Verantwortung: Smartphone

Immer verlockender werden die Verheißungen der mobilen Alleskönner: Schnelle günstige Datenanbindungen und Apps für Alles und Jeden, und nebenbei darf das liebgewonnene private Smartphone nun auch im beruflichen Alltag mitmischen. An manchen Tagen bin ich versucht diese Möglichkeiten gänzlich auszuschöpfen, sie zu genießen. Doch dann beginnt ein neuer Arbeitstag im Testlabor, der mir wieder die Schattenseiten vor Augen hält: Apps die ungefragt Daten verschicken, Schutzfunktionen, die wir durch Verbiegen eines einzigen Bits umgehen können und die Reaktion des Herstellers, dass gegenwärtig die Kunden mehr Sicherheit und Privatsphäre nicht nachfragen.

Es gibt aber auch Tage die zeigen, dass es anders geht: Datenschutzkonform und mit mehr Sicherheit für die Daten, wenn auch mit der einen oder anderen Einschränkung in der Bedienung oder Funktion. Ob sich diese Lösungen aber durchsetzen werden, hängt von der Akzeptanz von uns Nutzern ab und von unseren Entscheidungen wie wir die vorhandenen Möglichkeiten einsetzen, welche Daten wir preisgeben und wie wir Sicherheitseinstellungen nutzen. Sind wir uns als Nutzer dieser Verantwortung immer bewusst und handeln entsprechend? Setzen wir mit unserem Kauf- und Nutzungsverhalten die richtigen Signale an die Hersteller und Anbieter?

Aus meiner Sicht stehen wir beim Lernprozess im Umgang mit dem Potential mobiler Geräte und Internetdienste noch am Anfang und kämpfen mit der Akzeptanz notwendiger Regeln. Als Belohnung winkt jedoch die freie Informationsquelle Internet und das Recht auf ihre unbeobachtete Nutzung.

Im vorliegenden Heft möchten die Autoren daher auf aktuelle Baustellen bei mobiler Dienstenutzung hinweisen und Anregungen zu gegenwärtig diskutierten Anwendung mit hohen Ansprüchen an den Schutz gegen Manipulation geben, wie bei der Smartphone-Geldbörse und dem Einsatz qualifizierter elektronischer Signaturen mit dem neuen Personalausweis.

Beginnend mit dem Beitrag zu Smartphone-Angriffsvektoren richten wir zunächst den Fokus auf aktuelle und potentielle Gefahren bei der Smartphone-Nutzung aus unterschiedlichen Perspektiven. Anwender und Unternehmen sollten sich dieser Aspekte bewusst sein und diese in ihre Nutzung und Richtlinien einbeziehen, um die Kontrolle über private und andere schützenswerte Daten zu behalten.

Den Apps, als zentralem Erfolgsfaktor der Smartphones – aber auch als ihre Achillesferse – widmen sich die Autoren mit Fragestellungen zu Risiken und der sicheren Handhabung: einem Bereich der kontrovers von Unternehmen, Lösungsanbietern und Sicherheitsforschung diskutiert wird. Die Einen sehen in mobilen Virenskannern und persönlichen Firewalls wichtige Schutzmechanismen, Andere lehnen dies als ungeeignet ab und fordern mehr Transparenz und Sicherheit in den App-Märkten. Unstrittig dürfte indes sein, dass sichere Anwendungen entsprechendes Know-how bei Entwicklern voraussetzen und diese Qualität sowohl Geld kostet als auch durch Tests nachgewiesen werden sollte.

Dennoch sollten wir nicht nur die Geräte selbst und installierte Anwendungen betrachten. Auch auf die Auswirkungen mobiler Geräte auf die Infrastruktur im Unternehmen, deren Schutz und die bestehenden Möglichkeiten durch Mobile Device Management soll hingewiesen werden. Eine mögliche Hilfestellung dabei könnte durch Anwendungen des Trusted Computing erbracht werden, wie der Beitrag zur sicheren Trennung privater und beruflicher Nutzerumgebungen innerhalb eines Geräts zeigt.

Wie bei allen jungen Technologien zeigt sich auch hier: Zunächst drängt die Neugier die Möglichkeiten auszuloten, aber mit ihrem Boom wird auch die Notwendigkeit zu Fragen von Missbrauch und Schutz drängender. Bis zum Etablieren von übergreifenden Sicherheitsstandards wird es vermutlich noch etwas dauern. Die Nachfrage nach Schutzmechanismen und sicheren Anwendungen hat aber bereits jetzt zu vielen Initiativen geführt die zukünftig mehr Schutz bieten könnten, wenn wir als Nutzer auch in Zukunft diesen Schutz aktiv einfordern.

Jens Heider