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 Sicherheitsrichtlinien der BitBox selber festzulegen.

## Motivation

Im letzten Teil der Einleitung wurde darauf hingewiesen, dass der Benutzer die Möglichkeit hat, die Sicherheitsrichtlinien der BitBox selber zu konfigurieren. Doch bevor auf die Möglichkeit der Einstellungen eingegangen wird, 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 Sicherheitsrichtlinien bisher nur während der Installation festlegen und hatte im Nachhinein keine Benutzerfreundliche Möglichkeit, um diese zu ändern. Der Anwender muss sich also den Umstand machen, die BitBox neu zu installieren, nur um die Sicherheitsrichtlinien zu ändern. Diese Methode sorgt zudem für eine schlechte Benutzererfahrung beim Benutzer, da die heutigen Endanwender es gewohnt sind, Konfigurationsmöglichkeiten 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 Sicherheitsrichtlinien 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 Sicherheitsrichtlinien 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 zur Laufzeit zwar 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 Begriffsdefnition

## Endpoint Security

### Begriffe und Konventionen

## IT - Security Policy

### Definition

### Bedeutung für Software Entwickler

### 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