REPORT

# Vertrauen in Cybersecurity-Anbieter im Jahr 2026

Erkenntnisse aus einer herstellerunabhängigen Befragung von 5.000 IT- und Security-Verantwortlichen

SOPHOS

# Einleitung

Wenn Unternehmen einen Cybersecurity-Anbieter auswählen, legen sie die kritische operationale Resilienz – Personal, Daten und Einnahmen – in die Hände dieses Anbieters.

Trotz dieser Abhängigkeit fehlt es den meisten Unternehmen laut einer neuen Studie von Sophos an Vertrauen in die Anbieter, auf die sie sich bei der Gewährleistung ihrer Sicherheit verlassen.

Um einen realen Einblick in das tatsächliche Cybersecurity-Vertrauen von Unternehmen und Einrichtungen zu erhalten, hat Sophos eine unabhängige, globale Befragung von 5.000 IT- und Cybersecurity-Entscheidern in 17 Ländern in Auftrag gegeben. Die vom Marktforschungsinstitut Vanson Bourne durchgeführte Befragung liefert ein statistisch signifikantes, realitätsnahes Bild davon, wie Vertrauen zwischen Cybersecurity-Käufern und Anbietern aufgebaut und verloren wird.

**5.000**

IT- und Security-Verantwortliche aus 17 ändern nahmen an einer herstellerunabhängigen globalen Umfrage teil

# Wichtigste Erkenntnisse

**Es fehlt an Vertrauen:** Lediglich 5 % der IT-Entscheider geben an, dass sowohl sie als auch ihr Unternehmen/ihre Organisation volles Vertrauen in ihre Cybersecurity-Anbieter haben.

**Nachweisbare Fakten sind ein wesentlicher Faktor für Vertrauen:** IT-Teams und die oberste Führungsebene sind sich einig, dass überprüfbare Artefakte des Cybersecurity-Reifegrads die wichtigsten Indikatoren für Vertrauenswürdigkeit darstellen.

**Die Beurteilung der Vertrauenswürdigkeit von Anbietern bleibt eine Herausforderung:** 79 % der Unternehmen finden es schwierig, die Vertrauenswürdigkeit neuer Cybersecurity-Anbieter zu beurteilen, während 62 % dies bei ihren bestehenden Anbietern als schwierig empfinden. Die Befragten nannten mehrere Faktoren, die das Vertrauen in die Anbieter beeinträchtigten, allen voran die Tatsache, dass die vom Anbieter bereitgestellten Informationen nicht sachlich oder detailliert genug waren.

**Dieses mangelnde Vertrauen hat Konsequenzen:** 51 % der Befragten geben an, dass mangelndes Vertrauen zu der Angst führt, dass das Unternehmen mit höherer Wahrscheinlichkeit von einem schwerwiegenden Cybervorfall betroffen sein wird.

**Fach- und Führungskräfte sind sich oft nicht einig:** 78 % der Befragten geben an, dass ihr IT-Team und die Geschäftsleitung/der Vorstand unterschiedliche Meinungen zur Vertrauenswürdigkeit ihrer Cybersecurity-Anbieter haben. Fast ein Drittel der Unternehmen, die an der Sophos-Umfrage teilgenommen haben, geben an, dass solche Meinungsverschiedenheiten „häufig“ vorkommen.

# Vertrauenswürdigkeit ist schwer einzuschätzen

Lediglich 5 % der IT-Entscheider geben an, dass sowohl sie als auch ihr Unternehmen volles Vertrauen in ihre Cybersecurity-Anbieter haben.

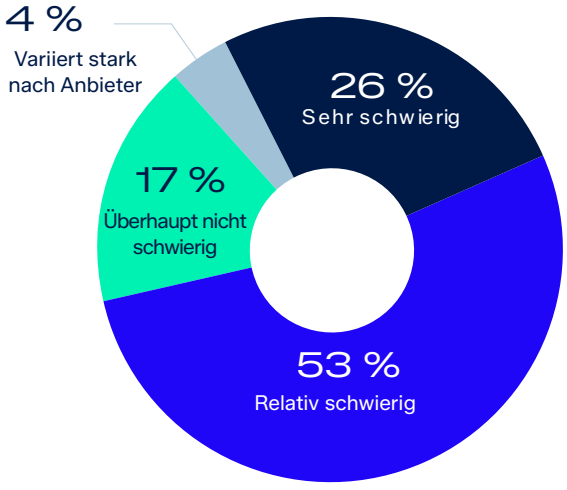
Wenn Sie von Ihrem Cybersecurity-Anbieter erwarten, dass er Ihr Netzwerk sicher und den Betrieb am Laufen hält, ist Vertrauen der Schlüssel. Cybersecurity-Anbieter sind diejenigen, die Ihr Unternehmen rund um die Uhr schützen, auch nachts und an Wochenenden oder wenn Mitarbeitende der IT-Abteilung im Urlaub sind. Kleine Unternehmer verfügen oft nicht einmal über eigenes IT-Personal, und ihre Cybersecurity-Produkte oder -Services können diese Lücke schließen.

Bevor Unternehmen entscheiden können, wem sie vertrauen, stehen sie vor einer noch grundlegenderen Herausforderung: Zunächst einmal geht es darum, die Vertrauenswürdigkeit eines Anbieters zu beurteilen.

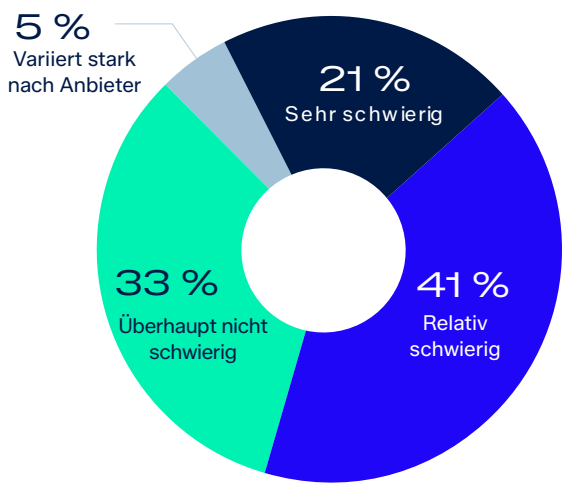
Der Umfrage zufolge geben 79 % der Befragten an, dass es schwierig sei, die Vertrauenswürdigkeit neuer Cybersecurity-Anbieter oder -Partner einzuschätzen. Dies verdeutlicht die weit verbreitete Schwierigkeit, Produkte zu vergleichen, Behauptungen zu überprüfen und zu verstehen, ob ein potenzieller Anbieter das Unternehmen tatsächlich schützen kann. 62 % haben zudem Schwierigkeiten, die Vertrauenswürdigkeit der Anbieter einzuschätzen, mit denen sie bereits zusammenarbeiten – ein Zeichen dafür, dass Vertrauenslücken nicht verschwinden, sobald ein Vertrag unterzeichnet ist (Abbildung 1).

**79 %**

Die befragten Unternehmen gaben an, dass es schwierig sei, die Vertrauenswürdigkeit neuer Cybersecurity-Anbieter/ Partner einzuschätzen




Bewertung **neuer** Cybersecurity-Anbieter und -Partner




Bewertung **bestehender** Cybersecurity-Anbieter und -Partner

*Abbildung 1: Wie schwierig ist es im Allgemeinen für Ihr Unternehmen, die Vertrauenswürdigkeit von Cybersecurity-Anbietern und -Partnern zu beurteilen? n=5.000*

## Hindernisse bei der Beurteilung des Vertrauens

Die Befragten nannten mehrere Gründe für mangelndes Vertrauen – die meisten davon sind in der Transparenz begründet. Viele haben Schwierigkeiten, die Angaben der Anbieter zu interpretieren, technische Details zu beurteilen oder die Informationen zu finden, die sie benötigen, um fundierte Entscheidungen treffen zu können.

Fast die Hälfte (47 %) gibt an, dass die von den Anbietern bereitgestellten Informationen nicht sachlich oder detailliert genug sind, und 45 % finden es schwierig, diese Informationen zu interpretieren oder zu verstehen. Weitere 43 % räumen ein, dass ihnen die Fähigkeiten oder Kenntnisse fehlen, um Anbieter effektiv zu beurteilen, 41 % stoßen auf widersprüchliche Informationen und 38 % haben Schwierigkeiten, die benötigten Informationen überhaupt zu finden (Abbildung 2).

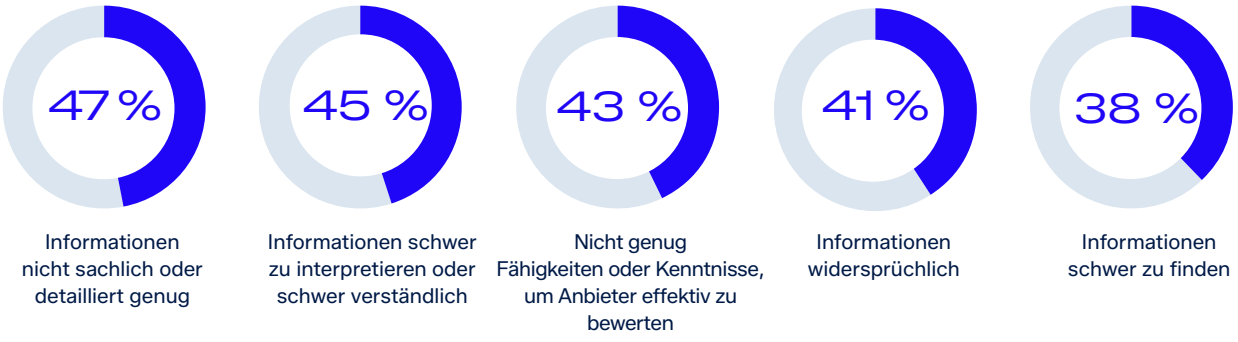



*Abbildung 2: Warum fällt es Ihrem Unternehmen schwer, die Vertrauenswürdigkeit von Cybersecurity-Anbietern einzuschätzen? n=4.483*

Der größte Unterschied zwischen kleinen Unternehmen (weniger als 250 Mitarbeitende) und Enterprise-Unternehmen (über 1.000 Mitarbeitende) besteht darin, dass KMUs viel häufiger die erforderlichen Fähigkeiten und Kenntnisse fehlen, um die Vertrauenswürdigkeit von Anbietern effektiv zu beurteilen – KMUs nannten dies 8 % häufiger als Befragte aus Enterprise-Unternehmen (Abbildung 3).

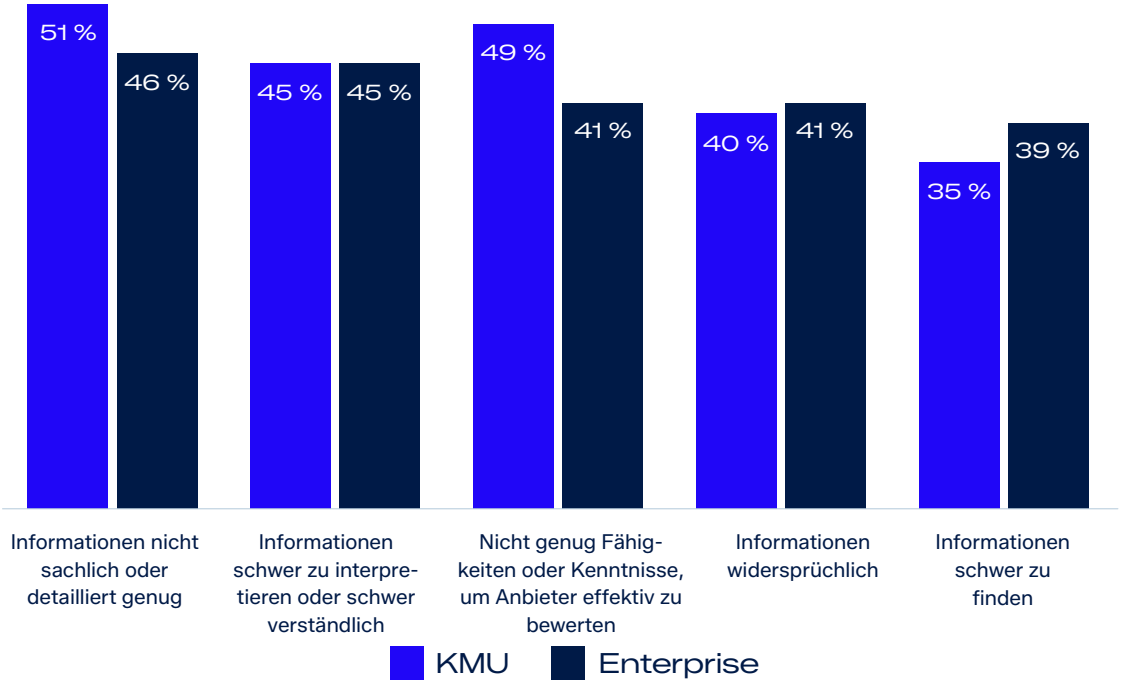



*Abbildung 3: Warum fällt es Ihrem Unternehmen schwer, die Vertrauenswürdigkeit von Cybersecurity-Anbietern einzuschätzen? n=504 (KMU), 2.260 (Enterprise-Unternehmen).*

# Mangelndes Vertrauen hat Konsequenzen

Diese Studie quantifiziert die Auswirkungen eines mangelnden Vertrauensverhältnisses zwischen einem Sicherheitsanbieter und seinen Kunden in mehrfacher Hinsicht. Auf die Auswirkungen des mangelnden Vertrauens in ihre Cybersecurity-Anbieter angesprochen, nannten die Befragten eine Mischung aus emotionalen und betrieblichen Konsequenzen:

- **51 %** berichten über eine zunehmende Besorgnis, dass ihr Unternehmen Opfer eines signifikanten Cybervorfalls werden könnte.
- **45 %** geben an, dass dies die Wahrscheinlichkeit erhöht, den Anbieter zu wechseln – für die meisten Unternehmen ein teurer und aufwändiger Prozess.
- **42 %** sehen erhöhte Beaufsichtigungsanforderungen.
- **41 %** berichten über ein verringertes Sicherheitsgefühl in Bezug auf ihren Cybersicherheits-Status.
- **38 %** äußern Bedenken, dass sie oder ihr Unternehmen möglicherweise den falschen Anbieter ausgewählt haben.

Diese geschilderten Auswirkungen erhöhen die ohnehin schon bestehenden operativen Anforderungen an IT- und Cybersecurity-Teams.

## Differenzen zwischen IT und Führungsetage

Eine weitere entscheidende Herausforderung ist die mangelnde Abstimmung zwischen den Personen, die täglich mit Cybersecurity-Tools arbeiten, und denjenigen, die die Verträge unterzeichnen. 78 % der Befragten geben an, dass ihr IT-Team und die Geschäftsleitung bzw. der Vorstand unterschiedliche Meinungen zur Vertrauenswürdigkeit ihrer Cybersecurity-Anbieter vertreten, und fast ein Drittel sagt, dass diese Differenzen „häufig" vorkommen (Abbildung 4).

Die Befragten gaben an, dass die oberste Führungsebene weiterhin stark in Kaufentscheidungen eingebunden ist. Lediglich 1 % der Unternehmen gaben an, dass Vorstand oder oberste Führungsebene keine Rolle bei Cybersecurity-Kaufentscheidungen spielen.

**1 %**

der befragten Unternehmen gab an, dass die Führungsebene keine Rolle bei Cybersecurity-Kaufentscheidungen spielt.

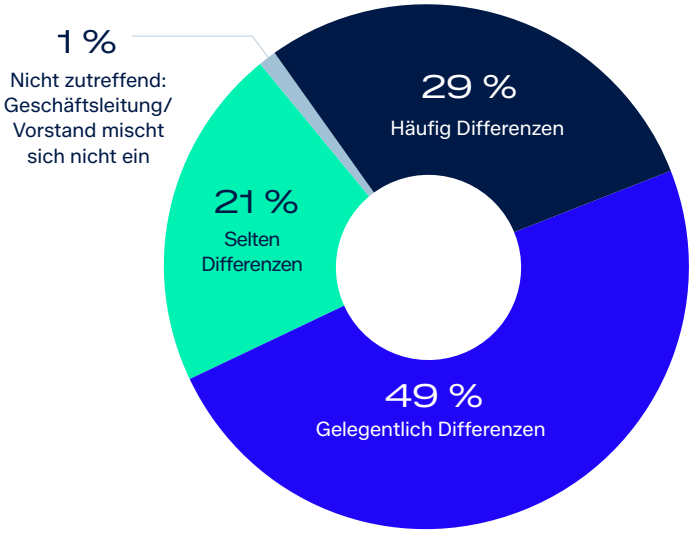



*Abbildung 4: Gibt es zwischen dem IT-Team und der Geschäftsleitung/dem Vorstand unterschiedliche Meinungen zur Vertrauenswürdigkeit Ihrer Cybersecurity-Anbieter? n=5.000.*

# Wie man Vertrauen in Cybersecurity aufbaut

Die Befragten gaben an, dass transparente, evidenzbasierte Security Practices von zentraler Bedeutung für den Aufbau von Vertrauen sind. Unternehmen wünschen sich Anbieter, die durch Offenheit, Klarheit und evidenzbasierte Sicherheitspraktiken Vertrauen schaffen.

Sowohl bei der obersten Führungsebene als auch bei den IT-Teams gelten „nachweisbare Artefakte, die als Indikator für den Cybersecurity-Reifegrad diesen" als wichtigster Faktor für das Vertrauen in Cybersecurity-Anbieter. Zu diesen Nachweisen gehören Bug-Bounty-Programme, ein öffentliches Trust Center, Warnhinweise, in denen Schwachstellen in ihren Produkten (sowie deren Bereinigung) detailliert beschrieben werden, Bewertungen durch Dritte und Zertifizierungen.

„Transparenz und zeitnahe Kommunikation bei Vorfällen und Offenlegungen" wurde von den Mitgliedern der Führungsetage als zweitwichtigster Faktor und von IT-Teams als drittwichtigster Faktor eingestuft.

# Welche Faktoren das Vertrauen in Cybersecurity-Anbieter stärken

| Treiber | Geschäftsleitung/ Vorstand | IT-/ Cyberteam | Einflussfaktoren |
|---|---|---|---|
| Primäre Treiber | 1. | 1. | Nachweisbare Indikatoren für den Cybersecurity-Reifegrad, z. B. Bug-Bounty-Programme, Trust Center, Sicherheitshinweise, Bewertungen durch Dritte, Zertifizierungen |
| | 2. | 3. | Transparenz und zeitnahe Kommunikation bei Vorfällen und Offenlegungen |
| | 3. | 4. | Expertenkommentare nach größeren Cybervorfällen, z. B. Zitate in der Presse, im Fernsehen |
| | 4. | 2. | Kontinuierliche Bereitstellung hochwertiger Cybersecurity-Services und -Produkte |
| | 5. | 5. | Performance in Analysten-Reports, z. B. Gartner Magic Quadrant |
| Sekundäre Treiber | 6. | 9. | Transparenz hinsichtlich interner Sicherheitsverfahren |
| | 7. | 7. | Performance in unabhängigen Tests, z. B. MITRE, SE Labs |
| | 8. | 6. | Reaktionsschneller und zuverlässiger Support |
| | 9. | 8. | Empfehlung Ihres Resellers/Cybersecurity-Partners |
| Tertiäre Treiber | 10. | 13. | Qualität der Veröffentlichungen zur Bedrohungsforschung |
| | 11. | 12. | Berichterstattung in der Finanz- und Wirtschaftspresse |
| | 12. | 11. | Erfahrungen anderer (Kollegen/Kunden) |
| | 13. | 10. | Persönliche Erfahrung |

*Welche Faktoren haben/hätten den größten Einfluss auf das Vertrauen der Geschäftsleitung/des Vorstands in einen Cybersecurity-Anbieter? Häufigste Antworten*
*Welche Faktoren haben/hätten den größten Einfluss auf das Vertrauen des IT-Cybersecurity-Teams in einen Cybersecurity-Anbieter? Häufigste Antworten*

# Wie Sophos das Vertrauen seiner Partner und Kunden gewinnt

Bei Sophos verstehen wir, dass Vertrauen aufgebaut werden muss – und nicht bloß gefordert. Wir arbeiten jeden Tag daran, es durch Transparenz, Integrität und ein unerschütterliches Engagement für Sicherheit und Datenschutz zu verdienen.

Im Mittelpunkt unserer Bemühungen steht das Sophos Trust Center, in dem wir Sicherheitshinweise veröffentlichen, Produktschwachstellen und deren Behebung dokumentieren, unseren Compliance-Status darlegen und erläutern, wie wir Kundendaten schützen.

Diese Transparenz zeigt sich auch in der Pacific Rim-Untersuchung von Sophos X-Ops, die eine fünfjährige Kampagne von in China ansässigen Angreifern öffentlich dokumentierte und detaillierte Taktiken, Techniken und Prozesse (TTPs), Indikatoren für eine Kompromittierung (IOCs) sowie Empfehlungen zur Abwehr zur Verfügung stellte, um Unternehmen dabei zu helfen, Resilienz branchenweit zu stärken.

Durch die Aufdeckung komplexer Aktivitäten von Nationalstaaten, die Zusammenarbeit mit öffentlichen Auftraggebern und anderen Anbietern sowie die Offenheit in Bezug auf Stärken und Schwächen unterstreicht Sophos, dass Vertrauen täglich durch Ehrlichkeit, Verantwortlichkeit und Engagement für den Schutz des gesamten digitalen Ökosystems erworben wird.

## Mehr erfahren

Weitere Informationen zu unseren Initiativen, mit denen wir Vertrauen schaffen, und zu unseren Ressourcen, die unsere Vertrauenswürdigkeit demonstrieren, finden Sie im Trust Center. Oder wenden Sie sich an Ihren Sophos-Ansprechpartner.

SOPHOS

# Weitere Informationen finden Sie im Trust Center oder wenden Sie sich an Ihren Sophos-Ansprechpartner.

**Sales DACH**
Tel.: +49 611 5858 0
E-Mail: sales@sophos.de