Verwaltung mobiler Geräte in der Cloud

Know-how Für die sichere Verwaltung von Endgeräten und Apps in der Cloud empfiehlt sich, einen Wechsel auf Microsoft-Technologie zu prüfen.

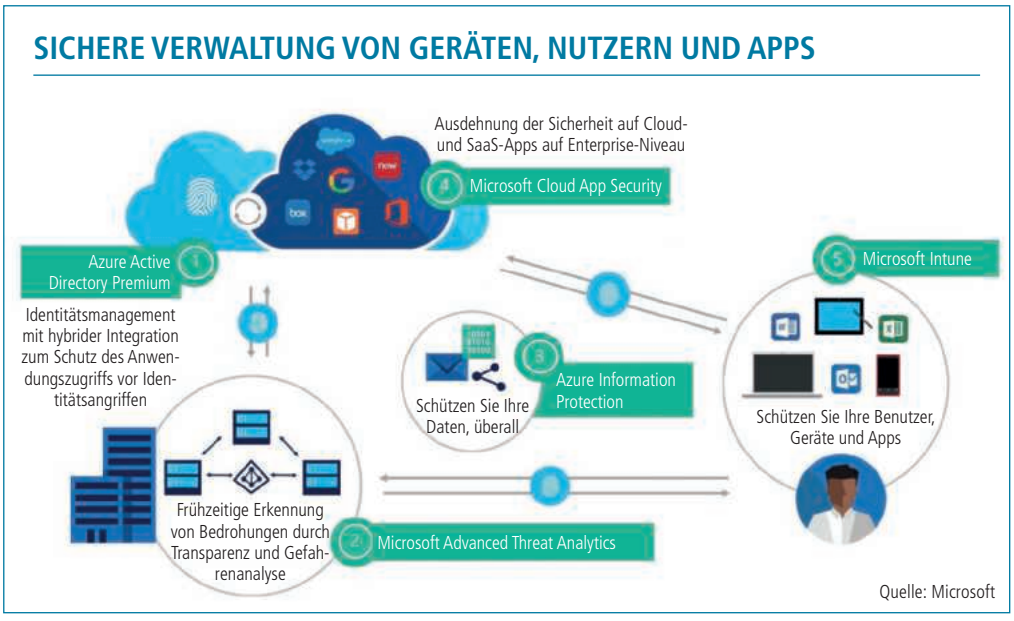
Von Jonas Hofer

Die sichere Verwaltung mobiler Endgeräte wie Smartphones, Tablets und Notebooks in Unternehmen wird auch heute noch mehrheitlich mit mächtigen Unified-Endpoint-Management-Lösungen verschiedener Hersteller gehandhabt. Mit der allgemein zunehmenden Akzeptanz für Cloud Services und der immer grösseren Durchdringung der Cloud-Angebote von Microsoft – namentlich der Office-Produkte in Microsoft 365 sowie den ergänzenden Abonnementsdiensten – ist die Zeit reif, auch für das Geräte- und App-Management eine Auslegeordnung vorzunehmen. Tatsächlich ist in Unternehmen mittlerweile diesbezüglich ein Sinneswandel festzustellen. Ausgehend von den Bedürfnissen und Möglichkeiten zum Management und dem sicheren Betrieb mobiler Geräte mit MacOS und Windows 10/11 sollen im Folgenden Gründe aufgezeigt werden, die einen Wechsel von Drittlösungen zu Microsoft-Technologien rechtfertigen.

Sicherheit wird oft stiefmütterlich behandelt

Da wäre einmal der technische Aspekt. Denn mit der Verschiebung von Anwendungen in die Cloud ist es folgerichtig, die Geräte auch dort zu verwalten, wo die Dienste betrieben werden – in der Cloud eben. Dann wäre da noch die Kostenfrage: In den Enterprise-Lizenzen von Microsoft 365 sind mit dem Endpoint Manager bereits teilweise Lizenzen für die entsprechenden Funktionalitäten eingeschlossen. Dies entspricht der gängigen Strategie des Herstellers, Funktionen in Services mitzuliefern, welche die Kunden zunächst nicht oder nur teilweise und erst mit der Zeit verwenden. So kann der Hersteller nach und nach die Akzeptanz für die Produkte steigern, die Services den Bedürfnissen gemäss weiterentwickeln und Marktanteile hinzugewinnen. Ein solches Vorgehen entspricht aber auch der Erweiterbarkeitslogik des Cloud-Gedankens: Kunden sollen Lösungen ausbauen und konfigurieren können, während der Anbieter Betriebs- und Anwendererfahrungen nutzt, um die Services mit der Zeit weiter anzupassen, auszubauen und zu verbessern. Mehr und mehr Unternehmen erkennen aus den genannten Gründen, dass für ihre Zwecke Wartungs- und Lizenzkosten eingespart werden können. Denn sie benötigen in der Cloud hauptsächlich Zugriff auf E-Mail, Kalender und Office-Apps und nicht die umfangreichen, meist on Premises betriebenen Werkzeuge von Drittherstellern und können deshalb die Funktionalitäten durch die bereits vorhandene Lösung von Microsoft 365 ersetzen.

Darüber hinaus gibt es nach wie vor noch sehr viele Unternehmen, die zwar Daten in die Cloud verlagern oder mit mobilen Endgeräten Zugriff auf Unternehmensinformationen ermöglichen, bei denen aber entsprechende Sicherheitsvorkehrungen noch ganz fehlen. Dabei sind es längst nicht nur kleinere Firmen, die dem Schutz der Daten nicht die nötige Aufmerksamkeit zukommen lassen. Die Erfahrung in der Praxis zeigt, dass durchaus auch bei Grossunternehmen die Sicherheitsfrage – gelinde gesagt – stiefmütterlich behandelt wird.



Die sichere Verwaltung von Geräten, Nutzern und Apps als Teil der diversen Sicherheitskomponenten in der Microsoft Cloud. Das Dispositiv besteht aus fünf Elementen.

Lizenzkosten sparen

Unternehmen, die ihre Daten bereits in Microsoft Cloud Services speichern, so etwa in Exchange Online für E-Mail, Sharepoint Online für Zusammenarbeit oder Onedrive für Filehosting, haben die Lizenzen zur Nutzung für den Endpoint Manager aufgrund der Lizenzstruktur in den E3-Lizenzen (oder höher) bereits in ihrem Abonnement inkludiert. In der Lösung wurden unlängst die Admin-Tools Intune zur Verwaltung von PCs und mobilen Endgeräten sowie der System Center Configuration Manager (SCCM) zur Verwaltung von Geräten und Software innerhalb von Unternehmen zusammengeführt. Da SCCM die Verwaltung von Tablets und Smartphones nicht unterstützte, mussten nämlich Unternehmen dafür teilweise zusätzlich Intune verwenden. Die Funktionen von SCCM können mittlerweile aber mit äquivalenten Funktionen in Intune ersetzt werden.

Wesentlich günstiger als vollwertige Enterprise-Lizenzen sind Frontline-Lizenzen. Diese werden für Mitarbeitende benötigt, die nicht über Büro-Arbeitsplätze mit PC oder Laptop verfügen, sondern lediglich ein Smartphone oder Tablet bei ihrer Arbeit verwenden. Solche Deskless-Angestellte arbeiten üblicherweise an Maschinen oder Geräten, in Service-Organisationen oder in sonstigen Tätigkeiten, für die kein vollwertiger Computer benötigt wird, und sie verwenden ihre mobilen Geräte beispielsweise nur für die Kenntnisnahme von Informationen oder die Beantwortung von E-Mails. Da Microsoft die Dienste der Azure-Plattform immer stärker pusht, steigt in Unternehmen auch immer mehr das Bewusstsein für die Bemühungen der Redmonder, im Bereich der IT-Managementlösungen stärker Fuss zu fassen. Lassen sich nun durch den Verzicht auf kostspielige und in vielen Fällen die Bedürfnisse der Firmen übererfüllende Lösungen Lizenz- und Wartungskosten von Drittanbietern einsparen, so kann dies durchaus ein Grund dafür sein, die Verwaltung von Geräten und Apps in der Microsoft Cloud in Erwägung zu ziehen und damit dem stetig wachsenden Kostendruck auf die IT ein Stück weit entgegenzuwirken. Immerhin können Firmen durch einen Wechsel je nach Unternehmensgrösse und eingesetzter Lösung ihre jährlichen Ausgaben im unteren bis mittleren fünfstelligen Bereich senken.

Weniger Komplexität und mehr Sicherheit

Mindestens ebenso bedeutend wie das Kostenthema ist die Frage der technischen Komplexität einer IT-Umgebung. Denn wenn schon Services für Mitarbeitende aus der Microsoft Cloud angeboten werden, die Identitäten ebenso mit Azure AD und Zugriffsmechanismen mit Conditional Access verwaltet werden, so sollten über kurz oder lang auch mobile Geräte und Apps in der Cloud gemanagt werden. So lässt sich damit beispielsweise für Conditional Access auch gleich der Gerätestatus miteinbeziehen und damit beispielsweise ein Zero-Trust-Prinzip nach dem Motto «vertraue niemandem, verifiziere jeden» in ein und derselben technischen Umgebung einfacher umsetzen. Es entfällt durch die Reduktion der Komplexität nämlich schon mal die Schnittstellenproblematik. Das Problem dabei: Sobald unterschiedliche Systeme miteinander verbunden werden müssen, kommt es früher oder später zu Schwierigkeiten. Denn Schnittstellen müssen ständig unterhalten werden. Drittherstellen von Mobile-Device-Management (MDM)-Lösungen müssen sich darum bemühen, mit den Gegebenheiten der Microsoft Cloud umgehen zu können, sodass ihre Plattformen auch dauerhaft unterstützt werden. Nicht selten geschieht dies allerdings nur reaktiv mit dem Resultat, dass der Kunde das Problem erst bemerkt, wenn etwas – beispielsweise der Zugriff auf Daten durch bestimmte Geräte – nicht mehr funktioniert. Laufen nun solche Verwaltungslösungen für Geräte in einem Rechenzentrum, kommt es immer wieder vor, dass die IT-Abteilung Änderungen erst beim Einspielen von Service Releases, üblicherweise einmal monatlich, bemerkt. Microsoft kündigt zwar Breaking Changes rechtzeitig an, also Änderungen am Code, die eine Client-Anwendung zu Fall bringen können, es bleibt aber diese Abhängigkeit der Drittanbieter, ihre Schnittstellen ständig anpassen zu müssen. Gelingt trotzdem beispielsweise mit einem iPhone, das in einem Drittsystem verwaltet wird, der Zugriff auf einen Service in Microsoft 365 nicht, so ist der Kunde der Leidtragende. An welchen Support soll er sich nun wenden – an Microsoft, Apple oder den Hersteller der MDM-Lösung? Nicht zu unterschätzen ist auch das Thema Know-how der Informatik-Abteilung: Je mehr verschiedene Hersteller in einer Umgebung vertreten sind, desto mehr Wissen muss bei der IT aufrechterhalten werden.

Wieviel Microsoft darf es sein?

Selbstverständlich ist die Ausgangslage für die Diskussion, wo Geräte und Apps verwaltet werden, in jedem Unternehmen eine andere. So macht es unter Umständen keinen Sinn, auf Microsoft Endpoint Manager zu setzen, wenn mit der bestehenden Lösung die Sicherheitsanforderungen gut erfüllt werden können und vor allem dann nicht, wenn der Grossteil der Daten und Services in einem Rechenzentrum oder in einer anderen als der Microsoft Cloud gehostet wird. Solange ein Unternehmen mehrere verteilte Systeme verwendet, braucht es eben auch die eingangs erwähnten Lösungen Dritter. Diese sind eben aufgrund ihrer Interoperabilität mit anderen Systemen exakt dazu da, auf unterschiedliche Umgebungen zugreifen zu können. Solche Lösungen laufen dann üblicherweise on Premises oder in Private Clouds. Wenn nun aber nach und nach Apps in die Cloud verschoben werden und ein Unternehmen mittel- oder langfristig auf die Microsoft Cloud setzt, ist irgendwann der Wendepunkt erreicht, an dem ein Wechsel angezeigt ist. Ein solcher ist auch in Erwägung zu ziehen, wenn Apps und Geräte in der Cloud verwaltet werden, aber weiterhin mobil auf Daten oder Fachanwendungen im Rechenzentrum zugegriffen werden muss. Dazu gibt es neben der «Notlösung» einer herkömmlichen, direkten VPN-Verbindung (Virtual Private Network) ins Rechenzentrum mit Azure AD Application Proxy, einer Funktionalität des Identitäts- und Zugriffsverwaltungsdienstes Azure AD, oder mit Tunnel for Intune ebenfalls Lösungen aus der Cloud des Hauses Microsoft. ■

DER AUTOR

Jonas Hofer ist Mobile Security Consultant bei Nomasis, einem Service-Anbieter für mobile, sichere IT-Arbeitsplätze. Als Spezialist in der Umsetzung von mobilen IT-Infrastrukturen betreut Nomasis über 200 aktive Kunden aus der Finanz- und Versicherungsbranche, den öffentlichen Diensten, Industrie, Gesundheitswesen, Handel und Bildung.