Implementierung einer Grafischen Benutzeroberfläche für die Konfiguration der Browser in the Box Security Policy

**Bachelorarbeit**

im Studiengang  
Informatik

vorgelegt von

**Ferhat Özmen**Matr.-Nr.: 008 204 835

am tt. Monat Jahr   
an der Hochschule Bochum

Erstprüfer/in: Prof. Dr. rer. nat. Rainer Lütticke  
Zweitprüfer/in: M.Sc. Clemens A. Schulz

# Kurzfassung

Inhaltsverzeichnis

[Kurzfassung 2](#_Toc442344325)

[Abbildungsverzeichnis 6](#_Toc442344326)

[Tabellenverzeichnis 6](#_Toc442344327)

[Abkürzungsverzeichnis 7](#_Toc442344328)

[Vorwort 8](#_Toc442344329)

[1 Einleitung 9](#_Toc442344330)

[1.1 Motivation 9](#_Toc442344331)

[1.2 Zielsetzung 9](#_Toc442344332)

[2 Grundlagen und Begriffsdefnition 10](#_Toc442344333)

[2.1 Endpoint Security 10](#_Toc442344334)

[2.1.1 Begriffe und Konventionen 10](#_Toc442344335)

[2.2 IT - Security Policy 10](#_Toc442344336)

[2.2.1 Definition 10](#_Toc442344337)

[2.2.2 Bedeutung für Software Entwickler 10](#_Toc442344338)

[2.2.3 Bedeutung für Software Anwender 10](#_Toc442344339)

[2.2.4 Aufbau einer Security Policy (Nach was?? Sirrix/SANS/BSI -> Clemens oder Norbert fragen) 10](#_Toc442344340)

[2.2.5 Typen von IT – Security Policies 10](#_Toc442344341)

[2.3 Browser in the Box 11](#_Toc442344342)

[2.4 Vorstellung 11](#_Toc442344343)

[2.4.1 Standalone 11](#_Toc442344344)

[2.4.2 Managed 11](#_Toc442344345)

[2.4.3 Bestehende Möglichkeit zur Konfiguration 11](#_Toc442344346)

[2.5 Technologien 11](#_Toc442344347)

[2.5.1 Virtual Box 11](#_Toc442344348)

[2.5.2 Python 11](#_Toc442344349)

[2.5.3 Abhängigkeiten 11](#_Toc442344350)

[2.6 Software Design 11](#_Toc442344351)

[2.6.1 Architektur 11](#_Toc442344352)

[2.6.2 Plattform 11](#_Toc442344353)

[2.6.3 Security Policy 11](#_Toc442344354)

[3 Implenetierung 12](#_Toc442344355)

[3.1 Grafische Benutzeroberfläche 12](#_Toc442344356)

[3.1.1 Details der Implementierung (Technisch) 12](#_Toc442344357)

[3.1.2 Beurteilung (Wieso letztendlich mit PySide e.t.c) 12](#_Toc442344358)

[3.2 Primäre Ziel der Implementierung 12](#_Toc442344359)

[3.3 Umsetzung (Wie die neue Konfiguration letztendlich umgesetzt wurde und warum e.t.c) 12](#_Toc442344360)

[4 Ergebnis 13](#_Toc442344361)

[4.1 Beispiele 13](#_Toc442344362)

[4.2 Benutzerfreundlichkeit 13](#_Toc442344363)

[4.2.1 Vorher 13](#_Toc442344364)

[4.2.2 Nachher 13](#_Toc442344365)

[5 Zusammenfassung 14](#_Toc442344366)

[6 Zusammenfassung und Ausblick 15](#_Toc442344367)

[Literaturverzeichnis 16](#_Toc442344368)

[Eidesstattliche Versicherung 17](#_Toc442344369)

[Auszug aus dem Strafgesetzbuch (StGB) 17](#_Toc442344370)

# Abbildungsverzeichnis

# Tabellenverzeichnis

# Abkürzungsverzeichnis

EPS Endpoint Security

BitBox Browser in the Box

VBox Virtual Box

# Vorwort

blablablalba

# Einleitung

Der Bedarf an Sicherheit ist heute eines der größten Bedürfnisse in der Informationstechnik. Die Bedrohung durch Wirtschaftsspionage und Cyberkriminelle nimmt weiter zu. Das wachsende Bedrohungspotential hat Auswirkung auf die Art und Weise wie Unternehmen mit der Sicherheit in der Informationstechnik umgehen. Die Unternehmen sind sich bewusst geworden, dass Sie im Firmennetzwerk, Internettechnologien wie z. B einen Browser nicht mehr ohne Sicherheitsmaßnahmen einsetzen können. Gerade in Zeiten in denen Antiviren Software keinen verlässlichen Schutz mehr bieten vor Angriffen über den Browser, erlaubt das Konzept von Browser in the Box ungehinderten Zugang zum Web und schützt das Betriebssystem vor Schadsoftware. Neben dem eigentlichen Schutz der Virtualisierten Umgebung, bekommt der Benutzer zusätzlich die Möglichkeit, die so geannten Security Policies der BitBox selber festzulegen.

## Motivation

Im letzten Teil der Einleitung wurde darauf hingewiesen, dass der Benutzer die Möglichkeit hat, die Security Policies der BitBox selber zu konfigurieren. Dabei muss klar gestellt werden, dass zwei Varianten von der BitBox entwickelt wurden. Die sogenannte Standalone Variante steht für Privatanwender kostenlos zur Verfügung. Die Managed Variante ist für Unternehmer, die allerdings Geld kostet. Die Unternehmerversion bietet die zentrale Administration aller BitBox Clients. Die Standalone Variante hingegen wird auf dem lokalen System verwaltet, es handelt sich also um eine Einzelplatz Lösung.

Allerdings konnte der Benutzer bei der Standalone Variante, die Einstellungen der Security Policies bisher nur während der Installation festlegen und hatte im Nachhinein keine Benutzerfreundliche Möglichkeit, um diese zu ändern. Der Anwender musste sich also den Umstand machen, die BitBox neu zu installieren, nur um die Policy zu ändern. Diese umständliche Methode sorgt zudem für eine schlechte Benutzererfahrung beim Benutzer, da die heutigen Endanwender es gewohnt sind, Konfigurationen an der Software, jederzeit durchführen zu können. Es ist also sehr wichtig, dem Benutzer diese Möglichkeit bei der BitBox Standalone ebenfalls zu ermöglichen.

## Zielsetzung

Im Rahmen dieser Bachelorarbeit soll die BitBox mit einer eigenständig laufenden Anwendung erweitert werden, die es dem Endbenutzer ermöglicht, die Security Policies über eine Komfortable und einfach zu bedienende Grafische Benutzeroberfläche einzustellen. Ziel ist es vor allem, dass diese Anwendung einen Benutzermodus anbietet und einen Administratormodus. Der Benutzermodus tritt in Kraft sobald die Anwendung aus der BitBox gestartet wird. Die Einstellungen des Benutzers müssen von der BitBox sofort übernommen werden, sofern diese vom Benutzer bestätigt wurden.

Der Administratormodus hingegen ist eine eigenständige Anwendung und wird vom Administrator außerhalb der BitBox gestartet. Die Einstellungen der Security Policies vorgenommen und in Form einer Policy Datei am gewünschten Ort gespeichert. Ziel hierbei ist es, dass der Administrator nicht für jede einzelne Installation der BitBox Standalone, die Einstellungen der Sicherheitsrichtlinien vornehmen muss, sondern die Policy Datei mit den gewünschten Einstellungen, der Installation beilegt und diese während der Installation automatisch übernommen werden. Dadurch soll dem Administrator überflüssige mehr Arbeit, erspart bleiben.

Der Benutzermodus muss zudem in den vorhandenen Quellcode der BitBox vollständig eingebunden sein. Die Anwendung selber startet zwar zur Laufzeit als eine eigenständige Ausführbare Anwendung, der Code selber ist allerdings mit der BitBox gekoppelt. Das bedeutet, dass der Benutzermodus teilweise vom Code der BitBox abhängig ist und somit außerhalb der BitBox nicht im Benutzermodus gestartet werden kann.

Der Administratormodus soll hingegen unabhängig vom Quellcode der BitBox funktionieren und steht deshalb in keiner Beziehung zum Quellcode der BitBox.

# Grundlagen und Begriffsdefinition

Dieses Kapitel bietet einen Einblick in die Grundlagen und Begriffsdefinition der Endpoint Security und Security Policy. Zunächst werden die Grundlagen, sowie einige Begriffsdefinitionen und Konventionen vermittelt, die in Bezug auf diese Bachelorarbeit eine Rolle spielen. Anschließend wird die BitBox näher vorgestellt und auf die Eingesetzten Technologien eingegangen, mit denen die BitBox Entwickelt wurde.

## Endpoint Security

Aufgrund der nicht klaren Definition des Begriffes Endpoint Security, ergibt sich die Notwendigkeit für die Klarstellung was denn mit Endpoint Security im Rahmen dieser Arbeit gemeint ist. Es muss also entschieden werden, was denn überhaupt Endpoints sind und welche Rolle die Sicherheit dabei spielt.

### Begriffe und Konventionen

Aus traditioneller Sicht betrachtet sind Endpoint Geräte vor allem Desktop Rechner und Laptops die an das Internet angeschlossen werden. Es sind also Systeme die Menschen benutzen um Daten zu erzeugen, löschen, manipulieren und versenden. Allerdings wissen wir, dass mittlerweile zu diesem Zweck nicht nur Desktop Rechner und Laptops eingesetzt werden, sondern Smartphones, Smart Watches, Mini-PCs und andere Hardware die am Endpunkt eines TCP/IP Netzwerkes angeschlossen werden. Deshalb kann man den Begriff Endpoint nicht auf bestimmte Geräte reduzieren oder erwarten dass dieser Begriff in Zukunft nicht sogar neu verstanden werden muss. Allerdings haben all diese Systeme etwas gemeinsam: Sie sind alle am Endpunkt eines TCP/IP Netzwerkes angeschlossen, die Verbindung kann dabei Kabellos (W-LAN, Mobile Internetverbindung) oder aber auch Kabelgebunden sein.

Sobald ein Endgerät mit einem Netzwerk verbunden ist, das eine Verbindung zum Internet hat, ist es automatisch der Gefahr ausgesetzt, dass es Gehackt, infiziert oder in irgendeiner anderen unerwünschten Weise manipuliert wird. Um derartiges zu vermeiden, muss das System die Möglichkeit anbieten, es so zu konfigurieren um derartige Angriffe abzuwehren.

Das System Windows zum Beispiel ist ein Endpunkt, wo der Benutzer über den Browser Zugang zum Internet bekommt und darüber auch mit dem Netzwerk interagiert. Windows, bietet die Kapazität einen speziellen Browser einzusetzen, mit dem die aufgezählten Angriffe abgewehrt werden können. Oder um es mit der Terminologie aus der Sicherheit in der Informationstechnik zu beschreiben: Eine Endpoint Security Lösung kann angewendet werden, für die Abwehr von Angriffen, die als Angriffsfläche den Browser des Endgerätes nutzen. Das Unternehmen Rohde & Schwarz Cybersecurity hat als Endpoint Security Lösung Browser in the Box entwickelt. Das heißt Angriffe aus dem Internet die über den Browser laufen sollen, würden nur innerhalb des gekapselten Browsers stattfinden und somit ins Leere gehen.

In der Gesamtheit versteht man unter Endpoint Security: Software, die Endgeräte vor Angriffen schützen soll.

## IT - Security Policy

Vor der eigentlichen Entwicklung von Endpoint Security Software, müssen die Security Policies (Sicherheitsrichtlinien) bestimmt werden. Für eine ausgereifte Endpoint Security Software, ist eine gut definierte Security Policy unabdingbar. Sie schreibt vor mit welcher Strategie, die Ziele, für die Informationssicherheit durch die Endpoint Security Software, erreicht werden. Vor allem in dieser Arbeit spielt die Security Policy eine wichtige Rolle. Schließlich war die Aufgabe, dem Benutzer eine Grafische Schnittstelle anzubieten, mit denen er die BitBox Security Policies konfigurieren kann.

Neben der eigentlichen Definition, ist wichtig zu verstehen welche Bedeutung die IT – Security Policy für den Software Entwickler hat und welche für den Anwender. Zudem werden Security Policies nach bestimmten Normen aufgebaut, auch hier muss geklärt werden, nach was die der BitBox angefertigt wurde. Ergänzend dazu hilft die Unterscheidung der Typen von Policies, um zu verstehen aus welchen Komponenten diese überhaupt aufgebaut werden können aber nicht müssen.

### Definition

Eine Security Policy ist eine auf höherer Ebene dokumentierte Anforderung, dessen Einhaltung von den Interessengruppen erwartet wird. Die Policy selber ist in der Regel kurz und formal gehalten. Im Idealfall sollte sie bündig und einfach zu verstehen sein, so dass jeder die in der Security Policy dargelegten Weisung einhalten kann. Wichtig zu verstehen ist hierbei, dass eine Security Policy nicht beschreibt, wie die Policy umgesetzt werden soll, sondern was konkret geschehen muss um die Sicherheit zu gewährleisten. Es ist also kein Dokument, das die technische Umsetzung beschreibt oder allgemein spezifische Lösungen vorgibt, für die Umsetzung der Security Policy in der Software selber.

Die Security Policy definiert Absichten und Regeln, deren Einhaltung dabei helfen soll die erforderte Sicherheit zu gewährleisten.

### Bedeutung für Software Entwickler

Die Entwickler bekommen wie bereits oben beschrieben, keine spezifische Lösung für die Implementierung der Security Policy vorgeschrieben. Die Entwickler müssen selber eine Lösung erarbeiten, wie sie die Policy in die Enpoint Security Software Umsätzen und am Ende implementieren.

Die Entwickler sind vor allem dazu verpflichtet bereits in der Entwurfsphase des Softwareentwicklungsprozesses, die Architektur und Entwurfsentscheidungen entsprechend der geforderten Security Policies zu wählen. Das heißt, dass keine Entscheidung getroffen werden darf, welche die gewünschten Policies nach der Implementierung, völlig oder teilweise nutzlos werden lässt.

Browser in the Box bietet zum Beispiel eine Security Policy an, wie Dateien die mit der BitBox heruntergeladen wurden, behandelt werden sollen. Der Benutzer hat die Möglichkeit die Policy so zu konfigurieren, dass alle heruntergeladenen Dateien automatisch abgelehnt werden, also die Datei nicht auf dem Host System gespeichert wird. Die Einhaltung der Policy soll gewährleisten, dass Schadprogramme oder andere schädlichen Dateien, nicht unkontrolliert auf dem Host System landen. Die Entwickler könnten den Entwurf der Software nun so gestalten, dass die Datei automatisch auf dem Host System sofort gelöscht wird, ohne dass der Benutzer etwas davon mit bekommt. Dadurch wäre aber die Policy nicht eingehalten worden, denn die Policy schreibt vor, dass diese Datei innerhalb der gekapselten Umgebung der BitBox bleiben soll und auf keinen Fall das Host System betreten darf, auch wenn diese Datei sofort gelöscht wird.

Für die Entwickler ist also sehr wichtig, dass sie Ihren Entwurf der Software so gestalten, dass auf alle Fälle die Security Policy genau eingehalten wird. Eine spätere Änderung, sofern dies überhaupt noch möglich ist, kann zu teilweise aufwendige Veränderung an der Software führen.

### Bedeutung für Software Anwender

### Aufbau einer Security Policy (Nach was?? Sirrix/SANS/BSI -> Clemens oder Norbert fragen)

### Typen von IT – Security Policies

#### Security Standards

#### Security Guidelines

#### Security Statements

## Browser in the Box

## Vorstellung

### Standalone

### Managed

### Bestehende Möglichkeit zur Konfiguration

## Technologien

### Virtual Box

### Python

### Abhängigkeiten

## Software Design

### Architektur

### Plattform

### Security Policy

#### Kopieren und Einfügen

#### Downloaden

#### Uploaden

#### Drucken

# Implenetierung

## Grafische Benutzeroberfläche

### Details der Implementierung (Technisch)

### Beurteilung (Wieso letztendlich mit PySide e.t.c)

## Primäre Ziel der Implementierung

## Umsetzung (Wie die neue Konfiguration letztendlich umgesetzt wurde und warum e.t.c)

# Ergebnis

## Beispiele

## Benutzerfreundlichkeit

### Vorher

### Nachher

# Zusammenfassung

# Zusammenfassung und Ausblick

# Literaturverzeichnis

# Eidesstattliche Versicherung

|  |  |  |  |
| --- | --- | --- | --- |
| Name:Ferhat |  | Vorname:Özmen |  |
| Matrikel-Nr.:008204835 |  | Studiengang:Informatik |  |

Hiermit versichere ich, ,Ferhat Özmen., an Eides statt, dass ich die vorliegende Bachelorarbeit mit dem Titel Implementierung einer Grafischen Benutzeroberfläche für die Konfiguration der Browser in the Box Security Policy selbständig und ohne fremde Hilfe verfasst und keine anderen als die angegebenen Hilfsmittel benutzt habe. Die Stellen der Arbeit, die dem Wortlaut oder dem Sinne nach anderen Werken ent­nommen wurden, sind in jedem Fall unter Angabe der Quelle kenntlich gemacht. Die Arbeit ist noch nicht veröffentlicht oder in anderer Form als Prüfungsleistung vorgelegt worden.

Ich habe die Bedeutung der eidesstattlichen Versicherung und prüfungsrechtlichen Folgen (§ 26 Abs. 2 Bachelor-SPO bzw. § 19 Abs. 2 Master-SPO der Hoch­schule der Medien Stuttgart) sowie die strafrechtlichen Folgen (siehe unten) einer unrichtigen oder unvollständigen eidesstattlichen Versicherung zur Kenntnis genommen.

## Auszug aus dem Strafgesetzbuch (StGB)

***§ 156 StGB*** Falsche Versicherung an Eides Statt

Wer von einer zur Abnahme einer Versicherung an Eides Statt zuständigen Behörde eine solche Versicherung falsch abgibt oder unter Berufung auf eine solche Versicherung falsch aussagt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

Ort, Datum Unterschrift