Windows 11 (nicht nur) aus Security-Sicht

Eingehegt

Renato Venzin, Remo Wobmann

Mit Windows 11 schaltet Microsoft etliche schon vorhandene Schutzmaßnahmen scharf und zieht die Zügel bei Hardwareanforderungen an. Teams- und Android-Integration schaffen neue Risiken.

Bereits im Vorfeld der am 5. Oktober 2021 offiziell veröffentlichten Windows-11-Version lösten vor allem die strengen Anforderungen an die Hardware Irritationen aus, führen sie doch dazu, dass Millionen von aus heutiger Sicht leistungsfähigen Computern in wenigen Jahren für den Betrieb von Windows nutzlos sind. Microsoft begründet die hohen Hardwarehürden damit, dass Windows 11 mit Fokus auf gesteigerte Zuverlässigkeit und Sicherheit bei gleichzeitig hoher Kompatibilität entwickelt worden sei. Es lohnt sich also, das neue Betriebssystem vor allem unter dem Blickwinkel der Sicherheit zu betrachten.

Auch die Änderungen bezüglich kompatibler Software und bekannter Applikationen muss man im Auge behalten. So ist der Internet Explorer nicht mehr vorhanden und wurde komplett durch Microsoft Edge ersetzt. Teams erhält eine zweite Version für persönliche Microsoft-Accounts, die standardmäßig installiert ist, und Android-Apps können nun über Windows Subsystem for Android (WSA) installiert und genutzt werden. Diese neuen Features eröffnen auch zusätzliche Angriffspunkte.

Hohe Ansprüche an CPU und Co.

Die von Microsoft publizierten Hardwareanforderungen für Windows enthalten zunächst die üblichen Ansprüche an RAM, Prozessorleistung und Speicher (Abbildung 1). Windows 11 erfordert jedoch auch Hardware, die für bisherige Versionen von Windows noch nicht zwingend notwendig war. Hierzu gehört das Trusted Platform Module (TPM), das zwar auch bei Windows 10 für neue Systeme vorausgesetzt wurde, jedoch nicht bei einem Upgrade von einer vorherigen Version. Doch vor allem die von Microsoft gepflegte Liste mit offiziell kompatiblen Prozessoren für den Betrieb von Windows 11 wurde in den vergangenen Monaten kontrovers diskutiert. So sollen die allermeisten vor 2018 produzierten Prozessoren als inkompatibel gelten (siehe ix.de/z8qf).

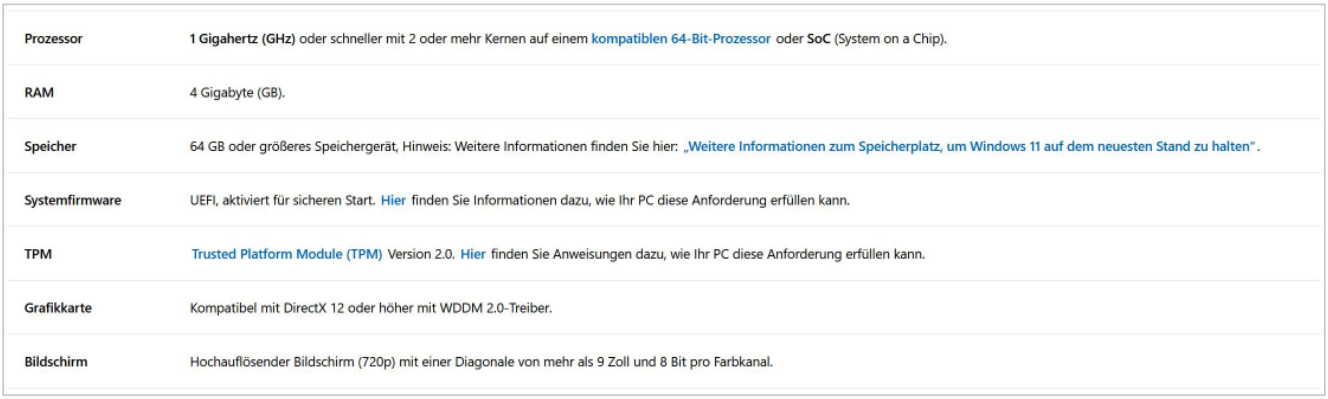
Als Grund für die hohen Anforderungen nennt Microsoft die Sicherheitsfunktionen, die auch in Windows 10 nutzbar sind: Secure Boot, Geräteverschlüsselung mittels BitLocker, Windows Hello, Virtualization Based Security (VBS) und Hypervisor-Protected Code Integrity (HVCI) (siehe ix.de/z8qf). Diese sollen laut Microsoft die Ausführung von Schadsoftware auf Windows-Systemen um bis zu 60 Prozent reduzieren. Im Unterschied zu Windows 10, wo sie noch standardmäßig deaktiviert waren, soll ihre Ausführung nun teils erforderlich sein, weshalb mittels der Anforderungen die Kompatibilität gewährleistet wird.

Dass mit Windows 11 nur altbekannte Sicherheitsfeatures zur Anwendung kommen, bezeugt auch die Windows 11 Security Baseline vom 5. Oktober 2021 (siehe ix.de/z8qf). Security Baselines stellt Microsoft jeweils bei der Einführung neuer Windows-Versionen oder nach Feature-Updates zur Verfügung. Administratoren nutzen sie, um trotz der großen Anzahl von Steuerelementen einen Grundschutz in puncto Sicherheit gewährleisten zu können und neue Sicherheitsfunktionen zu aktivieren.

Windows 11 läuft nur auf Prozessoren, die die Sicherheitsfunktionen performant ausführen können und bei denen das neue DCH-Treibermodell umgesetzt ist. Damit die künftig aktivierten Sicherheitsfunktionen die Leistung möglichst wenig beeinträchtigen, sind sie von der Software in die Hardware gewandert. Bei Prozessoren älterer Generationen muss HVCI teilweise mittels Software emuliert werden, was zu weniger Rechenleistung bei gleichzeitig erhöhtem Stromverbrauch führt. Inzwischen ließ Microsoft in Zusammenarbeit mit den Chipherstellern die entsprechenden Funktionen direkt in die Chips einbauen. Bei den Herstellern erhielt die Technologie unterschiedliche Namen, bei Intel „Mode-based execute control for EPT“ (MBEC), bei AMD „Guest-mode execute trap for NPT“ (GMET) und bei ARM „Translation table stage 2 Unprivileged Execute-never“ (TTS2UXN).

Secure Boot als Schutz gegen Rootkits

Die Grundlage für die Aktivierung der Schutzfunktionen ist damit geschaffen. Interessant dürfte jedoch sein, ob die Software von Drittherstellern mit Windows 11 kompatibel ist. Gemäß Microsoft sollte das



Prozessor	**1 Gigahertz (GHz)** oder schneller mit 2 oder mehr Kernen auf einem kompatiblen 64-Bit-Prozessor oder **SoC** (System on a Chip).
RAM	4 Gigabyte (GB).
Speicher	64 GB oder größeres Speichergerät, Hinweis: Weitere Informationen finden Sie hier: „Weitere Informationen zum Speicherplatz, um Windows 11 auf dem neuesten Stand zu halten".
Systemfirmware	UEFI, aktiviert für sicheren Start. Hier finden Sie Informationen dazu, wie Ihr PC diese Anforderung erfüllen kann.
TPM	Trusted Platform Module (TPM) Version 2.0. Hier finden Sie Anweisungen dazu, wie Ihr PC diese Anforderung erfüllen kann.
Grafikkarte	Kompatibel mit DirectX 12 oder höher mit WDDM 2.0-Treiber.
Bildschirm	Hochauflösender Bildschirm (720p) mit einer Diagonale von mehr als 9 Zoll und 8 Bit pro Farbkanal.

In der Anforderungsliste für Windows 11 ist das Trusted Platform Module (TPM) jetzt vorgeschrieben (Abb. 1).

speziell für sicherheitsrelevante und DLP-Tools mit dem Hersteller geklärt werden.

Gegen Rootkits, also Schadsoftware, die sich unterhalb der Betriebssystemebene einnistet, ist Antivirensoftware machtlos. Diesem Angriffsvektor wirkt Secure Boot entgegen, das beim Booten des Systems die Integrität sicherstellt. Dies geschieht, indem die Integrität der Firmware und Software vom UEFI über den Bootloader des Betriebssystems, den Kernel, Systemtreiber, Systemdateien bis zum Early-Launch-AntiMalware-Treiber (ELAM) sichergestellt wird. Ist die Integrität des Systems nicht bestätigt, kann ein Verwaltungswerkzeug wie Intune oder Microsoft Endpoint Configuration Manager Maßnahmen ergreifen und dem Gerät sogar den Zugang zum Netzwerk verweigern.

BitLocker, schon seit Windows Vista dabei, dient bei Windows 11 weiterhin zur vollständigen Verschlüsselung des Datenspeichers. Vor allem bei mobilen Geräten ist dies wichtig, da diese häufig physisch exponiert sind. Für die komfortable und sichere Verwendung von BitLocker ist ein TPM unabdingbar, da das Schlüsselmaterial für die Entschlüsselung darin abgelegt ist. Wie in den vergangenen Windows-Versionen wird BitLocker auch bei Windows 11 in der Home-Version nicht verfügbar sein.

Hardwarevirtualisierung ermöglicht virtualisierungsbasierte Sicherheit (VBS), die einen vom normalen Betriebssystem getrennten, sicheren Speicherbereich erstellt (siehe ix.de/z8qf). Windows kann diesen „virtuellen Sicherheitsmodus" nutzen, um eine Reihe von Sicherheitslösungen zu etablieren, die einen deutlich verbesserten Schutz vor Schwachstellen im Betriebssystem bieten und die Verwendung bösartiger Exploits verhindern, die versuchen, die Schutzmaßnahmen zu umgehen. Hypervisor-Enforced Code Integrity (HVCI) ist eine dieser Lösungen. In Windows wird es als „Speicherintegrität" bezeichnet und eingesetzt, um Codeintegritätsrichtlinien durchzusetzen.

Zero Trust: Traue keinem

Bedrohungen kommen zunehmend aus dem Inneren der eigenen Infrastruktur. Ein wichtiges Ziel, das sich Microsoft (und viele andere Hersteller) deshalb gesetzt haben, ist Zero Trust. Der Grundsatz lautet: Keinem Gerät, Nutzer oder Dienst innerhalb oder außerhalb des eigenen Netzwerks wird vertraut. Um dies bewerkstelligen zu können, sind umfangreiche Maßnahmen zur Authentifizierung sämtlicher Nutzer, Dienste und Systeme erforderlich. Das zwingend notwendige TPM 2.0 weist in diese Richtung.

Da Systeme heutzutage vernetzt sind, ist Malware nahezu unvermeidbar. Statt erst bei Verdacht durch Benutzer oder Netzwerkadministratoren aktiv zu werden, sollten kritische Daten auf Servern und Computern von vornherein isoliert werden. Das schwächste Glied in einem modernen Netz ist das Gerät des Benutzers selbst. Dort sind die Zugangsdaten für Angreifer ein interessantes Ziel. Microsoft versucht deshalb, sich weg von lokalen Passwörtern zu bewegen und zu einer biometrischen Authentifizierung überzugehen. Bei der Installation der Home-Version von Windows 11 wird beispielsweise die Verwendung eines Microsoft-Kontos vorgeschrieben. Dort bietet es sich an, Windows Hello mit biometrischen Anmeldeverfahren zu nutzen. Passwörter, die Angreifern oft Tür und Tor öffnen, werden damit im Verbraucherumfeld zurückgedrängt – zumindest beim lokalen System.

Sicherheitsfeatures in der CPU mit Microsoft Pluton

In den letzten Jahren hat Microsoft eng mit AMD, Intel und Qualcomm zusammengearbeitet, um den Vertrauensanker des Gesamtsystems direkt im Prozessor unterzubringen. Dabei entstand der Sicherheitsprozessor Microsoft Pluton. Hier verwendet Microsoft die Chip-to-Cloud-Sicherheitstechnologie, die schon in der Xbox eingesetzt wird, erstmals mit Windows.

Ohne Pluton befindet sich das TPM als Hardwaremodul auf der Hauptplatine. Da der Prozessor mit diesem kommunizieren muss, kann die Verbindung bei physischem Zugang abgehört werden. Pluton emuliert selbst die Funktion eines TPM 2.0-Moduls, wodurch die Ausnutzung dieser Schwachstelle stark erschwert wird, da alles im Prozessor integriert ist. Sicherheitsfunktionen wie BitLocker und Secure Boot, die auf

iX-TRACT

- Mittels strikter Hardwareanforderungen schafft sich Microsoft die Möglichkeit, in Windows 11 die in den letzten Jahren entwickelten Sicherheitsfunktionen zu aktivieren.
- Die Verwendung von Passwörtern soll zugunsten biometrischer Anmeldeverfahren zurückgedrängt werden.
- Trusted Platform Modules (TPMs) stellen die Integrität des Gesamtsystems sicher. TPM-spezifische Schwachstellen soll künftig Microsoft Pluton beseitigen.
- Der Internet Explorer ist entfernt, der IE Mode im Edge-Browser bleibt inklusive Trident Engine erhalten.
- Microsoft Teams ist neu nativ ins System integriert. Die private Teams-Version kann zusätzliche Angriffsflächen erzeugen.
- Das Windows Subsystem for Android ist zwar freigegeben, doch Apps sind erst testweise verfügbar und Informationen sowie Konfigurationsmöglichkeiten bisher spärlich vorhanden.

dem TPM aufbauen, werden auf diese Weise noch sicherer. Künftig soll Pluton auch Anmeldeinformationen, die ID der Benutzer, Verschlüsselungscodes und persönliche Daten vor Schadsoftware oder bei Diebstahl des PCs schützen. Der Sicherheitsprozessor wird ab 2022 in ausgewählten neuen Windows-PCs ausgeliefert.

TPM deaktivieren: möglich, aber nicht empfehlenswert

Im Web kursieren Anleitungen, mit Änderungen in der Windows Registry die Anforderungen an ein TPM 2.0 für Windows 11 zu umgehen. Microsoft ermöglicht dies zu Testzwecken. Die Umsetzung deaktiviert die entsprechenden Schutzfunktionen und ist damit auf Produktivsystemen nicht zu empfehlen. Sofern die Hardwareanforderungen den Betrieb von Windows 11 nicht erfüllen, bleibt Windows 10 noch für einige Zeit die richtige Wahl als Betriebssystem. Es wird noch bis zum 14. Oktober 2025 unterstützt.

Nach 25 Jahren erstmals ohne Internet Explorer

Windows 11 ist das erste Microsoft-Betriebssystem seit Windows 95, auf dem kein Internet Explorer vorinstalliert ist. Spuren davon wird es aber weiterhin geben. Denn der Internet Explorer (IE) Mode des Edge-Browsers bleibt erhalten, um Legacy-Seiten darstellen zu können, und zwar bis mindestens 2029. Also ist auch bei Windows 11 die Trident MSHTML Engine des Internet Explorer noch an Bord.

Firmen, die den IE Mode nicht benötigen, können diesen weiterhin (wie in Windows 10) deaktivieren. Für Systemadministratoren, die sich bisher noch nicht mit diesem Feature auseinandergesetzt haben, ist es beim Wechsel auf Windows 11 sicher sinnvoll, sich einzulesen und die Einstellungen an die firmeninterne Systemlandschaft anzupassen.

Damit der IE Mode funktioniert, ist das optionale Feature Internet Explorer Mode vorinstalliert. Es lässt sich aber entfernen. Dadurch können die Benutzer zwar in Microsoft Edge noch immer Seiten definieren, die mit der Internet Explorer Engine dargestellt werden sollen, aber beim Zugriffsversuch erscheint eine Fehlermeldung (Abbildung 3).

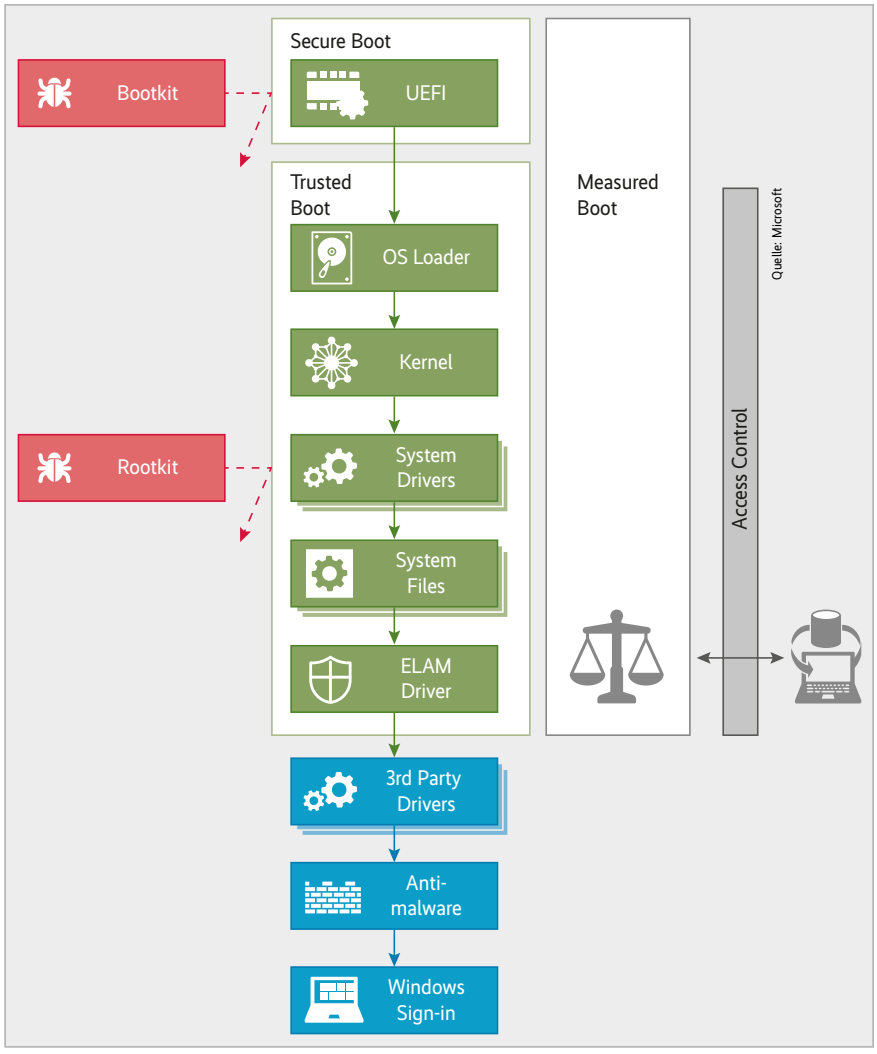
Neu in Windows 11 ist die standardmäßige Integration von Microsoft Teams, das der neuen Chatapplikation zugrunde liegt. Diese und das dazugehörige Teams für persönliche Accounts, die dazu dienen sollen, möglichst einfach mit Bekannten und Verwandten zu chatten, sind auf persönliche Microsoft-Accounts beschränkt. Das heißt, dass für Arbeits- und Schulaccounts weiterhin die bisher bekannte Teams-Version verwendet und installiert wird.

Nicht ungefährlich: Teams für persönliche Benutzer

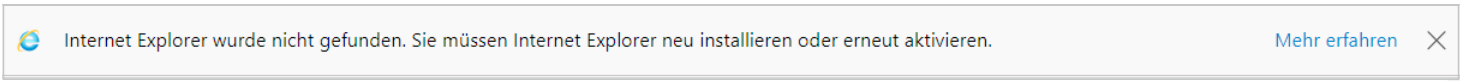
Durch die standardmäßig installierte „private“ Teams-Version entsteht eine weitere Angriffsfläche. Während die „Work“-Variante die Kommunikation mit externen Personen mittels Federation oder Guest Access einschränken kann (siehe ix.de/z8qf), ist dies bei der Chatversion nicht sinnvoll, da sie schließlich genau dafür ausgelegt ist. Da Phishing via Microsoft Teams kein neues Phänomen ist, hat Microsoft einige Vorkehrungen getroffen (siehe ix.de/z8qf). Zudem erhalten Benutzer bei jedem Kontaktversuch einen Warnhinweis und als weitere Barriere für Phishingangriffe die Möglichkeit, eine Vorschau anzuzeigen.

Dennoch ist anzunehmen, dass Angreifer versuchen werden, diesen Kanal auszunutzen – ähnlich wie bei E-Mail-Phishing, wo [Extern]-Tags in der Betreffzeile oder Warnhinweise beim Öffnen von Anhängen auch keinen hundertprozentigen Schutz bieten.

Neben der Bedrohung durch Phishing sind auch potenzielle zusätzliche Schwachstellen nicht zu vernachlässigen. Einige, wie CVE-2020-17091, CVE-2020-10146 und TRA-2021-231, wurden bereits entdeckt (siehe ix.de/z8qf). In Zukunft werden vermutlich weitere auftauchen. Zero-Click-Schwachstellen, die keine Benutzerinter-



Die Secure-Boot-Kette soll Windows-Systeme vor Rootkits schützen (Abb. 2).



Ist der IE-Mode in Edge deaktiviert, führen Legacy-Seiten zu einer Fehlermeldung (Abb. 3).

aktion benötigen, wie im Zusammenhang mit CVE-2020-10146, sind besonders gefährlich. Potenzielle Schwachstellen könnten auch Sicherheitsvorkehrungen wie die Vorabinfo bei Kontaktversuch umgehbar machen. Auch könnten sich Angreifer durch Social Engineering als vertrauenswürdige Absender ausgeben und erst wenn diese erste Barriere nicht mehr existiert, versuchen, Schwachstellen auszunutzen.

Die einfachste Maßnahme wäre, die Applikation zu deinstallieren und die Benutzer anzuweisen, für persönliche Kommunikation auch persönliche Geräte zu verwenden. Doch durch das Vorhandensein von Chat/Teams auf allen Windows-11-Geräten wird vor allem bei Mitarbeitern mit direktem Kundenkontakt der Wunsch verstärkt, diesen Kommunikationsweg auch zu verwenden.

Firmen, die die Chatfunktion nutzen möchten, sollten wie bei anderen Kommunikationsmitteln mit Awareness-Maßnahmen arbeiten. Die Beschäftigten sollten entsprechend geschult werden, um Phishingangriffe möglichst zu unterbinden, Updates sollten zeitnah eingespielt und die Infrastruktur sollte anderweitig abgesichert werden, sodass verdächtiges Verhalten erkannt wird und bei einer Kompromittierung eines Gerätes die Möglichkeiten eines Angreifers eingedämmt werden, um das betroffene Gerät zu isolieren.

Integration von Android-Apps noch nicht ganz ausgereift

Eine der unerwarteten Änderungen, die in zahlreichen Medien, Foren und Blogs Furore machte, ist sicher die Integration von Android-Apps ohne Emulator, der bisher immer nötig war, um Android-Apps unter Windows auszuführen. Dies soll nun dank der neuen Intel Bridge Technology nicht mehr nötig sein. Sie verwendet einen Post-Compiler, der dazu dient, die Android-Apps auf x86-Umgebungen laufen zu lassen.

Als dieser Artikel entstand, war diese Möglichkeit erst testweise für die Developer Preview und für die US-Region verfügbar (siehe ix.de/z8qf). Bis zum offiziellen Release können sich also noch Dinge ändern oder neue Funktionen hinzukommen. Während die meisten verfügbaren Funktionen getestet werden konnten, war der Amazon Appstore aufgrund der Restriktion auf US-Accounts nicht verfügbar. Was die Sicherheitsaspekte angeht, gibt es derzeit nur sehr eingeschränkte Informationen. Auch GPOs oder Einstellungen in Intune sind noch nicht vorhanden.

Obwohl die Technik von Intel entwickelt wurde, funktioniert die Post-Kompilierung der Nicht-x86-Instruktionen auf x86-Instruktionen auf allen x86-CPUs, also auch denen von AMD. Geräte mit ARM-Prozessoren werden ebenfalls nicht ausgenommen sein. Da diese die Instruktionen bereits verstehen, benötigen sie diese Übersetzungsschicht erst gar nicht. Durch diese Technologie sollten fast alle Apps, die sich auf Android-Geräten installieren lassen, auch unter Windows funktionieren. Eine Garantie besteht hierfür jedoch noch nicht.

Android-Apps nur über Amazon Store

Um die Apps zur Verfügung zu stellen, wird nicht der Google Play Store verwendet, sondern der Underground AppStore von Amazon. Unter Android würde das eine Abschwächung der Sicherheit darstellen, da die Installation von nicht vertrauenswürdigen Quellen aktiviert werden muss – was auch die Installation jeglicher anderen Applikation erlaubt. Bei Windows ist dies hingegen grundsätzlich nicht der Fall.

Ein weiterer Store vergrößert dennoch die Angriffsfläche. Microsoft wie auch Amazon betonen zwar, dass die in ihre jeweiligen Stores hochgeladenen Programme genau überprüft werden und sicher sind, dennoch gab es bei beiden Stores immer wieder Fälle, in denen sie Schadsoftware verteilt haben (siehe ix.de/z8qf). Um Apps aus dem Amazon Store herunterzuladen, ist natürlich ein Amazon-Account nötig. Ob und wie dieser in einem Business-Umfeld verwaltet werden kann, ist derzeit noch nicht klar und wird dadurch verkompliziert, dass die Apps grundsätzlich über den Microsoft Store aufrufbar sind, aber dann über den Amazon Appstore heruntergeladen und installiert werden. Auch hierzu gibt es noch keine Statements oder Richtlinien und es steht noch nicht fest, ob sich wie bisher Zugriffe auf App-Basis einschränken lassen oder ob der Amazon Store vollständig deaktiviert werden muss. Auch ob eine Integration der Benutzeraccounts möglich sein wird oder ob man auch in Zukunft persönliche Amazon-Accounts benutzen muss, ist bisher noch nicht bekannt.

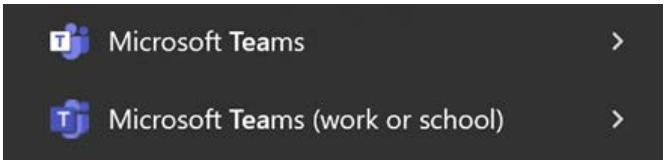
Installation von Apps auch durch die Hintertür

Wird der Amazon Appstore oder eine Android-App aus dem Microsoft Store installiert, kommt im Hintergrund auch unmittelbar das benötigte Windows Subsystem for Android (WSA) mit der Android-Version 11 mit auf das System. Alternativ kann das WSA auch direkt installiert und konfiguriert werden. Danach können die Apps normal über den Store heruntergeladen werden und erscheinen wie Microsoft-Store-Apps im Startmenü und in der Suche. Statt der Schaltfläche „Get“ für Microsoft-Store-Apps erscheint bei den Amazon-Apps „Get from Amazon AppStore“.

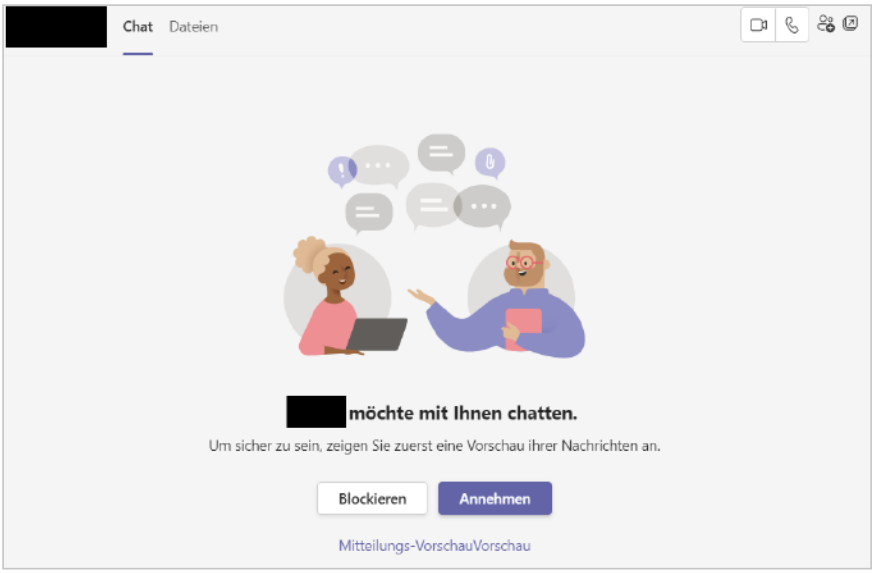
Neben der Installation über Stores können beliebige APKs wie bei Android auch über Sideloading installiert werden. Dazu kann wie bei physischen Android-Geräten die Android Debug Bridge (ADB) verwendet werden (siehe ix.de/z8qf).

ADB erfordert keine Installation und lässt sich direkt aus dem Ordner „Downloads“ ausführen. Standardmäßig können Benutzer dafür die Einstellungen des WSA ändern und den Developer Mode aktivieren, damit das Sideloading funktioniert. Microsoft-Entwickler haben bestätigt, dass dies so gewünscht ist. So kann ein Benutzer, für den das WSA aktiviert ist, beliebige Apps sideloaden und im WSA-Container ausführen.

Damit wird in aller Regel die Installationsrichtlinie des Unternehmens geschwächt, da Benutzer potenziell App-Locker oder sonstige Einschränkungen umgehen und unerwünschte Software installieren können. Es steht zu erwarten, dass



Das doppelte Teams: Wer Microsoft Teams im Unternehmen oder zur Ausbildung nutzt, braucht zusätzlich zur bereits installierten privaten Version eine zweite (Abb. 4).



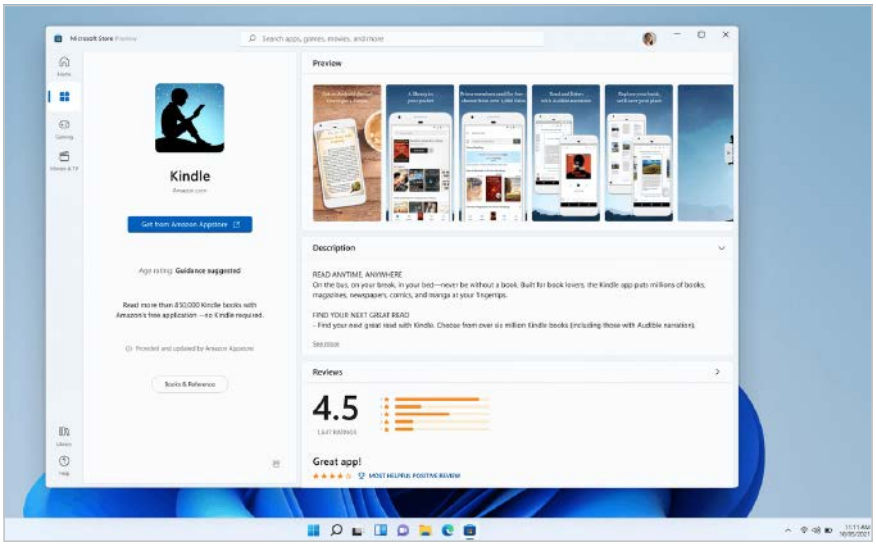
Bei Kontaktversuchen via Teams warnt eine Nachricht und ermöglicht die Anzeige im Vorschaumodus (Abb. 5).

dies in Zukunft über Gruppenrichtlinien oder Intune einschränkbar ist, allerdings sind derzeit noch keine Informationen oder entsprechende Einstellungen verfügbar. Auch die Microsoft Docs erwähnen bisher nur, dass die Installation von Android-Apps möglich ist, nähere Informationen zum Thema Einschränkung und Absicherung der Applikation sind noch nicht vorhanden (siehe ix.de/z8qf).

Zusätzliche Absicherung nötig

Ähnlich wie das Windows Subsystem for Linux läuft auch das Windows Subsystem for Android in einem Container, der vom normalen Betriebssystem isoliert ist. Bisher gibt es kein Share für den Datenaustausch wie das WSL$ Share beim bei Subsystem für Linux. Es können aber Daten über ADB übertragen werden.

Laut Microsoft können sowohl Treiber im Kernel-Mode wie auch Applikationen mit Medium Integrity Level auf die Android-Container und den App-Speicher zugreifen (siehe ix.de/z8qf). Dieses Level ist für Standardapplikationen und Benutzer festgelegt. Also wird es erforderlich sein, sensible Daten anderweitig zu schützen. Microsoft schreibt auch, dass das Android Subsystem Daten softwarebasiert auf Dateibasis verschlüsselt. Allerdings gibt es dazu keine weiteren Informationen. Die genaue Funktionsweise muss also erst noch erforscht oder von Microsoft dokumentiert werden, ehe klar ist, welche Zugriffe möglich sind und welche nicht.



Der Microsoft Store in Windows 11 integriert den Amazon Store zur Installation von Android-Apps (Abb. 6).

Insgesamt ist also das Windows Subsystem for Android noch nicht in einem finalen Stadium, diverse Änderungen und Updates werden wohl folgen. Dies ist auch am Statement zu den Hardwareanforderungen ersichtlich: „Additional requirements anticipated and will be communicated as the product is rolled out to select geographies“ (siehe ix.de/z8qf).

Auch hinsichtlich der Einschränkungen und sonstigen Konfigurationsmöglichkeiten im Businessumfeld hat Microsoft bisher nicht viel kommuniziert oder implementiert. Also sollte man sich überlegen, ob man mit der Nutzung dieser Funktionen nicht noch abwarten möchte. Mit dem offiziellen Release des Features dürften auch die entsprechenden Funktionen und Best Practices folgen.

Fazit

Mit Windows 11 werden erweiterte Sicherheitsfunktionen aus der Windows-10-Ära weitergeführt und mittels strikter Hardwareanforderungen kompatibel zu den in Betrieb befindlichen Systemen gemacht. Das Ziel war also nicht, neue Sicherheitsfunktionen einzuführen, sondern bestehende einsetzbar zu machen. Zudem führen die Zero-Trust-Ansätze zu sichereren Systemlandschaften, da den Systemen und Applikationen von Grund auf misstraut wird und sich diese stets authentifizieren müssen. Mit dem Entfernen des Internet Explorer schneidet Microsoft alte Zöpfe ab. Die native Teams-Integration und das Windows Subsystem for Android inklusive App-Store stellen Sicherheitsverantwortliche in Unternehmen vor neue Herausforderungen. (ulw@ix.de)

Quellen

Zahlreiche Links zu Microsoft-Quellen und weitere Informationen über hardwarebasierte Sicherheitsmaßnahmen, den IE Mode, Teams/Chat und Android Apps in Windows 11 sind unter ix.de/z8qf zu finden.

Renato Venzin

ist Penetration Tester bei der Oneconsult AG. In seiner täglichen Arbeit unterstützt er Kunden dabei, Schwachstellen zu entdecken und zu beheben.

Remo Wobmann

ist System Engineer und Penetration Tester bei der Oneconsult AG. Bei seiner täglichen Arbeit ist er auf das Eindringen in IT-Systeme, andererseits auf deren Absicherung spezialisiert.