Report

Cybersicherheit für KMU: Komplexität begegnen und Resilienz aufbauen

Eine weltweite Studie über Cybersicherheitsbewusstsein und Erfahrungen von KMU – sowie ein Leitfaden zur Orientierung in einer sich wandelnden Welt.

Inhaltsverzeichnis

Vorwort von Ben Aung, Chief Risk Officer bei Sage

Zusammenarbeit und klare Leitlinien können die Cybersicherheit von KMU stärken

Kleine und mittlere Unternehmen (KMU) sollten sich auf Rentabilität und Wachstum konzentrieren können, ohne dass Sorgen über Cybersicherheit den Verantwortlichen den Schlaf rauben. Die Zusammenarbeit zwischen Regierungen, Branchenverbänden, Cybersicherheitsfirmen und Technologieunternehmen ist von entscheidender Bedeutung, um Cybersicherheit für KMU zu vereinfachen und sie in die Lage zu versetzen, sich in der komplexen Landschaft von heute sicher zu bewegen und ihre Cyber-Resilienz zu verbessern.

Das Fehlen kohärenter Beratung und Leitfäden für KMU erschwert es ihnen allerdings, sich zu schützen, Mitarbeiter zu schulen und auf die richtigen Tools zuzugreifen, um sich in der komplexen Cybersicherheitslandschaft von heute zurechtzufinden.

KMU sind das Rückgrat unserer Volkswirtschaften und entscheidende Glieder der globalen Lieferketten. Die technologischen Innovationen und die Vernetzung, welche die Produktivität der Unternehmen entfesselt haben, bergen auch Risiken für die Cybersicherheit. Diese Risiken können für KMU sogar noch akuter sein.

Wenn uns das letzte Jahrzehnt etwas gelehrt hat, dann, dass es schwierig ist, Cybersicherheit zu gewährleisten. Jedes Unternehmen mit einem digitalen Fußabdruck ist ein Ziel für Cyberkriminelle, und die Größe einer Organisation schützt sie nicht davor in das Fadenkreuz der Angreifer zu geraten. Ransomware-Attacken sind nicht mehr nur großen Unternehmen vorbehalten, sondern auch viele KMU werden Opfer dieser Angriffe, die verheerende Folgen nach sich ziehen können. Aufgrund des Mangels an präzisen Daten ist es unmöglich, die tatsächlichen Auswirkungen von Ransomware auf KMU zu quantifizieren, aber unsere Untersuchungen zeigen, dass eines von vier KMU allein im letzten Jahr mehrere Cybersicherheitsvorfälle erlebt hat. Daher ist es nicht überraschend, dass KMU-Entscheider Cybersicherheit ernst nehmen. Unsere Studie zeigt auch, dass zwei Drittel bereit sind, mehr Geld auszugeben, um eine bessere Sicherheit für ihr Unternehmen zu gewährleisten. 70 Prozent der Befragten betrachten Cyberbedrohungen als ein großes Problem.

KMU-Entscheider wollen ihr Unternehmen vor Angriffen schützen – wie die Daten in diesem Report und die Gespräche mit unseren KMU-Kunden zeigen –, haben allerdings große Herausforderungen zu bewältigen. Aufgrund der im Vergleich zu größeren Unternehmen geringen Budgets müssen KMU bei ihren Investitionen in Sicherheit und Technologie Prioritäten setzen, um das beste Preis-Leistungs-Verhältnis zu erzielen.

Die wichtigsten Ergebnisse

der KMU hatten im vergangenen Jahr einen Cybersicherheitsvorfall

erwarten, dass die Investitionen in Cybersicherheit im kommenden Jahr steigen oder gleichbleiben werden

der KMU geben an, dass Cybersicherheit Teil ihrer Kultur ist, aber die meisten sprechen nur darüber, wenn sich intern etwas ändert oder schiefläuft

Diese Studie zeigt:

- Wie KMU in den wichtigsten Märkten weltweit die sich entwickelnde Cybersicherheitslandschaft erleben. 48 Prozent hatten im vergangenen Jahr einen Cybersicherheitsvorfall.
- Es herrscht ein grundlegendes, teils unangebrachtes Vertrauen in die Gewährleistung der Cybersicherheit. 76 Prozent geben an, dass sie diese regelmäßig überprüfen, obwohl 7 von 10 die Bedrohungen große Sorgen bereiten.
- Die sich ständig weiterentwickelnde Bedrohungslandschaft hält KMU-Verantwortliche nachts wach. Für mehr als die Hälfte (51%) besteht die größte Herausforderung darin, sich über neue Bedrohungen auf dem Laufenden zu halten. Die nächstgroßen Herausforderungen bestehen darin, sicherzustellen, dass die Mitarbeiter wissen, was von ihnen erwartet wird (45%), in der Aufklärung der Mitarbeiter über Cybersicherheit (44%) und den Kosten (43%).
- Es ergibt sich ein uneinheitliches Bild von Cybersicherheitskultur. Zwei Drittel sagen, Cybersicherheit sei Teil ihrer Kultur, während jedoch nur 4 von 10 regelmäßig darüber sprechen.
- KMU sind bereit, mehr in Cybersicherheit zu investieren. Sie benötigen jedoch Hilfe, um Wissens- und Bildungslücken zu schließen, und werden nach wie vor durch unwirksame und unklare Richtlinien behindert. 52 Prozent wünschen sich Unterstützung bei der Aus- und Weiterbildung.
- Sie wünschen sich diese Unterstützung von Cybersicherheitsunternehmen (56%), Regierungen (45%) und vertrauenswürdigen Technologiepartnern (43%). Entsprechende Unterstützung kann die Belastung von KMU mit begrenzten Ressourcen verringern, sich selbst zu schützen, und ermöglicht ihnen, ihre Cybersicherheitsfähigkeiten zu verbessern.

Orientierung in der Cybersicherheitslandschaft

Orientierung in der Cybersicherheitslandschaft

Fast die Hälfte der Umfrageteilnehmer war im vergangenen Jahr mit Cybervorfällen konfrontiert, was darauf hindeutet, dass die gemeldeten Vorfälle nur die Spitze des Eisbergs darstellen. Diese Unternehmen sind sich der Cyberbedrohungen, mit denen sie konfrontiert sind, sehr wohl bewusst, haben aber oft mit einer Vielzahl von Herausforderungen zu kämpfen, um sich gegenüber den gefühlt jede Woche neu auftauchenden Schwachstellen und Risiken zu wappnen.

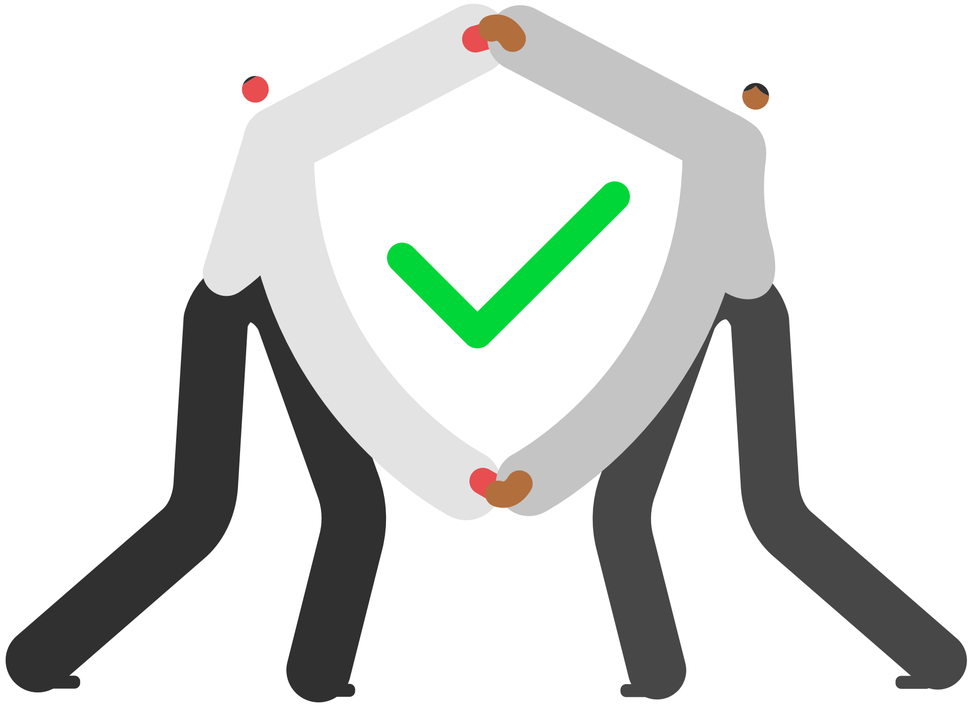
Die größte Herausforderung besteht für KMU darin, sich über neue Bedrohungen auf dem Laufenden zu halten. Das trifft auf insgesamt 51 Prozent der KMU zu und auf 54 Prozent der KMU im Vereinigten Königreich. Weitere Herausforderungen bestehen darin, sicherzustellen, dass die Mitarbeiter wissen, was von ihnen erwartet wird (45%), in der Aufklärung der Mitarbeiter über Cybersicherheit (44%) und den Kosten (43%). Diese Statistiken unterstreichen, dass ein erheblicher Teil der KMU zwar erkennt, dass sie bedroht sind, aber nicht unbedingt weiß, was dagegen zu tun ist. KMU brauchen Hilfe, um bei all den Informationen über neue Bedrohungen die relevanten von den irrelevanten zu unterscheiden, ergänzt durch einfache, praktische Ratschläge, die es ihnen ermöglichen, sich auf das zu konzentrieren, was für den Erfolg ihres Unternehmens relevant ist.

der KMU hatten im vergangenen Jahr mehr als einen Cybersicherheitsvorfall zu verzeichnen

besteht die größte Herausforderung darin, mit neuen Bedrohungen Schritt zu halten

Cybersicherheit für KMU voranbringen

Cybersicherheit für KMU voranbringen



Wir müssen Cybersicherheit menschlich betrachten. Unser Ziel ist es, das Thema zu vereinfachen, zu entmystifizieren und KMU die Angst vor dem zu nehmen, was sie oft als komplex und beängstigend wahrnehmen. **Auf diese Weise befähigen wir sie, Cybersicherheit in ihre alltäglichen Aktivitäten und Gespräche zu integrieren**, Cyberresilienz gegenüber Cyberbedrohungen aufzubauen und ihre Unternehmen zukunftssicher zu machen.

Sophia Adhami
Leiterin Cyber Security Engagement bei Sage

KMU haben oft nur begrenzte IT-Ressourcen bei konkurrierenden Anforderungen. Ohne eine zweckdienliche Anleitung und Unterstützung ist es für sie wesentlich schwieriger, fundierte Risikomanagement-Entscheidungen darüber zu treffen, wo sie investieren und mit welchen Risiken sie je nach Branche und Geschäftsumfeld leben können. Vielen wird nicht klar sein, wie eine kleine Anzahl sorgfältig durchdachter Cybersicherheitskontrollen dazu beitragen kann, die große Mehrheit der Angriffe einzudämmen, denen sie ausgesetzt sind. Es heißt oft, bei der Cybersicherheit gehe es darum, „die grundlegenden Maßnahmen richtig umzusetzen“, aber worin diese „grundlegenden Maßnahmen“ bestehen, wird oft missverstanden. KMU müssen entscheiden, welche Basis-Kontrollen für sie richtig sind. Dafür ist eine Kombination aus internem Wissen und externer Beratung erforderlich.

Cybersicherheitsgrundlagen

19 Prozent der KMU verlassen sich ausschließlich auf das, was sie als grundlegende Kontrollen betrachten. Allerdings kann selbst das, was wir als „grundlegende“ Cybersicherheitsmaßnahmen bezeichnen, komplex umzusetzen sein.

Fundamentale Aspekte der Cybersicherheit – wie das Patchen von Systemen, Erstellung von Sicherungskopien von Daten, Zugriffskontrollen, Zwei-Faktor-Authentifizierung, die Inventarisierung aller Geräte und das Monitoring – können immer noch spezielle Fähigkeiten und Tools für Implementierung und Betrieb erfordern.

Es ist bemerkenswert, dass 46 Prozent der KMU keine Firewall einsetzen, obwohl 84 Prozent behaupten, damit vertraut zu sein. Weltweit vernachlässigen 42 Prozent die Sicherung kritischer Daten. Interessanterweise sind britische KMU (62%) in dieser Hinsicht sorgfältiger als ihre US-amerikanischen Pendants (55%).

Viele KMU zeigen sich vom Cybersicherheitsjargon überfordert. Begriffe wie „Ende-zu-Ende-Verschlüsselung“, „Ransomware“, „Bring Your Own Device (BYOD)“ und „Endpoint Detection“ werden im KMU-Bereich am schlechtesten verstanden.

KMU müssen verstehen, wie man grundlegende Maßnahmen auswählt und wirksam einsetzt. Und sie müssen wissen, wann und wie man sie durch fortschrittlichere Kontrollen ergänzt.

19%

der KMU verlassen sich auf Basis-Kontrollen

58%

der KMU erstellen eine Sicherungskopie ihrer Daten

Remote-Work-Szenarien absichern

KMU erkennen die Notwendigkeit, in der heutigen heterogenen Landschaft Geschäftsabläufe schützen zu müssen, die außerhalb der herkömmlichen Arbeitsplatzumgebung stattfinden.

73 Prozent nutzen Systeme, die sicheres Arbeiten von zu Hause ermöglichen. 63 Prozent greifen dafür auf andere Systeme als in ihrer Büroumgebung zurück. In Ermangelung spezieller IT- oder Cybersicherheitsexperten bestehen berechtigte Bedenken hinsichtlich der Fähigkeit von KMU, die spezifischen Cybersicherheitsrisiken beim mobilen Arbeiten zu bewältigen.

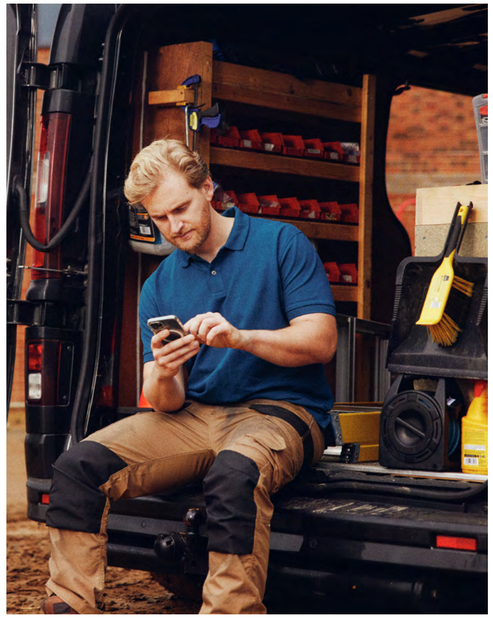
Während 82 Prozent irgendeine Form von Sicherheitskontrolle eingeführt haben, überwachen nur 57 Prozent die Sicherheit beim mobilen Arbeiten genau. Von denjenigen, die über einen Plan oder ein Verfahren zur Bewältigung von Risiken beim mobilen Arbeiten verfügen, geben 25 Prozent zu, dass dieser Plan bzw. dieses Verfahren nicht durchgängig befolgt wird. Beachtliche 71 Prozent der KMU in den USA überwachen die Sicherheit beim mobilen Arbeiten genau, deutlich mehr als im weltweiten Durchschnitt. Im Vereinigten Königreich unterscheiden jedoch nur 57 Prozent zwischen der Sicherheit im Büro und der Sicherheit beim mobilen Arbeiten – eine Zahl, die deutlich unter den 78 Prozent der französischen KMU liegt.

82%

der KMU verfügen über Maßnahmen, um die Risiken durch Mitarbeiter zu reduzieren, die sich von außen in das Unternehmensnetz einloggen

25%

derjenigen, die über solche Maßnahmen verfügen, geben zu, dass sich nicht alle daran halten



Förderung einer proaktiven Cybersicherheitskultur

Förderung einer proaktiven Cybersicherheitskultur

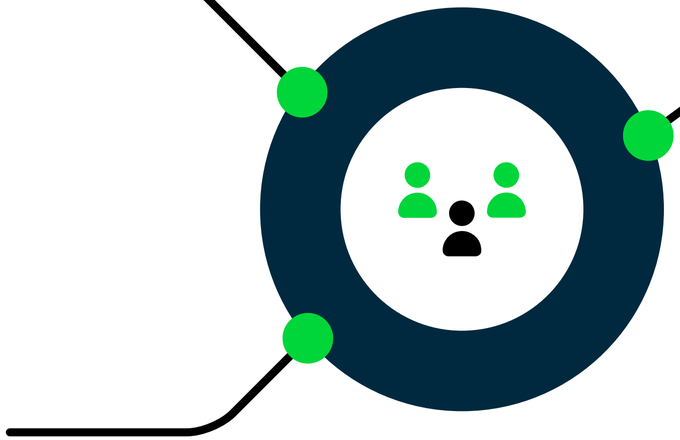
Große Unternehmen haben schon lange verstanden, dass die Absicherung eines Unternehmens eine solide Cybersicherheitskultur erfordert, die die technischen Kontrollen ergänzt. Wenn sie gut umgesetzt wird, kann eine am Menschen orientierte Cybersicherheitsstrategie – bei der Unternehmen ihre Mitarbeiter befähigen und darauf vertrauen, dass sie die richtigen Sicherheitsentscheidungen treffen – den Bedarf an teuren oder aufwändigen Sicherheitskontrollen tatsächlich ersetzen. Bei KMU scheint es jedoch eine Diskrepanz zwischen ihrer Vorstellung von einer guten Sicherheitskultur und den tatsächlichen Praktiken in ihren Unternehmen zu geben.

Zwei Drittel der KMU sind der Meinung, dass die Cybersicherheit in ihrer Unternehmenskultur verankert ist. Besonders deutlich ist dies bei südafrikanischen, australischen und US-amerikanischen KMU. Allerdings sprechen nur 4 von 10 KMU routinemäßig über Cybersicherheit. 16 Prozent adressieren das Thema erst, wenn etwas schiefgelaufen ist. 11 Prozent der Kleinstunternehmen geben zu, dass sie überhaupt nie über Cybersicherheit sprechen.

Es gibt zahlreiche budgetfreundliche Möglichkeiten für KMU, ihre Cybersicherheitskultur zu verbessern: Klare Vorgaben von oben und Führungskräfte, die mit gutem Beispiel vorangehen, der Einsatz von Schulungsinstrumenten, um die Kenntnisse zu erweitern, Dinge für die Mitarbeiter so einfach und intuitiv wie möglich gestalten (insbesondere das Melden von verdächtigen Nachrichten wie Phishing-E-Mails) und einfach regelmäßig über Cybersicherheit sprechen. All diese Dinge machen einen großen Unterschied und verringern das Stigma der Komplexität von Cybersicherheit.

Zwei Drittel

der KMU geben an, dass Cybersicherheit Teil ihrer Unternehmenskultur ist



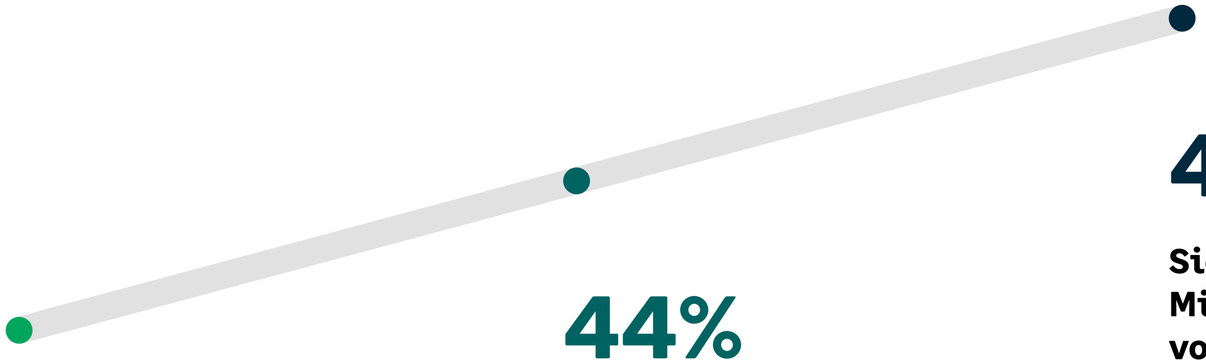
4 von 10

KMU sprechen regelmäßig über Cybersicherheit

16%

diskutieren nur über Cybersicherheit, wenn etwas schief läuft

Die gängigsten Cybersicherheitsherausforderungen



43%

Verstehen, welche Art von Sicherheit erforderlich ist

44%

Mitarbeiter in Sachen Cybersicherheit schulen

45%

Sicherstellen, dass Mitarbeiter wissen, was von ihnen erwartet wird

In der heutigen digitalen Welt sind Cybersicherheitshürden für Unternehmen wie das unsere eine ständige Realität. Wir sind täglich mit Datenschutzverletzungen, Phishing-Versuchen und Ransomware-Angriffen konfrontiert – es ist ein Labyrinth da draußen. Für ein kleines Unternehmen ist es eine echte Herausforderung, Sicherheit und Wachstum unter einen Hut zu bringen. Die Cyberwelt ist ein Rätsel, das wir nicht ignorieren können. Es geht darum, sich zu schützen und gleichzeitig weiterzuentwickeln, und wir müssen Lösungen finden, die zu unserer Größe passen. Auf diesem Weg ist die Unterstützung durch Technologieunternehmen und staatliche Stellen von entscheidender Bedeutung. Mit ihrer Hilfe können wir uns in dieser komplizierten Landschaft mit mehr Zuversicht bewegen.

Lynne Pace
CFO & VP of Finance bei Danson Construction

Bereit für Cybersicherheit

Bereit für Cybersicherheit

Cybersicherheit erfordert laufende Investitionen – es gibt keine Patentrezepte oder Allheilmittel. In zunehmendem Maße wird Cybersicherheit in Technologien wie Cloud-Ressourcen oder Betriebssysteme „eingebaut“, und neue Technologien wie KI-Tools sind sehr vielversprechend, bringen aber auch potenziell neue Risiken und Kosten mit sich. Um effektiv zu sein und den Cyberbedrohungen einen Schritt voraus zu bleiben, müssen Unternehmen aller Größenordnungen ihre Investitionen sorgfältig planen. Das bedeutet häufig, das Ausgabenniveau beizubehalten oder zu erhöhen. Gleichzeitig suchen Unternehmen nach Möglichkeiten, ein gutes Sicherheitsniveau auf effizientere Weise zu erzielen.

Dies schlägt sich in unserer Studie nieder, aus der hervorgeht, dass überwältigende 91 Prozent der KMU davon ausgehen, dass ihre Investitionen in die Cybersicherheit im nächsten Jahr steigen oder gleichbleiben werden. Vor allem bevorzugen KMU Anbieter, die der Sicherheit Priorität einräumen. Beachtliche 68 Prozent wählten einen teureren Anbieter, wenn dieser ein höheres Maß an Sicherheit nachweisen konnte und die Datenschutz- und Sicherheitsaspekte seines Angebots transparent kommunizierte.

In dem Bemühen, Wissenslücken zu schließen und die Zuversicht zu stärken, fordern KMU aktiv Unterstützung – vor allem von staatlichen Stellen – bei der Aus- und Weiterbildung zur Cybersicherheit. Nur 6 Prozent der KMU rechnen mit einem Rückgang ihrer Investitionen in die Cybersicherheit. Für 44 Prozent dieser Unternehmen beeinflussen wirtschaftliche Unsicherheit und steigende Lebenshaltungskosten ihre Ausgaben für Cybersicherheit. Interessanterweise beobachten 29 Prozent eine Verbesserung der Bedrohungslage in diesem Jahr. Frankreich, Spanien und Kanada sind die Länder, in denen die meisten KMU einen Rückgang ihrer Investitionen in die Cybersicherheit erwarten.

a **91% der KMU erwarten, dass die Investitionen in Cybersicherheit im nächsten Jahr steigen oder gleichbleiben werden**

b **68% wählten einen teureren Anbieter, wenn dieser ein höheres Maß an Sicherheit nachweisen konnte**

c **64% oder KMU nutzen eine Cyberversicherung – 74% planen, sie im nächsten Jahr zu nutzen**

d **52% wünschen sich mehr Unterstützung bei Aus- und Weiterbildung in Sachen Cybersicherheit**

e **44% geben an, dass wirtschaftliche Unsicherheit/ gestiegene Lebenshaltungskosten die Budgets für Cybersicherheit reduziert haben**

Cyberkriminalität ist heutzutage eine echte Bedrohung für kleine und mittelständische Unternehmen. Ihre digitale Präsenz kann zu einer potenziellen Schwachstelle innerhalb der Lieferkette werden. Die Abhängigkeit von großen Lieferanten und staatlichen Behörden erfordert ein gemeinsames Vorgehen. Gleichzeitig bietet die Bewältigung dieser Herausforderungen auch eine einzigartige Gelegenheit, sich einen deutlichen Wettbewerbsvorteil zu verschaffen, indem der Ruf eines Unternehmens verbessert und Vertrauen aufgebaut wird.

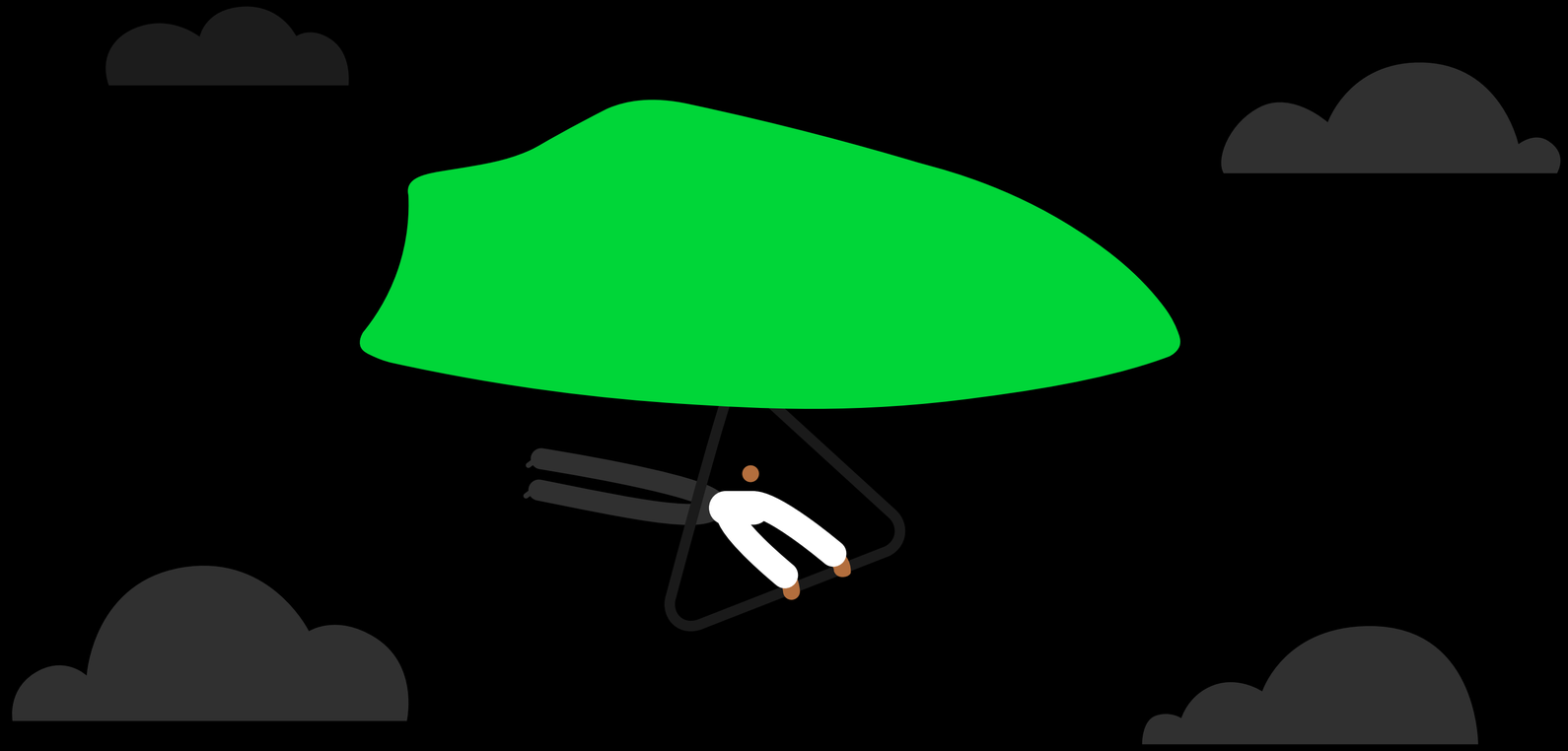
Simon Borwick
Cyber Security Partner bei PwC UK

Schlussfolgerung

KMU bemühen sich aktiv um die Cybersicherheit ihres Unternehmens. Aber sie sehen sich praktisch auf Schritt und Tritt mit Herausforderungen konfrontiert. Diese Hürden reichen von komplexen Ratschlägen, die nicht auf ihre Risiken und Bedürfnisse zugeschnitten sind, bis hin zu mangelnder Unterstützung durch staatliche Stellen und Technologiepartner. So wissen sie nicht, welche Lösungen für sie geeignet sind, oder können sie aufgrund begrenzter Kenntnisse und Ressourcen nicht umsetzen.

Größere Unternehmen und Behörden müssen es KMU erleichtern, zuverlässige Cybersicherheit „out of the box“ zu nutzen, und dazu beitragen, den Mitarbeitern ihre wirtschaftliche Bedeutung verständlich zu machen.

Zu verstehen, wie man die „grundlegenden“ Kontrollen durch den Einsatz der richtigen technischen Services, z.B. die Cloud, optimiert, kann die Belastung für Unternehmen mit knappen Ressourcen verringern. Durch die Bereitstellung sicherer Software, gezielte Beratung und die Vermittlung von Kenntnissen können KMU die Cybersicherheit in den Geschäftsalltag integrieren und sich auf ihr Wachstum konzentrieren.



Länderspezifische Informationen

Vereinigtes Königreich, USA, Frankreich, Deutschland, Portugal, Spanien, Südafrika, Kanada und Australien

Vereinigtes Königreich

Kultur und Anwendungsbereiche verbesserungswürdig

KMU im Vereinigten Königreich meldeten die wenigsten Cybersicherheitsvorfälle in den letzten zwölf Monaten (42% meldeten einen). Dies steht im erheblichen Gegensatz zu Frankreich (60%) und Deutschland (55%).

Allerdings scheinen sie bei der Umsetzung von Maßnahmen zum Schutz von mobilem Arbeiten hinter anderen Ländern zurückzubleiben. Nur 57 Prozent haben unterschiedliche Richtlinien für mobiles Arbeiten und Büroarbeit eingeführt, verglichen mit 78 Prozent in Frankreich. Dies macht sie anfällig für die besonderen Bedrohungen, die mit dem mobilen Arbeiten verbunden sind, z. B. ungeschützte WiFi-Verbindungen.

Vielleicht ist dies ein Grund dafür, dass mehr KMU im Vereinigten Königreich (54%) als im weltweiten Durchschnitt (51%) es als größte Herausforderung ansehen, den neuesten Bedrohungen zuvorzukommen, dass sich mehr Unternehmen Unterstützung bei der Aus- und Weiterbildung wünschen (57% gegenüber 52% weltweit), und dass etwas weniger Unternehmen die Cybersicherheit als Teil ihrer Kultur betrachten (67% gegenüber 69% weltweit).

57%

der KMU im Vereinigten Königreich haben unterschiedliche Richtlinien für Büro und Homeoffice

Vereinigte Staaten

Raum für Verbesserung bei „Cyber-Motivation“

Mehr als drei Viertel der KMU in den USA sind der Meinung, dass Cybersicherheit Teil ihrer Unternehmenskultur ist – deutlich mehr als der weltweite Durchschnitt von 69 Prozent. Zudem nutzen US-KMU am ehesten eine Cyberversicherung (67%). Dies deckt sich mit der Aussage von 77 Prozent, dass sie aktiv in Cybersicherheitsmaßnahmen für ihr Unternehmen investieren, und erklärt, warum diese Gruppe die größte Zuversicht zeigt, dass kleine Unternehmen Cybersicherheit ernst nehmen.

Obwohl mehr US-KMU regelmäßig über Cybersicherheit diskutieren als der weltweite Durchschnitt (45% gegenüber 40%), gibt es noch Raum für Verbesserungen, um sicherzustellen, dass die Mitarbeiter motiviert und geschult sind, Angriffe zu bekämpfen.

Wenn es um spezifische Cybersicherheitsherausforderungen geht, werden die größten Herausforderungen darin gesehen, sich über neue Bedrohungen auf dem Laufenden zu halten (49%) und die Mitarbeiter in puncto Cybersicherheit zu informieren (43%). Dieser befund steht im Einklang mit den weltweiten Daten.

76%

der US-KMU stimmen zu, dass Cybersicherheit Teil ihrer Kultur ist

Kanada

Identifizierung von Bedrohungen höchste Priorität

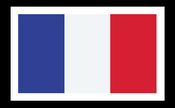
Weniger KMU in Kanada nutzen unterschiedliche Sicherheitsvorkehrungen für Mitarbeiter im Büro und zu Hause. Kanada ist – neben Frankreich und Spanien – eines der Länder, in denen der höchste Prozentsatz der KMU erwartet, dass die Investitionen in Cybersicherheit in den nächsten zwölf Monaten zurückgehen werden.

Dabei wünschen sich nur 48 Prozent mehr Unterstützung bei Aus- und Weiterbildung zur Cybersicherheit – was auf eine Diskrepanz zwischen Herausforderung und möglicher Lösung hindeutet.

Kanada liegt auch leicht unter dem weltweiten Durchschnitt derjenigen KMU, die Cybersicherheit als Teil ihrer derzeitigen Kultur betrachten. 63 Prozent der kanadischen Unternehmen stimmen dem zu, im Vergleich zu 69 Prozent weltweit.

59%

der kanadischen KMU haben unterschiedliche Richtlinien für Büroarbeit und mobiles Arbeiten



Frankreich

Erklären fehlende Investitionen mangelnde Besorgnis?

Neben spanischen sind französische KMU am zuversichtlichsten (82%), was das Management ihrer Cybersicherheit angeht. Und sie haben Schritte unternommen, um die Arbeit im Homeoffice zu regeln: 72 Prozent haben unterschiedliche Richtlinien für die Arbeit von zu Hause und im Büro.

Sie sehen es auch am wenigsten als Herausforderung an (39%), sich über neue Bedrohungen auf dem Laufenden zu halten (gegenüber 51% weltweit), und setzen weniger grundlegende Kontrollen ein als KMU in anderen Ländern. Nur 50 Prozent geben an, dass sie eine Cyberversicherung nutzen, wobei 8 Prozent die Kosten als abschreckenden Faktor nennen.

Dies ist ein besorgniserregender Trend, weil 60 Prozent der französischen KMU im vergangenen Jahr Vorfälle gemeldet haben und mehr KMU in Frankreich als in jedem anderen Land außer Spanien erwarten, dass sie ihre Investitionen in die Cybersicherheit in Zukunft verringern werden.

39%

der französischen KMU geben an, dass es eine Herausforderung ist, mit neuen Cyberbedrohungen Schritt zu halten

Spanien

Geringste Wahrscheinlichkeit, über Cybersicherheit zu sprechen

Knapp drei Viertel (73%) der KMU in Spanien geben an, dass sie sich nicht regelmäßig mit dem Thema Cybersicherheit auseinandersetzen, der geringste Wert aller Länder. Dies steht im Widerspruch zu ihrer festen Überzeugung (71%), dass Cybersicherheit Teil ihrer Kultur ist.

Spanische KMU sind auch zufriedener mit dem Niveau des angebotenen Cybersicherheits-Supports als andere Länder: 45 Prozent der Befragten wünschen sich mehr Unterstützung im Vergleich zu 52 Prozent weltweit. Neben Frankreich erwarten jedoch auch hier mehr KMU als anderswo, dass sie ihre Investitionen in die Cybersicherheit verringern werden. Dadurch wird es schwieriger, mit neuen Bedrohungen Schritt zu halten und die Mitarbeiter zu schulen – die beiden größten Herausforderungen in dem Land.

27%

der spanischen KMU diskutieren regelmäßig über Cybersicherheit

Deutschland

Kontrast zwischen Anzahl der Vorfälle und Kenntnis/Besorgnis

55% der KMU in Deutschland meldeten im vergangenen Jahr mindestens einen Cybersicherheitsvorfall. Nur französische KMU meldeten mehr. Die Statistiken deuten darauf hin, dass Schulung und Unterstützung verbessert werden müssen, um die Anzahl der Vorfälle zu verringern.

Deutsche KMU überprüfen ihre Cybersicherheit am wenigsten (68% gegenüber 76% im weltweiten Durchschnitt), sind am wenigsten besorgt (54%) und 20 Prozent haben keine Pläne, eine Cyberversicherung abzuschließen. Sie haben auch ein geringeres Verständnis von Cyberbegriffen wie „Ransomware“ (60% wissen nicht, was damit gemeint ist).

Dies erklärt vielleicht, warum nur 41 Prozent es als eine Herausforderung ansehen, mit neuen Bedrohungen Schritt zu halten.

68%

der deutschen KMU überprüfen ihre Cybersicherheit regelmäßig

Portugal

Wunsch nach Unterstützung bei Schulung und Rekrutierung

Mehr als die Hälfte der portugiesischen KMU ist der Ansicht, dass die Schulung der Mitarbeiter in Fragen der Cybersicherheit ihre größte Herausforderung ist – weit mehr als der weltweite Durchschnitt von 44 Prozent.

Sie konstatieren auch verschiedene Lücken bei Qualifikation und operativen Abläufen. 40 Prozent geben zu, dass sie Schwierigkeiten haben, Mitarbeiter mit Cybersicherheitskenntnissen zu rekrutieren, 56 Prozent sind sich nicht sicher, ob ihre Zulieferer sicher arbeiten, und Portugal hat das geringste Vertrauen (46%), dass kleine Unternehmen die Cybersicherheit ernst nehmen.

Da nur etwa zwei Drittel der portugiesischen KMU selbst in Cybersicherheitsmaßnahmen investieren, muss diese Unterstützung sich möglicherweise aus externen Quellen und Richtlinien speisen. Mit 71 Prozent der portugiesischen KMU, die Cybersicherheit als Teil ihrer Unternehmenskultur betrachten, scheint eine derartige Unterstützung willkommen.

Fur

55%

der portugiesischen KMU ist die Schulung der Mitarbeiter in Sachen Cybersicherheit die größte Herausforderung

Südafrika

Aus- und Weiterbildung höchste Priorität

Trotz oder gerade wegen der hohen Investitionen in Cybersicherheitsmaßnahmen fordern die südafrikanischen KMU eine bessere Aus- und Weiterbildung über Cybersicherheit – ein Zeichen für die Komplexität derzeitige Leitfäden und Richtlinien sowie die Notwendigkeit, das Bewusstsein für Schulungsmöglichkeiten zu schärfen. Die Zahl derjenigen, die sich mehr Unterstützung wünschen (69%), ist ein dramatischer Ausreißer im Vergleich zum weltweiten Durchschnitt von 52 Prozent.

Es überrascht daher nicht, dass 55 Prozent der Befragten die Ausbildung der Mitarbeiter als größte Herausforderung ansehen – auch dies liegt deutlich über dem weltweiten Durchschnitt von 44 Prozent.

Interessanterweise war der häufigste in Südafrika gemeldete Cybersicherheitsvorfall der Diebstahl von Laptops. Ransomware-Angriffe wurden hingegen seltener gemeldet (9%) als im weltweiten Durchschnitt (13%).

69%

der südafrikanischen KMU wünschen sich mehr Unterstützung bei der Aus- und Weiterbildung

Australien

Cybersicherheitskultur ist Gemeingut

Drei Viertel der australischen kleinen und mittleren Unternehmen sind der Meinung, dass Cybersicherheit Teil ihrer Unternehmenskultur ist, im Vergleich zu 69 Prozent weltweit.

Trotzdem oder gerade deshalb wünschen sie sich mehr Unternehmen KMU-Unterstützung bei Aus- und Weiterbildung. Damit liegen australische KMU weltweit an zweiter Stelle und über dem globalen Durchschnitt von 52 Prozent. Dies könnte auch erklären, warum mehr (57%) als der weltweite Durchschnitt (51%) es als größte Herausforderung ansehen, über die neuesten Bedrohungen auf dem Laufenden zu bleiben.

Auch die Schulung der Mitarbeiter ist für mehr australische KMU ein Anliegen (48%) als für den weltweiten Durchschnitt (44%).

75%

der australischen KMU betrachten Cybersicherheit als Teil ihrer Kultur

Methodik

Sages Untersuchung wurde von dem unabhängigen Marktforschungsunternehmen Danebury Research zwischen dem 4. und dem 15. April 2023 mittels 2.100 Online-Interviews mit Entscheidungsträgern in kleinen und mittleren Unternehmen mit 9 bis 499 Mitarbeitern durchgeführt. Die 2.100 Interviews umfassten neun Länder: Vereinigtes Königreich, USA, Frankreich, Deutschland, Portugal, Spanien, Südafrika, Kanada und Australien.

Land	Stichprobengröße
Vereingtes Königreich	500
USA	500
Frankreich	100
Deutschland	100
Portugal	100
Spanien	100
Südafrika	100
Kanada	500
Australien	100

Über Sage

Sage hat es sich zur Aufgabe gemacht, Barrieren zu beseitigen, damit jeder erfolgreich sein kann. Dies gilt vor allem für die Millionen kleinen und mittelständischen Unternehmen, die von Sage und seinen Partnern betreut werden. Kunden vertrauen unseren IT-Systemen, die für mehr Transparenz sowie flexiblere und effizientere Abläufe in den Bereichen Buchhaltung, Unternehmens- und Personalmanagement sorgen. Durch die Digitalisierung von Geschäftsprozessen sowie von Beziehungen zu Kunden, Lieferanten, Mitarbeitern, Banken und Behörden bringt unser digitales Netzwerk kleine und mittlere Betriebe näher zusammen. Unternehmen kommen damit auch schneller an relevante Informationen und können Geschäftsabläufe reibungsloser gestalten. Barrieren abzubauen, bedeutet für Sage auch, dass das Unternehmen eigene Ressourcen wie Zeit, Technologie und Erfahrung nutzt, um digitale wie wirtschaftliche Ungleichheit sowie die Klimakrise zu bekämpfen.

Über Danebury Research

Danebury Research ist ein globales Full-Service-Marktforschungsunternehmen mit Sitz in Stockbridge, Hampshire. Es arbeitet sowohl mit Agenturen und Kunden auf globaler Ebene zusammen. Mit dem Zugang zu einem Panel von über 200 Millionen potenziellen Teilnehmern hat sich Danebury Research der Aufgabe verschrieben, mutige Entscheidungen durch die Bereitstellung von zuverlässigen, genauen und repräsentativen Daten zu unterstützen. Zu den von Danebury Research angebotenen Dienstleistungen gehören Marktforschung, Markenforschung, Umfragen zur Kundenzufriedenheit, Mitarbeiterbefragungen und PR-Umfragen.

Weitere Informationen über Danebury Research und seine Marktforschungsdienste finden Sie auf der Website des Unternehmens: **www.daneburyresearch.com**.

Sage

sage.com