Achtung vor mobilen Bedrohungen

Blaulichtorganisationen sollten wegen der zunehmenden Verwendung von Smartphones und Tablets ihr Risikomanagement unter die Lupe nehmen.

Von Jonas Hofer, Mobile Security Engineer, Nomasis

Wenn Blaulichtorganisationen die Verwendung mobiler Geräte wie Smartphones und Tablets zulassen, müssen diese auch im Risikomanagement berücksichtigt werden. In der Praxis legen aber Sicherheitsverantwortliche den Schwerpunkt vor allem auf konventionelle PC-Endgeräte. Sie nutzen dabei zwar Anwendungen zum Management mobiler Geräte, gehen aber fälschlicherweise davon aus, dass diese auch vor mobilen Bedrohungen schützen. Aber Achtung: Enterprise-Mobility-Management-Anwendungen sind gut darin, Geräte zu verwalten, Daten auf Geräten zu löschen, private und Daten des Arbeitgebers auf dem Gerät zu separieren, Zugriffe auf Anwendungen und Inhalte zu erlauben oder Nutzer zu authentifizieren. Einen ausreichenden Schutz aber können nur Lösungen bieten, welche das gesamte Spektrum mobiler Risiken abdecken. Diese betreffen nicht nur Apps, sondern finden auch auf Geräte-, Netzwerk- und Inhalte-Ebene statt. So können etwa bösartige Apps Informationen auslesen, Hardware beschädigen oder unberechtigten Fernzugriff gewähren. Nicht umsonst liefern namhafte Software-Hersteller regelmässig Patches, um in ihren Apps enthaltene Lecks zu schliessen. Aber dies geschieht erst, wenn ein Vorfall die Schwachstelle an den Tag bringt. In der Zwischenzeit bleiben Geräte den Angriffen aus dem Web ausgesetzt. Wenn dann auch noch Nutzer die zur Verfügung gestellten Releases nicht installieren, können Hacker Daten während der Verbindung über WLAN oder Mobilfunk abfangen.

nomasis
secures your mobility

Integriert und benutzerfreundlich

Es bedarf deshalb entsprechender Schutzmassnahmen durch speziell dafür entwickelte «Endpoint Security»-Lösungen, wie z. B. Lookout. Eine solche muss vor anwendungsbasierten Bedrohungen Schutz bieten, netzwerkbasierte Bedrohungen und nicht autorisierte Nutzungen erkennen, Apps sichtbar machen, die aus nicht offiziellen App-Stores heruntergeladen werden und benutzerdefinierte Richtlinien für Problembenachrichtigungen für verschiedene Bedrohungsarten ermöglichen. Diese Lösungen beinhalten eine App für die Mitarbeitergeräte, welche über die Mobile-Device-Management-Software ausgerollt wird. Neben der App auf Mitarbeitergeräten wird als zweite Komponente eine Konsole benützt, in der die Geräte und entsprechende Bedrohungen sowie Problembehandlungsszenarien aufgelistet sind. Eine Aktivierung dieser Funktionen sollte im Hintergrund für den Nutzer unsichtbar ablaufen. Ist aber eine manuelle Interaktion erforderlich, muss diese möglichst einfach zu handhaben sein. Zum Beispiel, dass der Nutzer mit einem Klick auf einen Button unberechtigte Apps deinstalliert. Tut er dies nicht, können von der IT Massnahmen ergriffen werden, etwa indem das Gerät in Quarantäne genommen wird. Mit solchen Vorkehrungen, die speziell auf die Bedrohungen durch den Einsatz von Smartphones und Tablets ausgerichtet sind, sollten Sicherheitsverantwortliche ihr Risikomanagement auf ein zeitgemässes Level heben.