DsiN-Praxisreport 2020
Mittelstand@IT-Sicherheit

DsiN-Schirmherrschaft:

Bundesministerium des Innern, für Bau und Heimat

Studien-Schirmherrschaft:

Bundesministerium für Wirtschaft und Energie

Eine Studie von:

DsiN Deutschland sicher im Netz

Deutschland sicher im Netz e.V.

DsiN leistet konkrete Hilfestellung für Verbraucher 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.

Gegründet wurde DsiN als gemeinnütziger Verein im Nationalen IT-Gipfelprozess der Bundesregierung und steht seit 2007 unter der Schirmherrschaft des Bundesministeriums des Innern.

Impressum

DsiN-Praxisreport Mittelstand 2020
Studie von Deutschland sicher im Netz e.V.
zur digitalen Sicherheitslage der kleinen
und mittleren Unternehmen in Deutschland

Verantwortlich: Dr. Michael Littger
Redaktion: Clara Schaksmeier
Gestaltung und Grafiken: KRAUT & KONFETTI
Stand: Oktober 2020

Deutschland sicher im Netz e.V.
Albrechtstraße 10 c
10117 Berlin
Telefon +49 30 27576 – 310
Telefax +49 30 2757651 – 310
info@sicher-im-netz.de

sicher-im-netz.de

IT-Sicherheit für einen starken Mittelstand

Thomas Jarzombek

Der Mittelstand steht für Innovation und Beschäftigung in Deutschland und ist eine wichtige Stütze unserer Gesellschaft. Die Corona-Pandemie hat den Mittelstand vor große Herausforderungen gestellt. Der Mittelstand hat dabei erneut eine hohe organisatorische Anpassungsfähigkeit bewiesen. Mit Hilfe der Digitalisierung und Vernetzung gelang es vielen Betrieben, routinierte Aufgabenbereiche neu zu organisieren. Arbeiten wurden ins Homeoffice verlagert, Betriebsprozesse neu strukturiert. Dabei wurde deutlich: Der digitale Fortschritt bietet auch in der Krise konkrete Lösungen und Chancen.

Damit gewachsen ist auch die Relevanz von IT-Sicherheit. Gerade die Arbeit im Homeoffice hat Schwachstellen offenbart. Der DsiN-Praxisreport 2020 gibt einen Einblick in die veränderten Anforderungen in der IT-Sicherheit im deutschen Mittelstand vor und in der Pandemie. Der Report zeigt, dass in wichtigen Bereichen der IT-Sicherheit Fortschritte erzielt wurden. So wurden in kleinen und mittleren Unternehmen mehr präventive Maßnahmen angestoßen. Das Bewusstsein bei Mitarbeiterinnen und Mitarbeitern für IT-Sicherheit ist gewachsen. Zugleich sind an anderer Stelle Handlungsbedarfe und -defizite deutlich geworden. Insbesondere bei der Umsetzung von operativen Sicherheitsmaßnahmen zeigen sich Nachholbedarfe.

Hier unterstützt das Bundesministerium für Wirtschaft und Energie mit Aufklärungs- und Sensibilisierungsmaßnahmen der Initiative „IT-Sicherheit in der Wirtschaft“. Das Bundeswirtschaftsministerium hat dazu in diesem Jahr die Transferstelle „IT-Sicherheit im Mittelstand“ (TISiM) auf den Weg gebracht. Gemeinsam mit Partnern wie dem Deutschen Industrie- und Handelskammertag stellt sie Angebote mit passgenauen Lösungen und Unterstützungsleistungen für Selbständige, kleine Unternehmen, Handwerk und Freiberufler bereit.

Ich wünsche Deutschland sicher im Netz e. V. weiterhin viel Erfolg für die wichtige Aufgabe, die IT-Sicherheit im deutschen Mittelstand konkret und nachhaltig zu verbessern.

Ich wünsche eine angenehme Lektüre.

Thomas Jarzombek, MdB

Beauftragter des Bundesministeriums für Wirtschaft und Energie
für die Digitale Wirtschaft und Start-Ups

Schirmherr DsiN-Praxisreport 2020 Mittelstand@IT-Sicherheit

Gute Zusammenarbeit – starke IT-Sicherheit

Dr. Michael Littger

Alexander Kläger

Der DsiN-Praxisreport 2020 beschreibt die Sicherheitslage in einem Zeitraum von zwölf Monaten – vor und während der coronabedingten Beschränkungen. Er zeigt, dass diese Beschränkungen in Bereichen wie Cloud Computing, elektronischen Kommunikationsformen und dezentral gesteuerten Betriebsprozessen zu einer vermehrten Nutzung geführt haben. Er zeigt aber auch, dass das Bewusstsein für die Schutzbedürftigkeit der eigenen Datenprozesse sowie die Handlungsbereitschaft für mehr IT-Sicherheit nicht in gleichem Maße Schritt hält. Während die Digitalisierung im Mittelstand sich mit und durch COVID-19 also weiter beschleunigt, gibt es im Sinne einer ganzheitlich gedachten Sicherheit für Betriebe noch viel zu tun: Es geht um die Motivation und Unterstützung auf allen Ebenen. Dabei geht es insbesondere um solche Unternehmen ins Visier, die selbst oftmals kaum über eigene IT-Expertise oder zuständige Abteilungen verfügen. Sie bedürfen zusätzlicher Initiativen sowie einer verständlichen Ansprache und geduldigen Unterstützungsarbeit.

Wir werden den Transfer und die Vermittlung passgenauer Angebote künftig ins Zentrum unserer Bemühungen um digitale Aufklärungsarbeit rücken. Es geht um eine möglichst individuelle Ansprache. Die neue Transferstelle IT-Sicherheit im Mittelstand (TISiM) wird hier ein Meilenstein in der bundesweiten Unterstützer-Infrastruktur für IT-Sicherheit sein, gerade für kleinere Betriebe und Selbstständige. Mit TISiM setzen wir auf Zusammenarbeit und Vernetzung aller Akteure. Aufklärungsarbeit, Vermittlung sowie Unterstützung können gewährleistet werden, wenn engagiertes Handeln auf sinnvolle Arbeitsaufteilung trifft. Es geht um Sicherheitsexpert:innen aus Wirtschaft und Wissenschaft, Aufklärer:innen und Wissensvermittler:innen in den Unternehmensnetzwerken sowie in behördlichen Einrichtungen.

Wir möchten auch Ihre Kompetenzen, Netzwerke und Erfahrungen mit IT-Sicherheit gern einbinden. Bringen Sie sich bei uns ein – als IT-Anbieter:innen und Dienstleister:innen, Wissensvermittler:innen oder engagiertes Unternehmen, das bereits selbst Erfahrungen mit Sicherheitsfragen gesammelt hat. Wir wollen mehr IT-Sicherheit für alle. Machen Sie mit! Mehr IT-Sicherheit kann ganz einfach sein.

Wir wünschen viel Freude bei der Lektüre!

Dr. Michael Littger
DsiN-Geschäftsführer

Alexander Kläger
Geschäftsführer SAP Deutschland SE & Co. KG.

Ziel und Design des Praxisreports

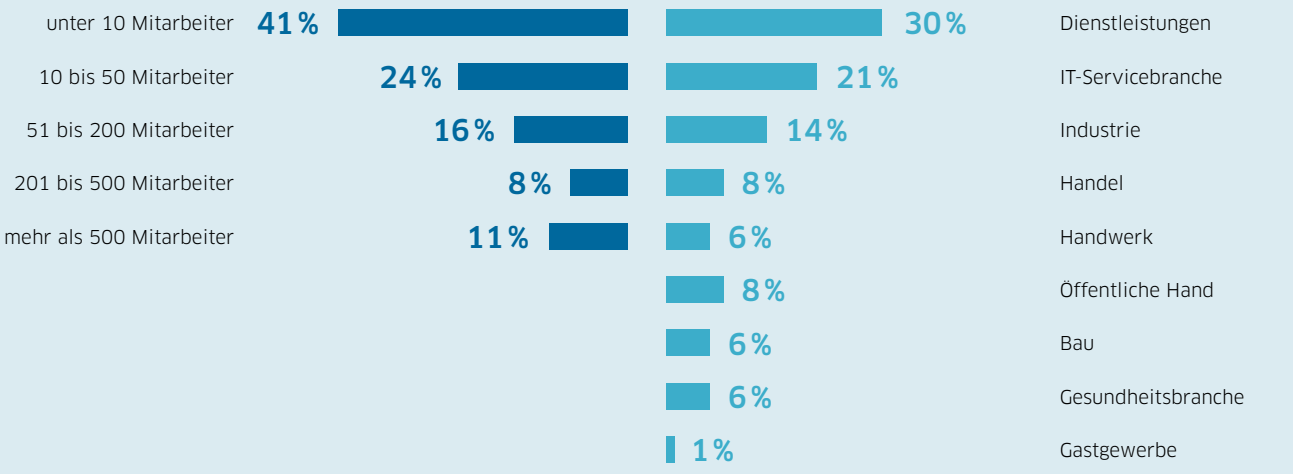
Beim Praxisreport handelt es sich um die Auswertung einer Befragung von Mitarbeiter:innen sowie leitenden Angestellten kleiner und mittlerer Unternehmen. Insgesamt 24 Themenfelder wurden anhand eines Fragenkatalogs beleuchtet und anschließend ausgewertet. Die Befragung fand im Zeitraum von April 2019 bis April 2020[1] statt und berücksichtigt 1.038 abgeschlossene Erhebungen.

Mit 41 Prozent sind Unternehmen mit weniger als 10 Beschäftigten die am stärksten repräsentierte Gruppe. Kleinunternehmen mit bis zu 50 Mitarbeiter:innen kommen mit 24 Prozent an zweiter Stelle. 24 Prozent der Befragten sind in Unternehmen mit bis zu 500 Beschäftigten tätig. Betrachtet man die Gesamtheit, wird deutlich, dass gut 90 Prozent aller befragten Unternehmen anhand des zentralen Größenkriteriums von bis zu 500 Beschäftigten zum Mittelstand zählen.

Der Blick auf die vertretenen Branchen macht deutlich, dass ein Drittel dem Bereich Dienstleistung angehört. 21 Prozent der Befragten sind in IT-Unternehmen tätig. Industrie (mit 13 Prozent) und Handel (mit 8 Prozent) bilden zusammen ein weiteres Fünftel der Befragten. Handwerk (6 Prozent) und Bau (4 Prozent) bilden zusammen fast 11 Prozent der repräsentierten Branchen ab. 6 Prozent der Mitarbeiter:innen kommen aus dem Gesundheitsbereich. Die öffentliche Hand ist mit 7 Prozent, das Gastgewerbe mit 1,5 Prozent vertreten.

Über die Hälfte der Befragten gab an, für IT-Sicherheit zertifiziert oder Ansprechperson für dieses Thema zu sein. 18 Prozent äußerten, dass sie sich im Bereich IT-Sicherheit nicht auskennen. Der Praxisreport 2018 bildet den Vorläufer des vorliegenden Reports und dient ihm in Einzelfällen als Bezugsgröße.

Abb. 1 / Aufteilung der befragten Unternehmen nach Größe und Branche



1 Es handelt sich bei dieser Betrachtung um den Zeitraum vor und zu Beginn der COVID-19-Pandemie.

Inhalt

Zentrale Ergebnisse

Durch die digitale Vernetzung von Betrieben, Dienstleistung und Produktion sind auch kleine und mittlere Unternehmen in wachsendem Maße von IT-Sicherheit abhängig. Das Bewusstsein für die Relevanz von IT-Sicherheit ist in den vergangenen Jahren gestiegen, gerade auch mit den Folgen von Corona. Auch werden mehr präventive Maßnahmen, wie zum Beispiel Schulungen und Sicherheitsvorkehrungen, umgesetzt. Zugleich ist ein großer Teil der befragten Unternehmen nach wie vor nicht ausreichend informiert und gesichert.

Datenschutz und Cybersecurity sichern Existenzen im Mittelstand. 87 Prozent der befragten Personen gaben an, dass ihre Unternehmensdaten mit IT-Sicherheit zusammenhängen. Mehr als die Hälfte erklärte sogar, die Existenz ihrer Unternehmen sei gefährdet, wenn Daten verloren gingen oder an die Konkurrenz weitergeleitet würden. Es wird deutlich, dass kleine und mittlere Unternehmen den Wert und den damit einhergehenden benötigten Schutz ihrer Daten mehr und mehr erkennen. Dennoch handeln nur knapp zwei Drittel konkret, um ihre IT-Sicherheit zu stärken. Mehr als ein Drittel bleibt inaktiv.

Es fehlen ganzheitliche Ansätze in den KMU. 46 Prozent der befragten KMU gaben an, bereits ein oder mehrere Male Opfer eines Cyberangriffs geworden zu sein. Die Dunkelziffer dürfte höher liegen, denn bei der Detektion von Angriffen bleibt ein großer Teil absolut passiv bzw. verlässt sich auf die Mitarbeitenden. Für diese gibt es seit 2018 den Angaben nach mehr Sicherheitsschulungen sowie mehr Awarenesskampagnen. Dennoch werden nicht alle im Unternehmen agierende Personen ausreichend eingebunden.

In der größten Verantwortung sehen die befragten KMU nach wie vor die Geschäftsführung. Diese sei entweder alleine oder gemeinsam mit einem/einer Sicherheitsbeauftragten für IT-Sicherheit zuständig. In knapp der Hälfte der Fälle trifft die Geschäftsleitung relevante Entscheidungen im Bereich IT-Sicherheit. Entsprechend liegt bei den führenden Positionen faktisch eine hohe Verantwortung.

Im Allgemeinen finden die offiziellen IT-Sicherheitsstandards bei KMU kaum Resonanz. Diese werden nur von 20 Prozent der KMU genutzt. Mehr als die Hälfte der Unternehmen bedient sich eigens definierte Maßnahmen zur Risikominimierung. Diese fallen in der Regel sehr spärlich aus. 70 Prozent der befragten KMU begnügen sich bestenfalls mit einer einmaligen Ermittlung ihrer individuellen Risikosituation. Diese passive Haltung spiegelt sich auch in einem weiterhin niedrigen Niveau beim Erstellen von Notfallplänen wider.

Mit fortschreitendem Digitalisierungsgrad werden Cyberversicherungen populärer. Diese werden immerhin bereits in jedem zweiten Unternehmen genutzt. Mit steigendem Einsatz von Cloud Computing und digitalen Datenspeicherungen ist ein proaktiver Umgang mit IT-Sicherheit sowie ein noch größeres Bewusstsein für Schutz- und Absicherungsmöglichkeiten unumgänglich. Der Praxisreport macht deutlich, dass vielen weder die Sicherheitsanforderungen noch die rechtlichen Rahmenbedingungen bekannt sind.

Die Erkenntnisse dieses Reports verlangen demnach nach konkreten Maßnahmen, die in unserem Drei-Punkte-Plan näher aufgeführt werden.

KAPITEL 1

Der digitale Mittelstand: IT-Sicherheit schützt Existenzen

Für den Großteil der Unternehmen ist die digitale Vernetzung Alltag geworden. Die COVID-19-Pandemie hat die digitale Vernetzung noch einmal verstärkt – von der Kommunikationsstruktur und den Betriebsabläufen über die Ablage von Daten und Kontakten bis hin zu Vertriebsfragen. Wie steht es dabei um die IT-Sicherheit im deutschen Mittelstand? Wo bestehen aktuelle Risikotrends und Handlungsbedarfe? Die vorliegenden Zahlen und Auswertungen geben einen Einblick in aktuelle Defizite und Bedarfe.

Bereits vor COVID-19: IT-Sicherheit in der Praxis muss verstärkt werden

Der Report zeigt die Abhängigkeit der Betriebe von einer störungsfreien IT und IT-Sicherheit sowie ihre Schutzbedürftigkeit auf. Auch auf die durch Cyberangriffe entstandenen Kosten aus Sicht der betroffenen Unternehmen wird eingegangen, um ein umfassendes Bild der IT-Sicherheitslage und ihrer Relevanz für Unternehmen zu gewinnen.

Steigende IT-Abhängigkeit in Betrieben

Das Bewusstsein, dass IT-Sicherheit im Unternehmen für den eigenen Erfolg eine zentrale Voraussetzung ist, wächst. Im Vergleich zu 2018 ist der Grad der direkten Abhängigkeit von IT-Sicherheit und den Betriebsabläufen der befragten Personen gestiegen.

Immer mehr Kleinstunternehmen nehmen einen Zusammenhang zwischen dem wirtschaftlichen Wohlergehen und ihrer IT-Sicherheit wahr. Noch vor zwei Jahren beschränkte sich das Bewusstsein dieser Korrelation eher auf größere Unternehmen. Das hat sich verändert. Nun sind insbesondere Kleinstunternehmen von IT-Sicherheit abhängig.

Seit Beginn der Erhebung vor sechs Jahren konnte eine Verlagerung der Branchen mit großer IT-Abhängigkeit beobachtet werden. Gehörte bislang die Gesundheitsbranche zu den meistgenannten Branchen, ist es nun die IT-Servicebranche mit der größten Korrelation von IT-Sicherheit und wirtschaftlichem Erfolg. Das Handwerk, das Baugewerbe sowie das Gastgewerbe haben aufgrund der Ausrichtungen vergleichsweise niedrige Kennwerte. Es ist zu vermuten, dass dies mit dem geringen Grad an Digitalisierung und Sensibilität aus Sicht der Betroffenen in diesen Branchen zusammenhängt.

Abb. 2 / DsiN-Praxisreport

Inwiefern sehen Sie einen Zusammenhang zwischen dem Erfolg Ihres Unternehmens und der Integrität, Vertraulichkeit oder Verfügbarkeit von Informationen – also der IT-Sicherheit?

6 %
der Befragten geben an, dass die Integrität, Vertraulichkeit und Verfügbarkeit von Informationen im Unternehmen für sie nicht wichtig sind.

7 %
sind der Meinung, dass ihre Betriebsabläufe auf diese Informationen weitgehend nicht angewiesen sind.

38 %
der beteiligten Unternehmen sind sogar der Meinung, dass ihre Betriebsabläufe unmittelbar von der IT-Sicherheit abhängen.

49 %
antworten, dass der Schutz dieser Informationen zwar wichtig, aber nicht existentiell ist.

Abb. 3 / DsiN-Praxisreport

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

Zustimmung bei:

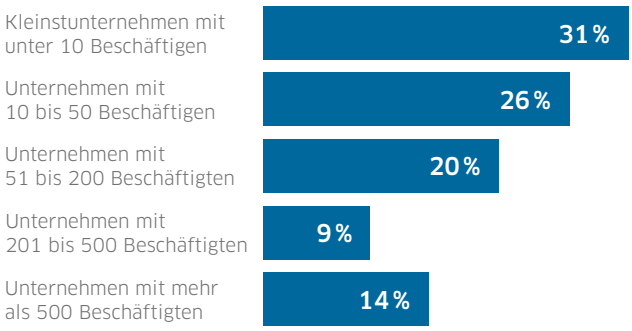
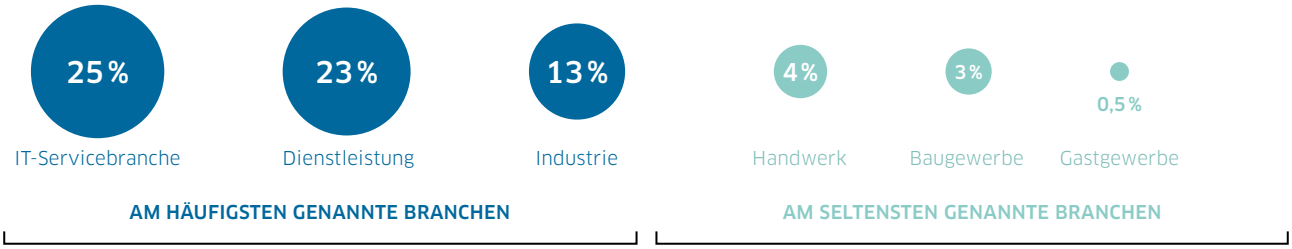


Abb. 4 / DsiN-Praxisreport

Wenn Sie einen direkten Zusammenhang zwischen wirtschaftlichem Wohlergehen und IT-Sicherheit sehen, welcher Branche gehören Sie an …

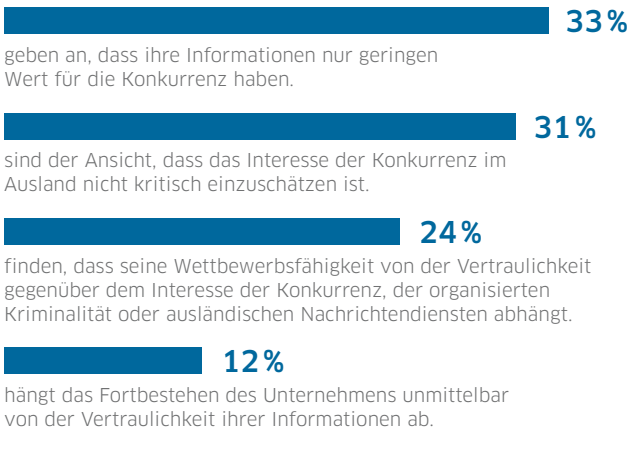


Zwölf Prozent sehen ihr Unternehmen als gefährdet an

Die IT-Daten und -Informationen des deutschen Mittelstandes werden von den betroffenen Betrieben als wertvoll wahrgenommen. Dies gilt auch für Start-ups und kleine Betriebe. Daher können Cyberangriffe für alle Unternehmen schädlich sein. Der deutsche Mittelstand schätzt die eigene Gefährdung durch Datenklau folgendermaßen ein:

Abb. 5 / DsiN-Praxisreport

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

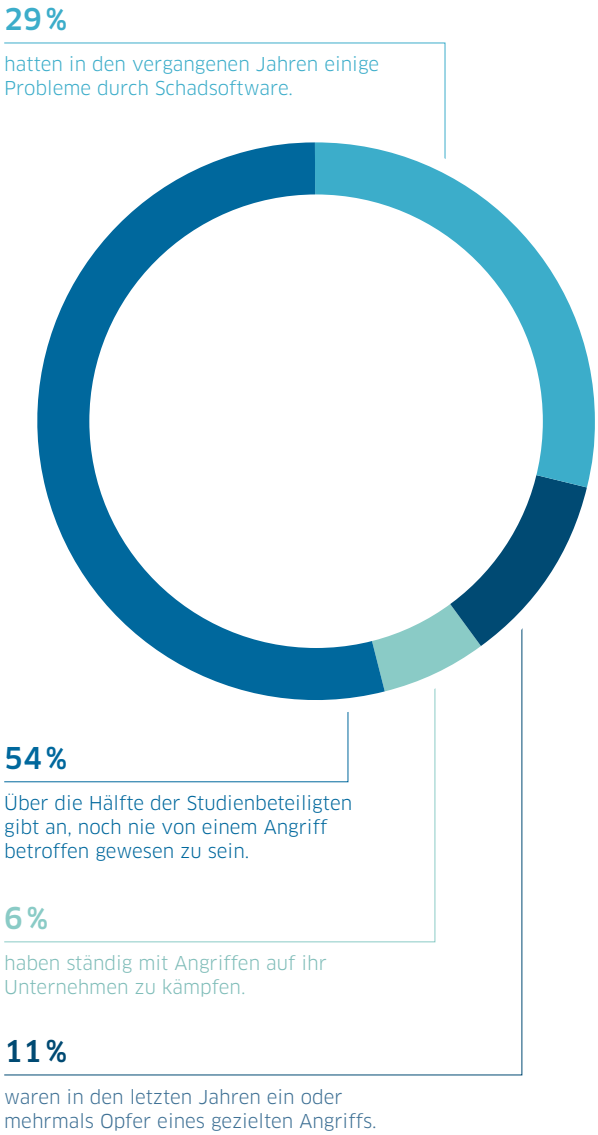


Vergleicht man die Ergebnisse von 2018 mit der aktuellen Auswertung, wird deutlich, dass das Bewusstsein für den Zusammenhang zwischen Informationssicherheit und Wettbewerbsfähigkeit leicht gestiegen ist. Dieses Bewusstsein ist jedoch nach wie vor überraschend gering ausgeprägt. Nur 12 Prozent (2018 waren es 10 Prozent) sagten aus, dass sie durch einen Angriff auf ihre Datenbestände ihre Existenz unmittelbar gefährdet sehen. Für fast ein Drittel hingegen hängt die Wettbewerbsfähigkeit von der Sicherheit ihrer vertraulichen Daten ab.

Rund 33 Prozent der KMU betrachten ihr eigenes Know-how als nicht schützenswert. Diese Zahl ist geringer als noch vor zwei Jahren. Dennoch sieht immer noch ein Drittel keinen besonderen Schutzbedarf ihres Know-hows im Hinblick auf das eigene wirtschaftliche Wohlergehen. Es wird jedoch vermutet, dass die Unternehmen sich bei dieser Frage auf besonders „sensible“ oder „kritische“ Daten konzentriert haben. Ein Verlust von Daten jeglicher Art kann bei allen Unternehmen zu folgenschweren Umständen führen. Das Bewusstsein dafür ist nur unzreichend ausgeprägt.

Abb. 6 / DsiN-Praxisreport

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



Die Zahlen verdeutlichen, dass das Wissen über die Angreifbarkeit der eigenen Daten, seien sie sensibel oder nicht, noch fehlt. Insbesondere in Zeiten, in denen ganze Existenzen von der Beschaffenheit der eigenen IT-Sicherheit abhängen, ist ein Nachholbedarf an Aufklärungsarbeit erkennbar. Umfassende Awarenesstrainings und -kampagnen sind hier vonnöten.

46 Prozent der Unternehmen wurden schon einmal angegriffen

Sind sich Unternehmen bewusst, dass erpresserische Angriffe durch Ransomware oder reputations- und vertrauensschädigende Datenleaks durch Social Engineering sehr ernsthafte Folgen haben können, die bis zum Verlust der Wettbewerbsfähigkeit führen? Wurden sie schon einmal Opfer eines IT-Angriffs?

Der Großteil der befragten Personen (54 Prozent) gab an, noch nie von einem Angriff betroffen gewesen zu sein. Dazu passt, dass nur in den seltensten Fällen ein Angriff sofort erkannt wird. Werden Betroffene im Zuge einer Ransomware-Attacke erpresst und sollen ein Lösegeld zahlen, fällt dies zwar auf. Werden jedoch Kundendaten, Produktinformationen oder andere Daten entwendet und ggf. weiterverkauft, kann es sein, dass das Unternehmen nie von der Cyberattacke erfährt, aber seine Wettbewerbsfähigkeit dennoch einbüßt. Von daher ist mit einer größeren Dunkelziffer zu rechnen.

74 Prozent der Betroffenen melden Schäden durch Angriffe

Das Ausmaß der Schäden kann unterschiedlich sein. Wir haben daher die befragten Personen, die bereits Opfer eines Angriffes wurden, gefragt, wie schwer dieser ausfiel:

Abb. 7 / DsiN-Praxisreport

Wie folgenreich waren die aus Angriffen resultierenden Schäden?

26 %
Etwas mehr als ein Viertel der Befragten gibt an, keinerlei Konsequenzen durch einen Angriff gehabt zu haben.

60 %
antworten, zwar einigen Aufwand, aber keine nachhaltigen Schäden davongetragen zu haben.

10 %
Knapp mehr als 10 Prozent schätzen den Aufwand zur Behebung der angriffsverursachten Schäden als erheblich, aber nicht existenzbedrohend ein.

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

Drei von vier Unternehmen hatten finanzielle Mehraufwendungen durch einen Cyberangriff. 14 Prozent gaben an, dass die Schäden eine erhebliche oder sogar sehr schwere Belastung waren. Ein Cyberangriff kann einen Schock für den Betrieb bedeuten. In vielen Fällen ist daher davon auszugehen, dass Schädigungen der Reputation auf Seiten der Kundschaft oder aber der Lieferanten und Partner oftmals unentdeckt bleiben, jedoch einen langfristigen und tiefgreifenden Einfluss auf die Wettbewerbsfähigkeit und den Erfolg eines Unternehmens haben.

Das Ausmaß der Schutzbedürftigkeit variiert zwischen den verschiedenen Branchen. Es hängt unter anderem von einer digitalen Einbindung der Betriebsabläufe, einem unmittelbaren Zusammenhang zwischen Digitalisierung und Arbeitsprozessen sowie der Ausführung der jeweiligen Berufe ab.

Die Zahlen zeigen, dass insbesondere der Handel unter den Folgeschäden durch Cyberangriffe leidet. Die Unterschiede zwischen den einzelnen Branchen sind bemerkenswert. Sie lassen darauf schließen, dass bei der Aufklärungsarbeit eine zielgruppengerechte Ansprache notwendig ist. Eine individuelle Begleitung auf dem Weg zu mehr IT-Sicherheit scheint unumgänglich.

37 Prozent der Betriebe ohne Risikoermittlung

Um die Wahrscheinlichkeit eines erfolgreichen Angriffes zu reduzieren, müssen diverse Vorkehrungen getroffen werden. Dazu gehört die Ermittlung des eigenen Risikoprofils und der Schutzbedürftigkeit. Wo ist mein Unternehmen besonders angreifbar? Wo liegen die Schwachstellen? Welche Bereiche müssen besonders geschützt werden?

Abb. 8 / DsiN-Praxisreport

Welche Branchen sind betroffen?

66 %
In der Dienstleistungsbranche geben 66 Prozent der Befragten an, keine nachhaltigen Schäden durch Angriffe erfahren zu haben.

63 %
Im Handwerk weisen 63 Prozent auf erhebliche oder schwere Folgen eines selbst erfahrenen Angriffs hin.

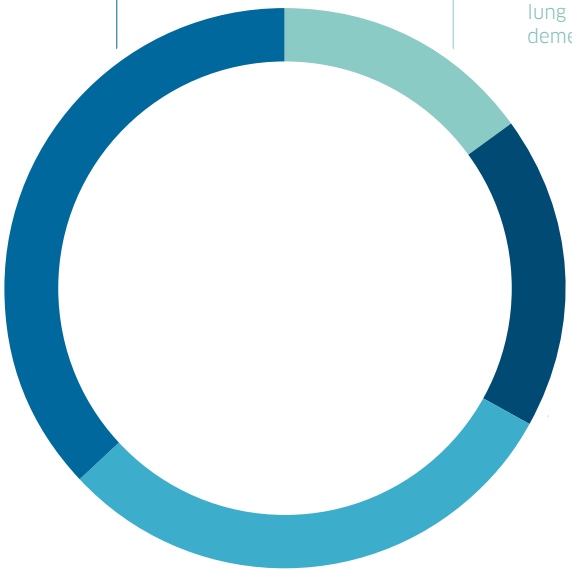
89 %
Im Handel liegt dieser Wert nach Auskunft der betroffenen Beschäftigten sogar bei 89 Prozent.

Bei einer profunden Risikoanalyse sind neben technischen und organisatorischen auch menschliche Faktoren zu berücksichtigen. Im häufigen Fall des „Social Engineering“ werden werden Mitarbeiter:innen dazu gebracht, Unternehmensdaten herauszugeben.

Vergleicht man die aktuellen Zahlen mit den Befragungsergebnissen von 2018, so wird deutlich, dass mehr Unternehmen eine Ermittlung aktueller Risikofaktoren, insbesondere in Form einer jährlichen Überprüfung, durchführen. Jedoch ist aufgrund der ständig weiterentwickelten Angriffsmethoden eine einmalige Überprüfung im Jahr zu wenig. An dieser Stelle muss das Bewusstsein gestärkt werden.

Abb. 9 / DsiN-Praxisreport

Wie wird die aktuelle Risikosituation überhaupt ermittelt?



37 %

der Befragten verzichten auf die Ermittlung aktueller Risikofaktoren.

15 %

führen eine kontinuierliche Risikoermittlung durch und passen ihre Einschätzung dementsprechend an.

18 %

Knapp über 18 Prozent ermitteln einmal jährlich ihre konkrete Risikosituation und überprüfen die vorhandenen Werte.

30 %

kennen ihre größten Risiken dank einer einmaligen Bestandsaufnahme.

FAZIT

IT-Risikomanagement durch Awareness & Maßnahmen verbessern

Die Ergebnisse verdeutlichen, dass es positive Entwicklungen hin zu mehr von mehr IT-Sicherheit gibt. So steigt das Bewusstsein für die Relevanz einer sicheren IT im Unternehmen, allerdings hinken die entsprechenden Sicherheitsmaßnahmen deutlich hinterher. Die aktuell ergriffenen Maßnahmen sind weder ausreichend noch flächendeckend. Insbesondere zeigt sich ein Nachholbedarf bei der Risikoanalyse und Aufdeckung von Schadensereignissen.

Unternehmen müssen sich auch verstärkt des Wertes ihrer eigenen Daten bewusst werden. Es geht darum, dass der Verlust von Daten, die auf den ersten Blick nicht relevant wirken, ebenfalls zu erheblichen Reputationsschäden und sowie Folgen in der Geschäftsfähigkeit führen kann.

Tipps und Angebote für die Praxis

- TISiM bietet ab 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 deren Umsetzung.
  www.tisim.de

- Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Regionale Mittelstand 4.0-Kompetenzzentren helfen mit Expertenwissen, Demonstrationszentren, Netzwerken zum Erfahrungsaustausch und praktischen Beispielen.
  www.mittelstand-digital.de

- Der DSGVO-Quick-Check bietet Ihnen mit 39 Fragen zu daten- und sicherheitsrelevanten Themen eine Bestandsaufnahme Ihres Unternehmens. Sie erhalten als Ergebnis eine Matrix, welche die Risikosituation in Ihrem Unternehmen darstellt.
  www.vds-quick-check.de

KAPITEL 2

Nachholbedarf: Grundlagen einer IT-Sicherheitskultur

Mit zunehmendem Digitalisierungsgrad wächst damit einhergehend auch die Angriffsfläche für Cyberattacken. Aufgrund der Vernetzung von Betriebsabläufen und Produktionsprozessen wird die Informations- und Kommunikationstechnik zu einer „kritischen Komponente“ im Unternehmen und Wirtschaft – mit umfassenden Auswirkungen auf die Wettbewerbsfähigkeit.

Zuständigkeiten und Kompetenzen für IT-Sicherheit

Abb. 10 / DsiN-Praxisreport

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

Wer ist in wechlem Maße für IT-Sicherheit zuständig? Wie steht es um die Vorkehrungen beim „Faktor Mensch" gegen Angriffe in KMU? Reichen diese gegen mögliche Einfallstore in der Software aus? Gibt es ein Bewusstsein dafür, dass jede:r Mitarbeiter:in eine potenzielle Schwachstelle für Unternehmen darstellt? Gibt es ein Bewusstsein für Social Engineering?

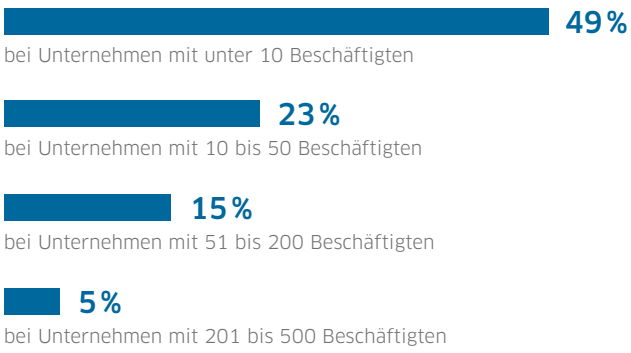
IT-Sicherheit: Leitungsebene in der Verantwortung

Welche Vorkehrungen erfolgen bei Mitarbeiter:innen und Vorgesetzten gegen Sicherheitsangriffe: Wer ist im deutschen Mittelstand für IT-Sicherheit verantwortlich?

Die Mehrheit der Befragten sieht heute die Geschäftsführung in der Verantwortung. Zwar liegt die Zahl unter dem Wert von 2018, doch für immerhin 49 Prozent gilt: IT-Sicherheit ist Chefsache. Überraschend erscheint, dass mehr als ein Viertel (28 Prozent) jede:n einzelne:n Mitarbeiter:in allein für sich verantwortlich sieht. Die Betrachtung nach Größe der Unternehmen führt zu einem differenzierten Ergebnis:

Abb. 11 / DsiN-Praxisreport

Die Beschäftigten sind unmittelbar für IT-Sicherheit zuständig:



Die Zahlen zeigen, dass IT-Sicherheit häufiger Chefsache ist, desto kleiner das Unternehmen ist. In fast jedem zweiten Kleinstunternehmen wird IT-Sicherheit über die Chefetage verantwortet.

Je kleiner das Unternehmen, desto mehr lastet die Verantwortung für die IT-Sicherheit auf den Schultern der Geschäftsleitung. Insbesondere bei Kleinstunternehmen wird fast jeder zweite Geschäftsführer als dafür verantwortlich gesehen. Dass IT-Sicherheit als Aufgabe der Führungsebene angesehen wird, kann auf die niedrige Mitarbeiter:innenzahl zurückgeführt werden. Dies könnte darauf hindeuten, dass keine explizite Zuständigkeit (in Person einer/s IT-Sicherheitsbeauftragten) vorliegt.

Es muss gewährleistet werden, dass Führungskräfte und Mitarbeitende Schulungen und Awarenesstrainings für ihre Verantwortungsbereiche erhalten. Nur mit einem entsprechenden Bewusstsein können sie die richtigen Entscheidungen treffen.

Entscheidung in Risikosituationen: Blick auf die Geschäftsführung

Im Falle einer Risikosituation muss schnell reagiert werden. Da jede:r im Unternehmen von einem Angriff betroffen sein kann, sollten allgemeine Krisenreaktionsmaßnahmen geschult werden. Insbesondere sollte schon im Vorfeld klar sein, wer in diesem Falle der bzw. die Ansprechpartner:in ist. Doch haben Unternehmen über eine entsprechende Rollenverteilung bereits nachgedacht? Wenn ja, wie?

Die Hälfte der befragten Personen sieht auch hier die Geschäftsführung im Fokus – analog zur Frage nach der Verantwortung. Insbesondere in Kleinstunternehmen ist das der Fall.

Abb. 12 / DsiN-Praxisreport

Die Geschäftsleitung ist unmittelbar für IT-Sicherheit zuständig:

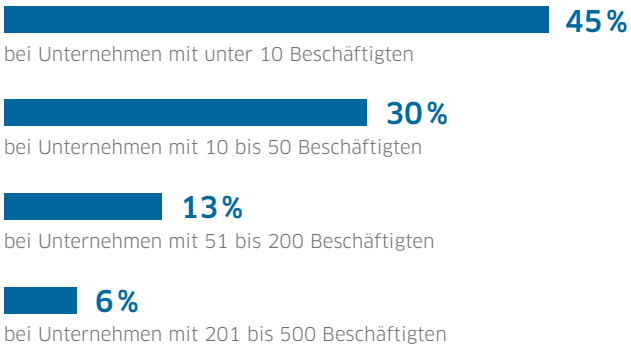
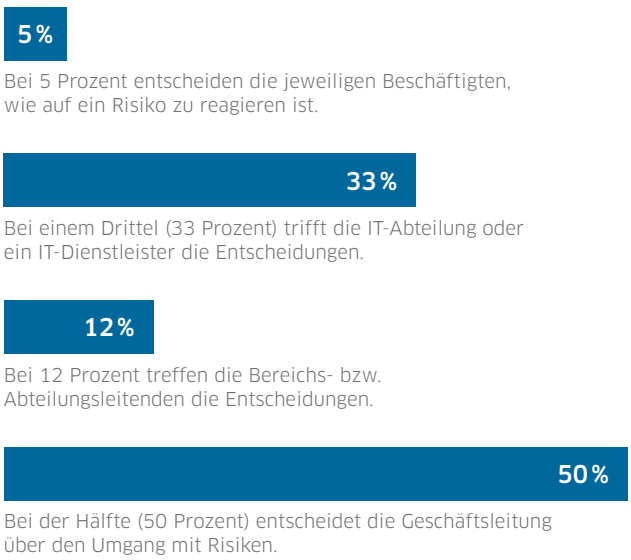


Abb. 13 / DsiN-Praxisreport

Wer im Unternehmen entscheidet über den konkreten Umgang mit Risiken?



Auch eine genauere Betrachtung nach der Unternehmensgröße führt zu aussagekräftigen Ergebnissen:

Abb. 14 / DsiN-Praxisreport

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

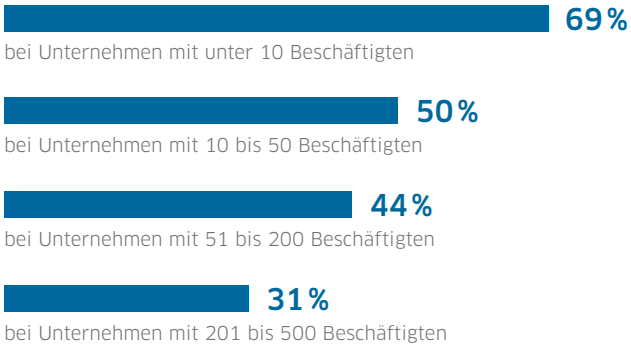
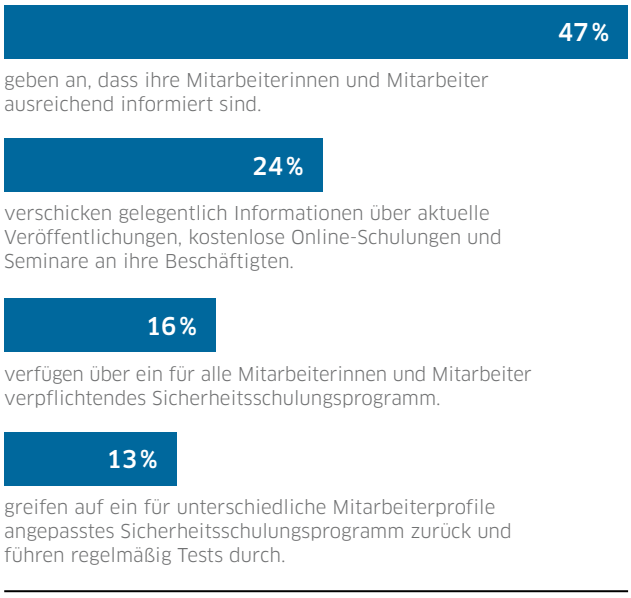


Abb. 15 / DsiN-Praxisreport

Auf welche Weise wird eine angemessene Sicherheitskompetenz der Mitarbeiter:innen gewährleistet?



Ein Bewusstsein für und ein Wissen über sinnvolle Präventions- und Reaktionsmaßnahmen sind daher für Geschäftsleiter:innen essenziell. Mit der wachsenden Größe eines Unternehmens nimmt dieser Wert ab.

IT-Sicherheitsschulungen: Fast die Hälfte ohne Unterstützung (47 Prozent)

Um alle Mitarbeitenden ihrer Verantwortung bewusst zu machen und sie entsprechend vorzubereiten, müssen sie geschult werden. Wie genau, sieht hier die Praxis bei Unternehmen aus?

Zwar werden im Vergleich zu 2018 mehr Mitarbeiter:innen verpflichtend geschult, dennoch ist diese Zahl sehr gering. Untersuchungen wie die Studie des Wissenschaftlichen Instituts für Infrastruktur und Kommunikationsdienste (WIK) von 2017 deuten darauf hin, dass die meisten Sicherheitsvorfälle durch Beschäftigte verursacht werden. Es ist also von großer Notwendigkeit, dass umfassende Aufklärungsmaßnahmen erfolgen. Nur mit einem geschulten Auge und einem Bewusstsein für das richtige Verhalten bei einem Angriff kann adäquat darauf reagiert werden.

Kompetenztrainings: Ein Viertel ohne gesonderte Maßnahmen

Wie wird IT-Sicherheit in der Praxis gelebt? Wie werden Angestellte informiert und erinnert? Damit IT-Sicherheit im Unternehmensalltag praktiziert werden kann, muss eine Sicherheitskultur bereits selbstverständlich sein. Wie realisieren Unternehmen dies?

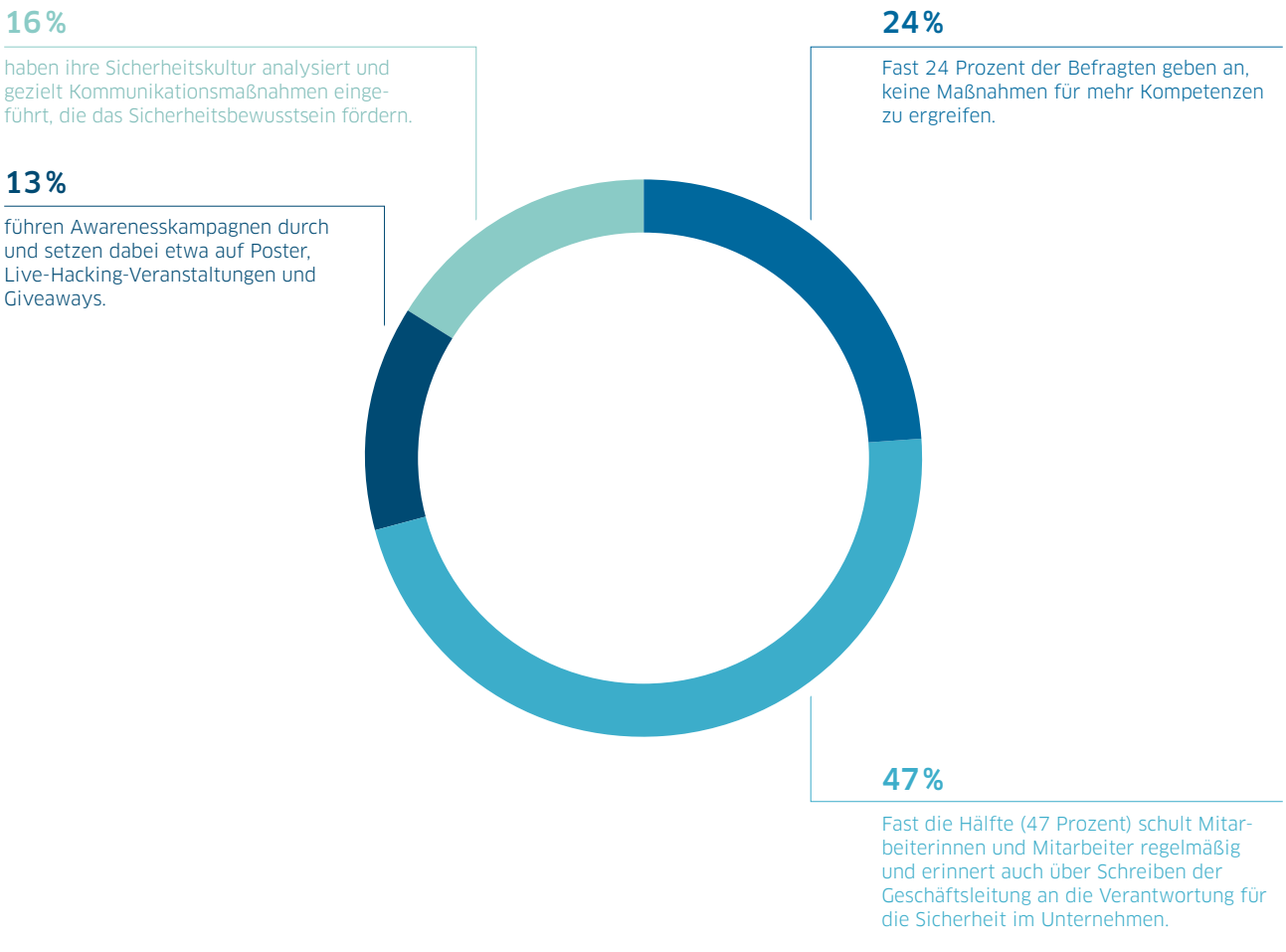
Im Vergleich zu 2018 nehmen sich mehr Unternehmen Zeit für die Entwicklung einer Sicherheitskultur. Erfreulich ist, dass jede zweite Geschäftsleitung eines KMU ihre Autorität, Vorbildfunktion und Reichweite durch Informationsmails an die Mitar-

beitenden nutzt. Eine nachhaltige Kulturtransformation wird in der Regel jedoch erst durch dauerhafte Maßnahmen erreicht.

Aufklärungsarbeit sollte nicht nur von oben kommen. Die Mitarbeiter:innen, insbesondere die Auszubildenden, in den Dialog miteinzubeziehen, kann ein großer Mehrwert für jedes Unternehmen sein. Awarenesskampagnen und gezielte Maßnahmen können zu einer angemessenen Sicherheitskultur beitragen. Dabei sollten perspektivisch partizipative und interaktive Ansätze anstelle frontaler Formate gefördert werden.

Abb. 16 / DsiN-Praxisreport

Wie sorgen Unternehmen für angemessene Kompetenztrainings?



FAZIT

IT-Sicherheit in Leitungsebenen stärken

Die befragten kleinen und mittleren Unternehmen sind auf die Leitungsebene fokussiert, wenn sie an IT-Sicherheit denken. Angesichts der noch zu wenig durchgeführten Schulungen und Awarenesstrainings für Mitarbeitende wird deutlich, dass darüber hinaus auch die Leitung geschult werden muss.

Zielgruppengerechte Ansprachen für Führungskräfte und Mitarbeiter:innen sind bei den Schulungsangeboten von großer Wichtigkeit, denn die Position im Unternehmen hat Einfluss auf die Perspektive, Verantwortung und den Handlungsrahmen. Nur wenn der Umgang mit IT-Sicherheit zielgerichtet und auf die Bedürfnisse der jeweiligen Person angepasst ist, kann er auch einen nachhaltigen Wandel im Denken und Verhalten hervorrufen.

Tipps und Angebote für die Praxis

- DsiN bietet mit Bottom-Up ein kostenfreies Bildungsangebot, damit Berufsschulen Auszubildende bereits während der dualen Ausbildung auf die Herausforderungen des Berufslebens vorbereiten können.
  www.dsin-berufsschulen.de

- Die Workshopreihe IT-Sicherheit@Mittelstand von DsiN und dem DIHK zeigt, worauf es bei IT-Sicherheit und Datenschutz in kleinen und mittleren Unternehmen ankommt. Erfahren Sie von Profis, welche Maßnahmen zur Stärkung Ihrer IT-Sicherheit in Frage kommen.
  www.it-sicherheit-mittelstand.org

- Die Workshopreihe von TISiM vermittelt in leicht verständlichen Workshop-modulen relevantes Wissen rund um IT-Sicherheit.
  www.tisim.de

KAPITEL 3

Wirkungsfelder stärken: Prävention, Detektion, Reaktion

IT-Sicherheit ist ein mehrteiliger Prozess mit den drei Wirkungsfeldern Prävention, Detektion und Reaktion. Entsprechende Maßnahmen sorgen dafür, Angriffen vorzubeugen, sie zu erkennen und im Ereignisfall wirkungsvoll zu reagieren. Abgestimmte Maßnahmepläne können helfen, Angriffe und Schäden so gering wie möglich zu halten. Doch wie ist der Mittelstand im Umgang mit IT-Schutz aufgestellt – und welche Rolle spielen ISO 27001/2, BSI IT-Grundschutz oder VdS 10000?

Organisatorische und technische Vorkehrungen (Prävention)

Wirksame Vorkehrungen im organisatorischen und technischen Bereich eines Unternehmens bilden das Fundament der IT-Sicherheit. Eine umfassende Identifikation von Schwachstellen und entsprechende Maßnahmen sollten prophylaktisch festgelegt werden, um präventiv gegen IT-Sicherheitsangriffe vorzugehen. Doch welche Maßnahmen werden in KMU heute praktiziert, wie sind sie miteinander verzahnt und aufeinander abgestimmt? In welchen Feldern – Prävention, Detektion, Reaktion – zeigen sich Nachholbedarfe?

Schutzmaßnahmen: 80 Prozent ohne Orientierung an anerkannten Standards

Wie werden Schutzmaßnahmen in deutschen Unternehmen ausgewählt und entwickelt? Was ist dabei die Rolle von IT-Sicherheitsstandards und externen Dienstleistern?

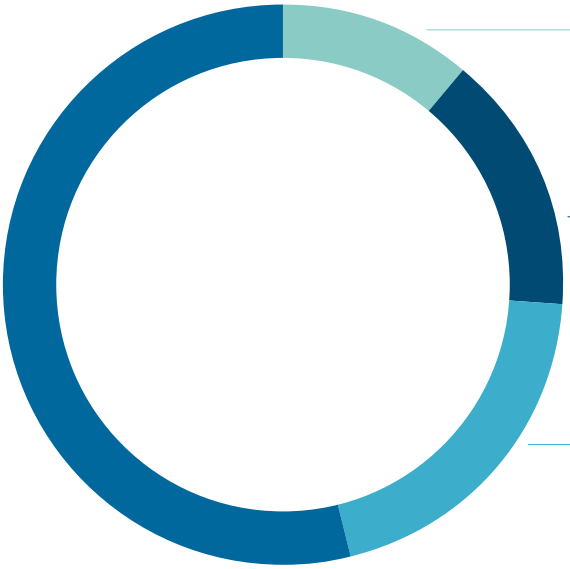
Die Zahl der Unternehmen, die Standards wie ISO 27001/2, BSI IT-Grundschutz oder VdS 10000 zur Risikominimierung mit passenden Maßnahmen nutzen, ist in den vergangenen Jahren stetig gestiegen. Auch werden mehr externe Dienstleister, die auf dieses Gebiet spezialisiert sind, zu Rate gezogen.

Mehr als die Hälfte der Unternehmen verlässt sich jedoch weitgehend auf die eigene Expertise zur Risikominimierung. Es wird vermutet, dass hier die Kosten externer Expertise als zu hoch eingeschätzt werden. Auch wird die Höhe der Schäden unterschätzt.

Zwar ist die Zahl der Unternehmen, die keinerlei Maßnahmen ergreifen, ein wenig gesunken – mit 15 Prozent ist sie jedoch weiterhin viel zu hoch. Hier wird deutlich, dass Aufklärungsarbeit geleistet und der Zugang zu passenden Angeboten erleichtert werden muss.

Abb. 17 / DsiN-Praxisreport

Wie werden Schutzmaßnahmen im Unternehmen überhaupt identifiziert und bewertet?



54 %

Über die Hälfte der an der Studie beteiligten Unternehmen (54 Prozent) erwägen eigene Maßnahmen zur Risikominimierung.

11 %

überlassen die Auswahl risikorelevanter Schutzmaßnahmen einem darauf spezialisierten externen Dienstleister.

15 %

treffen keinerlei Maßnahmen zur Risikominimierung.

20 %

Ein Fünftel (20 Prozent) verwendet Standards wie ISO 27001/2, BSI IT-Grundschutz oder VdS 10000 zur Risikominimierung mit passenden Maßnahmen.

Schutzmaßnahmen konkret: Nur die Hälfte der E-Mails sind verschlüsselt

Vernetzte Kommunikation ist die Basis der Zusammenarbeit in Projekten und Unternehmen. Nachrichten, die über ein Chatprogramm oder E-Mails versendet werden, gehören heute zur Grundausstattung fast jeden Unternehmens. Dementsprechend ist es wichtig, umsichtig mit angehängten Dateien sowie sensiblen Informationen umzugehen und Sicherheitsvorkehrungen zu treffen.

Verglichen mit 2018 sichern immer mehr Befragte die Daten in ihren Anhängen ab. Dennoch trifft nur etwas mehr als die Hälfte Sicherheitsvorkehrungen für den Versand von Nachrichten. 22 Prozent nutzen eine Verschlüsselung oder eine elektronische Signatur. Weitere 11 Prozent versenden keine Anhänge, sondern laden die Dateien nur auf dedizierten Austauschplattformen hoch.

19 Prozent bedienen sich des Passwortschutzes. Die Zahl ist überraschend gering, da eine Passwortverschlüsselung in der Regel sehr einfach umzusetzen ist. Auch hier scheinen das Wissen darüber sowie eine kurze Heranführung an das Thema zu fehlen.

Wirksamkeit von Schutzmaßnahmen: Alarmierende Inaktivität

Daten, Techniken, Anwendungen und Anforderungen für Software sowie für Schutzmaßnahmen verändern sich ständig. Um sicherzugehen, dass die unternehmenseigenen Maßnahmen wirksam sind, ist eine regelmäßige Prüfung unumgänglich. Wie sieht es in der Praxis damit aus?

Allgemein ist die Zahl der Überprüfungen der Schutzmaßnahmen gestiegen. Dennoch verhalten sich 77 Prozent der befragten Unternehmen sehr passiv in Bezug auf eine regelmäßige Überprüfung der

Abb. 18 / DsiN-Praxisreport

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

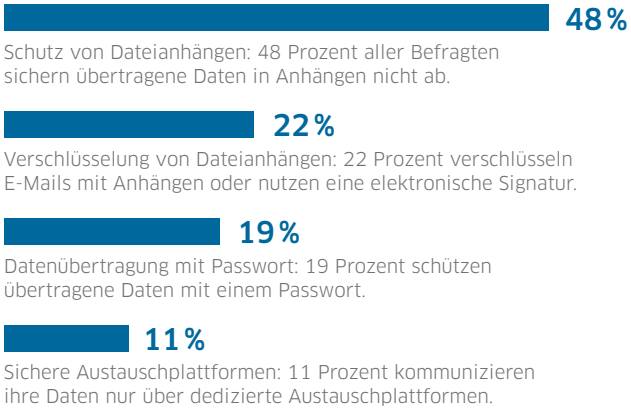
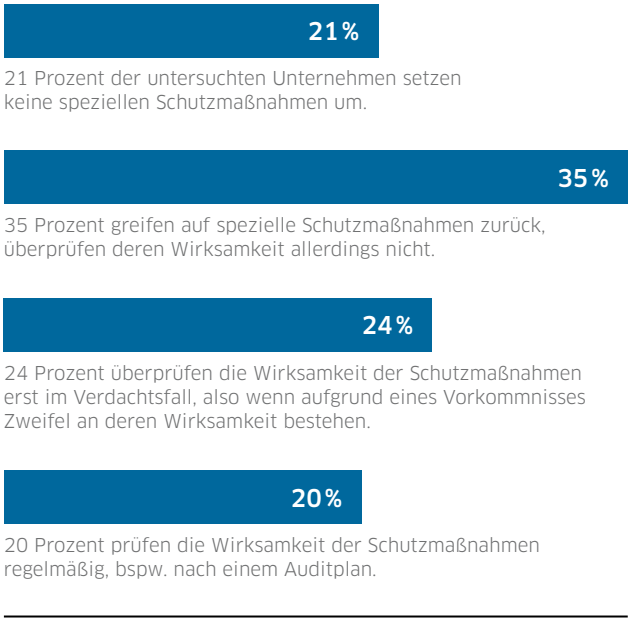


Abb. 19 / DsiN-Praxisreport

Wird die Wirksamkeit von Schutzmaßnahmen in Ihrem Betrieb überprüft?



Maßnahmen. 24 Prozent werden erst aktiv, wenn ein Vorfall gemeldet wurde. Nur 20 Prozent prüfen die Wirksamkeit der Schutzmaßnahmen tatsächlich. Es ist hierbei anzumerken, dass ein Angriff nicht immer erkannt wird und somit auch in Fällen von unentdeckten Cyberattacken viele Unternehmen inaktiv bleiben.

Es wird dringend empfohlen, die Wirksamkeit der Schutzmaßnahmen regelmäßig zu überprüfen. Dies kann zum Beispiel durch einen Auditplan geschehen. Unternehmen, die ihren Partnern und Lieferanten versichern können, dass sie sich regelmäßig überprüfen (lassen), genießen ein größeres Vertrauen. Von daher ist ein Bewusstsein darüber und ein aktiver Umgang mit der Überprüfung der Wirksamkeit von Schutzmaßnahmen für kleine und mittlere Unternehmen essenziell.

Schadensvermeidung durch Angriffserkennung (Detektion)

Angriffe rechtzeitig zu erkennen, ist ein elementarer Bestandteil einer funktionierenden IT-Sicherheitsstrategie. Nur wenn Attacken rechtzeitig erkannt werden, können diese abgewendet und Schäden, seien sie finanzieller oder anderer Art, vermieden werden.

Fast ein Drittel der Unternehmen erkennt Angriffe nicht

Es gibt zahlreiche technologische Möglichkeiten, um Angriffe auf die IT zu detektieren. So kann automatisiert gewährleistet werden, dass ein Angriff erkannt wird. Auch externe Dienstleister bieten eine Angriffserkennung an. Bei Angriffen durch den Menschen, zum Beispiel im Form von Social Engineering, sind die Mitarbeitenden in der Verantwortung, diese zu erkennen und zu melden.

Vor diesem Hintergrund stellt sich die Frage, auf welche Maßnahmen KMU setzen, um Angriffe überhaupt zu erkennen.

Abb. 20 / DsiN-Praxisreport

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

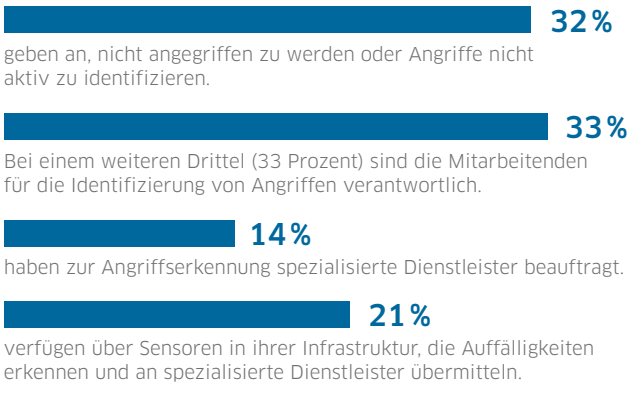
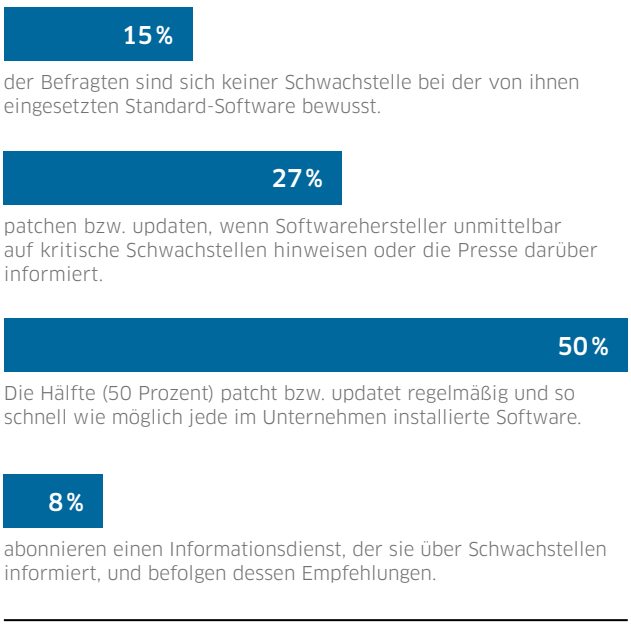


Abb. 21 / DsiN-Praxisreport

Wie wird mit Schwachstellen in Standardsoftware umgegangen?



Bemerkenswert hoch ist immer noch die Zahl der Unternehmen, die sich passiv verhalten. Ein Drittel gab an, nicht angegriffen zu werden oder die Angriffe nicht aktiv zu identifizieren. Ein weiteres Drittel sieht die Mitarbeitenden in der Verantwortung. Nur die wenigsten, 14 Prozent, beauftragen einen spezialisierten Dienstleister. Dafür haben 21 Prozent Sensoren in der eigenen Infrastruktur. Schlagen diese Alarm, wird auch hier ein externer Dienstleister angefragt.

Externe Hilfe kann eine gute Unterstützung sein. Ebenfalls ist schnelles Handeln gefragt. Passivität kann zu fatalen Folgen führen. Durch eine umfassende Angriffserkennung können Schäden vermieden und abgewendet werden. Da ein Teil auch hier die Mitarbeitenden in der Verantwortung sieht, ist eine Schulung wichtig. IT-Sicherheits-Notfall-Pläne und Awarenesstrainings sind hier vonnöten. Auch regelmäßige „Alarmübungen“ sind hilfreich.

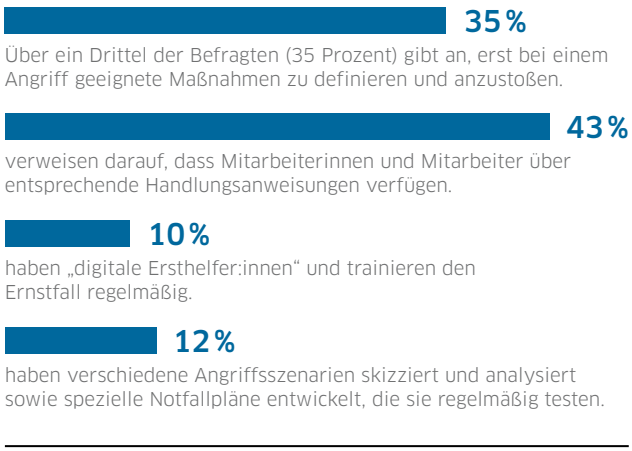
Schwachstellen in Standardsoftware: Großteil updatet regelmäßig

Wird eine Software entwickelt, kann es sein, dass im Nachhinein Schwachstellen auftauchen. Die Hersteller haben ein großes Interesse, diese zu vermeiden bzw. schnellstmöglich zu beheben. Meist geschieht dies im Zuge von Softwareaktualisierungen, die eingefordert werden. Um diese umzusetzen, müssen die Softwarenutzer:innen die Aktualisierung auch entsprechend durchführen. Doch wird Standardsoftware im deutschen Mittelstand regelmäßig aktualisiert?

27 Prozent gehen den Aktualisierungsanfragen nach, sobald die Hersteller oder die Presse über Schwachstellen berichteten. Der Großteil, knapp 60 Prozent, greift regelmäßig auf das automatische oder manuelle Aktualisieren zurück oder hat einen speziellen Informationsdienst abonniert.

Abb. 22 / DsiN-Praxisreport

Wie reagiert Ihr Unternehmen auf (mögliche) Angriffe?



Nach wie vor fehlt einem nicht zu vernachlässigenden Teil, 15 Prozent, das Bewusstsein für mögliche Schwachstellen. Es hat auch kein Paradigmenwechsel auf diesem Gebiet stattgefunden, was einen weiteren Aufklärungsbedarf aufzeigt. Denn automatisierte Softwareupdates sind schnell installiert, wenn es erst ein Bewusstsein für ihre Notwendigkeit gibt.

Richtig Handeln im Krisenfall (Reaktion)

Trotz regelmäßigen Softwareupdates und Angriffserkennungen können manche Cyberattacken nicht rechtzeitig abgewehrt werden. Doch wie reagiert man am besten in einem Schadensfall? Eine schnelle, klare Reaktion mit entsprechenden Abläufen kann weiterführende Schäden und Folgen vermeiden. Es gilt, den Regelbetrieb schnellstmöglich wiederherzustellen.

Ein Drittel ist nicht vorbereitet

Sich nicht nur präventiv auf Angriffe einzustellen, sondern auch für den Notfall vorbereitet zu sein, ist für eine umfassende IT-Sicherheit unumgänglich.

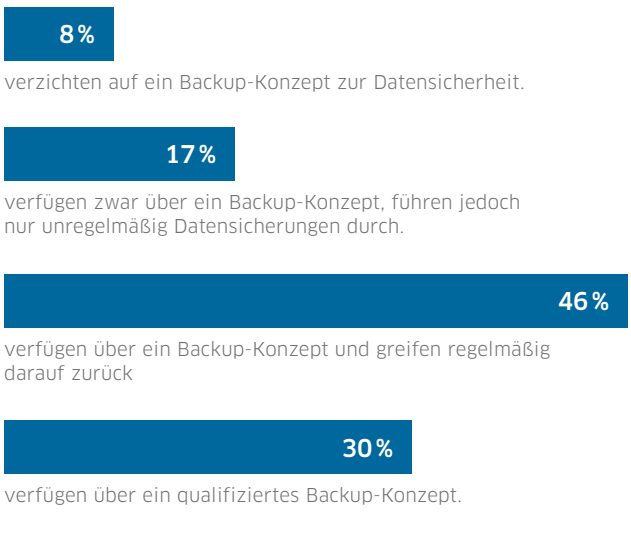
Daher sollte jedes Unternehmen den Ernstfall einmal proben bzw. ihn durchgehen. Doch sind KMU für den Worst Case gewappnet?

Idealerweise gibt es im Unternehmen Notfallpläne, die ähnlich wie in einer Brandsimulation regelmäßig getestet werden. 12 Prozent haben diese in ihrem Unternehmen implementiert. Weitere 10 Prozent haben „digitale Ersthelfer:innen", also „Feuerwehrleute", für den Ernstfall ernannt. Somit ist ein klares und strukturiertes Vorgehen im Falle eines Angriffes möglich.

Werden Maßnahmen erst beim Angriff definiert, was bei 35 Prozent der befragten KMU der Fall ist, kann es zu Zeitverlusten und groben Fehlern kommen. Angesichts der zunehmenden Vernetzung mit Zulieferern und Industrie und dadurch wachsenden Anforderungen – auch mit Blick auf die Compliance – ist eine solche Haltung als kritisch zu erachten. Es wird also auch mit Bezug auf das reaktive Verhalten ein Handlungsbedarf in Form von Aufklärung und der Erstellung von Notfallplänen deutlich.

Abb. 23 / DsiN-Praxisreport

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



Backup-Konzepte: Ein Viertel ist gar nicht oder kaum gesichert

Es kann schnell passieren: durch Sorglosigkeit, höhere Gewalt oder Cyberangriffe. Die Rede ist von Datenverlusten. Gehen Daten aufgrund technischer oder externer Einwirkungen verloren, können sie mit Hilfe eines Backups schnell wiederhergestellt werden. Datensicherungen sind daher eine effektive Einzelmaßnahme zur Schadensbegrenzung nach einem Angriff, der Datenverluste zur Folge hatte. Regelmäßige Backups und Sicherungen sind elementar für eine gelungene IT-Sicherheit. Doch führen die befragten KMU diese auch tatsächlich durch?

Seit 2018 ist die Zahl der Unternehmen mit einem qualifizierten Backup, also einer Sicherung, welche die zu sichernden Systeme, die Art der Sicherung und regelmäßige Wiederherstellungstests definiert, leicht gestiegen. Ein Viertel der befragten Unternehmen (25 Prozent) führt keine oder nur unregelmäßige Backups durch.

Angesichts der immer größeren Verbreitung von Ransomware, bei der Zugänge zu Daten gesperrt und nur im Zuge einer Lösegeldzahlung wieder freigegeben werden, ist es wichtiger denn je, dass Daten auch auf anderen Plattformen gespeichert sind. Ein Bewusstsein für die Fragilität von Daten und die Möglichkeit von Sicherungen würde die Zahl der Unternehmen mit (qualifizierten) regelmäßigen Backups erhöhen.

FAZIT

Passgenaue Angebote für mehr IT-Sicherheit

Ein umfassendes IT-Sicherheitskonzept beinhaltet eine starke Abwehr von Angriffen durch präventive Maßnahmen. Dennoch sollte auch der Ernstfall geprobt werden. IT-Notfallpläne und Schulungen zum/zur IT-Ersthelfer:in sind als reaktive Maßnahme unumgänglich. Um jedoch auch für den schlimmsten Fall, einen Verlust an Daten, gewappnet zu sein, müssen Datensicherungen stattfinden. Die Zahlen zeigen, dass Maßnahmen der Detektion und Reaktion nach wie vor erforderlich sind, insbesondere mit Bezug auf die Befähigung der Mitarbeitenden. Ein passives Verhalten im Umgang mit Schutzmaßnahmen ist grob fahrlässig.

Wie in Kapitel 2 deutlich wurde, muss hier die federführende Geschäftsleitung geschult und digital aufgeklärt werden. Alle Mitarbeitenden können etwas tun, besonders, wenn sie selbst Opfer eines Social-Engineering-Angriffes werden. Jede:r Einzelne kann entscheidend zur Abwehr von Gefahren beitragen und im Krisenfall geeignete Maßnahmen ergreifen, wenn eine entsprechende Schulung erfolgt ist.

Tipps und Angebote für die Praxis

- Der DsiN-Blog liefert Expertenbeiträge 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.
  www.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.
  www.sicher-im-netz.de/siba

KAPITEL 4

Vernetzter Alltag: IT-Sicherheit ist „Conditio sine qua non“

Digitale Innovation im Mittelstand ist heute die Grundlage für Wettbewerbsfähigkeit – somit wachsen auch die Anforderungen an IT-Sicherheit und Datenschutz. Für KMU stellen diese Transformationen eine unerwartet hohe Herausforderung dar. Zugleich nehmen die Optionen für wirksame Sicherheit im Unternehmen zu. Auch die Angebote der Cyberversicherungen wachsen, um IT-Sicherheit und ihre Risiken in den Griff zu bekommen und eine adäquate Vorsorge zu betreiben.

IT-Praxis im Fokus: Drei aktuelle Themenfelder

Die voranschreitende Digitalisierung verändert Betriebsstrukturen. Online-Verkaufsplattformen oder Cloud Computing sind effizient und sichern die eigene Wettbewerbsfähigkeit. Sie sind aber auch ein beliebtes Ziel von Cyberkriminellen. Wie vernetzt ist der deutsche Mittelstand? Wie und wo werden Waren und Güter verkauft? Und wie gut kennt sich der deutsche Mittelstand mit Cloud Computing aus? Gelebte IT-Sicherheitskultur hängt entscheidend von der Praxis ab – sowohl in technologischer als auch organisatorischer Hinsicht.

Plattformen: Handel und Vertrieb im Mittelstand

Onlinehandel und -vertrieb sind aus der heutigen Welt nicht mehr wegzudenken. Sowohl im B2B- als auch im B2C-Bereich finden sich immer mehr digitale Vertriebsstrukturen. Doch wie steht es um die damit einhergehenden Sicherheitsvorkehrungen?

Da in diesem Praxisreport branchenübergreifend befragt wurde, gaben 56 Prozent an, nichts über das Internet zu vertreiben. Die 44 Prozent, die über das Internet ihre Waren, Güter oder Dienstleistungen verkaufen, nutzen zum Großteil dafür bekannte, branchenübergreifende Vertriebsplattformen. Nur 9 Prozent bedienen sich branchenspezifischer Möglichkeiten. Doch wie sieht es beim Vertrieb über Verkaufsplattformen mit den konkreten Sicherheitsvorkehrungen aus?

Bemerkenswert ist der leichte Rückgang der durchgeführten Penetrationstests seit 2018. Immerhin führt weniger als ein Fünftel der Befragten regelmäßige Penetrationstests durch. Gerade Kleinstunternehmen ohne eigene IT-Abteilung profitieren von auf automatisierte Penetrationstests spezialisierten Dienstleistern, mit deren Hilfe sie ihre eigenen Webangebote auf Sicherheitslücken testen lassen können.

Positiv zu vermerken ist, dass 14 Prozent der befragten Unternehmen ihre Plattformen zertifizieren lassen. Immer mehr Endverbraucher:innen achten auf Gütesiegel und Absicherung. Von daher ist eine Zertifizierung nicht nur für die IT-Sicherheit von Vorteil; sie steigert über den Weg der Außenwirkung auch die Wettbewerbsfähigkeit.

Abb. 24 / DsiN-Praxisreport

Welche digitalen Verkaufsplattformen nutzen Sie – und worauf achten Sie in Bezug auf IT-Sicherheitsaspekte?

56 %
der Befragten vertreiben nichts über das Internet.

18 %
nutzen die dafür bekannten, branchenübergreifenden Vertriebsplattformen.

9 %
nutzen branchenspezifische Vertriebsplattformen.

17 %
nutzen eine eigene Vertriebsplattform.

Abb. 25 / DsiN-Praxisreport

Welche Sicherheitsmaßnahmen setzen Sie bei der Nutzung Ihrer Vertriebsplattform ein?

11 %
der befragten Unternehmen verzichten auf Sicherheitsmaßnahmen.

14 %
haben ihre Vertriebsplattform gemäß den Normen für Informationssicherheit zertifizieren lassen.

18 %
lassen regelmäßig Penetrationstests durchführen, um Schwachstellen auf ihren Vertriebsplattformen aufzudecken.

57 %
verlassen sich auf die Sicherheitsmaßnahmen des Anbieters.

Dass 11 Prozent bei der Nutzung ihrer Vertriebsplattformen auf Sicherheitsmaßnahmen verzichten, zeigt, dass hier digitale Aufklärungsarbeit notwendig ist.

Cloud im Mittelstand: immer relevanter

Mit Hilfe von Clouds können KMU Betriebsabläufe effektiv, dezentral und kostengünstig steuern. Wie umsichtig nutzt der Mittelstand daher das Cloud Computing?

Die Zahl der Unternehmen, die Cloud Computing einsetzt, ist seit 2018 um sechs Prozentpunkte gestiegen. Immer mehr Unternehmen setzen also auch hier auf digitale Strukturen, obwohl etwas mehr als die Hälfte der Befragten ihre Daten noch nicht in eine Cloud übertragen hat.

Mit den IT-Sicherheitsanforderungen haben sich von den Unternehmen mit einer Cloud lediglich 29 Prozent auseinandergesetzt. 18 Prozent haben keinen Einblick in diese oder die rechtlichen Rahmenbedingungen.

Dieses Kriterium sollte bei der Wahl eines Cloud-Anbieters eine entscheidende Rolle spielen. Standardisierte Vorgaben wie in der „Trusted Cloud“ können hier eine wichtige Orientierung bieten.

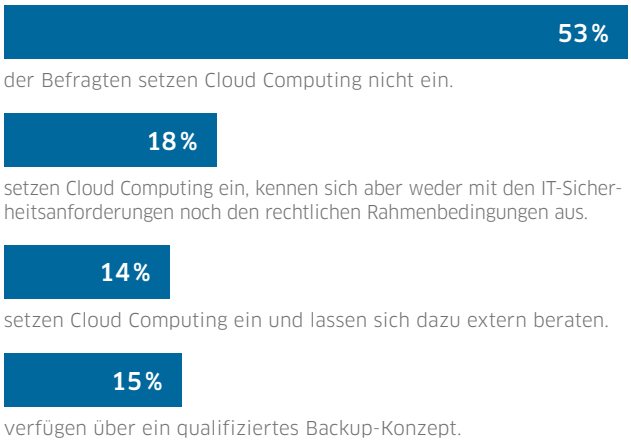
Partner und Zulieferer: immer mehr Absicherung

Gefahren lauern überall. Bedauerlicherweise entstehen Schwachstellen insbesondere an Schnittstellen zu Partnern oder Lieferanten. Ist Unternehmen dieser Umstand auch bewusst?

Immer weniger Unternehmen vertrauen ihren Lieferanten und Partnern blind. Ihre Zahl ist seit 2018 von 40 Prozent auf 31 Prozent gesunken. Demnach lässt der Großteil der befragten KMU eine Vertraulichkeitserklärung unterschreiben.

Abb. 26 / DsiN-Praxisreport

Wie sieht es mit der Nutzung von Cloud Computing aus?



Zum Teil ist dies sogar ein regelmäßig wiederholter und elementarer Teil der Zusammenarbeit.

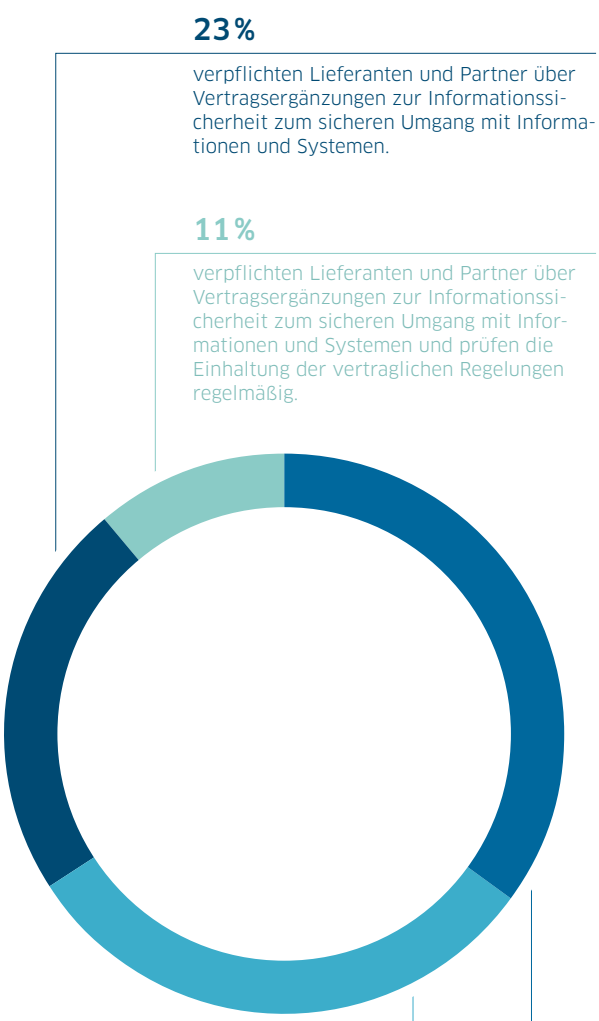
Eine vertragliche Absicherung in Form einer Vertraulichkeitserklärung schützt nicht nur die eigene IT. Sie hat darüber hinaus auch eine Strahlkraft und kann zu mehr Vertrauen in der Zusammenarbeit von Lieferanten und Partnern führen.

Cyberversicherungen für Betriebe

Die erhöhten Risiken für die Wettbewerbsfähigkeit von Unternehmen, die mit einem möglichen Ausfall oder auch der Beeinträchtigung von Systemen und Daten einhergehen, werfen die Frage nach der Art und dem Umfang eines Risikomanagements auf. Eine Möglichkeit, die mit der Digitalisierung verbundenen Risiken und sogenannte „Restrisiken“ zu managen, sind Cyberversicherungen. In welchem Umfang werden diese heute vom Mittelstand in Anspruch genommen?

Abb. 27 / DsiN-Praxisreport

Wie gehen KMU mit Lieferanten und Partnern im Hinblick auf Informationssicherheit um?



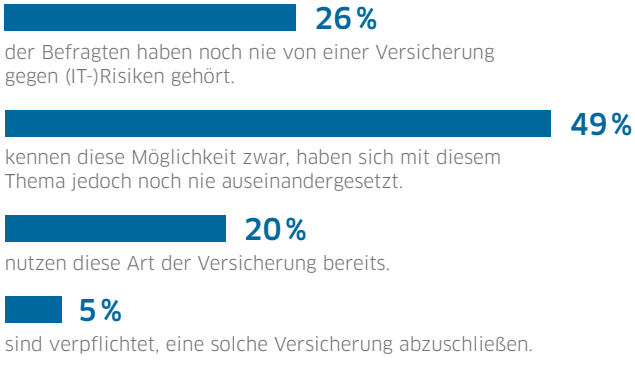
Über präventive, reaktive Maßnahmen und Backups hinaus kann man auch eine Versicherung abschließen, die einem im Falle eines Datenverlusts hilft. Wird diese Art des Risikomanagements von KMU in Deutschland als Teil der Sicherheitsstrategie in Betracht gezogen?

Immer mehr kennen die Möglichkeit der Cyberversicherung. Die Zahl derer, die davon zum ersten Mal über die Befragung erfuhren, ist seit 2018 von 31 Prozent auf 26 Prozent gesunken. Demnach ist der Großteil der Befragten über diese Option im Bilde. 5 Prozent gaben sogar an, dass sie verpflichtet sind, eine Cyberversicherung abzuschließen.

Dass es auf diesem Gebiet weiterhin Aufklärungsbedarf gibt, wird dennoch deutlich. Über das Thema Cyberversicherung muss umfassend informiert werden. Die Vorteile und Kosten müssen beleuchtet und die Konditionen dargelegt werden. So ist es ein häufiger Trugschluss, dass eine Cyberversicherung bei Fahrlässigkeit im Management oder Berufsalltag greift. Es gibt viele Möglichkeiten, sich unverbindlich zu informieren.

Abb. 28 / DsiN-Praxisreport

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



FAZIT

IT-Sicherheit gehört zum „ehrbaren Kaufmannsbild“

Unachtsamkeit, Unwissenheit oder fahrlässiges Handeln haben schwere Folgen. Schäden können Unternehmen in doppelter Weise teuer zu stehen kommen. Nachträgliche Korrekturen sind meist aufwändiger als eine direkte Implementierung von Vorkehrungen. Darüber hinaus fallen nach einem Angriff auch Kosten zur Schadensbehebung sowie möglicherweise Einbußen durch einen Reputationsverlust oder Betriebsausfall an.

Durch systematische Aufklärung zu technischen und verhaltensbedingten Vorkehrungen der IT-Sicherheit können Vorbehalte gegenüber dem Thema sowie Hemmschwellen, sich damit zu befassen, abgebaut werden. Unsicherheiten können im Dialog und auf dem Wege der Aufklärungsarbeit schnell gelöst werden. Das Aufzeigen einzelner Schwachstellen, verbunden mit einem konkreten Verweis auf Umsetzungsmöglichkeiten sowie weiterführende Hilfestellungen, ist für kleine und mittlere Unternehmen eine große Stütze auf dem Weg zu mehr IT-Sicherheit.

Tipps und Angebote für die Praxis

- TISiM bietet passgenaue Informationen aus einer Hand. Sie bündelt, bereitet praxisnah auf und vermittelt Angebote zum Thema IT-Sicherheit. Außerdem unterstützt sie kleine und mittlere Unternehmen, Handwerksbetriebe und Selbstständige bei deren Umsetzung.
  www.tisim.de

- Mit der Trusted-Cloud-Plattform und dem dazugehörigen Label erhalten Sie einen unabhängigen und transparenten Marktplatz für vertrauenswürdige Cloud Services.
  www.trusted-cloud.de

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

Drei-Punkte-Plan für IT-Schutz im Mittelstand

Vorkehrungen beim Datenschutz und bei der Cybersecurity sichern Existenzen im Mittelstand. Deshalb müssen sie zur Selbstverständlichkeit in jedem Unternehmen werden – auch für Selbstständige, Handwerker: innen, Freiberufler:innen und bei kleinen und mittleren Betrieben. Der Praxisreport 2020 zeigt, dass dieser Stand noch lange nicht erreicht ist – und der Handlungsbedarf mit der Pandemie weiter zunimmt.

Durch die Zunahme der dezentralen und ortsunabhängigen Zusammenarbeit als Folge von COVID-19 haben die einhergehenden IT-Sicherheitsfragen an Brisanz gewonnen.

1.

Kultur der IT-Sicherheit voranbringen

Positive Beispiele aus der Wirtschaft für mehr IT-Sicherheit sollten zum Vorbild für gute Unternehmensführung gemacht werden - und andere Unternehmen zu inspirieren. Denn IT-Sicherheit betrifft alle Akteure der Wirtschaft. Mit der Verschmelzung von Digitalisierung und Geschäftserfolgen sollte der Diskurs über IT-Sicherheitserfordernisse im Unternehmen zusätzlich an Fahrt gewinnen. Es ist von großer Notwendigkeit, IT-Sicherheit als Wettbewerbsvorteil zu verstehen. Sicherheit sollte daher in jedem Betrieb möglich gemacht werden, auf eine einfache Art und Weise.

2.

Kooperationsgedanke stärken

Für die Einbindung aller Betriebe muss die digitale Aufklärungsarbeit verstetigt und professionalisiert werden. Im Kern geht es um die Koordination der drei Bereiche: IT-Sicherheitsexpertise, didaktische Aufbereitung, engmaschige Verbreitung durch Befähigungs-Infrastrukturen. Bestmögliche Kooperationen und Abstimmungen vermeiden Redundanzen und fördern zusätzliche Ressourcen. So können entsprechende IT-Kompetenzen über zusätzliche Ansprechpartner:innen den Weg zum Unternehmen finden und gerade kleinere Betriebe künftig besser erreichen.

3.

Umsetzung beim KMU fördern

Um die Umsetzung von Maßnahmen zu fördern, sollte der Fokus auf die Entwicklung von Befähigungs-Infrastrukturen gelegt werden. Über sie können kleine und mittlere Unternehmen vor Ort zur Umsetzung ermuntert werden. Entsprechend können aktuelle Bedarfe bei kleinen und mittleren Unternehmen bedient werden. Befähigungs-Infrastrukturen sind dabei in einem ständigen Lern- und Entwicklungsprozess zu begreifen, die ihre Relevanz über die Reflexion aktueller IT-Sicherheitsanforderungen permanent unter Beweis stellen müssen. In diesem Zusammenspiel kann IT-Sicherheit für alle Unternehmen gelingen.

Ausblick: IT-Sicherheit in Zeiten von Corona

Die COVID-19-Pandemie stellt den deutschen Mittelstand vor neue Herausforderungen: Büroarbeitsplätze werden ins Home-Office umgesiedelt, der Vertrieb verlagert sich ins Internet, die Zusammenarbeit im Betrieb erfolgt dezentral und ortsunabhängig. Blickt man auf die im Report 2020 erfassten Monate März und April, in denen es zum ersten Lockdown kam, und vergleicht diese mit der gesamtjährlichen Situation, lassen sich bestimmte Entwicklungen während der ersten Eintrittsphase der Pandemie herauslesen und Tendenzen feststellen:

Das Engagement für IT-Sicherheit im Bereich Awareness sinkt zunächst

Mit den wirtschaftlichen Einbrüchen liegt das Augenmerk vieler kleiner und mittlerer Unternehmen zunächst nicht auf fortlaufenden IT-Sicherheitstrainings für Mitarbeiter:innen. Es stehen andere Themen im Vordergrund. Diese Reaktion widerspricht der wachsenden Relevanz für IT-Sicherheit. Denn durch den verstärkten Einsatz von IT können sich in den Übergangsphasen Cyberkriminelle die Unsicherheiten der Unternehmen zu Nutze machen. Es bleibt abzuwarten, ob diese Tendenz anhält oder nur eine vorübergehende Vernachlässigung angesichts „drängender“ Anliegen ist.

Leicht vermehrt präventive und reaktive Maßnahmen

Zugleich zeichnete sich nach dem Lockdown durch COVID-19 ein erhöhter Einsatz von ausgewählten Einzelmaßnahmen für IT-Sicherheit ab. Mehr Unternehmen gaben an, Sensoren zur Detektion im Einsatz zu haben und ihre Angriffe aktiver zu identifizieren. Auch insgesamt lag der Fokus nach COVID-19 vorwiegend auf technischen Vorkehrungen.

Mit Digitalisierung wachsen IT-Sicherheitsbedarfe

Ob sich diese ersten Tendenzen bestätigen, wird der Praxisreport 2021 zeigen. Deutlich wird bereits jetzt, dass Bedarfe für IT-Sicherheitstrainings und ein zielgruppengerechtes Angebot an passgenauen Aktionen und Maßnahmen zunehmen.

sicher-im-netz.de

Ein Handlungsversprechen von:

SAP®