SOPHOS

Vier Bedrohungen für die Datensicherheit im Post-PC-Zeitalter

BYOD-Verwaltung, Mobilgeräte, Cloud Storage und soziale Netzwerke

Von Gerhard Eschelbeck, Chief Technology Officer, und
David Schwartzberg, Senior Security Engineer

40 Jahre lang bestimmte der PC, wie wir arbeiten. Heute jedoch wollen wir überall und jederzeit die aktuellsten Informationen abrufen können. Diese Anforderungen sind es, die neue Gerätetypen wie Smartphones und Tablets erfolgreich gemacht haben. Sie läuten damit das Post-PC-Zeitalter ein. Und das bringt gleich vier neue Bedrohungen für die Datensicherheit mit: BYOD (Bring Your Own Device), Mobilgeräte, Cloud Storage und soziale Netzwerke. Dieses White Paper informiert Sie über diese neuen Bedrohungen und zeigt Ihnen, wie Sie am besten damit umgehen.

Was ist das Post-PC-Zeitalter?

Die moderne Technik hat unsere Möglichkeiten des Datenzugriffs erheblich erweitert und neue Gerätetypen hervorgebracht, die den klassischen PC ablösen. Tim Cook, der CEO von Apple, hat diese Entwicklung mit dem Begriff „Post-PC-Ära" umschrieben, und Branchenanalysten geben ihm da recht. Untersuchungen von JP Morgan und der Gartner Group erwarten, dass die Zahl der 2012 verkauften Smartphones (657 Mio.) die der verkauften PCs (368 Mio.) um fast das Doppelte übertreffen wird.[2] IDC geht davon aus, dass die Verkaufszahlen von Tablet-PCs in diesem Jahr auf 106 Mio. steigen werden. Und Forrester Research schätzt, dass die meisten Benutzer ab 2016 in erster Linie Tablet-PCs nutzen werden.[3]

Wir erreichen damit eine neue Stufe der technischen Entwicklung, in der Benutzer bequemer und unabhängiger auf Daten zugreifen können als je zuvor. Allerdings ruft das auch neue Probleme auf den Plan. Schützenswerte Daten und geistiges Eigentum sehen sich vier neuen Bedrohungen ausgesetzt. Die folgenden vier Abschnitte stellen Ihnen die Techniken der Post-PC-Ära vor und zeigen die damit einhergehenden neuen Gefahren auf. Sie erklären auch, wie Sie damit am besten umgehen.

1. **Bring Your Own Device (BYOD)**
2. **Mobilgeräte**
3. **Cloud Storage**
4. **Soziale Netzwerke**

1. „The post-PC world is real and it's here", The Globe and Mail, http://www.theglobeandmail.com/technology/gadgets-and-gear/the-post-pc-world-is-real-and-its-here/article4098023/
2. „Smartphone, tablet sales outpace PC growth", Thomson Reuters, http://graphics.thomsonreuters.com/12/02/GLB_TECHMKTB0212_SC.html
3. „Tablets will be preferred devices by 2016", Computerworld, http://www.computerworld.com/s/article/9226890/Tablets_Will_Be_Preferred_Devices_by_2016

Bedrohung Nummer 1: BYOD

Das Kürzel BYOD (Bring Your Own Device) beschreibt den Trend, dass Mitarbeiter heute immer öfter ihre eigenen Geräte in das Unternehmen mitbringen und damit auch auf Server zugreifen. Sie könnten das einfach schriftlich verbieten – doch das löst das Problem nicht, es verstärkt es stattdessen: Die Mitarbeiter werden nämlich trotzdem eigene Geräte mitbringen, und diese entziehen sich dann weiterhin Ihrer Kontrolle und wichtigen Sicherheitsrichtlinien.

Als IT-Manager betrachten Sie den BYOD-Trend am besten wie eine neue Technik. Reagieren Sie einfach darauf, indem Sie die Bereitstellung planen, umsetzen und kontrollieren.

Stellen Sie sich folgende Fragen:

1. **Wer ist Eigentümer des Geräts?** Hier hat sich in letzter Zeit viel verändert. Früher gehörten die Geräte fast immer dem Unternehmen. Heute sind die Benutzer oft auch die Besitzer, zumindest im Fall BYOD.

2. **Wer verwaltet das Gerät?** Früher war das fast immer das Unternehmen selbst. Heute übernimmt diese Aufgabe immer öfter auch der Anwender.

3. **Wer sichert das Gerät?** Der Benutzer sieht sich da nur selten in der Verantwortung, obwohl ihm das Gerät gehört. Und das, obwohl die auf dem Gerät gespeicherten Daten zum schützenswerten Unternehmenseigentum gehören.

Auf Basis der Antworten können Sie die Risiken und Vorteile von BYOD besser einschätzen.

Je nach Unternehmenskultur und rechtlichen Rahmenbedingungen können Sie für Ihr Unternehmen sehr flexibel entscheiden, in welchem Umfang BYOD begrüßenswert erscheint. Einigen Firmen ist das Risiko möglicherweise zu groß, sie entscheiden sich bewusst gegen ein BYOD-Programm.

Wegen Datensicherheitsbedenken verbot IBM im Mai 2012 seinen 400.000 Mitarbeitern zwei sehr beliebte Anwendungen. Zum einen den Cloud-Storage-Dienst Dropbox, mit dem sich Dateien sowohl lokal als auch im Web speichern und transportieren lassen. Zum anderen Siri, die persönliche Assistentin des Apple iPhone. Siri erkennt gesprochene Fragen und sendet hierfür Tonaufnahmen an Apple-Server, die sie in Text umsetzen. Außerdem kann Siri per Spracheingabe SMS-Nachrichten und E-Mails erstellen. Diese Nachrichten könnten vertrauliche, geschützte Daten enthalten.[4]

Der Erfolg Ihres eigenen BYOD-Programms hängt am Ende davon ab, ob Ihre Mitarbeiter bereit sind, ihre privaten Geräte nur im Rahmen der Unternehmensvorschriften zu verwenden. Ihre Sicherheitsrichtlinien sollten daher genau festlegen, ob und wie BYOD in Ihrem Unternehmen erlaubt ist.

Nur so sind Sie in der Lage, Sicherheitsbestimmungen auf Geräteebene durchzusetzen und das geistige Eigentum des Unternehmens auch dann zu schützen, wenn Geräte verloren gehen oder gestohlen werden.

4 „IBM: Sorry, Siri. You're not welcome here", InformationWeek, http://www.informationweek.com/news/security/mobile/240000882

So sichern Sie BYOD-Geräte

Zur Sicherung Ihrer BYOD-Geräte gehen Sie am besten genauso vor wie bei den bereits vorhandenen Geräten in Ihrem Netzwerk. Am wichtigsten sind folgende Sicherheitsmaßnahmen:

- Durchsetzung strenger Kennwörter auf allen Geräten
- Virenschutz und Data Loss Prevention (DLP)
- Vollständige Verschlüsselung von Festplatten, Wechseldatenträgern und Cloud Storage
- Mobile Device Management (MDM), u.a. zum Fernlöschen vertraulicher Daten, falls ein Gerät verloren geht oder gestohlen wird
- Application Control, um unerwünschte Anwendungen zu blockieren

Setzen Sie Verschlüsselung sowohl bei der Übertragung als auch bei der Speicherung von Daten ein. Je sicherer die auf Geräten verwendeten Kennwörter sind, desto besser schützen Sie damit die Daten vor Unbefugten. Wird trotzdem mal ein Gerätekennwort geknackt, stellt die Verschlüsselung der Daten auf dem Gerät eine zweite Sicherheitsbarriere dar. Ein Hacker müsste auch diese überwinden, um Daten zu stehlen.

Machen Sie Ihre Mitarbeiter mit der Idee mehrstufiger Schutzebenen bekannt. Sie werden schnell einsehen, wie und warum sie damit ihre persönlichen Geräte am Arbeitsplatz absichern. Machen Sie deutlich, dass der Benutzer Verantwortung für seine Daten übernimmt, indem er sein Gerät mit einem Kennwort schützt.

Kennwort- und Virenschutz alleine reichen jedoch nicht. Führen Sie für BYOD-Geräte zusätzlich ein gewisses Maß an Application Control ein. Mitarbeiter sollten auf Anwendungen, die sie im LAN nutzen, auch aus der Ferne zugreifen können, z.B. über eine VPN-Verbindung.

Ein erfolgreiches BYOD-Programm gestattet Benutzern, auch außerhalb der Arbeitszeiten produktiv zu sein. Wenn sie nicht arbeiten, sollen sie trotzdem problemlos Spaß haben können, etwa Statusmeldungen posten oder sich mit einem Spiel vergnügen.

Wie auch immer Ihre BYOD-Richtlinien aussehen: Stellen Sie sicher, dass diese durchsetzbar sind und die zentrale IT damit Anwendungen remote bereitstellen kann.

Festlegen von Richtlinien und Compliance-Standards

Formulieren Sie offizielle Richtlinien für BYOD. Beziehen sich Ihre Richtlinien ausnahmslos auf alle aktuell verfügbaren Geräte? Möchten Sie die Verwendung privater Geräte auf bestimmte Hardware und Software beschränken? Wie sieht es mit Geräten aus, die in der Zukunft auf den Markt kommen?

Der Markt für mobile Handheld-Geräte entwickelt sich rasant, ständig kommen neue Versionen und Hersteller dazu. Ihre BYOD-Richtlinien sollten sich deswegen schnell und flexibel möglichen Änderungen anpassen können. Halten Sie strategische Richtlinien schriftlich fest, basierend auf dem Stand der Technik von heute und Ihren Erwartungen an die Technik von morgen. Führen Sie außerdem ein System ein, das Ihre schriftlichen Richtlinien durchsetzt und somit Verwaltbarkeit, revisionssichere Modellierung, Steuerung und Sicherheit bietet.

Achten Sie bei der Implementierung darauf, dass die Lösung auch eine Remote-Verwaltung für Geräte beinhaltet. So bleiben Ihre Richtlinien stets relevant und zuverlässig. Das gilt erst recht für Branchen mit strengen Compliance- und Prüfungsstandards.

Ein Einblick in die Mobilfunkverträge Ihrer Mitarbeiter bietet darüber hinaus die Chance, bessere Verträge auszuhandeln und die Kosten zu reduzieren. Die Hotspot- oder Tethering-Optionen der verwendeten Pauschaltarife auszureizen, kann z.B. das Nutzungserlebnis Ihrer Mitarbeiter verbessern. Prüfen Sie, ob Sie mit reinen Datentarifen für persönliche Geräte u.U. besser fahren, als wenn Sie Home Offices mit Fernwahl- und ISP-Tarifen ausstatten.

Die 7 Schritte zu einem BYOD-Sicherheitsplan

BYOD-Programme und Sicherheit schließen sich nicht aus. Es kommt nur auf die richtige Planung an. Die könnte z.B. wie folgt aussehen:

1. Finden Sie heraus, welche Risiken BYOD mit sich bringt.

- Ermitteln Sie, wie diese Risiken Ihr Unternehmen beeinträchtigen könnten.
- Ordnen Sie, wo es geht, jedem Risiko eine Richtlinie zu.

2. Stellen Sie für die Implementierung von BYOD ein Experten-Gremium aus folgenden Mitgliedern zusammen:

- Interessensvertreter des Unternehmens
- Interessensvertreter der IT
- Interessensvertreter des Datenschutzes

3. Entscheiden Sie, wie die Richtlinien für Geräte, die auf Ihr Netzwerk zugreifen, durchgesetzt werden sollen:

- Für Mobilgeräte (Smartphones)
- Für Tablet-PCs (iPad)
- Für Mobilcomputer (Laptops, Netbooks, Ultrabooks)

4. Planen Sie ein Projekt, das folgende Punkte gewährleisten kann:

- Remote-Geräteverwaltung
- Application Control, um unerwünschte Anwendungen zu blockieren
- Richtlinieneinhaltung und Prüfungsberichte
- Daten- und Geräteverschlüsselung
- Erhöhung der Sicherheit von Cloud-Storage
- Bereinigung der Geräte, wenn sie nicht mehr verwendet werden
- Entzug des Gerätezugriffs, wenn der Mitarbeiter das Unternehmen verlässt

5. Vergleichen Sie die Lösungen.

- Berücksichtigen Sie den Einfluss verschiedener Lösungen auf Ihr bestehendes Netzwerk.
- Überlegen Sie sich, wie Sie das bestehende System verbessern können, bevor Sie den nächsten Schritt gehen.

6. Implementieren Sie die Lösungen.

- Beginnen Sie mit einer Pilotgruppe, deren Mitglieder aus den betroffenen Fachabteilungen stammen.
- Erweitern Sie das Pilotprojekt dann nach und nach auf ganze Abteilungen.
- Machen Sie das BYOD-Programm schließlich für alle Mitarbeiter zugänglich.

7. Reevaluieren Sie die Lösungen in regelmäßigen Abständen.

- Berücksichtigen Sie dabei Anbieter und vertrauenswürdige Berater.
- Nutzen Sie Roadmaps, um die nächsten Prüfschritte zu planen.
- Denken Sie an kostensparende Gruppentarife.

Bedrohung Nummer 2: Mobilgeräte

Für die Datensicherheit sind Mobilgeräte stets eine Bedrohung, ganz egal, ob sie Unternehmenseigentum sind oder den Mitarbeitern gehören. Mobile Geräte sind letztlich nur tragbare Computer. Daher sollten Sie sie genauso schützen wie Ihre normalen PCs. Suchen Sie nach Möglichkeiten, die Geräte und die auf ihnen gespeicherten Daten vor unbefugten Zugriffen zu schützen.

Die jährliche Studie des Ponemon Institutes zu den Kosten, die Datenschutzverletzungen in den USA verursachen, schätzte diese 2012 auf durchschnittlich 194 USD (ca. 155 EUR) pro gestohlenem oder verlorenem Datensatz und 5,5 Mio USD (ca. 4,4 Mio. EUR) pro Vorfall.[5] Datenschutzverletzungen durch Angriffe stiegen von 31 % im Jahr 2010 auf 37 % im Jahr 2011. Der Diebstahl von Mobilgeräten verursachte 28 % der Datenschutzverletzungen.[6]

Verschiedene Gremien wachen über die Einhaltung nationaler und globaler Regeln für den Umgang mit Daten. Unternehmen, die Kundendaten auf unverschlüsselten Geräten verlieren, müssen mit Bußgeldern rechnen. Neben Kosten für Kreditprüfungsdienste, Bußgelder und Gerichtsverfahren droht eine Schädigung der Unternehmensreputation.

Bevor Sie BYOD-Geräte in Ihrem Unternehmen zulassen, sollten Sie im Rahmen einer Arbeitsrichtlinie für mobile Mitarbeiter mehrere Faktoren berücksichtigen: Welche zusätzlichen Anwendungen müssen installiert werden? Wie lassen sich Geräte schützen? Wie lässt sich der Netzwerkzugriff sicher gestalten? Und was ist mit den Daten auf dem Gerät?

5. „Cost of data breaches falls for first time in seven years", PC World, http://www.pcworld.com/businesscenter/article/252195/cost_of_data_breaches_falls_for_first_time_in_seven_years.html

6. „Data breach costs drop", InformationWeek, http://www.informationweek.com/news/security/attacks/232602891

7 Tipps zur Sicherung von Mobilgeräten

Ein mobiles BYOD-Programm ist stets ein Balanceakt: Sie erlauben Ihren Mitarbeitern, eigene Geräte für die Arbeit zu verwenden, müssen zugleich aber auf die Sicherheit des Unternehmens achten.

Ihre Mitarbeiter sind dabei die erste und oft auch beste Verteidigungslinie gegen Datendiebstahl. Sie müssen nur verstehen, wie sie ihre Mobilgeräte optimal einsetzen und dabei die enthaltenen, vertraulichen Daten schützen können. Mitarbeiter mit eigenen Geräten müssen die bestehenden Richtlinien befolgen, damit auch das Unternehmen als Ganzes alle gegebenen Vorschriften einhalten kann.

Halten Sie sich an die folgenden sieben Tipps von Sophos und dem Ponemon Institute, um Geräte und die darauf gespeicherten Daten zu schützen.

Tipp 1: Entwickeln Sie eine Unternehmensstrategie für mobile Sicherheit. Beginnen Sie mit der Klassifizierung der Daten auf Mobilgeräten. Dazu gehören regulierte Daten (Kreditkartendaten), nicht regulierte Kundendaten (Einkaufsverlauf, E-Mail-Adressen), nicht regulierte, vertrauliche Unternehmensdaten (IP-Adressen, Geschäftspläne und Finanzdaten) und Mitarbeiterdaten.

Tipp 2: Erstellen Sie umfassende Richtlinien und Leitfäden für alle Mitarbeiter und Auftragnehmer, die Mobilgeräte in Ihrer Arbeitsumgebung verwenden. Führen Sie Sicherheitsverfahren und Richtlinien für eine „vertretbare Nutzung“ (Accepted Use Policy, AUP) ein, mit denen Sie gezielt Risiken einzelner Gerätegruppen angehen. Mitarbeiter sollten darin zu allen Themen Antworten finden: Welche Datentypen sie nicht auf Geräten speichern sollen, wie sie unbedenkliche Anwendungen finden und herunterladen und wie und wo sie den Verlust oder Diebstahl eines Geräts anzeigen.

Tipp 3: Schaffen Sie Verantwortungsbewusstsein. Unternehmen und andere Organisationen sind dazu verpflichtet, ihren Mitarbeitern Richtlinien, Verfahren und Techniken zur Verfügung zu stellen, mit denen sie ihre Mobilgeräte schützen können. Umgekehrt müssen sich Mitarbeiter ihrer wichtigen persönlichen Verantwortung beim Umgang mit Mobilgeräten bewusst sein.

Tipp 4: Schulen Sie Ihre Mitarbeiter in Sachen Sicherheit, damit sie weniger Fehler machen. Belassen Sie es nicht bei der Einführung von Richtlinien und der Kontrolle von Mitarbeitern. Rufen Sie darüber hinaus ein Schulungsprogramm ins Leben. Machen Sie Ihre Mitarbeiter mit den vielen möglichen Sicherheitsrisiken bei Mobilgeräten vertraut.

Tipp 5: Nutzen Sie Application Control, Mobile Device Management (MDM), Patching und andere Systeme, um Hackerangriffe und Malware-Infektionen abzuwehren. Unserer Meinung nach reichen Blacklisting-Methoden nicht aus, um zu kontrollieren, welche Anwendungen Angestellte auf ihre Mobilgeräte herunterladen dürfen. Viele Angriffe auf mobile Geräte nutzen gezielt deren Schwachstellen aus: Stellen Sie daher unbedingt sicher, dass Betriebssysteme und Anwendungen wie Browser, PDF-Reader und Flash-Player stets gepatcht und auf dem neuesten Stand sind.

Tipp 6: Nutzen Sie Funktionen wie Fernlöschung, Mobilgeräte-Verschlüsselung und Diebstahlschutz, um das Risiko von Datenverlusten zu minimieren. Ein verlorenes oder gestohlenes Mobilgerät mit verschlüsselten Daten verursacht deutlich weniger Kosten als eines mit unverschlüsselten. Laut einer Studie des Ponemon Institute vom Mai 2009 summieren sich die finanziellen Folgen eines gestohlenen Laptops auf insgesamt 49.256 USD (ca. 39.325 EUR). Verschlüsselung kann diese Kosten um mehr als 20.000 USD (ca. 16.000 EUR) reduzieren.

Tipp 7: Verschaffen Sie sich einen Überblick über die Datenschutzprobleme bei Mobilgeräten. Wenn personenbezogene Daten von Kunden und Mitarbeitern in unbefugte Hände gelangen, schädigt das den Ruf des Unternehmens. Auch drohen hohe Bußgelder. Untersuchen Sie, über welche Wege die Daten durch das Unternehmen fließen und was das für die Einhaltung von Datenschutzrichtlinien bedeutet.

Umfrage zum Thema mobile Sicherheit 2012

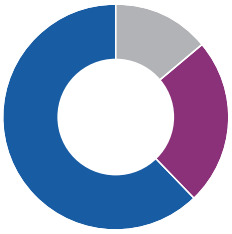
- 62 % der Unternehmen erlauben ihren Mitarbeitern, persönliche Mobilgeräte bei der Arbeit zu verwenden, nur 24 % entwickeln dafür klare Richtlinien.
- 84 % der Befragten geben an, dass der Verlust oder Diebstahl von Mobilgeräten ein großes Sicherheitsproblem darstellt.
- 31 % sehen in mobiler Malware aus öffentlichen App Stores ein großes Sicherheitsproblem.
- 42 % erlauben ihren Mitarbeitern, sich eigene Anwendungen auf Privatgeräte zu installieren, die unbeschränkt auf alle Firmendaten zugreifen können.
- 87 % geben an, dass die Sicherung von Daten auf Mobilgeräten wichtig oder sehr wichtig ist, aber nur 14 % schreiben für Mobilgeräte eine Hardware-Verschlüsselung vor.
- 48 % haben in den vergangenen 12 Monaten ein Mobilgerät mit Firmendaten verloren; 12 % geben an, dass dieser Datenverlust eine öffentliche Stellungnahme erforderlich machte.

Quelle: „2012 State of Mobile Security“ mit den Ergebnissen aus der aktuellen Umfrage zum Thema mobile Sicherheit 2012 von InformationWeek. Im Rahmen dieser Umfrage wurden mehr als 300 Unternehmenstechnologie-Experten befragt. Mit freundlicher Genehmigung von InformationWeek Reports (http://reports.informationweek.com), einem Dienstanbieter für peer-basierte IT-Forschung und -Analyse.

Holen Sie sich weitere Tipps. Laden Sie „7 Tipps zur Absicherung mobiler Mitarbeiter“ von Sophos.com herunter

Erfahren Sie, wie Sophos Mobile Control Ihnen dabei hilft, Ihre Daten zu schützen, Ihre Anwendungen zu verwalten und Compliance-Anforderungen zu erfüllen

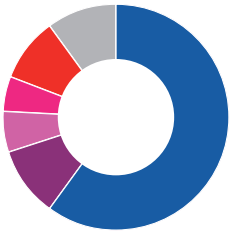
Richtlinien für persönliche Mobilgeräte



Gestatten Ihre Unternehmensrichtlinien den Mitarbeitern, für die Arbeit persönliche Mobilgeräte zu verwenden?

- Ja **62 %**
- Nein, aber wir entwickeln gerade eine neue Richtlinie **24 %**
- Nein, aber wir planen, die Verwendung persönlicher Geräte zu erlauben **14 %**

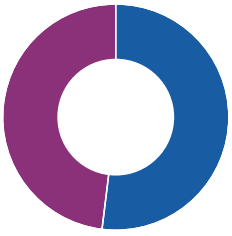
Sicherheitsprobleme bei Mobilgeräten



Wie viele der von Ihnen verwalteten Mobilgeräte einschließlich Laptops verursachen im Laufe eines Jahres Sicherheitsprobleme?

- Weniger als 10 % **60 %**
- 11 % bis 20 % **10 %**
- 21 % bis 30 % **6 %**
- Mehr als 30 % **5 %**
- Wir erfassen keine Kennzahlen zu Sicherheitsproblemen **9 %**
- Weiß nicht **10 %**

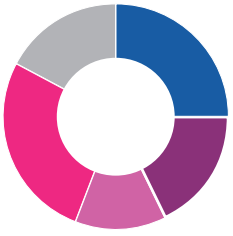
Verlorene Mobilgeräte



Ist Ihnen in den vergangenen 12 Monaten ein Mobilgerät (auch Laptop und Netbook) abhanden gekommen, auf dem Unternehmensdaten gespeichert waren?

- Nein **52 %**
- Ja **48 %**

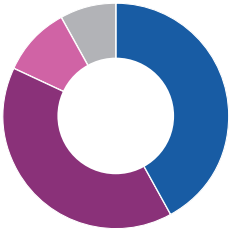
Mobile Device Management



Besitzt Ihr Unternehmen bereits ein Mobilgeräteverwaltungssystem oder plant dessen Einführung?

- Ja, wir haben ein MDM-System **25 %**
- Ja, in den kommenden 12 Monaten **18 %**
- Ja, in den kommenden 24 Monaten **13 %**
- Nein **27 %**
- Weiß nicht **17 %**

Richtlinie zur Verwendung persönlicher Mobilgeräte



Welche der folgenden Aussagen beschreibt am besten Ihre aktuelle oder künftige Richtlinie zur Verwendung persönlicher Geräte?*

- Benutzer können beliebige Geräte in unserem Netzwerk verwenden, sofern sie gewisse Richtlinien einhalten **42 %**
- Benutzer können bestimmte Geräte verwenden und müssen darauf unsere Geräteverwaltungssoftware ausführen **40 %**
- Wir lassen persönliche Geräte ohne jede Einschränkung zu **10 %**
- Sonstiges **8 %**

Daten: Umfrage von InformationWeek zum Thema mobile Sicherheit unter 32 Unternehmenstechnologie-Experten, März 2012

* Grundlage: 278 Befragte in Unternehmen, die eine Richtlinie zur Verwendung persönlicher Mobilgeräte haben oder gerade entwickeln.

Bedrohung Nummer 3: Cloud Storage

Cloud-Storage-Dienste werden immer beliebter– über 50 Millionen Benutzer verwenden sie schon. Der Komfort, den sie bieten, hat allerdings seinen Preis. Werden neue Techniken populär, macht sie das als Angriffsziel interessant.

Cloud-Storage-Anbieter haben beispielsweise vollen Zugriff auf Ihre Daten und bestimmen, wo diese gespeichert werden. Sie als Benutzer kennen hingegen weder die genutzte Infrastruktur noch die darin getroffenen Sicherheitsmaßnahmen. Befindet sich der Cloud-Speicher in einem anderen Land, hat das zudem rechtliche Konsequenzen.

Trotz dieser Risiken steigt die Nachfrage nach Cloud-Storage-Diensten im Arbeitsumfeld immer weiter an. In einer Umfrage in den USA und Großbritannien gaben von 4.000 befragten Arbeitnehmern 66 % an, auch am Arbeitsplatz Dateien über kostenlose Plattformen zu transportieren. Aus dieser Gruppe verschweigen allerdings 55 % ihrer eigenen IT-Abteilung, dass sie solche Dienste nutzen.[7]

Bei einer Sicherheitskonferenz fand Sophos unlängst heraus, dass 45 % der 214 Konferenzteilnehmer solche Dienste beruflich verwenden. 64 % der Teilnehmer finden solche Dienste „beängstigend".

Unabhängige Forschungseinrichtungen bestätigen diese Zahlen. In einer Umfrage von Ernst & Young aus dem Jahr 2011 gaben 61 % der befragten Unternehmen an, Cloud Storage entweder schon zu nutzen oder den Einsatz zu planen. 52 % der Unternehmen und Einrichtungen hatten allerdings noch keine Kontrollmechanismen zur Risikominderung eingeführt.

Cloud-Storage-Anbieter garantieren selten ein Backup. Im Falle eines Datenverlusts oder wenn der Dienstanbieter seinen Service einstellt, besteht keine garantierte Möglichkeit, die Daten wiederherzustellen.

Wenn Sie Ihre Daten einem Cloud-Speicher anvertrauen, kann bereits eine einzige Datenschutzverletzung Ihr gesamtes Unternehmen gefährden.

Die folgenden Erwägungen sollten in Ihre strategische Planung einfließen:

- Wer verwaltet Ihre Daten?
- Behalten Sie die Kontrolle über Ihre Daten?
- Welche Konsequenzen drohen im Falle einer Datenschutzverletzung?
- Wie wahrscheinlich sind Datenlecks?
- Können Sie die Sicherheit Ihrer Daten garantieren?

Sie können diese Fragen kaum beantworten, wenn Ihre Mitarbeiter Cloud Storage ohne Ihr Wissen oder Ihre Zustimmung und unter Missachtung von Verschlüsselungsrichtlinien nutzen. Sofern Sie den Zugriff auf Cloud-Dienste nicht bereits kontrollieren und enthaltene Daten stets verschlüsseln lassen, sollten Sie umgehend entsprechende Mechanismen implementieren.

7. „Workforce mobilization: What your IT department should know", SkyDox, http://www.skydox.com/workforce-mobilization-what-your-it-department-should-know

In nur drei einfachen Schritten sorgen Sie für den verantwortungsbewussten Umgang mit Cloud-Diensten und optimieren gleichzeitig den Datenschutz im Unternehmen.

1. Implementieren Sie Web-Richtlinien mit URL-Filterung.

Die URL-Filterung kontrolliert den Zugriff auf öffentliche Cloud-Storage-Webseiten und verhindert den Aufruf unerwünschter Webseiten.

2. Kontrollieren Sie Anwendungen mit Application Control.

Mit Application Control-Funktionen erlauben oder sperren Sie definierte Anwendungen für alle Mitarbeiter oder ausgewählte Gruppen.

3. Verschlüsseln Sie Ihre Daten.

Lassen Sie Dateien vor dem Hochladen in die Cloud von allen verwalteten Endpoints automatisch verschlüsseln.

Mitarbeiter verfügen dabei über ihre eigenen Schlüssel. Das bedeutet, sie können den Cloud-Storage-Dienst frei wählen. Die Verschlüsselung erfolgt automatisch und vor der Synchronisierung der Dateien. Die vollständige Kontrolle über die Sicherheit der Daten verbleibt also bei Ihnen. Über Sicherheitslecks beim Cloud-Storage-Anbieter müssen Sie sich deswegen keine Gedanken mehr machen.

Autorisierte Benutzer oder Gruppen greifen über zentrale Nachschlüssel auf Dateien zu, die für andere weiterhin verschlüsselt bleiben. Vergisst ein Benutzer sein Kennwort und verliert auf diese Weise seinen Schlüssel, so ist das kein Problem. Der Sicherheitsbeauftragte im Unternehmen kann die Schlüssel abrufen und so den autorisierten Mitarbeitern trotzdem Zugriff auf die Dateien ermöglichen.

Laden Sie „Probleme mit Dropbox?“, unser White Paper zum Thema Cloud Storage, herunter

Bedrohung Nummer 4: Soziale Netzwerke

Mit dem explosiven Wachstum sozialer Netzwerke wie Facebook (850 Mio. Benutzer), Twitter (140 Mio. Benutzer)[8] und LinkedIn (161 Mio. Benutzer)[9] steigt auch die Zahl von Malware, Spam und Datenschutzverletzungen.

Ein erstaunlicher Wert verdeutlicht, wie weit diese Entwicklung schon gediehen ist: Laut Forbes sind 50 % aller Smartphones 24 Stunden am Tag mit Facebook verbunden.[10]

Weil sie so beliebt sind, ziehen soziale Netzwerke naturgemäß Malware-Autoren, Spammer, Identitätsdiebe und andere Cyberkriminelle an. Soziale Netzwerke fördern und verstärken beispielsweise die unausgesprochenen Vertrauensverhältnisse zwischen ihren Benutzern. Wird jedoch ein völlig Fremder zum „Freund", kann er dieses Vertrauen missbrauchen und Sie, Ihre Netzwerkkonten und vielleicht sogar Ihre Identität und Ihre Bankkonten missbrauchen.

Bei LinkedIn kam es im Juni 2012 zu einer Datenschutzverletzung, als gehashte Kennwörter online einzusehen waren. Die SophosLabs zählten nach Abzug von Doppeleinträgen 5,8 Mio. eindeutige Kennwort-Hashes und stellten fest, dass 3,5 Mio. davon bereits mit Brute-Force-Methoden geknackt worden waren. Das bedeutet, dass über 60 % der gestohlenen Passwörter öffentlich bekannt sind und sich längst in den Händen von Kriminellen befinden können. Sophos empfahl daher allen Benutzern von LinkedIn, ihr Kennwort zu ändern.[11]

Die Freigabeaktivitäten in sozialen Netzwerken eröffnen auch andere Angriffswege, z.B.:

Clickjacking, ein Exploit, bei dem sich hinter normalen Buttons und anderen klickbaren Feldern schädliche Inhalte oder Funktionen verbergen. Die SophosLabs fanden Clickjacking-Links bereits hinter typischen Schlagzeilen wie „Lady Gaga tot in Hotelzimmer aufgefunden", „Tsunami in Japan spült Wal in Gebäude" oder „Justin Bieber erstochen". Der Benutzer glaubt, auf einen bestimmten Link zu klicken (z.B., um ein Video anzusehen); tatsächlich klickt er aber auf eine unsichtbare Schaltfläche mit dem Clickjacking-Wurm.

8. AVG Community Powered Threat Report, http://aa-download.avg.com/filedir/news/AVG_Community_Powered_Threat_Report_Q1_2012.pdf
9. http://press.linkedin.com/about
10. „50% of smartphones connect to Facebook every hour of the day", Forbes, http://www.forbes.com/sites/ericsavitz/2012/06/05/half-of-all-smartphones-connect-to-facebook-every-hour-of-the-day/
11. „LinkedIn confirms hack, over 60% of stolen passwords already cracked", Naked Security blog, http://nakedsecurity.sophos.com/2012/06/06/linkedin-confirms-hack-over-60-of-stolen-passwords-already-cracked/

Likejacking, ein Clickjacking-Angriff, der Facebook-Benutzer auf normale Links klicken lässt, die heimlich eine Facebook-Seite mit „Gefällt mir" markieren. Diese „Gefällt mir"-Hinweise tauchen dann in Ihrem Facebook-Profil und Ihrem News-Feed auf. Auch Ihre Freunde sehen sie dort, klicken ebenfalls darauf und verbreiten so die entführten „Likes" weiter.

Facebook ergreift Maßnahmen gegen wachsendes Benutzerrisiko

Mit seinen fast 900 Millionen Benutzern ist Facebook ein wahrer Malware-Magnet geworden. Zum Schutz seiner Benutzer arbeitet Facebook mit fünf Antiviren-Unternehmen zusammen, zu denen auch Sophos gehört. Für das URL-Blacklist-System von Facebook machen sie schädliche Webadressen ausfindig. Von dieser Zusammenarbeit profitiert die wachsende Zahl der Unternehmen, die einen Firmenauftritt bei Facebook erstellen und dabei ganz sicher sein möchten, dass Benutzer sorglos auf Links klicken können, ohne Malware oder Viren auf ihre Computer herunterzuladen.

So sichern Sie Benutzer von sozialen Netzwerken ab

Legen Sie Richtlinien für soziale Netzwerke fest und stellen Sie ihre Durchsetzung sicher. Die Richtlinie sollte detailliert aufzeigen, wie soziale Netzwerke genutzt werden dürfen und wie nicht. Auch die Konsequenzen beim Verstoß gegen diesen Verhaltenskodex müssen klar sein, etwa beim nachlässigen Umgang mit vertraulichen Kundendaten oder geistigem Eigentum.

Erklären Sie die Gefahren sozialer Netzwerke und wie man diese vermeiden kann. Erstellen Sie ein Schulungsprogramm, das die alltäglichen Bedrohungen auf den Webseiten sozialer Netzwerke erklärt. Zeigen Sie Phishing-Beispiele und erläutern Sie, weshalb man nicht einfach auf den Link eines Freundes klicken sollte. Ihre Mitarbeiter müssen sich bewusst werden, wie schnell sie ohne ihr Wissen einen Virus auf einen Firmen-PC oder ein Mobilgerät herunterladen, der sich dann sofort im ganzen Unternehmensnetzwerk verbreiten kann.

Stellen Sie sicher, dass Ihre Benutzer mit den Grundprinzipien des Datenschutzes und der Kennwortwahl vertraut sind. Dazu gehören: Auswahl und Geheimhaltung eines starken, eindeutigen Kennworts, regelmäßige Überprüfung der Privatsphäre-Einstellungen und sorgfältige Auswahl der Konfiguration, Vorsicht beim Download von Anwendungen, Befreundung nur mit wirklich bekannten Personen.

Sophos Complete Security Suite

Unsere Sophos Complete Security Suite schützt Sie überall – in Ihrem Netzwerk, auf Ihren Servern und Endpoint-PCs und sogar auf Mobilgeräten. Da alle Schutzelemente von Sophos stammen, ergänzen sie sich perfekt. Die Lösung ist besonders benutzerfreundlich, spart Ihnen Zeit und Geld und stammt von einem Anbieter Ihres Vertrauens.

- Web-Schutz, der die besten Funktionen aus Endpoint-, Cloud- und Gateway-Sicherheit vereint, um Benutzer immer und überall zu schützen
- Verschlüsselung, bereitgestellt und verwaltet über unsere Antiviren-Konsole
- Einheitliche Richtlinien für Data Loss Prevention (DLP) auf E-Mail- und Endpoint-Ebene
- Mobile Security für iPhone, iPad, Android, Blackberry und Windows Mobile
- Höchste Aktualität beim Erkennen von Bedrohungen aller Art, sichergestellt durch unsere SophosLabs-Analysten, die ununterbrochen gefährliche Webseiten, Bedrohungen, Spam und vieles mehr beobachten
- Alles von einem Anbieter, mit 24-Stunden-Support von zertifizierten Experten

Erstellt mit der Unterstützung von:

Barbara Hudson, Product Marketing Manager

Beth Jones, SophosLabs

Thomas Lippert, Senior Product Manager

Chris Pace, Product Marketing Manager

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858-0
+49 721 255 16-0
E-Mail: sales@sophos.de

Boston, USA | Oxford, UK

Sophos White Paper 06.12v1.dNA

SOPHOS