



# iPhone in Unternehmen

## Überblick über die Sicherheit



### Geräteschutz

- Komplexe Passcodes
- Passcode-Ablauf
- Verlauf für die Passcode-Wiederverwendung
- Maximale Anzahl an Fehleingaben
- Passcode-Zwang für kabellose Verbindungen
- Progressiver Geräteschutz

### Datenschutz

- Remote Wipe-Funktion
- Local-Wipe-Funktion
- Verschlüsselte Konfigurationsprofile
- Verschlüsselte iTunes Datensicherung
- Hardwareverschlüsselung (iPhone 3GS)

### Netzwerksicherheit

- Cisco IPSec, L2TP, PPTP VPN-Protokolle
- SSL/TLS mit X.509-Zertifikaten
- WPA/WPA2 Enterprise mit 802.1X
- Zertifikatbasierte Authentifizierung
- RSA SecurID, CRYPTOCARD

### Plattformsicherheit

- Laufzeitschutz
- Verbindliche Codesignierung
- Schlüsselbunddienste
- Allgemeine Crypto APIs

Das iPhone kann sicher auf Unternehmensdienste zugreifen und die Daten auf dem Gerät schützen. Es bietet leistungsfähige Verschlüsselung für die Datenübertragung, bewährte Authentifizierungsmethoden für den Zugang zu Unternehmensdiensten und auf dem iPhone 3GS auch Hardwareverschlüsselung aller auf dem Gerät gespeicherten Daten. Das iPhone bietet außerdem sicheren Schutz über die Verwendung von Passcode-Richtlinien, die kabellos verteilt und eingeführt werden können. Und falls das Gerät in die falschen Hände gerät, können Benutzer und IT-Administratoren einen Remote-Wipe-Befehl aktivieren, um sicherzustellen, dass vertrauliche Informationen gelöscht werden.

Wenn Sie über die Sicherheit des iPhone im Unternehmenseinsatz nachdenken, ist es hilfreich, über folgende Punkte Bescheid zu wissen:

- Methoden zur Verhinderung nicht autorisierter Verwendung des Geräts
- Schutz gespeicherter Daten, auch wenn das Gerät gestohlen oder verloren wird
- Netzwerkprotokolle und Datenverschlüsselung bei der Übertragung
- Sichere Plattformgrundlage mit iPhone OS

Der gleichzeitige Einsatz dieser Funktionen bietet eine sichere Mobile-Computing-Plattform.

## Gerätesteuerung und Schutz

Die Einführung strenger Richtlinien für den Zugriff auf das iPhone sind unverzichtbar, um Unternehmensdaten zu schützen. Passcode-Zwang ist der primäre Schutz gegen unbefugten Zugriff und kann kabellos konfiguriert und umgesetzt werden. Zusätzlich bietet das iPhone sichere Methoden zur Konfiguration des Geräts in einer Unternehmensumgebung, in der bestimmte Einstellungen, Richtlinien und Einschränkungen umgesetzt werden müssen. Diese Methoden bieten flexible Optionen zur Einrichtung eines Standardmaßes an Schutz für autorisierte Benutzer.

### Passcode-Richtlinien

Eine Geräte-Passcode verhindert, dass unbefugte Benutzer auf die Daten auf dem iPhone zugreifen oder auf andere Weise Zugriff auf das Gerät erhalten. Um Ihrem Sicherheitsbedürfnis gerecht zu werden, ermöglicht das iPhone OS Ihnen, aus einer umfangreichen Sammlung an Passcode-Anforderungen zu wählen, darunter Zeitüberschreitungsintervalle, Passcode-Komplexität und Passcode-Änderungshäufigkeit.

Die folgenden Microsoft Exchange ActiveSync-Passcode-Richtlinien werden unterstützt:

- Zwingende Eingabe eines Gerätekennworts
- Mindestlänge für Kennwörter
- Maximale Anzahl an Kennwort-Fehleingaben
- Kennwort muss aus Ziffern und Buchstaben bestehen
- Inaktivität in Minuten

In Microsoft Exchange Server 2007 werden außerdem weitere Passcode-Richtlinien unterstützt:

- Einfaches Kennwort zulassen oder ablehnen
- Kennwortablauf
- Kennwortverlauf
- Richtlinienaktualisierungsvorgabe
- Mindestanzahl komplexer Zeichen in einem Kennwort

### Richtlinienzwang

Die oben beschriebenen Richtlinien können auf zwei Arten auf dem iPhone festgelegt werden. Wenn das Gerät für den Zugriff auf einen Microsoft Exchange-Account konfiguriert ist, werden die Exchange ActiveSync-Richtlinien per Push-Funktion kabellos auf das Gerät übertragen. Dies ermöglicht es, Richtlinien ohne Aktivität des Benutzers einzuführen und zu aktualisieren.

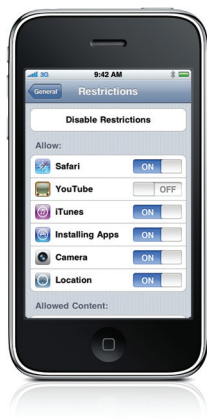
Richtlinien können auch als Teil eines Konfigurationsprofils für den Benutzer installiert werden. Ein Profil kann so definiert werden, dass das Löschen nur mit einem Administratorkennwort möglich ist oder dass es auf dem Gerät gesperrt ist und nicht ohne vollständiges Löschen aller Geräteinhalte entfernt werden kann.

### Sichere Gerätekonfiguration

Bei Konfigurationsprofilen handelt es sich um XML-Dateien, die Gerätesicherheitsrichtlinien und Einschränkungen, VPN-Konfigurationsinformationen, Wi-Fi-Einstellungen, E-Mail- und Kalender-Accounts sowie Authentifizierungszertifikate enthalten, die es dem iPhone ermöglichen, mit Ihren Unternehmenssystemen zu arbeiten. Die Möglichkeit, Passcode-Richtlinien in Kombination mit Geräteeinstellungen in einem Konfigurationsprofil einzuführen, stellt sicher, dass die Geräte innerhalb Ihres Unternehmens alle korrekt und gemäß den Sicherheitsstandards Ihres Unternehmens konfiguriert sind. Und da Konfigurationsprofile sowohl verschlüsselt als auch gesperrt werden können, können die Einstellungen nicht entfernt, verändert oder für andere freigegeben werden.

Konfigurationsprofile können sowohl signiert als auch verschlüsselt werden. Das Signieren eines Konfigurationsprofils stellt sicher, dass die so eingeführten Einstellungen nicht verändert werden können. Die Verschlüsselung eines Konfigurationsprofils schützt die Inhalte und ermöglicht die Installation nur auf dem vorgesehenen Gerät. Konfigurationsprofile werden über CMS (Cryptographic Message Syntax, RFC 3852) mit 3DES- und AES-128-Unterstützung verschlüsselt.

Beim erstmaligen Übertragen verschlüsselter Konfigurationsprofile müssen diese per USB-Synchronisierung mit dem iPhone Konfigurationsprogramm oder per kabelloser Registrierung und Verteilung übertragen werden. Zusätzlich zu diesen Methoden kann die nachfolgende Verteilung verschlüsselter Konfigurationsprofile als E-Mail-Anhang oder über eine Website erfolgen, auf die die Benutzer Zugriff haben.



### Verfügbare Einschränkungen

- Zugriff auf ungeeignete und eindeutige Inhalte im iTunes Store
- Nutzung von Safari
- Nutzung von YouTube
- Zugriff auf den iTunes Store
- Nutzung von App Store und iTunes zur Installation von Programmen
- Nutzung der Kamera (kann auch mit einer Exchange-Richtlinie gesteuert werden)

### Geräteeinschränkungen

Geräteeinschränkungen bestimmen, auf welche iPhone Funktionen der Benutzer auf dem Gerät zugreifen kann. Normalerweise handelt es sich dabei um netzwerkfähige Programme wie Safari, YouTube und den iTunes Store, aber über Einschränkungen können auch Dinge wie die Installation von Anwendungen oder die Benutzung der Kamera gesteuert werden. Über Geräteeinschränkungen können Sie das Gerät nach Ihren Anforderungen konfigurieren und den Benutzern die Verwendung des Geräts im Rahmen der Unternehmenspraktiken gestatten. Einschränkungen werden über ein Konfigurationsprofil eingeführt oder können manuell auf jedem Gerät eingerichtet werden. Darüber hinaus können Einschränkungen der Kameranutzung kabellos über Microsoft Exchange Server 2007 eingeführt werden.

Zusätzlich zum Festlegen von Einschränkungen und Richtlinien auf dem Gerät kann das iTunes Schreibtischprogramm durch die IT-Abteilung konfiguriert und gesteuert werden. Hierzu gehört das Unterbinden des Zugriffs auf ungeeignete oder eindeutige Inhalte, das Festlegen, auf welche Netzwerkdienste der Benutzer innerhalb von iTunes zugreifen kann, und ob neue Softwareaktualisierungen zur Installation für den Benutzer verfügbar sind.



### Progressiver Geräteschutz

Das iPhone kann für die automatische Löschung nach mehreren falschen Passcode-Eingaben konfiguriert werden. Wenn der Benutzer wiederholt den falschen Passcode eingibt, wird das iPhone für einen immer längeren Zeitraum deaktiviert. Nach zu vielen erfolglosen Versuchen werden alle Daten und Einstellungen auf dem Gerät gelöscht.

## Datenschutz

Der Schutz von auf dem iPhone gespeicherten Daten ist in jeder Umgebung mit einem hohen Anteil an vertraulichen Unternehmens- oder Kundeninformationen wichtig. Zusätzlich zur Datenverschlüsselung während der Übertragung verfügt das iPhone 3GS über Hardwareverschlüsselung für auf dem Gerät gespeicherte Daten.

Wenn ein Gerät verloren oder gestohlen wird, ist es wichtig, das Gerät zu deaktivieren und die Daten zu löschen. Es zahlt sich auch aus, eine Richtlinie einzurichten, die das Gerät nach einer festgelegten Anzahl falscher Passcode-Eingaben löscht. Dies ist eine der Schlüsselfunktionen gegen Versuche, unautorisiert auf ein Gerät zuzugreifen.

### Verschlüsselung

Das iPhone 3GS bietet eine hardwarebasierte Verschlüsselung. Die Hardwareverschlüsselung des iPhone 3GS verwendet AES 256-Bit-Verschlüsselung zum Schutz aller Daten auf dem Gerät. Die Verschlüsselung ist dauerhaft aktiviert und kann nicht durch den Benutzer deaktiviert werden.

Außerdem können in iTunes gesicherte Daten, die auf dem Computer eines Benutzers gespeichert sind, verschlüsselt werden. Wenn ein verschlüsseltes Konfigurationsprofil auf dem Gerät eines Benutzers gespeichert wird, wird diese Funktion automatisch aktiviert. Zum weiteren Schutz der Programmdateien haben Entwickler Zugriff auf APIs, die es ihnen ermöglichen, Daten in ihren eigenen Programmdateispeichern zu verschlüsseln.

### Remote Wipe-Funktion

Das iPhone unterstützt Remote Wipe. Wenn ein Gerät verloren oder gestohlen wird, können der Administrator oder Gerätebesitzer einen Remote Wipe-Befehl starten, der alle Daten löscht und das Gerät deaktiviert. Wenn das Gerät mit einem Exchange-Account konfiguriert ist, kann der Administrator den Remote-Wipe-Befehl über die Exchange Management Console (Exchange Server 2007) oder das Exchange ActiveSync Mobile Administration Web Tool (Exchange Server 2003 oder 2007) starten. Benutzer von Exchange Server 2007 können den Remote Wipe-Befehl auch direkt über Outlook Web Access starten.

### Local-Wipe-Funktion

Das iPhone kann auch für die automatische lokale Löschung nach mehreren falschen Passcode-Eingaben konfiguriert werden. Die ist eine Schlüsselmaßnahme gegen Brute-Force-Angriffe mit dem Ziel, Zugriff auf das Gerät zu erhalten. Standardmäßig wird das iPhone automatisch nach 10 fehlgeschlagenen Passcode-Eingaben gelöscht. Wie bei anderen Passcode-Richtlinien kann die Anzahl fehlgeschlagener Eingaben über ein Konfigurationsprofil oder kabellos über Microsoft Exchange ActiveSync-Richtlinien festgelegt werden.

## Sichere Netzwerkkommunikation

Mobilgerätebenutzer müssen in der Lage sein, weltweit auf Unternehmensinformationsnetzwerke zuzugreifen, aber gleichzeitig muss sichergestellt sein, dass die Benutzer autorisiert sind und dass ihre Daten während der Übertragung geschützt sind. Das iPhone bietet bewährte Technologien, um diese sicherheitsrelevanten Ziele bei der Kommunikation über Wi-Fi- und Mobilfunknetzwerke zu erreichen.

### VPN

Viele Unternehmensumgebungen verfügen über eine Form virtueller privater Netzwerke. Diese sicheren Netzwerkdienste werden bereits eingesetzt und erfordern für gewöhnlich nur minimalen Einrichtungs- und Konfigurationsaufwand mit dem iPhone.

Das iPhone integriert über die Unterstützung von Cisco IPsec, L2TP, und PPTP mit einer großen Anzahl häufig genutzter VPN-Technologien. Die Unterstützung für diese Protokolle stellt sicher, dass das höchste IP-basierte Verschlüsselungsniveau für die Übertragung vertraulicher Informationen eingehalten wird. Das iPhone unterstützt die Netzwerkproxy-Konfiguration sowie Split-IP-Tunneling, sodass der Datenverkehr zu öffentlichen oder privaten Netzwerkdomains entsprechend Ihrer spezifischen Unternehmensrichtlinien abgewickelt wird.



#### VPN-Protokolle

- Cisco IPSec
- L2TP/IPSec
- PPTP

#### Authentifizierungsmethoden

- Kennwort (MSCHAPv2)
- RSA SecureID
- CRYPTOCARD
- Digitale x.509 -Zertifikate
- "Shared Secret"

#### 802.1x-Authentifizierungsprotokolle

- EAP-TLS
- EAP-TTLS
- EAP-FAST
- EAP-SIM
- PEAP v0, v1
- LEAP

#### Unterstützte Zertifikatformate

Das iPhone unterstützt X.509-Zertifikate mit RSA-Schlüssel. Es werden die Dateierweiterungen .der, .crt, und .cer erkannt.

Zusätzlich zu einem sicheren Zugriff auf vorhandene VPN-Umgebungen bietet das iPhone bewährte Methoden zur Benutzerauthentifizierung. Die Authentifizierung über standardmäßige digitale x.509-Zertifikate bietet dem Benutzer optimierten Zugriff auf Unternehmensressourcen und eine realisierbare Alternative zu hardwarebasierten Tokens. Darüber hinaus ermöglicht es die Zertifikatauthentifizierung, auf dem iPhone die Nutzung der Vorteile von VPN-On-Demand, was den VPN-Authentifizierungsprozess transparent macht und dennoch sicheren, zertifizierten Zugriff auf Netzwerkdienste bietet.

Für Unternehmensumgebungen, in denen Two-Factor-Tokens erforderlich sind, integriert das iPhone mit RSA SecureID und CRYPTOCARD.

#### SSL/TLS

Das iPhone unterstützt SSL v3 und Transport Layer Security (TLS v1), den Sicherheitsstandard der neuen Generation für das Internet. Safari, Kalender, Mail und andere Internetprogramme starten diese Verfahren automatisch, um einen verschlüsselten Kommunikationskanal zwischen iPhone und Unternehmensdiensten zu bieten.

#### WPA/WPA2

Das iPhone unterstützt WPA2 Enterprise für authentifizierten Zugriff auf das Drahtlosnetzwerk Ihres Unternehmens. WPA2 Enterprise verwendet 128-Bit-AES-Verschlüsselung und bietet dem Benutzer das höchste Niveau an Sicherheit, dass Ihre Daten geschützt sind, auch wenn Sie Kommunikationsdaten über ein Wi-Fi-Netzwerk senden oder empfangen. Und durch die Unterstützung von 802.1X kann das iPhone in eine große Anzahl an RADIUS-Authentifizierungsumgebungen integriert werden.

## Sichere Plattformgrundlage

Das iPhone OS ist eine Plattform, bei deren Entwicklung der Sicherheitsgedanke zugrunde lag. Es enthält einen offenen Ansatz für den Programmlaufzeitschutz und erfordert eine verbindliche Programm-Signierung, um sicherzustellen, dass Programme nicht verändert werden können. Das iPhone OS verfügt außerdem über ein sicheres Framework, das die sichere Speicherung von Programm- und Netzwerkdienstzertifikaten in einem verschlüsselten Schlüsselbund unterstützt. Für Entwickler bietet es eine allgemeine Verschlüsselungsarchitektur, die verwendet werden kann, um Programmdatenspeicher zu verschlüsseln.

#### Laufzeitschutz

Die Programme auf dem Gerät sind „offen“ angelegt, sodass sie auf Daten, die von anderen Programmen gespeichert wurden, zugreifen können. Darüber hinaus sind die Systemdateien, Ressourcen und der Kernel vom Programmbereich des Benutzers abgegrenzt. Wenn ein Programm auf Daten eines anderen Programms zugreifen muss, kann dies nur über die APIs und Dienste des iPhone OS geschehen. Außerdem wird die Codeerstellung verhindert.

#### Verbindliche Codesignierung

Alle iPhone Programme müssen signiert sein. Die Programme im Lieferumfang des Geräts sind von Apple signiert. Drittanbieterprogramme sind von dem jeweiligen Entwickler mit einem von Apple bereitgestellten Zertifikat signiert. Dadurch ist sichergestellt, dass Programme nicht manipuliert oder verändert wurden. Zusätzlich werden Laufzeitprüfungen vorgenommen, um sicherzustellen, dass das Programm seit der letzten Verwendung nicht als nicht mehr vertrauenswürdig eingestuft wurde.

Die Verwendung von individuellen oder unternehmensinternen Programmen kann über ein Bereitstellungsprofil gesteuert werden. Der Benutzer muss das Bereitstellungsprofil installieren, um das Programm ausführen zu können. Der Administrator kann außerdem die Verwendung eines Programms auf ein bestimmtes Gerät beschränken.

#### Sicheres Authentifizierungs-Framework

Das iPhone bietet einen sicheren, verschlüsselten Schlüsselbund zur Speicherung digitaler Identitäten, Benutzernamen und Kennwörter. Die Schlüsselbunddaten sind partitioniert, damit Anwendungen mit einer anderen Identität nicht auf von Drittanbieterprogrammen gespeicherte Zertifikate zugreifen können. Dies bietet einen Mechanismus zur Sicherung der Authentifizierungszertifikate auf dem iPhone für eine ganze Reihe an Programmen und Diensten innerhalb des Unternehmens.

### Allgemeine Crypto-Architektur

Programmentwickler haben Zugriff auf Verschlüsselungs-APIs, die sie nutzen können, um die Daten ihrer Anwendungen noch besser zu schützen. Die Daten können mit bewährten Methoden wie AES, RC4, oder 3DES symmetrisch verschlüsselt werden. Zusätzlich bietet das iPhone Hardwarbeschleunigung für AES- und SHA1-Verschlüsselung für die maximale Programmleistung.

### Ein revolutionäres Telefon, durch und durch sicher

Das iPhone 3GS bietet Verschlüsselungsschutz für Daten in der Übermittlung, auf dem Gerät oder in einer iTunes Sicherungsdatei. Egal, ob der Benutzer auf Unternehmens-E-Mails zugreift, eine private Website besucht, oder sich am Unternehmensnetzwerk authentifiziert, das iPhone bietet die Sicherheit, dass nur autorisierte Benutzer Zugriff auf vertrauliche Unternehmensdaten haben. Durch die Unterstützung von gängigen Unternehmensstandards entsprechender Netzwerkfunktionen und umfassenden Methoden zur Vermeidung von Datenverlust kann das iPhone mit der Sicherheit eingesetzt werden, dass Sie damit auch bewährte Methoden für die Mobilgerätesicherheit und den Datenschutz implementieren.

### Weitere Ressourcen

Bereitstellungshandbuch für Unternehmen

[http://manuals.info.apple.com/en\\_US/Enterprise\\_Deployment\\_Guide.pdf](http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf)

Bereitstellungsressourcen und -Szenarios für Unternehmen

<http://www.apple.com/iphone/enterprise/integration.html>