Sicherheitsrichtlinien für den Einsatz mobiler Endgeräte

Michael Föck

Die erste technische Revolution war die Einführung des PC, die zweite Revolution die Einführung des mobilen Telefons, die dritte Revolution war das Internet und jetzt wachsen alle Techniken zur Digitalwirtschaft zusammen. Dadurch ergeben sich neue Nutzungs- und Anwendungsmöglichkeiten, aber auch zahlreiche, zusätzliche Herausforderungen. Über mobile Endgeräte ist der Zugang zur IT-Infrastruktur eines Unternehmens ortsunabhängig möglich. Weil ein Smartphone immer und überall verfügbar ist, kann es aber auch immer und überall angegriffen werden.

Michael Föck ist als Geschäftsführer für den Bereich professional Services der Thinking Objects GmbH verantwortlich. Die prof. Services arbeiten vorwiegend an der Schnittstelle zwischen Fachbereich und Rechenzentrum.

Viele Nutzer mobiler Endgeräte sind keine IT-Spezialisten und müssen deshalb über Vorgaben zur sicheren Verwendung der mobilen Endgeräte angeleitet werden. Nur so kann unbeabsichtigtes Fehlverhalten der Anwender proaktiv verhindert werden. Die Konzentration auf rein technische Möglichkeiten würde zu kurz greifen. Es gibt Herausforderungen, denen ausschließlich über organisatorische Maßnahmen begegnet werden kann. Nur eine integrierte Lösung bestehend aus Richtlinien und technischen Abwehrmaßnahmen bringt ein Höchstmaß an Sicherheit.

In diesem Beitrag lesen Sie:

- warum Richtlinien für Smartphones nicht nur nützlich sondern unbedingt erforderlich sind,
- wie mit technischen und organisatorischen Maßnahmen die Sicherheit beim Smartphone Einsatz signifikant erhöht werden kann,
- wie Richtlinien entwickelt werden, die Anwender akzeptieren.

Ein Computersystem mit einem Hauptspeicher, in der Endausbaustufe von 4 Kilowords (Ki) RAM und 32 Ki Storage, war ausreichend, um sicher zum Mond hin und wieder zurück zufliegen. Jede, noch so einfache App, benötigt heute wesentlich mehr Speicher. Inzwischen sind Smartphones mit 2 GB RAM-Speicher (das entspricht ca. 1,5 Mio. Ki) der Standard. Damit sind mobile Anwendungen möglich geworden, die vor einigen Jahren noch nicht denkbar waren.

Wenn in den folgenden Ausführungen der Begriff Smartphone verwendet wird, dann werden unter dem Begriff Smartphone auch Tablet Computer verstanden.

Notwendigkeit von Richtlinien

Mit tragbaren Geräten, die einen Zugang zum Internet haben, entstand eine neue Situation in den Unternehmen. Endgeräte konnten jetzt auch außerhalb des Firmengeländes und der Büros angegriffen werden. Außerdem bestand zum ersten Mal die Situation, dass Geräte verloren gehen konnten. Einige Unternehmen haben in dieser Situation bereits Richtlinien für Laptops und Notebooks eingeführt.

Beispiel: Bei Banken und Versicherungen wurden zugleich mit der Einführung der tragbaren Geräte auch gleich entsprechende Richtlinien entwickelt. So war es u. a. durch die Richtlinien verboten, das Notebook im Zug am Sitzplatz zurückzulassen. Egal wohin sich der Besitzer im Zug bewegte, er musste sein Notebook immer bei sich haben.

Heute kann ein noch leistungsfähigerer Rechner sogar in die Tasche gesteckt werden. Dies hat nicht nur eine Vielzahl neuer Angriffsmöglichkeiten ergeben, sondern auch die Anzahl der kriminellen Nutzer dramatisch erhöht. Anfang 2015 hatten 3 Mrd. Menschen ständig Zugriff auf das Internet.

Beispiel: Mancher Nutzer lässt sein Smartphone im Mantel und gibt ihn an der Garderobe ab. Wenn das Smartphone nicht durch einen PIN geschützt ist, haben, ab dem Moment der Abgabe, möglicherweise fremde Personen Zugriff auf Firmendaten oder die IT-Infrastruktur des Unternehmens. Eine PIN mit vier Stellen ▶

ist jedoch noch keine ausreichende Lösung. Bei einer vierstelligen PIN, die nur Ziffern erlaubt, entstehen 10^4 Möglichkeiten. Wenn nur drei falsche Eingaben zulässig sind, beträgt die Wahrscheinlichkeit die PIN zu erraten 1 : 3 333. Aus diesem Grund muss der Umgang damit über Richtlinien geregelt werden. Dazu gehören wichtige Festlegungen wie z. B. Länge der PIN, Änderungsrhythmus usw.

Mit Smartphones sind erstmalig Endgeräte im Unternehmensnetz verfügbar, auf denen die parallele Nutzung privater und gewerblicher Applikationen der Standardfall ist. Auch aufgrund der Regelungen des Bundesdatenschutzgesetzes (BDSG) müssen private und gewerbliche Daten streng voneinander getrennt werden.

Während RIM (BlackBerry®) seine Geräte speziell für den Einsatz in Unternehmen konzipiert hatte, wurde die aktuelle Generation der Smartphones zunächst primär für den privaten Einsatz konzipiert. Bei dieser spielt das Teilen von Informationen und Bildern eine wichtige Rolle. Die Nutzung in einem gewerblichen Umfeld fordert das genaue Gegenteil. Nur Informationen, die speziell vom Unternehmen freigegeben sind, dürfen mit der Öffentlichkeit geteilt werden. Der Informationsfluss wird durch viele andere Gesetze geregelt. So legt z. B. das Aktiengesetz fest, dass über wichtige Vorgänge im Unternehmen zuerst die Aktionäre informiert werden müssen.

Auch durch den Einsatz der Smartphones steigt die Zahl der Internetnutzer kontinuierlich an. Damit verbunden ist leider auch ein Anstieg unseriöser und krimineller Nutzer. Spezielle Formen der Internetkriminalität werden durch den Einsatz von Smartphones ermöglicht oder zumindest begünstigt. Aus diesem Grund ist es entscheidend, dass die Anwender die Richtlinien als ‚persönlichen Schutzschild' akzeptieren.

In Vordergrund der Bemühungen steht der Schutz der Daten, die auf dem Smartphone verfügbar sind oder zu denen Zugriff besteht. Zunächst müssen viele Anwender überzeugt werden, dass ihre Daten einen Wert haben.

Innerhalb der Richtlinien muss geregelt werden, welche Daten überhaupt auf einem Smartphone gespeichert werden dürfen. Dabei sollte auch geregelt werden, welche Daten via E-Mail verschickt werden sollten. Bei vielen Dokumenten reicht es, einen Link auf den Speicherort zu verschicken.

Viele kostenfreie Apps speichern alle Daten vom Smartphone und übertragen sie an den Anbieter. Das erfolgt für den nicht speziell ausgebildeten Anwender so intransparent, dass er es nicht bemerkt.

Das fehlende Wissen und häufig auch überraschend wenig Misstrauen im Umgang mit den Angeboten aus dem Internet, bilden eine weitere Gefahrenquelle. Viele Formen der Kriminalität, die erfolgreich über das Internet betrieben werden, sind schon seit vielen Jahrzehnten bekannt. Vor 30 - 40 Jahren wurden Inhaber von Euroscheckkarten angerufen und telefonisch um die Herausgabe der Geheimzahl gebeten. Dabei wurde der Inhaber der Euroscheckkarte mit einer gezielten Meldung so überrumpelt, dass er die Nummer herausgegeben hat. Heute werden die Internetnutzer mit Phishing E-Mails auf eine ähnliche Art angegriffen.

Regelungsinhalte

Richtlinien können von anderen Unternehmen nicht exakt übernommen werden. Jedes Unternehmen muss seinen Regelungsbedarf im Rahmen seiner Unternehmenskultur ermitteln. Trotzdem ist der Erfahrungsaustausch innerhalb einer Branche sehr sinnvoll.

Am Anfang einer Smartphone Einführung müssen die Ziele festgelegt werden. Auf der Basis der Ziele und der daraus abgeleiteten Anwendungsszenarien wird eine Risikoanalyse erstellt. Zusätzlich muss vor der Smartphone Einführung – sofern noch nicht erfolgt – eine Klassifizierung der Unternehmensdaten, in Bezug auf die Vertraulichkeit, vorgenommen werden.

Internetdienste wie Twitter oder Facebook laden dazu ein, Informationen mit anderen Personen zu teilen. Innerhalb sozialer Netzwerke wird nicht zwischen privaten und gewerblichen Informationen unterschieden. Eine unkontrollierte Übertragung von Informationen aus einem Unternehmen muss in jedem Fall vermieden werden. Aus diesem Grund muss das Publizieren von Unternehmensinformationen jedem Mitarbeiter (auch als Privatperson) verboten werden. Nur entsprechend autorisierte Abteilungen im Unternehmen, die für Öffentlichkeitsarbeit verantwortlich sind, publizieren Daten.

Durch neue Formen der Infrastruktur entstehen neue, zusätzliche Gefahren. An vielen Stellen ist ein öffentliches WLAN verfügbar. Das lässt Applikationen wie ‚virtuelle' Stadtführer zu. Damit der Zugriff einfach möglich ist, sind die meisten dieser WLAN-Knoten unverschlüsselt. Zu Hause oder in Firmenumgebungen erfolgt der Zugriff dagegen verschlüsselt. Für einen unausgebildeten Anwender ist der Unterschied kaum erkennbar und die resultierenden Konsequenzen sind nicht deutlich. Der nicht spezialisierte Anwender benötigt für ein solches Umfeld Anweisungen, um sich korrekt zu verhalten. So sollten z. B. in offenen Umgebungen keine Online-Bankgeschäfte gemacht werden.

Auf der Basis der Risikoanalyse und der Datenklassifizierung wird eine Matrix erstellt, welche Risiken mit technischen, mit organisatorischen Maßnahmen oder einer Kombination aus beiden abgemildert oder beseitigt werden. Auch mit guten, ausgewogenen Richtlinien werden nicht alle Risiken eliminiert. Restrisiken sind unausweichlich beim zukünftigen Gebrauch (Bild 1).

BOYD

Die Abkürzung steht für den englischen Begriff ‚bring your own device'. Darunter wird verstanden, dass Mitarbeiter ihre eigenen Geräte zur Arbeit mitbringen und diese an die

☐ Verhalten bei
- Nutzung der Smartphones z. B. Schutzfolien gegen unbefugte Einsichtnahme usw.
- Nutzung im Inland
  (Sperren von Rufnummern, Umgang mit der Kamera, Verbot von Aufzeichnungen, Verhalten bei offenem WLAN usw.)
- Nutzung im Ausland
  (Achtung: Exportrestriktionen von US-Geräten aufgrund geltender US-Gesetze beachten!)
- Verlust des Smartphones
  (vorbeugende Maßnahmen, Verhaltensregeln bei Verlust)
- Nutzung von Apps
  (Einschränkung der Nutzung von Apps, verbotenen Apps)
- Privater Nutzung (falls erlaubt)

☐ Zulassung bzw. Verbot von Diensten
(z. B. keine Überweisungen, Rufnummernmissbrauch usw.)
☐ Umgang mit Social Media
☐ Festlegung von Nutzerprofilen
☐ Änderungen an der vorgegebenen Konfiguration
☐ Einstellungen zum persönlichen Schutz der Anwender
(Ausschalten der Ortung, Verschlüsselung, Regelungen zur Erreichbarkeit usw.)
☐ Regelung des Umgangs mit personen- und ortsabhängigen Daten
- auf den Endgeräten
- auf den IT-Systemen für Verwaltung und Betrieb der Geräte

☐ Regelungen zur Arbeitszeit
☐ Regelungen zur Gesundheitsvorsorge
☐ Spezielle Regelungen für Administratoren
☐ Gerätespezifische Regelungen

Bild 1: Mögliche Themenbereiche für Richtlinien.

Unternehmens-IT anbinden. Sie nutzen private Smartphones sowohl für private als auch für die Anwendungen im Unternehmen. Die Hersteller von MDM (Mobile Device Management) Systemen stellen BYOD immer wieder in den Vordergrund. Während es in Europa ein ungewohntes Konzept ist, hat dies in den USA Tradition. Dort ist es üblich, dass Handwerker bei Antritt einer Stelle ihr eigenes Werkzeug mitbringen.

Viele MDM-Hersteller werben damit, dass MDM-Systeme einen gesetzeskonformen Umgang mit den unterschiedlichen Daten auf dem Smartphone in Deutschland gewährleisten. Dieser Hinweis ist richtig, wenn ausschließlich die Vorschriften des BDSG betrachtet werden. Dies schreibt eine strikte Trennung von geschäftlichen und privaten Daten auf einem Endgerät vor. Neben dem BDSG gibt es eine Fülle anderer deutscher Gesetze, die im Umgang mit BYOD eine Rolle spielen. Die rechtliche Situation ist bei BYOD so komplex, dass eine ausführliche Rechtsberatung notwendig ist. Die Entscheider sollten schließlich die Frage stellen, ob der Aufwand gerechtfertigt ist.

Neben der wirtschaftlichen und rechtlichen Thematik sollten mindestens diese Punkte beachtet werden:
- Nur Spezialisten können Daten auf den Smartphones so löschen, dass sie nicht mehr rekonstruiert werden können. Wenn Nutzer ihre eigenen Geräte auf eBay verkaufen, können vermeintlich gelöschte Daten vom Käufer wiederhergestellt werden.
- Durch viele unterschiedliche Geräte mit unterschiedlichen Betriebssystemen kann der interne Aufwand für den Support enorm ansteigen.
- Verlust der Fähigkeit zur zentralen Steuerung von Updates und Rollouts.

Es können, auch über ausführliche Regelungen, nicht alle Risiken vermieden werden. Aufgrund der unterschiedlichen Gesetze ergibt sich eine sehr komplexe Situation und es muss mit erheblichen Restrisiken gelebt werden.

Die Technik der Smartphones ist sehr unterschiedlich, sodass eine Einigung auf möglichst einen Hersteller und nur wenige Gerätetypen vorteilhaft ist. Andernfalls ist der Betrieb der Geräte wirtschaftlich nicht tragbar. Smartphones, bei denen Hard- und Software von einem Hersteller kommen, bieten ein höheres Maß an Sicherheit als andere Geräte im Rahmen von BYOD.

Beispiel: In einer Richtlinie muss hinterlegt werden, dass iPhones® nicht im eingeschalteten Zustand an Fremdgeräte zum Laden angeschlossen werden dürfen. Nur so kann verhindert werden, dass die Daten vom Gerät abgezogen werden. Nach dem Laden bootet das Smartphone, was keine Gefahr birgt. Solange der Unlock-Code nicht eingegeben wird, bleiben die Daten im Smartphone verschlüsselt. Im Idealfall geschützt durch einen Geräteschlüssel und einen Schlüssel des Anwenders, wenn der Gerätehersteller die derzeitig verfügbaren Sicherheitskomponenten in seiner Hard- und Software korrekt umsetzt.

Erstellungsprozess

Werden zuerst die Smartphones an die Nutzer ausgeliefert und anschließend Richtlinien einführt, ist sehr viel Kraft notwendig, um alle Nutzer auf diese einzustimmen. Insofern empfiehlt es sich, dass Richtlinien und Endgeräte gemeinsam eingeführt werden. ▶

Die Richtlinien dürfen nicht allein von der IT erstellt, sondern alle Betroffenen sollten integriert werden. In Unternehmen mit Betriebsrat ist dieser in jedem Fall und frühzeitig einzubeziehen. Ein großer Vorteil entsteht dadurch, dass die Richtlinien im Zusammenhang mit Veranstaltungen eingeführt werden. Dort werden die Nutzer für die Problematik sensibilisiert und können die Richtlinien als nützliche Unterstützung empfinden.

Vor der Einführung von Richtlinien müssen mindestens folgende Themenkomplexe geklärt sein:

- Welche Ziele sind mit dem Smartphone Einsatz zu erreichen?
- Daten welcher Klassifizierung liegen auf den Smartphones?
- Auf Daten welcher Klassifizierung wird extern zugegriffen?
- Welche Smartphones werden eingesetzt?
- Welche Gruppen im Unternehmen werden mit Smartphones ausgestattet?
- Welche branchenspezifischen Regelungen sind zu beachten?

Nach der Zusammenstellung und Überprüfung der relevanten Fakten wird ein erster Entwurf erstellt. In diesem Stadium kann die Federführung bei der IT liegen. Im nächsten Schritt wird der Entwurf rechtlich geprüft. Auf der Basis der Ergebnisse der rechtlichen Prüfung werden die endgültigen Richtlinien erstellt und die Einführung geplant.

Die Erstellung der Richtlinien ist jedoch nur der Anfang aller Aktivitäten. Die Richtlinien müssen stets an veränderte Verhältnisse angepasst oder aufgrund von Erfahrungen verändert werden. So muss mit der Einführung der Richtlinien festgelegt werden, wer für die Weiterentwicklung der Richtlinien verantwortlich ist. Nur die stetige Anpassung der Richtlinien sichert deren Akzeptanz.

Ausblick

In Zukunft wird es keine dedizierten Telefone mehr geben. Das Telefonieren werden Brillen, Mützen, Jacken und andere Kleidungsstücke oder Accessoires übernehmen. Die ersten Prototypen sind bereits verfügbar.

Ein anderer Trend führt zum Zusammenwachsen von Smartphone und Tablet. Die ersten faltbaren Displays wurden bereits der Öffentlichkeit vorgestellt. Bis zur Serienreife wird es noch einige Zeit dauern, aber das Tablet der Zukunft wird ein solches Display haben, was die Anwendungsmöglichkeiten weiter erhöht.

Die neue EU-Datenschutzregelung wird die doppelte Nutzung (privat und geschäftlich) noch mehr erschweren und eventuell sogar unmöglich machen. Im inzwischen veröffentlichen Entwurf wurden die Strafen drastisch erhöht und die Unternehmen müssen auch die Betroffenen über Verstöße informieren. Das Gesetzgebungsverfahren wird das Konzept noch verändern, aber der Trend ist absehbar. Die Politik wird die Regeln verschärfen.

Immer häufiger werden Unternehmen oder staatliche Organisationen aus dem Internet angegriffen. Der unglaubliche NSA-Skandal hat gezeigt, was vor einiger Zeit möglich war und wie sorglos Internetnutzer mit ihren Daten umgehen. Viele Ausspähungen waren nur möglich, weil die Internetnutzer es ermöglicht haben. Beim Thema Sensibilisierung der Internetnutzer stehen wir am Anfang der Entwicklung. In Zukunft müssen zusätzlich zu den technischen Fertigkeiten auch die Verhaltensregeln vermittelt werden. ■

Kontakt:

Michael Föck
Thinking Objects GmbH
Lilienthalstraße 2/1
70825 Korntal-Münchingen
Tel.: +49 711 88770220
E-Mail: michael.foeck@topalis.com

Literatur

[1] Biegsam und flexibel, Artikel aus Süddeutsche.de vom 6.11.2013 http://www.sueddeutsche.de/digital/zukunft-des-smartphones-biegsam-und-flexibel-1.1811544.
[2] Bundesamt für Sicherheit in der Informationstechnik, Überblickpapier Smartphones https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_Smartphone_pdf.pdf.
[3] Verschärte Spielregeln für BYOD http://ibmexperts.computerwoche.de/mobile-enterprise/artikel/verschaerfte-spielregeln-fuer-byod.

Schlüsselwörter:
Smartphone, Sicherheit, Richtlinien, Sicherheitsrichtlinien, Schutzbedarf

Guidelines for using mobile devices

Mobile devices have changed our way of life and will change it even more in the future. Always and everywhere we have access to the Internet. In trains, railway stations, city centers, airports, etc. free use of wireless LAN is already the norm today. The usage is easy and almost most the time unencrypted. Thus, from these queries have had no problems, are guidelines for the use of smartphones absolutely necessary, because then the non-technical users are guided and sensitised.

Keywords:
smartphone, security, guideline, security guideline, protection requirement analysis