Das Ende der Paranoia?

Das Internet bietet uns Informationen in Hülle und Fülle. Doch jede Nutzung trägt dazu bei, dass auch unser Verhalten und unsere Daten Teil dieser Informationen werden. Diese Erkenntnis ist vermutlich mit den immer neuen Enthüllungen über den Datenhunger der NSA mehr denn je präsent. So analysiert auch Ingo Ruhmann in der Forum-Rubik den dadurch verursachten Schaden und betrachtet die Folgen für die IT-Sicherheit.

Aus technischer Sicht sind die verwendeten Methoden der NSA jedoch wenig spektakulär. Es werden schlicht lange bekannte Schwächen und entsprechend hoher Einfluss sehr konsequent ausgenutzt. Zumindest in technischer Hinsicht eine Vorgehensweise, die nicht exklusiv Geheimdiensten vorbehalten ist, aber deren Erwähnung gerne als zu paranoid eingeschätzt wurde. So sind die medienwirksamen Enthüllungen eigentlich eine wichtige Erinnerung daran, dass Investitionen in Sicherheitsmaßnahmen und deren flächendeckenden Verwendung keine Frage der Einhaltung von enervierenden Richtlinien ist, sondern zu einer Reduktion des realen Risikos führt. Wenn man also das konsequente Ausnutzen von Schwachstellen als reale Gefahr vor Augen geführt bekommt, lohnt die Suche nach weiteren potentiellen Angriffszielen, die es zu schützen gilt.

Mit dem Schwerpunkt-Thema Mobile System Security richten wir daher zunächst den Blick auf Angriffspotentiale und Schutzmechanismen für Smart Mobile Devices (SMDs) im Allgemeinen. Mit der Analyse der Defizite verfügbarer Schutzmechanismen und dem Problem der Abwehr bisher unbekannter Angriffsmuster wird der Ansatz eines Anomalieerkennungsverfahrens für SMDs motiviert.

Im Anschluss der allgemeinen Betrachtung der SMDs werden die Herausforderungen und Strategien für den Umgang mit Apps im Arbeitsumfeld dargestellt. Einem Umfeld das für Angreifer hoch interessante Informationen enthält und dessen Produkte in meinem Testlaboralltag häufig ein breites Spektrum an ausnutzbaren Schwächen aufweisen. Zudem durchdringen SMDs kontinuierlich die verschiedensten Arbeitswelten und spielen in immer mehr Bereichen des Privatlebens eine zentrale Rolle. Gute Voraussetzungen, nicht nur für die NSA.

Einem konkreten Einsatzgebiet der SMDs widmet sich ein Beitrag mit der Betrachtung von NFC Bezahllösungen. Den aufgezeigten Angriffsszenarien kann mit zusätzlichen Sicherheitsmechanismen begegnet werden, bei deren Einsatz es jedoch sowohl technische als auch organisatorische Hürden zu überwinden gilt.

Aber auch die allgemeine und allgegenwärtige Verwendung von SMDs über die unterschiedlichen Zugangsnetze hinweg stellt Herausforderungen in der Abwehr von Angriffen bei gleichzeitiger Wahrung einer größtmöglichen Nutzbarkeit dar. Daher betrachtet ein weiterer Beitrag auch die Herausforderungen bei der sicheren mobilen Nutzung heterogener Netzwerke und eine neue Möglichkeit der Umsetzung. Mit der Nutzung des Extensible Authentication Protocols (EAP) werden die existierenden Verfahren für den Zugriffsschutz in einem einheitlichen Ansatz berücksichtigt.

Auch bei den vorgesellten Aspekten des Themenschwerpunktes ist somit eine zentrale Frage: Lässt sich der resultierende Angriff automatisieren und welche Voraussetzungen muss ein Angreifer dazu erfüllen? Die Ressourcen der NSA sind sicherlich immens, aber dennoch ist eine großflächige Informationsabschöpfung auf die Automatisierbarkeit der zugrundeliegenden Angriffe angewiesen und auch andere Angreifer können sich dieser Techniken bedienen. Fatal ist daher das Argument, dass es ohnehin keinen vollständigen Schutz gebe und daher sich auch eine Verbesserung in Teilbereichen nicht lohne. Wie auch bei der Bewertung gegen andere Angreifer gilt: der notwendige Aufwand bei der Durchführung eines Angriffs stellt die Hürde da, nicht die Machbarkeit an sich.

Es wird sich zeigen in welchem Maße die Enthüllungen nachhaltig zu einem vermehrten Einsatz von Verschlüsselung und anderen Schutzmaßnahmen führen und ob sich eine höhere Akzeptanz dieser Maßnahmen einstellt. Bis dahin bleibt nun die Gewissheit, dass ein gesundes Misstrauen und das Anwenden bewährter Schutzmaßnahmen nicht übertrieben sind.

Jens Heider