OpenSecurity Benutzerhandbuch

Mihai Bartha
AIT Austrian Institute of Technology

June 24, 2014

1 Vorwort

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, 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.

Das von der FFG[1] geförderte Open Security[2] 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.

Die Open Security Aplikation bietet eine Lösung, die sicherstellt, dass alle auf tragbare Geräten gespeicherten Daten automatisch verschlüsselt werden. Persönliche Daten von BürgerInnen können ausschließlich verschlüsselt auf USB-Speichermedien gespeichert werden. 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.

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).

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 dieser Sicherheitslösung.

[1] Österreichische Forschungsförderungsgesellschaft
[2] http://www.opensecurity.at

2 Sicheres Surfen

Die OpenSecurity Managerr (OSM) ist eine lokal instaliertes Dienst welche die interaktion mit Internet Resourcen mediiert und sicheres Browsing ermöglicht. Beim Start einer Browser-Sitzung kümmert sich der OSM um die Aufbau einer Umgebung welche speziell nur für diese Sitzung verantwortlich ist. Beim beenden der Browser Sitzung wird dieses Umgebung entsorg und jegliche Temporäre Daten und nicht gesicherte heruntergeladene Dateien gelöscht.

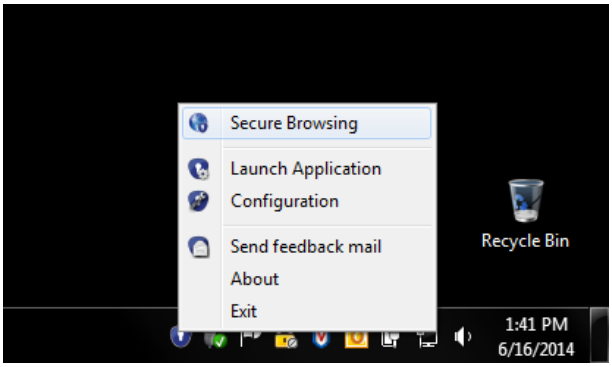

Figure 1: OpenSecurity TrayIcon

Eine neue Browser Sitzung kann mittels der in die Taskleiste befindliche OpenSecurity TrayIcon (blaues Schlüsselloch Symbol) gestartet werden. Durch einen click mit die rechte Mouse Taste auf die TrayIcon erscheint der Opensecurity Menü (Figure 1). Nach Auswahl der ersten Menüeintrag (Secure Browsing) wird die Browser Sitzung gestartet und der Eingebauten Browser angezeigt (Figure 2).

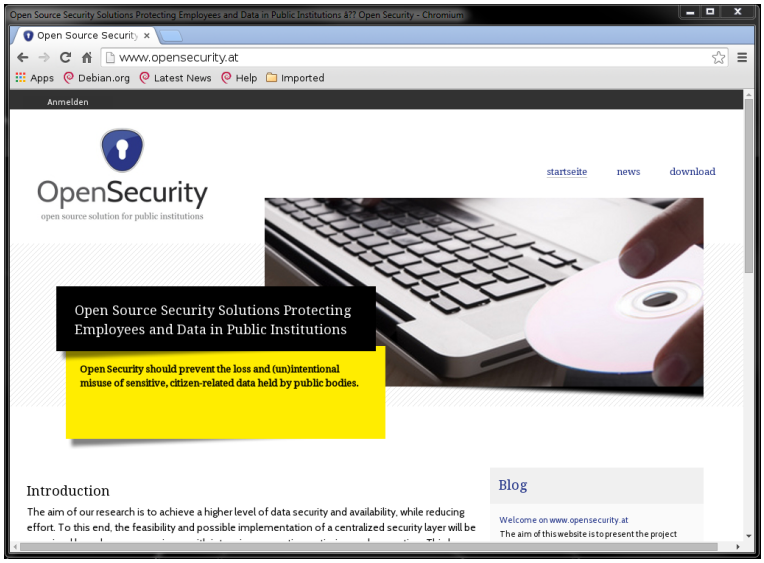

Figure 2: OpenSecurity Browser

Während eine bestehende Browser Sitzung der Benutzer kann Dateien von Internet herunterladen. Diese Dateien befinden sich auf eine automatisch angelegtes Netzlaufwerk namens *Download*. Das Zugriff auf dieses Verzeichniss ist möglich via Windows Explorer (Figure 3). Zu beachten ist dass die Inhalte der Download Verzeichniss sind nach dem Beenden der Sitzung unwiederruflich gelöscht. Inhalte die mann behalten möchte sollten gesichert werden bevor der Browser geschlossen wird. In gegensatz erden die Browser Einstellungen und gespeicherte Lesezeichen automatisch gesichert und gehen dadurch nicht verloren.

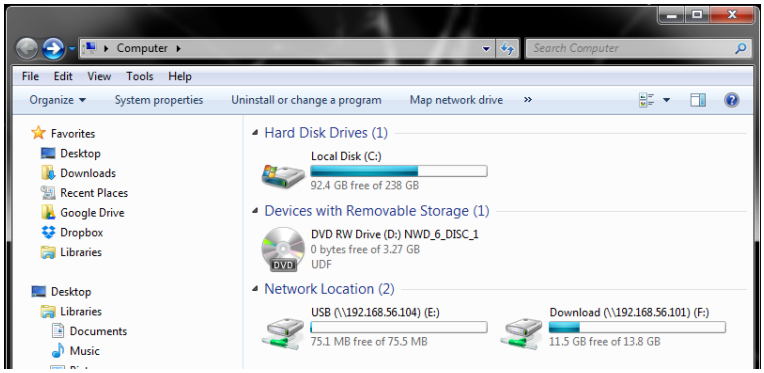

Figure 3: OpenSecurity Download Verzeichniss

3 Sichere Datenverwaltung auf externen Trägern

Der Umgang mit Daten auf externen Trägern wie USB Sticks hat neben dem Ziel den Anwender und damit das Host System von Malware zu schützen auch die Intention sensible Daten nur verschlüsselt auf diese Medien abzulegen. Analog zum Download Bereich aus vorigem Kapitel über das Sichere Surfen wird auch hier der Dateninhalt als eine Netzlaufwerk namens *USB* eingebunden (Figure 3). Vielmehr ein in OpenSecurity eingebautes Anti Viren System System prüft auch hier die betroffenen Dateien. Wird eine Datei als kompromittiert erkannt, schlägt eine Öffnen dieser Datei somit mit einer entsprechenden Fehlermeldung fehl.

Das exportieren von Daten ist nur auf verschlüsselte, für den Zweck vorbereitete, USB Speicher Medien möglich. Beim verbinden einer solche Medium wird der Benutzer angefordert eine Sicherheitsschlüssel einzugeben (Figure 4).

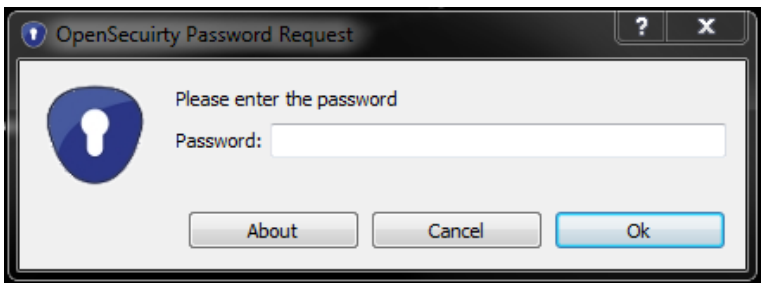

Figure 4: Schlüssel Anforderung

Sobald die richtige Schlüssel angegeben wird ist der betroffene medium entsperrt und Daten können gelesen bzw. geschrieben werden. Die Inhalte befinden sich in der *encrypted* Unterverzeichniss der *USB* Netzlaufwerk (Figure 5).

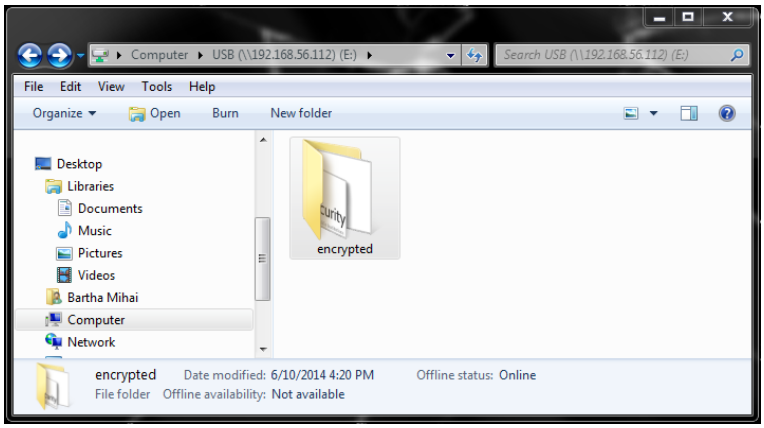

Figure 5: Verschlüsselte Verzeichniss (encrypted)

Das Ablegen und Speichern von Dateien auf dem Medium erzwingt das Verschlüsseln dieser Dateien. Eine versuch Dateien auf nicht verschlüsselte Medien zu Speichern ist nicht möglich und resultiert in eine Schreibzugrif Fehlermeldung (Figure 6)

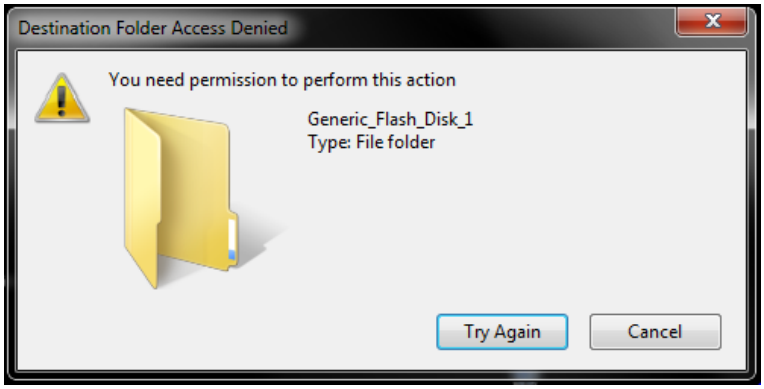

Figure 6: Fehlermeldung Unverschlüsseltes Speichern

4 Ausführen von Anwendungen

OpenSecurity verwendet in hintergrund Linux basierte Virtuelle Maschinen. Das bestehende Windows System wird dadurch mit neue Anwendungen erweitert (z.b. sicheres PDF viewer). Die in OpenSecurity installierte Anwendungen können durch Auswahl der *Launch Application* Menüeintrag in der TrayIcon ausgeführt werden (Figure 1). Mithilfe der Auswahlmaske in (Figure 7) wird die Ziel Virtuelle Maschine ausgewählt und die gewünschte Anwendung.

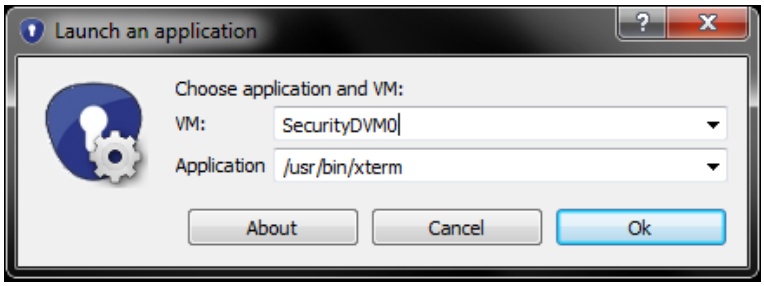

Figure 7: Ausführen von Anwendungen

Als Ergebniss dieser Beispiel wird die Fenster des X-Term anwendung angezeigt (Figure 8).

Figure 8: XTerm Anwendungsfenster

5 Konfiguration und Status und Feedback

Der *Send Feedback mail* Menüeintrag der TrayIcon kann dazu verwendet werden Probleme in bezug auf der OpenSecurity Software zu melden und Unterstützung anzufordern. Nach auswahl wird der lokal installierte standard eMail Anwendung gestartet (bsp. Outlook) und eine neue and Support adressierte eMail erstellt.

Auf die Konfiguration und Status Informationen des OpenSecurity Systems kann durch auswahl der *Configuration* Eintrag in der TrayIcon zugegriffen werden. Die Konfigurationsfenster (Figure 9) liefert informationen über der OpenSecurity Dienst zustand (*Service Status*), version (*Version*, lokal installierte Vorlage fur die Virtuelle Machinen (*Initial Template*) und laufende Virtuelle Maschinen (*Maschines*).

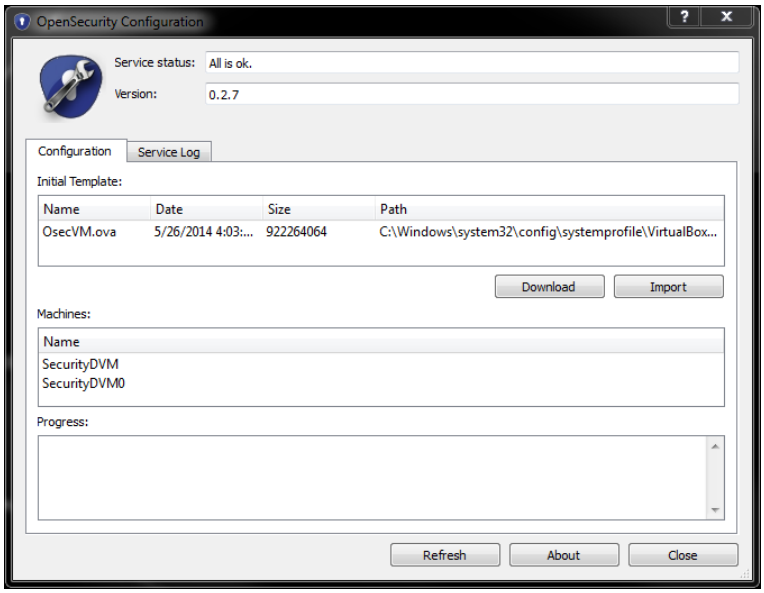

Figure 9: Konfigurationsfenster

Die lokal installierte VM Vorlage kann aktualisiert werden in zwei Schritten. Durch auswahl der Download Knopf wird die neueste Vorlage heruntergeladen. Dies kann anhängig von Netzwerkverbindung unterschiedlich lang dauern. Weiters durch auswalhl der *Import* Knopf wird die neue Vorlage importiert und aktualisiert. Wärend der Import Schritt werden alle laufende OpenSecurity Sitzungen terminiert und der OpenSecurity Dienst angehalten. Sicheres Browsing und Datenverwaltung auf externe Datenträger ist wärend diese zeit Nicht möglich. Der Konfiguration Ansicht kann durch auwhahl der *Refresh* Knopf aktualisiert werden. Der OpenSecurity Dienst Log kann duch auswahl der *Service Log* Karteireiter angesehen werden (Figure 10).

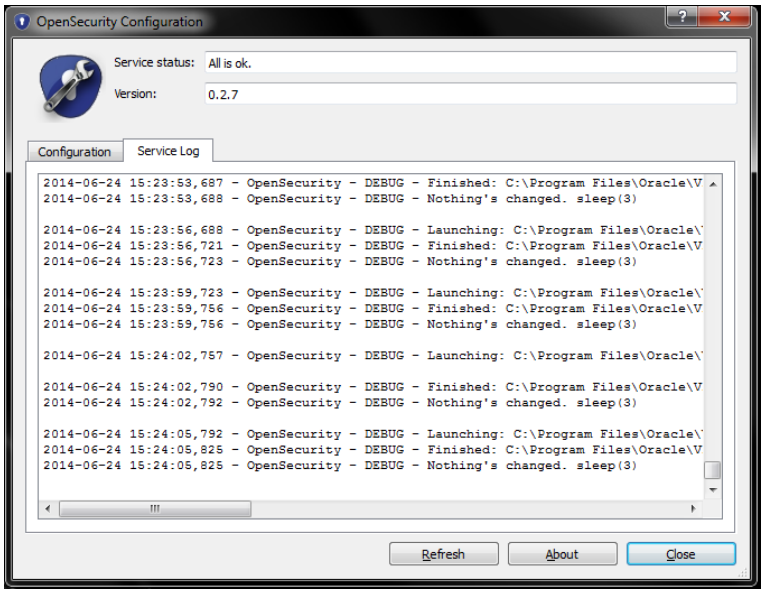

Figure 10: Dienst Log Ansicht