Whitepaper

Die geschäftliche Notwendigkeit sicherer Endgeräte

Gesponsert von: Apple

Tom Mainelli Michael Suby
September 2023

IDC-STANDPUNKT

Was bereitet IT-Entscheidungsträgern schlaflose Nächte? Die IT-Sicherheit. Denn kluge IT-Entscheidungsträger wissen, dass das gesamte Unternehmen über Nacht gefährdet sein kann , egal wie gut ein Unternehmen geführt wird oder wie beliebt sein Produkt oder seine Dienstleistung ist –, wenn die Sicherheit versagt.

Und leider wird die Welt auch nicht sicherer. Wirtschaftsspionage, Schurkenstaaten, das organisierte Verbrechen und sogar Gelegenheitsdiebe sind inzwischen in Sachen Technologie alle auf dem neuesten Stand. Um den Angreifern immer einen Schritt voraus zu sein, muss die IT-Abteilung wachsam bleiben und stets bereit sein, für den Schutz der Mitarbeiter, Kunden und Daten neue Anbieter und Technologien zu nutzen.

Die Liste der Sicherheitsprobleme, mit denen die IT konfrontiert ist, ist lang. Sie reicht von den Endgeräten (Rechnern) über Rechenzentren bis hin zu den alles verbindenden Netzwerken und der Software, auf der alles läuft. Dieser Artikel beschäftigt sich mit der Bedeutung der Sicherung von Endgeräten. Denn die Sicherheit in all diesen anderen Bereichen ist letztlich wenig wert, wenn die Endgeräte nicht sicher sind.

Eine der größten Hürden bei der Sicherung von Endgeräten besteht darin, dass sichere Endgeräte für die Endbenutzer herkömmlich oft Abstriche bedeuten, weil diese Geräte eingeschränkt und schwer zu nutzen sind. In diesem Fall findet die andere wichtige Schwachstelle in jedem Sicherheitssystem – nämlich der Benutzer – oft Wege, um zur Erledigung der Arbeit Sicherungen zu umgehen. Wird Sicherheit zum Reibungspunkt für den Benutzer, erfüllt sie nicht mehr ihren Zweck.

Technologische Fortschritte machen zunehmend ein hochwertiges Benutzererlebnis bei gleichzeitiger Gewährleistung der Sicherheit möglich. Fortschritte bei der Erkennung von Malware, beim Schutz von Daten, bei der Authentifizierung und bei der Verschmelzung von Hardware und Software bedeuten, dass die Endgeräte von heute für bessere Sicherheit keine Abstriche bei der Produktivität mehr machen müssen.

METHODEN

Im Juli 2023 führte IDC eine Online-Umfrage unter IT-Entscheidungsträgern in den USA und Kanada (n=513) durch. In dieser fragten wir nach ihren Ansichten zum Thema Sicherheit allgemein und zur Bedeutung der Sicherung von Rechner-Endgeräten im Besonderen. Die Befragten repräsentieren einen Mix aus Unternehmen mit mindestens 500 Beschäftigten aus einer Bandbreite verschiedener Branchen. Diese IT-Entscheidungsträger unterstützen eine Reihe von Betriebssystemen, u. a.

Microsoft Windows, Apple macOS und Google ChromeOS. Sie sind entweder für die Auswahl, den Einkauf oder die Bereitstellung von Sicherheitssoftware für ihr Unternehmen verantwortlich oder managen die dafür zuständigen Mitarbeiter.

SITUATIONSÜBERBLICK

Sicherheit fällt weiterhin in den Aufgabenbereich der Führungsebene. Zukunftsorientierte Unternehmen erkennen an, dass gute Sicherheit kein Luxus, sondern vielmehr eine Voraussetzung für ein gesundes und florierendes Unternehmen ist, das in einer sich ständig wandelnden Gefährdungsumgebung agiert, in der koordinierte und finanziell gut ausgestattete Angreifer aktiv sind.

IDCs Future Enterprise Resiliency and Spending Survey (FERS) vom März 2023 unter IT-Entscheidungsträgern in Unternehmen mit 500 oder mehr Mitarbeitern zufolge waren über 50 % der befragten Unternehmen weltweit in den letzten 12 Monaten von einem Ransomware-Angriff betroffen, der zu einer Störung ihrer Geschäftstätigkeit führte. Mehr als ein Drittel dieser Teilnehmergruppe gab an, dass der Angriff die Geschäftstätigkeit eine Woche oder länger störte. Größere Unternehmen verfügen zwar über robustere Sicherheitsprotokolle, sind jedoch keineswegs vor solchen Angriffen gefeit. In der Tat betrafen Ransomware-Störungen prozentual am stärksten die Unternehmen in der Kategorie 1000 bis 2499 Mitarbeiter (71 %), 2500 bis 4999 Mitarbeiter (72 %) und 5000 bis 9999 Mitarbeiter (70 %). Anders gesagt: Unabhängig von seiner Größe ist kein Unternehmen gegen solche Angriffe immun.

Dieselbe Befragung zeigt auch, dass Endgeräte der Hauptangriffspunkt für Ransomware-Angriffe sind. Zu den Einfallstoren für Angriffe gehören das Browsen im Internet (21 %), Wechseldatenträger (18 %), E-Mail-Anhänge (17 %), die Lieferkette (17 %), URLs in einer E-Mail (14 %) und der Zugriff durch Insider (8 %).

Da auch weiterhin mehr Mitarbeiter hybrid oder remote arbeiten, sind Ransomware und andere Sicherheitsrisiken für die IT-Abteilung noch problematischer geworden. IDCs Endpoint Security Survey aus dem Dezember 2022 zeigte, dass über 97 % der Unternehmen einen Teil ihrer Mitarbeiter remote arbeiten lassen. Auch wenn diese Zahl in den kommenden 12 Monaten etwas zurückgehen dürfte, wird sie in absehbarer Zukunft sehr hoch bleiben.

Angesichts der anhaltenden Probleme, die Unternehmen mit einer großen Anzahl von Remotemitarbeitern haben, setzen immer mehr Unternehmen auf Zero-Trust-Strategien. Zu den Schwerpunkten der Best Practices gehören die Einrichtung einer Baseline von Sicherheitskontrollen, fortschrittliche Endgerät-Sicherheitsmaßnahmen, Geräte-Attestierung (um sicherzustellen, dass sich nur legitime Geräte mit dem Netzwerk verbinden) und eine robuste Benutzerauthentifizierung.

Berücksichtigt man all das, überrascht es nicht, dass die Teilnehmer in unserer Umfrage mehrheitlich die Verbesserung der allgemeinen Datensicherheit und die Gewährleistung der Sicherheit von Rechnern als ihre wichtigsten IT-Prioritäten wählten (siehe Abbildung 1).

Es ist erwähnenswert, dass in der nachstehenden Abbildung das drittwichtigste IT-Thema die Verbesserung der Mitarbeiterproduktivität durch bessere Geräte war. Als die Teilnehmer gebeten wurden, ihre drei wichtigsten Themen insgesamt zu nennen, wurde „Bessere Geräte“ am häufigsten gewählt. Dies ist eine wichtige Erkenntnis, an die die IT sich erinnern sollte: Sicherheit ist wichtig, aber sie darf nicht auf Kosten der Mitarbeiterproduktivität gehen. Die besten Geräte kombinieren hervorragende Sicherheit und Endbenutzerzufriedenheit ohne Behinderung durch die Sicherheit.

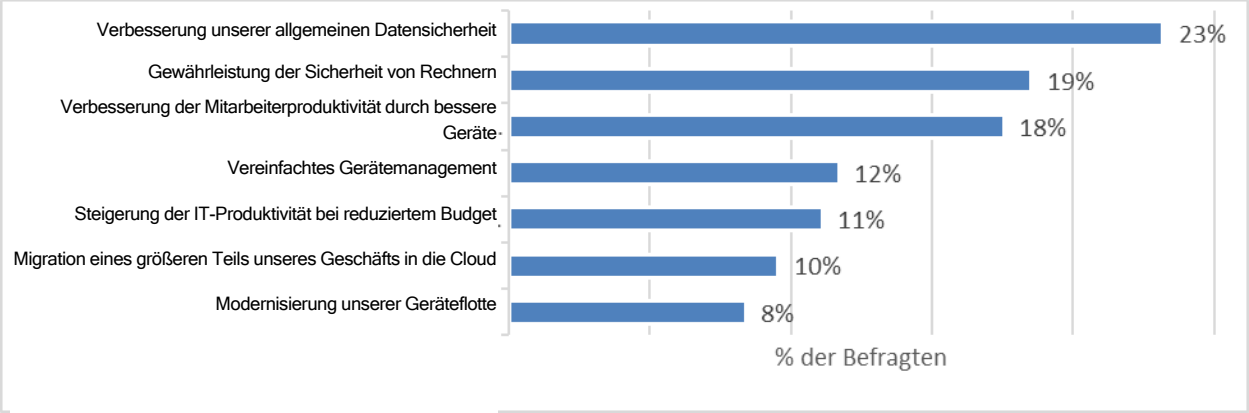
Auf die Frage an IT-Entscheidungsträger, was für sie der wichtigste Faktor bei der Wahl ihres nächsten Computeranbieters ist, stand die Sicherheit an erster Stelle – noch vor Leistung, der Unterstützung bestehender Anwendungen und der Integration in die vorhandene IT-Infrastruktur. Besonders interessant ist, dass „Spezifikationen“ ganz am Ende der Liste standen.

Einen Überblick über die wichtigsten IT-Prioritäten finden Sie in Abbildung 1. Die wichtigsten Überlegungen bei der Auswahl eines Computeranbieters finden Sie in Abbildung 2.

ABBILDUNG 1

Wichtigste IT-Prioritäten: Daten- und Endgerätesicherheit

F. Welche der folgenden IT-Themen haben für Ihr Unternehmen derzeit hohe Priorität?



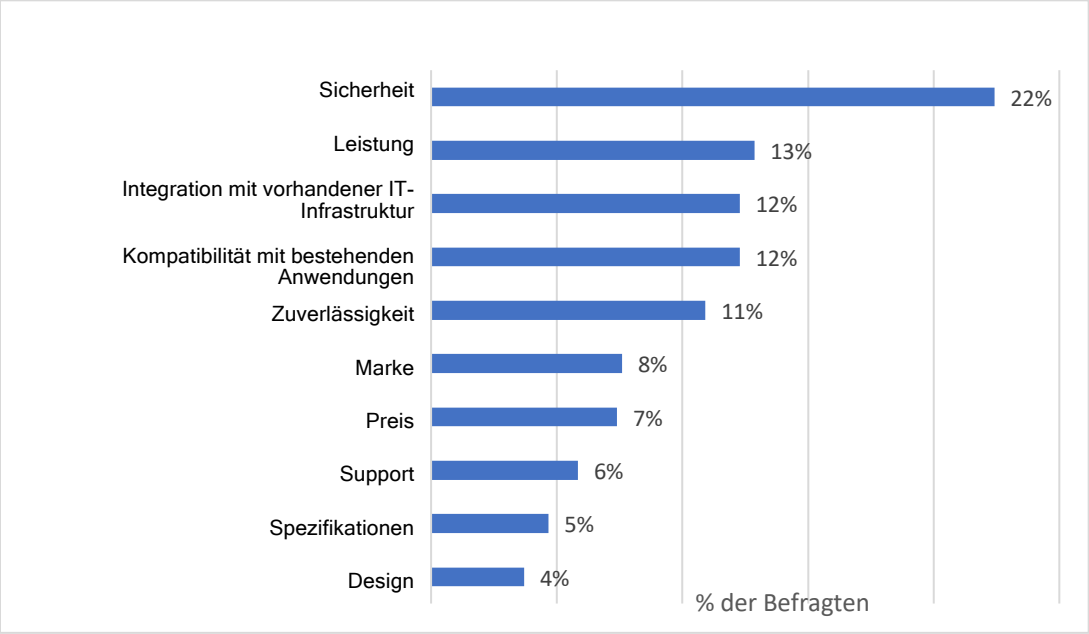
Quelle: IDCs Secure Endpoint Survey, n=513

Hinweis: Die Daten umfassen die als am wichtigsten eingestuften Optionen (Einstufung als Nr. 1).

ABBILDUNG 2

Wichtigste Faktoren bei Auswahl eines Computeranbieters

F. Was sind die wichtigsten Entscheidungsfaktoren bei Auswahl eines Rechners für Ihr Unternehmen?



Quelle: IDCs Secure Endpoint Survey, n=513

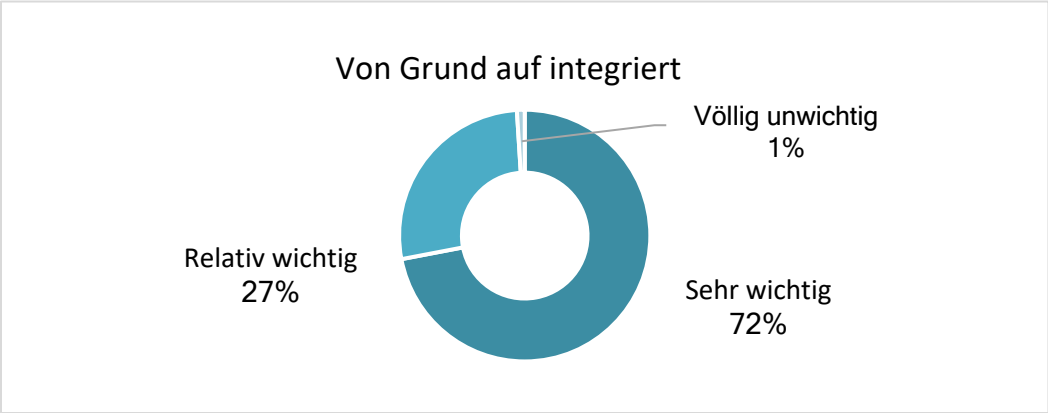
Hinweis: Die Daten umfassen die als am wichtigsten eingestuften Optionen (Einstufung als Nr. 1).

Zwei Konzepte, die bei den Teilnehmern auf großen Zuspruch trafen, waren integrierte Sicherheit und integrierter Schutz von Daten. Die Frage lautete: „Wie wichtig finden Sie es, Rechner von Grund auf mit Sicherheit auszustatten – einschließlich Prozessor, Firmware und Betriebssystem –, um sie vor aktuellen und zukünftigen Bedrohungen zu schützen?“. Die Antwort war überwältigend positiv: 72 % sehen dies als sehr wichtig und 27 % als relativ wichtig. Nur 1 % sahen es als überhaupt nicht wichtig. Bei Aufschlüsselung der Daten fällt auf, dass bei IT-Entscheidungsträgern aus Unternehmen des Gesundheitswesens und des Finanzsektors der Prozentsatz derer, die das Thema als sehr wichtig einstuften, noch höher war (84 % bzw. 75 %). Das Konzept des integrierten Schutzes von Daten erhielt eine ähnlich hohe Bewertung. Die Frage lautete: „Wie wichtig ist es Ihrer Meinung nach, dass Funktionen zur Datenverschlüsselung in die Rechner-Hardware integriert sind?“. 71 % sahen dies als sehr wichtig, 29 % als relativ wichtig und 0 % als unwichtig. Einzelheiten zur integrierten Sicherheit und zur integrierten Datenverschlüsselung finden Sie in Abbildung 3.

ABBILDUNG 3

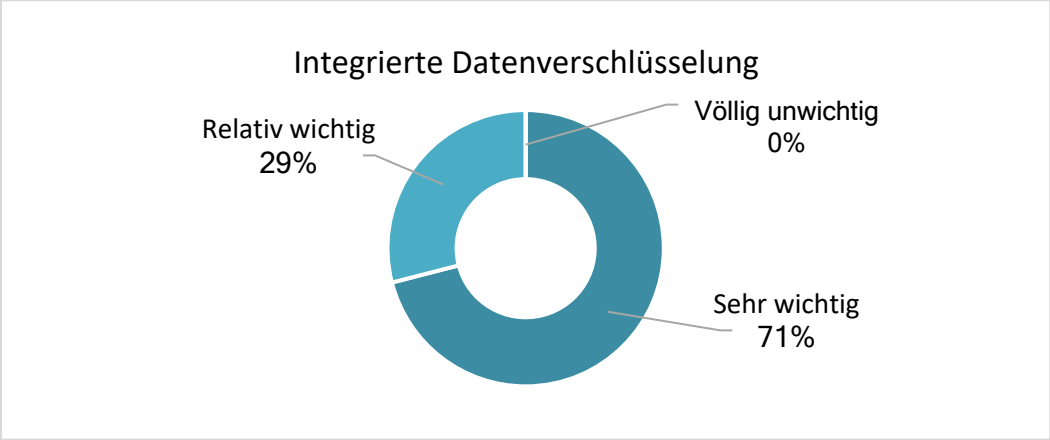
Bedeutung integrierter Sicherheit und integrierter Datenverschlüsselung

F. Wie wichtig finden Sie es, Rechner von Grund auf mit Sicherheit auszustatten - einschließlich Prozessor, Firmware und Betriebssystem -, um sie vor aktuellen und zukünftigen Bedrohungen zu schützen?



Quelle: IDCs Secure Endpoint Survey, n=513

F. Wie wichtig ist es Ihrer Meinung nach, dass Funktionen zur Datenverschlüsselung in die Rechner-Hardware integriert sind?



Quelle: IDCs Secure Endpoint Survey, n=513

Hardware mit von Grund auf integrierter Sicherheit und Datenverschlüsselung ist von maßgeblicher Bedeutung, jedoch wissen Sicherheitsexperten auch, dass das schwächste Glied in jeder Sicherheitskette in der Regel die Endbenutzer selbst sind. Deswegen ist die Benutzerauthentifizierung so entscheidend, und die Technologieanbieter arbeiten hart an der Weiterentwicklung der Authentifizierung. Leider zeigt unsere Befragung, dass viele Unternehmen hier im Rückstandsind.

Positiv ist zu verzeichnen, dass 68 % der Unternehmen den Befragten zufolge komplexe Passwörter verlangen, und dass 63 % zweistufige Authentifizierung verwenden. Weniger positiv ist, dass nur 23 % Single-Sign-On-Technologien (SSO) einsetzen und nur 20 % biometrische Sicherheit (wie Fingerabdruck oder Gesichtserkennung) verwenden. Es ist anzumerken, dass 56 % der Befragten die biometrische Authentifizierung als deutlich sicherer als Passwörter bezeichneten, 35 % als etwas sicherer, 9 % als gleich sicher und keiner der Befragten (0 %) als weniger sicher.

Eine wichtige neue Authentifizierungstechnologie, die kürzlich eingeführt wurde, ist der Passkey (Hauptschlüssel). Ein Passkey ist eine digitale Anmeldeinformation, die ein Schlüsselpaar nutzt und so viel sicherer als ein Passwort ist. Da diese Technologie neu ist, setzen nur 14 % der Unternehmen den Befragten zufolge diese ein, aber kluge IT-Entscheidungsträger sollten sich schon heute genau mit dieser Technologie auseinandersetzen. Einzelheiten zur Verwendung der Benutzerauthentifizierung finden Sie in Abbildung 4.

ABBILDUNG 4

Methoden zur Benutzerauthentifizierung

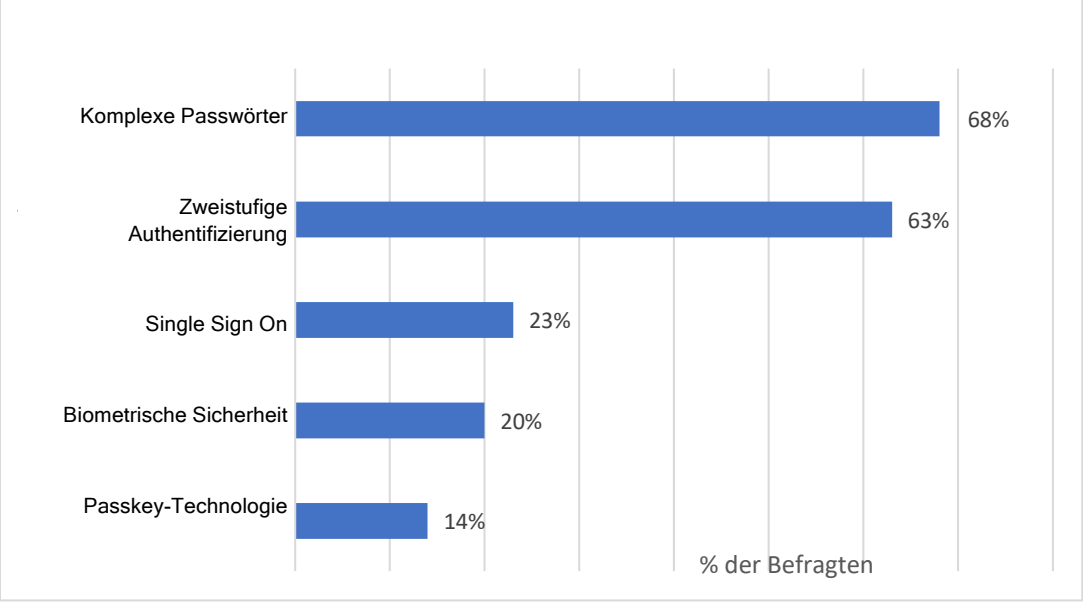
F1. Verlangt Ihr Unternehmen von Mitarbeitern die Verwendung komplexer Passwörter zur Anmeldung am Rechner?

F2. Gibt es in Ihrem Unternehmen Rechner, die biometrische Sicherheitsmaßnahmen wie Fingerabdruck-Scans unterstützen?

F3. Hat Ihr Unternehmen schon begonnen, sich mit den Vorteilen der Passkey-Technologie auseinanderzusetzen?

F4. Ist in Ihrem Unternehmen eine zweistufige Authentifizierung erforderlich?

F5. Nutzt Ihr Unternehmen Single-Sign-On (SSO)-Funktionen? (J/N)



Quelle: IDCs Secure Endpoint Survey, n=513

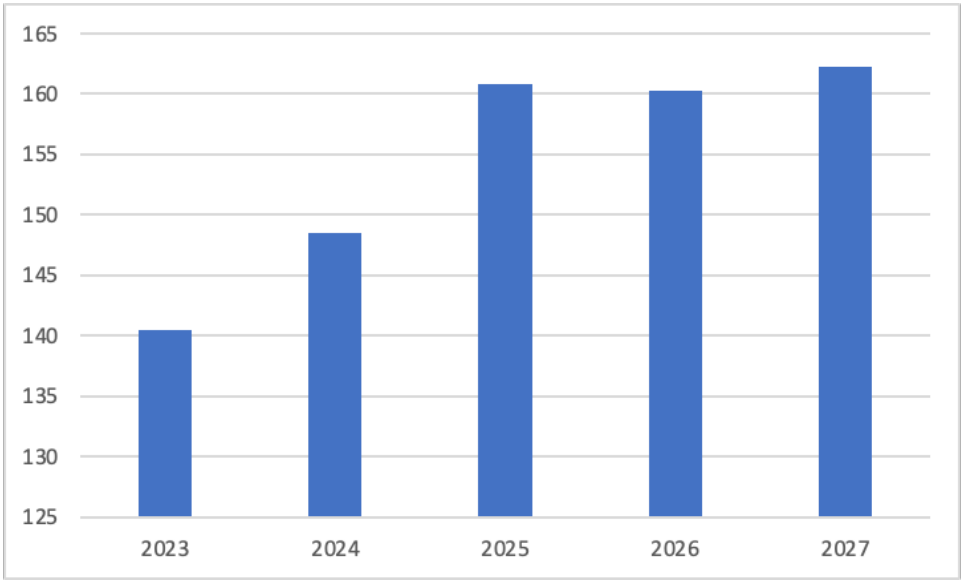
Die Daten geben der Prozentanteil der Ja-Antworten wieder.

Ein erschreckend hoher Anteil der teilnehmenden Unternehmen nutzt noch nicht einmal grundlegende Authentifizierungsprotokolle wie komplexe Passwörter (32 %) oder zweistufige Authentifizierung (37 %). **Eine vielversprechende Möglichkeit** besteht darin sicherzustellen, dass Ihr Unternehmen in der gesamten Organisation eine einheitliche Authentifizierungsform einführt. Nach Implementierung dieser Grundlage sollten SSO-Funktionen in Kombination mit einem robusten Master-Authentifizierungsprotokoll in Erwägung gezogen werden. Schließlich sollten Sie sich bei Ihrem nächsten Hardware-Upgrade Computer genauer ansehen, die Authentifizierung höchster Ebene unterstützen können: biometrische Sicherheit und Passkey-Technologie. Bei Ermöglichung von Biometrie und Passkeys können sich Mitarbeiter zukünftig schnell und sicher bei ihren Rechnern und von dort aus sofort bei ihren Apps und Websites anmelden.

Mit diesem letzten Aspekt – dem nächsten Hardware-Upgrade – beenden wir diesen Abschnitt. In vielen Unternehmen ist die Rechnerflotte veraltet und muss ersetzt werden. Selbst wenn Ihr Unternehmen einen erheblichen Anteil neuer Endgeräte erst 2020 gekauft hat, rückt für diese Rechner schnell ein Alter von vier Jahren heran. In der Zwischenzeit hat sich die Hardwaresicherheit ständig gemäß den entstehenden Bedrohungen weiterentwickelt. Möglicherweise ebenso wichtig ist, dass viele dieser Produkte vor dem großen Wandel hin zu Remote- und Hybridarbeit gekauft wurden und somit nicht über hochwertige Kameras, Mikrofone und Lautsprecher verfügen, die die Mitarbeiter jetzt für wichtige Onlinekonferenz- und Collaboration-Apps benötigen. Nach mehreren Jahren mit rückläufigen Umsätzen prognostiziert der Personal Computing Device Tracker von IDC für die nächsten Jahre ein Wachstum in dieser Kategorie. Hinweis: Gewerbliche Einheiten sind Einheiten, die von Nicht-Verbrauchern gekauft werden. Die Prognose von IDC für Rechner für private und gewerbliche Zwecke ist in Abbildung 5 dargestellt.

ABBILDUNG 5

Weltweite Prognose für gewerbliche Rechner



Quelle: IDC PCD Tracker, August 2023

Unternehmen sollten den Rechnerbedarf ihrer Mitarbeiter ständig neu bewerten, um auf dem Markt wettbewerbsfähig zu bleiben und Spitzenkräfte zu werben und zu binden. Während die IT-Abteilung früher schwierige Kompromisse zwischen Sicherheit und Mitarbeiterzufriedenheit eingehen musste, kann der richtige Anbieter heute zu einer Lösung ohne erforderliche Abstriche beitragen. Schließlich ist eine **weitere empfehlenswerte Best Practice** die Anwendung von Zero-Trust-Zugriffsprinzipien im Zuge Ihrer nächsten Hardware-Bereitstellung. Bei dieser Strategie wird davon ausgegangen, dass alle Geräte, die auf Unternehmensressourcen zugreifen wollen, erst nach Überprüfung als vertrauenswürdig gelten. Zero-Trust setzt Technologien und Prozesse ein, um den Sicherheitsstatus des Geräts (am besten vom Prozessor bis hin zu kritischen IT- und Sicherheitsanwendungen), des für die Verbindung verwendeten Netzwerks (z. B. öffentliches WLAN oder privates Netzwerk) und die Benutzeridentität zu bestätigen.

Erwägungen zum Mac im Unternehmen

Immer mehr IT-Abteilungen unterstützen heutzutage Macs, und unsere Umfrage verweist auf einen entscheidenden Grund dafür. 76 % der Befragten, die einen Mix verschiedener Betriebssysteme ihrer installierten Geräteflotte repräsentieren, sagten, dass sie Macs für sicherer als andere Rechner halten. Der wichtigste Grund für die Einführung von Macs in den nächsten 12 Monaten ist die Überzeugung, dass Macs sicherer sind (47 %), dicht gefolgt von der einfachen Bereitstellung und dem unkomplizierten Management (36 %).

Apple ist ganz auf ein großartiges Benutzererlebnis bei gleichzeitig verbesserter Sicherheit fokussiert, indem die Sicherheit bei Apple vom Prozessor bis hin zur Software eingebettet wird. Ein Beispiel dafür ist die Touch ID von Apple, eine integrierte biometrische Sicherheitsfunktion. Apple Hardware verfügt über Secure Enclave: Damit wird der Passcode zum Schutz der Touch ID-Daten verschlüsselt und gesichert.

Apple Kunden-Spotlight

„Eine der wirklich wichtigen Eigenschaften von Apple-Produkten ist, dass Schutz der Daten und Sicherheit in das Produkt selbst eingebettet sind. Sie sind kein nachträglicher Gedanke und das wissen wir sehr zu schätzen.“ – Linda Jojo, Executive Vice President und Chief Customer Officer, United Airlines

Um das Risiko kompromittierter Betriebssysteme und Startsequenzen auszuschalten, haben Macs Secure Boot und Signed System Volume. Mit Secure Boot kann beim Start nur die kryptografisch zertifizierte Version von macOS gestartet werden und Signed System Volume schützt die Integrität des Betriebssystems während der Laufzeit. Auch veraltete Software bedeutet ein Cyberrisiko: Apple minimiert dies durch die Automatisierung und Sicherung der End-to-End-Distribution und -Installation von Softwareupdates.

Hervorragende Software von Drittanbietern ist für die Mitarbeiterproduktivität entscheidend, aber sie muss auch frei von Malware sein. Apple verfolgt einen vielschichtigen Ansatz zur Verhinderung von Schadsoftware. Der Mac App Store von Apple prüft jede App auf Malware. Da Software für Macs auch aus dem Internet heruntergeladen werden kann, verpflichtet Apple die Entwickler dazu, ihre Anwendungen dem Apple Notary Service vorzulegen, der auch auf Malware scannt. Apples Gatekeeper (im macOS inbegriffen) prüft die Beglaubigung durch den Notarservice und verhindert die Ausführung nicht signierter Anwendungen. Zudem blockiert und entfernt XProtect – das Anti-Malware-Tool von Apple – jede bekannte Schadsoftware.

Daten gehören zu den wertvollsten Ressourcen eines Unternehmens und müssen entsprechend geschützt werden. Die Kombination aus prozessor-gesicherter FileVault-Verschlüsselung, von Apple

unterstützten VPN-Protokollen und End-to-End-Verschlüsselung in Apple-Diensten (z. B. iMessage und iCloud) gewährleistet den Schutz von Daten in Ruhe, im Transit und bei Nutzung.

Da Social Engineering zu den raffiniertesten Fähigkeiten der Bedrohungsakteure gehört, müssen die Endbenutzer in der Abwehr wachsam sein. Dies ist eine schwierige Aufgabe – aber Apple unterstützt hier mit der Safari-Warnung vor betrügerischen Websites. Da Authentifizierungsdaten oft von Bedrohungsakteuren gestohlen werden, erleichtert die Passkey-Unterstützung durch Apple Unternehmen die Modernisierung ihrer Authentifizierungsmethoden, ohne dabei die positive Endbenutzererfahrung zu opfern.

Gute Sicherheit ist auf robustes Gerätemanagement abgestimmt. Hierfür bietet Apple eine Reihe von Gerätemanagement-Funktionen, u. a. das integrierte Management-Framework mit Mobile Device Management (MDM). Der Apple Business Manager erlaubt die Zero-Touch-Bereitstellung und ist mit MDM-Lösungen verbunden. Die Endpoint Security APIs für Mac ermöglichen wiederum Entwicklern die Erstellung von Lösungen für Überwachung und Analyse von Sicherheitsgefahren und die Reaktion darauf. Apple bietet auch Identitätsintegrationen mit einem integrierten SSO-Framework, das mit modernen Identitätsanbietern (IdPs) zusammenarbeitet.

Und schließlich stellt Apple diese Sicherheitsfunktionen, inklusive größerer und kleinerer Softwareupdates, seinen Unternehmens- oder Privatkunden über macOS ohne zusätzliche Kosten bereit.

CHANCEN/HERAUSFORDERUNGEN

Trotz einer sich ständig entwickelnden Bedrohungsumgebung steht die IT vor der Schwierigkeit, mit weniger Geld, weniger IT-Mitarbeitern und weniger Ressourcen mehr bewirken zu sollen. Neben der Handhabung laufender Sicherheitsrisiken, mit denen alle Unternehmen konfrontiert sind, sollen viele IT-Organisationen auch die Produktivität und Zufriedenheit der Mitarbeiter anhand der von ihnen bereitgestellten Hardware, Software und Leistungen messbar verbessern. Die erfolgreiche Bewältigung beider Aufgaben – Verbesserung der Sicherheit ebenso wie der Mitarbeiterproduktivität und -zufriedenheit – mag fast unmöglich scheinen. Sie stellt für die IT aber auch eine große Chance dar. Sie bietet die Möglichkeit, eingekaufte Hardware, Software und Leistungen, die Anbieter und die Form des Einsatzes für die zunehmend hybride Belegschaft ganz neu zu beurteilen. Zudem ist es dringend notwendig, die Modelle der Gesamtbetriebskosten (Total Cost of Ownership, TCO) neu durchzurechnen, damit sie besser widerspiegeln, wie Unternehmen heute Technologie kaufen und nutzen.

FAZIT

Sicherheit ist eine Hauptsorge der IT und wird dies auch bleiben. In einer Zeit knapper IT-Budgets, in der umfangreiche Hardware-Upgrades anstehen, ist eine Neubewertung der Anbieter sinnvoll, bei denen Sie in Zukunft Geld ausgeben wollen. Überlegen Sie die Implementierung von Best Practices für die Authentifizierung und Zero-Touch-Bereitstellungen und kaufen Sie Hardware, die diese Veränderungen möglich macht. Priorisieren Sie Sicherheit nicht auf Kosten der Mitarbeiterproduktivität und -zufriedenheit und nutzen Sie stattdessen Anbieter von Rechnern mit integrierter Sicherheit und Datenverschlüsselung, bei denen Sie sich auf die Bereitstellung von sowohl Sicherheit als auch positiver Endbenutzererfahrung verlassen können.

Über IDC

International Data Corporation (IDC) ist der weltweit führende Anbieter von Marktinformationen, Beratungsdienstleistungen und Veranstaltungen auf dem Gebiet der Informationstechnologie und der Telekommunikation sowie der Verbrauchertechnologiemärkte. IDC unterstützt IT-Profis, Geschäftsleute und Investoren bei fundierten Entscheidungen über Geschäftsstrategien und den Einkauf von Technologie. Mehr als 1100 IDC-Analysten in mehr als 110 Ländern bieten globale, regionale und lokale Expertise zu Chancen und Trends in Technologie und Wirtschaft. Seit 50 Jahren bietet IDC strategische Einsichten, um unseren Kunden zu helfen, ihre wichtigsten geschäftlichen Ziele zu erreichen. IDC ist ein Tochterunternehmen von IDG, einem weltweit führenden Medien-, Forschungs- und Veranstaltungs-Technologieunternehmen.

Internationaler IDC-Hauptsitz

140 Kendrick Street
Building B
Needham, MA 02494, USA
USA
+1 508 872 8200
Twitter: @IDC
blogs.idc.com
www.idc.com