DsiN-Praxisreport 2021/22
Mittelstand@IT-Sicherheit

DsiN-Schirmherrschaft:

Bundesministerium des Innern und für Heimat

Studien-Schirmherrschaft:

Bundesministerium für Wirtschaft und Klimaschutz

Eine Studie von:

DsiN Deutschland sicher im Netz

sicher-im-netz.de

Starke Partner für eine sichere Digitalisierung

Michael Kellner

Der Mittelstand ist das Rückgrat unserer Wirtschaft. Er steht für Wachstum, Beschäftigung und Innovation. Die Coronapandemie hat uns alle vor große Herausforderungen gestellt. Viele Mittelständler:innen haben sich dabei digitaler und innovativer aufgestellt. Nun sehen sich kleine und mittlere Unternehmen und Handwerksbetriebe mit neuen Herausforderungen konfrontiert: Materialengpässe durch stockende Lieferketten, einen durch die Pandemie verschärften Fachkräftemangel und steigende Energiepreise. Digitale Technologien wie Künstliche Intelligenz oder Blockchain können helfen, Materialbeschaffung zu optimieren, Fachkräfte aus- und weiterzubilden oder die Energieeffizienz zu erhöhen und damit aktuelle Herausforderungen zu bewältigen.

Die zunehmende Digitalisierung von Wirtschaft und Gesellschaft bedeutet auch, dass Cyberkriminelle auf eine größere Angriffsfläche treffen, die es zu schützen gilt. Sie versuchen verstärkt, Unternehmen mit sogenannter Ransomware zu Lösegeldzahlungen zu erpressen. Häufig greifen sie Lieferketten mit Supply-Chain-Attacken an, in deren Fokus mittelständische Zuliefernde stehen. Große Verluste durch Produktionsausfälle, der Verlust sensibler Daten oder Reputationsschäden können auch im Mittelstand die Folgen sein.

Dieser Praxisreport zeigt: Das Bewusstsein für Cybersicherheit steigt, doch noch immer gibt es zu viele kleine und mittlere Unternehmen, die sich nicht ausreichend vor Cyberrisiken schützen. Hackerangriffe werden häufig nicht ausreichend erkannt; auch wissen zu viele Mittelständler:innen noch nicht um ihre Schwachstellen.

Für eine sichere, nachhaltige und erfolgreiche Digitalisierung brauchen Mittelständler:innen starke Partner. Mit der vom Bundesministerium für Wirtschaft und Klimaschutz geförderten Transferstelle IT-Sicherheit im Mittelstand unterstützen Deutschland sicher im Netz e. V., der DIHK, die Hochschule Mannheim sowie die Fraunhofer-Institute FOKUS und IAO Handwerksbetriebe KMU mit praktischen Angeboten, um die Cybersicherheit im Mittelstand zu erhöhen.

Ergreifen Sie die Chancen der Digitalisierung und schützen Sie sich vor ihren Risiken!

Michael Kellner
Parlamentarischer Staatssekretär beim
Bundesminister für Wirtschaft und Klimaschutz

IT-Sicherheit im Netzwerk – machen Sie mit!

Dr. Michael Littger

Susanne Diehm

Der diesjährige DsiN-Praxisreport 2022 ist die siebte Erhebung zur Sicherheitslage in kleinen und mittleren Betrieben mit einem Fokus auf den veränderten Herausforderungen durch die Coronapandemie. Die Ergebnisse zeigen: Es besteht erheblicher Nachholbedarf für mehr IT-Sicherheit auf allen Ebenen. Die digitalen Angriffsflächen haben in Folge der Pandemie zugenommen, durch Homeoffice und Video-Meetings, zusätzliches Dokumentensharing, Cloud-Computing sowie virtuelle Produktionsprozesse. Damit entstanden zusätzliche Einfallstore für Cyberattacken. Zugleich stiegen die Aktivitäten der Angreifer; Angriffsmethoden sind vielfältiger geworden.

Insgesamt sind die Anforderungen zur Absicherung von Unternehmen merklich gewachsen. Praxisnahe Ansätze gewinnen an Bedeutung, die die Sicherheit ganzheitlich betrachten, also unter technischen, regulativen und verhaltensbedingten Vorkehrungen. Die Realität im Jahr 2022 hinkt diesen Anforderungen in den meisten Betrieben hinterher: Die Engagements für IT-Sicherheit steigen zu langsam, relevante Aktionsfelder wie die Risikoermittlung sind gar rückläufig. Dies ist bemerkenswert, da das Risikobewusstsein vieler Unternehmen durchaus gestiegen ist.

Es gibt aber auch hoffnungsvolle Signale in dieser IT-Sicherheitslage. So erleben wir im täglichen Umgang mit Betrieben und Unternehmern ein wachsendes Interesse nach wirksamer IT-Sicherheit. Vielfach erscheint der mangelnde Zugang zu Angeboten und Lösungen als Hürde. Für die Zukunft ist daher entscheidend, IT-Sicherheit weiter zu vereinfachen und Einstiegshürden zu senken. Diesen Ansatz verfolgen die 75 regionalen Standorte von TISiM, der Transferstelle IT-Sicherheit im Mittelstand. In der Kombination von regionalen Partnern und zentralen Hilfestellungen wie dem Sec-O-Mat werden Unternehmen Maßnahmen aufgezeigt, die passgenau und einfach sind. Im Rahmen eines aufsuchenden Ansatzes erscheint dieser als wirkungsvoller Baustein einer zukunftsfähigen Architektur für Cybersicherheit.

Schon heute laden wir Sie ein: Werden Sie Teil des bundesweiten Netzwerks von TISiM oder weiterer IT-Sicherheitsinitiativen von DsiN, ob als Unternehmen, als Trainer:in, regionaler Netzwerk- und Kompetenzpartner oder als IT-Dienstleistende. Mehr IT-Sicherheit kann ganz einfach sein.

Wir wünschen viel Freude bei der Lektüre!

Dr. Michael Littger
DsiN-Geschäftsführer

Susanne Diehm
Mitglied des SAP Management Teams für Mittel- und Osteuropa

DsiN-Praxisreport – Methodik und Zielsetzung

Datengrundlage für den Praxisreport 2022 ist die Erhebung des „DsiN-Sicherheitscheck“[1] unter Mitarbeitenden und Führungskräften aus dem Mittelstand. Befragungen aus 24 Themenfeldern werden im regelmäßigen Rhythmus ausgewertet. In diesem Jahr wurden insgesamt 1.339 vollständig beantwortete Fragebögen in einem verlängerten Befragungszeitraum der Coronabeschränkungen von Mai 2020 bis Januar 2022 berücksichtigt.

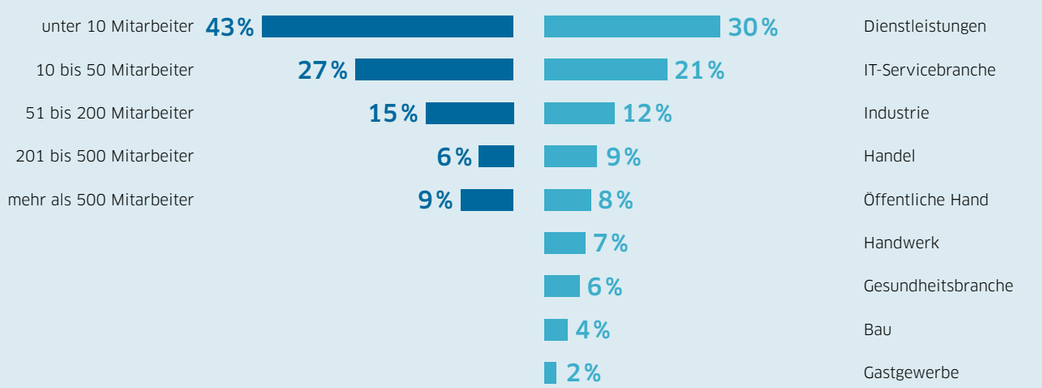
43 Prozent der Befragten im aktuellen Erhebungszeitraum kommen aus Kleinstunternehmen mit weniger als zehn Beschäftigten. Der Anteil an Unternehmen mit zehn bis 50 Beschäftigten betrug 27 Prozent. 15 Prozent der Befragten sind Unternehmen mit 51 bis 200 Beschäftigten zuzuordnen, 6 Prozent zu Unternehmen mit 201 bis 500 Beschäftigten. Die Gruppe der Unternehmen über 51 Beschäftigten ist damit etwas geringer als im Vorjahr. Rund 9 Prozent der Befragten stammen aus Unternehmen mit mehr als 500 Beschäftigten.

Der Praxisreport repräsentiert einen Mix an Branchen. Knapp ein Drittel aller befragten Unternehmen kommt aus dem Bereich Dienstleistung (30 Prozent). Wie auch im Vorjahr lag der Anteil der IT-Unternehmen bei 21 Prozent, gefolgt von Industrie (12 Prozent) und Handel (9 Prozent) mit zusammen ebenfalls 21 Prozent. Weitere 7 Prozent repräsentieren das Handwerk, fast gleichauf mit der Gesundheitsbranche (6 Prozent) und der öffentlichen Hand mit 8 Prozent. Aus dem Gastgewerbe stammen 2 Prozent der Befragten.

Hinweis: Bedingt durch ein festgesetztes Rundungsverfahren kann die Summe der Verteilungswerte in den Abbildungen von 100 Prozent abweichen.

Abb. 1 / DsiN-Praxisreport

Aufteilung der befragten Unternehmen nach Größe und Branche



1 Abrufbar unter www.dsin-sicherheitscheck.de.

Inhalt

Fazit: IT-Sicherheit durch vereinfachten Zugang

Infolge der COVID-19-Pandemie kamen in mittelständischen und kleinen Unternehmen (KMU) vielfältigere digitale Anwendungen zum Einsatz, die zudem häufiger genutzt wurden. Die Abhängigkeit von IT-Sicherheit sowie auch die Verwundbarkeit durch IT-Risiken ist in der Folge gewachsen. Zwar erkennen Unternehmen die Relevanz der IT-Sicherheit öfters an, die Nachholbedarfe zur Einführung von IT-Strategien und -Maßnahmen sind jedoch unverändert hoch. Grundlegende Themenfelder wie Risikoermittlung, Schulung von Mitarbeitenden, Prävention von Cyberangriffen sowie die Absicherung der internen und externen Kommunikation wurden während der Coronapandemie vernachlässigt.

Eine Mehrheit der Befragten von 86 Prozent gibt an, dass die ungestörte Arbeit des Betriebs (Integrität) unmittelbar von einer sicheren IT abhängt. Jeder zweite Betrieb befürchtet, dass die eigene unternehmerische Existenz bedroht sei, wenn beispielsweise Daten verloren gingen oder an die Konkurrenz gelängen. Interessant: je kleiner ein Unternehmen, desto häufiger die Befürchtung von Schäden. Zwar ist das Bewusstsein für IT-Sicherheit inzwischen auch bei Mitarbeitenden und Führungskräften weitverbreitet – es mangelt jedoch an der konsequenten Einführung von Maßnahmen.

→ Trotz der gewachsenen Relevanz von mobilem Arbeiten in der Pandemie sieht nur knapp ein Drittel (30 Prozent) der Unternehmen eine klare Trennung der geschäftlichen und privaten Nutzung vor. Eine Mehrheit der Unternehmen erlaubt die Privatnutzung der geschäftlichen IT-Systeme sogar explizit. Nur jedes fünfte Unternehmen hat Richtlinien erlassen.

Eine Herausforderung bei IT-Sicherheitsmaßnahmen in Betrieben ist oftmals, dass die ergriffenen Maßnahmen realen Sicherheitsgefahren nicht standhalten (70 Prozent). So geben rund zwei von drei Betrieben (65 Prozent) an, dass sie ihre Mitarbeitenden regelmäßig trainieren oder Angriffsszenarien simulieren. Aber nur eine Minderheit setzt dabei auf anerkannte Standards. Auch werden Maßnahmen der IT-Sicherheit nur in der Ausnahme auf ihre Wirksamkeit überprüft. Der Anteil der Unternehmen, die ohne jede Vorkehrung gegen IT-Schwachstellen ihr Geschäft betreiben, ist leicht auf 17 Prozent gestiegen.

Insgesamt ergibt das Lagebild zur IT-Sicherheit in der Praxis ein Defizit bei KMU, auf die eher wachsenden Risiken der Digitalisierung mit wirkungsvollen Schutzmaßnahmen zu reagieren. Bei standardisierten IT-Diensten herrscht ein weitgehendes Vertrauen in die mitgelieferten Schutzvorkehrungen. Auch bei Betriebsprozessen und sonstigen Kommunikationsdiensten wird auf gesonderte Vorkehrungen verzichtet – obwohl Störungen auf dieser Betriebsebene laut der Befragungen das eigene Fortbestehen bedrohen könnten. Hier können Hilfestellungen unterstützen, die die vielfältigen Bedarfe der IT-Sicherheit aufgreifen und passgenaue Ansätze und Maßnahmen vermitteln.

KAPITEL 1

IT-Sicherheitsbedarfe steigen, Vorkehrungen stagnieren

Trotz einer gewachsenen Digitalisierung in Unternehmen in der Pandemie fällt auf, dass die tatsächlichen Schutzvorkehrungen den gestiegenen IT-Sicherheitsbedürfnissen nicht nachkommen. Der Umgang mit dem Risiko von Cyberangriffen und weiteren IT-Sicherheitsrisiken ist dabei stark von der Größe und Branche eines Unternehmens abhängig. Meistens sind kleine Betriebe im Bereich Dienstleistung, IT und Industrie von erfolgreichen Angriffen betroffen.

Verletzbarkeit durch IT-Sicherheit bei 86 Prozent der KMU

Die meisten Befragten betrachten ihr Unternehmen als abhängig von der IT-Sicherheit (86 Prozent): Ein Drittel der Befragten (37 Prozent) gibt an, dass IT-Sicherheit für ihr Unternehmen wichtig sei, für jedes zweite Unternehmen (49 Prozent) ist sie sogar existenziell. Diese Werte sind in der Pandemie weitgehend stabil geblieben.

Je größer das Unternehmen ist, desto geringer wird die Abhängigkeit und Verletzbarkeit des eigenen Unternehmens durch IT-Sicherheit empfunden: Ab 50 Mitarbeitenden sinkt die gefühlte Abhängigkeit auf nur noch 8 bis 18 Prozent (s. Abb. 3). Dem könnte zugrunde liegen, dass größere Unternehmen über stärkere Resilienzen verfügen, während sich IT-Störungen bei kleineren Unternehmen unmittelbarer auf das Geschäftshandeln auswirken.

→ Größere Unternehmen verfügen über stärkere Resilienzen.

Im Jahr der Pandemie ist insbesondere in der Dienstleistungsbranche das Bewusstsein der Verletzbarkeit durch IT gestiegen (s. Abb. 4). Sie steht nun an der Spitze, gefolgt von der IT-Servicebranche und der Industrie. Diese Entwicklung korreliert mit den gewachsenen Online-Aktivitäten der Dienstleistungsbranche in der Pandemie. Wie auch in den Vorjahren weisen Handwerk, Bau und Gastgewerbe vergleichsweise geringe Werte auf. Auch die Gesundheitsbranche ist 2022 nicht mehr unter den ersten 3 Plätzen mit den größten Abhängigkeiten vertreten (s. Abb. 3).

→ Industrie an 3. Stelle der verletzbaren Branchen durch IT.

32 Prozent halten Vertraulichkeit der IT für „existenziell“

Jedes dritte Unternehmen (32 Prozent) gibt an, dass mangelnde Vertraulichkeit grundlegende Risiken im Geschäft begründen würden (s. Abb. 5, S. 10). Ein Drittel dieser Unternehmen (11 Prozent) sieht darin sogar die eigene Existenz bedroht, 21 Prozent befürchten Wettbewerbsbeeinträchtigung, im Vergleich zur Zeit vor der Coronapandemie eine Zunahme von 3 Prozentpunkten.

Zwei von drei Unternehmen sehen in der IT-Vertraulichkeit keine Relevanz für ihre Wettbewerbsfähigkeit oder den Bestand des Unternehmens (67 Prozent). Dieser Wert überrascht, da integren Informationsbeständen heute vielfältige Bedeutung zukommt – vom geordneten Betriebsablauf über vertrauliche Listen der Mitarbeitenden bis zu Details über Partnerschaften und Prozessabläufe. Das Bewusstsein der Schutzbedürftigkeit könnte hier vielfach noch auf die sensiblen Bereiche eines Unternehmens beschränkt sein. Die grundlegende Bedeutung und Vulnerabilität von Informationen bedürfte danach zusätzlicher Aufmerksamkeit.

42 Prozent der KMU verzeichnen Cyberangriffe

Zwei von fünf Unternehmen waren in den vergangenen Monaten von sicherheitsrelevanten Vorfällen betroffen (42 Prozent), 5 Prozent aller Betriebe haben sogar permanent mit Angriffen zu kämpfen. Demgegenüber waren 58 Prozent der Unternehmen nach eigenen Angaben von keinen Cyberangriffen betroffen. Die Zahl der betroffenen Unternehmen hat sich danach um vier Prozentpunkte reduziert. Hier ist zu beachten, dass Cyberangriffe vielfach unentdeckt bleiben können, sodass der Umfang der tatsächlich Betroffenen höher ausfallen dürfte (s. Abb. 6, S. 10).

Fast jedes fünfte KMU meldet erhebliche Schadensfolge

Nicht jeder Cyberangriff muss auch zu Schäden oder anderen negativen Auswirkungen führen. Insbesondere bei frühzeitiger Erkennung oder wirksamer Abwehr

Abb. 2 / DsiN-Praxisreport

Inwiefern hängt der Erfolg Ihres Unternehmens von der IT-Sicherheit ab, also der Integrität, Vertraulichkeit oder Verfügbarkeit von Informationen?

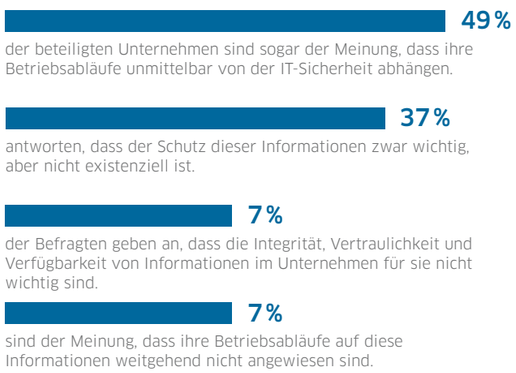


Abb. 3 / DsiN-Praxisreport

Sehen Sie einen direkten Zusammenhang zwischen wirtschaftlichem Wohlergehen und IT-Sicherheit?

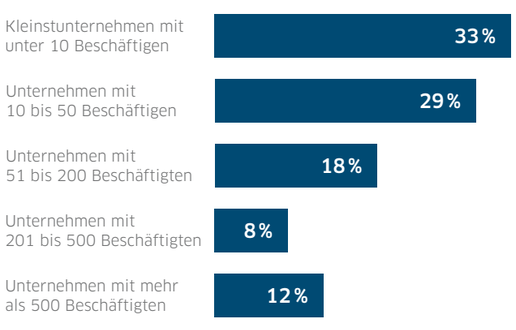


Abb. 4 / DsiN-Praxisreport

Wenn Sie einen direkten Zusammenhang der IT-Sicherheit auf das wirtschaftliche Wohlergehen sehen, welcher Branche gehören Sie an?

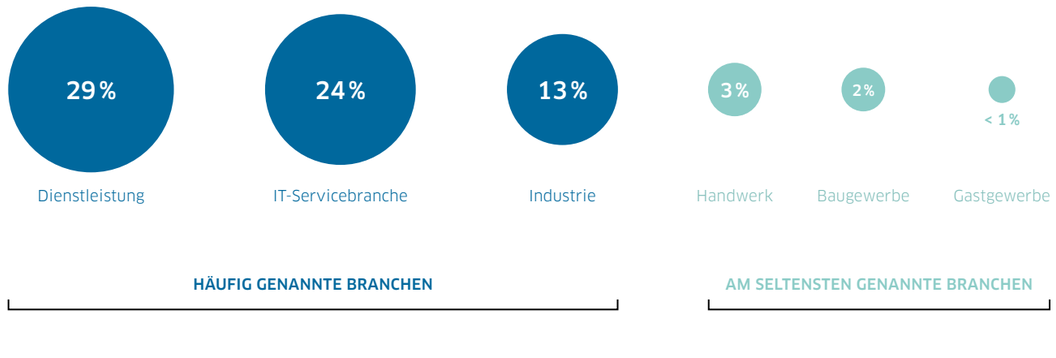


Abb. 5 / DsiN-Praxisreport

Wie schätzen Sie die Gefährdung der Vertraulichkeit und Integrität ihrer IT-gestützten Informationen durch Angriffe anderer Unternehmen ein?

35 %
geben an, dass ihre Informationen nur geringen Wert für die Konkurrenz haben.

32 %
sind der Ansicht, dass das Interesse der Konkurrenz im Ausland nicht kritisch einzuschätzen ist.

21 %
finden, dass ihre Wettbewerbsfähigkeit von der Vertraulichkeit gegenüber dem Interesse der Konkurrenz, der organisierten Kriminalität oder ausländischen Nachrichtendiensten abhängt.

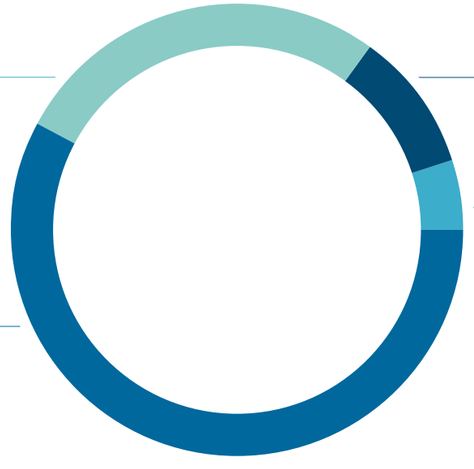
11 %
Für 11 Prozent hängt das Fortbestehen des Unternehmens unmittelbar von der Vertraulichkeit ihrer Informationen ab.

können Angriffe folgenlos bleiben. Wir haben daher nach den Auswirkungen der Angriffe auf das Unternehmen gefragt (s. Abb. 7).

Mehr als drei von vier Unternehmen geben an, durch Cyberangriffe zusätzliche Aufwände oder Schäden erlitten zu haben (76 Prozent). Davon erlebten fast 13 Prozent der Unternehmen Angriffe mit erheblichen, aber nicht existenzgefährdenden Schäden. Dieser Wert ist in der Coronazeit um 3 Prozentpunkte – oder prozentual um 30 Prozent – gegenüber dem Vorjahr gestiegen. Fast jeder zwanzigste Angriff (4 Prozent) hatte sogar schwere Belastungen zur Folge. Hierin nicht enthalten sind sogenannte weiche Schäden wie Reputationsverluste und Beeinträchtigung von Vertrauen, die oftmals schwer messbar sind, mittelfristig jedoch die Bindung

Abb. 6 / DsiN-Praxisreport

Waren die befragten Unternehmen in der Vergangenheit schon einmal von einem IT-Angriff betroffen?



27 %
hatten in den vergangenen Jahren einige Probleme durch Schadsoftware.

10 %
waren in den letzten Jahren ein oder mehrmals Opfer eines gezielten Angriffs.

5 %
Knapp 5 Prozent haben ständig mit Angriffen auf ihr Unternehmen zu kämpfen.

58 %
geben an, noch nie von einem Angriff betroffen gewesen zu sein.

von Kundschaft, Lieferfirmen und sonstigen Partnern spürbar beeinträchtigen können.

Ein Blick auf die Sicherheitslage in den unterschiedlichen Branchen zeigt Unterschiede in den Schadensneigungen. Im Gastgewerbe trifft jeder zweite erfolgreiche Angriff die Branche erheblich oder existenzbedrohend. Im Handel verursacht noch jeder fünfte Angriff denselben Schaden. In der Industrie und der Gesundheitsbranche ist dies im Vergleich nur rund jeder zehnte Angriff.

Zwei Drittel der KMU verzichten auf Risikoermittlung

Eine Voraussetzung für wirksame Schutzvorkehrungen im Unternehmen sind Kenntnisse der eigenen Bedrohungs- und Angriffslage. Die Wahrscheinlichkeit

Abb. 7 / DsiN-Praxisreport

Wie folgenreich waren die aus Angriffen resultierenden Schäden?

24 %
geben an, keinerlei Konsequenzen durch einen Angriff gehabt zu haben.

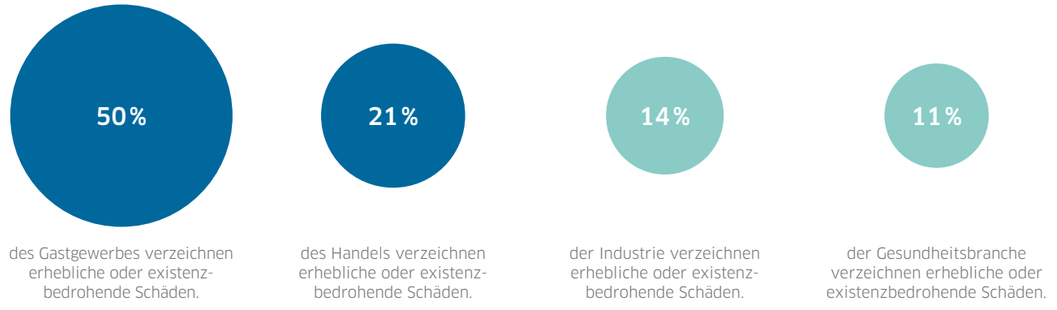
59 %
antworten, zwar einigen Aufwand, aber keine nachhaltigen Schäden davongetragen zu haben.

13 %
schätzen den Aufwand zur Behebung der angriffsverursachten Schäden als erheblich, aber nicht existenzbedrohend ein.

4 %
der Unternehmen werten die Folgen eines Angriffs als eine schwere Belastung.

Abb. 8 / DsiN-Praxisreport

Ranking nach Branche – Anteil erheblicher oder existenzbedrohender Vorfälle



50 % des Gastgewerbes verzeichnen erhebliche oder existenzbedrohende Schäden.

21 % des Handels verzeichnen erhebliche oder existenzbedrohende Schäden.

14 % der Industrie verzeichnen erhebliche oder existenzbedrohende Schäden.

11 % der Gesundheitsbranche verzeichnen erhebliche oder existenzbedrohende Schäden.

MIT ZUNAHME

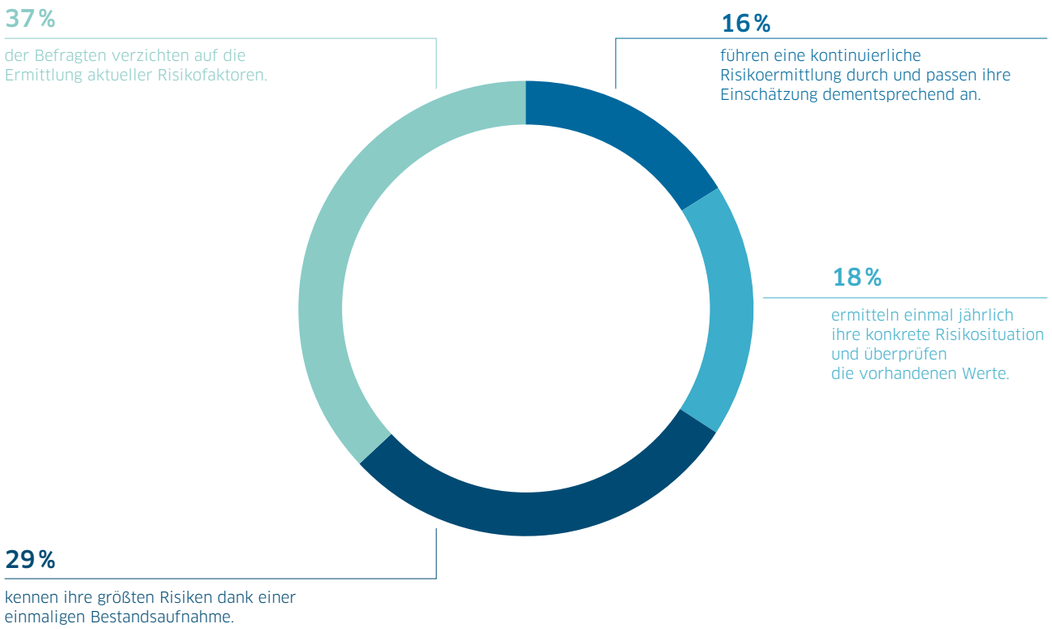
MIT ABNAHME

eines folgenreichen Angriffs kann durch die Identifikation der Schwachstellen erheblich reduziert werden. Darüber hinaus können schützenswerte Bereiche besonders gesichert werden. Eine Ermittlung des eigenen Risikoprofils sollte daher in keinem Unternehmen fehlen.

Im Vergleich zum Vorjahr ist das Niveau der Risikoermittlung nahezu unverändert – und damit weiterhin nicht zufriedenstellend: Zwei von drei Unternehmen (66 Prozent) begnügen sich mit einer einmaligen Bestandsaufnahme (29 Prozent) oder verzichten komplett auf eine Risikoermittlung (37 Prozent). 18 Prozent der Befragten führen jährliche Risikoermittlungen durch und nur 16 Prozentpunkte betreiben eine kontinuierliche Risikoermittlung. Damit besteht auf diesem Feld insgesamt ein hoher Nachholbedarf in Deutschland.

Abb. 9 / DsiN-Praxisreport

Wann werden Risikosituationen von Unternehmen ermittelt?



FAZIT

Handlungsdefizit bei IT-Sicherheit wächst in der Krise

Die Ergebnisse zeigen einen umfänglichen Bedarf an zusätzlichen Schutzmaßnahmen, der durch die Coronapandemie noch größer ausfällt. Obwohl sich die meisten Vorkehrungen mit überschaubarem Aufwand durchführen ließen, findet das Feld der Risikoermittlung weiterhin zu wenig Beachtung. Ein weiteres Bedarfsfeld ist der mangelnde Schutz von Unternehmensinformationen. Hier bedarf es zusätzlicher Aufmerksamkeit über den Wert von digitalen Informationen, die über den Schutz eigentlicher Betriebsgeheimnisse hinausgehen und heute die Integrität ganzer Betriebsprozesse und -einrichtungen umfassen.

Erfreulich erscheint, dass trotz dieser Defizite die Zahl der wahrgenommenen Cyberangriffe nicht wesentlich gestiegen ist. Gleichwohl sind die Fälle mit schweren, auch existenzgefährdenden Folgen von 10 auf 13 Prozent angestiegen (+30 Prozent).

Tipps und Angebote für die Praxis

- **TISiM** bietet seit Januar 2021 passgenaue Informationen aus einer Hand. Sie bündelt, bereitet praxisnah auf und vermittelt Angebote zum Thema IT-Sicherheit. Darüber hinaus unterstützt sie kleine und mittlere Unternehmen, Handwerksbetriebe und Selbstständige bei der Umsetzung.
  tisim.de

- **Mittelstand-Digital** informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Mittelstand-Digital-Zentren helfen mit Expert:innenwissen, Demonstrationszentren, Netzwerken zum Erfahrungsaustausch und praktischen Beispielen.
  mittelstand-digital.de

- **DSGVO-Quick-Check** bietet Ihnen in zehn Minuten eine Bestandsaufnahme Ihres Unternehmens zu daten- und sicherheitsrelevanten Fragestellungen. Sie erhalten als Ergebnis eine Matrix, welche die Risikosituation in Ihrem Unternehmen darstellt.
  vds-quick-check.de

KAPITEL 2

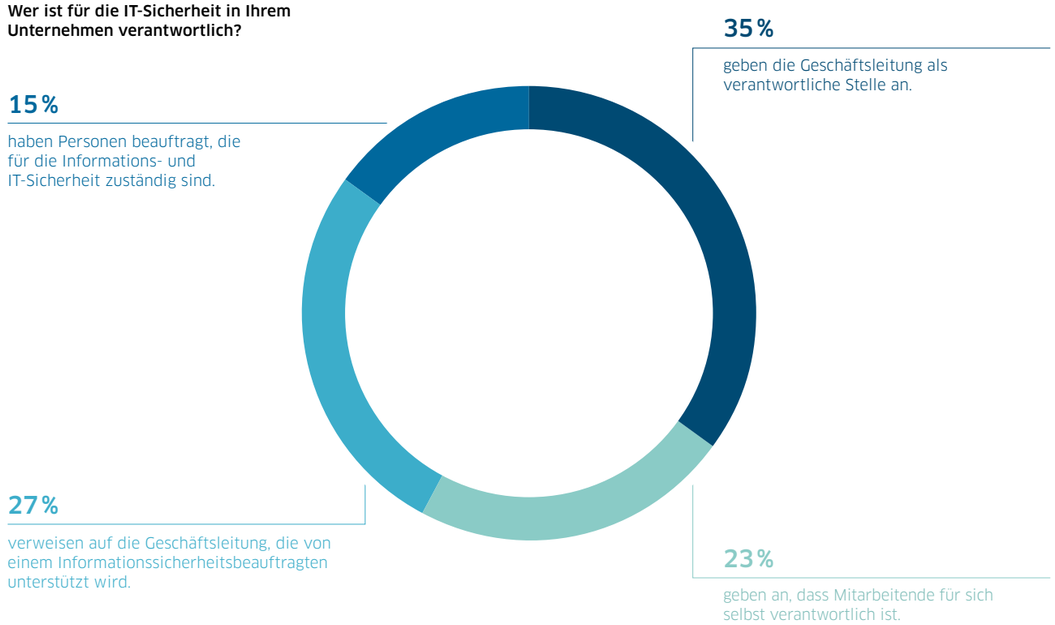
Aufholbedarfe bei IT-Sicherheitskultur in KMU

Die Digitalisierung der Geschäftsprozesse führt zu mehr Angriffsfläche für Cyberattacken. Es geht um digitale Vernetzung aller Betriebsabläufe und Produktionsprozesse. Die Wettbewerbsfähigkeit des deutschen Mittelstands ist in zunehmendem Maße von einer geschützten Informations- und Kommunikationstechnik abhängig. Diese erhöht die Abhängigkeit von einer sicheren IT als Voraussetzung für wirtschaftliches Wohlergehen.

IT-Sicherheit durch Verantwortlichkeiten

Abb. 10 / DsiN-Praxisreport

Wer ist für die IT-Sicherheit in Ihrem Unternehmen verantwortlich?



Die diesjährigen Daten deuten auf eine wachsende Verantwortungsbereitschaft der Führungsebene oder Geschäftsleitungen im Umgang mit IT-Sicherheitsthemen hin. So lassen sich Führungskräfte durch IT-Sicherheitsbeauftragte unterstützen. Diese begleiten bei strategischen und operativen Fragestellungen zur IT-Sicherheit oder sind auch Ansprechperson für sonstige Mitarbeitende.

Steigende Unterstützung durch IT-Sicherheitsbeauftragte

Wie begegnen Mitarbeitende und Geschäftsführungen potenziellen Cyberangriffen und wer ist in den Unternehmen für IT-Sicherheit verantwortlich? Die Zahlen untermauern, dass die Verantwortlichkeiten für IT-Sicherheit mit 35 Prozent weiterhin vorrangig bei der Geschäftsleitung verortet werden. Erfreulich erscheint, dass bei weiteren 27 Prozent ausdrücklich eine IT-Sicherheitsexpertise in die Verantwortung mit eingebunden ist. 15 Prozent der Unternehmen verorten die Verantwortung dagegen ausschließlich auf Sicherheitsbeauftragte.

Aber leider gilt auch, dass immer noch fast jedes vierte Unternehmen (23 Prozent) seine Mitarbeitenden beim Thema IT-Sicherheit auf sich allein stellt. Ein Blick auf die Unternehmensgröße zeigt zudem: je kleiner das Unternehmen, desto häufiger müssen Mitarbeitende bei dem Thema selbst entscheiden.

Auch die Verortung des Themas IT-Sicherheit auf die Geschäftsführung ist von der Unternehmensgröße abhängig: je kleiner das Unternehmen, desto häufiger ist die Leitung selbst für das Thema unmittelbar zuständig. Daraus lässt sich ableiten, dass die Ansprache zu Awareness-Trainings bei dieser Unternehmensgröße auf Leitungsebene priorisiert werden muss, um nachhaltige Effekte zu bewirken.

Abb. 11 / DsiN-Praxisreport

Wie hoch ist der Anteil der Beschäftigten, die unmittelbar für IT-Sicherheit zuständig sind?

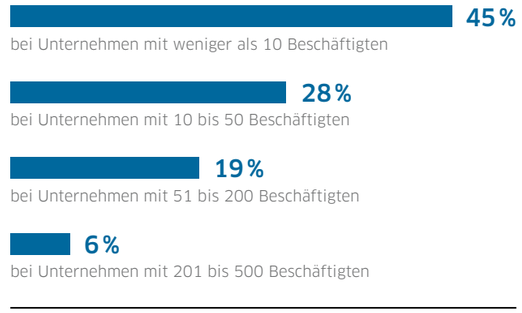
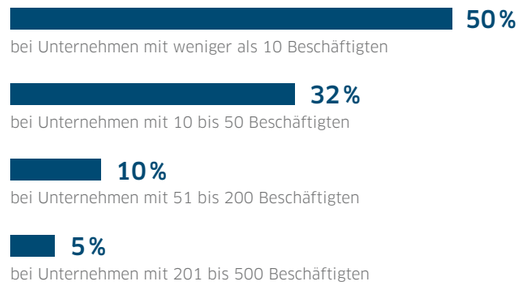


Abb. 12 / DsiN-Praxisreport

Wo ist die Geschäftsleitung unmittelbar für IT-Sicherheit zuständig?



Umgang mit IT-Vorfällen: Der Chef entscheidet

Im akuten Falle eines Angriffs müssen wichtige Entscheidungen im Unternehmen schnell getroffen werden. Wer übernimmt diese Entscheidungen im konkreten Ernstfall? Notfallpläne sorgen in der Regel für klare Zuständigkeiten und Maßnahmen, die im Fall der Fälle greifen. Insbesondere muss klar sein, wer im Unternehmen bei IT-Notfällen anzusprechen ist. Wie sind Unternehmen auf diese Vorfälle vorbereitet?

In 60 Prozent der KMU entscheiden Führungspersonen über den Umgang mit Risiken. Im Vergleich zum Vorjahr ist dieser Anteil um 2 Prozentpunkte zurückgegangen. Vergleichsweise klein bleibt mit 5 Prozent

Abb. 13 / DsiN-Praxisreport

Wer im Unternehmen entscheidet über den konkreten Umgang mit Risiken?

5 %
der Beschäftigten entscheiden, wie auf ein Risiko zu reagieren ist.

34 %
lassen die IT-Abteilung oder den IT-Dienstleistenden die Entscheidungen treffen.

10 %
der Bereichs- bzw. Abteilungsleitenden treffen die Entscheidungen.

50 %
überlassen der Geschäftsleitung den Umgang mit Risiken.

Abb. 14 / DsiN-Praxisreport

In welcher Unternehmensgröße entscheidet die Geschäftsführung im Fall einer akuten Bedrohungslage selbst?

60 %
bei Unternehmen mit weniger als 10 Beschäftigten

51 %
bei Unternehmen mit 10 bis 50 Beschäftigten

47 %
bei Unternehmen mit 51 bis 200 Beschäftigten

32 %
bei Unternehmen mit 201 bis 500 Beschäftigten

auch der Anteil der Unternehmen, in denen der Umgang von den Mitarbeitenden selbst entschieden wird. 34 Prozent der Unternehmen betrauen eine IT-Abteilung oder externe Dienstleistende mit dieser Aufgabe.

Eine Betrachtung nach Unternehmensgröße im Umgang mit akuten Bedrohungslagen zeigt, dass bei 60 Prozent der befragten Kleinstunternehmen mit weniger als 10 Mitarbeitenden die Geschäftsführung über Reaktionen entscheidet. Mit wachsender Unternehmensgröße reduziert sich der Anteil auf nur noch 32 Prozent bei Unternehmen mit bis zu 500 Mitarbeitenden.

Passgenaue Sicherheitsschulungsprogramme rückläufig

Sicherheitskompetenzen von Mitarbeitenden sind eine zentrale Voraussetzung für die IT-Sicherheit in Unternehmen. Wie wird IT-Sicherheitskompetenz in der Unternehmenspraxis gefördert? Welche Maßnahmen finden sich im Unternehmensalltag, um eine Sicherheitskultur zu etablieren?

Die Anzahl der Betriebe, die keine Maßnahmen zur Kompetenzförderung veranlassen, liegt heute bei 44 Prozent – und damit 3 Prozentpunkte besser als vor Corona (47 Prozent). Ein verpflichtendes Sicherheitsschulungsprogramm zur Steigerung der Sicherheitskompetenz für alle Mitarbeitenden behält die gleiche Bedeutung. Auf weiterhin niedrigem Niveau ist die Anzahl der Betriebe, die individuell angepasste Sicherheitsschulungen bieten – mit nur 6 Prozent.

25 Prozent ohne Ansätze für IT-Sicherheitskultur

Welchen Stellenwert hat die Entwicklung einer IT-Sicherheitskultur in der Praxis deutscher Unternehmen? Für jedes vierte Unternehmen (25 Prozent) spielt die Förderung von Digitalkompetenzen im Betriebsalltag keine Rolle – dieser Wert ist fast identisch mit der Zeit vor der Coronapandemie (24 Prozent). Auch bieten fast unverändert immerhin 59 Prozent aller Unternehmen Unterstützung an in Form von regelmäßigen Schulungsmaßnahmen (48 Prozent) oder sogar Awareness-Kampagnen (11 Prozent). Diese können Poster oder auch Live-Hacks umfassen. Dem gegenüber geben 16 Prozent der Unternehmen an, dezidiert Maßnahmen zu ergreifen, um eine IT-Sicherheitskultur im Unternehmen zu etablieren.

Abb. 15 / DsiN-Praxisreport

Auf welche Weise wird eine angemessene Sicherheitskompetenz der Mitarbeitenden gewährleistet?

44 %
geben an, dass ihre Mitarbeitenden ausreichend informiert sind (keine Vorkehrungen).

34 %
verschicken gelegentlich Informationen über aktuelle Veröffentlichungen, kostenlose Online-Schulungen und Seminare an ihre Beschäftigten.

16 %
verfügen über ein für alle Mitarbeitenden verpflichtendes Sicherheitsschulungsprogramm.

6 %
greifen auf ein für unterschiedliche Profile von Mitarbeitenden angepasstes Sicherheitsschulungsprogramm zurück und führen regelmäßig Tests durch.

Abb. 16 / DsiN-Praxisreport

Wie sorgen Unternehmen für angemessene Kompetenztrainings?

16 %
haben ihre Sicherheitskultur analysiert und gezielt Kommunikationsmaßnahmen eingeführt, die das Sicherheitsbewusstsein fördern.

25 %
der Befragten geben an, keine Maßnahmen für mehr Kompetenzen zu ergreifen.

48 %
schulen Mitarbeitende regelmäßig und erinnern auch über Schreiben der Geschäftsleitung an die Verantwortung für die Sicherheit im Unternehmen.

11 %
führen Awareness-Kampagnen durch und setzen dabei etwa auf Poster, Live-Hacking-Veranstaltungen und Give-aways.

FAZIT

IT-Sicherheitskultur in Unternehmen stärken

Die Ergebnisse zeigen trotz einiger positiver Entwicklungen immer noch starke Nachholbedarfe bei der Etablierung einer unternehmensinternen IT-Sicherheitskultur. So gibt es positive Tendenzen etwa bei der Zuständigkeit für die IT-Sicherheit in KMU. Sie hat sich in der Coronazeit tendenziell von den Mitarbeitenden auf Personen mit eigener IT-Expertise verlagert. Dadurch kann IT-Sicherheitsvorfällen wirkungsvoller begegnet werden.

Angesichts des Trends durch die Coronapandemie zu Homeoffice sind Bemühungen zu würdigen, die auf mehr IT-Sicherheitskompetenz von Mitarbeitenden setzen. Hierzu gehören verpflichtende Sicherheitsschulungsprogramme für alle Mitarbeitenden sowie weitere Initiativen, die in der Pandemie auf dem Niveau vor Corona gehalten werden konnten, jedoch nicht ausgebaut wurden. Ein Viertel aller Unternehmen verzichtet weiterhin auf grundsätzliche Maßnahmen zur Schulung von Mitarbeitenden.

Während eine gut etablierte IT-Sicherheitskultur den Schutz vor IT-Risiken wirksam erhöhen kann, finden sich entsprechende Ansätze nur bei einer Minderheit von Unternehmen. Diese gilt es daher zu fördern. Das Ziel sollte sein, dass mindestens die Hälfte aller Betriebe entsprechende Vorkehrungen vornimmt.

Tipps und Angebote für die Praxis

- Der **DsiN-Digitalführerschein** bietet für Mitarbeitende in Betrieben eine kostenlose Möglichkeit, die eigenen IT-Kompetenzen zu testen, erweitern und mit einem Zertifikat nachzuweisen. Für Unternehmen ermöglicht der DiFü eine rein digitale und kostenfreie Möglichkeit der Weiterbildung.
  difü.de

- Die **DsiN-Passwortkarte** vereinfacht den Einsatz sicherer Passwörter. In wenigen Schritten wird deren Anwendung im täglichen Gebrauch erleichtert.
  sicher-im-netz.de/dsin-passwortkarte

- Die Workshopreihe **IT-Sicherheit@Mittelstand** von DsiN und dem Deutschen Industrie- und Handelskammertag (DIHK) richtet sich an KMU, die Sicherheit und Datenschutz in ihrem Unternehmen optimieren wollen. Die Workshops motivieren und befähigen zur praktischen Umsetzung von IT-Sicherheitsmaßnahmen.
  sicher-im-netz.de/it-sicherheitmittelstand-workshop-reihe

KAPITEL 3

Ganzheitliche IT-Sicherheit bleibt Ausnahme

Die zusätzliche Digitalisierung im Zuge der Coronapandemie erhöht die Anforderungen an IT-Sicherheit. Jedes Gerät oder jede Technologie, ob zu Hause oder im Büro, kann zum Einfallstor für Angriffe werden. Damit gewinnt auch die ganzheitliche Betrachtung von Schutzvorkehrungen in den Unternehmen an Relevanz. Es geht um kluge Strategien sowie ihre Umsetzung durch wirksame Maßnahmen.

Prävention: Schutzmaßnahmen einbinden und anpassen

Die Forderung nach einem ganzheitlichen Ansatz für IT-Sicherheit gewinnt durch die wachsenden Sicherheitsanforderungen in der Pandemie an Bedeutung. Auch steigen die Anforderungen an Flexibilität und Monitoring der laufenden Sicherheitsmaßnahmen und ihrer Wirksamkeit bei einer sich verändernden Bedrohungslage. Für Kleinstunternehmen kommt hinzu, die Herausforderungen mit weniger Inhouse-Expertise und Ressourcen meistern zu müssen.

IT-Sicherheitsstandard in KMU bleibt Ausnahme

Im Vergleich zum Vorjahr ist die Zahl der Unternehmen mit 20 Prozent konstant geblieben, die ihre IT-Schutzmaßnahmen an Standards wie ISO 27001/2, BSI IT-Grundschutz oder VdS 10000 ausrichten. 13 Prozent überlassen sämtliche Vorkehrungen einem externen Dienstleistenden (+ 2 Prozent gegenüber dem Vorjahr), während sich eine Mehrheit an nicht näher spezifizierbaren Erwägungen orientiert (53 Prozent). 14 Prozent verzichten auf jede Maßnahme. Insgesamt ergibt sich im Vergleich zum Vorjahr eine nur minimale Verbesserung der Gesamtlage.

50 Prozent verzichten bei E-Mails auf Schutzvorkehrungen

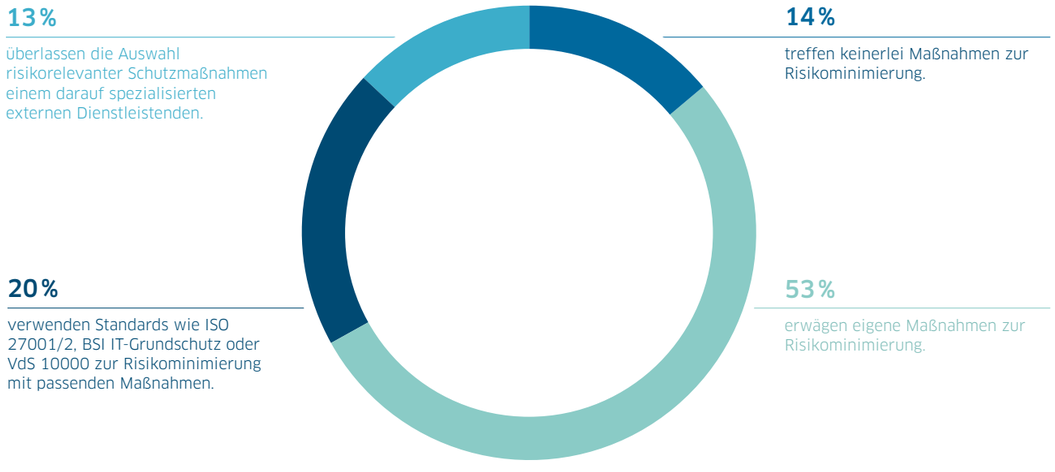
Zu den weitverbreiteten Formen der betrieblichen Kommunikation gehört auch während der Coronapandemie die E-Mail. Sie ist sehr anfällig für Angriffe und Kompromittierungen. Dennoch verzichtet jedes zweite Unternehmen (50 Prozent) auf den Schutz von E-Mail-Anhängen. Dieser Anteil ist damit gegenüber der Zeit vor der Pandemie erneut gestiegen(+ 2 Prozentpunkte).

18 Prozent der KMU nutzen in der E-Mail-Korrespondenz eine Verschlüsselung oder eine elektronische Signatur. Jedoch ist dieser Anteil um 4 Prozentpunkte gesunken. Der Gebrauch eines Passwortschutzes zur Absicherung des Informationsaustauschs steigt leicht um 2 Prozentpunkte auf aktuell 21 Prozent. Der Anteil von Unternehmen, in denen dezidierte, auf Sicherheit geprüfte Plattformen für den Informationsaustausch verwendet werden, bleibt mit 12 Prozent fast konstant (+ 1 Prozent).

Insgesamt ist damit ein negativer Trend bei E-Mail-Schutzvorkehrungen zu erkennen. Dieser Trend scheint angesichts der zunehmenden Risiken überraschend, ist aber erklärbar, wenn wegen vermehrter Nutzung von E-Mail-Kommunikation aus dem Homeoffice von zusätzlicher Sicherheitsvorsorge abgesehen wird. Insoweit ist der Bedarf gestiegen, diese Risiken durch IT-Schutzvorkehrungen nachträglich abzusichern.

Abb. 17 / DsiN-Praxisreport

Wie werden Schutzmaßnahmen im Unternehmen überhaupt identifiziert und bewertet?



Nur jedes zweite Unternehmen regelt Homeoffice

Mit der Coronapandemie gewinnt der sichere Umgang von IT-Geräten im Homeoffice an Bedeutung. Dabei geht es sowohl um die Nutzung dienstlicher IT für private Zwecke als auch umgekehrt um die dienstliche Nutzung von privater Infrastruktur und IT. Sie führen zu einer neuen Verflechtung von genutzten Geräten und Diensten mit neuen Anforderungen gegen Cyberrisiken. Wie haben sich die Unternehmen darauf vorbereitet?

Auffällig ist die Vielfalt der Praxis im Umgang mit Homeoffice: Jedes dritte Unternehmen unterscheidet nach eigener Angabe strikt zwischen geschäftlicher und privater Nutzung der IT (30 Prozent). 22 Prozent sehen eine Richtlinie für den Umgang mit privater und dienstlicher IT vor, während knapp die Hälfte der sonstigen Unternehmen ohne weitere Vorgaben eine Mischung von dienstlichen und privaten Zwecken auf den dienstlich genutzten Geräten zulässt. 23 Prozent der Unternehmen billigen dabei auch die Verwendung privater Geräte für dienstliche Zwecke.

Damit wird erkennbar, dass insgesamt keine klare Orientierung besteht, welchen Strategien für eine

Abb. 18 / DsiN-Praxisreport

Welche Schutzmaßnahmen nutzen Sie für den Versand elektronischer Nachrichten mit Blick auf Anhänge?

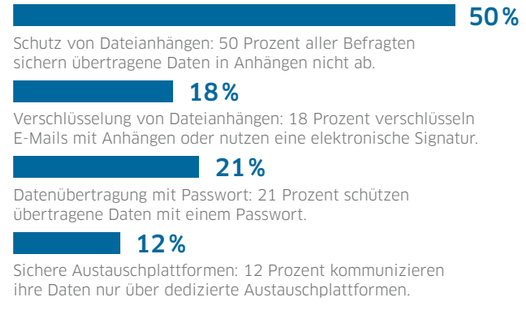
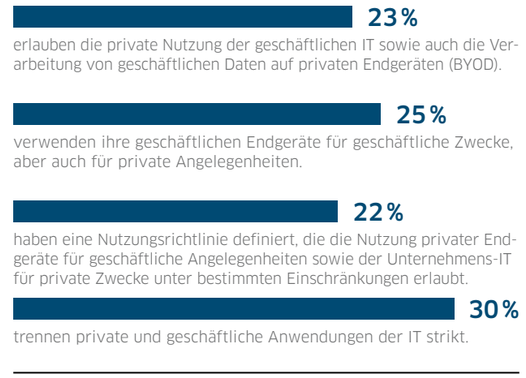


Abb. 19 / DsiN-Praxisreport

Wie gehen Sie mit Privatnutzung im Umfeld der IT um?



Erweiterung der Büroflächen ins Private unter Sicherheitsaspekten zu folgen ist. Hier besteht Entwicklungsbedarf in der Bereitstellung entsprechender Unterstützung sowie auch in der Sensibilisierung des Themas bei den KMU, entsprechende Angebote anzunehmen.

Überprüfung von Schutzmaßnahmen rückläufig

Die regelmäßige Ermittlung der Wirksamkeit von Sicherheitsprogrammen ist von grundlegender Bedeutung. Ziel ist es, die Zuverlässigkeit zu gewährleisten, potenzielle Sicherheitslücken aufzudecken und Probleme bei der Einhaltung von Vorschriften zu entdecken und zu verstehen. Doch wie sieht es in der Praxis damit aus?

Im Studienvergleich hat sich die Zahl der KMU, die die Wirksamkeit ihrer Schutzmaßnahmen im Verdachtsfall überprüfen, von 25 Prozent vor auf 27 Prozent nach der Pandemie erhöht. Ein Fünftel der KMU prüft regelmäßig – fast unverändert seit Pandemiebeginn – die Wirksamkeit der Schutzmaßnahmen.

Die Wirksamkeitsprüfung von IT-Schutz ist auch nach der Coronapandemie längst keine Selbstverständlichkeit. Nur jedes fünfte KMU befasst sich mit dem Thema und überprüft regelmäßig seine Vorkehrungen. Klar ist, dass hier ein Nachholbedarf vorliegt: IT-Sicherheit ist kein einmaliger Zustand, sondern ein kontinuierlicher Prozess, der immer wieder an sich wandelnde und neue Herausforderungen angepasst werden muss.

Abb. 20 / DsiN-Praxisreport

Wird die Wirksamkeit von Schutzmaßnahmen in Ihrem Betrieb überprüft?

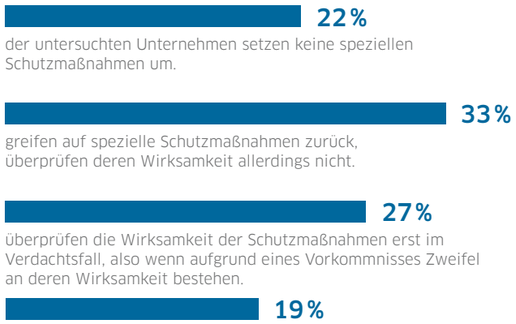
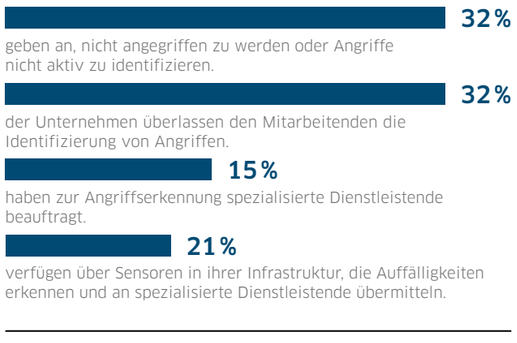


Abb. 21 / DsiN-Praxisreport

Wie erkennen Sie in Ihrem Betrieb einen Angriff durch oder auf die IT?



Detektion: knapp zwei Drittel ohne Angriffserkennung

Das Ziel von Angriffserkennung (Detektion) ist die schnelle und wirksame Reaktion auf eingetretene IT-Sicherheitsvorfälle, um potenziellen Schaden für das Unternehmen abzuwenden. Diese Aufgabe wird traditionell durch Dienstleistende übernommen. Wie hat sich diese Entwicklung während der Coronapandemie weiterentwickelt?

Die Anzahl an Unternehmen, die Angriffe weder selbst noch durch Dritte identifizieren, liegt mit knapp einem Drittel auf dem Vorjahresniveau. Ein weiteres Drittel gibt an, die Verantwortung liege bei den Mitarbeitenden. Rund jedes fünfte Unternehmen (21 Prozent) verfügt über Sensoren in der Infrastruktur, die Auffälligkeiten erkennen und an Dienstleistungsunternehmen weitergeben. 15 Prozent der Befragten greifen auf externe Dienstleistende zur Unterstützung zurück. Damit verfügt insgesamt nur ein gutes Drittel aller Unternehmen über eine empfehlenswerte Praxis im Umgang mit der Angriffserkennung.

Eine Professionalisierung und Verbreitung von Cyberangriffen durch Corona erhöht auch die Anforderungen an Detektionsmaßnahmen. Dies umfasst sowohl standardisierte Angriffe, etwa mit dem Ziel mehrstufiger Erpressungsangriffe, als auch die steigenden Ransomware-Angriffe mit der Folge von Erpressungen.

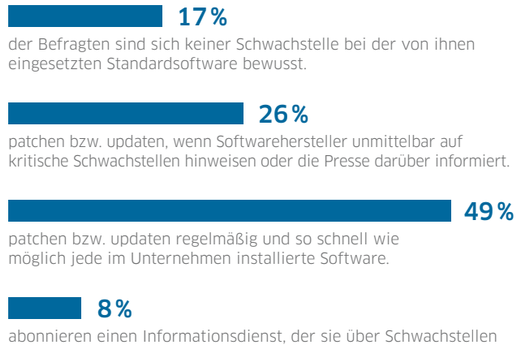
Vor diesem Hintergrund erscheinen die Ergebnisse alarmierend, da davon auszugehen ist, dass Cyberangriffe erst sehr spät entdeckt werden und der Schaden damit größer wird. Hier sollten Aufklärungsaktivitäten ansetzen und auch Mitarbeitende eingebunden werden, über die viele der Angriffe erfolgen, zum Beispiel durch ungesicherte E-Mails.

Umsetzung von Software-Updates stagniert

Der Einsatz von Software in Unternehmen erfordert regelmäßige Updates, damit Sicherheitslücken geschlossen und zusätzliche Sicherheitsfunktionen hinzugefügt werden können. Aktualisierungen und Updates tragen maßgeblich präventiv zur IT-Sicherheit bei und sind verhältnismäßig unkompliziert anwendbar. Daher verringert fortwährende Softwarepflege das Angriffsrisiko erheblich. Doch wie sieht es mit der tatsächlichen Anwendung von Software-Updates als Sicherheitsmaßnahme in den Unternehmen aus?

Abb. 22 / DsiN-Praxisreport

Wie wird mit Schwachstellen in Standardsoftware umgegangen?



Knapp die Hälfte der KMU (49 Prozent) führt ohne Aufforderungen regelmäßig Patches und Updates durch. 26 Prozent der KMU führen Aktualisierungsanfragen meist erst dann durch, wenn die Hersteller oder die Presse über Schwachstellen berichten. Nur ein kleiner Teil (17 Prozent) ist sich keiner Schwachstelle bei den eingesetzten Programmen bewusst. Dieser Anteil ist sogar 2 Prozentpunkte gegenüber der Zeit vor Corona gewachsen.

Diese Defizite in der Praxis im Umgang mit Sicherheits-Udpates gewinnen durch die Coronapandemie an zusätzlicher Relevanz, so, wie die zusätzliche Verwendung von IT-Diensten zu mehr Verletzlichkeit führt. Die Dienste erfordern daher ihrerseits eine zusätzliche Aufmerksamkeit in der schnellen Durchführung von Sicherheits-Updates.

Reaktion: Jedes dritte Unternehmen verzichtet auf Notfallpläne

Notfallpläne, die an jeden Mitarbeitenden kommuniziert werden und digitale Ersthelfende, die im Falle eines Angriffs reagieren, können die Schadenswahrscheinlichkeit wirksam reduzieren. Doch wie sieht es mit der Praxis in den befragten Unternehmen aus? Wie bereiten sich KMU auf mögliche Stör- und Angriffsfälle vor?

Abb. 23 / DsiN-Praxisreport

Wie reagiert Ihr Unternehmen auf (mögliche) Angriffe?

34 %
geben an, erst bei einem Angriff geeignete Maßnahmen zu definieren und anzustoßen.

44 %
verweisen darauf, dass Mitarbeitende über entsprechende Handlungsanweisungen verfügen.

11 %
haben digitale Ersthelfende und trainieren den Ernstfall regelmäßig.

11 %
haben verschiedene Angriffsszenarien skizziert und analysiert sowie spezielle Notfallpläne entwickelt, die sie regelmäßig testen.

Abb. 24 / DsiN-Praxisreport

Setzen Sie auf ein Back-up-Konzept, um Ihre Daten regelmäßig zu sichern?

9 %
verzichten auf ein Back-up-Konzept zur Datensicherheit.

16 %
verfügen zwar über ein Back-up-Konzept, führen jedoch nur unregelmäßig Datensicherungen durch.

46 %
verfügen über ein Back-up-Konzept und greifen regelmäßig darauf zurück.

29 %
Prozent verfügen über ein qualifiziertes Back-up-Konzept.

Zu einer zuverlässigen IT-Sicherheitsstrategie gehört die Vorbereitung für den Ernstfall. Sie umfasst Notfallpläne, die regelmäßig getestet werden sollten. 11 Prozent setzen solche Pläne im Unternehmen ein. Darüber hinaus kommen in 11 Prozent der befragten Unternehmen digitale Ersthelfende zum Einsatz (+ 1 Prozent). 44 Prozent der Unternehmen geben an, Mitarbeitende für den digitalen Notfall vorbereitet zu haben.

Jedes dritte Unternehmen hingegen verzichtet auf Maßnahmen im Vorfeld (34 Prozent) und würde erst im Falle eines Angriffs mögliche Reaktionen anstoßen. Diese Haltung wird den heutigen Anforderungen jedoch weder unter dem Aspekt der IT-Sicherheit noch den datenschutzrechtlichen Anforderungen gerecht.

Ein Viertel der KMU ohne Back-up-Konzept

Ransomware bleibt eine der gefährlichsten Bedrohungen von Unternehmensdaten und -informationen. Durch die Pandemie ist die Häufigkeit von Erpressung durch die Verschlüsselung von Daten nochmals angestiegen. Datensicherungen und systematische Back-up-Strategien können die Angriffe zwar nicht verhindern, jedoch im Angriffsfall als Versicherung eines Unternehmens dienen. Jeglicher Datenverlust kann zu schweren finanziellen oder sogar existenziellen Schäden führen.

Aktuell setzen 9 Prozent der KMU kein Konzept zur Datensicherung ein. Prozentual ist dieser Anteil um 13 Prozent gestiegen. Bei 16 Prozent werden zwar ein Back-up-Konzept eingesetzt, jedoch nur unregelmäßig eine Datensicherung durchgeführt. Rund 75 Prozent haben ein Back-up-Konzept und führen regelmäßig Sicherungen durch. Damit zeigt sich in diesem Bereich der IT-Sicherheit ein ausgeprägtes Sicherheitsbewusstsein im deutschen Mittelstand, das weiterhin ausbaubar ist.

FAZIT

Einfallstore aufdecken und rechtzeitig reagieren

Die Mehrheit der Unternehmen verzichtet trotz (steigender) Anforderungen der IT-Sicherheit auf ganzheitliche Maßnahmen. Grundlegende Maßnahmen wie wirksame Absicherungen von E-Mails, aber auch die Einrichtung von Notfallplänen werden vernachlässigt. Weiterführende Maßnahmen wie die Risikoanalyse stellen die Ausnahme dar. Gerade durch die vergrößerte Angriffsfläche infolge von Corona steigt aber die Bedeutung eines ganzheitlichen IT-Schutzes. Hier sollten Ansätze in der Praxis verfolgt werden, die IT-Sicherheit stärker präventiv behandeln, Fehler identifizieren und diese reaktiv in den Blick nehmen. Es geht darum, sich besser auf Angriffe vorzubereiten, sozusagen als unternehmerisches Selbstverständnis. Umso bedeutsamer wird es daher sein, IT-Sicherheitsmaßnahmen einfach zugänglich zu machen und den ersten Schritt zur Umsetzung mit Unterstützung zu verstärken.

Tipps und Angebote für die Praxis

- Der **DsiN-Blog** liefert Expert:innenbeiträge rund um den sicheren digitalen Geschäftsalltag in kleinen und mittleren Unternehmen. Zahlreiche Gastautor:innen informieren regelmäßig über aktuelle Entwicklungen hinsichtlich IT-Strategie, Datenschutz, eGovernment oder Cloud-Computing.
  dsin-blog.de

- Die **SiBa-App** von DsiN informiert über sicherheitskritische Vorfälle und stellt erste Handlungsempfehlungen und Sicherheitstipps bereit. Der Informationsdienst ist eine nützliche Quelle, um über aktuelle Risiken informiert zu sein.
  sicher-im-netz.de/siba

- Der **Sec-O-Mat** liefert nach Beantwortung einer kurzen Befragung zu IT-sicherheitsrelevanten Themen in wenigen Minuten eine Übersicht zu konkreten Sicherheitsbedarfen Ihres Unternehmens. Nach Registrierung im Sec-O-Mat wird der Aktionsplan mit passenden Handlungsempfehlungen von kostenfreien Schulungen bis zu aufwendigeren IT-Sicherheitslösungen erstellt.
  sec-o-mat.de

- Im Frühjahr 2022 wurde die **TISiM-App** veröffentlicht. Ihr Mehrwert liegt darin, in spielerischer Art ein besseres Verständnis über die eigenen Optionen zu gewinnen und diese in den betrieblichen Alltag effizient zu integrieren.
  tisim.de/app/

KAPITEL 4

Sicherheitspraxis im Fokus: IT-Themen & Trends

Bestärkt durch pandemische Einschränkungen haben digitale Lösungen verstärkt auch in den Alltag von kleineren Unternehmen gefunden. Betroffen sind nahezu alle Bereiche der Wertschöpfung – von Bestellung, Dienstleistung und Produktion bis zur Lieferungslogistik und Kundenkommunikation. Zu den Treibern gehören cloudbasierte Services und Plattformen. Ein zusätzlicher Trend zur Absicherung von Risiken sind Cyberversicherungen, auch für kleinere Unternehmen.

Mehr Zuspruch für Cloud und Plattformen

Die voranschreitende Vernetzung in der Zeit der Pandemie verändert die Praxis von Betriebsstrukturen sowie Unternehmenskooperation. Digitale Plattformen und Lösungen aus der Cloud finden Zuspruch und beeinflussen die Arbeitsstrukturen und Zusammenarbeit innerhalb von Unternehmen. Zugleich schaffen sie neue IT-Risiken sowie Angriffsflächen für Cyberkriminelle. Welche Folgen bewirken diese Veränderungen, welche Veränderungen entstehen dabei für die IT-Sicherheit und ihre Absicherungen durch Cyberversicherungen?

Wachsendes Zutrauen in IT-Schutz „by default“

Das Internet fördert heute auf vielfältige Weise den Vertrieb und Umsatz mit Geschäfts- oder Privatkunden, die durch die pandemiebedingten Einschränkungen zusätzliche Relevanz gewonnen haben. Insbesondere Online-Marktplätze ermöglichen in vielen Branchen neue Wettbewerbschancen – mit neuen Anforderungen an die IT-Sicherheit.

Die Anzahl von KMU, die Verkaufsplattformen für eigene Zwecke nutzen, ist gegenüber dem Vorjahr leicht um 1 Prozentpunkt gestiegen: 45 Prozent der Unternehmen sind auf solchen Plattformen aktiv, davon 19 Prozent über etablierte, 9 Prozent über branchenspezifische Anbieter sowie knapp ein Fünftel (17 Prozent) über eigene Vertriebsplattformen.

Die Sicherheitspraxis bei der Nutzung von Vertriebsplattformen offenbart, dass der Anteil der Unternehmen, die sich auf die standardisierten Sicherheitsmaßnahmen des Plattformanbieters verlassen, mit 65 Prozent ganze 8 Prozentpunkte über dem Wert vor Corona liegt. Zugleich sinkt der Anteil der Unternehmen, die sich ihre Sicherheit zusätzlich zertifizieren lassen. Jedes zehnte Unternehmen verzichtet komplett auf sämtliche Schutzvorkehrungen. Immerhin 16 Prozent geben an, regelmäßige Penetrationstests zur Überprüfung der Sicherheit durchzuführen – minus 2 Prozentpunkte gegenüber der Zeit vor Corona.

Mögliche Ursachen für die Beschränkung der Schutzvorkehrungen auf die mitgelieferte Sicherheit der Plattformen könnte steigendes Zutrauen in die Wirksamkeit dieser Dienste sein. Alternativ könnte es auch auf Bequemlichkeit oder mangelnde Fokussierung in der Pandemie auf zusätzliche Absicherung zurückzuführen sein. Für eine bewusste Entscheidung zum Umgang mit dem Thema sind zusätzliche Aufklärungsangebote geboten.

Abb. 25 / DsiN-Praxisreport

Welche digitalen Verkaufsplattformen nutzen Sie?

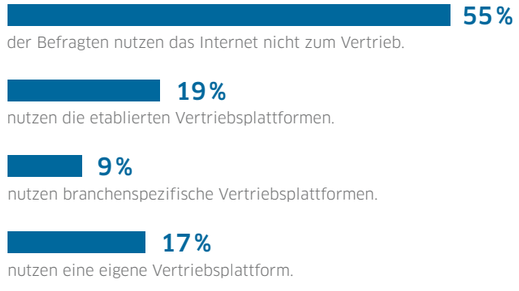
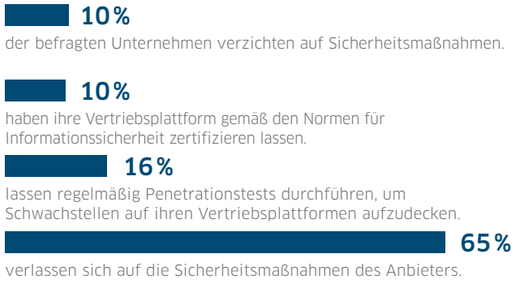


Abb. 26 / DsiN-Praxisreport

Welche Sicherheitsmaßnahmen setzen Sie bei der Nutzung Ihrer Vertriebsplattform ein?



Zuwachs bei Cloud-Computing – Rückgang der IT-Sicherheitsaufwände

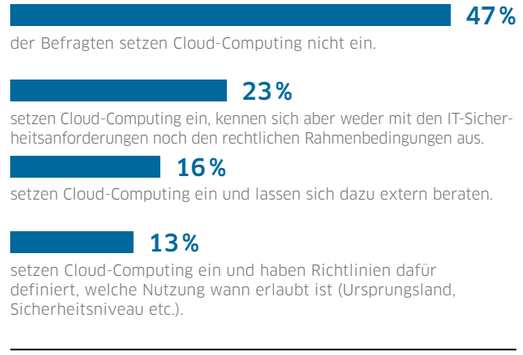
Die Verlagerung von Dienstleistungen in die Cloud ist ein anhaltender Trend, der sich auch im Jahr der Pandemie weiter fortsetzt – ebenso bei kleineren Unternehmen. Mit diesem Trend wachsen die Anforderungen an IT-Sicherheit sowie die Absicherung der Daten. Wie sieht die Praxis des Mittelstands im Umgang mit Cloud-Computing aus?

Im Vergleich zu 2020 hat die Nutzung von Cloud-Computing im Mittelstand weiter zugenommen: Erstmals nutzen über die Hälfte aller Unternehmen (53 Prozent) die Cloud – ein Zuwachs von 6 Prozentpunkten gegenüber der Zeit vor Corona. Damit hat sich der Trend zur Verbreitung der Cloud während der Pandemie nochmals beschleunigt.

Die Praxis der IT-Sicherheit der Unternehmen in der Cloud zeigt zugleich, dass die Auseinandersetzung mit IT-Sicherheitsanforderungen rückläufig ist: 23 Prozent geben an, über keine Kenntnisse – weder zu den IT-Sicherheitsanforderungen noch zu den rechtlichen Rahmenbedingungen – zu verfügen (+ 5 Prozent mehr als vor der Coronapandemie). 16 Prozent lassen sich beim Einsatz von Cloudlösungen beraten und 13 Prozent (- 2 Prozent) verfügen über eigene Richtlinien für die Nutzung von Clouddiensten. Eigene Richtlinien bieten Vorteile, insbesondere im Umgang mit individualisierbaren Cloudangeboten. Standardisierte Vorgaben wie in der „Trusted Cloud“ (siehe Tipps und Angebote für die Praxis) können hier eine Orientierung bieten.

Abb. 27 / DsiN-Praxisreport

Wie sieht es mit der Nutzung von Cloud-Computing aus?



IT-Partnerschaften: Vertrauen statt Kontrolle

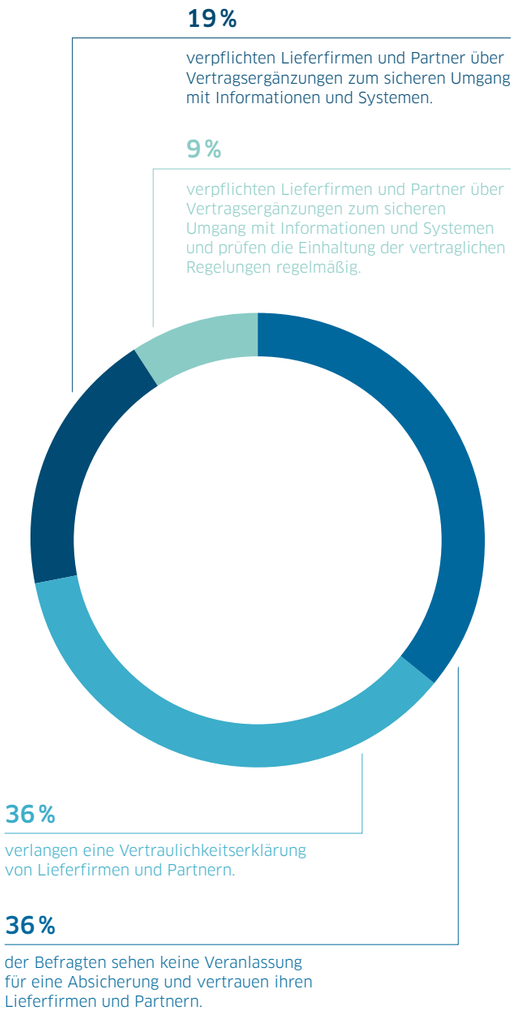
Die Digitalisierung der Geschäftsprozesse führt zu einer engeren Verflechtung der Unternehmen mit Partnern oder Lieferfirmen, da über deren Schnittstellen neue IT-Sicherheitsrisiken entstehen. Wie gestalten sich IT-Sicherheitsfragen in der Zusammenarbeit zwischen Partnern, welche Veränderungen sind erkennbar?

Die Anzahl der Unternehmen, die keinerlei Absicherung zu IT-Sicherheitsaspekten von ihren Lieferfirmen oder Geschäftspartnern im Zuge der digitalen Zusammenarbeit verlangen, nimmt während Corona nochmals um 5 Prozentpunkte zu und liegt jetzt bei 36 Prozent. Zugleich sinkt der Anteil an Unternehmen, die verpflichtende Vertragsergänzungen zur Informationssicherheit von ihren Partnern vorsehen um 4 Prozent gegenüber dem Vorjahr auf 19 Prozent. Auch der Anteil an Unternehmen, die die vertraglichen Änderungen regelmäßig überprüfen, geht auf 9 Prozent zurück (Vorjahr: 11 Prozent).

Damit wird auch in diesem Bereich sichtbar, dass im Zuge der Coronapandemie die Sicherheitsvorkehrungen keinesfalls verbessert wurden, sondern sogar rückläufig waren. Dies mag überraschen, da bereits eine einfache Absicherung in Form einer Vertraulichkeitserklärung die eigenen Risiken spürbar reduzieren kann. Hier wird ein zusätzlicher Bedarf an Aufklärungsarbeit erkennbar, welcher sich auf IT-Sicherheit im Bereich der Lieferketten und Partnerschaften bezieht.

Abb. 28 / DsiN-Praxisreport

Wie gehen KMU mit Lieferfirmen und Partnern in Hinblick auf Informationssicherheit um?



Kaum verändert: Praxis der Cyberversicherungen

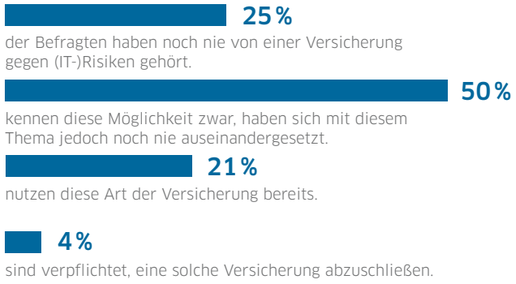
Die umfassende Digitalisierung von Betriebs- und Produktionsprozessen erhöht die Anforderungen an IT-Sicherheit sowie die Schadensrisiken durch Sicherheitsvorfälle. Zum Schutz vor möglichen Schäden kann der Abschluss einer Versicherung sinnvoll sein. Eine Cyberversicherung kann darüber hinaus die Prävention verbessern, indem konkrete Vorkehrungen von der Versicherung eingefordert werden. Inwiefern hat sich die Nutzung von solchen Versicherungen im Vergleich mit den Ergebnissen des letzten Praxisreports verändert?

Die Bekanntheit von Versicherung gegen IT-Risiken hat sich noch einmal leicht um 1 Prozentpunkt auf 75 Prozent erhöht. 50 Prozent von diesem Anteil haben sich mit dem Thema jedoch noch nie proaktiv auseinandergesetzt (vor Corona: 49 Prozent).
4 Prozent gaben an, dass sie verpflichtet sind, eine Cyberversicherung abzuschließen.

Die Zahlen folgen damit einem Trend zur Verbreitung der Versicherbarkeit von Cyberrisiken – zeigen aber keine auffälligen Veränderungen im Vergleich zur Zeit vor Corona.

Abb. 29 / DsiN-Praxisreport

Haben Sie jemals die Möglichkeit erwogen, eine Versicherung gegen (IT-)Risiken abzuschließen?



FAZIT

Digitale Expansion mit IT-Sicherheit verknüpfen

Die wachsende Verbreitung von Cloud-Computing während der Pandemie hat nicht dazu geführt, dass Unternehmen sich auch mit den Sicherheitsfragen aktiv befassen – im Gegenteil. Ein ähnliches Bild zeichnet auch die Verbreitung zur Absicherung von IT-Risiken durch Cyberversicherungen sowie die Absicherung von Partnerschaften bei IT-Sicherheitsbelangen.

Insgesamt entsteht der Eindruck, dass die digitale Expansion während der Coronazeit ohne eine entsprechende Verstärkung der IT-Sicherheitsvorkehrungen einhergegangen ist. KMU vertrauen stattdessen darauf, dass IT-Sicherheit schon hinreichend geschützt sei. Dieser fatalistische Ansatz scheint die realen Bedingungen um wachsende IT-Sicherheitsvorfälle nicht angemessen zu berücksichtigen. Hier sind Ansätze erforderlich, die KMU auf die Handlungsoptionen hinweisen und zur Durchführung grundlegender Maßnahmen ermuntern.

Gezielte Aufklärungsarbeit verdeutlicht, an welchen Stellen im Unternehmen potenzielle Sicherheitslücken von Angreifern ausgenutzt werden und macht dadurch den Einsatz passgenauer Sicherheitsvorkehrungen möglich. Zu oft werden unerkannte Sicherheitslücken zur Bedrohung von Unternehmen.

Tipps und Angebote für die Praxis

- Mit dem **DsiN-Cloud-Scout** unterstützt DsiN kleine und mittelständische Unternehmen dabei, die IT-Sicherheitsvorteile von Cloud-Computing besser zu nutzen und Schwachstellen zu vermeiden. Er bietet in zehn bis 15 Minuten einen spielerischen Überblick zu sicherheitsrelevanten Fragen und hilft, die Vorteile von Cloudlösungen sicher zu nutzen.
  sicher-im-netz.de/dsin-cloud-scout

- Der **DsiN-Datenschutz-Navigator** zeigt auf, worauf Sie beim Datenschutz achten müssen. Sie erhalten einen ersten Überblick über Themen, die einer zusätzlichen Beachtung bedürfen.
  datenschutz-navigator.org

Ausblick: IT-Sicherheit im Zeitalter der Digitalisierung

Die Ergebnisse des DsiN-Praxisreports 2022 belegen zum siebten Mal in Folge den Nachholbedarf der IT-Sicherheit im deutschen Mittelstand. Die DsiN-Studie zeigt auf, dass gerade mit Blick auf die zusätzliche Digitalisierung während der Pandemie zu wenig Maßnahmen von kleinen und mittleren Betrieben erfolgen. Die Zahl der IT-Sicherheitsvorfälle bleibt daher weiterhin hoch, die Anzahl der Cyberangriffe, die zu einem erheblichen Schaden für Unternehmen führen, nimmt zu.

Mit der Coronapandemie und einer verstärkten Digitalisierung wachsen die Herausforderungen, sich gegen Cyberkriminelle zu schützen. Dies ist insbesondere in der Dienstleistungsbranche der Fall. Zu der vulnerablen Gruppe im Mittelstand gehören aber auch grundsätzlich kleinere Unternehmen, die sich keine eigene IT-Abteilung oder -Expert:innen leisten (können oder wollen). Es geht darum, alle Unternehmen, die über keine ausreichende Inhouse-Expertise verfügen, einfach und konkret zu unterstützen. Dies gilt umso mehr, als die abstrakte Bedrohungslage des Ukrainekriegs künftig möglicherweise in konkrete Bedrohungsszenarien umschlagen könnte.

Es geht daher um drei Schlaglichter:

1.
Auch in den kommenden Jahren wird IT-Sicherheit eine hohe Relevanz für Unternehmen darstellen.

2.
IT-Sicherheitstrainings, passgenaue Aktionen und Maßnahmen und ein zielgruppengerechtes Angebot zum Ausbau der IT-Sicherheitskompetenzen für Unternehmen und Mitarbeitende müssen verstärkt werden.

3.
Durch konsequente Weiterentwicklung von Transferinfrastrukturen für IT-Sicherheit und dem damit verbundenen Ausbau der Zusammenarbeit mit der Wirtschaft werden Angebote zugänglich gemacht, die zielgerichtet die Cybersicherheit erhöhen und zur Wettbewerbsfähigkeit der Unternehmen beitragen.

Deutschland sicher im Netz e.V.
DsiN leistet konkrete Hilfestellung für Verbrauchende sowie für kleine und mittlere Unternehmen im sicheren Umgang mit dem Internet. Dafür entwickelt DsiN praktische Angebote und Anleitungen im Verbund mit Unternehmen, Verbänden und Vereinen. Als produktunabhängige Plattform für Aufklärungsinitiativen ist DsiN für neue Mitglieder offen, die IT-Sicherheit als maßgeblich für den Erfolg der Digitalisierung betrachten.

In der Digitalen Agenda der Bundesregierung wurde ein Ausbau der Zusammenarbeit und Unterstützung von DsiN beschlossen. Schon heute verstärkt DsiN seine Aufklärungsarbeit: Für Verbrauchende stehen kostenlose Anleitungen zum souveränen digitalen Umgang im Netz im Mittelpunkt wie die SiBa-App zu aktuellen Warnmeldungen und das DsiN-Webportal.

Gegründet wurde DsiN als gemeinnütziger Verein im Nationalen IT-Gipfelprozess der Bundesregierung und steht seit 2007 unter der Schirmherrschaft des Bundesministeriums des Innern. DsiN möchte seine Aufklärungsarbeit im Dialog mit der Politik, der Wissenschaft und weiteren Akteur:innen der digitalen Gesellschaft weiter stärken.

Impressum

DsiN-Praxisreport Mittelstand 2021/22
Studie von Deutschland sicher im Netz e.V. zur digitalen Sicherheitslage der kleinen und mittleren Unternehmen in Deutschland

Verantwortlich: Dr. Michael Littger
Redaktion: Jan Lietz, Christina Mersch, Marius Thielmann
Gestaltung und Grafiken: KRAUT & KONFETTI
Stand: Juni 2022

Bildquellen:
Titel: zeljkosantrac/iStock, Seite 1 (Michael Kellner): BMWK/Susanne Eriksson, Seite 2 (Michael Littger): Deutschland sicher im Netz e.V., Seite 2 (Susanne Diehm): SAP Deutschland, Seite 6: bedya/Adobe Stock, Seite 14: mapodile/iStock, Seite 21: charlesdeluvio/Unsplash, Seite 22: ridvan_celik/iStock, Seite 30: svetikd/iStock

Deutschland sicher im Netz e.V.
Albrechtstraße 10c
10117 Berlin
Telefon +49 30 767581 – 510
presse@sicher-im-netz.de

sicher-im-netz.de

Ein Handlungsversprechen von: