Mobile Security – Spagat zwischen Endanwender- und Unternehmensinteressen

Nichts ist beliebter, als das private mobile Endgerät auch im Berufsalltag zu nutzen. Anders sieht es bei denen aus, die solche Geräte in die Unternehmens-IT zu integrieren haben. Sie stehen vor einer anspruchsvollen Aufgabe und vor neuen Sicherheitsherausforderungen. Cyrill Peter

Der Wandel ist in vollem Gang und wird in Zukunft nichts an Intensität einbüssen: Das Stichwort lautet Bring your own Device (BYOD). Private mobile Endgeräte wie Smartphones, Tablets, iPads und Co., die primär für den privaten Konsum entwickelt wurden, finden ihren Weg in die Unternehmenswelt. Ihre explosionsartige Verbreitung sowie die rasant steigende Nutzung von Apps, die wachsenden mobilen Bandbreiten und die interaktiven sozialen Netzwerke verwischen die Grenzen zwischen Berufsleben und Freizeit immer weiter. Heute gehen laut einer IDC-Studie bereits bis zu 40 Prozent der IT-Manager davon aus, dass Firmenapplikationen auf privaten Endgeräten benutzt werden. Sogar 70 Prozent der Mitarbeitenden geben an, dies zu tun. Diese Entwicklung führt auch zu neuen Herausforderungen bezüglich Eigentumsmodellen: Bei BYOD werden private Geräte für den Job genutzt. Umgekehrt erwarten die Mitarbeitenden, dass sie die vom Unternehmen zur Verfügung gestellten mobilen Geräte auch für private Zwecke nutzen können.

Hinter dieser Entwicklung steht ein grundlegender Umbruch im IT-Markt, der mit dem Begriff «Consumerization of IT» umrissen wird. Geräte und Anwendungen, die als Trends zuerst das private Umfeld erobern, erzwingen aufgrund ihrer Beliebtheit eine Konvergenz mit der Unternehmens-IT. So treiben nicht mehr nur die Anbieter professioneller Businesslösungen die Entwicklung voran, sondern immer öfter auch die Hersteller von Consumer-Geräten. Die Mitarbeitenden gewinnen viel grösseren Einfluss auf die Hard- und Software sowie die Apps, die im Unternehmen zum Einsatz kommen. Währenddem stehen die IT-Verantwortlichen zum einen vor der Aufgabe, das Zusammenspiel der bestehenden Infrastrukturen mit diesen neuen Möglichkeiten zu gewährleisten. Zum anderen müssen sie auch die sichere Nutzung der mobilen Geräte und der Informationen, auf die sie zugreifen, garantieren.

Cyrill Peter ist Leiter ICT Security Product Management & Innovation bei der Swisscom (Schweiz) AG, Grosskunden.

Ohne Plan läuft nichts

Zwar machen die mobilen Geräte vieles einfacher und effizienter, doch die Unternehmen sind mit dem früher weitestgehend unbekannten Problem konfrontiert, dass sich der private und der geschäftliche Datenverkehr vermischen. Hier lauern viele Risiken, nicht zuletzt weil diese neuen Formen der Kommunikation auf offenen oder halboffenen Betriebssystemen basieren. Diese machen den Firmen zu schaffen, weil sie Einfallstore für Schad-Software sind und sich immer mehr Malware auf die neuen Alleskönner fokussiert. Je mehr infizierte Geräte unkontrolliert auf unternehmenseigene Netze zugreifen können, desto grösser wird ein möglicher Schaden. Zudem wächst die Anzahl der verlorenen oder gestohlenen Geräte, auf denen Firmendaten abgespeichert sind.

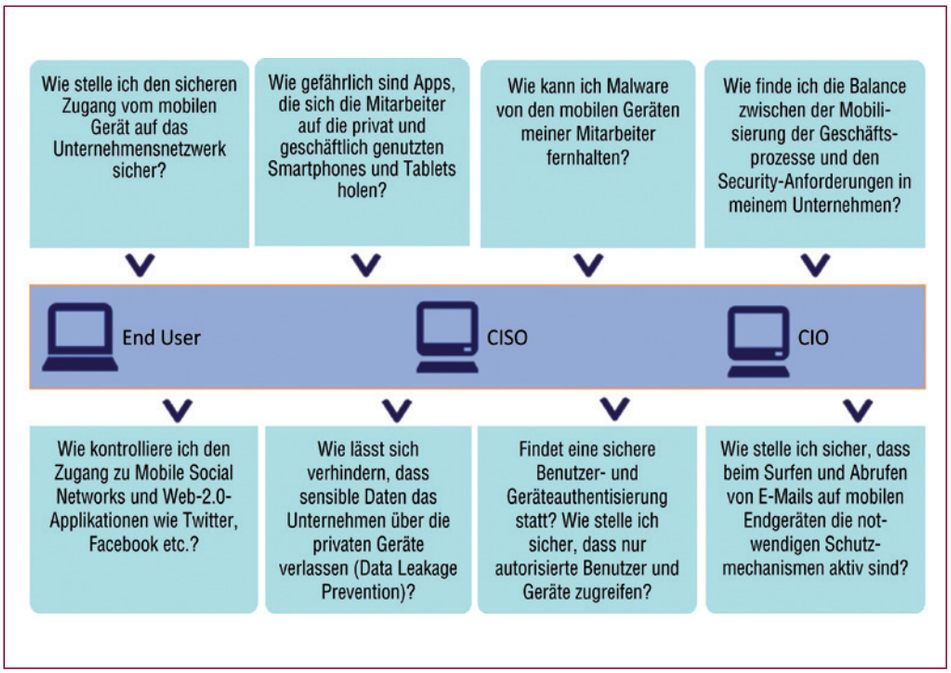
Um solche Risiken zu minimieren, sind die strukturierte Steuerung und der sichere Einsatz der mobilen Geräte inklusive aller damit einhergehenden Anwendungen unumgänglich geworden. Mobile-Security-Lösungen, wie sie professionelle Provider in verschiedenen Ausprägungen anbieten, helfen, den Spagat zwischen den Sicherheitsansprüchen der Unternehmen und dem Einsatz von mobilen Geräten zu schaffen. Zwar wäre es aus Sicherheitsgründen und aus Betriebssicht durchaus klug, die Nutzung privater Geräte einfach zu verbieten. Wie die aktuelle IT-Consumerization zeigt, lässt sich dies aber technisch nicht durchsetzen. Im Gegenteil riskieren die Unternehmen vielmehr eine Art Wettrüsten gegen die eigenen Mitarbeitenden, finden diese doch immer Wege, private Geräte ins Firmennetzwerk zu schleusen.

Viel besser ist es deshalb, die eigene IT-Infrastruktur gezielt auf die neuen Herausforderungen auszurichten. Denn es ist unumgänglich, das richtige Verhältnis zwischen der nötigen Sicherheit und der Freiheit zur Nutzung innovativer Anwendungen zu finden. Dieses Verhältnis ist kein absoluter Wert, sondern sieht für jede Branche und jedes Unternehmen etwas anders aus. Wer eine klare Ausrichtung für sein Unternehmen finden will, muss deshalb zunächst strategisch entscheiden, wohin die Reise gehen soll. Dabei gilt es zu klären, was die konkreten Anwendungsfälle im eigenen Unternehmen sind und welche Sicherheitsbedürfnisse adressiert werden müssen. Die Basis dafür bilden eine detaillierte Analyse der Situation sowie die Erstellung eines Risikoprofils, das am einfachsten gemeinsam mit externen Profis von darauf spezialisierten Providern aufgegleist werden kann. Einfach nur einen vorhandenen Sicherheitsansatz zu implementieren, reicht dabei nicht aus. Vielmehr ist in jedem Fall eine klare Richtlinie zum Umgang mit der mobilen, internetbasierten Kommunikation nötig. Diese muss selbstverständlich mit den bestehenden Sicherheitsrichtlinien des Unternehmens korrespondieren – und nicht nur für die mobile Welt gelten.

Verbindliche Regeln sind unumgänglich

Zentral ist die klare Definition von Unternehmensregeln und Sicherheitsrichtlinien für den Gerätezugriff, für die App-Nutzung und für den Zugriff auf Internet und Intranet. Zudem sind Passwortvorgaben sowie plattformspezifische Parameter auf den Endgeräten zu definieren und einzustellen. Dabei sollen die Richtlinien die verschiedenen Bedürfnisse berücksichtigen. Ein Aussendienstmitarbeiter zum Beispiel hat andere Ansprüche betreffend Mobilität als ein Mit-

arbeiter im Innendienst, der die geschäftliche Korrespondenz erledigt. Darum ist zu bestimmen, wie gearbeitet werden soll: Sind nur der E-Mail-Zugriff, die Kontakte und der Kalender mobil verfügbar oder die komplette Office- oder Business-Lösung? Je nachdem gestalten sich die Sicherheitsanforderungen unterschiedlich, und die einfache Authentifizierung stellt andere Ansprüche als eine zertifikatsbasierte. Grundsätzlich muss klar definiert sein, wem welche Daten zugänglich sein sollen. Doch egal um welches Unternehmen es sich handelt, am Ende der Strategiearbeit kommt dem zentralen Management der Endgeräte immer eine Schlüsselrolle zu.



Mobile-Security-Herausforderungen Grafik: Swisscom

Das saubere Aufgleisen der Möglichkeit zur eindeutigen Authentisierung von Usern und Endgeräten ist wichtig. Insbesondere die Geräteverschlüsselung ist heute unumgänglich, weil etwa Smartphones oder Tablets oft als mobile Büros eingesetzt werden. Diese enthalten dann grösstenteils sensitive Daten aus Business-Apps, Kontaktdaten von Geschäftspartnern und nicht selten vertrauliche Geschäftsinformationen. Mit dem Einsatz einer Mobile-Device-Management-Lösung und der damit geschaffenen Transparenz und Kontrolle über die Mobile-Device-Flotte lässt sich auch das Entfernen von Nutzungsbeschränkungen auf den Geräten (Jailbreaks) vermeiden. Die Integrität der Geräte und der Daten muss gewährleistet sein. Zudem unterstützt die zentrale Plattform die interne IT bei der Verteilung und der Kontrolle von Software aus den App-Stores und von unternehmenseigenen Applikationen. Hinzu kommen die einheitliche Verwaltung und die Durchsetzung von spezifischen Unternehmensrichtlinien. So werden nicht nur die Passwörter zentral verwaltet, sondern auch die Zugriffsmöglichkeiten auf spezifischen Anwendungen gesteuert und die Parameter definiert, die den Zugriff «on the air» auf externe Datenträger regeln.

Security im Fokus

Im Zentrum von Mobile-Security-Lösungen stehen immer das einfache und sichere Gerätemanagement, der sichere Zugang und insbesondere die Datensicherheit. Ob Geräteverlust, Diebstahl oder das Ausscheiden eines Mitarbeiters, ein Anruf beim IT-Dienstleister oder der eigenen IT-Abteilung genügt, um die Geschäftsdaten gezielt per Knopfdruck über das Funknetz zu löschen und das persönliche Firmen-Log-in zu sperren. Damit die Geräte und die Benutzer zusätzlich von überall auf das firmeneigene Intranet zugreifen können, müssen auch der Datenverkehr und die Kommunikation zwischen den mobilen Endgeräten und dem Firmennetz vertraulich funktionieren. Via Remote-Access-Lösungen (RAS) lässt sich hierfür ein mobiles VPN (Virtuell Private Network) einrichten. Dabei kommen modernste Verschlüsselungstechnologien und auf Wunsch auch starke Authentisierungsmethoden zum Einsatz, die je nach Anspruch auch die Authentisierung mittels digitaler Zertifikate umfassen.

Auch für den gesicherten und kontrollierten Zugang ins Internet via Apps und Mobile-Browser gibt es Lösungen. Dabei muss der Benutzer beim Surfen via mobiles Gerät vor den Gefahren des Internets geschützt werden. Mobile-Security-Lösungen wie Mobile Content Security filtern mobil abgerufene Inhalte und garantieren die sichere Nutzung des Internet- und Mailverkehrs. Dafür steht unter anderem das sogenannte URL-Filtering zum Schutz vor unliebsamen und gefährlichen Inhalten wie Malware zur Verfügung. Ausserdem lässt sich so auch der Zugriff auf die Web-2.0-Welt wie Facebook, Twitter und Co. inklusive den dazugehörigen Apps beherrschen. Die Massnahmen lassen sich auch mit mobilen Data Leakage Prevention kombinieren. Damit kann sichergestellt werden, dass keine Firmengeheimnisse das Unternehmen via mobiles Gerät verlassen.

Der richtige Mix macht's

Heute ist es notwendig, eine zunehmende Anzahl mobiler Geräte zu unterstützen und zu sichern. Die dadurch entstehenden Herausforderungen werden jedoch durch eine Reihe von Faktoren erschwert, insbesondere durch die Vielfalt von Plattformen und Geräten. Die Bestimmung der Richtlinien ist eine Gratwanderung. Einerseits gilt es, die Risiken der Nutzung von Endgeräten im Unternehmen so zu minimieren, dass sie nicht durch zu grosse Restriktionen zum Umgehen einladen. Andererseits dürfen die Barrieren auch nicht so niedrig sein, dass sie Tür und Tor für immer aggressiver auftretende Cyberkriminelle öffnen. Berücksichtigt man zudem noch die immer stärkere Konsumentenorientierung der IT, die Explosion von firmeneigenen und privaten mobilen Geräten plus Apps sowie die Tatsache, dass es für Mobilität schlichtweg keine ganzheitlichen Sicherheitslösungen gibt, so lässt sich leicht feststellen, dass dieses Thema auch in Zukunft eine grosse Herausforderungen für die IT der Unternehmen darstellen wird. <