OpenSecurity Benutzerhandbuch zu Version 1.0

Mihai Bartha
AIT Austrian Institute of Technology

November 25, 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 Applikation 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

Der OpenSecurity Manager (OSM) ist ein lokal installierter Dienst, welcher die Interaktion mit Internet Ressourcen moderiert und sicheres Browsing ermöglicht. Beim Start einer Browsersitzung kümmert sich der OSM um den Aufbau einer Umgebung, welche speziell nur für diese Sitzung verantwortlich ist. Beim Beenden der Browsersitzung wird diese Umgebung entsorgt bzw. vernichtet und jegliche temporäre Daten und nicht gesicherte heruntergeladene Dateien gelöscht.

Zum Starten einer durch OpenSecurity gesicherten Browsersitzung dient ein Doppelklick auf das nach der Installation verfügbare Desktop Icon (Figure 1).

Figure 1: OpenSecurity Secure Browsing Desktop Icon

Eine Alternative dazu ist der Start einer neuen Browsersitzung mittels des in der Taskleiste befindlichen OpenSecurity TrayIcons (blaues Schlüsselloch Symbol). Durch einen Klick mit der rechten Maustaste auf das TrayIcon erscheint das OpenSecurity Menü (Figure 2). Nach Auswahl des ersten Menüeintrags ("Secure Browsing") wird die Browser Sitzung gestartet und der eingebauten Browser angezeigt (Figure 4).

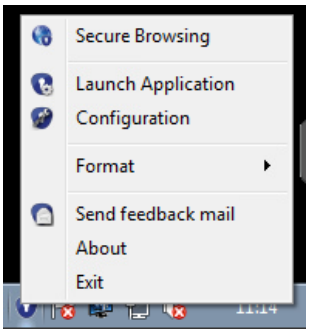

Figure 2: OpenSecurity TrayIcon

Während einer bestehender Browsersitzung kann der Benutzer Dateien von Internet herunterladen. Diese Dateien sind unter einem automatisch angelegtem Netzlaufwerk "*Download*" zugreifbar (Figure 3). Zu beachten ist, dass die Inhalte des Download Verzeichnisses nach dem Beenden der Sitzung unwiderruflich gelöscht sind. Sind über die Browsersitzung hinaus darin befindliche Dateien von Belang, so empfehlen wir diese aus diesem Verzeichnis lokal zu speichern.

Browser Einstellungen und gespeicherte Lesezeichen werden allerdings automatisch gesichert und gehen nicht verloren.

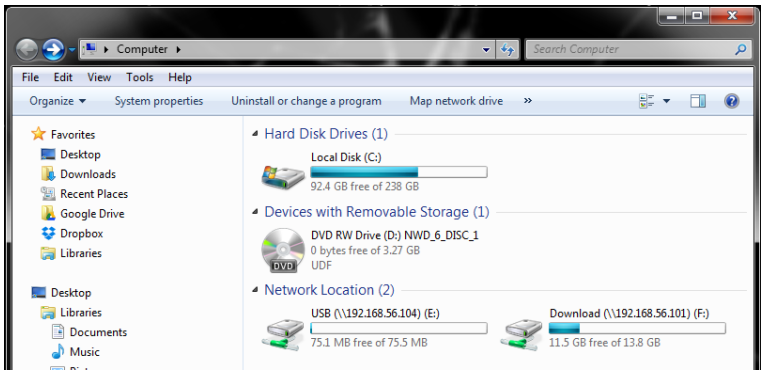

Figure 3: OpenSecurity Download Verzeichniss

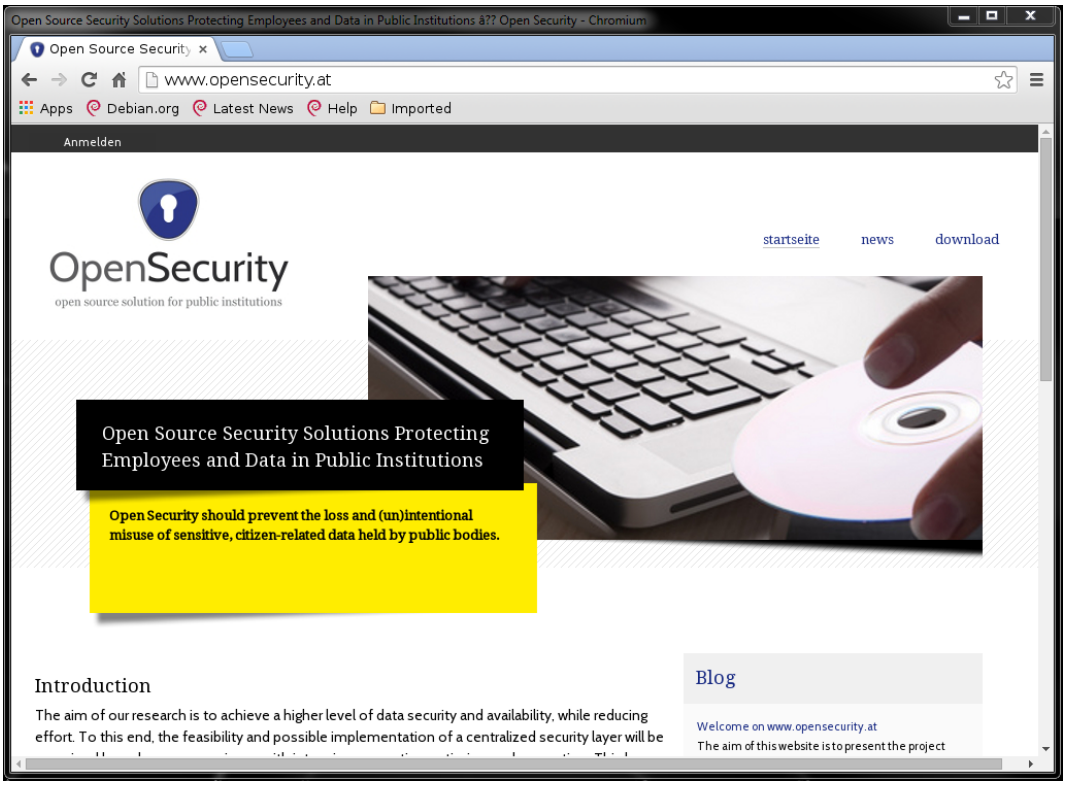

Figure 4: OpenSecurity Browser

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 dem vorigen Kapitel über das Sichere Surfen wird auch hier der Dateninhalt als ein Netzlaufwerk namens "*USB*" eingebunden (Figure 3). Ein in OpenSecurity eingebautes Anti Viren System System prüft hier die betroffenen Dateien. Wird eine Datei als kompromittiert erkannt, schlägt eine Öffnen dieser Datei mit einer entsprechenden Fehlermeldung fehl.

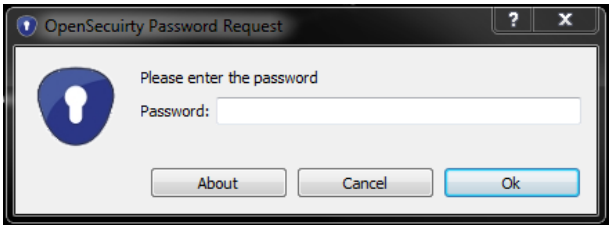

Figure 5: Schlüssel Anforderung

Das Exportieren von Daten ist nur auf verschlüsselte, für diesen Zweck vorbereitete, USB Speicher Medien möglich. Beim Verbinden eines solche Mediums wird der Benutzer aufgefordert ein Sicherheitsschlüssel bzw. Passwort einzugeben (Figure 5).

Sobald der richtige Schlüssel angegeben wurde, ist das betroffene Medium entsperrt und die Daten können gelesen bzw. geschrieben werden. Die Inhalte befinden sich in dem "*encrypted*" Unterverzeichnisses des "*USB*" Netzlaufwerk (Figure 6).

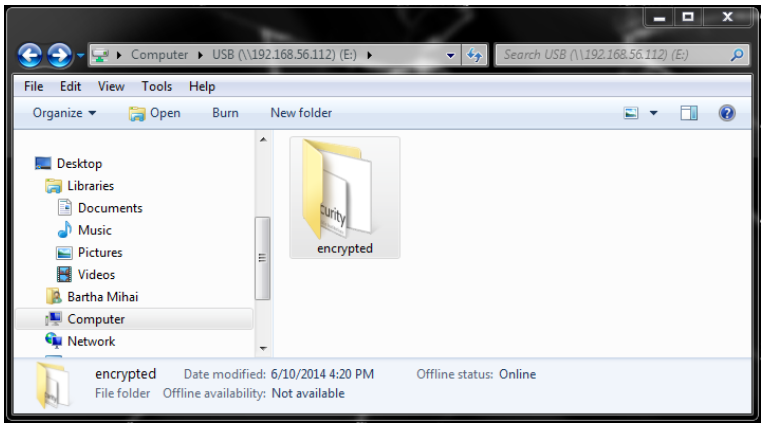

Figure 6: Verschlüsselte Verzeichniss (encrypted)

Das Ablegen und Speichern von Dateien auf dem Medium erzwingt das Verschlüsseln dieser Dateien. Ein Versuch Dateien auf nicht verschlüsselte Medien zu speichern ist nicht möglich und resultiert in einer Fehlermeldung (Schreibzugriffsrechte fehlen) (Figure 7).

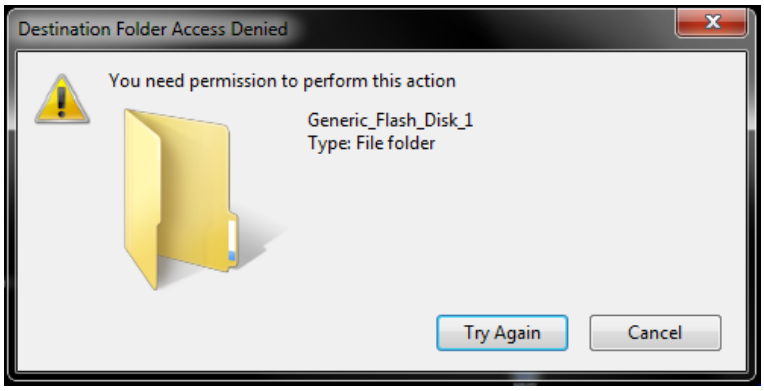

Figure 7: Fehlermeldung unverschlüsseltes Speichern

Datenträger können über den Menüpunkt "*Format*" im TrayIcon formatiert werden. Der User wird anschließend nach einem Schlüssel bzw. Passwort gefragt. Optional kann zusätzlich ein Keyfile angegeben werden.

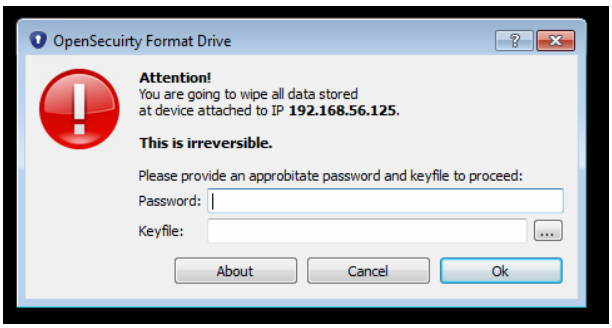

Figure 8: Formatierten und Verschlüsseln eines USB Sticks

Beachten Sie bitte, dass diese Aktion nicht mehr rückgängig gemacht werden kann. Daten, welche sich auf den USB Stick an der angeschlossenen VM befinden, werden vernichtet.

4 Ausführen von Anwendungen

OpenSecurity verwendet im Hintergrund Linux basierte Virtuelle Maschinen. Das bestehende Windows System kann dadurch mit neuen Anwendungen erweitert werden, bsp. mit einem sicheren PDF Viewer. Die in OpenSecurity installierten Anwendungen können durch Auswahl des "*Launch Application*" Menüeintrag aus dem TrayIcon ausgeführt werden (Figure 2). Mithilfe der Auswahlmaske in (Figure 9) wird die Virtuelle Maschine ausgewählt sowie die gewünschte Anwendung.

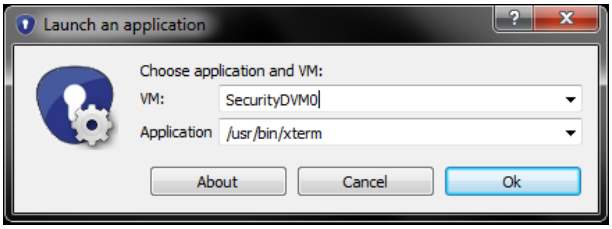

Figure 9: Ausführen von Anwendungen

Als Ergebnis dieses Beispiels wird in einem Fenster eine X-Term Anwendung angezeigt (Figure 10).

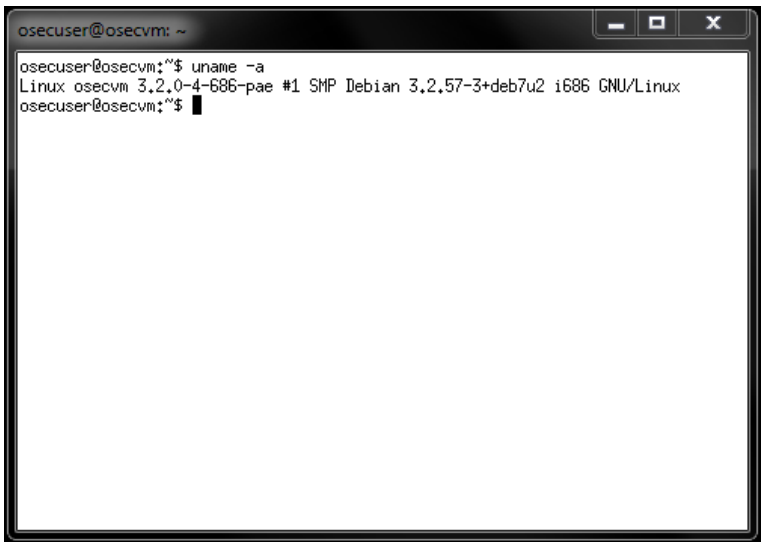

Figure 10: XTerm Anwendungsfenster

5 Konfiguration, Status und Feedback

Der "*Send feedback mail*" Menüeintrag der TrayIcon kann dazu verwendet werden, Probleme im Umgang mit der OpenSecurity Software zu melden und Unterstützung anzufordern. Nach Anwahl wird die lokal installierte Standard E-Mail Anwendung gestartet (bsp. Outlook) und eine neue an den OpenSecurity Support adressierte E-Mail erstellt.

Auf die Konfiguration und Status Informationen des OpenSecurity Systems kann durch Auswahl der "*Configuration*" Eintrags im TrayIcon zugegriffen werden. Das Konfigurationsfenster (Figure 11) liefert Informationen über den Zustand des OpenSecurity Dienstes ("*Service Status*"), Version ("*Version*"), lokal installierte Vorlagen für die Virtuelle Maschinen ("*Initial Template*") und laufende Virtuelle Maschinen ("*Maschines*").

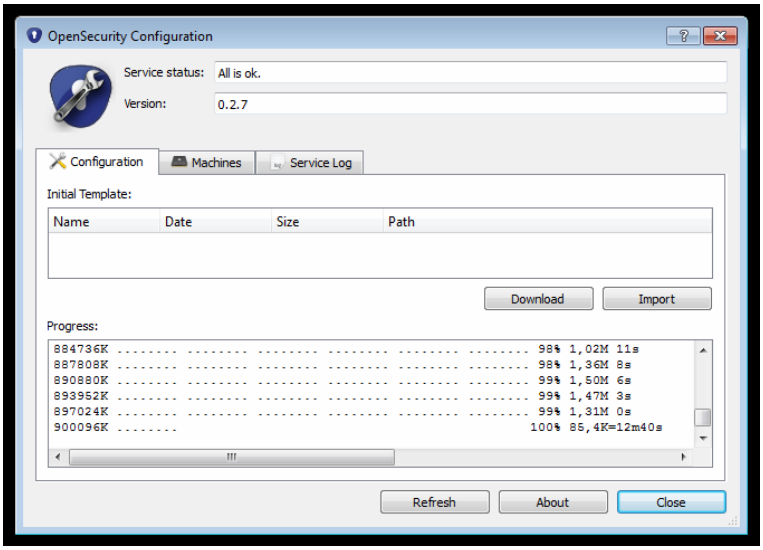

Figure 11: Konfigurationsfenster

Die lokal installierte Vorlage für instantiierende Virtuelle Maschinen kann in zwei Schritten aktualisiert werden. Durch Auswahl des "Download" Buttons wird die neueste Vorlage heruntergeladen. Da diese Vorlagen ein vollständiges Betriebssystem beinhaltet sind diese Dateien recht groß. Durch Auswahl des "*Import*" Buttons wird eine neue Vorlage importiert und aktualisiert. Während des Import Schrittes werden alle laufende OpenSecurity Sitzungen terminiert und der OpenSecurity Dienst angehalten. Sicheres Browsing und Datenverwaltung auf externe Datenträger ist während dieser Zeit nicht möglich.

Die Ansicht der Konfiguration kann durch Auswahl des "*Refresh*" Buttons aktualisiert werden.

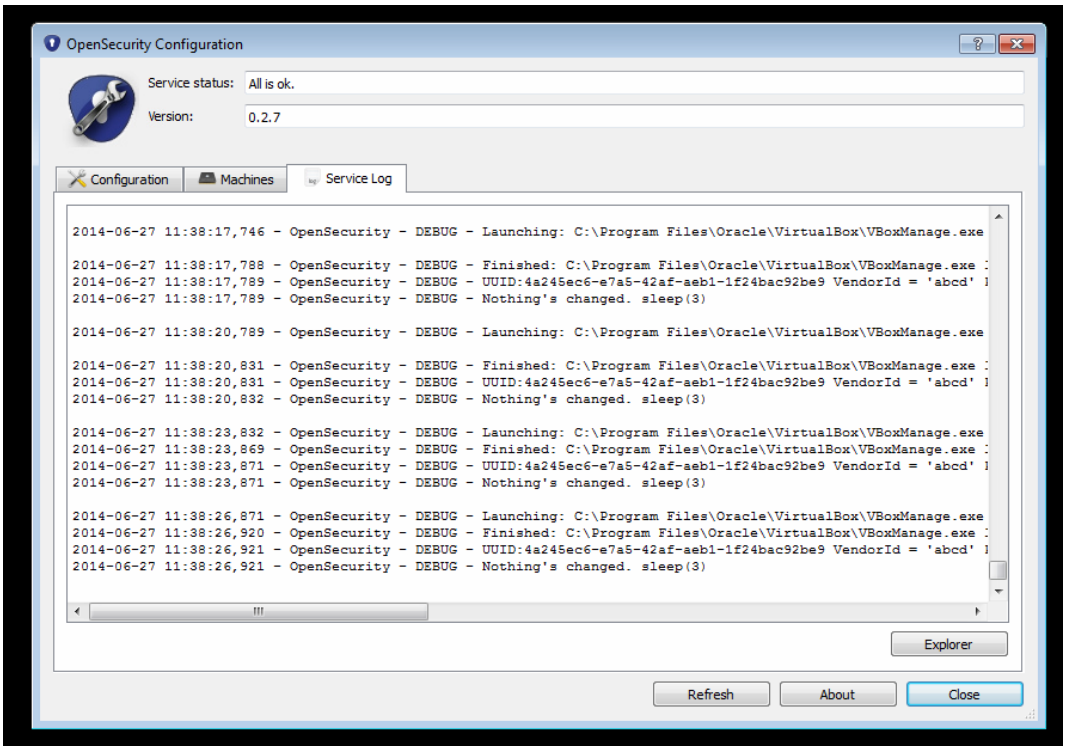

Figure 12: Dienst Log Ansicht

Im Karteireiter "*Service Log*" ist der Log des OpenSecurity Dienstes sichtbar (Figure 12). Hier können die Tätigkeiten des OpenSecurity Systems mitverfolgt werden. Ein Klick auf den "*Explorer*" Button öffnet den Windows Explorer auf dem Pfad zur Logdatei. Somit kann im Supportfall die Logdatei an E-Mails angehängt werden um dem OpenSecurity Team mehr Analysemöglichkeiten einzuräumen.