**IBM Software**
White Paper – Thought Leadership

# Schneller Wandel zum sicheren mobilen Unternehmen

*Risikominimierung durch mehr mobile Sicherheit im Unternehmen und optimale Ausnutzung des Geschäftspotenzials*

IBM

## Inhalte



## Einleitung

Seit über zwei Jahrzehnten kämpfen die Unternehmen nun schon mit den Sicherheitsproblemen des drahtlosen Arbeitsplatzes. Laptop-Computer waren die ersten Geräte, die die Grenzen herkömmlicher Umgebungen aufweichten. Mittlerweile sind Smartphones und Tablet-PCs zunehmend zu professionellen Arbeitswerkzeugen geworden. Im Jahr 2011 haben die Verkaufszahlen bei Smartphones zum ersten Mal die PC-Verkaufszahlen übertroffen – Analysten sind der Überzeugung, dass die Smartphone-Verkäufe bis zum Jahr 2016 die Grenze von 1,5 Mrd. verkauften Einheiten überschreiten werden.[1] Man geht davon aus, dass ebenfalls bis 2016 über 350 Millionen Menschen ihr Smartphone für die Arbeit nutzen werden.[2]

Unternehmen weltweit nutzen die Vorteile dieser Entwicklung, da der Einsatz mobiler Geräte – einschließlich der persönlichen, für die Arbeit genutzten Geräte – die Reaktionsfähigkeit, Dynamik in den Geschäftsabläufen und die Produktivität erhöhen können. Je mehr Mitarbeiter jedoch ihre mobilen Geräte mit dem Unternehmensnetzwerk verbinden – und Geräte, die in erster Linie für den Verbrauchermarkt konzipiert wurden, in Geschäftsumgebungen eindringen, informelle Verhaltensweisen aus der persönlichen Kommunikation im geschäftlichen Bereich genutzt werden und Geschäftsdaten und private Daten oft Seite an Seite auf derselben mobilen Pattform gespeichert werden –, wird das Thema Sicherheit in der gesamten IT-Umgebung immer wichtiger und deutlich komplexer.

Dadurch kommt es in der Unternehmensumgebung auf verschiedenen Ebenen zu Sicherheitsbedrohungen und einem geradezu dramatischen Anstieg bei den intelligenten Attacken. Die Führungskräfte fordern deshalb von ihren IT-Abteilungen einen proaktiven Ansatz für den Schutz kritischer Daten und Infrastrukturen. In diesem White Paper wird auf die wichtigsten Herausforderungen eingegangen. Zudem werden Strategien für die Risikominimierung vorgestellt und Möglichkeiten für den sicheren Umgang mit Mobiltechnologien im Unternehmen untersucht.

## Was ist anders bei mobilen Geräten, Anwendungen, Zugriffsmöglichkeiten – und Sicherheitsbedrohungen?

Mobile Geräte, Anwendungen und Zugriffsmuster verändern die Art und Weise, wie Unternehmen mit ihren Kunden, Mitarbeitern und Partnern kommunizieren. Weltweit nutzen Unternehmen zunehmend das mobile Leistungsspektrum, um neue Geschäftschancen zu erschließen und ihre Geschäftsmodelle zu verändern. Gleichzeitig sind sie bestrebt, ihr eigenes Leistungsspektrum zu erweitern und orts- und zeitunabhängig bereitzustellen. Dabei stellen sie jedoch fest, dass für das Management mobiler Geräte, für Anwendungen und für Zugriffsoptionen neue Prozesse implementiert werden müssen – und um das mobile Unternehmen gegen Bedrohungen zu schützen.

Daher sind mit dieser neuen Mobilität – auf einem sicheren VPN im Unternehmen oder in einem öffentlichen Wi-Fi-Hotspot – Verhaltensweisen, Technologien und Sicherheitsbedrohungen verbunden, die sich von denjenigen einer herkömmlichen Büroumgebung unterscheiden. Einige dieser speziellen Herausforderungen sind nachfolgend aufgeführt:

- **Mobile Geräte werden an verschiedenen Standorten genutzt**. Mobile Geräte werden häufig außerhalb des Unternehmensnetzwerks verwendet. Zudem nutzen viele Benutzer eine Vielzahl von Netzwerken, um auf ihre Konten zuzugreifen. Authentifizierung ist ein wichtiges Kriterium, da die Integrität von Transaktionen oder der Kommunikation schnell beeinträchtigt werden kann. Daher sollte der Zugriff nur auf Basis erkennbarer Faktoren wie Kontext des Standorts, Gerätemerkmale, Anwendungsinformationen, Zeit und Netzwerk gewährt werden.

- **Mobile Geräte und die Anwendungen, die sie unterstützen, sind sehr vielschichtig**. Benutzer haben in der Regel mehrere Geräte, deren Status sich immer wieder verändert. Unterschiedliche Betriebssysteme unterstützen möglicherweise unterschiedliche Sicherheitsmechanismen und die Mitarbeiter installieren vielleicht unterschiedliche Anwendungen auf ihren Geräten. Möglicherweise werden auch vertrauliche Geschäftsinformationen auf diesen Geräten gespeichert, sodass Geräteverluste oder Mitarbeiterfluktuationen genauso gefährlich werden können wie eine Attacke. Das Unternehmen benötigt daher eine umfassende Transparenz zu Geräten und Anwendungen, um solche Bedrohungen bis ins Detail verstehen zu können.
- **Mobile Geräte sind für viele Benutzer mittlerweile zum primären Interaktionskanal geworden**. Gefährliche Angriffe auf mobile Geräte und die darauf installierten Anwendungen können Attacken auf das gesamte Unternehmensnetzwerk nach sich ziehen oder ganze Systeme infizieren. Die enorme Verbreitung dieser Geräte kann zudem die Kosten und die Komplexität beim IT-Management – und beim Datenschutz – erhöhen.
- **Mobile Geräte werden häufig von mehreren Personen genutzt**. Smartphones und Tablet-PCs können auch von Familienmitgliedern und Arbeitskollegen genutzt werden, sodass diese Geräte unterschiedliche Sicherheitsprofile brauchen. Hierzu folgendes Beispiel: Ein Mitarbeiter und seine fünf Jahre alte Tochter können zwar beide auf persönliche Fotos zugreifen, jedoch sollte nur der Mitarbeiter Zugang zu den Unternehmensgewinnen im letzten Quartal haben. Die Authentifizierung und Berechtigung nur eines bestimmten Benutzers oder Geräts bietet möglicherweise nicht das erforderliche hohe Maß an Kontrolle und Schutz.
- **Bei der Mobilität gilt die Priorität den Erfahrungen des Benutzers**. Es gibt viele Benutzer, die ihre Entscheidungen hinsichtlich Geräten und Anwendungen auf Basis ihrer persönlichen Vorstellungen treffen. Somit können Sicherheitskontrollen, die für den Bereich Mobilität nicht geeignet sind, dazu führen, dass Bestimmungen nicht eingehalten werden oder Benutzer an solchen Initiativen nicht teilnehmen. Sicherheitsmaßnahmen, die nahtlos in die Benutzererfahrungen eingebunden werden können, z. B. sichere, aber einfach zu verwaltende Kennwörter oder die kontrollierte und gleichzeitig einfache Installation von Anwendungen, können helfen, Bestimmungen einzuhalten und die Produktivität der Benutzer zu erhöhen.

Die zentrale Herausforderung liegt deshalb darin, Mittel und Wege zu finden, um möglichen Sicherheitsbedrohungen erfolgreich zu begegnen, ohne den Enthusiasmus der Mitarbeiter, mobile Geräte und Anwendungen zu nutzen, einzuschränken. Mithilfe eines proaktiven, geschichteten Ansatzes für die Sicherheit in mobilen Unternehmen können IT-Abteilungen helfen, die Geschäftsprozesse effizienter und zukunftsorientierter zu gestalten – und weniger als „Sicherheitspolizei“ agieren, die der Nutzung neuer Technologien eher im Weg steht. Unternehmen, die sich für integrierte Sicherheitslösungen und einen adaptiven Sicherheitsframework entscheiden, können ihren Mitarbeitern helfen, orts- und zeitunabhängig mit weniger Aufwand mehr zu erreichen.

## Mobilität kann für Benutzer ein Segen sein – für die IT jedoch zum Fluch werden

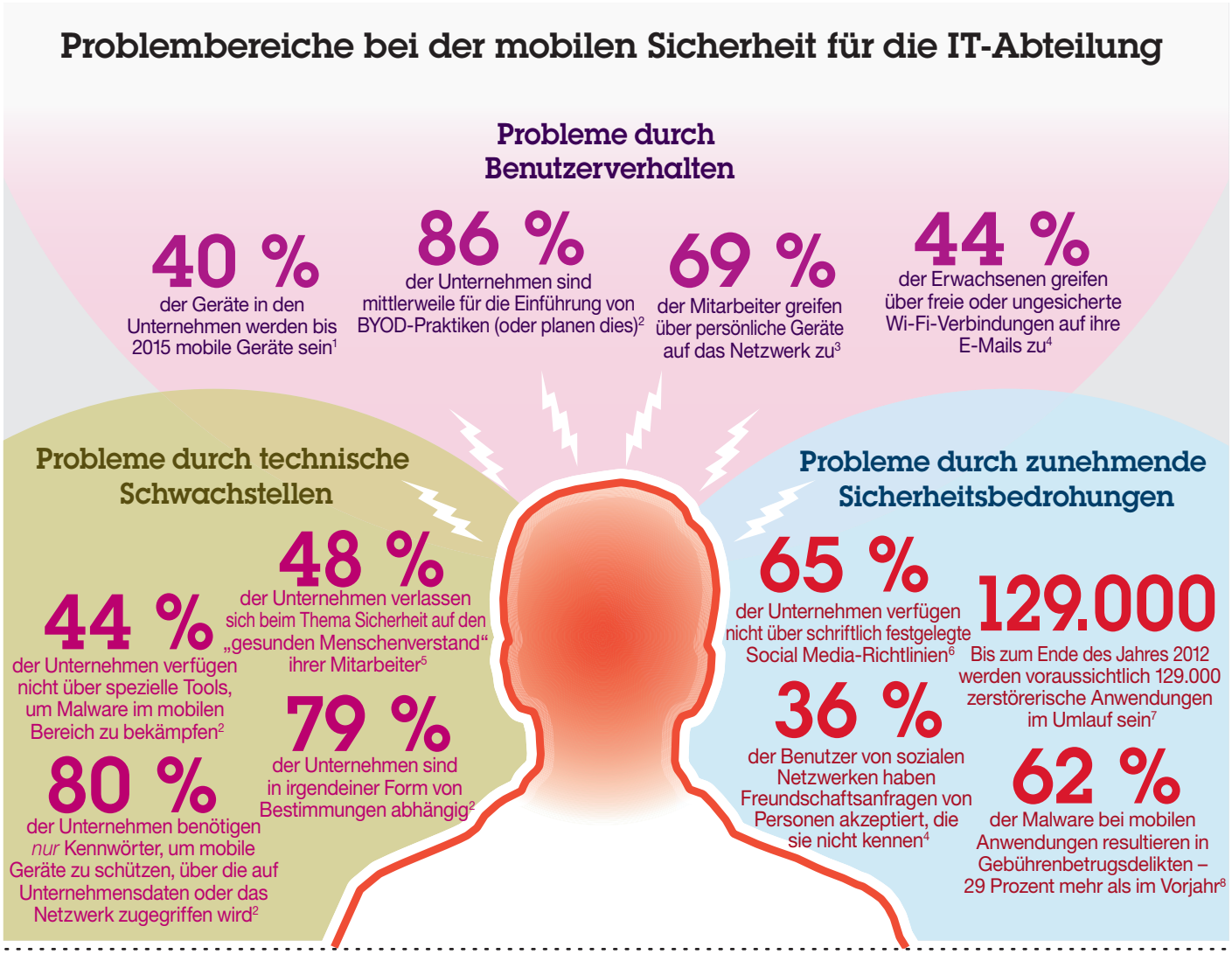
Sobald der Bereich IT Operations die besonderen Merkmale mobiler Geräte, Anwendungen und Zugriffsmöglichkeiten erkannt hat, treten unmittelbar spezielle Herausforderungen auf. Die Probleme, denen sich CIOs (Chief Information Officer) und IT-Administratoren gegenübersehen, haben in der Regel drei Ursachen – Benutzerverhalten, technische Schwachstellen und die zunehmenden Sicherheitsbedrohungen.

### Benutzerverhalten

Smartphones und Tablet-PCs, die in zunehmendem Maß geschäftlich genutzt werden, fungieren – ebenso wie Laptops und Desktop-PCs – als Endpunkte. Hierzu gehören beispielsweise iPhone-, Android- und Blackberry-Smartphones, iPad-, Android- und andere Tablet-PCs, sprach-/nur-textfähige Mobiltelefone (Telefone ohne Datenzugang), Netbooks oder Ultralight-Laptops und andere leistungsfähige, tätigkeitsspezifische mobile Geräte.

Dabei stellt sich die Frage: Wem gehören diese Geräte? Viele Unternehmen konzentrieren sich mittlerweile auf so genannte BYOD-Programme, bei denen die Mitarbeiter ihre eigenen mobilen Geräte mitbringen können, um auf E-Mails, Daten und Anwendungen im Unternehmen zuzugreifen. Solche BYOD-Programme können helfen, die IT-Betriebs- und Gerätekosten zu senken, die Mitarbeiterproduktivität zu verbessern und sich von anderen Unternehmen abzuheben. Aber bereits die enorme Menge an unterschiedlichen Geräten und die Geschwindigkeit, mit der diese auf den Markt kommen, können für die IT sichtbare Managementprobleme hervorrufen. Die Art und Weise, wie diese Geräte genutzt werden, kann zudem zu Sicherheitsproblemen führen und denjenigen Kopfzerbrechen bereiten, die für die Sicherheit der Unternehmensdaten und die Einhaltung von Bestimmungen verantwortlich sind.

# Problembereiche bei der mobilen Sicherheit für die IT-Abteilung




1 IBM Prognose.

2 Michael Finneran, „2012 State of Mobile Security“, *InformationWeek,* Mai 2012. http://reports.informationweek.com/abstract/21/8792/security/research-2012-state-of-mobile-security.html

3 Information Security FS, „CISO - Chief Information Security Officer Role: From ‘Digital Bouncer’ to Strategist“. http://www.wbresearch.com/InformationSecurityFS/ciso.aspx

4 Symantec, „2012 North Cybercrime Report“. http://www.slideshare.net/marianmerritt/2012-norton-cybercrime-report-14175700

5 Jim Rapoza, „Buyer’s Guide to Mobile Device Management“ *InformationWeek, November 2011. http://reports.informationweek.com/*abstract/18/8546/Mobility-Wireless/buyer-s-guide-mdm.htmp

6 IBM Corp., „IBM X-Force 2011 Trend and Risk Report“, März 2012. http://www-935.ibm.com/services/us/iss/xforce/trendreports/

7 Trend Micro, „Behind the Anroid Menace: Malicious Apps“, Security Intelligence Blog, 2011. http://blog.trendmicro.com/trendlabs-security-intelligence/infographic-behind-the-android-menace-malicious-apps/

8 Lookout Mobile Security, „State of Mobile Security 2012“, 2012. https://www.lookout.com/resources/reports/state-of-mobile-security-2012

### Technische Schwachstellen

Heute legt jeder im Unternehmen, von der IT-Abteilung bis zu den leitenden Angestellten, mehr als je zuvor das Hauptaugenmerk auf die Sicherheit von Geräten, Anwendungen und Zugriffsoptionen. Viele halten den Verlust oder Diebstahl von Geräten für eines des wichtigsten Probleme bei der mobilen Sicherheit[3], da beeinträchtigte oder gestohlene Daten den Ruf des Unternehmens ernsthaft beschädigen oder sich negativ auf die Wettbewerbsfähigkeit auswirken können.

Ein effektives Konzept für mobile Sicherheit geht über die reine Gerätesicherheit hinaus und umfasst durchgängig hohe Sicherheitsstandards. Dabei muss sich die IT-Abteilung um vielfältige mobile Risiken kümmern: nicht sichere Datenspeicher, mangelhafte Kontrollmechanismen auf Serverseite, unzureichender Schutz auf Transportebene, Injectionattacken auf Clientseite und unzureichende Berechtigungs- und Authentifizierungsmechanismen. Um externen Sicherheitsbedrohungen vorzubeugen, sind leistungsfähige Datensicherheitsmechanismen auf mobilen Geräten erforderlich. Hinzu kommen strenge Authentifizierungsmaßnahmen, um den Netzwerkzugriff zu steuern. Anders lassen sich solche Risiken nicht minimieren.

### Zunehmende Sicherheitsbedrohungen

IT-Abteilungen haben bisher immer im so genannten reaktiven Modus gehandelt und nur auf Sicherheitsrisiken reagiert, wenn ein Problem bereits aufgetreten war. Durch die Geschwindigkeit, mit der sich Mobiltechnologien verändern, und die Notwendigkeit für die Benutzer, für ein effektives Arbeiten immer direkten Zugriff zu haben, sind reaktive Verhaltensweisen überfordert und nicht mehr sicher genug. Da Mobiltechnologien für die meisten Unternehmen noch relativ neu sind, bieten vorhandene Sicherheitsmaßnahmen häufig keinen adäquaten Schutz.

Mögliche Bedrohungen zielen mittlerweile auf bestimmte Verhaltensweisen des Benutzers oder technische Schwachstellen ab, die durch Anfälligkeiten im Mobilbereich bewirkt werden. Hierzu gehören beispielsweise Social Engineering, Identitätsdiebstahl, außer Kontrolle geratene Anwendungen, Man-in-the-Middle- oder Denial-of-Service-Attacken. Als Reaktion darauf müssen die Unternehmen verschiedene Bereiche wesentlich sorgfältiger handhaben. Hierzu gehört beispielsweise die Nutzung sozialer Netzwerke durch die Mitarbeiter, in denen oftmals Informationen zu sorglos ausgetauscht werden. Die Unternehmen müssen die verwendeten Geräte deutlich intensiver überwachen, um sicherzustellen, dass ihre Betriebssysteme nicht gehackt oder gerootet werden. Das Herunterladen von Anwendungen, die zerstörerischen Code enthalten, wodurch vertrauliche Unternehmens- und persönliche Daten offengelegt und Infrastrukturen beschädigt werden können, muss besser kontrolliert werden.

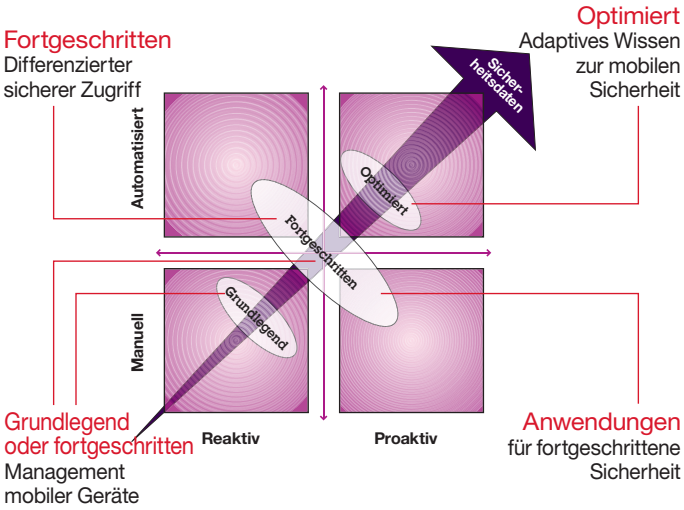
## Vier Schritte zu mehr Sicherheit im mobilen Unternehmen

Das breite Spektrum an Smartphones und Tablet-PCs, die im Unternehmen verwendet werden, und die wachsenden Sicherheitsbedrohungen bei mobilen Geräten, Anwendungen und beim System-/Datenzugriff bedeuten für die IT-Abteilungen, dass sie sich bei der Definition umfassender Sicherheitsstandards und Kontrollmechanismen auf eine schwierige Zeit einstellen müssen. Es gibt jedoch einige Schritte, die die Unternehmen einleiten können.

### Sichere mobile Geräte: Die Basis für eine sichere Umgebung

Das Management von mobilen Geräten ist in der Regel einer der Meilensteine der Mobilitätsstrategie eines Unternehmens – und oft die erste Investition, die getätigt wird. Ursächlich hierfür ist die Problematik, dass sich Risiken erst gezielt handhaben lassen, wenn der Umfang dessen bekannt ist, was geschützt werden soll. Mit einer Lösung für das Management mobiler Geräte kann die IT-Abteilung die Anzahl der im Unternehmen genutzten Geräte verfolgen und überwachen. Mit derselben Endpunkt-Managementlösung lassen sich sowohl mitarbeitereigene als auch unternehmenseigene Geräte verwalten.

**Vier Schritte zu mehr Sicherheit im mobilen Unternehmen**



Die durch solche Technologien bereitgestellten Sicherheitsmechanismen dürfen sich für den Benutzer nicht negativ auswirken – vielmehr müssen sie ein sicheres Arbeiten ermöglichen, um das Gerät selbst sowie die auf ihm gespeicherten bzw. übertragenen vertraulichen Daten zu schützen. Idealerweise ist eine solche Lösung eine Erweiterung zu einer vorhandenen Endpunkt-Managementlösung, sodass eine zentrale Sicht zu allen Unternehmenssystemen gegeben ist.

Eine effektive Lösung für das Management mobiler Geräte kann helfen, Datenverluste zu vermeiden, indem die Daten für die Übertragung verschlüsselt werden und auf verloren gegangenen oder gestohlenen Geräten eine Datenbereinigung durchgeführt wird. Zudem kann der Zugriff auf Geräte durch Sperrmechanismen verhindert werden. Anti-Malware, Jailbreak-Erkennung, Non-Compliance-Erkennung und Sicherheitsupdates auf den Geräten sind weitere Maßnahmen für mehr Sicherheit.

Die richtige Managementlösung für mobile Geräte hilft Unternehmen, Richtlinien für vorschriftsmäßige Verbindungen zu definieren. Hierzu werden u. a. in so genannten Blacklists Anwendungen erfasst, die nicht berechtigt sind, auf Ressourcen des Unternehmens zuzugreifen. Außerdem werden umfangreiche Daten zur mobilen Sicherheit dokumentiert, um dem Thema Sicherheit die gebotene Aufmerksamkeit zukommen zu lassen. Durch die kontinuierliche Weiterentwicklung eines geeigneten Funktionsspektrums können sich die Unternehmen auf die immer komplexer werdenden Bedrohungen und Attacken vorbereiten.

Mit der richtigen Managementlösung für mobile Geräte können sie den Anwendungszugriff durch entsprechende Benutzerauthentifizierungen und die Möglichkeit, Anwendungen zu inaktivieren, weiter einschränken. Neben der Erfüllung der technischen Voraussetzungen kann eine solche Lösung außerdem helfen, die IT-Kosten zu kontrollieren und den Managementaufwand zu reduzieren, sobald die Anzahl der zu verwaltenden Endpunkte zunimmt.

### Geschützter mobiler Zugriff: das Gut-Böse-Schema optimal umgesetzt

IT-Unternehmen müssen dafür sorgen, dass der sichere Zugriff auf Ressourcen gewährleistet ist. Hierfür muss die kontextspezifische Natur des mobilen Zugriffs in Betracht gezogen werden. Standort, Netzwerk, Benutzer und viele andere Merkmale einer mobilen Interaktion können das Risiko beeinflussen, das mit dem Zugriff auf Unternehmsdaten und -ressourcen verbunden ist. Je nach Risikostufe kann dies die Entscheidung für die Gewährung oder Verweigerung des Zugriffs, die Wahl des Authentifizierungsschemas und der Serviceberechtigung für die Interaktion beeinflussen.

Bei der Zugriffssteuerung muss die Authentifizierung sowohl für den Benutzer als auch das Gerät erfolgen. Die Schemata müssen auf Basis von deren Eignung für mobile Benutzer angewendet werden – z. B. biometrische Daten oder Einmalkennwörter. Unternehmen müssen zudem beachten, dass sie eine Umgebung mit leistungsfähigen Funktionen für das Sitzungsmanagement aufbauen, um das Risiko von Man-in-the-Middle-Attacken zu minimieren, die hauptsächlich in nicht vertrauenswürdigen Netzwerken vorzufinden sind. Eine effektive Lösung für mobilen Zugriff kann durch Technologien wie VPNs sicheren Zugriff auf Unternehmenssysteme gewährleisten. Da mobile Benutzer häufig mehrere Aufgaben auf einmal ausführen, muss darauf geachtet werden, dass auch mehrere Verbindungen sicher sind. Eine leistungsfähige Managementlösung für mobilen Zugriff kann helfen, den unberechtigten Zugriff auf Unternehmenssysteme zu unterbinden, konsistente Unternehmensrichtlinien umzusetzen und geltende Bestimmungen einzuhalten.

Ein auf Standards basierender Mobile Access Manager ermöglicht durchgehende Sicherheit für Unternehmensdaten und -anwendungen, ohne die Produktivität der Benutzer zu beeinträchtigen. Für mobile Mitarbeiter, Kunden und Partner können unterschiedliche Ebenen des sicheren Zugriffs definiert werden.

### Sichere mobile Anwendungen: wo sich Richtlinien und Standards auszahlen

Neben den geräte- und zugriffsspezifischen Herausforderungen sehen sich Unternehmen häufig auch mit ernsthaften Sicherheitsrisiken bei mobilen Anwendungen konfrontiert. So kann beispielsweise Malware in Anwendungen verborgen sein, die aus öffentlich zugänglichen App-Stores heruntergeladen werden. Ein weiteres Beispiel: Teams in den Bereichen Marketing oder Vertrieb entwickeln Ad-hoc-Anwendungen, um Marktchancen zu nutzen oder der wachsenden Nachfrage gerecht zu werden. Häufig werden dabei jedoch Sicherheitsaspekte und strukturierte Entwicklungsprozesse vernachlässigt, die die Ursache für weitere Risiken sind. Die rasante Übernahme neuer Technologien kann zu Lücken bei der Sicherheit mobiler Anwendungen führen. Darüber hinaus unterstützen mobile Anwendungen häufig mehrere Interaktionspunkte, die das Risikopotenzial weiter erhöhen.

Unternehmen entwickeln, nutzen und vernetzen zunehmend mobile Anwendungen für Mitarbeiter, Kunden und Partner. Die wenigsten Unternehmen sind jedoch in der Lage, alle mobilen Awendungen bereitzustellen, die die Benutzer wollen. So wenden diese sich oft an andere Anbieter. In der Folge müssen die Unternehmen besonders wachsam sein, wenn es um die Einhaltung ihrer Sicherheitsrichtlinien geht, da andere Anwendungsanbieter z. B. geringere Sicherheitsstandards zugrunde legen – oder möglicherweise überhaupt keine Sicherheitstests durchgeführt haben. Unternehmen können

sich gegen herkömmliche Viren, die es auf ihre mobilen Anwendungen abgesehen haben, schützen, indem sie sicherstellen, dass die betreffenden Geräte nicht gehackt oder gerootet wurden. Um sich auch gegen die zunehmende Gefahr durch außer Kontrolle geratene Anwendungen zu schützen, die durch zerstörerischen Code oder infizierte Daten in gefährdeten Anwendungen hervorgerufen wird, müssen Unternehmen genauestens prüfen, ob die betreffenden Anwendungen seit der letzten Interaktion geändert wurden.

Unternehmen können sich also durch einen proaktiven Ansatz bei der Sicherheit von mobilen Anwendungen entsprechend schützen. Die Implementierung von Patches und Behebung von Schwachstellen erst nach der Implementierung von Anwendungen kann sehr kostspielig und zeitaufwendig werden – durch aktuelle Sicherheitsprodukte lassen sich Prozesse wie Sicherheitstests und Risikomanagement jedoch automatisieren. Unternehmen sollten sich für eine mobile Anwendungsplattform entscheiden, die Entwickler dahingehend unterstützt, dass sich Sicherheitsfunktionen wie die Verschlüsselung lokaler Anwendungsdaten während der Entwurfs- und Buildprozesse problemlos einbinden lassen. Von der Entwicklung bis zum Test können geeignete Lösungen Anwendungen durchsuchen, Schwachstellen erkennen und Berichte zu Sicherheitslücken erstellen. Außerdem lassen sich damit Probleme beheben, bevor die Anwendung implementiert wird – Sicherheitsfunktionen werden also bereits beim Design der Anwendungen berücksichtigt und kommen nicht erst zum Einsatz, wenn der Ernstfall bereits eingetreten ist.

### Aussagekräftige Informationen zur mobilen Sicherheit: Wissen als Voraussetzung für effizientes Handeln

Neue Verhaltensweisen bei den Benutzern und neue Arten von Bedrohungen sind immer die Vorläufer für sicherheitsspezifische Best Practices. In der von Dynamik und Social Media geprägten und verbraucherorientierten mobilen Welt von heute führen neue Geräte und Anwendungsfunktionen zu neuen Arten von Interaktionen bei den Benutzern, auf die die IT erst später aufmerksam wird. Da neue Bedrohungen neue Schwachstellen aufdecken und gezielt auf bestimmte Attacken ausgerichtet sind, sind für das richtige Sicherheitskonzept in der Regel leistungsfähige Überwachungsfunktionen in den Sicherheitslösungen erforderlich – obwohl diese in vielen Fällen leider fehlen.

Das Thema Sicherheit zu ignorieren und keine entsprechenden Maßnahmen zu ergreifen, ist jedoch keine Option. Sicherheitsverletzungen ziehen nicht nur finanzielle Nachteile durch gesetzliche Bestimmungen nach sich, sondern können in einem zunehmend von Wettbewerb geprägten Umfeld auch dazu führen, dass geschäftliche Chancen nicht genutzt werden und das Vertrauensverhältnis zu Kunden, Partnern und Mitarbeitern getrübt wird.

Daher ist es absolut wichtig, eine sicherheitsrelevante Wissensbasis aufzubauen, indem Sicherheitsereignisse aus allen Bereichen der mobilen Sicherheit erfasst, Ergebnisse analysiert und aussagekräftige Detailinformationen erarbeitet werden. Nur so lassen sich gesetzliche Bestimmungen sowie prüfungs- und geschäftsrelevante Anforderungen einhalten.

Je mobiler die Mitarbeiter werden, desto mehr gewinnt das Thema Sicherheit für Geräte, Zugriffsmöglichkeiten und Anwendungen im Unternehmen an Bedeutung. Hacker werden nicht aufgeben, Schwachstellen zu finden und auszunutzen. Es werden immer mehr unterschiedliche Arten von Geräten, Plattformen und Anwendungen auf den Markt kommen. Ein adaptiver Ansatz zum Thema mobile Sicherheit kann helfen, Risiken effizient zu handhaben und Bedrohungen abzuwenden.

## Fazit

In den heutigen, von Mobilität geprägten Unternehmen ist die Sicherheit ein wichtiges Thema, damit Mitarbeiter sicher und zuverlässig die Vorteile intelligenter mobiler Geräte nutzen können. Benutzerverhalten, technische Schwachstellen und die schnell wachsenden Sicherheitsbedrohungen bringen zahlreiche Herausforderungen mit sich. Ausreichender Schutz und hohe Zuverlässigkeit lassen sich in den Unternehmen nur erreichen, wenn die Sicherheitskonzepte an den betrieblichen Prioritäten ausgerichtet werden. Optimal geeignet hierfür ist eine kostengünstige und einfach zu verwaltende Lösung mit einem abgestuften Konzept, bei der die mobile Sicherheit in bestehende Technologien und die Unternehmenskultur einfließt.

Das integrierte und umfassende IBM® Sicherheitskonzept bietet die zentrale Sicherheitsstruktur, die moderne Unternehmen brauchen. Mit einem ganzheitlichen Ansatz für die geschäftsorientierte Sicherheit stellen IBM Lösungen sicher, dass die richtigen Personen zum richtigen Zeitpunkt auf die richtigen Ressourcen zugreifen können, kritische Daten bei der Übertragung oder Speicherung geschützt sind, aufkommende Bedrohungen erkannt werden und Schutzmechanismen im gesamten IT-Umfeld implementiert sind.

## Weitere Informationen

Wenn Sie mehr über IBM Lösungen für mobile Sicherheit erfahren möchten, wenden Sie sich bitte an den zuständigen IBM Vertriebsbeauftragten oder IBM Business Partner, oder besuchen Sie uns unter: **ibm.com**/mobile-security

Mithilfe von IBM Global Financing (IGF) können Sie die Software, die Ihr Unternehmen benötigt, kosteneffizient erwerben. Wir bieten Kunden individuelle Finanzierungslösungen, die auf ihre geschäftlichen Zielsetzungen abgestimmt sind und ihnen helfen, ihren Cashflow zu verbessern und die Gesamtkosten zu senken. Finanzieren Sie wichtige IT-Anschaffungen mit IGF und verschaffen Sie Ihrem Unternehmen einen Vorsprung. Weitere Informationen finden Sie im Internet unter: **ibm.com**/financing/de/

## Über die Autoren

**Darren Argyle, *CISSP CISM***
IBM Global Security Solutions Leader
E-Mail: darren.argyle@uk.ibm.com
twitter.com/D_Argyle

**Vijay Dheap**
IBM Global Product Manager for Mobile Security
IBM Master Inventor
E-Mail: vdheap@us.ibm.com
twitter.com/dheap

[1] Alex Cocotas, „Smartphone Market Forecast: Sales Will Exceed 1.5 Billion Units a Year by 2016“, *BI Intelligence*, Februar 2012. http://articles.businessinsider.com/2012-02-29/research/31109566_1_smartphones-pc-sales-mobile-phone-sales

[2] Forrester Research, „Mobile is the New Face of Engagement“, Februar 2012. http://www-935.ibm.com/services/us/igs/secure-mobility-infographic.html

[3] Michael Finneran, „2012 State of Mobile Security“, *InformationWeek*, Mai 2012. http://reports.informationweek.com/abstract/21/8792/security/research-2012-state-of-mobile-security.html

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
Germany
**ibm.com**/de

IBM Österreich
Obere Donaustrasse 95
1020 Wien
**ibm.com**/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
**ibm.com**/ch

Die IBM Homepage finden Sie unter: **ibm.com**/de



WGW03012-DEDE-01