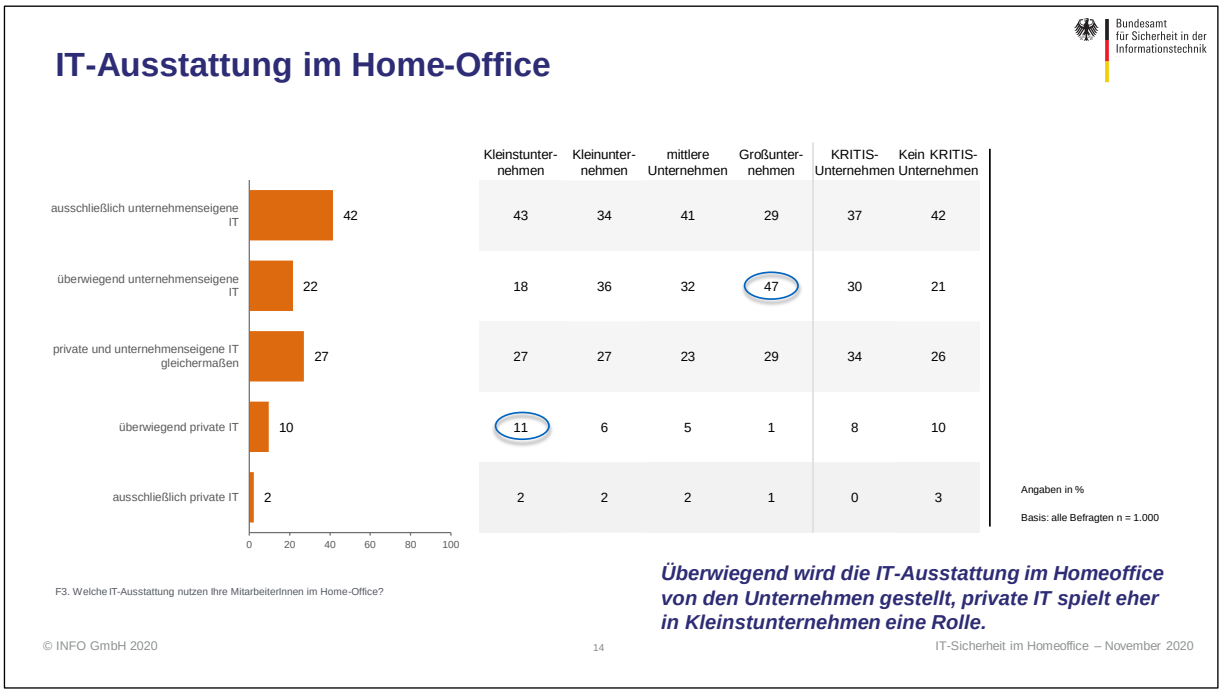

Abbildung 3 - IT-Ausstattung im Home-Office.

5. Sicherheitsmaßnahmen

5.1. Umsetzung technischer Sicherheitsmaßnahmen

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?

Abgesehen von der Umsetzung einfacher technischer Sicherheitsmaßnahmen **vernachlässigen zu viele Unternehmen weitere empfohlene Schritte.**

Die meisten der für das mobile Arbeiten besonders wichtigen Maßnahmen wurden von den Unternehmen **schon vor der Corona-Krise umgesetzt**; im vergangenen Jahr kamen nur wenige Investitionen hinzu.

Zwei Drittel haben ein VPN eingerichtet und verschlüsseln Datenträger, über die Hälfte hat eine Mehrfaktor-Authentifizierung und die Segmentierung bzw. Absicherung von Netzen implementiert. Besonders problematisch ist, dass nur 38 Prozent der Unternehmen ein Mobile Device Management eingeführt haben.

Trotz gestiegener Cyber-Gefahr **haben nur wenige Unternehmen die Umsetzung fehlender Schutzmaßnahmen vorgesehen**. Oben auf der Liste stehen hier die Mehr-Faktor-Authentifizierung, das Mobile Device Management sowie die Verschlüsselung der

Telekommunikation, deren Einführung jeweils 12 Prozent planen.

Vor allem die mobilen Endgeräte bleiben die Sicherheitslücke Nummer 1: Jedes zweite Unternehmen plant hier keinen weiteren Schutz (31 Prozent) oder kann die Frage nicht beantworten (19 Prozent).

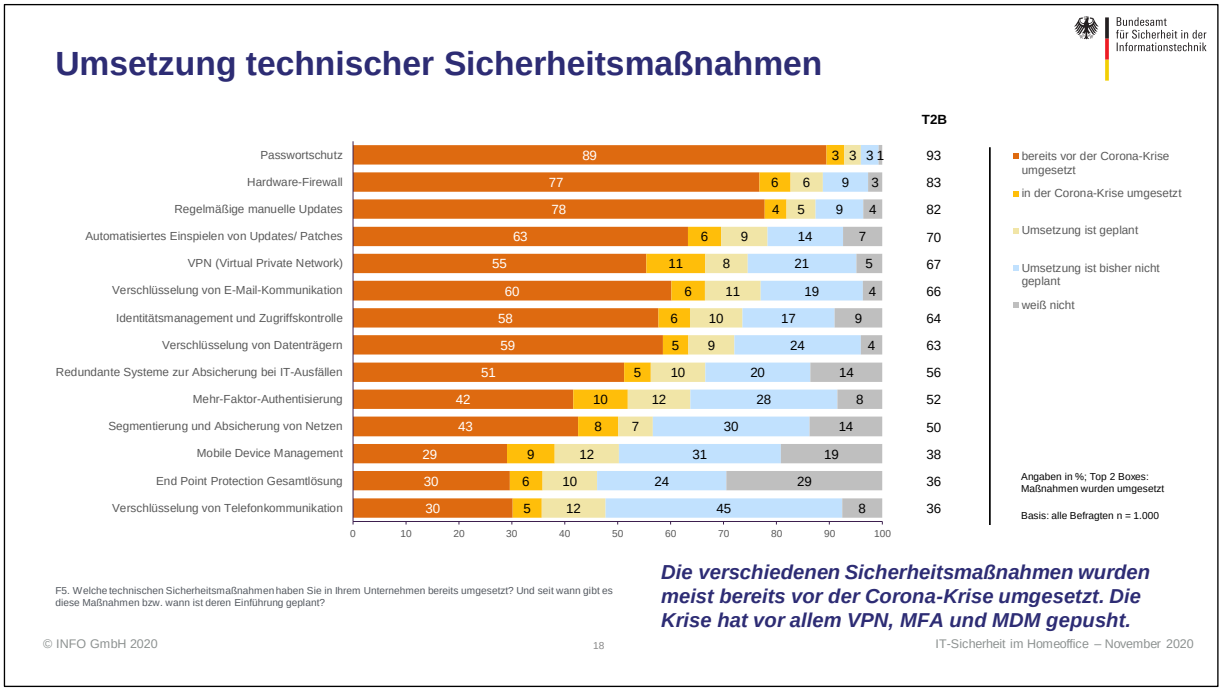

Abbildung 4 - Umsetzung technischer Sicherheitsmaßnahmen.

Die drei mit Abstand am häufigsten umgesetzten Maßnahmen sind: Passwortschutz (93 Prozent), Hardware-Firewall (83 Prozent) und regelmäßige manuelle Updates (82 Prozent).

Neben den im obigen Chart bereits erwähnten Maßnahmen spielen 70 Prozent der Unternehmen Updates/ Patches automatisch ein, zwei Drittel verschlüsseln die E-Mail-Kommunikation (66 Prozent) und bieten eine Sicherung durch Identitätsmanagement und Zugriffskontrolle (64 Prozent). Über die Hälfte der Unternehmen haben redundante Systeme zur Absicherung bei IT-Ausfällen (56 Prozent).

Vernachlässigt werden neben dem Mobile Device Management auch das Endpoint Protection-System (36 Prozent) und die Verschlüsselung der Telekommunikation (36 Prozent).

Was die IT-Sicherheit angeht, gibt es allerdings erhebliche Unterschiede: **Je kleiner das Unternehmen, desto schlechter ist der Schutz.**

Während Großunternehmen überwiegend die meisten der vorgelegten Maßnahmen umgesetzt haben, ist der Schutz bei vielen kleineren Unternehmen mangelhaft, insbesondere bei den mobilen Endgeräten.

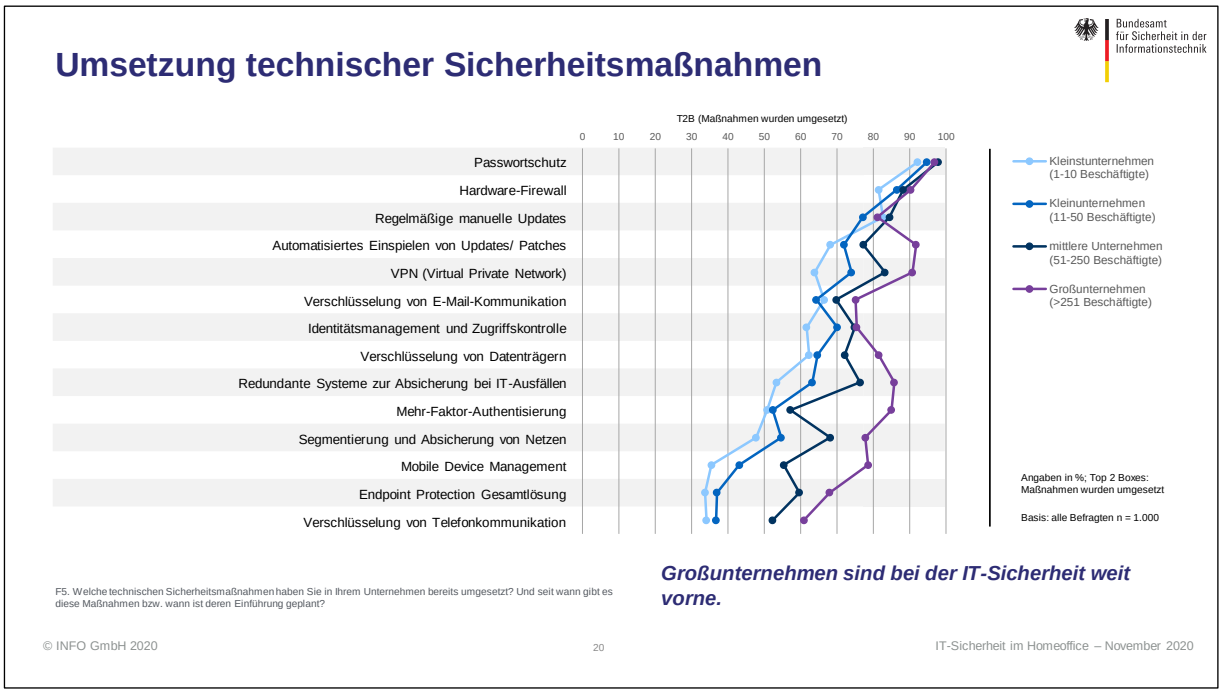

Abbildung 5 - Umsetzung technischer Sicherheitsmaßnahmen nach Unternehmensgröße.

5.2. Umsetzung organisatorischer Sicherheitsmaßnahmen

Im organisatorischen Bereich steht mit großem Abstand die Mitarbeitersensibilisierung an erster Stelle (80 Prozent), gefolgt von einem Notfallmanagement (60 Prozent) und einer IT-Sicherheitsstrategie (59 Prozent). Dem Leitgedanken, dass Cyber-Sicherheit Chefsache sei, folgen jedoch nur 51 Prozent der Unternehmen.

Deutlich seltener ist die Beauftragung eines externen Sicherheitsdienstleisters (35 Prozent), die Etablierung eines/r internen Informationssicherheitsbeauftragten (30 Prozent) und der Aufbau eines Informationssicherheits-Management-Systems (30 Prozent).

Klarer Nachholbedarf besteht bei Notfallübungen: Nur 24 Prozent der Unternehmen lassen ihre Beschäftigten regelmäßig trainieren, was bei einem Angriff zu tun ist.

Auch der Personaleinsatz scheint offenbar limitiert: Nur 18 Prozent der Unternehmen haben eine eigene Abteilung „IT-Sicherheit“ aufgebaut, und nur 16 Prozent haben neues Personal im IT-Sicherheitsbereich eingestellt. In diesem Bereich besteht die geringste Aussicht auf Verbesserung: Auch für die Zukunft planen nur wenige Firmen eine personelle Erweiterung, drei Viertel haben dies nicht vor.

Die meisten der getroffenen organisatorischen Sicherheitsmaßnahmen wurden zwar bereits vor der Corona-Krise getroffen, aber obwohl viele der abgefragten Maßnahmen bisher noch nicht umgesetzt wurden, ist bei ihnen auch **eine zukünftige Umsetzung nicht geplant**. Insbesondere die größere Einbindung ihrer Mitarbeitenden ist, abgesehen von der

Sensibilisierung für das Thema, sehr häufig nicht vorgesehen: Bei deutlich über der Hälfte der Unternehmen sind keine regelmäßigen Notfallübungen oder die Ernennung eines IT-Sicherheitsbeauftragen geplant.

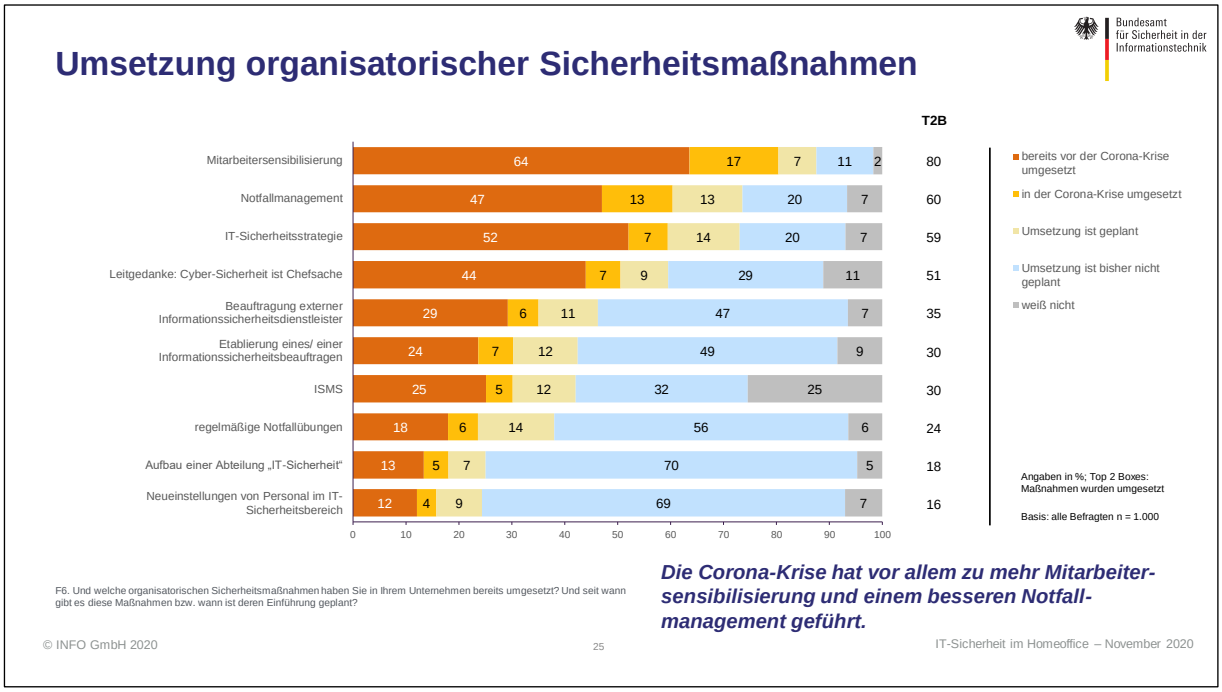

Abbildung 6 - Umsetzung organisatorischer Sicherheitsmaßnahmen.

Auch bei den organisatorischen Sicherheitsmaßnahmen zeigen sich deutliche Differenzen zwischen größeren und kleineren Betrieben. Die Großunternehmen haben nahezu alle abgefragten Maßnahmen häufiger bereits implementiert, vor allem die Beauftragung externer Dienstleister, die Etablierung von Sicherheitsbeauftragten, eines ISMS, die regelmäßige Durchführung von Notfallübungen sowie den Aufbau einer IT-Sicherheitsabteilung.

Kleine Unternehmen haben insgesamt weniger Maßnahmen umgesetzt. Insbesondere Neueinstellungen, der Aufbau einer eigenen Abteilung für IT-Sicherheit sowie regelmäßige Notfallübungen wurden kaum umgesetzt. Im Vergleich zu größeren Unternehmen ist der Abstand bei der Etablierung eines IT-Sicherheitsbeauftragten sowie einer IT-Sicherheitsstrategie, aber auch Notfallübungen und der Beauftragung externer Dienstleister für die IT-Sicherheit am größten.

Nur bei der mangelhaften Umsetzung des Leitgedankens „Cyber-Sicherheit ist Chefsache“ zeigt sich ein einheitliches Meinungsbild bei Unternehmen aller Größenklassen auf einem ähnlich geringen Niveau von 50 bis unter 55 Prozent.

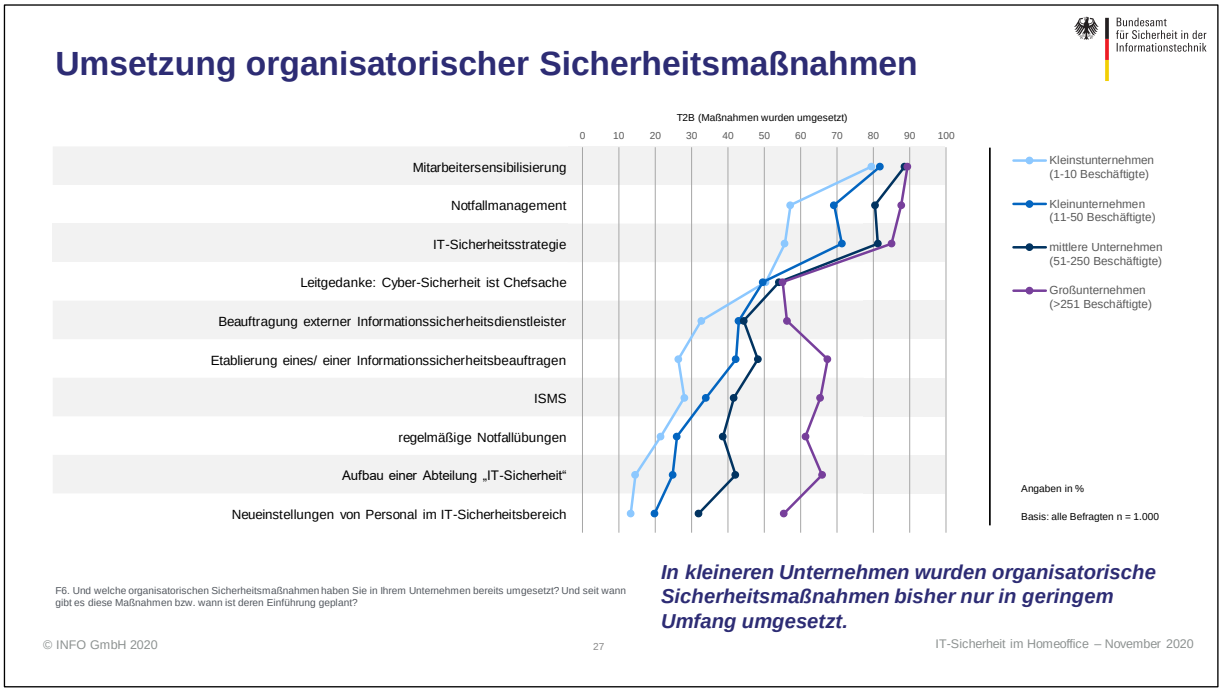

Abbildung 7 - Umsetzung organisatorischer Sicherheitsmaßnahmen nach Unternehmensgröße.

5.3. Budget für IT-Sicherheit

Dass IT-Schutzmaßnahmen für die meisten Unternehmen nicht an erster Stelle stehen, spiegelt sich auch in ihren Ausgaben wider. **Gut die Hälfte der Unternehmen investiert höchstens 10 Prozent ihres IT-Budgets** in Cyber-Sicherheit, nur jedes fünfte gibt dafür mindestens 25 Prozent oder mehr aus. 4 Prozent der befragten Unternehmen planen gar kein Budget für den Bereich „Cyber-Sicherheit“ ein.

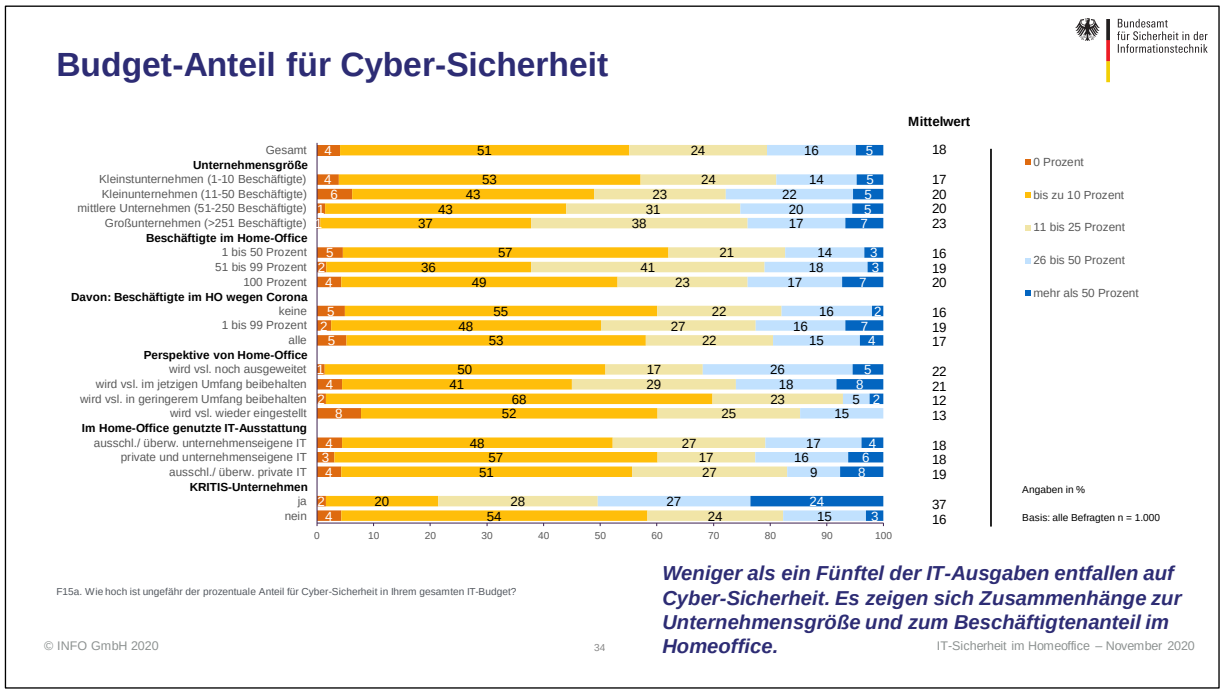

Abbildung 8 - Budget-Anteil für Cyber-Sicherheit.

In knapp zwei Drittel der Unternehmen blieb das Budget währen der COVID-19-Krise unverändert. Trotz verstärkter Nutzung des Home-Offices haben nur 17 Prozent der Unternehmen mehr Geld in die IT-Sicherheit investiert, davon werden 11 Prozent explizit mit der Cyber-Sicherheitslage begründet. Eine spätere Erhöhung haben nur 5 Prozent geplant, in 4 Prozent der Firmen wurde das Budget sogar gekürzt.

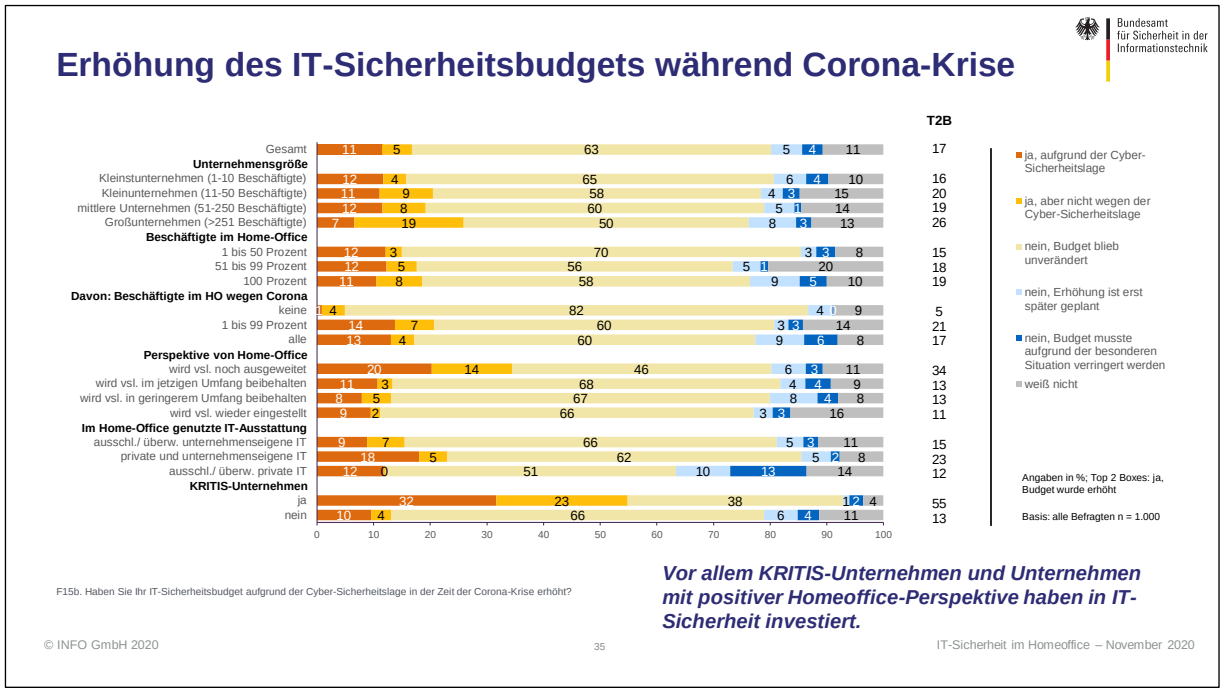

Abbildung 9 - Erhöhung des IT-Sicherheitsbudgets während Corona-Krise.

Gefragt nach weiteren Sicherheitsmaßnahmen, bestätigten **nur 7 Prozent der Unternehmen, Maßnahmen für die IT-Sicherheit des Home-Office zu planen**. Großunternehmen haben eher langfristigere Investitionen budgetiert (18 Prozent) als - ausgerechnet - die kleinen Unternehmen, die den größten Nachholbedarf haben.

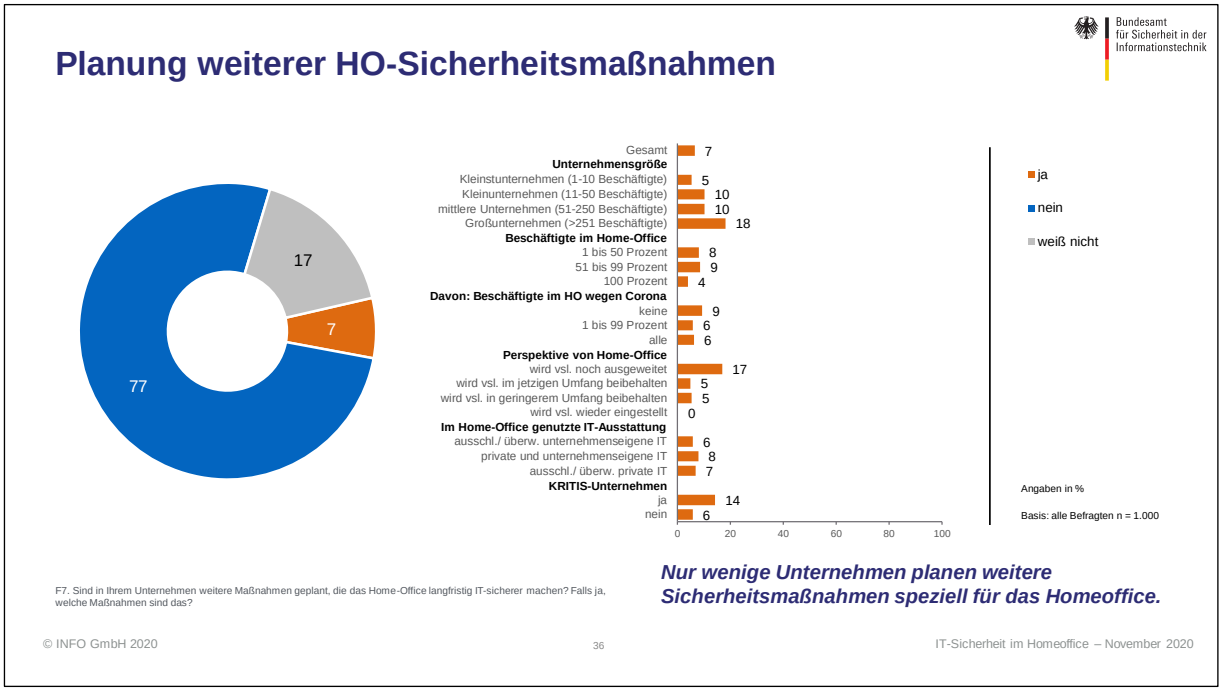

Abbildung 10 - Planung weiterer HO-Sicherheitsmaßnahmen.

6. Cyber-Angriffe während der Home-Office-Zeit

6.1. Notwendige Reaktionen auf Cyber-Angriffe

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?

8 Prozent der befragten Unternehmen mussten während der Corona-Krise auf Cyber-Attacken reagieren. **Am stärksten betroffen waren Großunternehmen** (24 Prozent), am stärksten verschont blieben Kleinstunternehmen (7 Prozent), kleinere und mittlere Unternehmen liegen mit 12 Prozent bzw. 14 Prozent dazwischen.

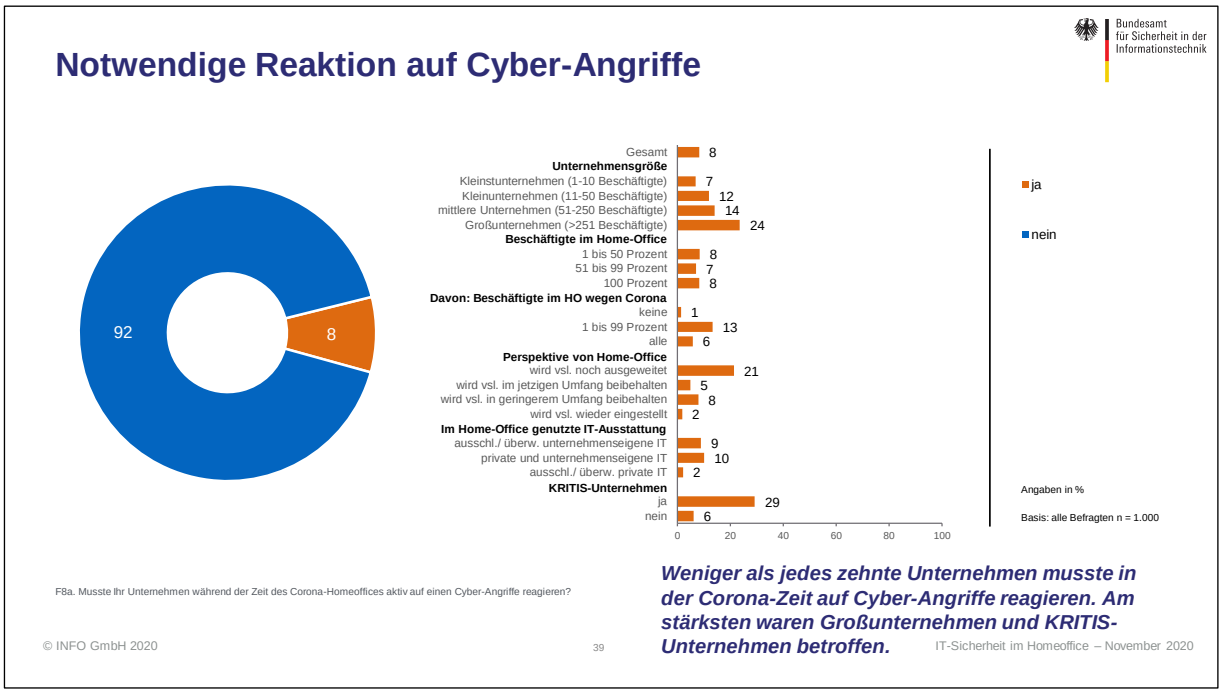

Abbildung 11 - Notwendige Reaktion auf Cyber-Angriffe.

6.2. Bewertung des Schadens durch Cyber-Angriffe

Für die Hälfte der betroffenen Unternehmen hatte ein Angriff auf ihre IT spürbare materielle Folgen.

Je kleiner die Firma, desto größer war der Schaden: Bei jedem zweiten kleinen Unternehmen, das von einer Cyberattacke betroffen war, hatte dies mindestens „eher schwere“ Folgen. Insgesamt 12 Prozent der attackierten Kleinstunternehmen und kleinen Unternehmen hatten sogar mit einem existenzbedrohenden Schaden zu kämpfen.

Von den betroffenen mittleren und großen Unternehmen geriet dagegen keines in eine existenzbedrohende Lage. Bei 38 Prozent der mittelgroßen Firmen war der Schaden „sehr“ (16 Prozent) oder „etwas“ (22 Prozent) schwer. Am glimpflichsten kamen die Großunternehmen davon: Nur 6 Prozent waren mit „sehr schweren“, weitere 27 Prozent mit „eher schweren“ materiellen Folgen konfrontiert.

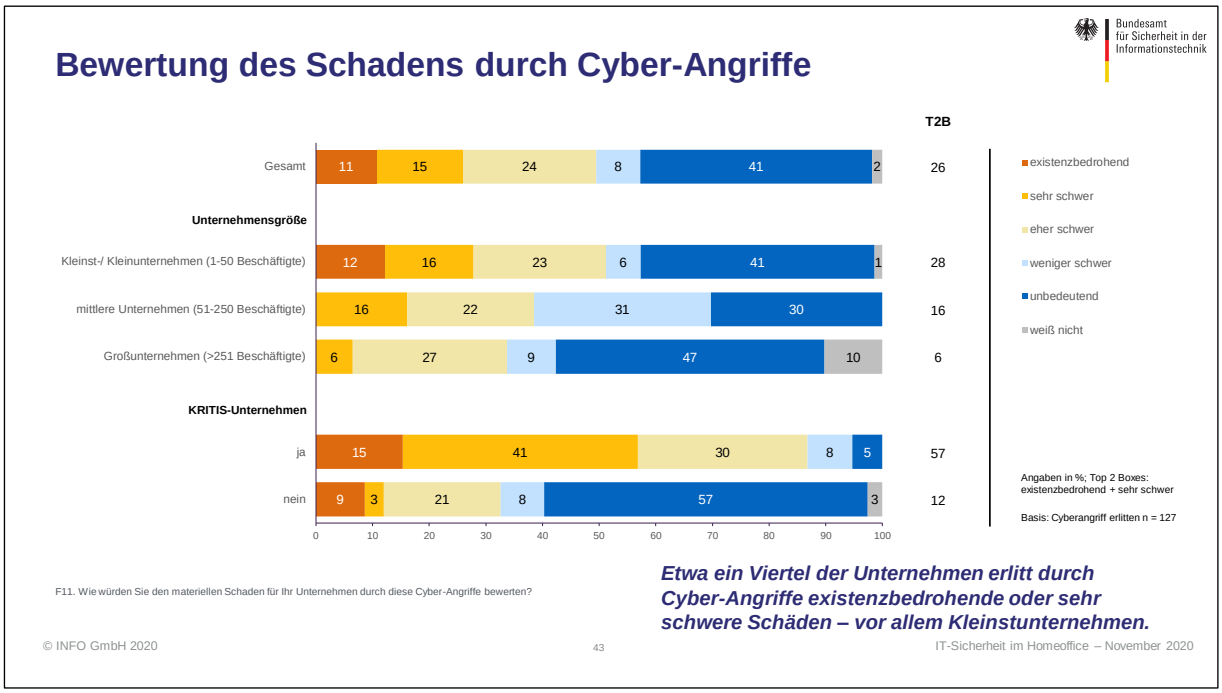

Abbildung 12 - Bewertung des Schadens durch Cyber-Angriffe.

7. Digitalisierung

7.1. Stand der IT-Entwicklung und Digitalisierung

Die COVID-19-Pandemie hat das Potential, die Arbeitswelt nachhaltig zu verändern. Unternehmen stellten Teile des Arbeitens auf Home-Office um, aber beschleunigten sie auch Digitalisierungsprozesse, um weiterhin arbeits- und wettbewerbsfähig zu bleiben?

Die befragten Unternehmen sind mit dem Stand ihrer IT-Entwicklung und Digitalisierung überwiegend zufrieden. Die Hälfte schätzt den Status Quo als „gut“ (39 Prozent) oder sogar „sehr gut“ (12 Prozent) ein. Weitere 37 Prozent vergeben ein „Befriedigend“, 9 Prozent die Note 4, und nur 4 Prozent stufen ihre Ausstattung als „schlecht“ oder „sehr schlecht“ ein.

Am besten schneiden die Großunternehmen ab: Sie bewerten ihre Ausstattung zu fast zwei Dritteln als „gut“ oder „sehr gut“ und nur zu 4 Prozent mit den Noten 4, 5 oder 6.

Je mehr Beschäftigte im Home-Office sind, desto besser fallen die Noten für die Digitalisierung des Unternehmens aus. Fast jede fünfte Firma mit mehr als 50 Prozent der Beschäftigten im Home-Office gibt sich selbst die Bestnote 1, bei Unternehmen, die zum Zeitpunkt der Befragung alle Beschäftigten im Home-Office arbeiten ließen, waren es immerhin noch 15 Prozent. Die beiden schlechtesten Noten wurden hier nur in Einzelfällen vergeben.

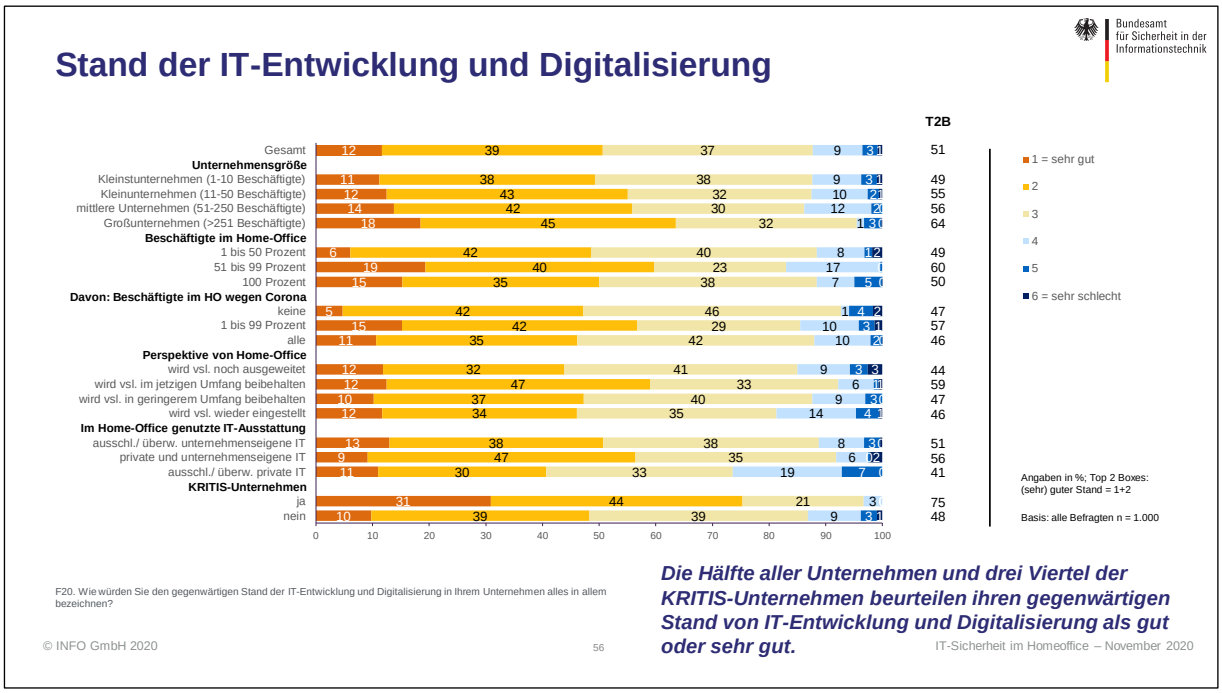

Abbildung 13 - Stand der IT-Entwicklung und Digitalisierung.

7.2. Digitalisierungsprojekte während der Corona-Krise

Ein Drittel der Unternehmen implementierte wegen der Pandemie neue Digitalisierungsprojekte, über die Hälfte davon wurden zeitlich vorgezogen.

Je größer die Firma, desto höher war hier das Engagement: 58 Prozent der Großunternehmen führten Digitalisierungsmaßnahmen durch, bei den mittleren und kleinen Unternehmen waren es 45 Prozent bzw. 41 Prozent. Dagegen gaben nur 31 Prozent der Kleinstunternehmen an, Digitalisierungsprojekte umgesetzt zu haben.

Eine gute Nachricht: **Wer an das Home-Office glaubt, investiert in die Digitalisierung:** Vor allem die Unternehmen, die ihr Home-Office-Angebot ausweiten wollen, haben weit überdurchschnittlich (63 Prozent) Digitalisierungsprojekte beschleunigt oder neu aufgesetzt. Bei denjenigen, die das Angebot nicht erweitern oder sogar verringern oder einstellen wollen, beträgt der Anteil nur 24 Prozent bis 30 Prozent.

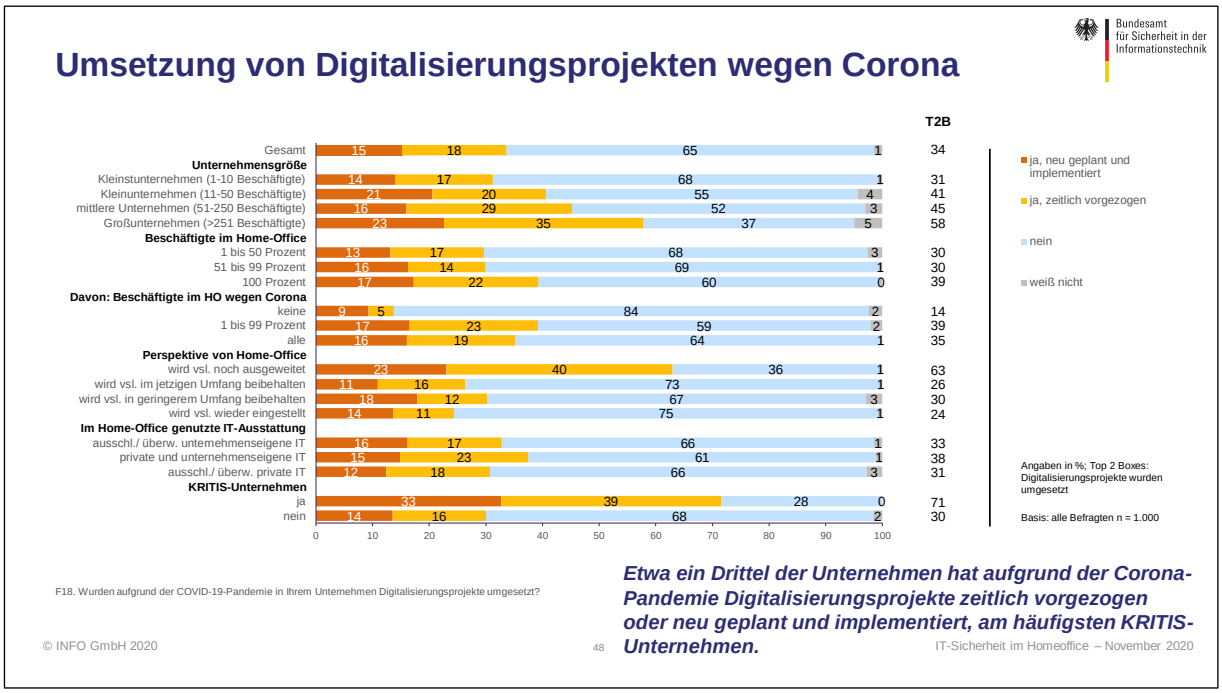

Abbildung 14 - Umsetzung von Digitalisierungsprojekten wegen Corona.

Die Corona-Krise wird von vielen Unternehmen als „Digitalisierungsturbo“ wahrgenommen: aber **auch hier spielt die Größe eine Rolle**: Zwei Drittel Großunternehmen, aber nur ein Drittel der Kleinstunternehmen stimmen dieser Aussage zu. Die kleinen und mittleren Firmen liegen mit 48 Prozent bzw. 46 Prozent Zustimmung dazwischen.

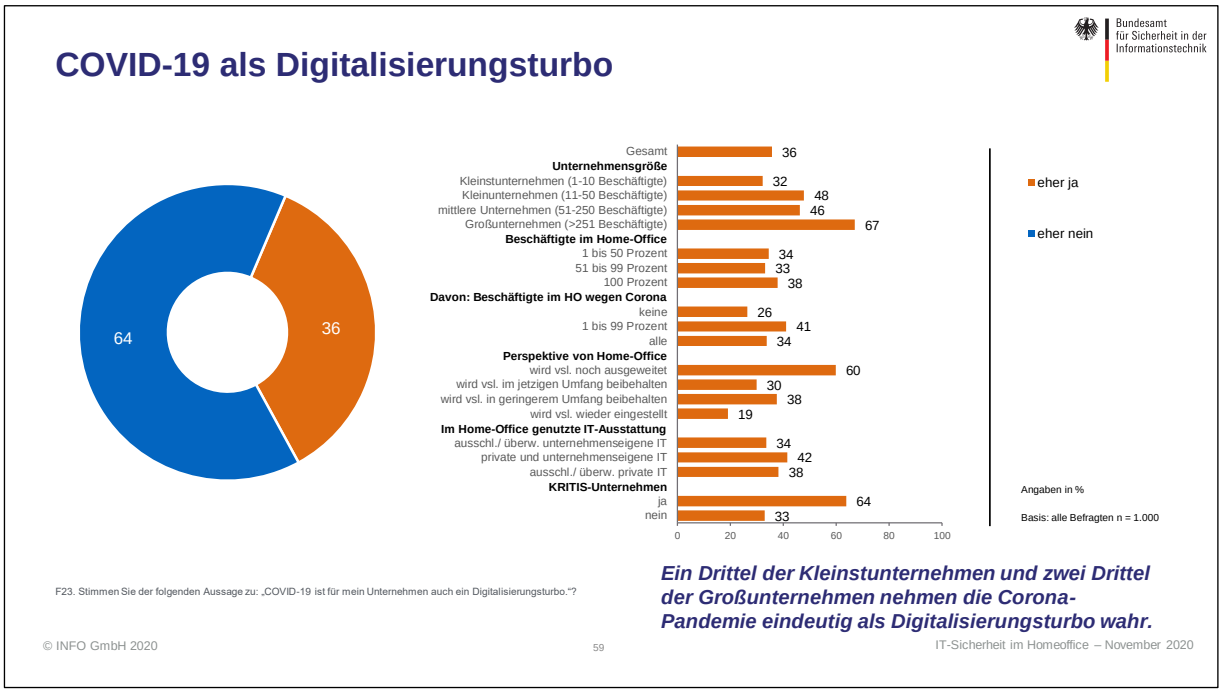

Abbildung 15 - COVID-19 als Digitalisierungsturbo.

7.3. Eingesetzte IT-Lösungen mit Home-Office-Bezug

Während der Corona-Krise ist vor allem die **Nutzung von Video-Konferenzsystemen stark angestiegen**: 38 Prozent der befragten Unternehmen führten diese IT-Lösung neu ein, sodass sich deren Nutzung gegenüber der Vor-Corona-Zeit (43 Prozent) nahezu verdoppelt hat.

Messengerdienste, Remote Desktop-Tools und der Fernzugriff auf Unternehmensressourcen, die von 71 bis 76 Prozent der Unternehmen verwendet werden, waren ganz überwiegend schon vor Beginn der Pandemie implementiert. Dies trifft ebenso auf Cloud-Dienstleistungen, die zwei Drittel aller Unternehmen nutzen, zu.

Den geringsten Einsatz (32 Prozent) finden Kollaborationstools für die dezentrale computergestützte Zusammenarbeit.

An einen Ausbau denken die wenigsten Unternehmen: Nur jeweils unter 10 Prozent planen die Einführung weiterer IT-Lösungen. Am häufigsten genannt wurden die Implementierung von Kollaborationstools (9 Prozent) und externe Clouddienstleistungen (8 Prozent).

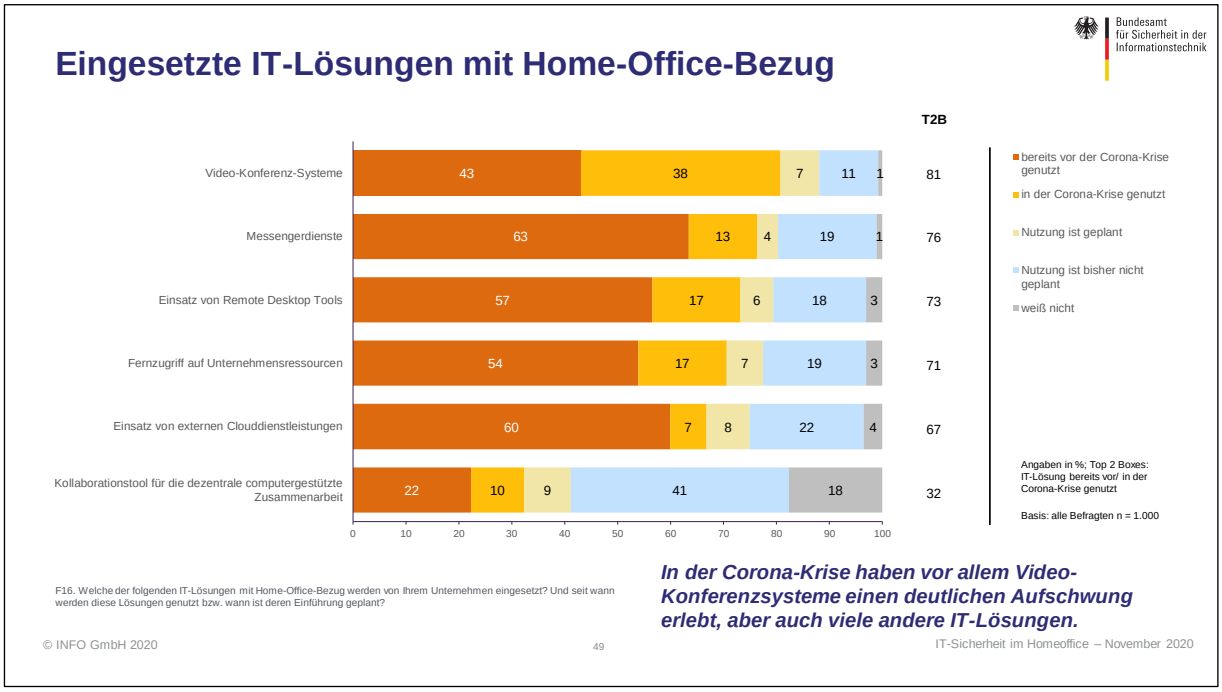

Abbildung 16 - Eingesetzte IT-Lösungen mit Home-Office-Bezug.

7.4. Informationssicherheit im Zuge der Digitalisierung

Bei der Digitalisierung von Geschäftsprozessen denkt nur jedes zweite Unternehmen (51 Prozent) IT-Sicherheit von Anfang an mit. 28 Prozent berücksichtigen dieses Thema erst im Laufe der Implementierung, und jede fünfte Firma beschäftigt sich erst danach damit oder weist ihm eine „untergeordnete Rolle“ zu.

Ob Informationssicherheit von vornherein für alle Prozesse mitgedacht wird, **hängt auch vom Stand der eigenen IT-Entwicklung und Digitalisierung ab**: Neun von zehn Firmen mit sehr guter Ausstattung bejahen das, bei Unternehmen mit guter Ausstattung sind es über zwei Drittel. Ist der Entwicklungsstand hingegen nur „befriedigend“, werden Sicherheitsfragen eher erst während (41 Prozent) als vor (36 Prozent) der Implementierung berücksichtigt. Ist der Entwicklungsstand „schlecht/ sehr schlecht“, beschäftigen sich dagegen nur 6 Prozent schon im Vorfeld damit und knapp zwei Drittel erst danach oder gar nicht.

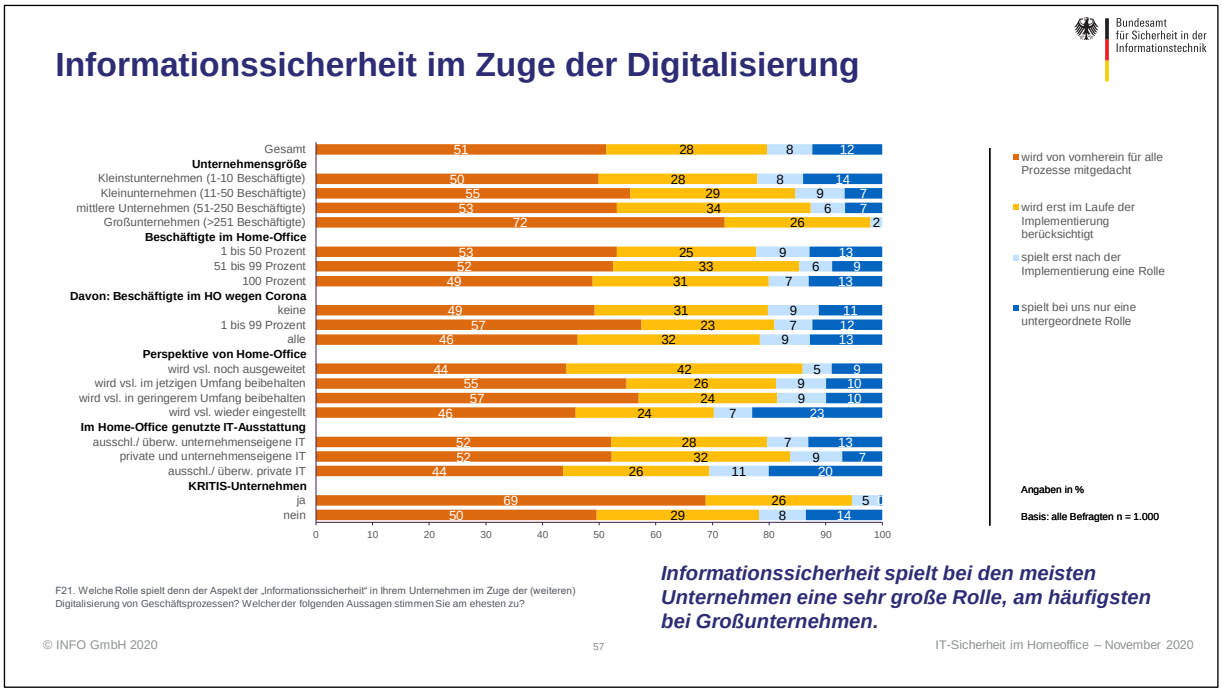

Abbildung 17 - Informationssicherheit im Zuge der Digitalisierung.

7.5. Bedeutung von IT-Lösungen aus Deutschland oder der EU

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

Besonders wichtig ist das für Großunternehmen und Unternehmen mit einem hohen Home-Office-Anteil. Von ihnen äußern jeweils rund drei Viertel den Wunsch nach deutschen bzw. europäischen IT-Lösungen.

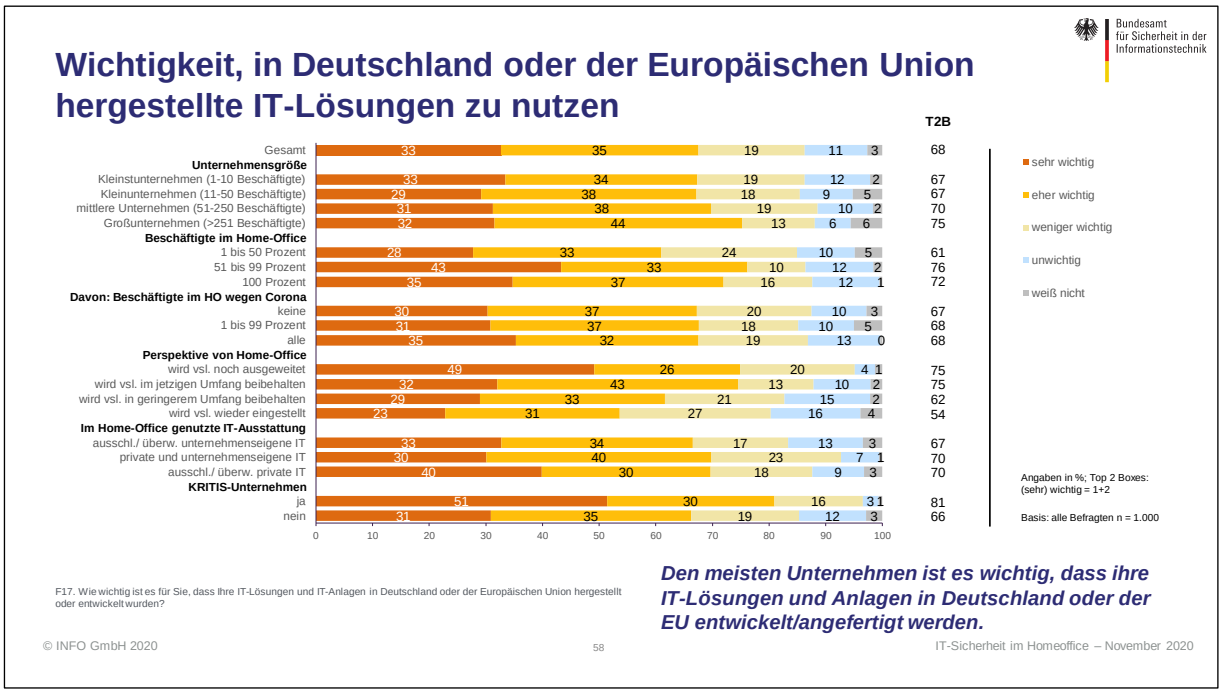

Abbildung 18 - Wichtigkeit, in Deutschland oder der Europäischen Union hergestellte IT-Lösungen zu nutzen.

8. Überblick Statistik

Befragt wurden in dieser Untersuchung überwiegend Klein- (15 Prozent) und Kleinstunternehmen (80 Prozent), 4 Prozent sind mittlere Unternehmen und 2 Prozent Großunternehmen.

Zwei Drittel der befragten Unternehmen gehören der Dienstleistungsbranche an, 18 Prozent sind in der Produktion tätig und 15 Prozent im Handel.

Die befragten Personen sind etwa zur Hälfte Geschäftsführer/in, Inhaber/in oder Vorstand ihres Unternehmens, 28 Prozent arbeiten im IT- und Datenschutzbereich, 42 Prozent sind Personalverantwortliche oder leitende Angestellte.

Ihre Informiertheit über IT-Sicherheit schätzen etwa 80 Prozent Befragten als „eher gut“ oder „sehr gut“ ein, jede/r Fünfte als schlecht.

Besser sieht es bei der technischen Ausstattung aus: Über sie fühlen sich fast alle gut informiert, nur 8 Prozent geben an, sich kaum auszukennen.

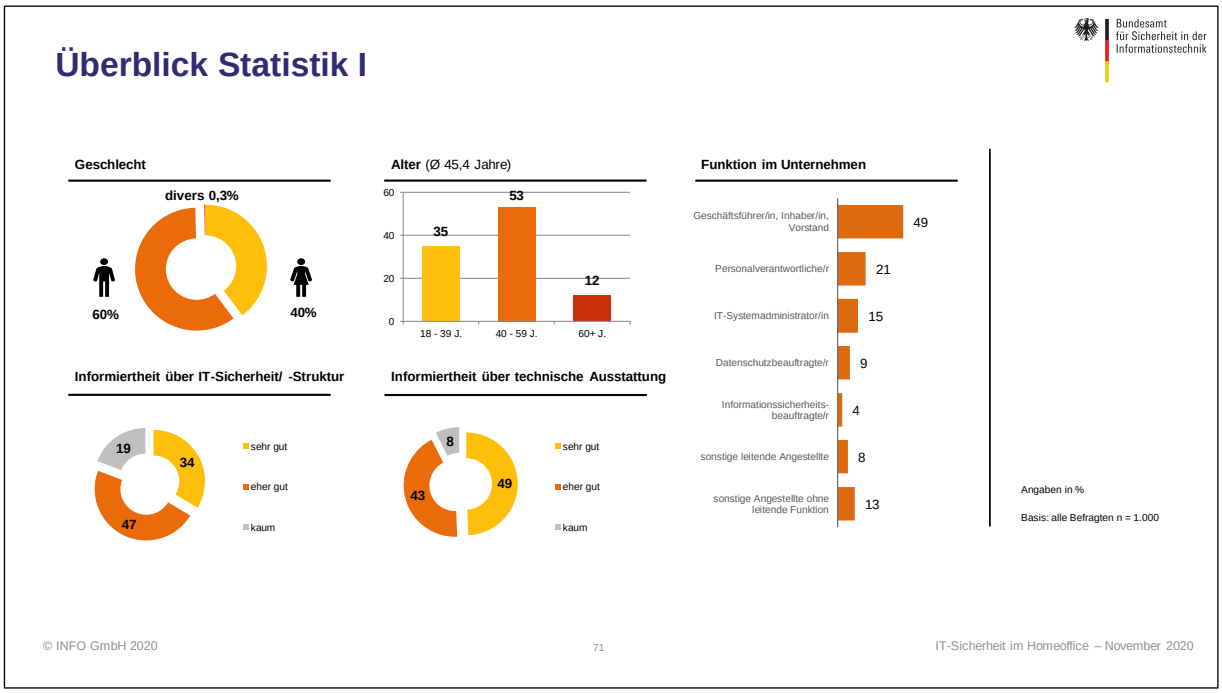

Abbildung 19 - Überblick Statistik I.

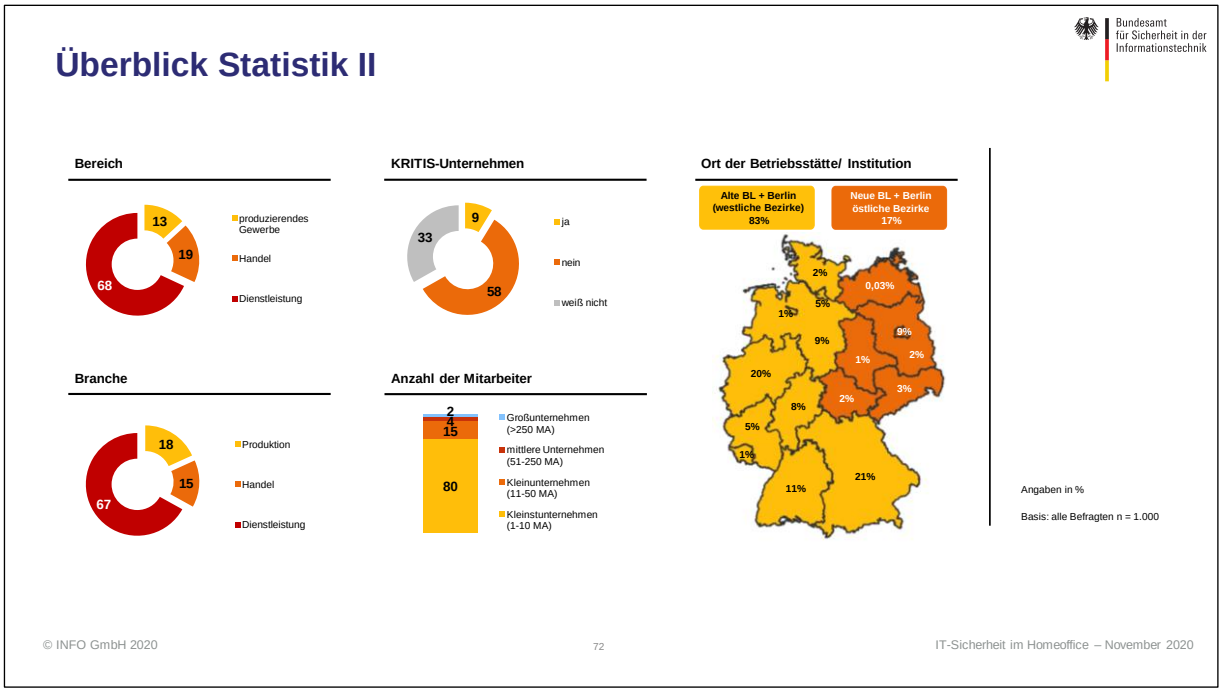

Abbildung 20 - Überblick Statistik II.