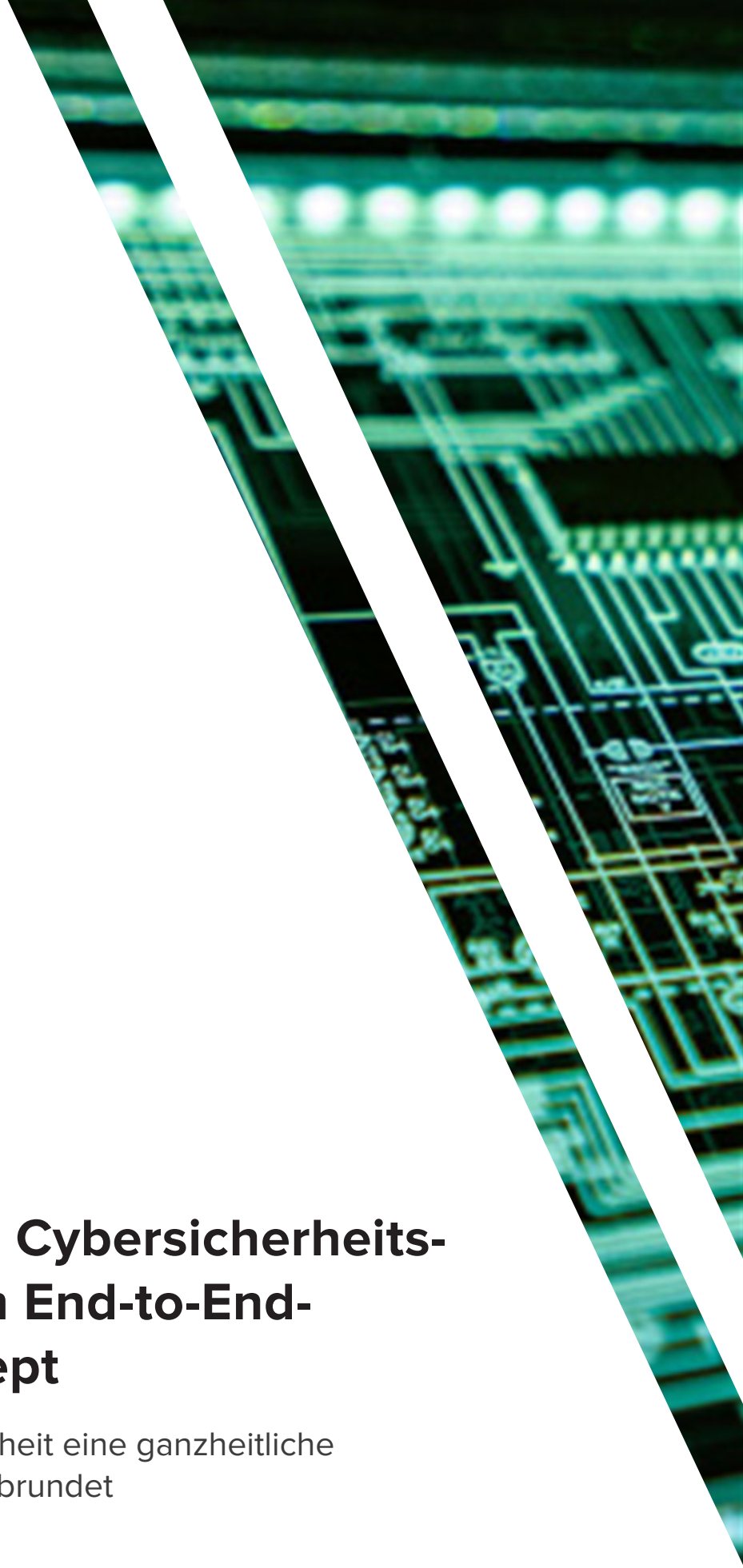
FORRESTER®



Bewältigung von Cybersicherheits-risiken mit einem End-to-End-Sicherheitskonzept

Wie die PC-Hardwaresicherheit eine ganzheitliche Cybersicherheitsstrategie abrundet

EIN STRATEGIEPAPIER VON FORRESTER CONSULTING IM AUFTRAG VON INTEL, SEPTEMBER 2022

Inhaltsverzeichnis

Projektteam:
Ana Brzezinska,
Senior Market Impact Consultant

Madeline Harrell,
Market Impact Consultant

Andrea Mendez Otero,
Market Impact Associate Consultant

Beitrag zur Studie:
Forrester-Forschungsgruppe Technology Architecture & Delivery

INFORMATIONEN ZU FORRESTER CONSULTING

Forrester Consulting bietet unabhängige und objektive, studienbasierte Beratung, um Führungskräften in ihren Unternehmen zum Erfolg zu verhelfen. Die Beratungsleistungen von Forrester reichen von kurzen Strategiegesprächen bis hin zu kundenspezifischen Projekten. Im direkten Austausch mit Ihnen unterstützen unsere Analysten Sie mit ihrem Fachwissen bei Ihren spezifischen geschäftlichen Herausforderungen. Weitere Informationen finden Sie unter forrester.com/consulting.

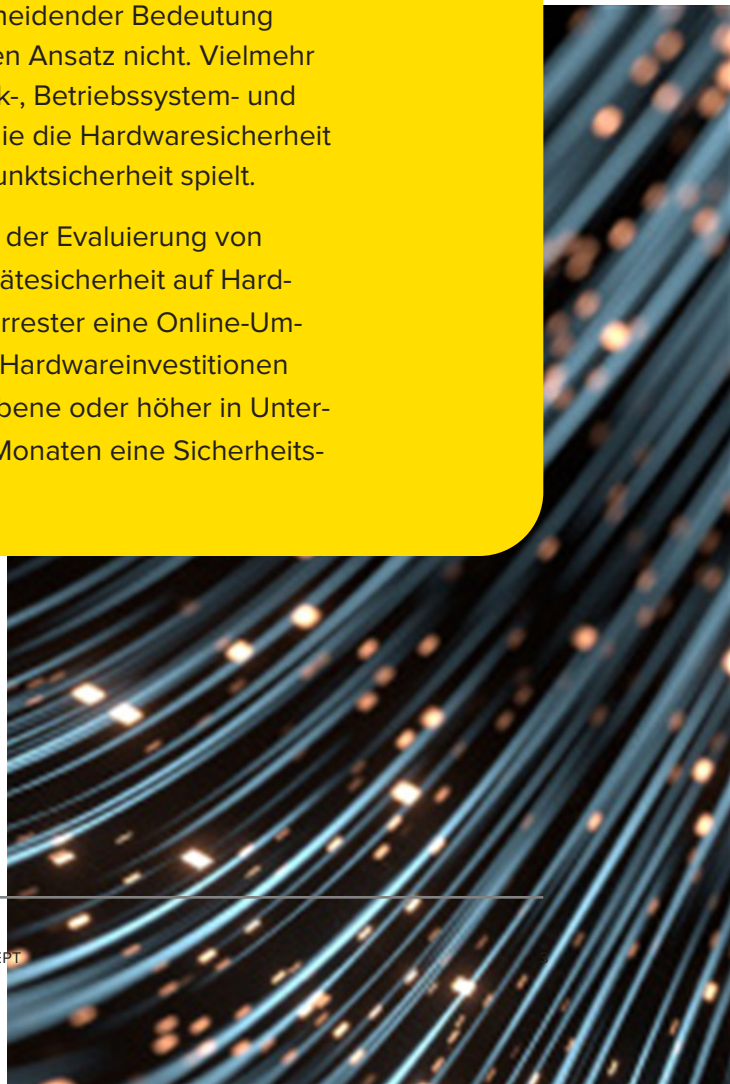
Zusammenfassung

Die Entwicklung einer ganzheitlichen Cybersicherheitsstrategie stellt für jedes Unternehmen eine Herausforderung dar – das gilt insbesondere im Zeitalter des hybriden Arbeitens und der stetigen Zunahme von Bedrohungen.[1] Zwar benötigen Unternehmen eine ganzheitliche Cybersicherheitsstrategie, die alle Aspekte des Geschäfts berücksichtigt; es sind aber vor allem die Endpunkte, die wichtig, gleichzeitig aber auch schwierig zu schützen sind.

Auch die Hardware – damit meinen wir hier die grundlegenden Komponenten eines PCs, die dem Betriebssystem zugrunde liegen, in Kombination mit der vom Systemhersteller bereitgestellten Schicht – muss zusammen mit den zu ihrem Schutz dienenden Sicherheitstools und -prozessen weiterentwickelt werden, ebenso wie andere Aspekte einer ganzheitlichen Sicherheitsstrategie. Aufgrund des breiten Spektrums der Hardwaresicherheit für Geräte – die Bandbreite reicht hier von der Vervielfachung der Formfaktoren über den Wildwuchs bei den Betriebssystemen bis hin zu einer Vielzahl komplexer Tools für Endpunktverwaltung und -sicherheit – stellt eine umfassende Absicherung von Endpunkten selbst für anspruchsvollste Organisationen eine Herausforderung dar.

Versierte Unternehmen wissen, dass ein ganzheitlicher Ansatz, der Sicherheitssoftware für Hardware, Netzwerk, Betriebssystem und Endpunkte beinhaltet, für eine umfassende Endpunktsicherheitslösung von entscheidender Bedeutung ist. Allerdings verfolgen die meisten Unternehmen diesen Ansatz nicht. Vielmehr legen sie den Schwerpunkt auf den Schutz auf Netzwerk-, Betriebssystem- und Richtlinienebene und vernachlässigen dabei die Rolle, die die Hardwaresicherheit bei der Schaffung einer soliden Grundlage für die Endpunktsicherheit spielt.

Im März 2022 beauftragte Intel Forrester Consulting mit der Evaluierung von Wahrnehmungen und Strategien im Hinblick auf die Gerätesicherheit auf Hardwareebene. Zur Untersuchung dieses Themas führte Forrester eine Online-Umfrage unter 647 für Technologieauswahl, Telearbeit und Hardwareinvestitionen verantwortlichen Entscheidungsträgern auf Direktorenebene oder höher in Unternehmen durch, bei denen in den vorangegangenen 12 Monaten eine Sicherheitsverletzung aufgetreten ist.



Wichtige Erkenntnisse

Unternehmen nehmen Cybersicherheit ernst, tun sich aber schwer damit, sie ganzheitlich anzugehen. Die Befragten gaben an, dass für sie die Netzwerksicherheit die höchste Priorität hat, dicht gefolgt von der Softwaresicherheit. Dagegen stuften zum jetzigen Zeitpunkt nur sehr wenige Befragte die Bedeutung der Hardwaresicherheit höher ein als leichter zugängliche Aspekte ihrer Sicherheitsstrategie, wie etwa die Cloud oder der Datenschutz.

Unternehmen wissen um die Bedeutung der Sicherheit auf Geräteebene, haben aber Probleme damit, eine ganzheitliche Strategie zur Verbesserung des allgemeinen Sicherheitsgefüges zu entwickeln. Unsere Untersuchung hat gezeigt, dass Schutzmaßnahmen auf der Hardwareebene Unternehmen zwar grundsätzlich vor der steigenden Zahl von Sicherheitsverletzungen schützen können, die Komplexität jedoch eine Hürde darstellt und das Wissen begrenzt ist.

Eine effektive Priorisierung der Sicherheit auf Hardwareebene fördert die Mitarbeitererfahrung, den Umsatz und den CX-Nutzen. Die Einbeziehung der Sicherheit auf Hardwareebene als Teil einer umfassenden Sicherheitsstrategie trägt zur Verbesserung der Mitarbeitererfahrung bei und wirkt sich somit auch auf das Kundenerlebnis und das wirtschaftliche Ergebnis aus.

PC-Cybersicherheit ohne Hardwareschutz: Bestenfalls unvollständig, womöglich sogar gefährlich

Cybersicherheit hat bei IT-Entscheidungsträgern oberste Priorität, insbesondere im Zuge der Umstellung von Unternehmen auf hybrides Arbeiten.[2] Allerdings halten viel zu viele Befragte an einer veralteten, netzwerkzentrierten Sichtweise fest und verfolgen einen althergebrachten, perimeterbasierten Ansatz, der jedoch in einer Welt, in der Daten zunehmend außerhalb des Unternehmensnetzwerks gespeichert werden, ineffektiv ist.[3] Leider hat dies auch zur Folge, dass IT-Verantwortliche häufig andere Bereiche des Cybersicherheitskonzepts – wie z. B. die Sicherheit auf Client-Hardware-Ebene – vernachlässigen und den Schwerpunkt ausschließlich auf die Netzwerk- und Softwaresicherheit legen. Nur 67 % der Befragten gaben an, dass Hardwaresicherheit Priorität genieße.

Zum Glück ändert sich das aber gerade. Die Befragten sind sich der Notwendigkeit bewusst, ihre Sicherheitsstrategien auf die Hardwareebene auszudehnen, die ganz weit unten auf der Halbleiterebene verankert ist, um so einen tiefgreifenden Abwehrmechanismus zu schaffen. Weil allerdings dieser Strategiewechsel so komplex ist, bleiben sie im Ungewissen und damit auch künftig anfällig für Sicherheitsverletzungen. Bei der Befragung von 647 für Technologieauswahl, Telearbeit und Hardwareinvestitionen verantwortlichen Entscheidungsträgern auf Direktorenebene oder höher in Unternehmen, bei denen in den vorangegangenen 12 Monaten eine Sicherheitsverletzung aufgetreten ist, haben wir festgestellt, dass ungeachtet der Bedeutung, die Führungskräfte in immer höherem Maße der Hardwaresicherheit zumessen, die meisten Unternehmen hier schlecht abschneiden. Dies hat Auswirkungen auf die folgenden Bereiche:

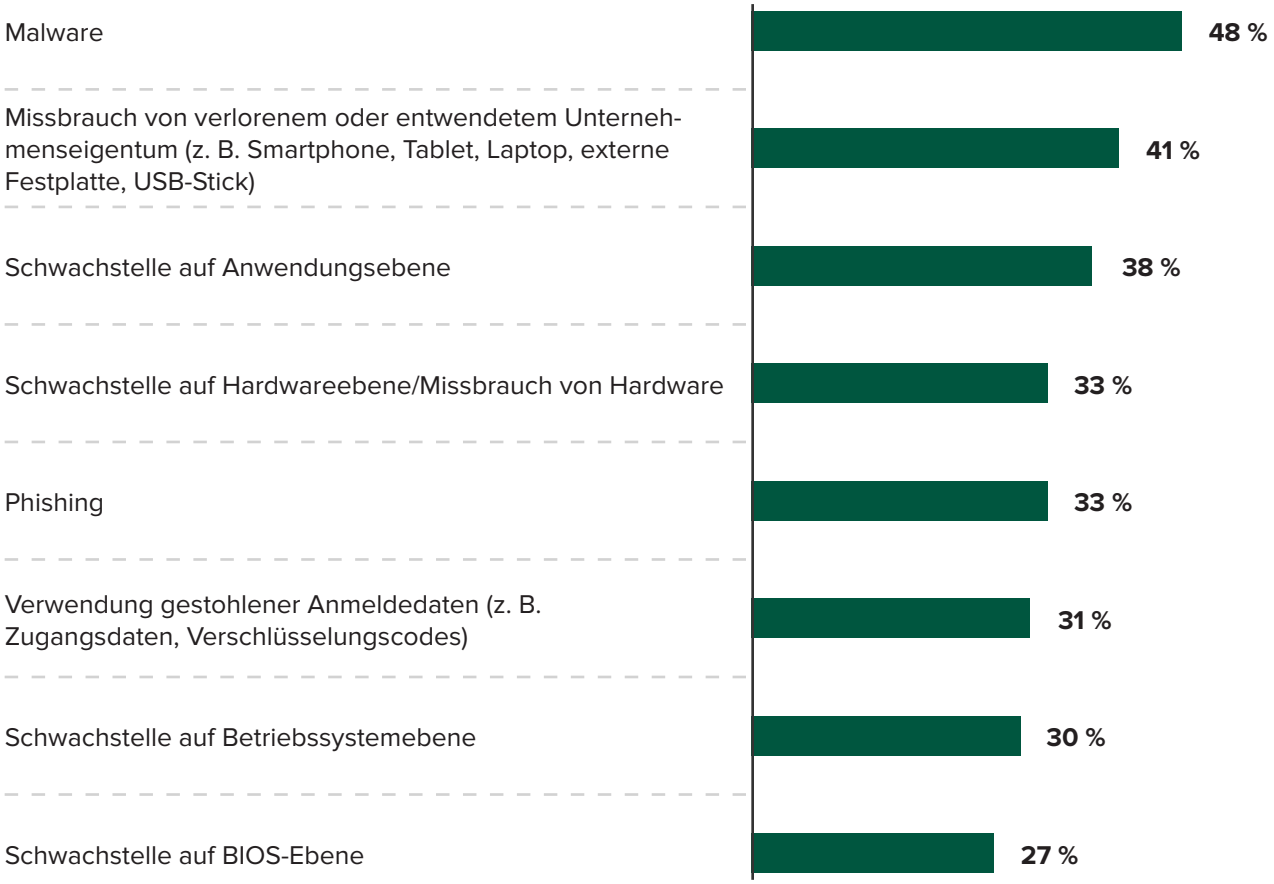
- **Kunden- und Markenvertrauen.** Aufgrund anhaltender Sicherheitsverletzungen – deren Ursache häufig auf Schwachstellen in der Hardware zurückzuführen sind – verlieren Kunden zunehmend das Vertrauen in die Unternehmen. Mehr als ein Drittel der Befragten (34 %) berichteten über einen Vertrauensverlust bei Kunden, 31 % über einen Vertrauensverlust in ihrem Partnernetzwerk und 28 % über Kundenabwanderungen aufgrund von Sicherheitsverletzungen.
- **Zeit- und Kostenaufwand für die Systemwiederherstellung.** Die Wiederherstellung des Systems nach Auftreten einer Sicherheitsverletzung kostet wertvolle Zeit und Ressourcen: im Durchschnitt 4,2 % des Gesamtumsatzes und etwa 1.187 Stunden für die Schadensbehe-

Im Schnitt kosten Sicherheitsverstöße die Unternehmen 4,2 % ihres Umsatzes und einen Zeitaufwand von 1.187 Stunden bis zur Wiederherstellung.

bung. Obwohl es für Sicherheitsverletzungen viele Ursachen gibt, führten 41 % der Befragten diese auf den Missbrauch von Endpunkten zurück (Abbildung 1). Viele Sicherheitsverletzungen betreffen physische Endpunkte, wobei Computer ganz oben auf der Liste stehen. Solche Vorfälle stellen aber nicht nur ein Sicherheitsproblem dar, sondern beeinträchtigen auch die Geschäftskontinuität und behindern die Mitarbeiter auch bei der Fortsetzung ihrer Arbeit und ihrer Produktivität. Ransomware und Schadcode bereiten IT-Entscheidungsträgern ebenfalls schlaflose Nächte. Die Befragten gaben an, dass der Schutz vor Schadcode der wichtigste Aspekt für die generelle Endpunktsicherheit sei.

Abbildung 1

„Sie haben bereits angegeben, dass bei Ihrem Unternehmen in den vergangenen 12 Monaten eine Sicherheitsverletzung aufgetreten ist. Worauf ist diese Sicherheitsverletzung in Ihrem Unternehmen zurückzuführen?“

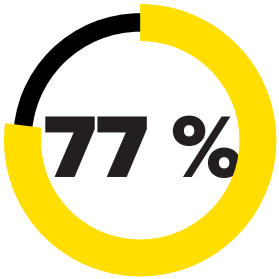


Basis: 647 für Technologieauswahl, Telearbeit und Hardwareinvestitionen verantwortliche Entscheidungsträger auf Direktorenebene oder höher in Unternehmen, bei denen in den vorangegangenen 12 Monaten eine Sicherheitsverletzung aufgetreten ist
Quelle: Studie im Auftrag von Intel, durchgeführt im März 2022 von Forrester Consulting

- **Mitarbeitererfahrung und Produktivität.** Anhaltende Sicherheitsverletzungen und die daraufhin erforderlichen umfangreichen Prüfungen beeinträchtigen die Produktivität der Mitarbeiter. 41 % der Befragten gaben an, dass die Häufigkeit von Audits infolge von Sicherheitsverletzungen zugenommen habe, und weitere 39 % berichteten, dass die Produktivität der Mitarbeiter dadurch gesunken oder gestört worden sei.
- **Wichtige Ziele der Cybersicherheit.** Aufgrund der Erfahrungen mit Sicherheitsverletzungen an Endpunkten – und deren Auswirkungen auf die Mitarbeiterproduktivität – sind sich die Befragten der Tatsache bewusst, dass die Sicherheit auf Hardwareebene ein wichtiges Thema ist und es sich lohnt, hier für ein einwandfreies Funktionieren Sorge zu tragen. Dadurch sehen sich diese veranlasst, diesem Thema in den kommenden 12 Monaten Priorität einzuräumen. Darüber hinaus arbeiten sie aufgrund der gemachten Erfahrungen daran, weitere Angriffe durch entsprechende Sicherheitsinvestitionen zu verhindern. 40 % der Befragten gaben an, dass sie als Folge einer Sicherheitsverletzung in die Sicherheit auf Hardwareebene investiert hätten. Allerdings gaben rund zwei Drittel der Befragten an, dass sie mit ihrem aktuellen Hardwarekonzept noch immer Risiken ausgesetzt seien. Das deutet darauf hin, dass ein stärker ganzheitlich orientierter Sicherheitsansatz auf Geräteebene erforderlich ist.

Trotz ihrer Wichtigkeit hat die Sicherheit von PC-Hardware ein Wahrnehmungsproblem

Obwohl die Befragten der Hardware in ihrer Sicherheitsstrategie zunehmend Priorität einräumen, sehen sich die meisten von ihnen nach wie vor mit Hardwareschwachstellen konfrontiert, denn viele IT-Entscheidungsträger sind sich der Rolle, die die Hardware im Rahmen des allgemeinen Sicherheitsgefüges spielt, gar nicht bewusst. So wissen viele zwar, dass die Hardware den Vertrauensanker der PC-Sicherheit bildet, aber sie verstehen nicht, wie sie mit den anderen Elementen ihrer Sicherheitsstrategie – wie etwa dem Netzwerk – zusammenhängt. Im Hinblick auf die Sicherheit für Geräte sind Maßnahmen bis hinab auf die Halbleiterebene für einen umfassenden Schutz unabdingbar. Hinzu kommt: Wenn Unternehmen sich nicht für die richtige Plattform entscheiden, sind sie nicht geschützt. Es gibt verschiedene Gründe dafür, dass Unternehmen sich gegenwärtig mit der Hardwaresicherheit schwertun:



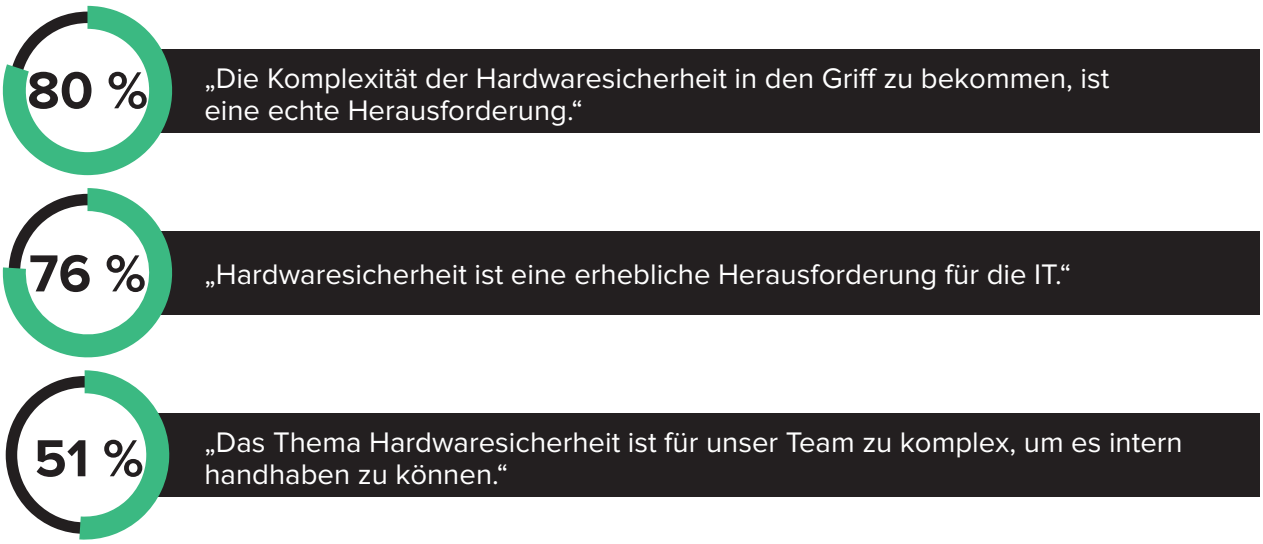
stimmen der Aussage zu, dass es den Aufwand lohnt, für ein ordnungsgemäßes Funktionieren der Sicherheit auf Hardwareebene zu sorgen.

- **Komplexität.** Unternehmen tun sich zugegebenermaßen mit der komplexen Problematik der Hardwaresicherheit schwer: 76 % der Befragten stimmten der Aussage zu, dass dieses Thema eine Herausforderung darstelle, und 51 % bestätigten, dass es für ihr Team zu komplex sei, um es intern zu managen, ohne sich auf Drittanbieter zu verlassen. Und das, obwohl pro Unternehmen im Schnitt etwa zwei Teams für die Endpunktsicherheit zuständig sind. Auch äußerten mehr als ein Viertel der Befragten, dass sie Probleme hätten, ihre zahlreichen Endpunktsicherheitstools zu integrieren und gemischte Umgebungen aus BYOD- und unternehmenseigenen Geräten zu managen. Darüber hinaus stellte die Bewältigung der Komplexität der Sicherheit auf Hardwareebene die größte Herausforderung für IT-Teams im Bereich der Endpunktsicherheit dar (Abbildung 2). Da eine ganzheitlich wirksame Strategie sich auf die Gesamtheit aller Sicherheitsmaßnahmen für Endpunkte auswirkt, sehen sich IT-Verantwortliche beim Ausarbeiten einer solchen Strategie oft überfordert. Zudem gibt es eine Fehlwahrnehmung im Hinblick auf die Komplexität der Angleichung von Hardware- und Softwaresicherheit. So gilt es für IT-Entscheidungsträger, die optimal zu den individuellen Anforderungen ihres Unternehmens passenden Sicherheitsfunktionen auszuwählen sowie eine voroptimierte Software, die diese Anforderungen am besten erfüllt.
- **Management und Ressourcen.** Die Herausforderungen, mit denen sich die IT-Abteilung bei der Endpunktsicherheit konfrontiert sieht, liegen vor allem

in den Bereichen Gerätemanagement und Ressourcen. So ist es etwa häufig schwierig, Endpunkt- und Sicherheitstechnologien unter einen Hut zu bringen, und es fehlt an Ressourcen wie Mitarbeitern, Zeit, Kompetenzen oder Unterstützung durch die Führungsetage. Üblicherweise kommen in den Unternehmen mehrere Produkte zur Verwaltung von Endbenutzercomputern, zur Bereitstellung von Softwarepaketen und zum Patchen von Sicherheitslücken zum Einsatz.[4] Zudem ist es schwierig, den zusätzlichen Aufwand an Zeit und Geld für Hardwareinvestitionen zu rechtfertigen, die aus Sicht der Anwender weitgehend unsichtbar bleiben.

Abbildung 2

„Bitte geben Sie an, wie sehr Sie den folgenden Aussagen zur Hardwaresicherheit zustimmen."



Basis: 647 für Technologieauswahl, Telearbeit und Hardwareinvestitionen verantwortliche Entscheidungsträger auf Direktorenebene oder höher in Unternehmen, bei denen in den vorangegangenen 12 Monaten eine Sicherheitsverletzung aufgetreten ist
Quelle: Studie im Auftrag von Intel, durchgeführt im März 2022 von Forrester Consulting

- **Abteilungsübergreifende Ausrichtung von IT und Geschäftsbereichen.** Nicht jeder ist sich über die Bedeutung der Hardwaresicherheit im Klaren. 83 % der befragten IT-Mitarbeiter gaben an, dass die Verbesserung der Sicherheit auf Hardwareebene in den nächsten 12 Monaten hohe oder sogar kritische Priorität hat, aber das liegt wahrscheinlich daran, dass sich die IT des Nutzens der Gerätesicherheit am ehesten bewusst ist. Aber auch die Entscheidungsträger aus den Geschäftsbereichen – konkret solche mit Budgetverantwortung – müssen erkennen, wie sich Investitionen in die Sicherheit auf Geräteebene positiv auf das Unternehmen auswirken. Sicherheit auf Hardwareebene ist jedoch für jeden im Unternehmen wichtig und nicht nur für die IT.[5] Für die Befragten, die Endgeräte nur über die IT-Abteilung erwerben, wirkten sich Sicherheitsverletzungen vor allem in Form von Produktivitätseinbußen bei den Mitarbeitern und der

verstärkten Durchführung von Audits aus. Unter den Befragten aus Unternehmen, die den Geschäftsbereichen die Möglichkeit geben, Kaufentscheidungen zu treffen, war die Häufigkeit von Audits das wichtigste Thema, gefolgt von den beträchtlichen finanziellen Auswirkungen. Doch IT und Geschäftsbereiche erkennen die negativen Auswirkungen von Sicherheitsverletzungen gleichermaßen – ganz gleich, ob diese produktivitätsbezogen sind oder sich nachteilig auf das wirtschaftliche Ergebnis auswirken.

- **Allgemeines Problembewusstsein.** Unternehmen tun sich schwer damit zu verstehen, wie gezielte Hardwareinvestitionen die Gestaltung der Betriebssystem- und Endpunktsicherheitssoftware-Richtlinien für verschiedene Klassen von Sicherheitssoftware unterstützen. Die Befragten stuften Hardware-Vertrauensanker und halbleitergestützte Sicherheit als nachrangigste Komponenten ihrer Endpunktsicherheitsstrategie ein – nach den Themen Verschlüsselung, Clouddiensten und Datenschutzmaßnahmen. Dies deutet darauf hin, dass Unternehmen den Schwerpunkt auf andere Bereiche ihrer Sicherheitsstrategien legen und die Hardware auf den letzten Platz der Liste verweisen. Das liegt wahrscheinlich daran, dass gar nicht verstanden wird, wie sich Hardwaresicherheit als Bestandteil einer umfassenderen Endpunktsicherheitsstrategie integrieren lässt. Es stellt sich also die Frage, welche Rolle die halbleitergestützte Sicherheit für die Sicherheit des Gesamtsystems spielt und wie man diese Verbindung stärken kann.

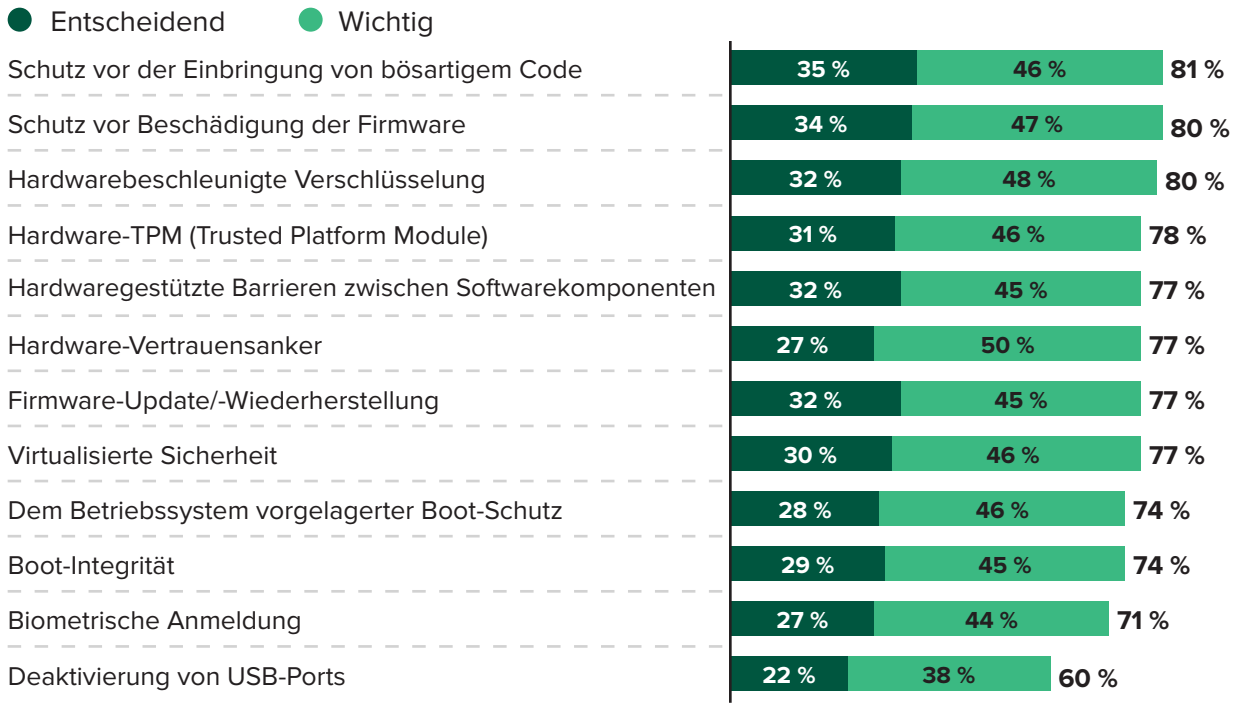
Implementierung von Sicherheitsmaßnahmen auf Hardwareebene zur Verbesserung der Effektivität des gesamten Sicherheitsstacks

Trotz dieser Herausforderungen müssen Sicherheits- und IT-Teams zur Vermeidung von Sicherheitsverstößen Sicherheitsvorkehrungen auf Hardwareebene treffen. Erfreulicherweise gaben 87 % der Befragten an, dass sie in den kommenden 12 Monaten (ab Q3/2022) vorrangig in Sicherheitsinitiativen investieren würden. Unternehmen stärken außerdem die strategische Implementierung von Sicherheitsmechanismen auf Hardwareebene durch eine Optimierung der Geräteverwaltungsrichtlinien auf Softwareebene: 84 % gaben an, dass eine wirksame Sicherheit auf Hardwareebene zu einem umfassenderen Vorgehen im Bereich der Sicherheit in ihrem Unternehmen führen werde. Zu den Vorteilen, die sich aus den strategischen Investitionen in die Sicherheit auf Hardwareebene für den gesamten Stack ergeben, gehören:

- **Schutz auf Richtlinienebene.** Hardwaresicherheit kann die Sicherheitssoftware für Betriebssysteme und hardwaregestützte Endpunkte verbessern. Zudem ist sie in manchen Fällen obligatorisch, um bestimmte Einstellungen im Betriebssystem aktivieren zu können. Die Befragten nannten im Zusammenhang mit integrierter Sicherheit auf Hardwareebene verschiedene Vorteile, z. B. weniger Sicherheitsverstöße und Sicherheitsvorfälle (46 %) und größeres Vertrauen in die Umsetzung eines hardwarenahen Datenschutzes. Sie schlugen zudem einen Bogen von ihr zur Prüfung der Vertrauenswürdigkeit von Geräten (45 %) und Daten (42 %) (siehe Abbildung 3).
- **Vorteile bei der Verwaltung.** Die Befragten erwähnten Vorteile für die IT, die sich aus der Priorisierung der Sicherheit auf Hardwareebene und deren Integration in Endpunktsicherheit und IT ergeben hätten. Hierzu gehörten eine einfachere Verwaltung für das IT-Team (52 %), eine vereinfachte Verwaltung sicherheitsrelevanter Ereignisse und Vorfälle (37 %) und eine geringere Anzahl von Sicherheitsagenten von Drittanbietern auf den Geräten (34 %) (siehe Abbildung 4).
- **Mitarbeitererfahrung und Kundenerlebnis.** Der augenfälligste Nutzen, der sich aus der integrierten Sicherheit auf Hardwareebene für die Mitarbeiter ergibt, ist die insgesamt verbesserte Benutzerfreundlichkeit. Integrierte Sicherheit auf Hardwareebene gewährleistet dies durch einfachere Sicherheitsprotokolle, leichtere Fehlerbeseitigung und besseren Zugang zur IT-Abteilung. Außerdem verbessert es die Benutzererfahrung von Mitarbeitern am PC durch Verkürzen der Bootzeiten und den Schutz sensibler personenbezogener Daten im Speicher im Falle einer Sicherheitsverletzung oder eines entwendeten Geräts. Die Verbesserung der Mitarbeitererfahrung führt aber auch zu einem besseren Kundenerlebnis: 84 % der Befragten gaben an, dass eine wirksame Sicherheit auf Hardwareebene das Vertrauen aufseiten der Kunden stärke.

Abbildung 3

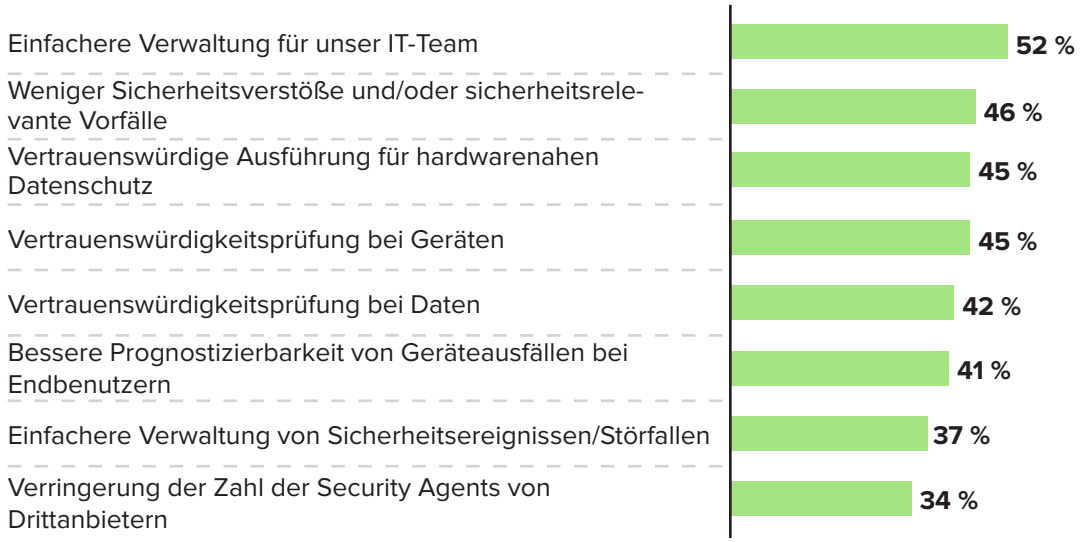
„Wie wichtig sind die folgenden Aspekte für Ihre allgemeine Endpunktsicherheit?“



Basis: 647 für Technologieauswahl, Telearbeit und Hardwareinvestitionen verantwortliche Entscheidungsträger auf Direktorenebene oder höher in Unternehmen, bei denen in den vorangegangenen 12 Monaten eine Sicherheitsverletzung aufgetreten ist
Hinweis: Aufgrund von Rundungen entsprechen die Prozentsätze in der Summe möglicherweise nicht den einzelnen Werten.
Quelle: Studie im Auftrag von Intel, durchgeführt im März 2022 von Forrester Consulting

Abbildung 4

„Welche Vorteile bietet integrierte Sicherheit auf Hardwareebene für Endpunktsicherheit und die IT?“



Basis: 647 für Technologieauswahl, Telearbeit und Hardwareinvestitionen verantwortliche Entscheidungsträger auf Direktorenebene oder höher in Unternehmen, bei denen in den vorangegangenen 12 Monaten eine Sicherheitsverletzung aufgetreten ist
Quelle: Studie im Auftrag von Intel, durchgeführt im März 2022 von Forrester Consulting

Wichtige Empfehlungen

Es ist offensichtlich, dass Unternehmen die Nutzung der Integration von Sicherheitsfunktionen auf Geräteebene in eine ganzheitliche Cybersicherheitsstrategie nicht ignorieren können. Die Frage aber lautet, wo sollen die Unternehmen anfangen? Ungeachtet der Komplexität und der hohen Kosten dieser Technologie haben Sie die Möglichkeit, Client-Hardwaresicheheit in Ihren Technologie-Stack zu integrieren.

Aus der von Forrester durchgeführten ausführlichen Befragung von IT-Entscheidungsträgern zur Hardwaresicherheit ergaben sich verschiedene wichtige Empfehlungen:

Am Anfang steht ein effektiver Gerätebeschaffungsprozess.

Die einfachste Möglichkeit zur Implementierung von Hardwaresicherheit besteht darin, Geräte zu kaufen, die bereits über entsprechende Funktionen verfügen. Viele OEM-Gerätehersteller implementieren in Zusammenarbeit mit Anbietern von Halbleitertechnik spezifische und maßgeschneiderte Funktionen. Berücksichtigen Sie diese Anforderungen von Anfang an in Ihren Ausschreibungen, statt sich erst nach dem Kauf Gedanken über die Hardwaresicherheit zu machen. So kann Ihr Unternehmen den Schwerpunkt auf den Kauf der passenden Tools mit den erforderlichen, in die Hardware integrierten Basisschutzfunktionen legen und weitere Sicherheitsmaßnahmen wie Problemerkennung und -beseitigung auf Endpunkten nachträglich hinzufügen.

Verknüpfung der Hardwarevorteile mit ortsunabhängigem Arbeiten.

Unsere Untersuchung hat gezeigt, dass 51 % der Unternehmen beabsichtigen, hybride Arbeitsformen einzuführen, und 15 % sogar planen, auf ein vollständig dezentrales Modell umzusteigen.[6] Daher spielt die Hardwaresicherheit bei der Umsetzung von Strategien für die Zukunft der Arbeit eine entscheidende Rolle. Warum? Weil die einzige Möglichkeit, Offline-Endgeräte effektiv zu managen, die nicht mit einem Unternehmensnetzwerk verbunden sind, Funktionen auf Hardwareebene sind – ein Phänomen, das bei verteilten Endgeräten immer häufiger anzutreffen ist. Integrierte Hardwareschutzmechanismen sorgen außerdem dafür, dass Endgeräte beim Transport zum Home-Office der Mitarbeiter besser geschützt sind.

Implementierung von Hardwaresicherheit bei der Aktualisierung der Geräte.

Viele Unternehmen aktualisieren ihren Gerätebestand, um von den Vorteilen aktueller Betriebssysteme zu profitieren. Dies bietet eine ausgezeichnete Gelegenheit zur Implementierung von Sicherheitsmaßnahmen auf Geräteebene, zumal viele moderne Betriebssysteme zum Zweck der Optimierung von Sicherheit, Verwaltung und Benutzerfreundlichkeit auf aktuellste Hardwareinnovationen zurückgreifen. Unternehmen profitieren außerdem im Zweifelsfall von einem besseren Schutz des Betriebssystems und der Hardware, wenn sie beide Upgrades gleichzeitig durchführen.

Informieren der Entscheidungsträger in den Geschäftsbereichen über die Vorteile des Kaufs von Geräten mit Hardwaresicherheitsfunktionen.

Es sind die Entscheidungsträger in den Geschäftsbereichen, die zum Großteil über Hardwareanschaffungen entscheiden — ein entscheidender Schwachpunkt für IT-Führungskräfte, die sich für mehr Transparenz in Bezug auf die Endpunktbestände einsetzen. Erstellen Sie eine Liste mit Empfehlungen für Geräte mit erweiterten Hardwareschutzfunktionen und legen Sie diese den Einkäufern in den Abteilungen vor. Wenn Sie diese Zielgruppen vom Mehrwert solcher Geräte überzeugen wollen, müssen Sie vor allem die geschäftlichen Vorteile, die die richtigen Sicherheitslösungen bieten, ins Blickfeld rücken.

Anhang A: Methodik

Im März 2022 beauftragte Intel Forrester Consulting mit der Evaluierung von Wahrnehmungen und Strategien im Hinblick auf die Gerätesicherheit auf Hardwareebene. Zur Untersuchung dieses Themas führte Forrester eine Online-Umfrage unter 647 für Technologieauswahl, Telearbeit und Hardwareinvestitionen verantwortlichen Entscheidungsträgern auf Direktorenebene oder höher in Unternehmen durch, bei denen in den vorangegangenen 12 Monaten eine Sicherheitsverletzung aufgetreten ist. Die Mitwirkenden erhielten zum Dank für ihre Teilnahme an der Befragung eine kleine Anerkennung. Die Studie wurde im Februar und März 2022 durchgeführt.

Anhang B: Demografische Daten

REGION	
Großbritannien	**17 %**
USA	**17 %**
Indien	**17 %**
Deutschland	**17 %**
Brasilien	**17 %**
Japan	**15 %**

ANZAHL DER MITARBEITER	
> 20.000	**11 %**
5.000 bis 19.999	**23 %**
1.000 bis 4.999	**15 %**
500 bis 999	**12 %**
100 bis 499	**8 %**
1 bis 99	**32 %**

FÜHRUNGSEBENE	
Führungskraft auf Leitungsebene	**22 %**
Vice President	**32 %**
Direktor	**46 %**

ABTEILUNG	
IT	**100 %**

ART DER SICHERHEITSVERLETZUNGEN IN DEN VERGANGENEN 12 MONATEN (Mehrfachnennungen möglich)	
Externer Angriff auf unsere Organisation	**58 %**
Interner Vorfall innerhalb unserer Organisation	**55 %**
Verlorengegangenes/gestohlenes Firmeneigentum	**55 %**
Angriffe oder Vorfälle, die unsere Geschäftspartner/Drittanbieter betrafen	**50 %**

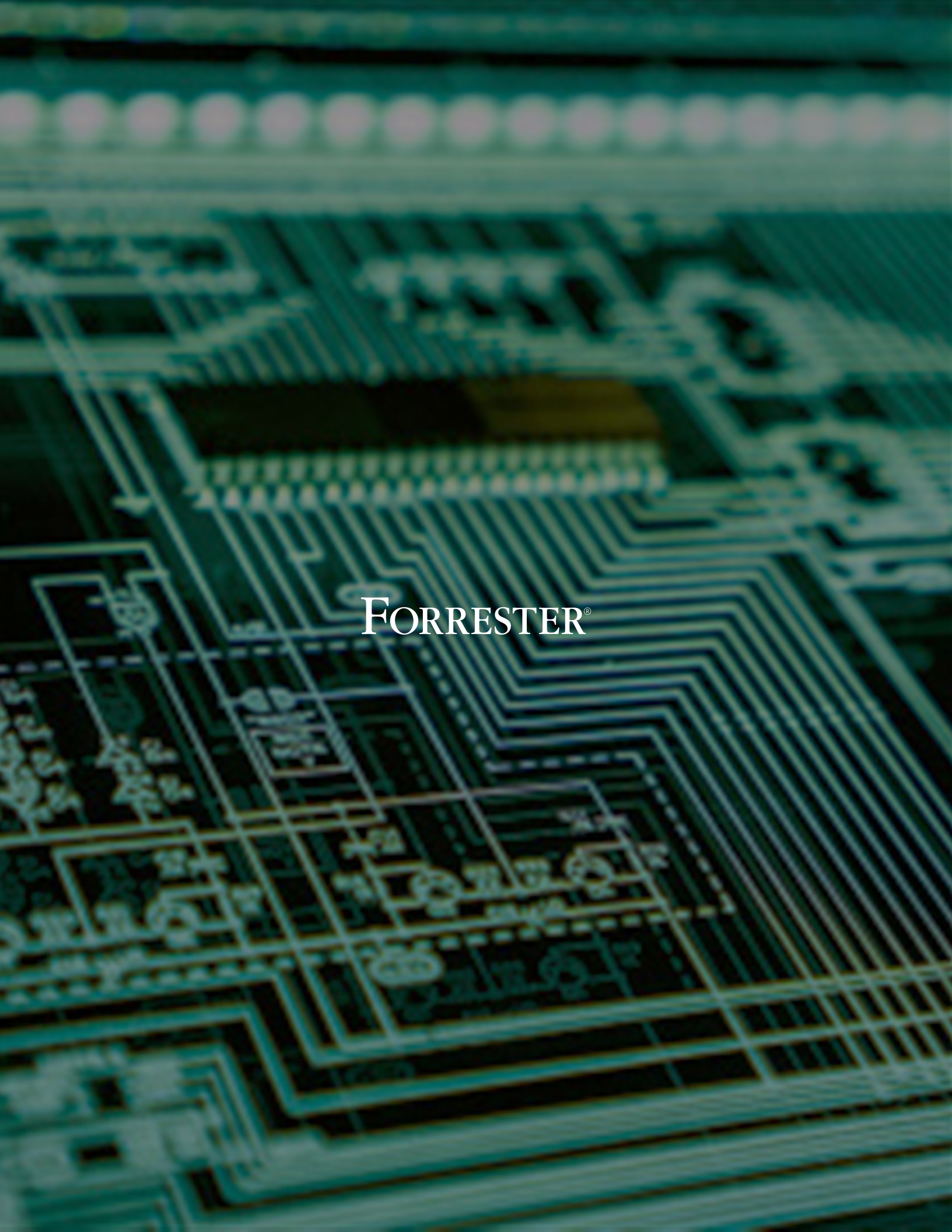
BRANCHE	
Technologie und Technologiedienstleistungen	**15 %**
Einzelhandel	**10 %**
Finanzdienstleistungen und Versicherungen	**8 %**
Fertigung und Werkstoffe	**8 %**
Telekommunikationsdienste	**5 %**
Gesundheitswesen	**5 %**
Unternehmensdienstleistungen	**5 %**
Transport und Logistik	**4 %**
Chemie und Metallverarbeitung	**4 %**
Verbraucherdienste	**4 %**
Konsumgüter und verarbeitendes Gewerbe	**4 %**
Bauwesen	**4 %**
Für alle übrigen Optionen wurden Anteile von maximal 3 % angegeben	**24 %**

Die Prozentwerte ergeben aufgrund von Rundungen nicht exakt 100 %.

Anhang D: Schlussbemerkungen

[1] „The Anywhere-Work Guide For Tech Pros, 2022“. Forrester Research, Inc., 16. Mai 2022.
[a3] „The Definition Of Modern Zero Trust, 2022“. Forrester Research, Inc., 24. Januar 2022.
[4] „The Forrester Wave™: Unified Endpoint Management, Q4 2021“. Forrester Research, Inc., 2. November 2021.
[5] „The Future Of Endpoint Management, 2022“. Forrester Research, Inc., 6. Juni 2022.
[6] „The Anywhere-Work Preflight Checklist, 2022“. Forrester Research, Inc., 16. Mai 2022.

Kein Produkt oder Bauteil bietet absolute Sicherheit.


FORRESTER®