Clientmanagement 2020

Auf zu neuen Ufern

von Martin Kuppinger

Der großen Diversifizierung der Clients im Unternehmen folgt der Wandel im Marktsegment Clientmanagement. Wo es früher lediglich galt, stationäre Windows-Maschinen zu administrieren, wartet heute auf den IT-Verantwortlichen ein Zoo aus PCs, Laptops, Smartphones und Tablets. Die Anbieter sind mit Begriffen wie Unified Endpoint Management und Workspace Management schnell bei der Hand, doch IT-Abteilungen sollten genau prüfen, welches Clientmanagement im Jahr 2020 und darüber hinaus zum eigenen IT-Betrieb passt.

Bei der Frage danach, wie das Clientmanagement in 2020 und den Folgejahren aussehen muss, stehen zwei Aspekte im Vordergrund. Der erste betrifft die Clients selbst und die Frage, welche zum Einsatz kommen und wie die Erwartungen von Anwendern an ihre Arbeitsumgebung aussehen. Die Nutzererwartungen an die Geräte, Betriebssysteme und die Einsatzart haben sich in den letzten Jahren und Jahrzehnten erheblich verändert. Der zweite Aspekt betrifft die Sicherheit und beleuchtet, wie sich sichere Arbeitsumgebungen in einer Zeit ständig wachsender Bedrohungen bereitstellen lassen. Dazu gehört auch die Fähigkeit, Geräte nach erfolgten Angriffen schnell wiederherstellen zu können, um Ausfallzeiten zu minimieren.

Neben diesen grundlegenden Einflussfaktoren gibt es aber auch weitere, die bei der Entscheidung darüber zu beachten sind, wie das Clientmanagement zukünftig gestaltet wird. Dazu zählen die veränderte Anwendungsbereitstellung, Clientmanagement aus der Cloud, die Integration mit ITSM-Lösungen (IT-Service-Management) sowie die unterschiedlichen Konzepte einerseits für das Management von Clients und andererseits für die Bereitstellung von virtuellen Arbeitsumgebungen, also den Digital Workspaces.

Ein Management für alle Clients

Ein Trend der letzten Jahre hat sich inzwischen etabliert: Heutzutage ist die Trennung zwischen klassischem, meist auf Windows ausgerichtetem Clientmanagement und der Verwaltung mobiler Endgeräte (EMM; Enterprise Mobility Management) eher die Ausnahme als die Regel. Die meisten der führenden Anbieter setzen auf "Unified Endpoint Management" (UEM), also auf Werkzeuge, mit denen sich alle Arten von Endgeräten verwalten lassen, von Windows-Desktops bis hin zu mobilen Endgeräten mit Android als Betriebssystem.

Auch das Patchmanagement, das vor einigen Jahren häufig noch eine separate Produktkategorie war, ist in dem heute benötigten Umfang typischerweise Teil von UEM. Es gibt zwar weiterhin spezialisierte Tools, ebenso wie es Patchmanagement auch in Endpoint-Security-Produkten gibt, die meisten UEM-Produkte liefern heute aber auch Patchmanagement als Funktionalität.

Die Funktionsbreite solcher Angebote geht damit inzwischen weit über das klassische Clientmanagement hinaus. Sie umfasst das Bereitstellen von konfigurierten Arbeitsumgebungen für die Mitarbeiter, die Inventarisierung, die Verwaltung von Betriebssystem und Anwendungen einschließlich des Sicherheitsmanagements, aber auch das Verwalten von Inhalten auf Endgeräten beispielsweise mit der Trennung von persönlichen und geschäftlichen Apps und Daten. Diese Funktionen müssen dabei die gesamte Bandbreite von typischen Clientbetriebssystemen sowohl für traditionelle als auch mobile Endgeräte abdecken, also zumindest die Unterstützung von Windows, iOS, macOS und Android – wobei einige Hersteller auch Linux-Clients verwalten können.

Ständige Veränderungen im Benutzerverhalten

Die Entwicklung hin zu UEM reflektiert auch das veränderte Nutzungsverhalten bei Endgeräten. Es ergibt es wenig Sinn, das Management von traditionellen und mobilen Endgeräten getrennt zu betreiben – weder vom administrativen Aufwand her noch von der Umsetzung einheitlicher Richtlinien über alle Geräte hinweg. Viele Anwendungen, angefangen bei Microsoft Office, werden heute – je nach Nutzungssituation – auf mehreren Endgeräten parallel genutzt.

Dass Mitarbeiter mehr als ein Endgerät haben und nutzen, ist dabei inzwischen eher die Regel als die Ausnahme. Ein Notebook und ein Smartphone sind in vielen Unternehmen heute die Basisausstattung für Mitarbeiter zumindest in den Verwaltungsbereichen. Aber selbst dort, wo viele Mitarbeiter nur einen klassischen Desktop-PC haben, gibt es in der Regel Nutzergruppen, die mobile Endgeräte nutzen. Gerade auf höheren Hierarchieebenen nimmt die Zahl der Geräte dabei oft zu, weil beispielsweise auch noch mit einem Tablet gearbeitet wird. Bei Mitarbeitern im Außendienst sind mindestens zwei Geräte, also Notebook und Smartphone, heute ebenfalls der Regelfall.

Hinzu kommt, dass es längst keine Einheitlichkeit bei den zu verwaltenden Geräten gibt. Die Zeiten, als IT-Verantwortliche alle Mitarbeiter, die mobil kommunizieren mussten, mit einem Blackberry ausrüsten konnten, sind längst vorbei. Es gilt, eine Balance zu finden zwischen einheitlichen Vorgaben und zentralem Management von Geräten auf der einen Seite und der Forderung gerade auch von jungen Mitarbeitern nach einer Arbeitsumgebung, die ihrem privaten Nutzungsverhalten von Geräten sowohl bezüglich Gerätetyp als auch Betriebssystem entspricht. Dies erfordert Lösungen für das Clientmanagement, die in der Lage sind, mit einer zunehmenden Heterogenität der Clients umzugehen.

Ob und in welchem Umfang und für welche Benutzergruppen eine größere Individualität der Clients zumindest bezüglich Gerätetyp und Betriebssystem zugelassen wird, ist dann eine Frage, deren Beantwortung von vielen Faktoren abhängt. Klar ist aber, dass modernes Clientmanagement die Flexibilität besitzen muss, um die unterschiedlichen und sich verändernden Anforderungen des Business, der IT-Sicherheit und der Nutzer zu unterstützen.

Zero Trust Security und mobile Nutzer

Diese Entwicklungen reflektieren die generelle Veränderung der IT-Nutzung. Der mobile Zugriff auf E-Mail und andere Daten ist heute in vielen Unternehmen der Regelfall. Arbeiten von unterwegs oder aus dem Home Office ist ebenfalls in vielen Organisationen längst zum Normalfall geworden und muss unterstützt werden.

Diese Entwicklung verläuft parallel zur Bereitstellung von Diensten aus der Cloud. Ein erheblicher Teil von Unternehmen nutzt inzwischen Office-Dienste aus der Cloud wie Microsoft Office 365 oder Google Docs. Damit gibt es aber auch nicht mehr den zentralen Perimeter um das unternehmensinterne Netzwerk, innerhalb dessen sich alle wichtigen Server, Anwendungen und Clients befinden.

In den letzten Jahren hat daher das Konzept der "Zero Trust Security" immer mehr an Bedeutung gewonnen. Dieser geht nicht mehr davon aus, dass einzelne, zentrale Komponenten wie eine Firewall einen sicheren Schutz bieten, sondern davon, dass jedes einzelne Element kompromittiert sein kann und eine einzelne Sicherheitslösung nicht ausreicht.

Ein Baustein in Zero-Trust-Security-Konzepten ist das Clientmanagement. Der Client muss geschützt sein, gleichzeitig muss der IT-Verantwortliche aber auch davon ausgehen, dass er erfolgreich angegriffen werden kann. Daher gilt es, Clients zentral zu verwalten – über alle Arten von Clients und Nutzungssituationen hinweg. Auch das ist einer der Gründe dafür, dass sich UEM immer mehr durchsetzt, wobei die Funktionalität eben nicht mehr nur das technischen Management von Clients und Anwendungen umfasst, sondern auch das Endpoint-Security-Management.

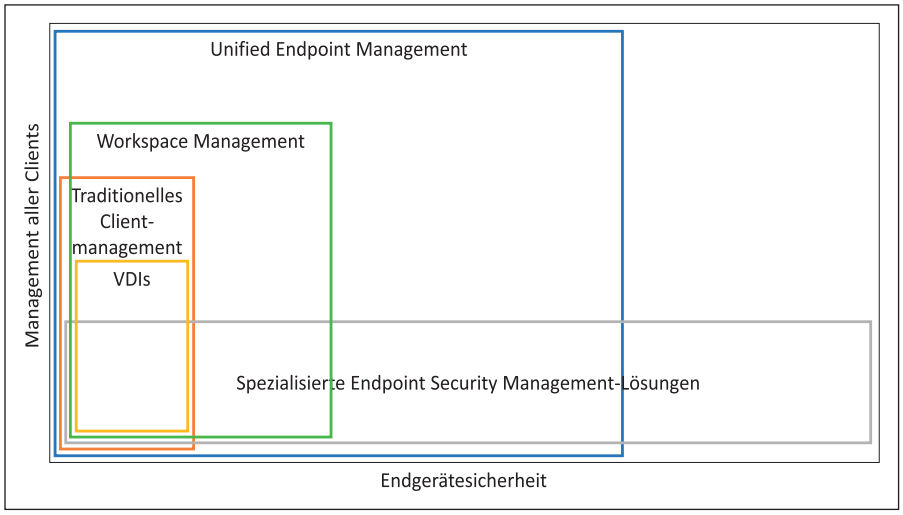
Je nach Art des Unternehmens und Nutzung der IT kann dem UEM dabei eine herausgehobene Bedeutung für die Sicherheit zukommen. Dort, wo Anwendungen nur noch aus der Cloud bezogen werden und Nutzer überwiegend mobil sind, spielt Netzwerksicherheit nur noch eine untergeordnete Rolle. Die Absicherung der Clouddienste, die starke Authentifizierung von Nutzern und eben die sichere Verwaltung von Clients über UEM sind in solchen Nutzungsszenarien die wesentlichen Bausteine für Zero Trust Security.

Schnelle Wiederherstellung als Kernaufgabe

Die unzähligen Berichte über erfolgreiche Angriffe auf Unternehmen in den vergangenen Jahren haben deutlich gemacht, dass es keine absolute Sicherheit gibt. Wir müssen heute in der IT davon ausgehen, dass früher oder später ein erfolgreicher Angriff erfolgt. Je nach Angriffsvektor und -ziel können dabei auch Clients betroffen sein.

Sowohl Ransomware als auch Trojaner und andere Angriffsformen können dabei zu Situationen führen, in denen sich Clients nicht mehr nutzen lassen und der Admin sie neu aufsetzen muss. Die Wiederherstellung der Arbeitsfähigkeit, das Disaster Recovery als Teil des Business-Continuity-Managements, wird zu einer unverzichtbaren Fähigkeit der IT. Sind erfolgreichen Angriffen fast unausweichlich, ist die Fähigkeit zur schnellen Beseitigung der Schäden essenziell.

Clientmanagement muss genau das unterstützen, also nicht mehr nur eine geplante Bereitstellung neuer Clients in definierten Prozessen und das kontinuierliche Management dieser Systeme, sondern auch die Wiederherstellung großer Mengen an Clientsystemen in kurzer Zeit in einem definierten, "sauberen" Zustand – und das möglichst ohne Verlust an Daten. Letzteres hat natürlich nicht nur mit dem Clientmanagement zu tun, sondern insbesondere auch mit den Vorgaben für die Speicherung von Daten und deren Umsetzung.



Die Funktionen von traditionellem Clientmanagement, Endpoint-Security, Workspace-Management, VDI und Unified Endpoint Management überschneiden sich.

Grundsätzlich sollten Daten möglichst nicht lokal liegen, damit sie bei Angriffen nicht verloren gehen.

Anwendungen und Patches aus der Cloud

Eine weitere Entwicklung, die Einfluss darauf hat, wie sich das Clientmanagement gestaltet, sind die eingesetzten Anwendungen. Organisationen, die beispielsweise noch mit Microsoft Office in klassischer Weise arbeiten, haben völlig andere Anforderungen als solche, die Office 365 nutzen und Microsoft die Clientanwendungen und -apps nach der erstmaligen Installation regelmäßig und automatisch aktualisiert.

Grundsätzlich ist dabei zunächst die Frage zu beantworten, ob Sie solche automatischen Aktualisierungen – wie sie bei Apps auf Smartphones ja ohnehin der Normalfall sind – nutzen möchten oder nicht. In den meisten Unternehmen, die auf diese Funktionen zurückgreifen, wird diese Frage aus der positiven Erfahrung bejaht. Es gibt keine aufwändigen Migrationsprozesse zu neuen Office-Versionen mehr, sondern viele kleine Änderungen, die automatisch verteilt werden, aber keine langwierige Planung, Migration oder Trainingsprogramme für die Nutzer erfordern. Damit entfallen aber wesentliche Aufgaben des Clientmanagements.

Ein ähnliches Bild gibt es beim Patchmanagement für Betriebssysteme und Anwendungen. Diese sind für viele Anwendungen wie eben Office 365 und generell für Apps heute ohnehin Teil der laufenden Aktualisierung.

Für Betriebssystempatches gibt es von allen Anbietern heute die Option für eine automatische Aktualisierung, wenn auch in unterschiedlicher Umsetzung. Während Microsoft in definierten Intervallen Sicherheitspatches bereitstellt, die das System automatisch verteilt, sind diese beispielsweise für iOS unregelmäßiger und an generelle Aktualisierungen des Betriebssystems gekoppelt.

In fast allen Nutzungsszenarien gilt es heute aber, die automatischen Aktualisierungen zu verwenden. Die Abwägung zwischen Risiken für die Verfügbarkeit und Funktion von Systemen durch die automatisierte Installation von Patches und den Risiken durch Angriffe fällt heute in den meisten Szenarien eindeutig zugunsten automatischer Patches aus. Die Probleme dadurch sind bei den großen Anbietern inzwischen sehr gering, während die Risiken durch Sicherheitslücken sehr hoch sind, weil sich solche Lücken automatisiert und unmittelbar von Angreifern ausnutzen lassen.

Damit müssen UEM-Suites aber zunehmend nur noch in Ausnahmefällen diese Aufgaben übernehmen. Für viele Systeme, auf denen im Wesentlichen Microsoft Office 365 läuft oder die mit Google Docs ohnehin nur auf cloudbasierende Dienste zugreifen, ist das Management von Anwendungsaktualisierungen und von Betriebssystempatches inzwischen zur Standardfunktion geworden, die nicht mehr das Clientmanagement leisten muss.

Rolle der Clientvirtualisierung

Bei der Frage nach dem zukünftigen Clientmanagement in einer Organisation sollten Sie sich auch damit beschäftigen, ob und in welchem Umfang virtuelle Clientumgebungen eine Rolle spielen sollen. Während klassische UEM-Werkzeuge auf die Verwaltung von lokalen Geräten vom Desktop-PC bis zum Smartphone ausgelegt sind, gibt es auf der anderen Seite die Desktopvirtualisierung oder Virtual Desktop Infrastructure (VDI), die virtuelle Arbeitsumgebungen entweder aus lokalen Rechenzentren oder aus der Cloud bereitstellt. Der Zugriff der Nutzer erfolgt dann remote auf die zentral verwalteten Arbeitsumgebungen. Allerdings lassen sich damit nicht alle Anwendungsumgebungen virtualisieren – der Fokus liegt auf Windows-Systemen.

Die Grenze zwischen UEM und VDI verläuft zunehmend fließend. Anbieter von "Digital Workspaces" kombinieren beide Bereiche, um einerseits virtuelle Desktops zu liefern, andererseits aber auch das Management anderer Systeme in einer integrierten Software abzudecken. Aus Kundensicht ist zu überlegen, ob es den Bedarf für solche virtualisierten Umgebungen gibt.

Die einfache und schnelle Bereitstellung von Clients bietet beispielsweise deutliche Vorteile, wenn es um die Wiederherstellung nach Angriffen geht. Auch für Remotezugriffe beispielsweise aus dem Home Office oder von externen Mitarbeitern können solche Umgebungen signifikante Vorteile bieten. Auf der anderen Seite gibt es über die Cloud inzwischen auch Ansätze für solche Nutzungsformen. Zudem sind VDIs auch limitiert, wenn es um eine breite Unterstützung unterschiedlicher Gerätetypen und Betriebssysteme geht.

Clientmanagement aus der Cloud

Ein weiterer wichtiger Aspekt ist schließlich noch die Frage, in welcher Form die

Organisation das Clientmanagement betrieben möchte. Inzwischen gibt es immer mehr reines Cloud-UEM und viele Anbieter in diesem Markt haben zudem Angebote, die diese Produkte auch als Service bereitstellen. Die Entscheidung über das geeignete Bereitstellungsmodell hängt in hohem Maße von der Cloudstrategie im Unternehmen ab. Wenn es bereits eine grundsätzliche "Cloud First"-Entscheidung gibt, spricht sehr viel dafür, auch UEM als Dienst aus dem Internet zu beziehen.

In Organisationen, die auch für die nächsten Jahre mit eher traditionellen Bereitstellungsmodellen und Nutzungsformen für Clients arbeiten, kommt dagegen auch ein lokal betriebenes UEM weiterhin in Betracht. Allerdings zeigt sich im Markt inzwischen deutlich, dass viele Unternehmen, die noch vor wenigen Jahren den Schritt in die Cloud sehr zurückhaltend betrachtet oder sogar weitgehend ausgeschlossen haben, umgeschwenkt sind und konsequent Cloud First verfolgen.

Daher sollten Sie auch bei einer Entscheidung für ein intern betriebenes UEM in jedem Fall prüfen, wie von dort in den kommenden Jahren ein Übergang zu einem cloudbasierten Betriebsmodell erfolgen kann.

Abschätzung notwendiger Zusatzfunktionen

Neben den Kernfunktionen von UEM liefern einige Anbieter noch zusätzliche Features. Dazu gehören beispielsweise das IT-Asset-Management, das Lizenzmanagement, Vertragsmanagement, Remote-Control-Funktionen, aber auch ITSM. Die Grenzen zwischen den verschiedenen Produktkategorien verlaufen auch hier fließend.

Bei der Entscheidung über den Funktionsumfang einer UEM-Lösung sollten Sie zunächst zwei Aspekte betrachten. Der eine ist die Frage danach, welche Werkzeuge bereits im Unternehmen vorhanden sind und welche Rolle diese in der Zukunft spielen können und sollen. Das Ziel sollte sein, für das IT-Infrastrukturmanagement ebenso wie für die Endgerätesicherheit mit einer definierten, geringen Zahl an Tools auszukommen und funktionale Überschneidungen zu mimieren. Das kann aber auch bedeuten, dass eine umfassende UEM-Software vorhandene Produkte ersetzt und konsolidiert, dies gilt auch im Bereich der Endgerätesicherheit.

Der zweite Aspekt ist die Anforderungsdefinition. Diese sollte einerseits umfassend, andererseits aber auch auf die wirklich wichtigen Funktionen fokussiert sein. Sie muss zudem berücksichtigen, wie sich die IT-Infrastruktur des Unternehmens – beispielsweise durch eine Verschiebung von Diensten in die Cloud – in den kommenden Jahren verändern könnte oder wird. Auf dieser Basis kann dann eine gezielte Auswahl erfolgen.

Grundsätzlich ist es bei der Funktionalität empfehlenswert, den Schwerpunkt auf die Kernfunktionen von UEM zu legen, wie sie in der Tabelle "Kernfunktionen des Unified Endpoint Managements" aufgeführt sind. Ein zu breiter Funktionsumfang birgt das Risiko, dass schlussendlich kein Produkt wirklich alle Bereiche in ausreichendem Umfang abdecken kann.

Fazit

Bei der Auswahl einer UEM-Suite für die nächsten Jahre ist die wichtigste Frage zweifelsohne, wie das IT-Betriebsmodell aussehen soll und welche Freiheitsgrade es bei den Clients für die Anwender geben soll und wird. Davon hängt ab, ob eher ein umfassendes Workspace-Management mit VDI-Funktionalität oder ein reines UEM-Werkzeug für die Verwaltung von lokalen Clientbetriebssystemen – vom Desktop bis hin zum Smartphone – in Frage kommt. Außerdem ergibt sich daraus, in welcher Breite Clientbetriebssysteme wie beispielsweise ChromeOS unterstützt werden müssen und welche Funktionen bei der Auswahlentscheidung das größte Gewicht erhalten.

Vor allem hängt davon aber auch ab, wo die UEM-Software betrieben wird. Die generelle Tendenz ist, dass immer mehr Dienste aus der Cloud bezogen werden. Daher sollten Sie bei allen Entscheidungen, die zu einer eingeschränkten Cloudfähigkeit führen, sehr genau abwägen, ob diese für die Zukunft wirklich passend sind. Die IT hat sich in den letzten Jahren grundlegend verändert und Investitionsentscheidungen für UEM müssen das berücksichtigen, um Geräte und Anwendungen in den heutigen und zukünftigen Nutzungsmodellen verwalten zu können. *(jp)*

Kernfunktionen des Unified Endpoint Managements

Funktionsbereich	Kernfunktion
Clientmanagement	- Identifikation und Onboarding von Endgeräten - Bereitstellung von konfigurierten Endgeräten - Konfigurationsanpassungen - Remotezugriff und -löschung - Inventarisierung
Anwendungsverteilung und -management	- Anwendungsbereitstellung zum Beispiel über einen App Store - Richtlinien zur Anwendungsnutzung und Überwachung - Whitelisting/Blacklisting von Apps und Anwendungen - Konfigurationsanpassungen für Anwendungen
Endpoint-Security	- Authentifizierung und kontextbasierende, adaptive Zugriffssteuerung - Zertifikatsmanagement - Analytische Funktionen zur Risikoidentifikation
Verwaltung von Inhalten und Daten	- Trennung von geschäftlichen und privaten Daten - Verhinderung von Datenlecks - Überwachung des Zugriffs auf sensitive Daten
Betriebssystemunterstützung	- Unterstützung gängiger Betriebssystemplattformen wie Windows, macOS, iOS und Android