Microsoft Surface | intel

Die 3 Säulen der modernen Endpoint Security.

Vorstellung eines sicheren, hybriden Arbeitsplatzes

Die Pandemie hat die Art und Weise, wie wir arbeiten, Geschäfte machen und Kundenbedürfnisse erfüllen, grundlegend verändert. Heute verlangsamen sich die Kurven der digitalen Akzeptanz nicht, sie beschleunigen sich.

Die Zunahme der Hybridarbeit erfordert, dass wir uns neue Fragen stellen, zum Beispiel, wie wir sicherstellen können, dass unsere Mitarbeiter, Daten und Endpunkte langfristig sicher sind. Hybridarbeit stellt für jedes Unternehmen einen ganzheitlichen Wandel dar, der einen neuen Ansatz für die Endpunktsicherheit erfordert.

Die digitale Transformation und der sich wandelnde Arbeitsplatz zeigen zwei sich überschneidende Trends auf: die Vielfalt und das Volumen von Endpunktgeräten und die Notwendigkeit, Daten und Systeme überall zu schützen. Es überrascht daher nicht, dass mehr als die Hälfte der Befragten der CIO Pulse-Umfrage von PwC die Verbesserung der Widerstandsfähigkeit in Bezug auf Cybersicherheit und Datenschutz als oberste Priorität einschätzten.[1]

Da Sicherheit für das digitale Geschäft immer wichtiger wird, arbeiten IT- und Sicherheitsteams enger denn je zusammen, um Bedrohungen und Schwachstellen in der gesamten IT-Architektur proaktiv zu identifizieren. Fast alle (96 %) der Unternehmen in der 2021 Global Digital Trust Insights-Studie gaben an, dass sie planten, ihre Cybersicherheitsstrategie aufgrund der Pandemie anzupassen – gegenüber 25 % im Vorjahr.[2]

Cybersicherheitsbedrohungen entwickeln sich ständig weiter, und Sicherheit spielt eine immer wichtigere Rolle bei unserer digitalen Geschäftsabwicklung. Unternehmen müssen Schwachstellen proaktiv identifizieren und Risiken im gesamten Unternehmen mindern. Die Zusammenarbeit an sicheren Endpunkt-Schutzstrategien für alle Gerätetypen – einschließlich Desktops, Laptops, Tablets und anderer Geräte, die Mitarbeiter verwenden – bedeutet, erweiterte Sicherheitslösungen, cloudbasierte Bereitstellungs- und moderne Geräteverwaltungstools in Betracht zu ziehen.

Vom Chip bis zur Cloud betrachtet Microsoft Surface mit der Unterstützung von Intel die sichersten verfügbaren Gerätefunktionen und entwickelt weiterhin Innovationen, um den sich ändernden Anforderungen der Kunden gerecht zu werden.

Moderner Endpunktschutz erfordert moderne Sicherheitsansätze, die einen mehrschichtigen Ansatz verfolgen, von der Gerätefirmware bis zur Cloud – und über alle Phasen des Lebenszyklus hinweg. Stellen Sie sicher, dass sich die Gerätesicherheit von innen aus dem Endpunkt über die Bereitstellung, die erneute Bereitstellung, die Außerbetriebnahme und bis hin zu allen Zugangspunkten zum Endpunktgerät erstreckt. In diesem E-Book geben wir einen Überblick über die drei Hauptsäulen, die eine moderne Endpunktstrategie bilden.

[1] 2020 CIO Pulse-Umfrage (Mai), PwC.
[2] 2021 Global Digital Trust Insights, PwC.

Nr. 1: Endpunktsicherheit beginnt bei der Hardware

Moderne Windows-Geräte wie Microsoft Surface enthalten ausgereifte, fortschrittliche Hardware und Firmware, die zum Schutz des Geräts entwickelt wurde. Diese Geräte verwenden die hardwaregestützten Sicherheitsfunktionen von Intel®-Prozessoren, die direkt in das Silizium integriert sind, um jede Schicht des Compute-Stacks zu schützen. Eine optimale Sicherheitsstrategie nutzt einen vollständigen Chip-to-Cloud-Ansatz für die Endpunktsicherheit.

Die Rolle von TPM und UEFI verstehen

Die beiden Gerätekomponenten, die am stärksten relevant für Sicherheit sind, sind das Trusted Platform Module (TPM) und die Unified Extensible Firmware Interface (UEFI).

TPM ist ein Krypto-Prozessor, der sowohl gegen physische Manipulationen als auch gegen die Versuche bösartiger Software, ihn zu ändern oder zu stören, resistent ist. TPM kann kryptografische Schlüssel generieren, speichern und steuern. Außerdem werden Ihre Daten schnell und einfach verschlüsselt, sodass nur autorisierte Personen darauf zugreifen können.

Die UEFI ist ein Mini-Betriebssystem, dessen Aufgabe es ist, das Hauptbetriebssystem zu laden. Die UEFI auf den meisten mit Intel ausgestatteten Surface-PCs wird von Microsoft proaktiv entwickelt und gewartet, um sicherzustellen, dass Updates automatisch mit Windows Update for Business veröffentlicht werden.[3] Dadurch werden wichtige Sicherheitsupdates nicht nur zeitnaher, sondern auch wahrscheinlicher angewendet.

Neben TPM und UEFI bieten integrierte, hardwarebasierte Sicherheitsfunktionen eine sicherere Grundlage.[3] Intel® Total Memory Encryption schützt Daten zusätzlich vor physischen Angriffen auf den Speicher, wie etwa Kaltstartangriffen.

IN ZAHLEN

5 Milliarden

Anzahl der auf Geräten pro Monat erkannten Bedrohungen.[4]

WICHTIGSTE SCHLUSSFOLGERUNGEN

Stellen Sie sicher, dass es für Ihre Endpunktgeräte Sicherheitsüberlegungen auf Hardwareebene gibt, um einen zunehmend kritischen Schwachpunkt effizient zu mindern.

[3] Surface Go und Surface Go 2 verwenden eine UEFI eines Drittanbieters und unterstützen DFCI nicht. DFCI ist derzeit für Surface Pro 7+, Surface Laptop Go, Surface Book 3, Surface Laptop 3, Surface Pro 7 und Surface Pro X verfügbar. Erfahren Sie mehr über das Verwalten der Surface UEFI-Einstellungen.

[4] The evolution of Microsoft Threat Protection, Juni-Update, Microsoft Security Blog, 2019.

Sicher starten

Beim Hochfahren eines PCs mit UEFI und TPM wird der Bootloader auf eine digitale Signatur mit einem vertrauenswürdigen Zertifikat aus den im TPM gespeicherten Zertifikaten überprüft. Dieser Vorgang wird als Sicherer Start bezeichnet und soll verhindern, dass nicht autorisierte Software beim Booten ausgeführt wird.

Gerätehersteller laden das TPM normalerweise mit ihren eigenen Zertifikaten, dem des UEFI-Autors und den von Microsoft bereitgestellten Zertifikaten. Auf zertifizierten Windows-PCs muss Sicherer Start für die Zertifizierung standardmäßig aktiviert sein. Diese Maßnahmen bieten einen wesentlichen Schutz vor Schadsoftware in der Startphase und vor Manipulationen mit Boot-Software. Diese gefährlichen und meist unsichtbaren Exploits sind in der Realität nach wie vor weit verbreitet.[5]

Schutzmaßnahmen in der Startphase hören nicht an dieser Stelle auf, Angreifer können auch versuchen, ein Gerät mit bösartiger Software zu kompromittieren, die so entwickelt wurde, dass sie in den frühen Phasen des Windows-Starts gestartet wird. Ein Beispiel dafür ist ZeroAccess, ein Windows-Rootkit auf Treiberebene, das verschlüsselte alternative NTFS-Datenströme zum Speichern verwendet. Um dieser Bedrohung zu begegnen, verwenden mit Intel ausgestattete Surface-Geräte einen Industriestandard namens Measured Boot. Dies ist ein Prozess, der vor dem Laden eines Anti-Malware-Produkts ausgeführt werden kann, wodurch zusätzliche Sicherheit geboten wird, dass der Startprozess nicht kompromittiert wurde. Außerdem hilft Intel® Boot Guard, die Umgebung vor dem Betriebssystem weiter vor Viren und Schadsoftwareangriffen zu schützen. Um zu verhindern, dass eingepflanzte Malware das Betriebssystem kompromittiert, kann Intel OS Guard das Betriebssystem daran hindern, Anwendungscode direkt auszuführen.

IN ZAHLEN

450,2 Millionen

Gesamtlieferungen für PC-Geräte im Jahr 2020, einschließlich Desktops, Notebooks, Workstations und Tablets.[6]

WICHTIGSTE SCHLUSSFOLGERUNGEN

Fortschrittliche Malware, die ausgeführt wird, bevor das Betriebssystem startet, ist eine echte Bedrohung und kann schwer zu entfernen sein. Best Practices und die neueste Sicherheitstechnologie, wie sie in Microsoft Surface-Geräten mit Intel zu finden sind, können verhindern, dass das Gerät überhaupt erst infiziert wird.

[5] Dark Reading, Oktober 2020.

[6] The Surge in PC Shipments Is Not Over with Solid Growth Expected During the Holiday Quarter and into 2021, According to IDC," IDC-Pressemitteilung, Dezember 2020.

Wie wichtig es ist, auf dem neuesten Stand zu sein

Die Aktualisierung des Betriebssystems und der Anwendungssoftware ist ein wesentlicher Bestandteil jedes gut durchdachten Plans für die Endpunktsicherheit. Mit Windows Update for Business und Microsoft System Center Configuration Manager (SCCM) können Sie diesen Prozess verwalten und gleichzeitig so schnell wie möglich Updates für die Benutzer abrufen.

Die gleichen Überlegungen bedeuten, dass Sie alte und unsichere Produkte außer Betrieb nehmen und durch moderne Versionen ersetzen, z. B. Microsoft Surface-Geräte als Ersatz für ältere Endpunkte und Office 365 als Ersatz für ältere Softwareversionen. Moderne Geräte und Software werden automatisch sicher und auf dem neuesten Stand gehalten.

Nr. 2: Stärkung der Zugangskontrolle

Für die meisten Unternehmen ist der primäre Schutz für Mitarbeitergeräte ein Kennwort. Längst ist jedoch klar, dass Kennwörter nicht die beste Lösung für das Problem der Authentifizierung sind und Angreifern leichte Einstiegspunkte bieten.

Neue Technologien machen es möglich, dass Kennwörter selten oder gar nicht benötigt werden. Schließlich sollten Sie in der Lage sein, Kennwörter vollständig aus Ihrem Identitätsverzeichnis zu entfernen – wodurch erhebliche Sicherheitslücken beseitigt werden.

Die Authentifizierung ist stärker, wenn sie mehr als einen Authentifizierungsfaktor und insbesondere mehr als einen Faktortyp umfasst.

Die mehrstufige Authentifizierung reduziert das Risiko vieler Angriffsformen drastisch, einschließlich Phishing, einer gängigen Methode für Angreifer, um sich Zugang zu einem Netzwerk zu verschaffen.

Eine Vielzahl anderer etablierter Methoden bietet eine starke Authentifizierung ohne die Einschränkungen von Kennwörtern.
Dazu gehören Biometrie und Smartcards.

Die klassischen Faktortypen sind:

Etwas, das Sie kennen:
In der Regel ein Kennwort.

Etwas, das Sie haben:
Dies kann ein digitales Zertifikat, eine Smartcard oder ein anderes Hardware-Token sein.

Etwas, das Sie sind:
Biometrische Daten, im Allgemeinen ein Fingerabdruck oder eine Gesichtserkennung.

Biometrische Authentifizierung – eindeutig für jede Person

Die Ausgereiftheit und Verfügbarkeit von biometrischen Authentifizierungsprodukten nimmt immer mehr zu. Microsoft Surface-Geräten, die mit Intel® ausgestattet sind, umfassen Windows Hello for Business, das die Möglichkeit bietet, den Benutzer entweder mit biometrischen Daten oder mit einer PIN zu authentifizieren. Diese Anmeldeinformationen sind an das Gerät gebunden und werden im TPM gespeichert. Die Möglichkeit, entweder eine PIN oder biometrische Daten zu verwenden, bedeutet, dass Sie die PIN verwenden können, wenn Sie die biometrischen Daten nicht verwenden können (z. B. wenn Sie einen Verband an dem Finger haben, den Sie zur Fingerabdruckerkennung verwenden). Beachten Sie, dass Microsoft keine biometrischen Daten in der Cloud speichert.

Um auf ein durch Windows Hello for Business geschütztes Gerät zuzugreifen, müssen Sie das Gerät und entweder die PIN oder die biometrischen Daten vorliegen haben. PINs sind in der Regel für jedes Gerät eindeutig, wodurch die Verwendung derselben PIN auf mehreren Geräten vermieden wird und der Schaden begrenzt wird, der durch eine kompromittierte PIN verursacht werden kann.

IN ZAHLEN

14 Milliarden USD

Wert des globalen Endpunktsicherheitsmarkts im Jahr 2020 mit einer prognostizierten kumulierten jährlichen Wachstumsrate von 8,0 % für den Zeitraum 2021-2026.[7]

WICHTIGSTE SCHLUSSFOLGERUNGEN

Biometrische Daten sind eine starke Form der Authentifizierung. Vielleicht vergessen Sie einmal ein Kennwort oder verlieren ein Hardware-Token, aber Ihr Gesicht haben Sie immer dabei.

[7] Endpoint Security Market – Growth, Trends, COVID-19 Impact and Forecasts (2021-2026), Mordor Intelligence, 2020.

Smartcard- und FIDO-Authentifizierung

Die stärkste Form der „Etwas, das Sie haben"-Authentifizierung ist ein kryptografisches Hardware-Token. Diese kostengünstigen Geräte enthalten Krypto-Prozessoren, die Daten mit einem sicheren privaten Schlüssel digital signieren. Der Schlüssel wird dann vom System mit dem entsprechenden öffentlichen Schlüssel validiert. Ein Laptop oder ein anderes auf diese Weise geschütztes Gerät kann ohne das Hardware-Token nicht verwendet werden. Bei diesem Ansatz müssen Sie sich keine Sorgen machen, wenn ein Laptop mit unverschlüsselten Daten verloren geht oder gestohlen wird.

Es ist möglich, ein digitales Zertifikat, das auf einem tragbaren Gerät, wie einem USB-Schlüssel, gespeichert ist, als Authentifizierungsfaktor zu verwenden, aber der Stand der Technik in diesem Bereich sind kleine Hardwaregeräte, die den CTAP-Standard (Client to Authenticator Protocols) zur Verbindung mit dem System über USB, und den Authentifizierungsstandard FIDO2 verwenden. FIDO-Standards („Fast Identity Online") werden von der FIDO Alliance definiert, einem Branchenverband, dessen Mission es ist, Authentifizierungsstandards als sicherere Alternative zu Kennwörtern zu entwickeln.

Viele Unternehmen liefern FIDO-zertifizierte Produkte. Einige von ihnen verfügen über einen Fingerabdruckleser und ermöglichen so die einfache Authentifizierung mit „Etwas, das Sie sind" und mit „Etwas, das Sie haben". Surface-Geräte mit Intel, Windows Hello und Windows Hello for Business sind als FIDO2-kompatibel zertifiziert.

IN ZAHLEN

51 %

der Unternehmen geben an, dass sie beim Aufdecken von Bedrohungen ineffektiv sind, weil ihre Lösungen für Endpunktsicherheit bei der Erkennung fortgeschrittener Angriffe nicht effektiv sind.[8]

WICHTIGSTE SCHLUSSFOLGERUNGEN

FIDO-Geräte erfordern zwar, dass der Benutzer das Gerät vorliegen hat, aber sie sind der Vorreiter in Sachen kostengünstige Authentifizierung.

[8] Third Annual Study on the State of Endpoint Security Risk, Ponemon Institute, Januar 2020.

Nr. 3: Verwalten des Endpunktlebenszyklus

Die Endpunktsicherheit ist während des gesamten Gerätelebenszyklus von der Bereitstellung bis zur Außerbetriebnahme ein Thema. Die Bereitstellung und Verwaltung von Hardwaregeräten erforderte früher, dass die IT Systemabbilder für jeden unterstützten Gerätetyp entwickelt und verwaltet. Dann musste für jedes einzelne System ein Techniker im Haus oder beim Gerätehersteller die Festplatte löschen und das richtige Betriebssystem-Image darauf anwenden, bevor es an den Benutzer gesendet wurde, um sicherzustellen, dass die genehmigte Software und Richtlinien festgelegt wurden.

Bereitstellen von Geräten von überall

Intelligente Clouddienste machen diesen zeitaufwendigen Schritt überflüssig. Windows Autopilot automatisiert beispielsweise alle Phasen des Gerätelebenszyklus für IT und Benutzer. Das Gerät wird direkt vom Hersteller an den Kunden versendet. Der Sicherheitsprozess beginnt mit dem Kauf des Geräts und der Hardwarehersteller sendet eine Datei mit den Hardware-IDs des neuen Geräts. Die IT lädt diese IDs mithilfe eines Active Directory-Administratorkontos in den Windows Autopilot-Bereitstellungsdienst hoch und beansprucht das Eigentum an diesen Geräten für die Organisation. Bereitstellungsprofile werden in Autopilot erstellt und den Geräten zugewiesen.

IN ZAHLEN

8,96 Mio. USD

Durchschnittliche Kosten eines erfolgreichen Angriffs auf Endpunkte aufgrund von Verlust der IT- und Endbenutzerproduktivität und Diebstahl von Informationsressourcen.[8]

WICHTIGSTE SCHLUSSFOLGERUNGEN

Die Wartung von Systemabbildern ist, unabhängig von Sicherheitsbedenken, eine Belastung für die IT. Die cloudbasierte Bereitstellung beschleunigt den Prozess und verbessert gleichzeitig die Gerätesicherheit.

[8] Third Annual Study on the State of Endpoint Security Risk, Ponemon Institute, Januar 2020.

Schnelle und einfache Einrichtung

Die Einrichtung beginnt, wenn der Benutzer das Gerät erhält und eine Verbindung zum Internet herstellt. Windows Autopilot erkennt, dass das Gerät zu Ihrer Organisation gehört und liefert die dafür erstellte Setuperfahrung.

Zu diesem Zeitpunkt ist das Gerät mit Microsoft Intune für die Verwaltung eingerichtet. Intune beginnt damit, Richtlinien und Software auf das Gerät zu übertragen. Viele der typischen Fragen, etwa zur Konfiguration und Registrierung, werden umgangen, weil das Bereitstellungsprofil sie bereits beantwortet hat. Mit nur wenigen Klicks ist das Gerät einsatzbereit, und viele der üblichen Angriffsmöglichkeiten auf das System wurden umgangen.

Optimierte Sicherheit mit Einrichtung

Wenn es die Hardware zulässt, kann die IT, wie bei mit Intel® ausgestatteten Microsoft Surface-PCs, einzelne Funktionen im Rahmen des Setups aktivieren oder deaktivieren. Dazu gehören die Kameras, die Micro-SD-Karte, Bluetooth, 4G LTE, ob der Computer von einem USB-Gerät booten kann usw. Bei Microsoft Surface-Geräten wird diese Funktion als Surface Enterprise Management Mode (SEMM) bezeichnet. Dieser Ansatz minimiert die Auswirkungen von Remotezugriff-Trojanern und anderen Methoden, die es Angreifern ermöglichen, die Kontrolle über Gerätekomponenten zu übernehmen.

Mit Microsoft Intune kann die IT auch ein Gerät bereinigen, entweder weil es verloren ging oder gestohlen wurde, oder um es einem anderen Benutzer zuzuweisen. Nach dem Löschen wird es auf die Out-of-Box-Experience zurückgesetzt. An diesem Punkt sind wieder die richtigen Anmeldeinformationen für die Einrichtung erforderlich.

WICHTIGSTE SCHLUSSFOLGERUNGEN

Alle Phasen des Produktlebenszyklus bieten Möglichkeiten zur Stärkung der Endgerätesicherheit. Die besten Tools wie Windows Autopilot und SEMM, die in mit Intel ausgestatteten Microsoft Surface-PCs enthalten sind, ermöglichen es der IT, robuste Sicherheitspraktiken in jeder Phase zu automatisieren.

Finden Sie Ihren Weg nach vorne

Die IT-Branche hat auf schmerzhafte Art und Weise gelernt, dass es keinen Ersatz für Defense-in-Depth gibt. Die Implementierung hardwarebasierter Sicherheit ist eine weithin anerkannte Best Practice, um rein softwarebasierte Ansätze zu erweitern. Es darf nichts geben, was schiefgehen kann, wodurch es zur Kompromittierung eines Systems oder wichtiger Daten kommen könnte. Besser noch, es darf auf keinen Fall mehrere Dinge geben, die schiefgehen können.

Selbst die sichersten Unternehmen können angegriffen werden, aber auch die talentiertesten und einfallsreichsten Hacker können besiegt werden. Hierfür müssen wir ihnen bei jedem Schritt Hindernisse in den Weg legen.

Am Endpunkt tun Sie dies, indem Sie das Gerät von Beginn des Lebenszyklus an sorgfältig verwalten, vom Benutzer nicht benötigte Berechtigungen entfernen, Updates auf allen Softwareebenen umgehend anwenden und Daten sowohl während der Übertragung als auch im Ruhezustand verschlüsseln.

Mit modernen Endpunktsystemen und der Software zu deren Verwaltung kann eine solche Kontrolle umgesetzt werden, ohne dass die Fähigkeit der Benutzer eingeschränkt werden muss, ihre Arbeit zu erledigen. Mit Intel ausgestattete Microsoft Surface-PCs und Verwaltungssysteme wie Windows Autopilot sind Beispiele für den Stand der Technik bei solchen Technologien.

Nichts, was mit dem Internet verbunden ist, ist unangreifbar, aber moderne Tools und Best Practices ermöglichen es Unternehmen jeder Größe, ein hohes Maß an Schutz sowohl vor ausgeklügelten Angreifern als auch vor Benutzerfehlern bereitzustellen.

Stellen Sie sich diese Fragen

- Sind Ihre aktuellen Sicherheitsvorkehrungen ausreichend?
- Verfügen Ihre Geräte über hardwaregestützte Sicherheitsfunktionen?
- Sind die Festplatten Ihrer Laptops auf Geräteebene mit Schlüsseln im TPM verschlüsselt?
- Sind für die Anmeldung am Gerät mehrere Faktoren erforderlich?
- Wird der Dieb daran gehindert, ein neues Betriebssystem von einem USB-Laufwerk zu booten?
- Werden Angreifer daran gehindert, in die UEFI-Einstellungen zu gehen und sie zu ändern?

Machen Sie den nächsten Schritt

Vom Chip bis zur Cloud bieten Microsoft Surface-PCs mit Intel-Prozessoren integrierten Schutz auf jeder Ebene. Sie können sicher sein, dass Sie die beste und optimale Implementierung von Sicherheit auf jeder Ebene des Compute-Stacks haben.

Als autorisierter Microsoft Surface-Handelspartner bieten wir eine Reihe von Geräten, Dienstleistungen und Support an, die Ihnen bei der Implementierung von Surface in Ihrem Unternehmen helfen. Von der Finanzierung über die Bereitstellung bis hin zum technischen Support nach dem Verkauf und Endbenutzerschulungen – wenden Sie sich an uns, um eine Lösung zu finden, die Ihren Geschäftsanforderungen entspricht.

Kontakt: [Reseller contact info]

Partner-Logo hier einfügen

© 2021 Microsoft Corporation. Alle Rechte vorbehalten. Dieses Dokument wird „wie besehen“ bereitgestellt. Die Informationen und geäußerten Ansichten in diesem Dokument, einschließlich URLs und anderer Verweise auf Internetwebsites, können ohne vorherige Ankündigung geändert werden. Das Nutzungsrisiko liegt bei Ihnen. Dieses Dokument gewährt Ihnen keinerlei Rechte am geistigen Eigentum eines Microsoft-Produkts. Sie können dieses Dokument zu internen Referenzzwecken kopieren und verwenden.