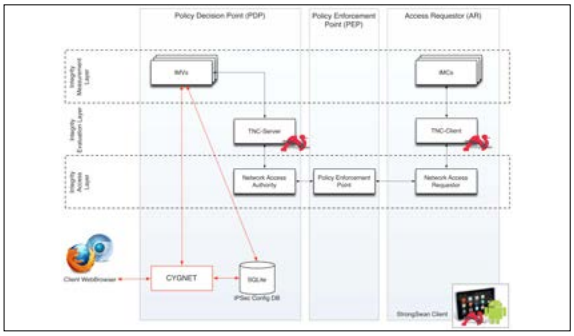
Stefan
Rohner

Marco
Tanner

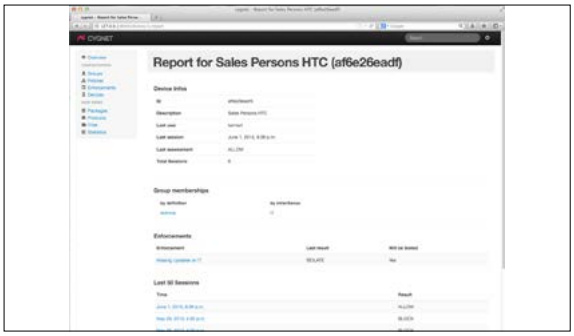
Diplomanden	Stefan Rohner, Marco Tanner
Examinator	Prof. Dr. Andreas Steffen
Experte	Dr. Ralf Hauser, PrivaSphere AG, Zürich
Themengebiet	Sicherheit

Cygnet

BYOD Malware Database Management Tool for Android



Übersicht der Komponenten



Screenshot der Overview-Ansicht

Ausgangslage: Jeder Informatikbetreiber muss sich heute mit der «Bring Your Own Device»(BYOD)-Thematik befassen, da Mitarbeitende mit ihren privaten Notebooks, Tablets oder Smartphones auf die Netzwerkdienste ihrer Organisation zugreifen möchten. Dies birgt Risiken, da diese Geräte nur teilweise kontrolliert werden können. Aufgrund der vielen unterschiedlichen Geräte und Client-Betriebssysteme können nur sehr schwer einheitliche Richtlinien für die Benutzung der Dienste erstellt werden. Durch den gleichzeitigen privaten Einsatz der Geräte kann es zu unfreiwilligen Datenfreigaben («Leaks») kommen. Malware, die sich auf Client-Geräten während des privaten Gebrauchs einnistet, kann sich während der geschäftlichen Verwendung im Firmennetzwerk verbreiten. Die strongSwan-VPN-Lösung versucht mit Implementierung des Trusted-Network-Connect-Standards, eine Milderung dieses Problems zu erreichen. Die vorliegende Arbeit soll eine Möglichkeit bieten, innerhalb einer BYOD-Umgebung eine möglichst einheitliche Richtlinie für alle Geräte zu konfigurieren, die von strongSwan durchgesetzt werden kann.

Vorgehen/Technologien: Cygnet wurde als webbasierte Applikation realisiert, um die Richtlinien zu definieren. Diese speichert Daten in einer SQLite-Datenbank, die gleichzeitig zum Datenaustausch mit strongSwan dient. Für die Webapplikation wurde auf das Python-Framework Django gesetzt, in Kombination mit JQuery für clientseitigen Code. Die Applikation ist für den Einsatz auf einem Apache-Webserver gedacht. Bei der Umsetzung wurde auf eine möglichst generische Implementierung geachtet. Die von strongSwan eingesetzten Integrity Measurement Verifier sind weiterhin Änderungen unterworfen und auch die Liste von möglichen Richtlinien ist noch unvollständig. Cygnet sollte dieser Dynamik gerecht werden. Es wurde eine Schnittstelle zu strongSwan definiert und implementiert, um Arbeitsschritte zwischen Cygnet und strongSwan zu übermitteln und Resultate auszuwerten. Dazu gehört eine Webapplikation, um die Richtlinien zu konfigurieren.

Ergebnis: Als Ergebnis liegt eine leicht bedienbare, ansprechende Applikation vor, die einem Administrator flexible Möglichkeiten bietet, eine umfassende Sicherheitsrichtlinie für die Clients seines Netzwerks zu konfigurieren und durchzusetzen.