Verwenden von Android™ im Unternehmen

Wer diese Publikation lesen sollte

Dieses Whitepaper ist bestimmt für CIOs, CISOs, VPs oder Leiter des IT-Betriebs, Leiter oder Manager der Mobilitätsstrategie, Mobilitätsarchitekten und Manager von Mobilitätsprogrammen. Diese Publikation bietet einen Überblick über die Herausforderungen im Zusammenhang mit der Verwaltung von Android-Geräten, zeigt in Momentaufnahmen, wie Unternehmen heute mit Android umgehen, und gibt eine kurze Übersicht über die unterschiedlichen Optionen, die IT-Abteilungen zur Verfügung stehen, um Android im Unternehmen souverän einzusetzen.

Symantec

Inhalt

Einführung

Nicht nur Verbraucher verwenden immer mehr Android-Geräte

Auch in Unternehmen spielen mobile Geräte und Apps heute eine immer größere Rolle. Die Einführung mobiler Geräte und Apps erfolgt möglicherweise jedoch noch schneller, als vielen Unternehmen bewusst ist. Mobile Geräte und Apps sind vielleicht schneller und einflussreicher als jede andere Technologie in Unternehmen eingedrungen. Laut der IDC-Publikation „Mobile World Congress 2014: The Enterprise Mobility Perspective“ ist „das dominierende Merkmal der Mobilität in Unternehmen bisher ihre Verbrauchersteuerung (Consumerization). Smartphones, Apps, mobiles Breitband, persönlicher Cloud-Speicherplatz und soziale Netzwerke verändern zusammen den Alltag der Verbraucher. Verbraucher bringen diese Vorteile auch in ihr Arbeitsleben mit, und die IT-Abteilungen von Unternehmen arbeiten daran, mit den Auswirkungen in Bereichen wie Datensicherheit, rechtliche Verantwortung und Telekommunikationskosten umzugehen.“[1]

Dies ist eine weltweite Bewegung. Da Unternehmen erkennen, dass Mitarbeiter häufig auf selbst gewählten Geräten am produktivsten sind, wächst BYOD (Bring Your Own Device) weltweit. In Regionen oder Branchen, in denen BYOD aufgrund von Datenschutzbedenken, Vorschriften und kulturellen Unterschieden langsamer wächst, bemühen sich Organisationen, ihren Mitarbeitern eine Auswahl an Geräten anzubieten – auch bekannt als CYOD-Modell (Choose Your Own Device). Als Open Source-Plattform stehen Android-Geräte in unterschiedlichen Preisklassen zur Verfügung, darunter attraktiv günstige Optionen sowohl für Verbraucher als auch für kostenbewusste Unternehmen, die ihren Mitarbeitern betriebseigene Geräte zur Verfügung stellen.

Android dominiert den Verbrauchermarkt mit einem weltweiten Marktanteil von 78,4 % im Jahr 2013, was eine Steigerung um 68 % gegenüber dem Vorjahr bedeutet.[2] Am Unternehmensmarkt sieht es anders aus. Die bevorzugte mobile Plattform scheint hier iOS zu sein, vor allem für Geräte im Besitz von Unternehmen.[3] Android gewinnt jedoch auch am Unternehmensmarkt an Boden.

Für die nächsten Jahre erwarten Analysten das Wachsen von zwei Trends mit enormen Auswirkungen auf die IT-Sicherheit in Unternehmen: eine stärkere Akzeptanz von BYOD in Ländern außerhalb von Nordamerika und eine größere Marktdurchdringung durch Android in Nordamerika und anderswo. Laut IDC werden sogar 58 % aller in Nordamerika ausgelieferten Android-Geräte zukünftig für Unternehmenszwecke verwendet werden; in der Region Asien-Pazifik werden diesbezüglich 45 % erwartet.[4] Die Einführung von Android als kostengünstige Option für Geräte im Besitz von Unternehmen wird vor allem in Regionen oder Branchen mit wirtschaftlichem Abschwung zunehmen; die geringere Bereitschaft zu BYOD außerhalb von Nordamerika kann jedoch die Einführungszahlen für Android insgesamt möglicherweise dämpfen.

Weltweit wird prognostiziert, dass sich beide Trends verstärken. Laut seiner aktuellen Publikation „Worldwide Business Use Smartphone 2013-2017 Forecast and Analysis“ erwartet IDC, dass der Anteil der Android-Mobiltelefone an den Geräten, die an Unternehmen als verantwortliche Empfänger geliefert werden, von ca. 20 % im Jahr 2013 auf über 50 % im Jahr 2017 ansteigen wird. Für denselben Zeitraum wird erwartet, dass Lieferungen an Mitarbeiter als verantwortliche Empfänger von 18,5 % auf 25,7 % ansteigen werden.[5]

Beim Marktanteil für dieses Segment der Mitarbeiter als verantwortlichen Empfänger ist Android führend mit fast 60 % des Marktes im Jahr 2012, und es wird prognostiziert, dass der Gesamtanteil Ende 2017 bei ca. 75 % liegen wird.[6] Für Unternehmen ist die Botschaft deutlich: Da der größere Anteil der Smartphone-Verwendung in der Verantwortung der Mitarbeiter liegt – in anderen Worten: BYOD – wird die Bedeutung von Android für die Unternehmens-IT noch steigen.

1- IDC, „Mobile World Congress 2014: The Enterprise Mobility Perspective“, Dokumentnr. LM55W, März 2014
2- Gartner, „Market Share: Mobile Phones by Region and Country 4Q13 and 2013“, Dokumentnr. 2665415, Februar 2014
3- IDC, „Worldwide Business Use Smartphone 2013–2017 Forecast and Analysis“, Dokumentnr. 241599, Juni 2013
4- IDC, „Worldwide Business Use Smartphone 2013–2017 Forecast and Analysis“, Dokumentnr. 241599, Juni 2013
5- IDC, „Worldwide Business Use Smartphone 2013–2017 Forecast and Analysis“, Dokumentnr. 241599, Juni 2013
6- IDC, „Worldwide Business Use Smartphone 2013–2017 Forecast and Analysis“, Dokumentnr. 241599, Juni 2013

Die Herausforderungen für Unternehmen als Pioniere im „Wilden Westen“

Die wachsende Bedeutung von Android für Unternehmen wird von Tag zu Tag deutlicher. Die Open Source-Plattform Android bietet den Vorteil einer großen Auswahl an Anbietern und Geräten. Dies kann zu wesentlichen Kosteneinsparungen verhelfen, was sowohl für Unternehmen als auch für Endbenutzer attraktiv ist. Leider hat Android auch den Ruf des „Wilden Westens“, der die Akzeptanz stören kann. Das Versprechen erhöhter, erschwinglicher Produktivität kann durch eine Reihe von Herausforderungen geschmälert werden, wie Fragmentierung der Plattform, mehrere App-Marktplätze und eine wachsende Bedrohungslandschaft.

Fragmentierung der Plattform: Zu allererst bedeutet jedes Plattform-Upgrade, dass mehrere Betriebssystemversionen gleichzeitig existieren. Laut OpenSignal kamen bei einer Untersuchung von 682.000 Android-Geräten 11.868 unterschiedliche Versionen zum Vorschein, während es im Vorjahr noch 3.997 waren.[7] Während iOS durch die einzigartige Steuerung von Apple gezähmt wird, hat sich die Open Source-Plattform von Android – die einen Segen für Verbraucher und Gerätehersteller bedeutet – auch als Fluch für Unternehmen herausgestellt. Statt nur eine Handvoll Image-Varianten muss die IT viele Dutzend Android-Images sichern, die sich nach Marke und sogar nach Mobilfunk-Netzanbieter unterscheiden.

Aufgrund dieses Open Source-Modells kann es schwierig sein, für alle Geräte zeitnah Patches zu erhalten. Um auf dem aktuellen Stand zu bleiben, muss die Unternehmens-IT Upgrades von einer langen Kette großer Unternehmen hinterherlaufen, die nicht unbedingt ein Interesse daran haben, kostenlose Software-Updates zur Verfügung zu stellen. Aus ihrer Sicht ist es kaum sinnvoll, Kunden mit älteren Geräten länger zu unterstützen, wenn sie neue Modelle verkaufen könnten. Daher gibt es eine breite Benutzerbasis, die ältere Android-Versionen verwendet. Diese Benutzer können neue Funktionen nicht nutzen, die Google einführt (außer, wenn sie ein neues Gerät kaufen), und sind aufgrund von Bugs und Schwachstellen im Code anfällig für Malware und Datendiebstahl. Ein Beispiel aus jüngster Zeit ist der Heartbleed-Ausbruch.

Mehrere App-Marktplätze: Jede iOS App wird über einen einzigen App-Marktplatz bereitgestellt, den Apple® App Store. Apple kontrolliert die Apps, bevor sie zur Verfügung gestellt werden. Dies bietet ein gewisses Maß an Zuverlässigkeit. Die große Zahl offizieller App Stores und Stores in der Grauzone plus die Möglichkeit, dass der Endbenutzer Android-Apps von einem lokalen Gerät auf ein anderes überträgt (Sideloading), trägt dem Markt der Android-Apps eine unwillkommene Ebene von Unvorhersagbarkeit ein. Während Google über ein automatisiertes System verfügt, das Apps in seinem Google Play™ Store scannt, kontrollieren viele andere Android-App-Marktplätze die Apps möglicherweise nicht. Einfach gesagt haben Unternehmen keine Möglichkeit zu erfahren, wo und wie ihre Endbenutzer ihre Apps beziehen.

Wachsende Bedrohungslandschaft: Von 2012 auf 2013 nahm die Android-Malware im mobilen Raum um 712 % zu. Im Bericht „Internet Security Threat Report: 2014“ stellten Forscher von Symantec™ fest, dass im Jahr 2013 jede Malware-Familie 57 Varianten umfasste, während es 2012 erst 38 waren. Allein mobile Geräte mit Android wurden von 3.262 Malware-Varianten heimgesucht. Außerdem ist es bemerkenswert, dass Malware für mobile Geräte im Jahr 2013 fast ausschließlich auf Android abzielte.[8] Selbst „legitime“ Apps stellen keine Sicherheitsgarantie dar; die Zunahme an Grayware bedeutet, dass Verbraucher häufig Apps verwenden, die zwar grundsätzlich legitim sind, aber ihre Grenzen überschreiten können, um Daten – einschließlich vertraulicher Daten – auf dem Gerät zu sammeln, ohne dass das Unternehmen dies genehmigt hat oder der Benutzer davon weiß. Auch wenn noch kein Unternehmen eine große IT-Sicherheitsverletzung über ein mobiles Gerät oder eine App gemeldet hat, stellen Schwachstellen bei Apps eine Sicherheitsbedrohung dar, die unvermeidlich zur Kompromittierung von Daten auf den Geräten der Endbenutzer führen wird – und neue Einfallstore für gezielte Angriffe auf Unternehmen öffnen wird.

7- OpenSignal, „Android Fragmentation Visualized“, Juli 2013, http://opensignal.com/reports/fragmentation-2013/
8- Symantec, „Internet Security Threat Report: 2014“, April 2014

Reaktionen von Unternehmen auf Android

Auch wenn die Wachstumsstatistiken dramatisch sind, wird die wahre Android-Saga an der Basis erzählt und gelebt – in Unternehmen, die ihre Mobilitätsoptionen abwägen. Unternehmen, die Android einführen, stehen zwar alle vor den gleichen Herausforderungen; die Reaktionen ihres Managements hängen jedoch von der Region, der Branche und den individuellen Anforderungen des jeweiligen Unternehmens ab. Es folgen Momentaufnahmen tatsächlicher Projekte mit Android in Unternehmen, einschließlich ihrer Ziele, ihrer Frustrationen und ihrer Bemühungen, ein vertretbares Gleichgewicht zwischen Produktivität und Sicherheit zu finden.

Flexibilität in der Region Asien-Pazifik: Versicherung in Hongkong erweitert ihre Reichweite auf sichere Weise

Kunden sind nicht bereit zu warten – das ist die Lektion, an die ein Versicherer in Hongkong bei der Analyse seiner Mobilitätsoptionen vor allem dachte. Um die Anforderungen seiner Vertreter an Geschwindigkeit und Flexibilität zu erfüllen, entschied der Versicherer, die Geräteauswahl nicht zu beschränken, sondern vertrauliche Daten in eine „Sandbox“ einzuschließen, indem er seine Versicherungs-Apps in einem Sicherheitsschutz versiegelte. Indem der Versicherer seine Apps versiegelt, statt Geräte zu beschränken, kann er Steuermechanismen für die Sicherheit auf App-Ebene implementieren, sodass das Unternehmen Android verwenden und die Herausforderungen umgehen kann, die durch das zugrunde liegende Betriebssystem und die Geräteverwaltungs-APIs entstehen, die es möglicherweise nicht unterstützt.

Wachsender Trend in EMEA: Nutzung der Offenheit von Android zum Vorteil des Unternehmens

In Europa ist die Marktdurchdringung von Android im Allgemeinen größer als in Nordamerika; mit Marktanteilen von 50–60 % liegt sie weit vor der aktuellen Position von iOS oder Microsoft®.[9] Der wichtigste Faktor? Die Kosten. Da BYOD in dieser Region zögerlicher eingeführt wird, stellen Organisationen ihren Mitarbeitern Android-Geräte bereit. In Ländern, die der wirtschaftliche Abschwung besonders hart getroffen hat, wie Spanien und Italien, sind kostengünstige Android-Optionen, wie die von Vodafone, sehr beliebt.

Aber Kosten sind nicht der einzige Faktor. Einige große Systemintegratoren mit wichtigen Behördenverträgen haben die Offenheit von Android zu ihrem Vorteil gewendet und individuelle Versionen des Betriebssystems entwickelt, die ihnen mehr Kontrolle über die Sicherheit ermöglichen. Andere, wie ein europäisches Unternehmen mit Tausenden von internationalen Vertriebsmitarbeitern, haben begonnen, ihre eigenen Apps für die Kontrolle über vertrauliche Daten zu entwickeln. In beiden Fällen wird die Notwendigkeit empfunden, den Schutz von der Geräteebene auf die Anwendungsebene zu verschieben, auf der er unabhängig vom Benutzerverhalten angewendet werden kann. Um Daten in Apps zu sichern sowie um Datenverkehr zu geschützten Gateways und durch diese zu leiten, beginnen Unternehmen, App Wrapping als eine zukunftsfähige Ergänzung zu den Steuermechanismen für das Mobile Device Management (MDM) zu sehen, die sie bereits anwenden.

Erfolgsstory in Nordamerika: Gesundheitsdienstleister erweitert Zugriff für Ärzte über versiegelte Apps

Ein großer, in ganz Kalifornien agierender Gesundheitsdienstleister hat sich für iOS als die mobile Plattform entschieden, die er für sein Pflege- und sonstiges Personal akzeptiert.

Dieser Dienstleister arbeitet jedoch auch mit zahlreichen Vertragsärzten zusammen, die eine Reihe von Android-Geräten bevorzugen. Der Dienstleister hat sich für eine Vorgehensweise entschieden, die die aktuellen Sicherheitsrichtlinien des Netzwerks aufrechterhält und zugleich Vertragsärzte auf sichere Weise einbindet. Da die E-Mail- und Patientendaten-Anwendungen des Netzwerks durch App Wrapping geschützt und über das Symantec App Center zur Verfügung gestellt werden, können Vertragspartner alle gewünschten mobilen Geräte verwenden, während das Gesundheitsnetzwerk zugleich seinen bewährten Umgang mit der IT-Sicherheit wahrt und konsistente Richtlinien für Sicherheit und Datenschutz aufrechterhält.

Individuelle Herausforderungen der Branche: Einzelhändler erwägt noch Optionen

In Nordamerika hat ein großer Einzelhändler einen hybriden Ansatz für mobile Plattformen für die Mitarbeiter an seinem Hauptsitz eingeführt: strikt nur iOS auf Geräten, die dem Unternehmen gehören, und Gestattung gemischter Plattformen auf Geräten in

[9] IDC, „Worldwide Business Use Smartphone 2013–2017 Forecast and Analysis“, Dokumentnr. 241599, Juni 2013

Mitarbeiterbesitz, sofern auf den Geräten genehmigte Steuermechanismen des MDM und Mobile Application Management (MAM) installiert sind. Das Unternehmen hat sich für iOS als Standard für seine Geräte entschieden, da „Apple höhere Konsistenz bietet“. In der BYOD-Umgebung sind Android-Geräte mit Rooting nicht zugelassen.

Android macht weniger als 20 % der BYOD-Umgebung des Einzelhändlers aus. Der Einzelhändler ist der Meinung, dass dies vor allem deshalb der Fall ist, weil viele Benutzer mit Apple-Geräten vertraut sind und sie komfortabel finden. Weniger Personen sind über Android informiert; und sie sehen Android möglicherweise als weniger benutzerfreundlich an, weil sie nicht wissen, welche Verbesserungen Google an diesem Betriebssystem vorgenommen hat.

Wie andere Unternehmen findet der Einzelhändler die Fragmentierung der Open Source-Plattform Android schwer zu verwalten und macht sich Sorgen um potenzielle Malware-Infektionen aus dem „Wilden Westen“ der App Stores und des Sideloading.

Viele Jahrgänge in den Griff bekommen: Eine Weinkellerei nimmt Android in ihre Auswahl mobiler Geräte auf

Für eine große Kellerei in Kalifornien hat die Unsicherheit hinsichtlich Android einen einfachen Grund. „Wir sind kein IT-Unternehmen“, sagt ihr Mobilitätsmanager. „Wir möchten nicht in eine große Anzahl Plattformen investieren.“ Die Kellerei hat den Eindruck, dass das Open Source-Modell der Hauptfaktor für die Fragmentierung bei Android ist. „Jedes neue Gerät hat ein neues Betriebssystem“, bemerkt der Manager. Die vielen Variationen von Android-Geräten fordern der IT-Abteilung der Kellerei eine große Lernkurve ab. „Wenn Benutzer einen Supportfall eröffnen“, sagt der Manager, „erwarten sie, dass die IT über das nötige Expertenwissen verfügt.“

Daher verwendet die Kellerei für die Mobilität überwiegend iOS, mit ein paar Tropfen BlackBerry und nur einem Hauch von Android. Da Android jedoch bei den Führungskräften so beliebt ist, muss die Kellerei Android-Benutzer berücksichtigen. Um dies zu erreichen, hat sie die Optionen eingeschränkt. „Wir verlangen, dass alle neuen Android-Geräte von Samsung stammen“, sagt der Manager. Indem die Kellerei MDM anwendet und eine App zum Schutz vor Bedrohungen mobiler Geräte installiert, kann sie die Mischung von Geräteoptionen verwalten, die ihre Mitarbeiter bevorzugen. Der Manager fügte hinzu, dass Lösungen, mit denen sich IT-Organisationen weniger darum kümmern müssten, was die zugrunde liegenden Betriebssysteme unterstützen, Android schmackhafter machen würden.

Bewältigen der Android-Herausforderung: Kurze Übersicht über Optionen für Unternehmen

In einer Umgebung, in der alles im Fluss ist, erwarten Unternehmen fundierte Entscheidungen, und die IT möchte mit flexiblen Optionen reagieren. In der folgenden Liste ist die Unternehmens-/Android-Landschaft zusammengefasst, beginnend mit der restriktivsten Option.

1) Nutzung von Android verbieten oder beschränken

In Unternehmen, die überwiegend selbst für die Geräte verantwortlich sind, sowie an Märkten, an denen die meisten Verbraucher iOS verwenden, ist es noch möglich, Einschränkungen für die Einführung von Android aufzuerlegen. Mit dieser Methode ist das Unternehmen jedoch auf teurere Geräte angewiesen, und die Flexibilität für die Endbenutzer wird begrenzt. Um die Komplexität zu umgehen, die durch die Fragmentierung entsteht, erwerben oder akzeptieren manche Unternehmen Android nur von einigen wenigen OEMs und/oder Service-Providern. Durch Verwendung einer begrenzten Anzahl Images kann die IT mehr Kontrolle über Geräte-Assets ausüben.

2) Android um MDM ergänzen

MDM hinzuzufügen, ist vielleicht die am weitesten verbreitete Vorgehensweise von Unternehmen, die Android-Geräte verwenden. Das Unternehmen erhält so einige grundlegende Schutzmechanismen, einschließlich der Durchsetzung von PINs und Kennwörtern für Geräte, Fernsperrung/-löschung von Geräten, Datenverschlüsselung auf dem Gerät und Erkennung von Rooting. Während MDM grundlegende Sicherheit bietet, schützt es nicht die Daten, wenn das Gerät gehackt oder über Malware oder gestohlene IDs darauf zugegriffen wird. Sich ausschließlich auf MDM in allen Bereichen des Unternehmens zu verlassen, bedeutet außerdem, dass die IT sich möglicherweise mit zu vielen unterschiedlichen Geräten abmühen muss.

3) Bedrohungsschutz hinzufügen

Auch Geräte mit MDM sind noch anfällig für Malware, Datenschutzrisiken und andere Bedrohungen. MDM um einen Bedrohungsschutz zu ergänzen, schützt nicht nur vor Apps, die ihre Grenzen überschreiten, sondern verhindert auch, dass infiltrierte Geräte zu Backdoors werden, über die das Eindringen in Unternehmenssysteme möglich ist. Ein effektiver Bedrohungsschutz bedeutet eine „Impfung“ gegen Malware und Grayware für mobile Geräte; er fängt den Zugriff auf betrügerische Websites und die Kommunikation mit solchen Websites ab; er bietet Verteidigung gegen Apps, die zu viele Daten sammeln, sowie gegen Remote-Scanning und -Löschung von Geräten; und er meldet dem Unternehmen Bedrohungen für mobile Geräte.

4) Mit MAM Schutz auf die App-Ebene bringen

Statt zu versuchen, zahlreiche Plattformen in den Griff zu bekommen – oder Steuermechanismen aufzuerlegen, die die Privatsphäre einschränken – entscheiden sich immer mehr Unternehmen für MAM-Lösungen, die Richtlinien-Steuermechanismen auf Ebene der Apps (statt auf Ebene des Geräts) bereitstellen. Durch Anwenden von Richtlinien auf einzelne Apps – ganz gleich, ob sie intern entwickelt wurden, aus externen Stores oder von Dritten stammen – kann die IT Unternehmensdaten sichern, ohne das Benutzererlebnis zu verschlechtern oder den Datenschutz für die Benutzer zu verletzen. Wenn die Kontrolle auf die App-Ebene verschoben wird, muss die IT sich weniger Sorgen darum machen, was das zugrunde liegende Betriebssystem enthält. Eine umfassende MAM-Lösung ermöglicht die Anwendung granularer Richtlinien pro App ohne Entwicklerressourcen, die dynamische Aktualisierung von Anwendungsrichtlinien, Kontrolle über die Bereitstellung mobiler Apps über einen App Store des Unternehmens, die Überwachung der App-Leistung und -Nutzung sowie die Fernlöschung von Apps und Daten ohne Beeinträchtigung der privaten Daten und Apps der Endbenutzer.

Fazit

Es könnte an der Zeit sein, Android willkommen zu heißen

Bis vor Kurzem haben Unternehmen sich im Wesentlichen von Android ferngehalten, auch wenn sie mobile Geräte und Apps eingeführt haben. Der wachsende Marktanteil von Android und der weltweite Siegeszug der Verbrauchersteuerung (Consumerization) bedeuten jedoch, dass Android mittlerweile zu groß ist, um ignoriert zu werden.

Während die Fragmentierung und der relativ offene Markt für Android-Apps weiterhin Sorgen bereiten, verfügen Unternehmen heute über ausgeklügelte Sicherheitsoptionen, wie herkömmliches MDM, fortgeschrittenen Bedrohungsschutz und Management mobiler Apps, mit denen Android weniger bedrohlich ist – und somit eine lohnendere Mobilitätsoption für die Steigerung der Produktivität zu geringeren Kosten darstellt.

Wie die praktischen Beispiele in dieser Publikation zeigen, können und sollten Unternehmen Android im Rahmen ihrer Mobilitätsstrategien in Betracht ziehen. Viele Unternehmen sind jedoch nicht darauf vorbereitet, dies allein zu erreichen. Und nur wenige IT-Anbieter verfügen über das umfangreiche Fachwissen, die breite Produktpalette und die bewährten Erfolge bei der Sicherheit, die erforderlich sind, um Android souverän zu verwalten. Als Unternehmen, das eine umfassende Lösung für alle Anforderungen an die Verwaltung und Sicherheit der Mobilität in Unternehmen anbietet, steht Symantec als vertrauenswürdiger Partner zur Verfügung, mit dem Sie in diesem Bereich auf Produktivität und Schutz hinarbeiten können.

Um mehr darüber zu erfahren, wie Sie Android im Unternehmen souverän verwenden können, besuchen Sie www.symantec.com/mobility.

Über Symantec

Die Symantec Corporation (NASDAQ: SYMC) unterstützt als Experte für Informationsschutz Anwender, Unternehmen und Regierungen dabei, die Möglichkeiten neuer Technologien jederzeit und überall zu ihrem Vorteil zu nutzen. Gegründet im April 1982 und ein Fortune 500-Unternehmen, betreibt Symantec eines der weltweit größten Data Intelligence Netzwerke und stellt führende Sicherheits-, Backup- und Availability-Lösungen überall dort bereit, wo sensible Informationen gespeichert, zugänglich gemacht und geteilt werden. Für das Unternehmen sind 21.500 Beschäftigte in mehr als 50 Ländern tätig. 99 Prozent der Fortune 500-Firmen sind Kunden von Symantec. Im Fiskaljahr 2013 verzeichnete das Unternehmen Einkünfte von 6,9 Milliarden US Dollar. Erfahren Sie mehr unter www.symantec.com. Sie können auch über folgende Website mit Symantec in Verbindung treten: go.symantec.com/socialmedia.

Unsere Geschäftsstellen und Kontaktnummern in den jeweiligen Ländern finden Sie auf unserer Website.

Symantec (Deutschland) GmbH
Hauptniederlassung
Wappenhalle, Konrad Zuse Platz 2-5
81829 München
Telefon: +49 (0) 89 / 94302 - 100
Telefax: +49 (0) 89 / 94302 - 550
www.symantec.com