Leitfaden für mehr App-Sicherheit im Geschäftsumfeld

Angesichts der hohen Verbreitung unsicherer Apps hat die TÜV TRUST IT (*http://www.it-tuv.com/*) zu dem Thema am 29.04.2014 eine umfangreiche Praxishilfe unter dem Titel „App-Sicherheit im Geschäftsumfeld" herausgegeben. Der Leitfaden beschreibt die typischen Sicherheitsprobleme mobiler Anwendungen auf den Smartphones der Unternehmen und skizziert konkrete Lösungswege für das Mobile Security-Management. Er wird kostenlos zur Verfügung gestellt.

Hintergrund des Leitfadens sind die Ergebnisse einer Untersuchung von etwa 1.000 Apps durch die TÜV TRUST IT, bei der in fast jeder zweiten App teils eklatante Sicherheitsmängel festgestellt wurden. So ermitteln Apps beispielsweise über eine eingeschaltete Lokalisierungsfunktion den Standort des Nutzers, greifen regelmäßig auf das Adressbuch zu oder übertragen ungefragt Daten auf einen Server im Internet. Insbesondere bei kostenlosen Apps ist häufig festzustellen, dass Werbenetzwerke und andere Datensammler im Hintergrund aktiv sind. Sie zielen darauf ab, auf möglichst viele Informationen des mobilen Users zuzugreifen, um sie anschließend zu veräußern. Allein das amerikanische Unternehmen flurry.com sammelt eigenen Angaben zufolge täglich Daten aus über 3,5 Milliarden App-Sessions.

Eine praxisgerechte Hilfestellung bietet hierfür der Leitfaden des Security-Spezialisten. Er beschäftigt sich ausführlich mit den Bedrohungen durch Smartphone-Apps und nimmt eine Kategorisierung der Apps nach ihrer Gefährdungsstufe vor. Für Sicherheitsverantwortliche in Unternehmen hilfreich ist die enthaltene Checkliste. Diese ermöglicht es, auf einfache und transparente Weise, eigene Verbesserungspotenziale aufzudecken. Abschließend stellt der Leitfaden die Methodik des TÜV AppCheckers vor, bei dem mit einem selbst entwickelten Prüf-Framework anhand eines unternehmensindividuellen Risikoprofils Apps auf alle relevanten Bedrohungen hin getestet werden können. Die Analysen erfolgen sowohl mittels einer stetig wachsenden Wissensdatenbank innerhalb des Prüf-Frameworks als auch durch ergänzende manuelle Prüfungen. Das Ergebnis ist eine Empfehlung zur Einordnung der untersuchten Apps in White- und Blacklists, die auch über Schnittstellen direkt in das Mobile Device Managementsystem des Unternehmens übertragen werden können. Auch Updates von Apps werden automatisch erneut analysiert.

Der Leitfaden „App-Sicherheit im Geschäftsumfeld" kann kostenlos bestellt werden bei: *info@it-tuv.com*

G&D: SIM-Kartenplattform für MyWallet der Deutschen Telekom

Giesecke & Devrient (G&D) liefert mit der NFC-fähigen SIM-Karte SkySIM CX das zentrale Sicherheitselement für die MyWallet genannte digitale Brieftasche der Deutschen Telekom. Die MyWallet kann von allen Mobilfunkkunden der Deutschen Telekom genutzt werden, die ein NFC-fähiges Smartphone benutzen. Als Sicherheitspartner liefert G&D auch die Bezahlapplikation MasterCard PayPass, um die elektronische Bezahlfunktion der virtuellen Kreditkarte von ClickandBuy International Limited als erstes Produkt in der digitalen Brieftasche der Deutschen Telekom zu gewährleisten.

Bedienerfreundliche Bezahl-, und zukünftig Ticketing- und Ausweisanwendungen stellen besondere Anforderungen an die Sicherheit der SIM-Karte. Gemeinsam mit G&D hat die Deutsche Telekom diese speziellen Anforderungen in einer Sicherheitsarchitektur für NFC-fähige SIM-Karten umgesetzt. Diese SIM-Karten verfügen über einen Datentresor, der in der Maximalausführung ein Datenvolumen von bis zu 1,3 Megabyte bereitstellt. Die SIM-Karten verfügen über einen leistungsfähigen Prozessor, der in der Lage ist, trotz Ver- und Entschlüsselungsvorgang, die gewünschten Anwendungen innerhalb besonders kurzer Zeit zu laden. Die Anwendungen, wie die Kreditkartenfunktion und die dazu benötigten Daten, sind in speziell gesicherten Bereichen der Karte untergebracht.

Die NFC-fähige SIM-Karte aus der SkySIM CX-Familie ist von EMVCo, American Express, MasterCard und Visa zugelassen und erfüllt damit insbesondere die hohen Anforderungen an sichere Bezahlanwendungen wie AMEX ExpressPay, MasterCard PayPass und Visa payWave. Auf der SIM-Karte lassen sich mehrere verschiedene NFC-Anwendungen gleichzeitig sicher ausführen. Die SkySIM-CX-Familie unterstützt außerdem die Transit-Anwendungen MIFARE, CIPURSE und Calypso. Die SIM-Karten sind in den Formfaktoren 2FF, Micro-SIM und Nano-SIM verfügbar und mit 2G-, 3G- und LTE-Netzen kompatibel.

NCP Secure VPN GovNet Box

Die NCP Secure VPN GovNet Box ist eine hochsichere VPN-Lösung für die Geheimhaltungsstufe VS-NfD (Verschlusssache – Nur für den Dienstgebrauch) speziell für Ministerien, Behörden, die Bundeswehr und Firmen im Geheimschutzbereich.

Die „Secure VPN GovNet Box" der Firma NCP hat die Sicherheitsfreigabe des Bundesamtes für Sichere Informationstechnik (BSI) erhalten. Die Hardware-Lösung, die NCP zusammen mit dem Fraunhofer SIT entwickelt hat, verschlüsselt die Internet-Kommunikation zwischen Standorten. Fraunhofer SIT war beteiligt an Design und Implementierung des Produkts und unterstützte NCP auch bei der Zertifizierung durch das BSI. Leitgedanke des Projekts war es, Unternehmen und Behörden einen vertraulichen Kommunikationskanal zur Verfügung zu stellen und so wirksam vor Wirtschaftsspionage zu schützen. „Die GovNetBox verwendet modernste Techniken der IT Sicherheit, wie etwa ein hardware-basiertes Schutzkonzept auf Basis von Trusted Computing.

Teil der Implementierung ist ein Trusted-Platform-Modul (TPM). Dabei handelt es sich um einen Chip, der im Rahmen von Trusted Computing-Konzepten verwendet wird. Mittels kryptographischer Verfahren prüft der TPM den Zustand von Software und Hardware. Er gewährt den Zugriff auf geheime Schlüssel nur, wenn die Software auf der VPN-Box nicht manipuliert wurde. Andernfalls verweigert er die Schlüssel. Der TPM wird in der Box zum Schutz von Konfigurationsdaten verwendet und hat als passives Element keinen weiteren Einfluss auf das Verhalten der Box. Schnittstellen und Standards für den TPM definiert die von verschiedenen Industrievertretern getriebene Trusted Computing Group.

Die NCP Secure VPN GovNet Box ist ein Baustein der NCP „Next Generation Network Access Technology"- einer ganzheitlichen Remote Access VPN-Lösung. Die vom BSI offiziell zugelassene GovNet-Box wird via USB an beliebige Endgeräte mit Windows Betriebssystem (ab XP) angeschlossen und basiert auf einem gehärteten Linux Betriebssystem.