PRÄSENTATION

JANUAR 2025

Sicherheit von Endgeräten: Wie Dell dabei hilft, KI-Einführung mit Cyber-Resilienz in Einklang zu bringen

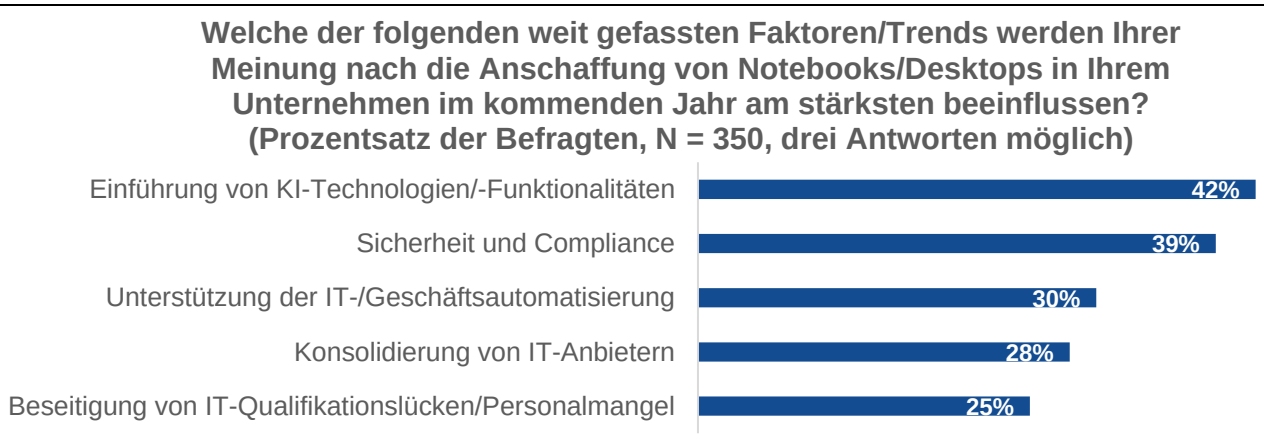
Gabe Knuth, Senior Analyst

Zusammenfassung: Die Bedeutung der Sicherheit von Endgeräten nimmt zu, da sowohl Unternehmen als auch Cyberkriminelle immer mehr KI-Lösungen einführen. Jüngste Untersuchungen der Enterprise Strategy Group von Informa TechTarget zeigen, welchem doppelten Druck IT-Teams ausgesetzt sind: Sie müssen für ausgeklügelte Cyberbedrohungen gerüstet sein und gleichzeitig transformative Innovationen ermöglichen.[1] In diesem Whitepaper wird untersucht, wie die Kombination aus Sicherheit unterhalb des Betriebssystems (below-the-OS security), sicherer Lieferketten-Verfahren und umfassenden Services Dell zu einem vertrauenswürdigen Partner für Unternehmen macht, die ihre Sicherheitslage stärken möchten.

Überblick – Das Problem

Da Unternehmen mit sich ständig weiterentwickelnden Cybersicherheitsbedrohungen konfrontiert sind, ist Sicherheit oft der Eckpfeiler jeder Technologieentscheidung. Dies gilt sowohl für die Cloud und das Rechenzentrum als auch für den PC, wo laut einem kürzlich von Dell in Auftrag gegebenen Forschungsprojekt der Enterprise Strategy Group Sicherheit zu den wichtigsten Merkmalen gehört, die den Kauf von Desktops und Laptops beeinflussen (siehe Abbildung 1). Besonders hervorzuheben ist, dass Unternehmen der Einführung von KI-Technologien und -Funktionalitäten eine ähnliche Priorität eingeräumt haben. Dies unterstreicht, dass Unternehmen vor Herausforderungen stehen, transformative Technologien wie KI zu integrieren und gleichzeitig Endgeräte vor immer komplexeren Cyberbedrohungen zu schützen.

Abbildung 1. Die 5 wichtigsten Faktoren, die den Kauf von Endgeräten beeinflussen



Quelle: Enterprise Strategy Group, ein Geschäftsbereich von Informa TechTarget

[1] Quelle: Enterprise Strategy Group Custom Research im Auftrag von Dell, *Client Trends and Competitive Landscape*, Juni 2024. Alle Forschungsreferenzen und Diagramme der Enterprise Strategy Group in dieser Präsentation stammen aus dieser Forschungsstudie, sofern nicht anders angegeben.

Das ist natürlich keine Überraschung. KI erweist sich bereits in an Benutzerinnen und Benutzer gerichtete Anwendungen als transformierend, sodass der Aufstieg auf der Prioritätsleiter so gut wie sicher war. Aber all die Dinge, die KI für die Benutzerproduktivität, Kreativität und das Geschäft im Allgemeinen tut, können sich auch Cyberkriminelle zunutze machen. Das bedeutet, dass diese Kombination aus KI-Einführung und Sicherheit (oder das Trio, wenn man Compliance separat betrachtet) wahrscheinlich immer Hand in Hand gehen wird.

Während die KI-Nutzung und die Bedenken von vielen Unternehmen noch immer definiert werden, sind sicherheitsbezogene Herausforderungen bereits etabliert, wie z. B.:

- Einhaltung der Hardware- und Software-Upgradezyklen (von 32 % der Befragten angegeben).
- Schutz vertraulicher Daten auf Laptops und Desktops (29 %)
- Ermöglichung der Hybridarbeit (27 %)
- Unterstützung einer wachsenden Zahl von Endusern (27 %)
- Patchmanagement (20 %)
- Management nicht autorisierter Anwendungsnutzung oder Konfigurationsänderungen (17 %)

Diese „klassischen“ Herausforderungen in Verbindung mit dem Aufkommen von KI und der zunehmenden Ausgereiftheit und dem zunehmenden Ausmaß von Angriffen zeichnen ein wenig beneidenswertes Bild für die IT. In Wahrheit ist es nicht möglich, alles zu blockieren. Daher ist es wichtig, alle verfügbaren Tools zu nutzen, um den Herausforderungen von heute und den Herausforderungen von morgen einen Schritt voraus zu sein.

Was können Unternehmen tun?

Um diese Herausforderungen zu bewältigen, müssen Unternehmen Sicherheitsfunktionen nutzen, die ihnen helfen, ihre aktuellen Initiativen auszubauen. Oft bedeutet dies, dass man über grundlegende Sicherheitsmaßnahmen und Schulungen für Enduser hinausschaut und sich stattdessen auf einen umfassenderen, mehrschichtigen Ansatz konzentriert, der zur Verbesserung der langfristigen Cyberresilienz beitragen kann.

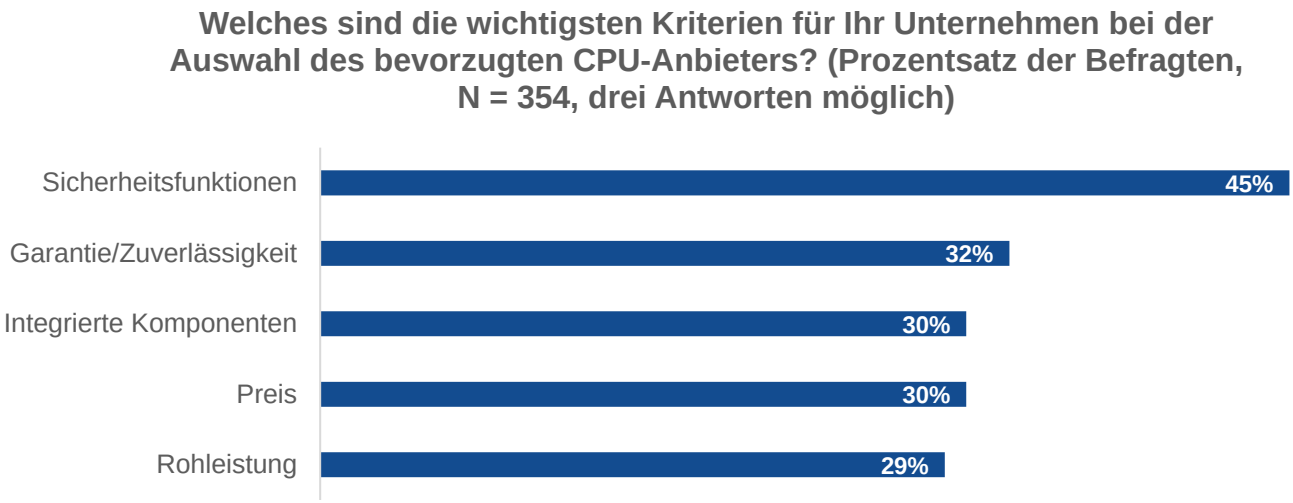
Eine der Ebenen, die häufig übersehen (oder zumindest vernachlässigt) wird, ist die Rolle, die die Sicherheit auf Hardwareebene, die sog. „Below-the-OS“-Sicherheit, spielt. Hardwarebasierte Sicherheit reduziert die gesamte Angriffsfläche eines Computers, wodurch Angriffe abgewehrt werden können, bevor sie sich verfestigen können. Eine stärkere Basissicherheit ergänzt softwarebasierte Konfigurations-, Analyse- und Fehlerbehebungstools, wodurch die Belastung der IT-Ressourcen verringert wird, die erkannte Probleme und Warnungen ständig analysieren.

Wenn die Hardware so große Bedeutung hat, warum wird sie dann so oft übersehen? Zu oft wird Hardware als Gebrauchsgegenstand angesehen – als notwendiges Übel, das Patches und Wartung erfordert. Oder, noch schlimmer, die Hardware wird bereitgestellt und dann völlig vergessen. Die Realität ist jedoch, dass jede Chipsatzgeneration mit erweiterten Sicherheitsfunktionen ausgestattet ist, die sowohl gegen Angriffe auf Firmware- als auch Hardwareebene schützen können. Neuerdings verfügt die Hardware über integrierte Sicherheitsmaßnahmen, die mit betriebssysteminternen Sicherheitstools zusammenarbeiten können, um tief in Anwendungen anomale Verhaltensweisen zu erkennen.

Während die Aktualisierung eines Geräts oder seiner Firmware in der Vergangenheit als etwas angesehen wurde, das nur dann durchgeführt wurde, wenn es veraltet war oder ein Problem auftrat, ist es in Wirklichkeit so, dass diese Updates häufig die allgemeine Sicherheitslage verbessern, insbesondere da diese Updates für

Enduser-Geräte gelten! Aus diesem Grund stehen Sicherheitsfunktionen ganz oben auf der Liste der Kriterien für die Auswahl eines CPU-Anbieters (siehe Abbildung 2).[2]

Abbildung 2. Die 5 wichtigsten Faktoren bei der Wahl eines CPU-Anbieters



Quelle: Enterprise Strategy Group, ein Geschäftsbereich von Informa TechTarget

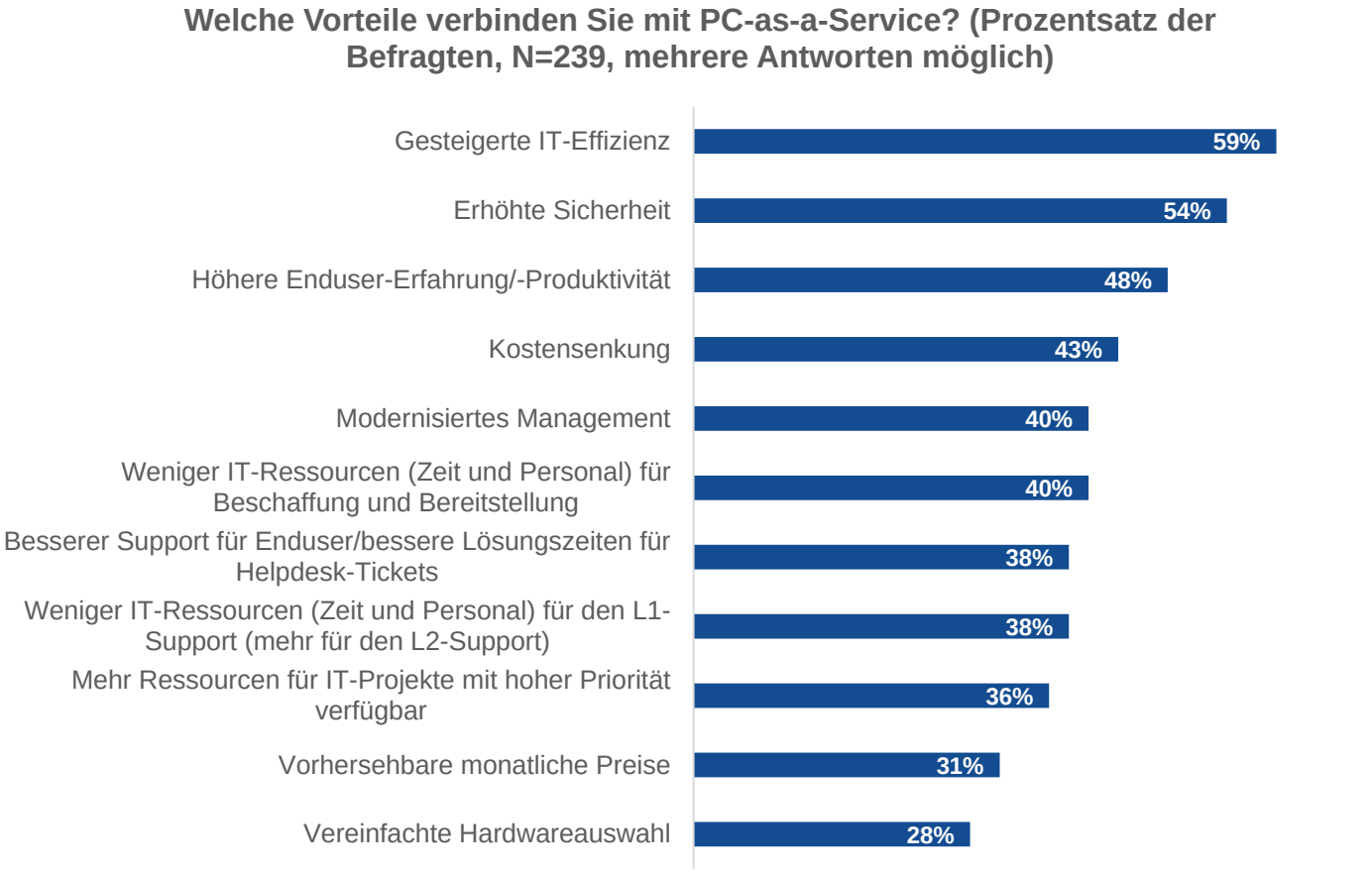
Es gibt auch Sicherheitsaspekte, die von Administratoren nicht oft in Betracht gezogen werden, wie die Sicherheit der Lieferkette, die von 40 % der Unternehmen als eine ihrer größten Herausforderungen bei der Beschaffung von Notebooks/Desktop-PCs bezeichnet wurde (nach Kostenmanagement, wachsenden Anforderungen der Enduser und Lieferzeit).

Insgesamt zeigt dies, dass Unternehmen mit Anbietern zusammenarbeiten müssen, die sich für Hardware- und Lieferketten-Sicherheit einsetzen. Dies wird sicherlich bei der Beschaffung hilfreich sein. Wenn wir uns jedoch in Erinnerung rufen, dass 32 % der Unternehmen Schwierigkeiten haben, mit den normalen Upgradezyklen Schritt zu halten, und 20 % das Patchmanagement als eine Herausforderung bezeichneten, können wir daraus schließen, dass Unternehmen auch bei den täglichen Sicherheitsaufgaben Hilfe benötigen könnten.

Angesichts dessen ist es nicht verwunderlich, dass Unternehmen zunehmend auf Managed Services wie „PC-as-a-Service“ (PCaaS) zurückgreifen. PCaaS vereinfacht die Beschaffung und den Support, indem es unterschiedliche Geräte und Servicelevels zu monatlichen Betriebskosten anbietet. Die Umfrage befragte die Teilnehmenden, die PCaaS verwenden, zu den wichtigsten Vorteilen, die sie damit verbinden. IT-Effizienz (59 %), erhöhte Sicherheit (54 %) und bessere Enduser-Erfahrung/-Produktivität (48 %) standen bei den Antworten im Vordergrund (siehe Abbildung 3). Dies zeigt, dass Services auch bei einem mehrschichtigen Sicherheitsansatz eine wichtige Rolle spielen können.

[2] Quelle: Vollständige Umfrageergebnisse der Enterprise Strategy Group, *Endpoint Device Trends*, Februar 2024.

Abbildung 3. PCaaS bietet weitreichende Vorteile, einschließlich erhöhter Sicherheit



Quelle: Enterprise Strategy Group, ein Geschäftsbereich von Informa TechTarget

Wie Dell Ihnen helfen kann

Als Marktführer in allen bisher diskutierten Bereichen (KI, Sicherheit, Benutzererfahrung usw.) befindet sich Dell in einer einzigartigen Position, um Kundinnen und Kunden bei der Erreichung ihrer Ziele zu unterstützen. Dell ist sich bewusst, dass die Sicherheit über den gesamten Lebenszyklus des Geräts hinweg umfassend sein muss, von der Lieferkette bis zum Recycling. Dell kontrolliert seine Lieferkette streng und gewährleistet Sicherheit und Verfügbarkeit über verschiedene globale Chip-Hersteller, -Einrichtungen und -Vertriebskanäle.

Die kommerziellen PCs und Laptops bieten über Dell Trusted Device und Dell SafeBIOS „Below-the-OS“-Sicherheit, d. h. eine Reihe von Funktionen, die die Integrität des Geräts bis hin zum BIOS- und Firmware-Level schützen. Dieses Feature in Verbindung mit Intel Core Silizium bedeutet, dass kommerzielle Dell-Geräte umfassende Sicherheit auf Hardwareebene bieten, die die Angriffsfläche jedes Geräts minimiert. Diese Kombination von Dell Trusted Devices mit Intel Prozessoren ist einer der Gründe, warum Dell als führendes Unternehmen bei der Sicherheit von Endgeräten gilt. Dell bietet auch eine eigene Software an, um sicherzustellen, dass Firmware, BIOS und Treiber des Geräts auf dem neuesten Stand sind. Dies ist besonders wichtig für Unternehmen, die mit der nicht autorisierten Nutzung von Apps und dem Patch-Management zu kämpfen haben.

Schließlich bietet Dell eine flexible Palette von Services zur Unterstützung von Unternehmen, die mit den wachsenden Anforderungen an das Management der Sicherheit von Endgeräten überfordert sind. ProSupport und ProSupport Plus bieten erweiterte technische Unterstützung und vorausschauende Problemlösung, um

sicherzustellen, dass Geräte sicher und betriebsbereit sind und nur minimale Ausfallzeiten auftreten. Für Unternehmen, die den IT-Betrieb weiter simplifizieren möchten, bietet Dell APEX PC-as-a-Service (APCaaS) eine umfassende Lösung, indem Hardware, Software und Lifecycle-Services in einem vorhersehbaren, abonnementbasierten Modell zusammengefasst werden.

Dieser ganzheitliche Ansatz, der eine ausgefeilte Lieferkette, modernste Hardware, robuste Software und flexible Services kombiniert, gibt Unternehmen den Vorsprung, den sie benötigen, um die Sicherheitsprobleme zu überwinden, die mit modernen Endgeräten verbunden sind, indem IT-Teams in die Lage versetzt werden, selbst angesichts zunehmender Komplexität und Ressourceneinschränkungen eine starke Sicherheitslage zu gewährleisten.

Fazit

Sicherheit ist eine ständige Herausforderung für IT-Teams und wird immer schwieriger, da dieselbe Technologie, die Ihren unternehmerischen Erfolg unterstützt, auch den Cyberkriminellen hilft. Aber es muss kein verlorener Kampf sein. Auch wenn neue Trends wie KI immer höhere Priorität erlangen, ist es wichtig, sich auf die Notwendigkeit einer umfassenden Endgeräte-Sicherheit zu konzentrieren. Unternehmen können wichtige Schritte setzen, um ihre Herausforderungen zu bewältigen, indem sie einen mehrschichtigen Ansatz entwickeln, der Hardware, Software und Services nutzt.

Häufig geht es dabei um die Zusammenarbeit mit vertrauenswürdigen Partnern, weshalb sich das Portfolio von Dell hervorsticht. Der Fokus von Dell auf die Sicherheit auf Hardwareebene, End-to-End-Schutz des Lebenszyklus und flexible Serviceangebote stellt sicher, dass Kundinnen und Kunden über die Tools und den Support verfügen, die sie benötigen, um sowohl die täglichen Sicherheitsaufgaben als auch die langfristigen strategischen Ziele für die Verbesserung der Sicherheit zu erfüllen und gleichzeitig neue Technologien einzuführen und daraus Nutzen zu ziehen. Kurz gesagt, die Lösungen von Dell sind gut geeignet, um die Anforderungen moderner IT-Umgebungen zu erfüllen.

In einer Welt, in der KI und Sicherheit zu gleichermaßen wichtigen Prioritäten werden, müssen Unternehmen Strategien entwickeln, die das Endgerät sowohl zu einem Tool für Produktivität als auch zu einem Schlüsselelement der Cybersicherheitsziele eines Unternehmens machen. Die Fähigkeit von Dell, diese Prioritäten in einem einheitlichen Ansatz zu kombinieren, macht Dell zu einer natürlichen Wahl für Unternehmen, die Innovation, Zuverlässigkeit und Sorgenfreiheit schätzen.

Weitere Informationen finden Sie unter dell.com/endpoint-security.

Informationen zur Enterprise Strategy Group
Die Enterprise Strategy Group von TechTarget bietet fokussierte und umsetzbare Marktinformationen, Studien zur Nachfrage, Beratung durch Analysten, GTM-Strategieberatung, Lösungsvalidierungen und individuelle Inhalte als Unterstützung beim An- und Verkauf von Unternehmenstechnologien.

contact@esg-global.com
www.esg-global.com