Security by Isolation Prinzipien in der öffentlichen Verwaltung

Sanfte Migration zu virtualisierten Anwendungen bei bestehenden Betrieb im Rahmen des Open Security Projekts

Mihai Bartha, Oliver Maurhart
AIT Austrian Institute of Technology

April 8, 2014

Abstract

Das Open Security Projekt integriert "Security by Isolation" Techniken in die öffentliche Verwaltung. Hauptaugenmerk liegt dabei auf den Schutz gegen Viren und Trojaner beim unbedarften und sorglosen Umgang mit dem Internet, Schutz gegen Infektionen mit Malware beim Laden von Dokumenten von Datenträgern wie USB-Sticks und ähnlichen sowie Schutz vor der unbeabsichtigten Veröffentlichung vertraulicher Informationen. Die Integration der Schutzmaßnahmen erfolgt dabei unaufdringlich in eine bestehende IT Infrastruktur ohne die vorhanden und verwendeten domainspezifischen Lösungen und Einrichtungen zu gefährden. Wir zeigen in dieser Arbeit wie eine sanfte Überführung und Migration einzelner bestehender Anwendungsfälle im großen Maßstab im öffentlichen Bereich mit Hilfe von Open Source bei gleichzeitigen Betrieb erfolgen kann. Die angestrebte Lösung richtet sich nach dem Security by Isolation Ansatz aus mittels diesem Applikations- und Systemgrenzen definiert werden um potentielle Schadsoftware einzugrenzen.

1 Motivation

Outgoing scenario Protect sensible data Secure interaction with the internet with removable storage devices

Jede Organisation muss ihre IT-Infrastruktur vor internen und externen Gefahren schützen. Besonders davon betroffen sind auch öffentliche Institutionen, welche private Bürgerdaten wie Strafregister, Krankengeschichte und Meldedaten oder für die Staatssicherheit relevante Informationen verwalten.

Wie Einzelfälle und Statistiken belegen[1], kommt es aber immer wieder und zunehmend häufiger zu Vorfällen, bei denen private Daten in falsche Hände geraten. Solche Daten können in kürzester Zeit weltweit über das Internet verteilt werden, was schnell zu Worst-Case-Szenarien führen kann. So können beispielsweise private Adressen von Polizeibeamten ihren Weg zu kriminellen Organisationen finden oder private Gesundheitsdaten in die Hände potenzieller zukünftiger Arbeitgeber.

Durch die sensible Natur dieser Informationen, sind die Nutzer solcher öffentlichen Einrichtungen oft zu geschlossenen und sicheren lokalen Netzwerk gedrängt. Diese Systeme verfügen oft über

[1] WELCHE?

keinen Zugang zum Internet (WWW) oder über Anschlüsse für tragbare Speichermedien (TSM) um den sorgfältigen Umgang mit diesen Daten zu gewährleisten.

Das von der FFG[2] geförderte Open Security[3] Projekt bietet eine Lösung, die Angestellten davor schützt, kritische oder sensible Daten ungewollt preiszugeben. Dieser Schutz beläuft sich auf den Verlust oder den Diebstahl von Datenträgern (z.B. USB-Sticks) und den Befall des Rechners oder Notebooks von Viren, Trojanern und dergleichen. Dabei soll jeder Computer oder Terminal einer Organisation so ausgestattet werden, dass unkontrollierter Datenaustausch verhindert wird.

Bei diesem Projekt kommt erschwerend zur Aufgabenstellung hinzu, dass die Zielumgebung ein heterogenes Anwendungs- und Systemspektrum aufweist, keines der betroffenen Systeme völlig neu aufgesetzt werden darf und ein Rollout zentral gesteuert auf mehreren Rechnern, möglicherweise entfernt in parallel, stattfindet.

Unser Lösungsansatz im Open Security Projekt ist eine Client Architektur, die sicherstellt, dass alle auf tragbare Geräten gespeicherten Daten basierend auf einem Digital Rights Management automatisch verschlüsselt werden. Persönliche Daten von BürgerInnen können ausschließlich verschlüsselt auf Festplatten, optischen oder USB-Speichern sowie externe Netzlaufwerken gespeichert werden. Durch Open Security soll jeder Computer oder Terminal einer Organisation unabhängig von seinem Betriebssystem davor geschützt werden, unkontrollierten Datenaustausch zuzulassen. Das Einbringen oder das Mitnehmen von elektronischen Daten durch die Benutzer soll, im Sinne des Institution und des Benutzers selbst so erfolgen, dass es zu keinem Schaden oder Missbrauch kommen kann. Der gestohlene Laptop, der verlorengegangene USB-Speicher oder das verlegte Mobile Device (wie Tablet-PC oder Smartphone) sollen zukünftig außer dem materiellen keinen weiteren Schaden verursachen.

Im Fall, dass Hardware (z.B. ein Notebook) oder Speichermedien (z.B. ein USB-Stick) verloren gehen oder gestohlen werden, sind keine sensiblen unverschlüsselten Daten gefährdet. Wurden dennoch sensible Daten preisgegeben, was aufgrund von Richtlinien genehmigt werden kann, dann rekonstruiert die Kontrollkette aus den aufgezeichneten Datenströmen den Ereignispfad. Anhand der Informationen aus einem zentralisierten Logging kann nachvollzogen werden, welche Daten die Organisation verlassen haben und auf welchem Weg (z.B. durch welchen Benutzer, Medium).

Die Innovation von Open Security besteht in der Verbindung des DLP[4]-Ansatzes mit einer zentralen Management-Lösung und einer "Sicherheit durch Isolation" Architektur.

Das Internet, als dicht vernetztes Gefüge untereinander verbundener Geräte, bietet eine ideale Angriffsfläche für sich selbst replizierenden Schadcode. Aus diesem Grund ist Anti-Virensoftware ein zentraler Bestandteil jeder Sicherheitsstrategie. Eine solche Lösung ist stark abhängig von Signatur-Updates und schützt nur vor bekannten Malware. Nicht entdecktes Malware kann als erstes den Update-Mechanismus des Antivirus deaktivieren um später nicht entdeckt zu werden.

Im Open Security Projekt werden die "Security by Isolation" Konzepte angewendet um mögliche durch Malware verursachten Schaden entgegenzuwirken und die eine zentralisierte oder lokale Anti-Virus Architektur mittels Virtualisierung implementiert.

2 Security by Isolation

TBD: Was ist eigentlich Security By Isolation ...

[2] Österreichische Forschungsförderungsgesellschaft
[3] http://www.opensecurity.at
[4] ERKLÄRUNG

3 Architektur

TBD: Was ist unsere Architektur ...