Cybersicherheit für kleine Unternehmen

McAfee-Ressourcenleitfaden

Inhalt

Einführung 3

Identifizierung der Risiken 4

Länderstatistiken 5

Sensibilisierung und Vorbereitung 6

Situation in einzelnen Ländern 7

Lösungsvorschläge 8

McAfee Business Protection 12

Über diese Studie 13

Ist Ihr Unternehmen vorbereitet? Ein Leitfaden zur Cybersicherheit für kleine Unternehmen

In den Nachrichten wird Cyberkriminalität oft als ein Problem für große Konzerne dargestellt, die Opfer von Ransomware oder Datenkompromittierungen werden. In Wirklichkeit ist diese Bedrohung in der Welt der KMU jedoch genauso präsent.

Aufgrund der zunehmenden Verfügbarkeit von Standard-Hacking-Tools, die den Einstieg für alle mit böswilligen Absichten erleichtern, erfolgen mittlerweile immer mehr Angriffe auf Unternehmen mit einem Jahresumsatz von 500.000 USD oder weniger.

Große Unternehmen können die durch Cyberkriminalität entstandenen Kosten meist problemlos schultern. Für kleine Unternehmen können solche Angriffe jedoch verheerend sein, da sie über keine soliden Abwehrmaßnahmen verfügen und somit leicht angreifbar sind. Im Durchschnitt werden bei einem E-Mail-Angriff auf Unternehmen (in der Regel durch gezieltes Phishing oder gehackte Konten) 125.611 USD erbeutet. Ransomware-Angreifer nehmen Unternehmensdaten für durchschnittlich 14.403 USD als Geiseln, und bei Datenlecks entsteht ein durchschnittlicher Verlust von 164.336 USD.

Auf der Grundlage einer weltweiten Umfrage unter 700 Geschäftsinhabern und IT-Fachleuten hat McAfee diesen Leitfaden erstellt, um Führungskräfte in Kleinunternehmen (mit weniger als 100 Beschäftigten) über diese wachsende Bedrohung zu informieren und ihnen die Werkzeuge an die Hand zu geben, mit denen sie ihre Mitarbeiter, Kunden und die Firma selbst schützen können.

Die Bedrohung durch Cyberkriminelle nimmt zu – ein Anlass zur Sorge für KMU

Viele Kleinunternehmen haben große Angst davor, gehackt zu werden, Geschäftsunterbrechungen zu erleiden oder aufgrund von Cyberkriminalität das Vertrauen ihrer Kunden zu verlieren.

Von 73 % der befragten Unternehmen wurde die Cybersicherheit als eines ihrer größten Risiken oder Schwachstellen genannt – und 24 % der befragten Inhaber und IT-Fachleute gaben an, dass sie sich täglich Sorgen über Cyberangriffe machen.

Diese Befürchtungen sind nur allzu berechtigt. Die Daten zeigen, dass Cyberangriffe auf dem Vormarsch sind: 44 % der befragten Kleinunternehmen wurden bereits einmal von einem Angriff getroffen, 17 % sogar mehrmals. Bei 67 % dieser betroffenen Unternehmen fand der Angriff in den letzten zwei Jahren statt, was darauf hindeutet, dass die Bedrohung durch Cyberkriminalität immer größer wird.

Für ein kleines Unternehmen kann selbst ein einziger Vorfall verheerende Auswirkungen auf das Geschäftsergebnis haben. Bei 61 % der Kleinunternehmen, die einen Cyberangriff erlebten, belief sich der damit verbundene Verlust auf mehr als 10.000 USD. Die Mehrheit der befragten Geschäftsinhaber und IT-Fachleute (60 %) gab an, dass sie und/oder ihre Mitarbeiter und Kollegen auch physisch oder psychisch durch den Angriff belastet wurden. In 58 % der Fälle dauerte es länger als eine Woche, um die IT-Probleme infolge des Angriffs zu lösen – ein Verlust wertvoller Geschäftszeit.

Das Hauptziel bei KMU sind Daten

- Mit der zunehmenden Vernetzung und Digitalisierung von Kleinunternehmen sammeln sich Datenbestände an, die für Hacker attraktiv sind.
- Fast die Hälfte der befragten Geschäftsinhaber/IT-Fachleute (46 %) sagen, dass der Verlust von Daten ihre größte Sorge ist.
- Diejenigen, die Opfer eines Cyberangriffs wurden, verloren in den meisten Fällen Kundendaten (38 %), Kennwörter (34 %) oder sonstige Dateien (34 %).

KMU-Inhaber fühlen sich über die Bedrohung durch Cyberkriminalität gut informiert …

Die meisten Unternehmer sind sich des Risikos bewusst, das Cyberkriminalität für ihren Betrieb darstellt. Laut unserer Umfrage sind 69 % der befragten Geschäftsinhaber und IT-Fachleute der Meinung, dass sie über ausreichend Kenntnisse verfügen, um Entscheidungen zur Cybersicherheit in ihrem Unternehmen zu treffen.
Im Allgemeinen sind sie sich darüber im Klaren, dass sie mit Bedrohungen rechnen und in deren Eindämmung investieren müssen: 84 % der befragten Kleinunternehmen verfügen derzeit über irgendeine Form von Online-Schutz, und 60 % geben an, dass es einen Aktionsplan für den Fall eines Cyberangriffs im Unternehmen gibt.

… dennoch sind viele nicht ausreichend für die zunehmende Komplexität und Häufigkeit dieser Bedrohungen ausgestattet

Obwohl Unternehmen wissen, dass Cybersicherheit ein Problem ist, haben sie oft nicht das nötige Personal oder die Ressourcen, um mit dieser wachsenden Bedrohung Schritt zu halten.
Trotz des hohen Maßes an Bewusstsein ist nur etwa die Hälfte (48 %) der Geschäftsinhaber/IT-Fachleute davon überzeugt, dass ihre Firma in der Lage ist, Cyberangriffe zu verhindern. Die meisten Kleinunternehmen (76 %) verwalten ihre Cybersicherheit ohne externe Hilfe.

- 17 % haben einen Mitarbeiter, der sich neben seiner Hauptaufgabe um die Verwaltung von Geräten und IT-Angelegenheiten kümmert.
- Nur 8 % der befragten Kleinunternehmen beauftragen einen externen Berater, der sie beim Kauf und der Installation von Cybersicherheitsprodukten unterstützt.

Zu viele Unternehmenseigentümer kümmern sich selbst um diese Angelegenheit – zusätzlich zu ihren vielen anderen Aufgaben. Und das betrifft nicht nur die Cybersicherheit: 45 % der befragten Geschäftsinhaber gaben an, dass sie mehr als 7 Stunden pro Woche für allgemeine IT-Angelegenheiten aufwenden.

Wie sich Hacker Zutritt verschaffen

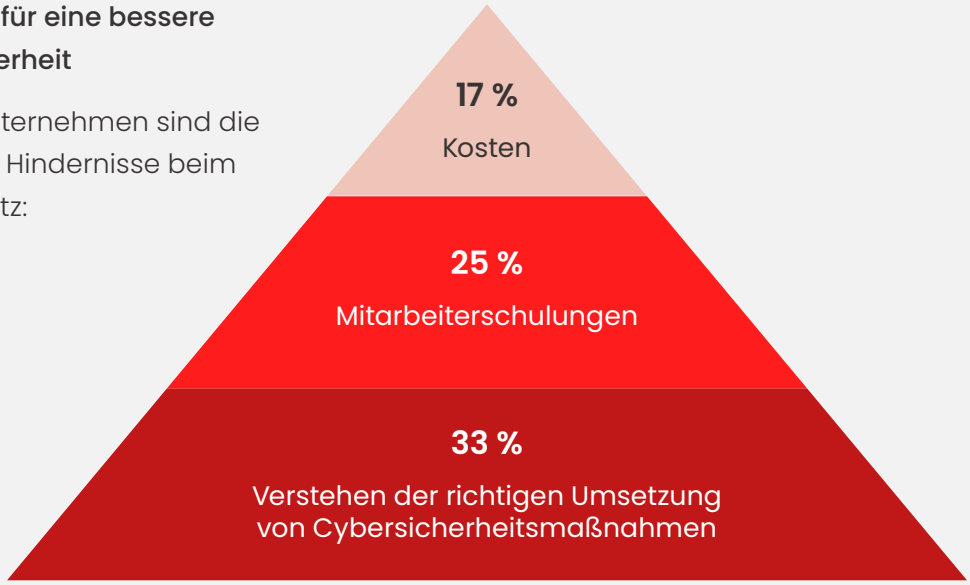
Es gibt zwar viele Möglichkeiten, wie Cyberkriminelle zuschlagen können, aber einige Methoden zählen zu ihren liebsten. Wachsamkeit und die Aufklärung Ihrer Mitarbeiter über diese Art von Angriffen und deren Vermeidung kann Unternehmen Zeit und Geld sparen.

Unsere Umfrage ergab, dass die meisten Angriffe (43 %) durch versehentliche Malware-Downloads ausgelöst wurden, weil ein Mitarbeiter auf einen Phishing-Link geklickt und/oder einen bösartigen Anhang geöffnet hat. In 36 % dieser Fälle wurden irrtümlich Anmeldedaten auf einer Phishing-Website eingegeben, und 35 % der Angriffe wurden durch ein schwaches Kennwort verursacht, das gehackt wurde.

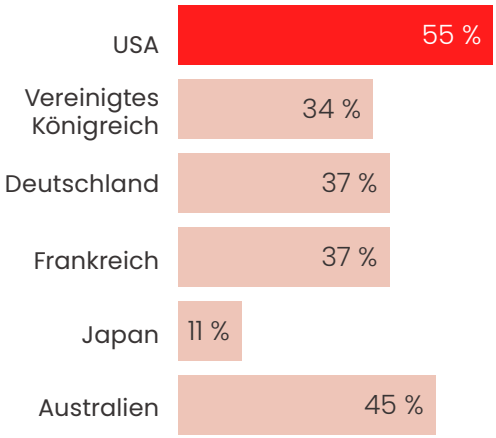
Es geht jedoch nicht nur um die Verhinderung von Cyberangriffen – es kommt auch vor, dass der Name eines Unternehmens bzw. seine Bekanntheit von Kriminellen als Waffe benutzt wird: 17 % der Umfrageteilnehmer gaben an, dass ihre eigenen Geschäftsinformationen bei Phishing-Angriffen auf andere Personen verwendet wurden.

Hindernisse für eine bessere Online-Sicherheit

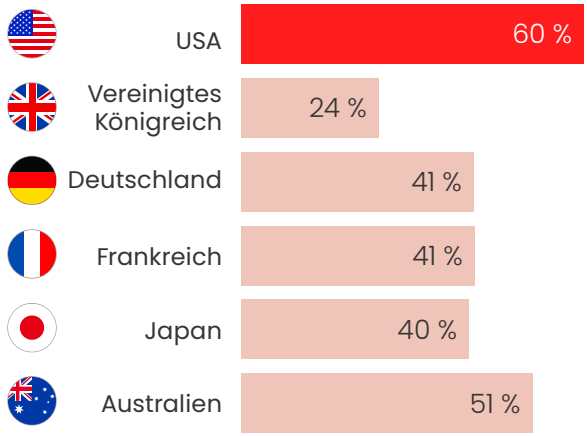
Für kleine Unternehmen sind die drei größten Hindernisse beim Online-Schutz:



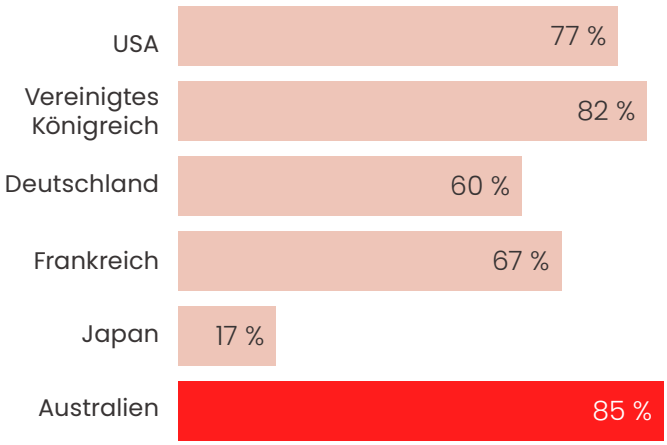
KMU in den USA haben die höchste Adoptionsrate von KI für die Cybersicherheit ...



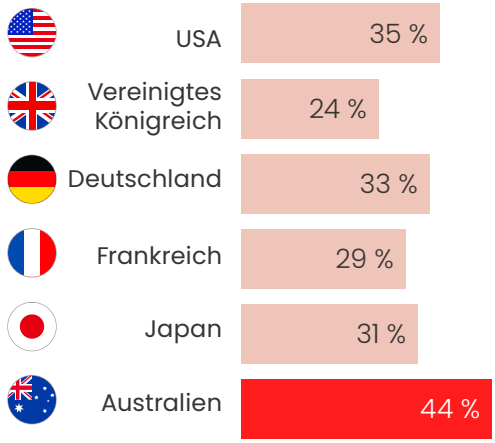
... sind aber auch am meisten besorgt über Cyberangriffe im Zusammenhang mit KI.



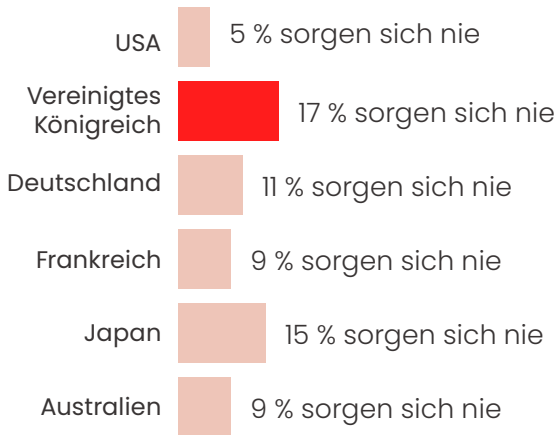
Australische KMU sind am zuversichtlichsten, dass ihre Mitarbeiter einen Betrug erkennen können ...



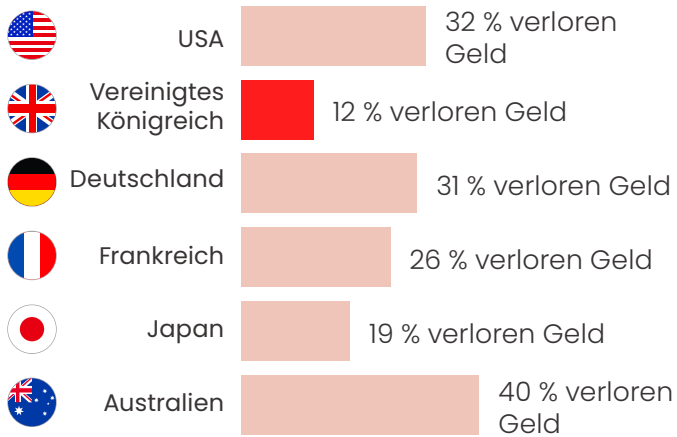
... geben jedoch häufiger an, dass ihr größtes Hindernis für den Online-Schutz darin besteht, zu verstehen, wie man Cybersicherheitsmaßnahmen umsetzt.



Britische KMU sorgen sich am wenigsten um Cyberangriffe ...



... und haben auch das niedrigste Risiko, bei einem Hackerangriff Geld zu verlieren.



Vorbereitung ist die wichtigste Abwehrmaßnahme

Der Schlüssel zu einer wirksamen Cybersicherheit liegt darin, vorbereitet zu sein. Die Vorbeugung eines Angriffs ist viel einfacher und weniger kostspielig für Ihr Unternehmen, als sich um die Folgen kümmern zu müssen. Hier sind einige wichtige Elemente eines guten Cybersicherheitsplans für KMU:

#1: Schulen Sie Ihre Mitarbeiter

Von den von uns befragten Kleinunternehmen schulen 72 % ihre Mitarbeiter zum Thema Cybersicherheit. Aber weniger als die Hälfte der Geschäftsinhaber und IT-Fachleute (46 %) haben volles Vertrauen in die Fähigkeit der Mitarbeiter/Kollegen, die notwendigen Schritte zum Schutz von Geräten und geistigem Eigentum zu unternehmen.

Cybersicherheitsschulungen sollten mehr sein als ein kurzes Video in der Einführungswoche. Jeder Mitarbeiter sollte wissen, was er tun kann, um Angriffe zu verhindern, wie das Unternehmen im Falle eines Angriffs vorgeht und welche Verantwortung er in Bezug auf Datensicherheit, Berichterstattung usw. hat.

#2: Führen Sie Risikobewertungen durch

Eine Risikobewertung kann dabei helfen, Schwachstellen zu ermitteln, die Einhaltung staatlicher Vorschriften und Bestimmungen zu gewährleisten und sicherzustellen, dass Ihr Unternehmen keinem Risiko eines größeren Angriffs ausgesetzt ist.

#3: Installieren Sie Virenschutz-Software

Ein Antivirus-Programm kann Ihre Geräte vor einer Vielzahl von Bedrohungen schützen, darunter Viren, Spyware, Ransomware und Phishing. Im besten Fall umfasst sie neben Schutzfunktionen auch Tools zum Bereinigen und Zurücksetzen von Geräten.

#4: Halten Sie Ihre Software auf dem neuesten Stand

Bei vielen der schädlicheren Malware-Angriffe werden Software-Schwachstellen in Betriebssystemen, Browsern und anderen wichtigen Programmen, die kleine Unternehmen verwenden, ausgenutzt.

Tatsächlich berichteten 30 % der Kleinunternehmen, die von Cyberangriffen betroffen waren, dass die Angriffe über eine Sicherheitslücke in veralteter oder nicht gepatchter Software erfolgten.
Software-Updates enthalten oft kritische Patches für Sicherheitslücken, was sie zu einer der besten – und einfachsten – Schutzmaßnahmen macht.

#5: Sichern Sie regelmäßig Ihre Dateien

Cyberangriffe führen häufig zu Datenausfällen. Deshalb ist es unerlässlich, regelmäßig Sicherungskopien von Dateien zu erstellen, damit die Daten bei Bedarf wiederhergestellt werden können.

#6: Verschlüsseln Sie wichtige Informationen

Durch Verschlüsselung können z. B. Website-Besitzer sensible Daten wie Kreditkartennummern, Kennwörter oder finanzielle Details in einen Code umwandeln, der von Cyberkriminellen nicht gelesen werden kann. In McAfee® Business Protection™ ist ein VPN enthalten, um Daten mittels einer äußerst starken WLAN-Verschlüsselung privat und sicher zu übermitteln.

#7: Beschränken Sie den Zugriff auf sensible Daten

Cyberangriffe sind nicht immer eine Hightech-Angelegenheit – Hacker verschaffen sich oft durch Social Engineering Zugang zu Daten. Bei der Ausarbeitung von Cybersicherheitsplänen müssen die Unternehmen stets die menschliche Komponente berücksichtigen.
Je weniger Personen Zugang zu wichtigen Daten haben, desto besser lassen sich die Auswirkungen einer Datenkompromittierung minimieren, und die Wahrscheinlichkeit sinkt, dass arglose Mitarbeiter autorisierten Datenzugriff erhalten. Die Erstellung eines Plans, der festlegt, welche Personen Zugang zu den verschiedenen Informationsebenen haben, kann helfen, für klare Rollen und Verantwortlichkeiten zu sorgen.

#8: Sichern Sie Ihr WLAN-Netzwerk

Drahtlosnetzwerke sind besonders anfällig für Cyberangriffe, da sie Funkwellen zur Datenübertragung

nutzen. Deshalb ist die Sicherung Ihres WLANs für den Schutz Ihrer Daten von entscheidender Bedeutung.

Der WLAN-Scan von McAfee erfolgt automatisch und warnt Sie, wenn Sie versuchen, eine Verbindung mit einem unsicheren Netzwerk herzustellen, damit Sie Ihr VPN einschalten oder ein anderes Netzwerk wählen können. So wissen Sie, dass die Verbindung sicher ist, bevor Sie sensible Daten darüber senden.

#9: Legen Sie strenge Kennwortrichtlinien fest

Um Ihre Konten wirksam vor Hackerangriffen zu schützen, ist es wichtig, dass Sie für jedes erstellte Konto ein sicheres Kennwort verwenden.

Ein sicheres Kennwort sollte mindestens 7-8 Zeichen lang sein und eine Kombination aus Zahlen, Symbolen und Groß- und Kleinbuchstaben enthalten. Weitere wichtige Maßnahmen sind, die Kennwörter täglich zu ändern, unterschiedliche Kennwörter für verschiedene Konten zu verwenden und sie niemals aufzuschreiben.

McAfee Business Protection bietet einen Kennwort-schutzstatus, der Warnungen sendet, wenn die Geräte des Unternehmens nicht kennwortgeschützt sind.

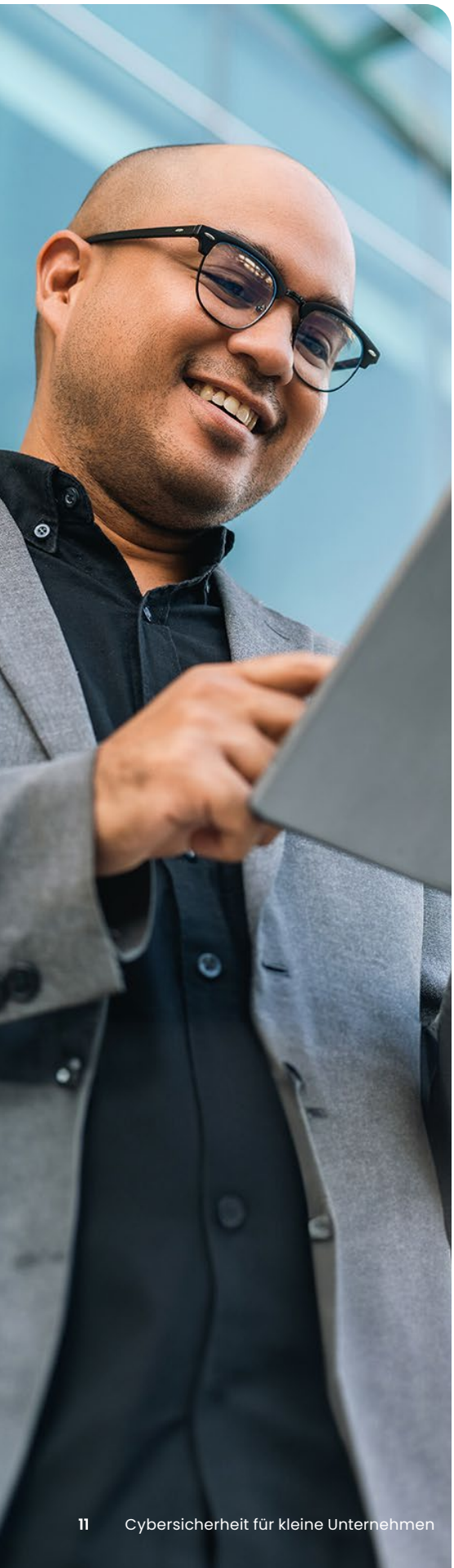
#10: Verwenden Sie einen Kennwort-Manager

Wenn Sie starke, eindeutige Kennwörter für jedes Gerät und jedes Konto erstellen, ist es schwierig, sich jedes einzelne zu merken. Ein Kennwort-Manager speichert diese für Sie und generiert automatisch die richtigen Anmeldedaten für jedes Konto.

McAfee® True Key wurde entwickelt, um lange, starke und eindeutige Kennwörter zu generieren. Es umfasst lokale Datenverschlüsselung, die Unterstützung zahlreicher Browser, die Möglichkeit der Synchronisierung zwischen PCs, Macs, iOS- und Android-Geräten sowie eine Vielzahl von Anmeldemethoden.

#11: Verwenden Sie eine Firewall

Eine Firewall schützt sowohl die Hardware als auch die Software und kann das Eindringen von Viren in Ihr Netzwerk blockieren. Mit einer Firewall können Sie den Netzwerkverkehr Ihres Unternehmens schützen und Hacker davon abhalten, Ihr Netzwerk anzugreifen, indem Sie bestimmte Websites blockieren.



#12: Nutzen Sie ein VPN (virtuelles privates Netzwerk)

VPNs verhindern, dass andere Ihre Daten bei der Übermittlung lesen können, und tragen so zu Ihrem Schutz bei. Für zusätzlichen Datenschutz verbergen VPNs Ihren Standort, indem sie die IP-Adresse eines Geräts durch eine andere IP-Adresse ersetzen. Die VPN-Verschlüsselung anonymisiert auch den Netzwerkverkehr, sodass Werbetreibende, die versuchen, gezielte oder auf Ihre Online-Aktivitäten basierende Werbung zu schalten, Ihre Surf- oder Suchgewohnheiten mit den üblichen Methoden nicht ermitteln können.

#13: Verhindern Sie physischen Diebstahl

Der Schutz Ihrer Hardware ist ebenso wichtig wie der Ihrer Software. Die Verhinderung des Zugriffs von Unbefugten auf die Geräte, deren physische Sicherung und das Hinzufügen von Trackern zur Wiedererlangung verlorener Geräte sind nur einige der Maßnahmen, die Unternehmer zum Schutz vor Diebstahl ergreifen können. Und durch die Einrichtung von Fernlöschfunktionen können sogar Daten auf verlorenen oder gestohlenen Geräten geschützt werden.

#14: Vernachlässigen Sie Mobilgeräte nicht

Da Mobilgeräte immer häufiger für geschäftliche Zwecke genutzt werden, müssen sie bei Ihren Plänen für die Cybersicherheit unbedingt berücksichtigt werden. Indem Sie Mitarbeiter dazu verpflichten, ihre Mobilgeräte mit Kennwörtern zu schützen, Sicherheitsanwendungen zu installieren und ihre Daten zu verschlüsseln, gehen Sie einen wichtigen Schritt, um Kriminellen keine Chance zu geben, Informationen von Mobilgeräten in öffentlichen Netzwerken zu stehlen.

#15: Achten Sie auf die Sicherheit von externen Partnern

Wenn Sie mit Geschäftspartnern oder Lieferanten zusammenarbeiten, die Zugang zu Ihren Systemen benötigen, müssen Sie gewährleisten, dass diese strenge Cybersicherheitspraktiken anwenden, bevor Sie den Zugang freigeben.

Wir stellen vor: McAfee Business Protection

Die Cyberkriminalität hat zunehmend auch kleine Unternehmen im Fokus. Doch mit den richtigen Werkzeugen und der optimalen Unterstützung können KMU ihre Betriebsabläufe vor Störungen sichern und ihre Mitarbeiter und Kunden schützen.

Wir freuen uns, den Kleinunternehmenskunden von Dell als exklusive Lösung McAfee® Business Protection™ anbieten zu können. McAfee Business Protection wurde speziell für KMU entwickelt und kann Ihnen dabei helfen, Ihr Unternehmen mit nur einer Lösung vor Hackern, Malware, Viren und mehr zu schützen.

Alles in Einem: Mit nur einer Lösung können das Unternehmen und alle seine Daten, Geräte, Online-Verbindungen und mehr geschützt werden.

Einfach und geführt: Die einfache Einrichtung mit automatischem Schutz und rechtzeitigen Warnungen macht die Absicherung des Unternehmens zu einem Kinderspiel. Alle Aufgaben können über die Sicherheitskonsole erfolgen. Frühzeitige Benachrichtigungen informieren Sie, wenn etwas Ihre Aufmerksamkeit erfordert – auch unterwegs.

Wächst mit Ihnen: Der Schutz hält mit dem Wachstum Ihres Unternehmens Schritt. Arbeitgeber können den Schutz problemlos auf jeden neuen Mitarbeiter und dessen Geräte ausweiten.

Zu den wichtigsten Merkmalen des Dienstes zählen:

- **Sicherheitskonsole:** Auf einem zentralen Dashboard sehen Sie den Schutzstatus des Unternehmens, können Mitarbeiter zur Einrichtung des Schutzes einladen und bei Bedarf Maßnahmen ergreifen. Sogar auf Ihrem Handy!
- **Bedrohungsschutz der nächsten Generation:** Preisgekrönter Schutz für eine unbegrenzte[1] Anzahl von Unternehmensgeräten vor bekannten und unbekannten Bedrohungen, einschließlich Malware, Ransomware, Viren und mehr, dank blitzschnellen Scans, die keine Leistungseinbußen verursachen.
- **Benutzerverwalteter Schutz:** Jeder Mitarbeiter erhält von seinem Arbeitgeber eine Einladung zur Einrichtung des Schutzes und kann dann seine eigenen Anmeldedaten erstellen, seinen individuellen Daten- und Geräteschutz einrichten und die erforderlichen Sicherheitsmaßnahmen ergreifen – alles im Rahmen von nur einem Unternehmensabonnement.
- **Secure VPN:** Mit Verschlüsselung auf Bankenniveau sind Ihre Daten überall anonym und sicher. Das VPN kann so eingestellt werden, dass es beim Zugriff auf ein unsicheres Netzwerk automatisch aktiviert wird.
- **Sicherheitsbericht:** Hebt den Status und unerledigte Punkte hervor, damit Sie den Schutz für Ihr Unternehmen, Ihre Geräte und Mitarbeiter bei Bedarf erhöhen können.
- **Experten-Support:** Das dedizierte Support-Team von McAfee bietet Ihnen rund um die Uhr technische Unterstützung und hilft Ihnen per Telefon oder Chat bei der Einrichtung von Schutzfunktionen und vielem mehr.

1. Unbegrenzt gilt für den angemessenen und vorhersehbaren Umfang eines typischen Kleinunternehmens.

Methodik/Über diese Studie

- Im September 2023 führte McAfee eine Studie über Online-Sicherheit bei Kleinunternehmen in sechs Ländern durch: USA, Vereinigtes Königreich, Deutschland, Frankreich, Japan, Australien.
- Die Befragten waren **[Geschäftsinhaber und IT-Fachleute]** von Unternehmen mit weniger als 250 Beschäftigten.
- Die Studie erfolgte zwischen dem 24. August und dem 5. September 2023 von MSI-ACI mittels eines Online-Fragebogens unter 700 Geschäftsinhabern und IT-Fachleuten in sechs Ländern.

Info zu McAfee

McAfee ist ein weltweit führendes Unternehmen im Bereich Online-Sicherheit. Bei uns liegt der Fokus auf dem Schutz von Menschen, nicht von Geräten. Unsere Lösungen passen sich an die Bedürfnisse unserer Kunden an und versetzen sie in die Lage, ihr digitales Leben durch integrierte, benutzerfreundliche Lösungen ohne Risiko zu genießen.
www.mcafee.com

Weitere Informationen finden Sie unter mcafee.com

6220 America Center Drive
San Jose, CA 95002
888.847.8766
www.mcafee.com

gd-cybersecurity-for-small-businesses_0124 JANUAR 2024