Windows 11

HP empfiehlt Windows 11 Pro
für Unternehmen.

Whitepaper

Mit Endpunktsicherheit gegen IT-Bedrohungen

So stärken kleine und mittlere Unternehmen ihre hybriden Arbeitswelten

Whitepaper

Mit Endpunktsicherheit gegen IT-Bedrohungen

So stärken kleine und mittlere Unternehmen ihre hybriden Arbeitswelten

Inhaltsverzeichnis

Warum ist Endpoint Security entscheidend für hybride Arbeitsmodelle? Eine Einleitung. **4**

Endpoint Security entmystifiziert: Ein Blick hinter die Kulissen der Endgeräte-Sicherheit **6**

Endpoint Security implementieren: Ein Schritt-für-Schritt-Leitfaden **7**

- **Schritt 1:** Sorgfältige Analyse bestehender Sicherheitskonzepte **7**
- **Schritt 2:** Einbindung von Endpoint-Security **8**
- **Schritt 3:** Berücksichtigung von Hybrid-Arbeitsumgebungen **9**
- **Schritt 4:** Mitarbeiteraufklärung und -Training **10**
- **Schritt 5:** Ständige Überwachung und Anpassung **10**

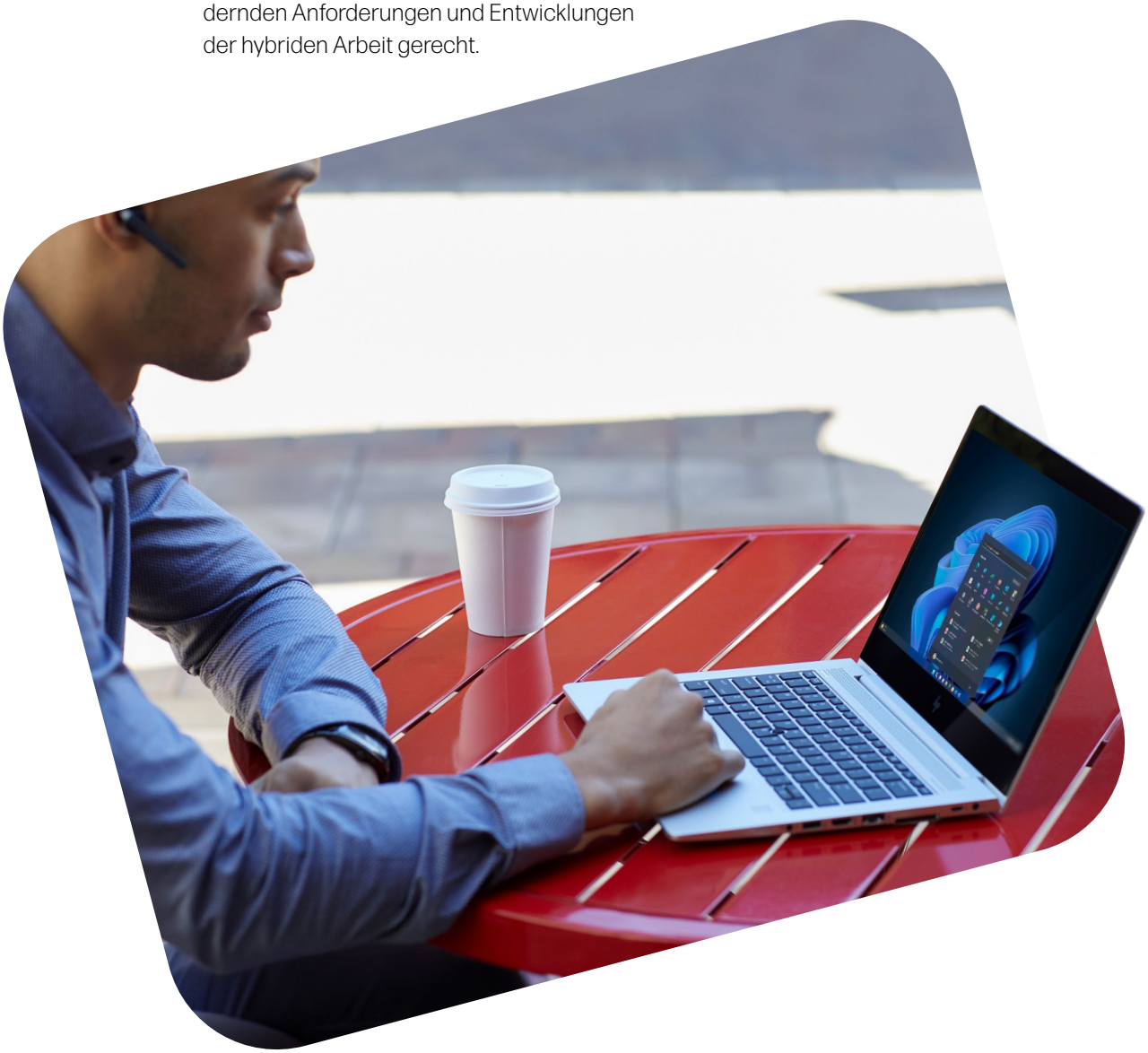
Management Summary

Die operative und strategische Weiterentwicklung von hybriden Arbeitsplatzmodellen konfrontiert die IT-Entscheider in kleinen und mittelständischen Unternehmen mit neuen Herausforderungen. Die Sicherheit von Endgeräten, die sowohl vor Ort als auch mobil genutzt werden, gewinnt zunehmend an Priorität.

Endpoint Security präsentiert sich als Konzept und Schlüsselelement, das durch gezielte Analyse, Implementierung und kontinuierliche Verbesserung einen effizienten Schutz vor Cyber-Bedrohungen bietet. Wenn IT-Verantwortliche bestimmte Dinge berücksichtigen und strukturiert vorgehen, werden sie den sich ständig ändernden Anforderungen und Entwicklungen der hybriden Arbeit gerecht.

Die wesentlichen Bestandteile dieser Sicherheitsinitiative sind die Integration von Hard- und Firmware-basierten Sicherheitskomponenten sowie zukunftsorientierte Schlüsseltechnologien wie künstlicher Intelligenz – letztendlich aber auch die kontinuierliche Sensibilisierung und Schulung des Personals.

Das vorliegende Whitepaper dient als Einführung, gibt praktische Hinweise für IT-Verantwortliche in kleinen und mittelständischen Unternehmen und bietet einen Leitfaden zur sofortigen Umsetzung.

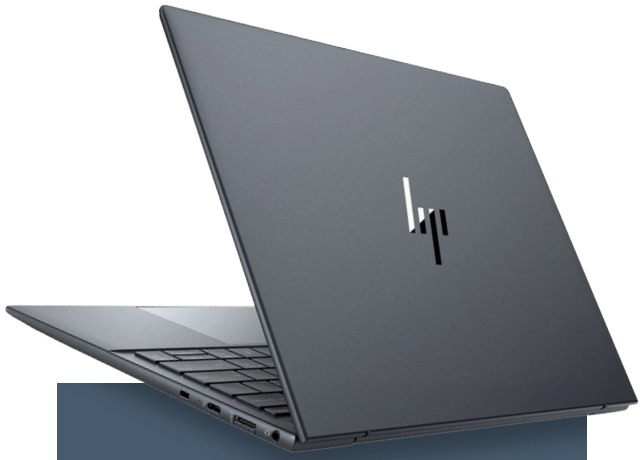


Warum ist Endpoint Security entscheidend für hybride Arbeitsmodelle? Eine Einleitung.

Das moderne Arbeitsumfeld konfrontiert IT-Entscheider in kleinen und mittelständischen Unternehmen (KMU) mit wahrhaft herkulischen Herausforderungen. Hybride Arbeitsoptionen weiterzuentwickeln, die Bedürfnisse aller Interessengruppen und Beteiligter zu erfüllen, den operativen Betrieb aufrechtzuerhalten und die Informationssicherheit zu wahren – all das verlangt einen proaktiven Ansatz. Hierbei nimmt die robuste Absicherung der Endgeräte eine zentrale Rolle ein, um Risiken wie Datenverlust, unerlaubten Zugriff oder Netzwerkangriffe zu minimieren.

Darüber hinaus gibt es Risiken im Zusammenhang mit alltäglichen Ereignissen wie dem Kauf unsicherer oder kompromittierter Geräte, die potenzielle Einfallstore für Cyber-Angriffe darstellen, oder dem Verlust oder Diebstahl von Computern. Cybervorfälle wie IT-Ausfälle, Ransomware-Angriffe und Datenlecks sind seit zwei Jahren das weltweit dominierende Risiko. Datenlecks bereiten den Unternehmen die größten Sorgen, gefolgt von Ransomware und Ausfällen in digitalen Lieferketten und Cloud-Diensten. Cyberangriffe, ob von Kriminellen oder staatlich unterstützten Hackern, durch menschliches Versagen oder technisches Versagen verursacht, führen zu erheblichen Betriebsunterbrechungen. Analysten der Allianz-Versicherung bestätigen, dass solche Unterbrechungen den größten Teil der Cyber-Versicherungsschäden ausmachen.

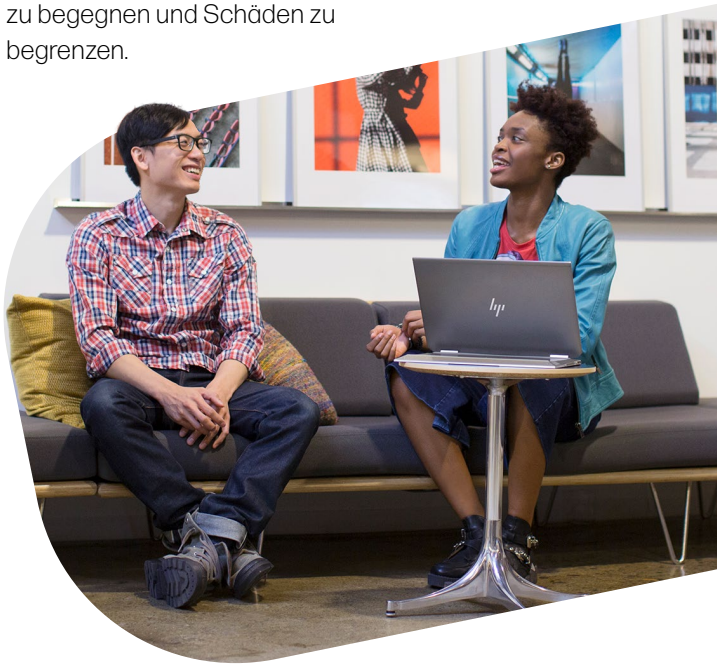
Da sich Angreifer zunehmend auf digitale und physische Lieferketten konzentrieren, nehmen sie mehrere Unternehmen ins Visier, was den Erpressungsdruck erhöht. Kleine und mittlere Unternehmen („small and medium businesses", SMB) sind zunehmend gefährdet, da größere Unternehmen ihre Cybersicherheit ausbauen. Werden Sie sich daher der Bedeutung einer umfassenden Cybersicherheitsstrategie bewusst, um den wachsenden Bedrohungen wirksam zu begegnen und Schäden zu begrenzen.



Bequem und ohne Sorgen von überall arbeiten

Mit Notebooks der Serie **„HP Elite Dragonfly"** erleben Sie eine unvergleichliche Mobilität, egal wo Sie arbeiten. Als Leichtgewicht von etwa 1 kg, mit einem 13,3-Zoll-HD-Bildschirm sowie vielfältigen und modernen Sicherheitsfunktionen erfüllt der Windows-11-Laptop alle Anforderungen in einer hybriden Arbeitswelt.

HP empfiehlt Windows 11 Pro für Unternehmen. Windows 11 Pro beruht auf den Zero Trust-Prinzipien, um Daten und Zugriff überall zu schützen.



Die Rolle von IT-Entscheidungsträgern im hybriden Arbeitsumfeld

Indem Sie als IT-Führungskraft eines Betriebs robuste, skalierbare und anpassungsfähige Technologieplattformen implementieren, fördern Sie flexible Arbeitsmodelle. Diese unterstützen einen fließenden Wechsel zwischen Büro- und Heimarbeit. Dabei muss die Plattformentwicklung im Einklang mit den Zielen des Unternehmens stehen und die Firmenkultur berücksichtigen. Ziel ist es, sowohl die Produktivität als auch die Zufriedenheit des Teams zu steigern.

Das angestrebte Ziel basiert auf einer durchdachten Sicherheitsstrategie, die den Datenschutz gewährleistet und Cyber-Bedrohungen abwehrt. Sie soll das Vertrauen der Angestellten in die Sicherheit ihres Arbeitsplatzes stärken. Es ist verständlich und nachvollziehbar, dass es in mittelständischen Unternehmen Herausforderungen wie begrenzte Ressourcen, fehlendes Fachwissen und manchmal auch eine nicht vollständig ausgereifte Risikobewertung geben kann. Diese Faktoren sollten für Sie jedoch keine Hindernisse sein, sondern vielmehr Gelegenheiten zur Entwicklung und Verbesserung – und im besten Fall muss sich niemand mehr um die Sicherheit Gedanken machen.

Der Schlüssel zur Sicherheit im hybriden Arbeitsumfeld

Die Absicherung von Endgeräten, den so genannten Endpunkten, ist ein wesentliches Element bei flexiblen Arbeitsstrukturen. Dadurch können Sie als IT-Entscheider eine Vielzahl von Herausforderungen und Gefahren bewältigen, die durch die breite Nutzung verschiedener Netzwerke und Geräte entstehen.

Die Erhöhung des Sicherheitsniveaus lässt sich durch strategische Entscheidungen bei der Beschaffung von Hardware erreichen. Dazu gehört beispielsweise die Auswahl von Laptops mit integrierten Sicherheitsfunktionen wie biometrischen Sensoren und Verschlüsselungstechnologien. Wichtig ist auch die Kompatibilität mit den Sicherheitsstandards des Unternehmens. Ein Beispiel hier für wäre ein Router, der den neuesten Sicherheitsstandard WPA3 unterstützt. Eine kontinuierliche Verbesserung der Endgerätesicherheit können Sie durch intelligente Managementprozesse erzielen. Dazu gehört das Einspielen von Software-Updates und Patches über ein zentrales Managementsystem, das die Aktualität von Betriebssystemen und Anwendungen auf allen Geräten sicherstellt.

Zusätzlich können spezielle Tools wie Antivirensoftware oder Intrusion Detection Systeme (IDS) eingesetzt werden, um Bedrohungen zu erkennen und abzuwehren. Auch mit der Automatisierung solcher Prozesse, etwa durch den Einsatz von Security Information and Event-Management-Systemen (SIEM), tragen Sie zur Erhöhung der Sicherheit bei.

Diese Maßnahmen gewinnen insbesondere in hybriden Arbeitsstrukturen an Bedeutung, die ein hohes Maß an Komplexität und Flexibilität erfordern. So ist zum Beispiel die Absicherung von Endgeräten über verschiedene Netze hinweg für das Arbeiten von unterwegs und zu Hause von zentraler Bedeutung.

HP Wolf Pro Security Edition – integrierte Sicherheit für den Mittelstand, einfach gemacht

Die umfassende Sicherheitslösung HP Wolf Pro Security Edition (WPSE) ist besonders benutzerfreundlich auch für Nichtfachleute, schont so IT-Experten-Ressourcen und fördert die Produktivität. Besonders kleine und mittlere Unternehmen profitieren vom geringen Aufwand für die Bereitstellung, der cloud-basierten Verwaltung und der vereinfachten, zentralisierten Wartung.

HP WPSE umfasst Bedrohungseindämmung, Zugangsdatenschutz und optionales NGAV (Next-Generation-Anti-Virus-Software), ist auf ausgewählten HP-Business-Notebooks für den Mittelstand vorinstalliert und für 1 Jahr kostenfrei nutzbar.

Sicherheit von HP

HP Wolf Security ist eine fortschrittliche Endpoint-Sicherheitslösung, die speziell für Unternehmen und Organisationen entwickelt wurde, um ihre Endgeräte wie PCs, Laptops und Tablets umfassend zu schützen. Neben den Softwarelösungen bietet HP auch Hardware-Sicherheitslösungen für Endgeräte an, um eine umfassende Sicherheitsstrategie zu gewährleisten.

Eine dieser Lösungen ist HP Sure Start, die selbstheilende BIOS-Sicherheit bietet. HP Sure Start schützt vor böswilligen Angriffen auf das BIOS, die den Startvorgang von Endgeräten kompromittieren könnten. Es stellt sicher, dass das BIOS auf dem neuesten Stand ist und unverändert bleibt, damit das Gerät sicher starten kann.

Eine weitere Hardware-Sicherheitslösung ist HP Sure Click, die eine hardwareunterstützte virtuelle Maschine verwendet, um den Browser in einer isolierten Umgebung auszuführen. Dadurch wird verhindert, dass Malware oder andere Bedrohungen das System infizieren oder Daten stehlen können.

Darüber hinaus bietet HP Wolf Security auch eine integrierte Hardware-Sicherheitslösung namens HP Sure Sense an, die maschinelles Lernen und künstliche Intelligenz nutzt, um Bedrohungen in Echtzeit zu erkennen und zu bekämpfen. HP Sure Sense kann auch den Einsatz herkömmlicher Antiviren-Tools ergänzen, um eine zusätzliche Schutzschicht für Endpunkte zu bieten.

Endpoint Security entmystifiziert: Ein Blick hinter die Kulissen der Endgeräte-Sicherheit

Endpoint Security umfasst zahlreiche Maßnahmen und Technologien zum Schutz von Endgeräten vor Cyber-Bedrohungen. Sie bildet eine starke Verteidigungslinie, um unberechtigte Zugriffe zu verhindern, Malware zu erkennen und zu bekämpfen sowie sensible Daten vor Verlust oder Diebstahl zu schützen. Die Geschichte der Endpunktsicherheit reicht bis in die 1980er Jahre zurück. Im Laufe der Zeit hat sie sich zu einem wesentlichen Bestandteil der IT-Sicherheit entwickelt.

Der ganzheitliche Ansatz: Mehrschichtiger Schutz für Endgeräte

Komponenten wie Antiviren- und Anti-Malware-Schutz, robuste Firewalls, regelmäßige Hardware- und Firmware-Updates, strikte Zugriffskontrollen und ein kontinuierliches Monitoring bilden heutzutage die Basis einer effektiven Endpoint-Security. Die Anforderungen an die IT-Sicherheit haben sich jedoch verändert:

- **Ransomware-Angriffe**, bei denen Daten verschlüsselt und dann gegen Lösegeld wiederfreigegeben werden, nehmen zu.
- Auch **Phishing-Angriffe**, bei denen Angreifer versuchen, an sensible Informationen zu gelangen, werden immer häufiger.
- Darüber hinaus stellen **Zero-Day-Angriffe**, die noch unbekannte Sicherheitslücken ausnutzen, eine ernstzunehmende Gefahr dar.
- Besonders besorgniserregend ist die Zunahme von **Social-Engineering-Angriffen** bei denen Angreifer menschliche Schwächen ausnutzen, um Zugang zu vertraulichen Informationen 'oder Systemen zu erhalten.

Angesichts der sich verändernden Bedrohungslandschaft und der zunehmenden Telearbeit reichen herkömmliche Lösungen jedoch nicht mehr aus. KMU müssen ihre Sicherheitsstrategien weiterentwickeln. Als IT-Verantwortlicher sollten Sie zusätzliche Maßnahmen wie Verhaltensanalysen, maschinelles Lernen und künstliche Intelligenz einsetzen, um verdächtige Aktivitäten und unbekannte Bedrohungen zu erkennen. Ein umfassender Ansatz, der Firewalls, Verschlüsselungstechnologien, Zugangskontrollen und regelmäßige Updates umfasst, ist von entscheidender Bedeutung.

Endgerätesicherheit in hybriden Arbeitsumgebungen: Neue Maßnahmen für moderne Bedrohungen

Endgerätesicherheit in hybriden Arbeitsumgebungen ist entscheidend, um komplexe Bedrohungen abzuwehren und sensible Daten zu schützen. Wichtig ist dabei ein ganzheitlicher Ansatz mit Integration von Hard- und Software, um gegen Malware, Phishing, Social Engineering, Zero-Day-Exploits und Insider-Bedrohungen gewappnet zu sein.

Moderne Plattformen bieten integrierte Sicherheitsfunktionen wie hardwarebasierte Verschlüsselungstechnologien. Durch spezifische BIOS-Einstellungen und erweiterte Konfigurationsoptionen können Sicherheitsrichtlinien durchgesetzt und die Resistenz gegenüber Angriffen erhöht werden. Mit dem Einsatz moderner Techniken, einschließlich der Analyse des Nutzerverhaltens, des maschinellen Lernens und der künstlichen Intelligenz, ermöglichen Sie die Identifizierung und Neutralisierung verdächtiger Vorgänge.

Endpoint Security implementieren: Ein Schritt-für-Schritt-Leitfaden

Für eine verantwortliche IT-Führungskraft eines kleinen oder mittelständischen Unternehmens ist die Entwicklung einer wirksamen Endpoint-Sicherheitsstrategie und deren Integration in bestehende Sicherheitssysteme von höchster Bedeutung – gerade im Lichte fortschreitender Hybrid-Work-Konzepte. Der folgende Leitfaden bietet eine strukturierte Vorgehensweise zur Implementierung von Endpoint-Security und unterstreicht die Bedeutung einzelner Aspekte in Hybrid-Arbeitsumgebungen.

Schritt 1: Sorgfältige Analyse bestehender Sicherheitskonzepte

Beginnen Sie mit einer tiefgreifenden Untersuchung Ihrer derzeitigen Sicherheitspraktiken. Identifizieren Sie Schwachstellen und Lücken, die potenziell Endpunkte gefährden. Priorisieren Sie aktuelle Bedrohungen und die Sicherheit von Hybrid-Arbeitsumgebungen. Beziehen Sie relevante Stakeholder ein und bewerten Sie vorhandene Maßnahmen wie Firewalls und Antiviren-Software. Durch Audits und Penetrationstests können Sie die Widerstandsfähigkeit Ihrer Systeme verifizieren.

Aufgaben und Checkpunkte:

- Überprüfen Sie die bestehenden Sicherheitsrichtlinien und -verfahren Ihres Unternehmens auf ihre Wirksamkeit und Relevanz.
- Führen Sie eine umfassende Bewertung der aktuellen Sicherheitsinfrastruktur durch, um Schwachstellen und potenzielle Angriffsvektoren zu identifizieren.
- Analysieren Sie vergangene Sicherheitsvorfälle und ihre Auswirkungen, um Muster und Trends zu erkennen und daraus Lehren zu ziehen.

Der umfassende Schutzschild: Innovative HP-Produkte für Endpoint Security

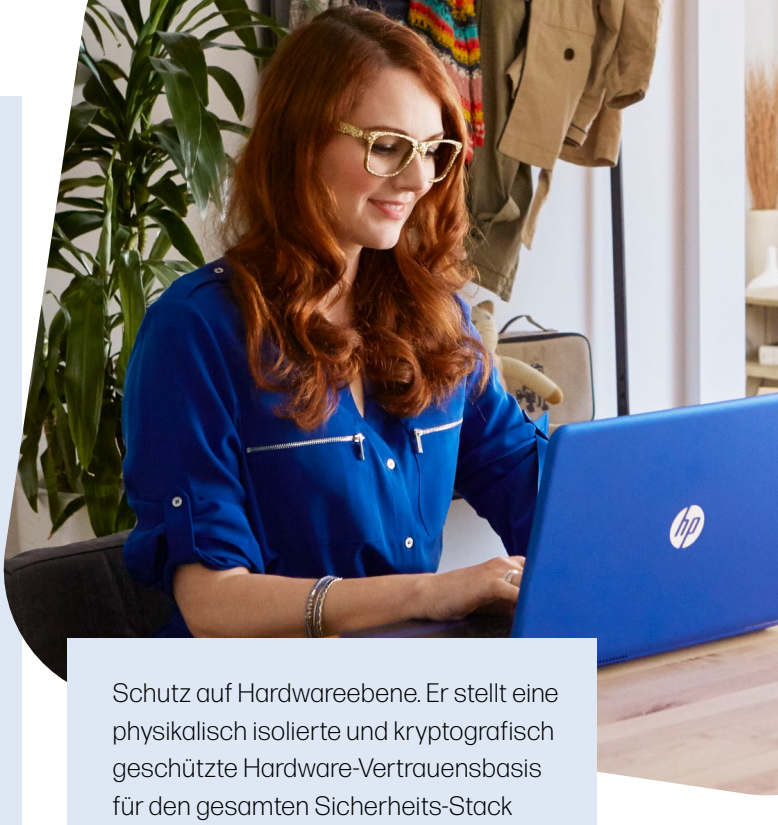
Bei der Sicherheit von Endgeräten gilt das HP-Portfolio als umfassender Unternehmensschutz vor Bedrohungen. Durch die Integration von Sicherheitskomponenten und -funktionen in die Hard- und Firmware von Geschäfts-PCs wird ein hardwarebasierter Schutz gewährleistet. Im Folgenden ein Überblick über verschiedenen Security-Elemente von HP, die sich an kleine und mittelständische Firmen richten.

Umfassende Sicherheit auf Geschäfts-PCs

HP Wolf Security ist eine umfassende Sicherheitslösung, die speziell für Unternehmens-PCs entwickelt wurde. Sie umfasst integrierte Sicherheitslösungen, hardwarebasierten Schutz, automatisierte Überwachung und Reaktion, KI-basierte Bedrohungserkennung sowie effiziente Wiederherstellungsoptionen. Die automatisierte Überwachung und Reaktion ermöglicht eine kontinuierliche Überprüfung des PC-Status, um ungewöhnliche Aktivitäten oder Angriffe zu erkennen und automatisch darauf zu reagieren. Die KI-basierte Bedrohungserkennung identifiziert fortschrittliche und unbekannte Bedrohungen, während effiziente Wiederherstellungsoptionen Ausfallzeiten minimieren und die Produktivität maximieren.

Der HP Endpoint Security Controller – eine zentrale Komponente

Eine zentrale Komponente des HP Endpoint Security Stacks ist der HP Endpoint Security Controller. Dieser Mikrocontroller gewährleistet einen hardwarebasierten, selbstheilenden und verwaltbaren



Schutz auf Hardwareebene. Er stellt eine physikalisch isolierte und kryptografisch geschützte Hardware-Vertrauensbasis für den gesamten Sicherheits-Stack bereit. Der Controller arbeitet unterhalb des Betriebssystems und ermöglicht wichtige Sicherheitsfunktionen wie Erkennung, Aktualisierung, Wiederherstellung und Verwaltung.

Sicheres BIOS-Management ohne Kompromisse

Ein bemerkenswertes Element des Portfolios ist HP Sure Start. Diese erkennt Integritätsverletzungen in der PC-BIOS-Firmware und den Einstellungen und leitet automatisch Selbstheilungsmaßnahmen ein. Dadurch wird sichergestellt, dass nur authentische Firmware und Einstellungen ausgeführt werden. Im Falle einer Beschädigung stellt HP Sure Start die korrekte Firmware und Einstellungen aus einer privaten Kopie wieder her.

Verbesserte BIOS-Verwaltung mit HP Sure Admin

HP Sure Admin ermöglicht eine verbesserte, sichere BIOS-Verwaltung durch den Ersatz von BIOS-Passwörtern durch einen öffentlichen Schlüssel, der vom IT-Sicherheitsteam verwaltet wird. Diese Lösung erlaubt eine sichere Kommunikation und Fernverwaltung der BIOS-Firmware-Konfiguration.

Effiziente Wiederherstellung auf Hardware-Ebene

Für eine schnelle und sichere Wiederherstellung auf Hardware-Ebene bietet HP Sure Recover eine effiziente Lösung. Sie ermöglicht die sichere Installation, Neuinstallation oder Wiederherstellung eines kompletten Betriebssystems. Das Recovery kann aus der Cloud erfolgen oder auf einem sicheren Embedded-Flash-Speicher abgelegt werden, um eine zügige Wiederinbetriebnahme unabhängig von den Netzwerkbedingungen zu gewährleisten.

Anwendungsisolierung durch HP Sure Click

HP Sure Click bietet Anwendungsisolierung mittels Mikro-Virtualisierung. Diese Technologie isoliert risikoreiche Aufgaben in virtuellen Einwegmaschinen, um bösartige Aktivitäten zu verhindern. Dielsolierung auf Hardware-Ebene ist bsonders widerstandsfähig gegen Softwareumgehungen.

Schritt 2: Einbindung von Endpoint-Security

Die Entwicklung einer ausgeklügelten Strategie zur Integration von Endpoint Security ist unverzichtbar. Hierbei sollten Sie die Anforderungen Ihrer Hybrid-Arbeitsumgebung berücksichtigen. Mit der Unterstützung Ihrer IT-Abteilung, falls vorhanden, und externer Berater oder Dienstleister können Sie bestehende Sicherheitskonzepte analysieren und klare Vorgaben für die Endpoint-Security-Integration festlegen. Implementieren Sie die ausgewählten Lösungen und stellen Sie eine effektive Zusammenarbeit mit vorhandenen Sicherheitssystemen sicher.

Aufgaben und Checkpunkte:

- Identifizieren Sie die verschiedenen Arten von Endgeräten (Desktop-Computer, Laptops, Mobilgeräte usw.), die im Unternehmen verwendet werden, und erstellen Sie eine Inventarliste.
- Evaluieren Sie Endpoint-Sicherheitslösungen, die Ihren spezifischen Anforderungen entspricht, um eine angemessene Auswahl zu treffen. Das beinhaltet das Einholen von Angeboten, den Vergleich der Angebote und die Bewertung verschiedener Aspekte wie Funktionalität, Zuverlässigkeit, Benutzerfreundlichkeit, Kosten, Support und technische Anforderungen.
- Implementieren Sie eine zentrale Verwaltungslösung für Endpoint-Sicherheit, um Gerätekonfigurationen, Patches und Sicherheitsrichtlinien effizient zu verwalten.

Schritt 3: Berücksichtigung von Hybrid-Arbeitsumgebungen

Hybride Arbeitsumgebungen erfordern eine flexible Herangehensweise an Endpoint-Security. Aspekte wie verschlüsselte Verbindungen und sichere Authentifizierung sind von zentraler Bedeutung. Geeignete Lösungen bieten Schutz sowohl für lokale als auch entfernte Endpunkte und unterstützen Funktionen für Remote-Management.

Aufgaben und Checkpunkte:

- Analysieren Sie die aktuellen Arbeitpraktiken und -anforderungen, um die spezifischen Herausforderungen der hybriden Arbeitsumgebung zu verstehen.
- Implementieren Sie eine sichere Netzwerkinfrastruktur, die sowohl physische als auch virtuelle Arbeitsplätze unterstützt.
- Erstellen Sie Richtlinien und Verfahren für den sicheren Zugriff auf Unternehmensressourcen von externen Standorten aus, einschließlich Authentifizierungsmethoden.

Schritt 4: Mitarbeiter-aufklärung und -Training

Eine effektive Endpoint-Security erfordert gut informiertes und geschultes Personal. Sensibilisieren Sie Ihre Mitarbeiter und Mitarbeiterinnen für Sicherheitsrisiken und fördern Sie geeignete Verhaltensweisen, besonders in Hybrid-Arbeitsumgebungen. Vermitteln Sie Sicherheitsrichtlinien und -verfahren und gewährleisten Sie, dass alle Angestellten Sicherheitsbedrohungen erkennen und melden können.

Aufgaben und Checkpunkte:

- Nutzen Sie Schulungsprogramme, um alle im Betrieb über die Bedeutung von Endpoint-Sicherheit aufzuklären und bewusstes Verhalten zu fördern.
- Führen Sie regelmäßige Sicherheitsschulungen durch, um alle Abteilungen über aktuelle Bedrohungen und bewährte Sicherheitspraktiken auf dem Laufenden zu halten.
- Etablieren Sie eine Kultur der Sicherheit, in der die Mitarbeiter und Mitarbeiterinnen proaktiv Bedrohungen melden und bewusste Sicherheitsentscheidungen treffen.

Schritt 5: Ständige Überwachung und Anpassung

Eine kontinuierliche Überwachung und Optimierung der Sicherheitsmaßnahmen ist der Schlüssel zu einer wirksamen Endpoint-Security. Ein robustes Monitoring-System ermöglicht die Echtzeiterkennung von Bedrohungen. Durch regelmäßige Überprüfungen und Aktualisierungen stellen Sie sicher, dass Sicherheitspatches auf allen Endpunkten auf dem neuesten Stand sind. Passen Sie Ihre Sicherheitsstrategie ständig an die sich verändernde Bedrohungslandschaft und die Anforderungen hybrider Arbeitsumgebungen an. Informationen zu diesem Thema können beispielsweise bei Heise Security, den HP-Sicherheitsbulletins oder dem BSI-Security-Newsletter gefunden werden.

Aufgaben und Checkpunkte:

- Implementieren Sie ein kontinuierliches Überwachungssystem, um potenzielle Sicherheitsvorfälle zu erkennen und schnell zu reagieren.
- Aktualisieren Sie regelmäßig die Sicherheitsrichtlinien und -verfahren, um mit den sich ständig weiterentwickelnden Bedrohungslandschaften Schritt zu halten.
- Führung Sie regelmäßiger Audits zur Überprüfung der Wirksamkeit der Endpunktsicherheitsstrategie durch und identifizieren Sie mögliche Verbesserungen.

Kontakt

Heise Medien GmbH & Co. KG
Abt. Heise Business Services

Hans-Pinsel-Straße 10b
85540 Haar bei München

business-services.heise.de

Registergericht:
Amtsgericht Hannover HRA 26709

Persönlich haftende Gesellschafterin:
Heise Medien Geschäftsführung GmbH
Amtsgericht Hannover, HRB 60405

Geschäftsführer:
Ansgar Heise, Beate Gerold

Verantwortlich für den Inhalt:
Heise Business Services,
Thomas Jannot, tj@heise.de

Layout:
Oliver Eismann, www.olivereismann.de

Haftung:
Für den Fall, dass Beiträge oder Informationen unzutreffend oder fehlerhaft sind, haftet der Verlag nur beim Nachweis grober Fahrlässigkeit. Für Beiträge, die namentlich gekennzeichnet sind, ist der jeweilige Autor verantwortlich.