TechTarget | Custom Media
White Paper

STARKE CYBERSICHERHEIT FÜR PCs DER NÄCHSTEN GENERATION UNTERSTÜTZEN

PCs waren früher ein leichtes Ziel für Hacker, und Cyberangriffe auf PCs haben für erhebliche negative finanzielle, betriebliche und regulatorische Auswirkungen gesorgt. Die PCs von heute und morgen profitieren jedoch von deutlichen Verbesserungen in den Methoden, mit denen sie geschützt werden. Das gilt sowohl in Bezug auf bewährte Praktiken für die Cybersicherheitshygiene als auch die Art und Weise, wie PCs – und ihre Kernkomponente – aufgebaut sind.

AMD
together we advance_

Einführung: Der Stand der Cybersicherheit für PCs ist … kompliziert.

Einerseits hat die Verwendung von PCs als ein wesentlicher Bestandteil riesiger, miteinander verbundener, globaler Netzwerke sie zu einem wichtigen Einstiegspunkt für Hacker gemacht – von ausgeklügelten Cybercrime-Banden über Schurkenstaaten bis hin zu böswilligen Insidern. Die bittere Realität ist, dass Endpunkte – von denen PCs die große Mehrheit ausmachen – ein häufiges Cybersicherheitsziel sind, um Anwendungen und Datenbanken zu infiltrieren und um seitlich in Netzwerken zu navigieren.

Es gibt jedoch auch gute Nachrichten: Organisationen sind sich jetzt bewusst, dass PCs und andere Endpunkte einen kritischen Angriffsvektor darstellen. Also haben sie wichtige Schritte unternommen, um ihre Cybersicherheitsverteidigung in ihrer breiten PC-Landschaft zu verstärken. Laut der Enterprise Strategy Group von TechTarget gibt fast die Hälfte – 44 % – der Organisationen an, dass die Stärkung der Cybersicherheit eine der wichtigsten Geschäftsprioritäten für ihre Endgerätestrategie ist.[1] Für Organisationen, die High-End-PCs mit „Premium-Preisen“ kaufen, ist Sicherheit der Kauftreiber Nr. 1 für diese Käufe.[2]

Viele dieser Schritte stellen eine zunehmende Nutzung bewährter Praktiken zum Schutz von PCs dar, z. B. verbesserte Sensibilisierung und Schulung der Benutzer, was beispielsweise die Vermeidung verdächtiger Hyperlinks und Anhänge oder die Beachtung von Passwortrichtlinien betrifft.

Ein weiterer wichtiger Schritt konzentriert sich jedoch auf die wichtigsten technologischen Fortschritte, die dem PC selbst zugrunde liegen. Sicherlich gibt es wertvolle und zuverlässige Sicherheitstools wie Endpunkterkennung und -reaktion, Verschlüsselung, Datenschutzlösungen und mehr. Aber auch wichtige technische Fortschritte werden auf dem PC selbst implementiert – insbesondere auf CPU-Ebene.

Heute und in der Zukunft ist die CPU mehr als nur ein unterstützendes Element für alles von der Rechnerleistung bis zur Energieverwaltung. Sie ist auch eine Sicherheitszentrale auf Chip-Ebene, über die Bedrohungen verhindert, erkannt, abgeschottet und entschärft werden.

Warum ein PC anfällig für Cyberangriffe ist

Egal, ob man es PC-Sicherheit nennt, wie es Cybersicherheitsexperten oft tun, oder Endpunktsicherheit, Organisationen müssen verstehen, dass persönliche Systeme oft der bevorzugte Angriffspunkt für versuchte Datenschutzverletzungen, Ransomware, Identitätsdiebstahl und andere Hacks sind. Wichtig ist, dass diese PC-basierten Angriffe oft genutzt werden, um die wertvollsten und wichtigsten Systeme einer Organisation auszuschalten, wie z. B. kritische Infrastruktur, geschäftskritische Anwendungen, geistiges Eigentum oder personenbezogene Daten.

Seit Jahren sind PCs nicht ausreichend gegen Cyberangriffe geschützt und verlassen sich zu oft auf einfache Antivirus-/Anti-Malware-Tools. Diese haben sich angesichts der immer raffinierteren Angriffe und Angreifer als völlig ungeeignet erwiesen, denn bei diesen Angriffen kommen oft innovative Tools mit künstlicher Intelligenz und Algorithmen für maschinelles Lernen zum Einsatz.

Zusätzlich hat der inzwischen verstärkte Trend zur Remote-/Hybrid-Arbeit die PCs als weitere kritische Schwachstelle entlarvt. Dadurch sind viele dieser PCs entweder aus Perspektive der Cybersicherheit nicht ausreichend geschützt, stellen eine Verbindung zu potenziell anfälligen Cloud-Services für Verbraucher her oder haben keine ausreichenden Ressourcen zur Unterstützung der Sicherheit in Echtzeit.

1 Quelle: Enterprise Strategy Group Research Report, Endpoint Device Trends: Evaluating a Shifting Desktop and Laptop Procurement, Management, OS, Feature, Application, and Spending Landscape, Februar 2024.

2 Ebenda.

Ein weiterer wichtiger Anlass zur Sorge für Cybersicherheitsprofis und IT-Teams ist die große – und immer weiter wachsende – Kompetenzlücke im Bereich Cybersicherheit, die Organisationen enorm unter Druck setzt, neue, innovative und effiziente Möglichkeiten zur Verbesserung der PC-Sicherheit zu finden. Eine Schätzung prognostiziert beispielsweise, dass die Kompetenzlücke im Bereich Cybersicherheit bis 2025 auf 3,5 Millionen Stellen anwachsen wird.[3] Warum ist dies immer noch ein Problem, Jahre nachdem dies erstmals festgestellt wurde? Laut Recherchen der Enterprise Strategy Group und der Information Systems Security Association sind 66 % der Sicherheitsprofis der Meinung, dass die Arbeit in ihrem Bereich in den letzten zwei Jahren schwieriger geworden ist. Gleichzeitig sagten beachtliche 27 % der Fachkräfte aus, dass ihre Arbeit jetzt einen hohen Schwierigkeitsgrad hat.[4]

Da mittlerweile so viele Geschäftsleute zumindest teilweise remote arbeiten und die Zahl und Vielfalt von Sicherheitslücken, die PCs und andere Endpunkte betreffen, weiter ansteigt, bemühen sich Organisationen, neue Möglichkeiten zur Verbesserung der PC-Cybersicherheit zu finden.

Wie PC-CPUs bei Cybersicherheit den Unterschied ausmachen

Es gibt viele Möglichkeiten, wie Organisationen zur Verbesserung der Sicherheit auf den PCs ihrer Benutzer beitragen können. Viele davon sind teuer, sowohl hinsichtlich der Kapitalausgaben als auch der Suche nach mehr Personal, das Aufgaben wie Überwachung, Verwaltung, Training und Schulung übernimmt.

Automatisierung hat dazu beigetragen, dass viele dieser manuellen Sicherheitsaufgaben in integrale Bestandteile der Sicherheitsprozesse und -verfahren umgewandelt wurden, ohne das vorhandene Personal oder bestehende Budgets übermäßig zu belasten. Künstliche Intelligenz hat ebenso in einigen Bereichen wie Bedrohungsdaten, Bedrohungsabwehr und Analyse des Geräteverhaltens einen Beitrag geleistet.

Eine der wichtigsten Quellen für eine verbesserte PC-Sicherheit ist jedoch der PC an sich. Insbesondere beinhalten die PCs von heute nicht nur werksseitig integrierte Tools wie Antivirensoftware und Datensicherungssoftware, sondern nutzen auch

Komponenten, die dazu beitragen, den Schutz des PCs vor Cyberangriffen zu verbessern.

Viele aktuelle PCs wurden z. B. mit CPUs, GPUs, Beschleunigern und Speichergeräten entwickelt, die Sicherheitsfunktionen zur Verbesserung des Datenschutzes und zur Abwehr von Cyberangriffen enthalten. Auf Hardware ausgerichtete Ansätze helfen, indem private und sensible Daten auf verschiedenen Ebenen, einschließlich Firmware, Chip und Betriebssystem, gesichert werden.

Bestimmte Prozessoren wurden so konzipiert, dass sie als Hardware-„Vertrauensanker“ fungieren, wenn der PC das Werk verlässt. So wird Integrität auf Systemebene durch Firmware-Authentifizierung beim Start bereitgestellt.

Weitere Funktionen, um eine PC-Umgebung sicherer zu machen, sind:

- Secure Boot.
- Biometrische Authentifizierung.
- Verschlüsselung.
- Unterstützung für wichtige Betriebssystemfunktionen, wie z. B.:
  - Integrierte Anti-Malware.
  - Automatische Updates.
  - Geräteschutz.
  - Remote Wipe.

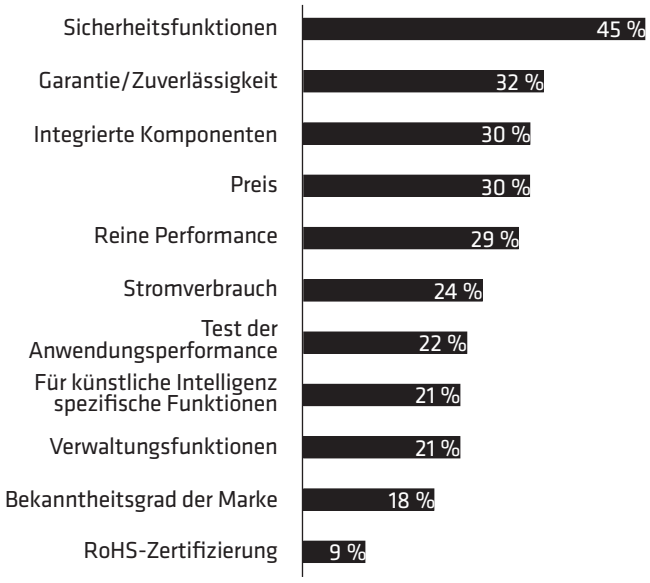
3 Quelle: TechTarget, „Cybersecurity Skills Gap: Why it Exists and How to Address it“, Januar 2024.

4 Ebenda.

Eine Herangehensweise, die AMD verfolgt, ist die Einführung eines mehrschichtigen Ansatzes für die PC-Sicherheit, bei dem Hardware und Software zum Schutz der Daten auf mehreren Ebenen aufeinander abgestimmt sind.

Macht die Entwicklung sicherheitsbezogener Funktionen in CPUs, GPUs und anderen PC-Komponenten einen Unterschied? Ja, laut Recherche der Enterprise Strategy Group. Organisationen wünschen sich natürlich hohe Performance, Zuverlässigkeit und enge Integration, wenn sie CPU-Anbieter prüfen. Allerdings geben Organisationen gegenüber der Enterprise Strategy Group an, dass Sicherheitsfunktionen – bei weitem – ihr wichtigstes Kriterium bei der Wahl des bevorzugten CPU-Anbieters sind. Tatsächlich sagte fast die Hälfte – 45 % – der Teilnehmer, dass Sicherheitsfunktionen ihre Top-Priorität bei einem CPU-Anbieter sind.[5]

Was sind für Ihre Organisation die wichtigsten Kriterien bei der Wahl des bevorzugten CPU-Anbieters? (Prozent der Teilnehmer, N = 354, drei Antworten möglich)



So können AMD Lösungen PC-Sicherheitsanforderungen angehen

Ein Unternehmen, das erhebliche Ressourcen für die Verbesserung der PC-Sicherheit für Partner und Kunden bereitstellt, ist AMD. Als etabliertes führendes Unternehmen für Mikroprozessoren, Beschleuniger und andere PC-Komponenten hat AMD einen einzigartigen Blickwinkel auf die Möglichkeiten zur Verbesserung der PC-Sicherheit.

Eine Herangehensweise, die AMD verfolgt, ist die Einführung eines mehrschichtigen Ansatzes für die PC-Sicherheit, bei dem Hardware und Software zum Schutz der Daten auf mehreren Ebenen aufeinander abgestimmt sind. Beispielsweise ist AMD Partnerschaften mit Microsoft und OEMs eingegangen, um eine mehrschichtige PC-Abwehr mit AMD Ryzen™ Prozessoren zu implementieren, mit der die Sicherheit vom Endpunkt über den Edge bis zur Cloud verbessert werden soll.

AMD Ryzen™ Prozessoren sind in Microsoft Pluton™ Sicherheitsprozessoren integriert, um Sicherheitsbedenken zu beseitigen, wo immer die PCs eingesetzt werden, insbesondere bei Anwendungsfällen für Hybrid-/Remote-Arbeit. Dieser Ansatz umfasst die Kommunikation für die Benutzerauthentifizierung auf Chip-Ebene statt über den Kommunikationsbus an das Betriebssystem, wodurch der Angriffsvektor verringert wird. Er nutzt zudem eine vollständige Systemverschlüsselung für verbesserten Datenschutz.

AMD Ryzen™ PRO Prozessoren beinhalten außerdem weitere Sicherheitsfunktionen:

- AMD Secure Prozessor, ein Sicherheits-Coprozessor.
- AMD Memory Guard für eine umfassende Systemspeicherverschlüsselung.
- AMD Shadow Stack, eine hardwarebasierte Sicherheitsfunktion für die Bereitstellung von Control-Flow-Schutz, um Malware daran zu hindern, Befehlsabläufe umzuleiten.

5 Quelle: Enterprise Strategy Group Research Report, Endpoint Device Trends: Evaluating a Shifting Desktop and Laptop Procurement, Management, OS, Feature, Application, and Spending Landscape, Februar 2024.

Fazit

Für IT-Organisationen und Sicherheitsexperten ist die mitunter harte Wahrheit, dass die Bekämpfung von Cybersicherheitsangriffen herausfordernder ist und größere potenzielle negative Auswirkungen birgt als je zuvor. Es muss auch beachtet werden, dass der PC oft der erste Angriffspunkt für Hacker ist, insbesondere im Zeitalter der weit verbreiteten Remote-Arbeit. Die PCs der Benutzer sind möglicherweise nicht ausreichend geschützt, haben oft keine geeigneten Sicherheitstools und halten sich nicht immer an die empfohlenen bewährten Praktiken, um Anwendungen, Daten, Geräte und Benutzeridentitäten zu schützen.

Allerdings gibt es einen Silberstreif am Horizont: Cybersicherheit ist jetzt ein strategisches Element für alle Organisationen, auch für deren Führungskräfte und Vorstandsmitglieder. Dies bedeutet, dass mehr Ressourcen für die Sicherung der Geräte bereitgestellt werden und IT-Profis, Sicherheitsteams und Endbenutzer viel besser geschult und aufgeklärt sind, wie sie ihre PC-Abwehr verbessern können.

Ein weiterer positiver Aspekt sind die wichtigen Fortschritte der PC-Unternehmen und ihrer Technologiepartner bei der Integration von Funktionen und Fähigkeiten, die dazu beitragen, dass diese Client-Systeme besser gegen Cyberbedrohungen gewappnet sind. Besonders führende Unternehmen für Technologiekomponenten wie AMD haben der Sicherheit eine hohe Priorität eingeräumt und integrieren viele Funktionen in ihre Prozessoren und Beschleuniger, um eine höhere PC-Sicherheit bereitzustellen.

WEITERE INFORMATIONEN DAZU, WIE AMD LÖSUNGEN ORGANISATIONEN DABEI HELFEN, IHRE PC-CYBERSICHERHEITSLAGE ZU VERBESSERN, FINDEN SIE UNTER HTTPS://WWW.AMD.COM/DE/TECHNOLOGIES/PRO-TECHNOLOGIES.

Dieses Dokument wurde von der TechTarget Inc. im Auftrag von AMD angefertigt.