Den Spagat zwischen Nutzerkomfort und IT-Sicherheit locker meistern

BYOD ohne MDM

BYOD (Bring Your Own Device) – Mitarbeiter nutzen ihre eigenen mobilen Geräte für geschäftliche Zwecke: Was zunächst nach einem unverhofften Geschenk klingt, ist in Wahrheit eines der größten Sicherheitsrisiken für Unternehmen. Langjährig etablierte Sicherheitsstrukturen werden plötzlich wirkungslos. IT-Verantwortliche kommen deshalb nicht daran vorbei, eine klare BYOD-Strategie zu definieren, Richtlinien zu erlassen und mittels geeigneter Werkzeuge eine sichere Umgebung zu schaffen. Die vermeintliche Freiheit der Benutzer entpuppt sich dabei nicht selten als Einschränkung.

IT-Verantwortlichen in Unternehmen machte schon vor der Konsumerisierung der IT der Mobile-Trend zu schaffen. Um das Sicherheitsrisiko für das Unternehmensnetzwerk und die Daten möglichst gering zu halten, war es üblich, sich auf eine bestimmte Hard- und Software-Strategie zu einigen und Geräte sowie mobile Anwendungen zentral zu verwalten und zu warten. Kurz gesagt, man strebte eine möglichst einheitliche IT-Infrastruktur an, um den Aufwand für Kontrolle, Wartung, Support und insbesondere Sicherung der Geräte möglichst gering zu halten. Die IT trieb einen enormen Aufwand, um die Rechner so sicher wie möglich zu machen, rollte Sicherheitsprofile aus, baute Firewalls auf und verschlüsselte Festplatten zum Schutz vor unerlaubtem Zugriff.

Das Phänomen BYOD stellte in wenigen Jahren alles auf den Kopf, steht das Ansinnen doch einer einheitlichen IT-Umgebung diametral entgegen: Firmenfremde Geräte aus dem Privatbereich kommen in allen möglichen auf dem Markt erhältlichen Varianten mit dem Unternehmensnetzwerk in Berührung und verarbeiten und speichern dabei Unternehmensdaten. BYOD, ursprünglich ein „Angeber-Phänomen" auf den Teppichetagen, hat sich Top-down derart ausgebreitet, dass es heute aus Unternehmen nicht mehr wegzudenken ist. Zu stark ist der Drang nach persönlicher Wahlfreiheit der Mitarbeiter – vom topmotivierten Kreativen in Kleinunternehmen bis hin zum einfachen Angestellten in Großkonzernen. Nicht zuletzt profitieren Unternehmen von einer gesteigerten Produktivität der Mitarbeiter, wenn diese dank BYOD insgesamt zufriedener sind im Job.

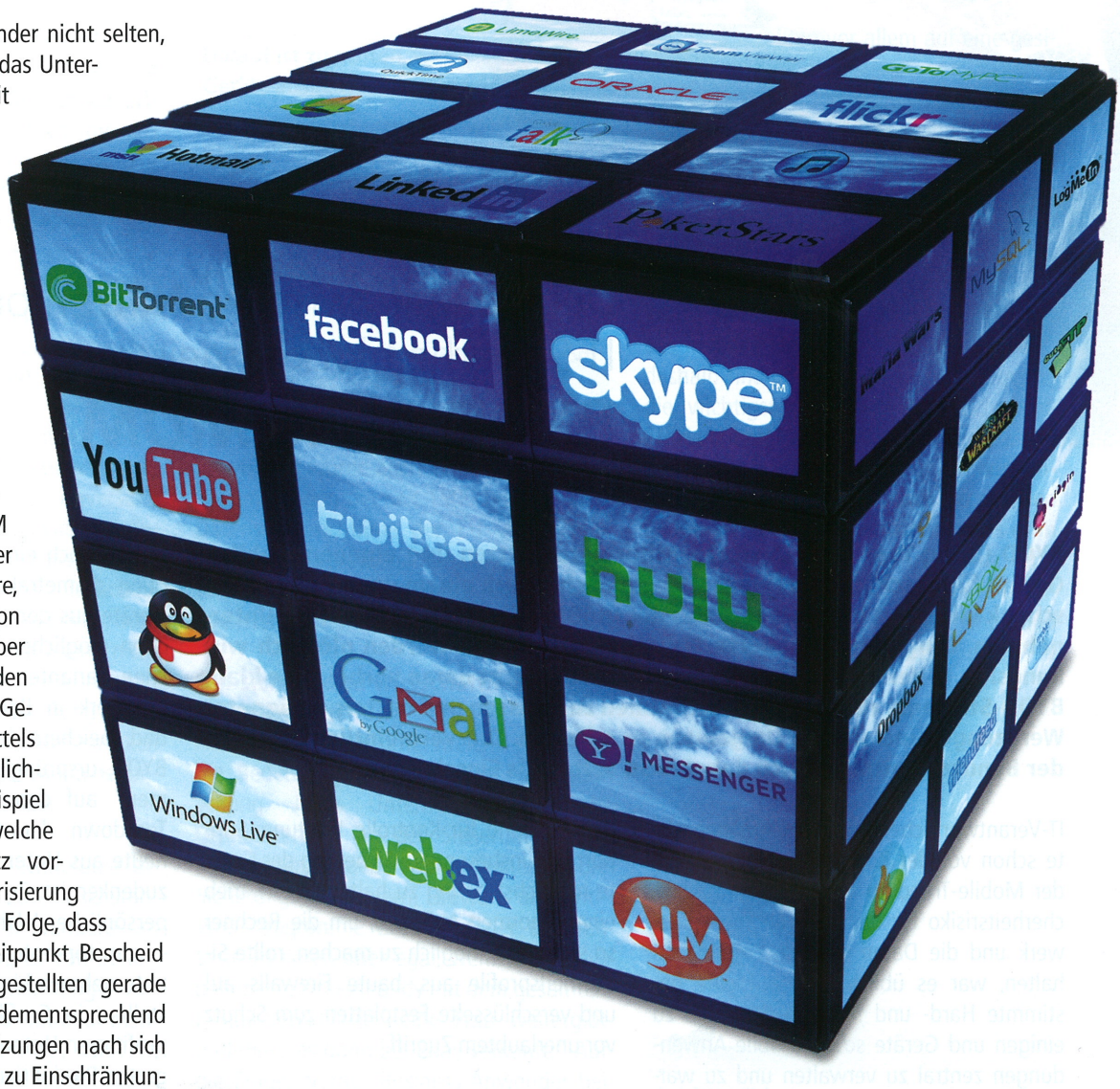
Wie die Sicherheit gewährleisten?

Der Grund für das Mitbringen der eigenen Geräte ist, dass Mitarbeiter mit demselben Gerät sowohl geschäftliche Anwendungen nutzen als auch gleichzeitig ihren gewohnten Kommunikationsgewohnheiten wie SMS oder Zugriff auf soziale Medien nachgehen wollen. Die Geräte werden deshalb zur Sicherheitsherausforderung, aber auch, weil Nutzer eigene Software im Unternehmensnetzwerk installieren. Sie verwenden nämlich immer häufiger nicht mehr nur die vom Arbeitgeber zur Verfügung gestellten Mittel, sondern laden eigene Collaboration-Lösungen herunter oder tauschen frischfröhlich Geschäftsdokumente über Google Docs, Dropbox und ähnliche Dienste aus. Dass solche Vorgehensweisen bösartigen Angriffen aus dem Internet Tür und Tor öffnen, versteht sich von selbst.

Dabei glauben die Anwender nicht selten, dass sie selbst und nicht das Unternehmen für die Sicherheit der Geräte und der Unternehmensdaten zuständig sind. Entsprechend wollen sie auch die Hoheit über ihre Daten und Geräte behalten. Gerade weil dem so ist, greift der bei firmeneigenen Geräten übliche MDM-Ansatz (Mobile Device Management) zur Lösung der Sicherheitsprobleme nicht. Bei MDM installiert der Arbeitgeber auf den Geräten Software, die dazu dient, private von geschäftlichen Daten sauber zu trennen und so den Schutz der Daten auf den Geräten sicherzustellen. Mittels MDM hat man die Möglichkeit zu prüfen, ob zum Beispiel Virenscanner aktiv oder welche Betriebssysteme im Netz vorhanden sind. Die Inventarisierung der Geräte hat zudem zur Folge, dass Arbeitgeber zu jedem Zeitpunkt Bescheid wissen, wo sich die Angestellten gerade aufhalten. MDM kann dementsprechend rechtliche Auseinandersetzungen nach sich ziehen. Es kann aber auch zu Einschränkungen der Nutzbarkeit der Geräte führen und steht darüber hinaus durch die Kontrolle und „Inbesitznahme" der Geräte durch den Arbeitgeber der freiheitsliebenden BYOD-Mentalität entgegen. Denn die Mitarbeiter möchten zwar ihre privaten Geräte für geschäftliche Zwecke nutzen können, wollen aber eigentlich nicht, dass der Arbeitgeber auf ihren Geräten irgendwelche Kontroll-Software installiert.

Geräte zulassen und Rechte beschränken

Die BYOD-Problematik geht also über die Verwendung zu unterschiedlichen Zwecken hinaus. Die eigentliche Herausforderung ist, dass Mitarbeiter ihre eigenen Anwendungen benutzen, was auch mit BYOA (Bring Your Own Application) umschrieben wird. Es sind bezüglich Sicherheit weniger die Endgeräte, die den IT-Leuten zu schaffen machen, sondern die Applikationen, die auf ihnen laufen. Deshalb setzen Security-Spezialisten wie WatchGuard bei der Authentifizierung der Geräte an – und nicht wie oft üblich bei der Umsetzung und Kontrolle einer BYOD-Strategie durch Mobile Device Management. Entsprechende UTM-Appliances (Unified Threat Management) erkennen dabei Geräte oder Applikationen, wenn sie im Netzwerk verwendet werden oder darauf vom Internet aus zugegriffen wird. Zur Sicherung der Umgebung kommt entweder eine Authentifizierung der Anwendungen oder der explizite Zugang via VPN-Tunnel zum Einsatz. Der Tunnel, welcher mittels Standardmethoden aufgebaut wird, garantiert dabei nicht nur die gesi-



Application Control: Die Kontrolle der Anwendungen ist wichtig, um zu wissen, welchen Gefahren das Netzwerk tagtäglich ausgesetzt ist. Quelle: WatchGuard Technologies

cherte Übertragung von Daten. Es kann ebenso der Traffic erfasst, überwacht, eingeschränkt und gemeldet werden. Diese Methoden sind seit Jahren bewährt, standardisiert und den IT-Administratoren vertraut. Es gibt also keinen Grund, das Sicherheitsproblem durch die direkte Verwaltung von Geräten unnötig zu verkomplizieren. Wichtig ist einzig, den Zugang via VPN-Tunnel nicht von privaten Geräten aus zuzulassen, weil diese verseucht sein können.

Weshalb stellt also BYOD dennoch eines der größten Sicherheitsprobleme dar? Der Grund ist schnell gefunden: Viele Unternehmen sind sich der Problematik zwar bewusst, setzen aber noch zu selten eine griffige Policy durch. Dies liegt meist daran, dass Unternehmen, gerade kleinere und mittelständische Firmen, nicht über eigene Sicherheitsbeauftragte verfügen. Oftmals obliegt nämlich das Thema Sicherheit quasi nebenher noch den Systemadministratoren, die nicht über das notwendige Know-how verfügen – erst recht nicht, wenn es um MDM geht. Umso einleuchtender ist deshalb der Einsatz von Authentifizierung und Applikationskontrolle, welcher aber auch nur dann greift, wenn die vorhandenen Netzwerksicherheitslösungen entsprechend einfach administrierbar sind. In der Praxis bedeutet das: Die Geräte zulassen und die Anwendungsrechte beschränken. Entweder der Mitarbeiter akzeptiert, dass sein Gerät hinsichtlich der Nutzung der geschäftlichen Anwendung eingeschränkt ist, oder er muss ein Firmengerät verwenden. Nur so ist der Systemadministrator in der Lage, mit dieser sicherheitsrelevanten und unternehmenskritischen Situation umzugehen.

Sicherheits-Policy festlegen

Die Definition der Benutzerrechte geschieht indes über die Identifikation des Anwenders, werden doch Sicherheitsregeln heutzutage innerhalb einer Firewall nicht mehr an der IP-Adresse, sondern an der Identität des Mitarbeiters festgemacht. Dieser wird aufgrund der Authentifizierungsstruktur einer Gruppe zugeteilt, dessen Mitgliedern auf sie zugeschnittene Rechte zugestanden werden. Diese Informationen können zur Ausführbarkeit von Diensten auf die Geräte selbst angewendet werden. Ein Beispiel: Ein Versicherungsvertreter möchte sein privates iPhone für die Bearbeitung von E-Mails verwenden und richtet sich dafür den Zugang auf den firmeninternen Exchange-Server ein. Er kann also E-Mails lesen, schreiben und versenden. Er erhält deshalb aber noch lange keinen Zugang auf die Unternehmensdaten, beispielsweise aufs ERP-System. Mit dem Firmen-Laptop (nicht mit dem Mobiltelefon) kann er hingegen über sein iPhone eine Internetverbindung und einen VPN-Tunnel zum Firmennetzwerk aufbauen. Denn im Gegensatz zu einem privaten Notebook erkennt das System den Firmenrechner und gewährt entsprechend Zugriff auf die Unternehmensdaten.

Ist deshalb die Freiheit dieses Mitarbeiters eingeschränkt? Ja, vielleicht – aber muss er wirklich auf dem iPhone eine größere Unternehmensanwendung bedienen können? Anspruchsvollere Arbeiten, etwa die Erstellung eines Angebots mit der Unternehmensanwendung oder die Erfassung von Kundendaten, kann er auf seinem iPhone sowieso nicht komfortabel und effizient ausführen. Und selbst wenn, gilt es bei der Benutzung von kritischen Daten mittels eigener Geräte die Reißleine zu ziehen! In der Mehrzahl der Fälle lässt sich schließlich das Problem auf die Nutzung von E-Mail herunterbrechen. Bei der BYOD-Diskussion sollte man sich ganz einfach die Frage stellen: Will der Angestellte mit seinem Gerät spielen oder soll er damit arbeiten?

Anwendungskontrolle zur Umsetzung von Richtlinien

Sicherheitsrichtlinien sollten immer auch auflisten, welche Geräte und Betriebssysteme genutzt werden dürfen und unterstützt werden. Zur Einhaltung der Richtlinien gilt es aber auch, Vereinbarungen zur zulässigen Nutzung zu treffen. Darin ist festzulegen, dass die Aktivitäten überwacht und eingeschränkt werden können, wann immer ein Angestellter mit seinem eigenen Gerät auf das Firmennetzwerk zugreift. Die Kontrolle der Anwendungen ist wichtig, um zu wissen, welchen Gefahren das Netzwerk tagtäglich ausgesetzt ist. Richtlinien müssen deshalb immer auch definieren, welche Anwendungen genutzt werden dürfen und welche nicht. Durch die Implementation von Anwendungskontrollmechanismen können die Vorgaben schließlich umgesetzt werden. Die Security Policy muss deshalb nicht nur definiert und umgesetzt, sondern auch permanent überwacht werden. Denn schützen kann man nur, was man kennt. Eine umfangreiche und gleichzeitig einfach zu handhabende Anwendungskontrolle ist deshalb besonders wichtig, denn nur so lässt sich nachvollziehen, wer erlaubt oder unerlaubt welche Applikationen benutzt.

Die Möglichkeiten gehen aber über die reine Sicherheitskontrolle hinaus. Durch Mitschreiben der Aktivitäten im Log-File werden alle Varianten der Steuerung möglich – von der Zulassung oder Ablehnung von Subfunktionen bis hin zur vollständigen Blockade. So kann beispielsweise definiert werden, wer Zugriff auf die Unternehmensdaten hat und ob er gleichzeitig Facebook nutzen kann oder nicht. Oder es kann bestimmten Gruppen, beispielsweise Mitarbeitern der Marketingabteilung, die Benutzung von Facebook, nicht aber von Facebook-Spielen ermöglicht werden. Die Herausforderungen in der IT, den Spagat zwischen Mitarbeiterzufriedenheit und Datensicherheit zu schaffen, steigen stetig. Sie können aber allesamt mit den bestehenden Mitteln und ohne Installation von Kontroll-Software auf den privaten Geräten durch eine einfach zu handhabende Steuerung der Aktivitäten im Unternehmensnetzwerk gemeistert werden. ■

Marc Drouvé,
Sales Engineer Manager EMEA,
WatchGuard Technologies

Für Abonnenten ist dieser Artikel auch digital auf www.datakontext.com verfügbar

Weitere Artikel/News zum Schwerpunkt unter www.datakontext.com/mobile