Modernes Endpoint Management mit Microsoft 365

Know-how Die Pflege der internen Windows Clients ist zentral für die Sicherheit, für den reibungslosen Betrieb und für die Zufriedenheit der Mitarbeiter. Doch wie sieht die optimale Verwaltung von Endpoints im Unternehmen aus?

Von Thomas Kurth

INHALT

Modernes Endpoint Management mit Microsoft 365	36
Ins Home Office – dank Cloud-only Strategie	40
Virtualisierter Arbeitsplatz: Jetzt erst recht im Trend	43
Fallbeispiel: Im Schnelltempo ins Home Office	45
Marktübersicht: VDI-Angebote aus der Schweizer Cloud	48

Endpoint Management ist ein Teilgebiet der Informatik und bildet mit den Endgeräten die Schnittstelle zwischen den Endbenutzern und allen IT Services. Wenn das Endgerät nicht korrekt konfiguriert ist oder Fehler aufweist, dann sind sofort alle Services betroffen. Im Grundsatz beinhaltet das Endpoint Management die zentrale Verwaltung der Betriebssysteme, Bereitstellung von Applikationen und Updates, die Inventarisierung, Konfiguration und Überwachung der Sicherheitsfunktionen. Als Erweiterung sind auch Asset Management sowie Hardware und Software Lifecycle Management wichtige Komponenten.

Evolution zum Modern Workplace

Noch vor über 10 Jahren war beim Thema Endpoint Management die Strategie klar: Es wurde mit allen Mitteln versucht, alles zu standardisieren und die Endbenutzer so einzuschränken, dass Sie nur noch genau ihre Arbeit erledigen konnten. Dies hat sich mit den ersten Handhelds und Smartphones und anderen Bring-Your-Own-Geräten verändert, die Informatik musste reagieren. Dabei wurde festgestellt, dass ein einfaches Blockieren neuer Technologien nur zu Umgehungslösungen von Seiten der Endbenutzer führt. Dasselbe erkennen wir heute mit der Nutzung von Cloud Apps: Obwohl diese in einem Unternehmen verboten sind (z.B. Dropbox), nutzen die Mitarbeiter sie trotzdem. Mit dem Modern Workplace wird versucht, weniger Einschränkungen zu definieren und den Benutzern mehr Freiheiten zu geben, aber dafür klare Sicherheitsrichtlinien zu definieren und diese über alle Zugriffsmöglichkeiten durchzusetzen. Für Android sollen dieselben Regeln gelten wie für Windows und iOS oder wenn der Zugriff über einen Browser aus einem Internetkaffee getätigt wird.

Sicherheitsanforderungen rücken den Endpoint in das Zentrum

Dadurch, dass Hacker-Angriffe und Malware vermehrt den Endbenutzer und nicht mehr die Netzwerk-Firewall angreifen, haben sich die Sicherheitsmassnahmen stark verändert. Insbesondere die Wichtigkeit und Frequenz der Bereitstellung von Updates für die Betriebssysteme, Treiber, Firmware und Applikationen erfordern automatisierte Prozesse. Mit Cloud-Intelligenz kann dies effizienter, einfacher und mit tieferem Risiko gelöst werden. Die Hersteller haben zudem den Support Lifecycle drastisch gekürzt und forcieren so Kunden, die Systeme zu aktualisieren. Erfreulich ist ebenfalls zu sehen, dass die Kompatibilität der Applikationen sich in den letzten Jahren stark verbessert hat und die meisten Middle-Applikationen wie Adobe Reader, Java oder Browser problemlos im Betrieb aktualisiert werden können.

Gesteigertes IT-Grundwissen der Mitarbeiter

Doch es haben sich nicht nur die technischen Gegebenheiten verändert, auch die Endbenutzer sind technikaffiner geworden, dadurch sind mehr Prozesse, wie zum Beispiel Password Reset oder Windows Autopilot, als Self-Service implementiert, um die Helpdesk-Organisationen zu entlasten. Ausserdem sind durch diese Affinität auch die Erwartungen an den Arbeitsplatz gestiegen.

Microsoft bietet unterschiedlichste Abonnemente für Unternehmen an, welche auf den ersten Blick kompliziert wirken. Dies ist vor allem die Herausforderung, wenn man am Beginn eines Projektes steht und erste einzelne Services nutzen möchte. Sobald mehrere Bestandteile genutzt werden, erhält man durch Microsoft 365 viele Vorteile, indem viele Funktionalitäten mitlizenziert sind. Wir erkennen den Trend, dass viele Unternehmen in den letzten Jahren von Office 365 und Enterprise Mobility und Security (EMS) auf die Unternehmenslizenz M365 E3 gewechselt haben. Microsoft 365 vereinfacht die Lizenzierung, da Grundlizenzen, wie zum Beispiel Intune, Windows 10 und auch Office, bereits enthalten und dadurch direkt nutzbar sind. Mit diesem Basis-Package sind die meisten Unternehmen bestens bedient und es bietet trotzdem die Möglichkeit, entweder spezifisch die Sicherheits- (M365 E5 Security) oder Compliance- (M365 E5 Compliance) Features oder die komplette E5-Variante bei Bedarf zu abonnieren.

MICROSOFT 365 LIZENZIERUNG

	M365 Business Premium Fr. 19.70	M365 F3 Fr. 9.80	M365 E3 Fr. 36.70	M365 E5 Fr. 62.70
Office 365	Office 365 Business Premium	Office 365 F3	Office 365 E3	Office 365 E5
Windows	Windows 10 Pro	Windows 10 Enterprise E3 (eingeschränkt)	Windows 10 Enterprise E3 pro User (inkl. VDA)	Windows 10 Enterprise E5 pro User (inkl. VDA)
Enterprise Mobility & Security	EMS SMB	EMS F1	EMS E3	EMS E5

Funktionen können je nach Bundle variieren, Details entnehmen Sie der Microsoft Homepage und Verträgen. Preise gemäss Homepage Microsoft Stand 28.5.2020.

■ einzeln erhältlich
□ nicht einzeln erhältlich

Quelle: Microsoft

Die Microsoft-Angebote für Unternehmen bieten verschiedene Konfigurationsmöglichkeiten.

Die initial höheren Kosten der Bundles können bei der Return-on-Investment-Kalkulation meist einfach begründet werden. Dies geschieht am einfachsten, indem bereits vorhandene Infrastrukturlösungen ebenfalls aus der Microsoft Cloud bezogen werden. Zum Beispiel können Microsoft-365-Kunden mit Intune bestehende MDM/MAM-Systeme ersetzen oder mit Azure AD Conditional Access MFA Lösungen optimieren und so andere Lizenzkosten reduzieren.

Microsoft Endpoint Manager

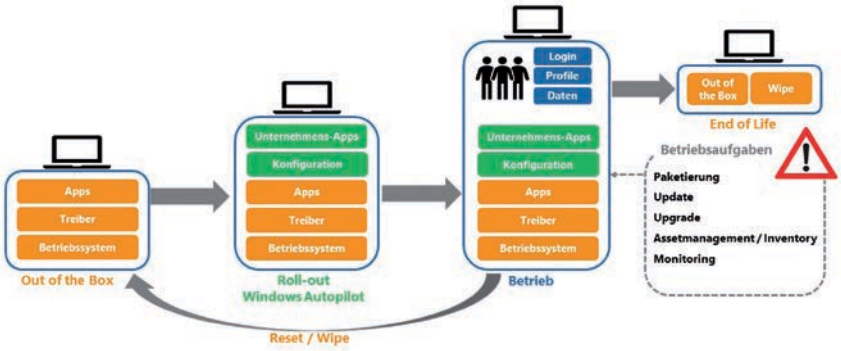
Microsoft hat im letzten Herbst die Produkte für Endpoint Management neu organisiert und unter dem Brand Microsoft Endpoint Manager (MEM) zusammengeführt. Dafür wurde auch ein eigens angepasstes Azure-Portal entwickelt, welches die relevanten Tools auf einer Oberfläche zusammenfasst. Die einzel-

nen Produkte sind so zusammen verbunden, dass Kunden selbst auswählen können, welche Funktionalität sie beispielsweise aus der Cloud oder On-Premises verwenden wollen. Zudem vereinfachen Szenario-basierte Konfigurationsassistenten den Einstieg, im Speziellen für KMU.

Microsoft Endpoint Configuration Manager

Die wichtigste Ankündigung war die Loslösung des Configuration Manager (MEMCM früher SCCM) aus der System-Center-Produktfamilie. Verstärkt wurde dies durch die offizielle Aussage, es handle sich dabei um ein Zeichen, dass dieses Produkt strategisch weiterentwickelt wird und nicht wie von einigen Quellen behauptet als Produkt auf dem Abstellgleis anzusehen ist. Schliesslich ist es auch eines der wenigen On-Premise-Produkte, das drei Mal pro Jahr erfolgreich ein neues Release Update mit vielen neuen Funktionalitäten bereitstellt. So bietet etwa die Funktionalität Cloud Management Gateway eine einfache Möglichkeit, Geräte ausserhalb des Unternehmens zu verwalten, was in der aktuellen Situation mit viel Home Office sehr nützlich ist.

CLIENT-LIFECYCLE VON WINDOWS-GERÄTEN



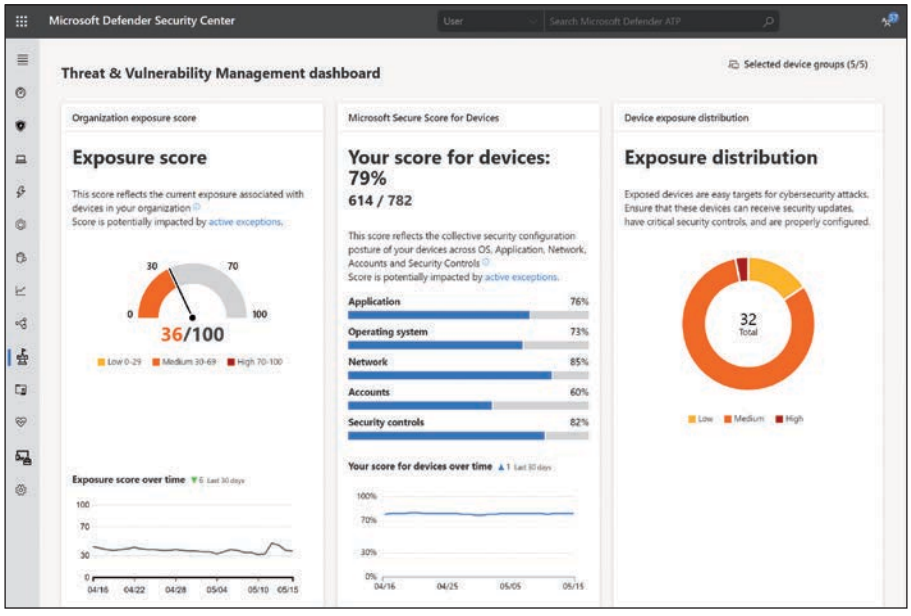
Windows Autopilot erlaubt im Client Lifecycle Management von Windows-Geräten das Zurücksetzen (Reset & Wipe) der Endpoints auf den Ursprungszustand (Out of the Box). Quelle: Basevision

Mobile Devices mit Microsoft Intune verwalten

Zu MEM gehört auch Microsoft Intune, welches sich in den letzten Jahren zu einem top Mobile-Device-Management-System entwickelt hat. Wir beobachten schon seit längerem, dass immer mehr Unternehmen durch die Lizenzsituation und auch durch diese Entwicklung von Drittanbieterprodukten Richtung Microsoft Intune wechseln und dadurch vom ganzen Microsoft-Cloud-Ökosystem profitieren können. Microsoft Intune eignet sich nicht nur für KMU, sondern auch für Grossunternehmen bestens, um Windows-, Android- und iOS-Geräte zu verwalten. Sofern ein Unternehmen bereits den Configuration Manager nutzt und dies auch weiterhin möchte, ist auch dies möglich. Durch den sogenannten Co-Management Mode können beide Verwaltungstools parallel genutzt werden, und mittels Schieberegler lässt sich pro Workload definieren, welches System diesen steuert. So kann zum Beispiel die Applikationsverteilung noch mit dem Configuration Manager gesteuert werden, aber Windows Updates bereits mit Intune.

Datengestützte Empfehlungen für Rollouts mit Desktop Analytics

Mit Desktop Analytics nutzt Microsoft die Cloud-Intelligenz, um Applikationsinkompatibilitäten und Testabläufe für die schnellen Update-Zyklen zu verbessern. Bisher wurden Testgeräte zufällig oder darauf basierend, dass Sie einem IT-Mitarbeiter zugeordnet sind, ausgewählt. Doch dies führt zu schlechten Testergebnissen, da diese Nutzergruppen meist nicht die wichtigsten Business-Applikationen verwenden. Desktop Analytics unterbreitet Vorschläge, um eine Testgruppe mit einer möglichst hohen Abdeckung von Applikationen und Treibern zu erstellen.



Das Microsoft Defender Security Center gibt Informationen zum Security-Status der Geräte aus und erlaubt feingliedrige Konfiguration der Sicherheitsmassnahmen.

Vereinfachte Bereitstellung von neuen Geräten

Das Bereitstellen von neuen Geräten, früher oft mit Images, benötigt viel Aufwand, um die korrekten Treiber und Konfigurationen für die jeweilige Gerätemodelle bereitzustellen. Windows Autopilot ermöglicht, diesen Schritt zu optimieren und das vom Hersteller konfigurierte Betriebssystem direkt ins Unternehmensnetzwerk einzubinden. Dadurch vereinfacht sich der Rollout, sodass ein Benutzer selbst ein Gerät in Betrieb nehmen oder zurücksetzen kann. Wichtig ist hierbei, dass die Geräte nur mit Windows, den Treibern und ohne spe-

KEY TAKE-AWAYS:

- Das beste von der Cloud und On-Premise kombiniert mit Microsoft Endpoint Manager.
- Self-Service anbieten.
- Automatisierung nutzen, um repetitive Betriebstätigkeiten zu vereinfachen.
- Anwendungsaktualisierungen planen und regelmässig durchführen.
- Treiber und Firmware proaktiv aktualisieren und konfigurieren.

zielle Zusatzapplikation (Trials, Spiele) bestellt werden. Microsoft nennt diese Bereitstellung Signature Edition, leider sind die Hersteller sehr unterschiedlich in deren Handhabung. Der Endbenutzer kann während dem Enrollment spezifische Einstellungen wie die Sprache oder das Tastaturlayout auswählen. Im Hintergrund werden unternehmensspezifische Konfigurationen angewendet, Anwendungen installiert und dem Unternehmensnetzwerk beigetreten. Am Ende ist das Gerät bereit für den Benutzer. Oft stellt sich die Frage, ob dies denn ein Endbenutzer kann. Klar kommt dies auf die Benutzer an, aber im Grossen und Ganzen können 90 Prozent von ihnen ihren Heimcomputer selbst in Betrieb nehmen, und daher funktioniert dies mit Windows Autopilot sehr gut.

Sobald sich der Benutzer anmeldet, werden spezifische Konfigurationen wie das Benutzerprofil angewendet, zudem kann der Benutzer nun Applikationen aus dem Applikationskatalog installieren. Ab diesem Zeitpunkt befindet sich das Gerät im produktiven Betrieb und die Workplace-Management-Aufgaben, wie die Inventarisierung und das Aktualisieren der unterschiedlichen Komponenten, beginnen.

Update- und Vulnerability Management

Die Anwendungsaktualisierung wurde durch die Möglichkeit, Update-Kataloge von Drittherstellern in MEMCM einzubinden, stark vereinfacht. Dadurch können zum Beispiel mit Patchmypc.com über 150 Anwendungen ohne Paketieraufwände automatisch aktualisiert werden. Dies reduziert die Aufwände für die Aufgabe drastisch. Insbesondere, da viele Middleware-Anwendungen mehrmals jährlich oder sogar monatlich Sicherheitslücken beheben, helfen die Update-Kataloge, sich von einer reaktiven Anwendungsaktualisierung in eine proaktive zu entwickeln. Interessant ist hier ebenfalls, dass Microsoft mit Microsoft Defender Advanced Threat Protection (MDATP) eine Vulnarability-Management-Lösung anbietet, die hilft, diese Prozesse zu überwachen. Dabei wird sofort aufgezeigt, für welche im Unternehmen eingesetzte Software bekannte Sicherheitslücken vorhanden sind.

Doch nicht nur die Anwendungen müssen aktualisiert werden, auch die Treiber und das Betriebssystem müssen regelmässig auf den neuesten Stand gebracht werden, um vor Sicherheitslücken zu schützen – aber auch, um von Geschwindigkeits- und Stabilitätsoptimierungen zu profitieren. Hier bietet Windows Update for Business bereits viele Treiber-Aktualisierungen über denselben Kanal wie die Windows Updates an. Dies kann etwa ein Grund sein, um diesen Workload von MEMCM nach Intune zu verschieben. Wenn aber mehr Kontrolle und Übersicht über diese Aktualisierungsprozesse gewünscht ist, wäre nach wie vor eine MEMCM-Integration die bessere Lösung.

Vereinfachtes Konfigurationsmanagement aus der Cloud

Mit Microsoft Intune besteht die Möglichkeit, spezielle Konfigurationen, aber auch die Sicherheitskomponenten zu verwalten. So ist es möglich, die Microsoft Security Baselines sehr einfach auf den Geräten bereitzustellen und zu aktualisieren. Diese Baselines helfen vielen Unternehmen, eine Grundsicherheit ohne hohen Rechercheaufwand und Vorkenntnisse zu erreichen. Zudem sind gegenüber den traditionellen GPOs auch Auswertungen möglich, ob die Einstellungen korrekt gesetzt wurden, und Abweichungen lassen sich erkennen. Dieser Feedback-Kanal für Einstellungen ist besonders wichtig, um durch Angreifer durchgeführte Manipulationen frühzeitig wahrzunehmen und Gegenmassnahmen einzuleiten.

Eingebaute Sicherheitsfunktionen nutzen und Upgrade-Prozesse vereinfachen

Um die schnellen Update-Zyklen des Betriebssystems mit möglichst wenig Abhängigkeiten ohne Probleme durchführen zu können, empfiehlt es sich möglichst, die Bordmittel zu verwenden und wenige bis keine Drittanbieter-Applikationen, die tief ins Betriebssystem eingreifen. Deshalb sollte man in Projekten Windows Defender und Microsoft Defender Advanced Threat Protection (MDATP) einsetzen, eine der neuesten Cyber-Abwehr-Technologien von Microsoft. Der Vorteil in Bezug auf Endpoint Management ist, dass beide Produkte fest ins Betriebssystem integriert und daher auch von Microsoft für das Upgrade getestet sind. Zudem integrieren sie sich in das zentrale Microsoft Threat Protection Backend, was es ermöglicht, mit anderen Microsoft-Sicherheitsprodukten Daten auszutauschen. Zu den Kernfunktionen gehören die Überwachung, verhaltensbasierte Bedrohungs- und Schadsoftware-Erkennung, automatische Wiederherstellung sowie die Erkennung von Sicherheits- und Konfigurationsproblemen in Echtzeit.

Fazit

Die Anforderungen der Benutzer an die Geräte und Applikationen, mit denen sie arbeiten wollen, haben sich in den letzten Jahren massiv verändert. Mit Microsoft 365 stellt Microsoft eine Produktpalette bereit, welche nicht nur Produktivitäts-Tools wie Office 365, Teams und PowerBI beinhaltet. Mit der Enterprise-Mobility-und-Security-Suite und Windows 10 kann Endpoint Management für einfache bis sehr komplexe und von traditionell On-Premise- bis Cloud-Only-Umgebungen optimal gelöst werden. Durch das Baukastensystem lassen sich genau die Funktionalitäten aktivieren, die dem eigenen Unternehmen und den Benutzern Vorteile bieten, um den Betrieb zu optimieren und den veränderten Anforderungen gerecht zu werden. ■

DER AUTOR

Thomas Kurth ist Mitgründer von Basevision und berät Kunden seit über zehn Jahren beim Umsetzen von Endpoint-Management-Projekten mit Microsoft-Technologien. Er teilt sein Wissen in Blogs, Referaten und Trainings und wurde dafür als Microsoft MVP ausgezeichnet.