OpenSecurity

open source solution for public institutions

# Projekt: OpenSecurity
# Spezifikation der Anforderungen

# Dokument Kontrollseite

| | |
|---|---|
| **Ersteller** | X-NET |
| **Editor** | Wolfgang Eibner |
| **Gegenstand** | OpenSecurity – Spezifikation der Anforderungen<br>PSP 1.2.2 Deliverable „Anforderungskatalog erstellt“ |
| **Meeting Daten** | |
| **Meeting Ort** | |
| **Herausgeber** | OpenSecurity Konsorzium |
| **Typ** | Text |
| **Format** | Application/msword |
| **Sprache** | DE-AT |
| **Erstellungsdatum** | 2013-07-04 |
| **Rechte** | © Copyright “OpenSecurity consortium”. |
| **Leserkreis** | ☒ internal |
| **Review Status** | ☐ draft<br>☒ final |
| **Erforderliche Aktion** | ☐ von Partnern zu überprüfen |

# Revision history

| Version | Date | Modified by | Comments |
|---|---|---|---|
| 0.1 | 2013-07-04 | Wolfgang Eibner | Initial outline |
| 0.2 | 2013-07-09 | Wolfgang Eibner | Some work on Chapter 1 |
| 0.3 | 2013-07-15 | Wolfgang Eibner | Some work on Chapter 2 |
| 0.4 | 2013-07-17 | Wolfgang Eibner | Interview section in Chapter 2 |
| 0.5 | 2013-07-22 | Wolfgang Eibner | Rework and corrections |
| 0.6 | 2013-07-24 | Wolfgang Eibner | Some work on Chapter 3 |
| 0.7 | 2013-07-25 | Wolfgang Eibner | Some work on Chapter 3 |
| 0.8 | 2013-07-26 | Wolfgang Eibner | Some work on Chapter 3 and 4 |
| 0.9 | 2013-07-28 | Wolfgang Eibner | Some work on Chapter 3 and 4 |
| 0.10 | 2013-07-29 | Wolfgang Eibner | Final draft |
| 1.00 | 2013-07-30 | Wolfgang Eibner | Fixed typos, etc.; Final version |
| 1.01 | 2014-09-08 | Michela Vignoli | Fixed typos, wording, etc. |
| 1.02 | 2014-09-08 | Michela Vignoli | Translation in German |

# Inhaltsangabe

# 1 Einführung

## 1.1 Über dieses Dokument

Dieses Dokument beinhaltet eine Zusammenfassung der Anforderungen des OpenSecurity Projektes. Sie wurden im ersten Teil des AP2 “Bedarf und Anwendung” identifiziert und evaluiert und sind die Basis von OpenSecuritys Architektur und Software Design.

## 1.2 Über das OpenSecurity Projekt

Die Synopsis des OpenSecurity Projekts, die im Antrag für KIRAS[i] präsentiert wurde:

“OpenSecurity soll den Verlust und (un)beabsichtigten Missbrauch von sensiblen, persönlichen Daten von BürgerInnen, die von öffentlichen Stellen verwaltet werden verhindern. Das Ziel unserer Forschung ist einen höheren Grad an Datensicherheit und -Verfügbarkeit zu erreichen sowie Aufwand zu reduzieren.

Zu diesem Zweck wird die Machbarkeit und mögliche Implementierung einer zentralisierten Sicherheitsschicht basierend auf unserer Erfahrung mit Intensive Computing, Antivirus und Verschlüsselung erforscht werden. Diese Schicht wird jegliche Kommunikation, die auf Client Geräten stattfindet kontrollieren, verifizieren und verschlüsseln. [...].

OpenSecurity wird unter einer Lizenz zur Verfügung gestellt werden, die sowohl öffentliche Verifikation als auch Anpassung an heterogene ICT Systemlandschaften ermöglicht.”[1]

Das OpenSecurity Konsortium schließt zwei Bedarfsträger ein: Die “IKT Linz Infrastruktur GmbH” (IKTL) und das “Bundesministerium für Landesverteidigung und Sport” (BMLVS).

## 1.3 Ansatz

In einer ersten Phase identifizierten wir Risiken und Szenarien im Zusammenhang mit Datenverlust, Datenmissbrauch und Malwareinfektion. Basierend auf diesen Szenarien generierten wir einen Fragebogen, der sowohl eine Umfrage zu den Datenschutzmechanismen und Workflows, die derzeit bei den Bedarfsträgern in Verwendung sind, als auch Fragen zu zukünftigen Bedarf und Anforderungen, die vom OpenSecurity Projekt gedeckt werden sollten. Zusätzlich wurden in den Fragebogen

[1] Übersetzung ins Deutsche von M. Vignoli

auch Fragen zu Themen aufgenommen, die mit der Arbeit in AP4 „Verschlüsselung“ zusammenhängen.

Der Fragebogen wurde mit beiden Bedarfsträgern in einem Interview am 22.02.2013 abgeschlossen. Danach fassten wir die Ergebnisse zusammen und identifizierten die Kernpunkte der OpenSecurity Architektur. Die Kernpunkte wurden mit Input aus den Konsortialmeetings im März und Juni ergänzt sowie Einschränkungen und Grenzen der Architektur bestimmt.

In der Folge generierten wir eine Liste von Anforderungen, die die Anforderungen unserer Bedarfsträger unter Bezugnahme der Kernpunkte und Einschränkungen beschreibt.

## 1.4 Weitere Struktur dieses Dokuments

In Kapitel 2 werden die Bedarfsanalyse inklusive Szenarien, Fragebogen, dem Interview und dessen Ergebnisse abgedeckt.

Basierend auf diesen Resultaten wurden Kernpunkte und wichtige Use Cases definiert. Sowohl diese als auch einige Einschränkungen werden in Kapitel 3 diskutiert.

In Kapitel 4 sind die aus der Bedarfsanalyse generierten Anforderungen an die OpenSecurity Architektur aufgelistet.

# 2 Bedarfsanalyse

## 2.1 Identifizierte Risiken und Szenarien

Da die OpenSecurity Schicht “jegliche Kommunikation, die auf Client Geräten stattfindet kontrollieren, verifizieren und verschlüsseln” soll, entschieden wir die Risiken anhand der möglichen I/O Channels und verbundenen (Netzwerk-) Geräten zu identifizieren (siehe Bild 1 für eine Übersicht).

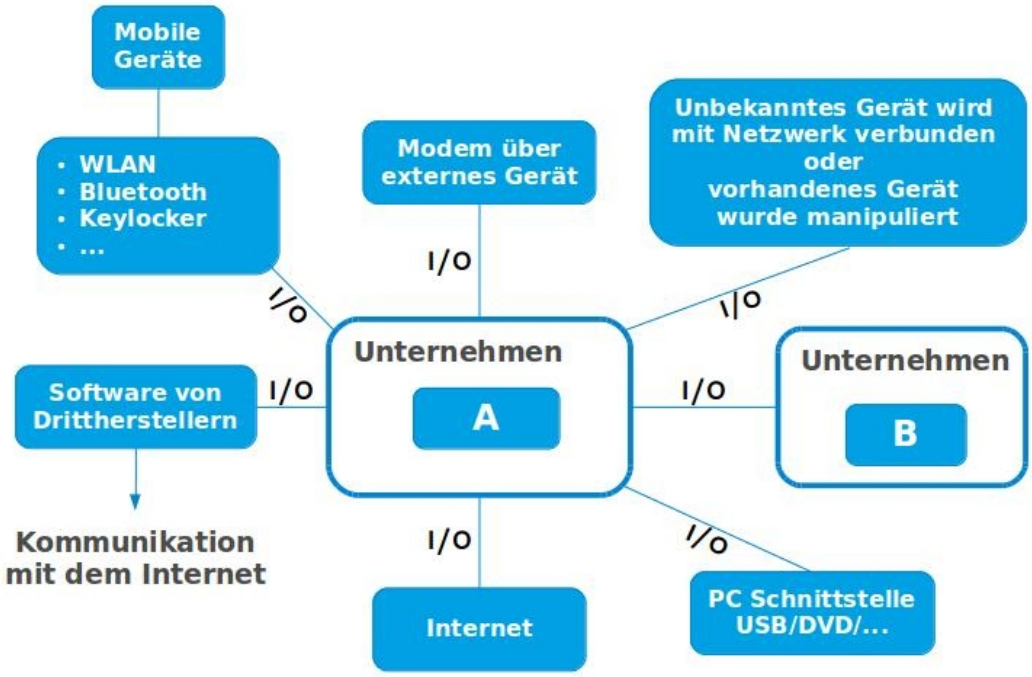


*Bild 1: Identifizierte Risiken und I/O Channels*

Basierend auf ihren primären Charakter “Speicher”/Gerät-I/O können die Risiken in drei verschiedene Risiko-Szenarien Gruppen unterteilt werden (plus einer Gruppe übriger Risiken).

### *2.1.1 Risiko-Szenario 1 – Speichermedien (USB Sticks, DVD, Blu-Ray, usw.)*

- Kopieren und exportieren von Daten (mutwillig/mit böswilliger Absicht)
- Kopieren und exportieren von Daten (beabsichtigt/erforderlich)
  - Verlust von Speichermedien

- Missbrauch durch Dritte (beabsichtigter Transfer und späterer Missbrauch, unbeobachteter Missbrauch)
- Manipulation der Daten beim Transport (Bruch der Übertragungsintegrität)

- Import von Daten (beabsichtigt/erforderlich)
  - erlaubt
  - unerlaubt
- Import von Daten (unbeabsichtigt oder mit böswilliger Absicht)
  - Malware
  - Manipulierte/fehlerhafte Information/Inhalt
- Hochfahren vom Speichermedium (z.B. starten eines schädlichen Betriebssystems)

### *2.1.2 Risiko-Szenario 2 – Internet/(unsichere) LAN Verbindungen*

- Copy/Paste/Upload
  - Durch einen Angestellten
  - Durch eine Applikation
- Mail Attachments senden
- Download von
  - Programmen und/oder Malware
  - Manipulierte/fehlerhafte Information/Inhalt
- Ausführung von (bereits vorhandener) Malware im LAN (z.B. von Netzwerkspeichern)
- Ein Smartphone als Modem oder alternative Internetverbindungsmechanismen verwenden

### *2.1.3 Risiko-Szenario 3 – Benutzung mobiler Geräte innerhalb und außerhalb des Unternehmens*

Daten werden (absichtlich) während der Arbeit im Unternehmen ohne Schutz kopiert. Danach wird das mobile Gerät (hauptsächlich Notebooks) aus dem Unternehmen transportiert (z.B. nach Hause) und ungeschützte Daten werden z.B. auf einen USB Stick kopiert.

Die Risiken dieses Szenarios ähneln den in Szenario 1 erwähnten. Sie müssen allerdings von der OpenSecurity Schicht anders behandelt werden, da mobile Geräte möglicherweise außerhalb des Firmennetzwerks genutzt werden.

### *2.1.4 Übrige Risiken und Szenarien*

- Screenshots / Screencasts
- Mikrofon / Soundcasts
- (Web)Kamera Aufnahmen, Videotelefonie (z.B. Skype)

## 2.2 Befragungen der Bedarfsträger

Wie in Abschnitt 1.3 erwähnt führten wir unsere Befragung[ii] mit beiden Bedarfsträgern in Interviews im Februar durch. Die folgenden Unterkapitel werden die Ergebnisse dieser Interviews wiedergeben. Ein Scan der Rohdaten kann hier gefunden werden[iii].

### *2.2.1 Datenimport und -export Szenario*

- Datenimport von und Datenexport auf ein externes Speichergerät soll möglich sein
  - auf den/vom lokalen Client Computer
  - auf den/vom lokalen (sicheren) Netzwerk – wenn möglich durch temporäres Speichern der Daten auf den lokalen Client Computer
- ein Workflow, der eine Quarantänestation/Inspection Bay enthält ist möglich, wenn
  - er einfach in bestehende IT Strukturen integriert werden kann
  - alle Workflows – mit Ausnahme von Fehlern und Sicherheitsverstößen – automatisiert sind und keine Supervisor-Interaktionen benötigen
  - er einfach und schnell ist [IKTL]
  - er auf mobilen Geräten ohne Verbindung zum Firmennetzwerk und Infrastruktur verwendet werden kann (Offline-Verfügbarkeit) – z.B. mit reduzierten Features [BMLVS]

Bezüglich Datenverschlüsselung und Entschlüsselung:

- BMLVS:
  - Die Daten sollen vor dem Export und (optional) nach dem Import verschlüsselt werden

    - Der User/die Userin soll einen User oder Gruppen Entschlüsselungs-Key eingeben (dies kontrolliert auch den Zugang von privilegierten Personen zu den verschlüsselten Daten)
- IKTL:
    - Die Daten sollen nur vor dem Export verschlüsselt werden
    - Die importierten Daten werden unverschlüsselt in Firmendateisystemen gespeichert werden
    - Standardisierte und weit verbreitete Verschlüsselungsalgorithmen sind sehr wichtig
- Import von Daten geschieht bereits verschlüsselt:
    - Dazu haben die Bedarfsträger keine klare Meinung
    - “User fragen, ob Daten entschlüsselt werden sollen” klingt nach einer guten Option
- Logging, insbesondere von Datenexport Aktivitäten, wurde als interessante Funktion erachtet
- Eine Überprüfung der Übertragungsintegrität (z.B. durch Hash-Summen) ist nicht notwendig

### *2.2.2 Internet/(unsichere) LAN Verbindung Szenario*

- Derzeitige und erwünschte Situation
    - IKTL: Derzeit wird der Internetzugang an User Workstations von Application-Layer-Firewalls kontrolliert. Der Internetzugang soll in einer OpenSecurity Umgebung einfach und schnell zu verwenden sein.
    - BMLVS: Derzeit können sich User außerhalb des Firmennetzwerks nur mit speziellen Client Computern Zugang zum Internet verschaffen. In Zukunft soll es möglich sein von den jeweiligen User Workstations sicher auf das Internet zuzugreifen.
- Nachdem die Maschine durch z.B. Malware kompromittiert wurde, soll es möglich sein diese leicht und schnell auf einen sauberen Zustand zurückzuversetzen. Es soll jedoch möglich sein Benutzereinstellungen im Internetzugangssystem (z.B. Bookmarks, Cookies) über eine Arbeitssitzung hinaus zu erhalten.
- Daten Import/Export vom/ins Internet kann, wie im Daten Import/Export Szenario, mittels einer Quarantänestation/Inspection Bay erfolgen; jedoch sollte eine Verschlüsselung nicht verbindlich sein.

- Copy & Paste von der Internet- zur Büroanwendungsumgebung sollte möglich sein; jedoch eventuell nur eingeschränkt (z.B. auf eine geringe Datenmenge).
- Emailzugang erfolgt über die Büroanwendungsumgebung.
- Andere verwendete Protokolle, welche in Betracht gezogen werden sollten: FTP, SFTP, FTPS.
    - Wie sollen firmeninterne Webseiten (Intranet) behandelt werden? [IKTL]Aus welcher Umgebung werden diese aufgerufen (Büroanwendungs- oder Internetumgebung)
    - Falls diese Intranet-Seiten auf externe Webseiten verweisen/diese benutzen: Wie können sie bzw. der/die UserIn Zugriff auf das Internet bekommen?

### *2.2.3 Mobile Geräte (hauptsächlich Notebooks) Szenario*

- Mobile Workstations:
    - Verschlüsselung: prinzipiell [BMLVS], größtenteils nicht [IKT]
    - Offline Funktionalität der OpenSecurity Schicht erwünscht [BMLVS]
    - Bei Datenexport ähnlich behandeln wie externe Speichergeräte
- Smartphones:
    - Derzeit keinen wesentlichen Bedarf [BMLVS]
    - Bereits im Einsatz und manchmal verschlüsselt [IKTL]

### *2.2.4 Verschlüsselung/Entschlüsselung*

Wie bereits erwähnt wurden in der Umfrage auch Themen im Zusammenhang mit dem Arbeitspaket 4 “Verschlüsselung” behandelt. Die Fragen zielten darauf ab die derzeitige Situation der Bedarfsträger und ihre zukünftigen Anforderungen an Verschlüsselungs-Funktionen der OpenSecurity Schicht zu evaluieren.

<u>BMLVS:</u>

- Clients und Server sind auf Dateisystemebene verschlüsselt
- Individuelle Dateien und Ordner werden für den Datentransfer verschlüsselt
- Benutzt werden weit verbreitete und standardisierte Verschlüsselungs-methoden; diese müssen sicher und zertifiziert sein, z.B. AES und TrueCrypt
- Auf geringe Vulnerabilität über lange Zeitspannen hinaus fokussiert (z.B. einige Jahre)

- Ver-/Entschlüsselung durch: Zertifikate bzw. Keyfiles und Passwort, public/private Keys oder Smartcards
- Die verwendete Verschlüsselungsmethode hängt von der Art der Daten und dem Zweck ihrer Nutzung (NATO, EU und nationale Richtlinien) ab; ein hauseigener Algorithmus für Hochsicherheitsbelange ist vorhanden

IKTL:

- Manche mobile Clients sind verschlüsselt
- Individuelle Dateien und Ordner werden für die Datenübertragung zum Teil verschlüsselt
- Auf Praktikabilität in einer breit gefächerten Usergruppe fokussiert, weshalb Verschlüsselung unkompliziert, schnell und einfach anzuwenden sein soll, z.B. BitLocker und TrueCrypt
- Ver-/Entschlüsselung (hauptsächlich) nur durch Passwort

# 3 Schlüsselaspekte und Use Cases

### *3.1.1 Schlüsselaspekte der Bedarfsträger*

Auf der Bedarfsanalyse in Kapitel 2 basierend identifizierten wir die folgenden Schlüsselaspekte unserer Bedarfsträger:

BMLVS‘ Fokus in OpenSecurity liegt auf der Gewährleistung von Sicherheit auf lange Sicht, sicheren Internetzugang und einer Lösung mit Offline-Funktionalität für mobile Workstations.

IKTL ist hingegen hauptsächlich auf Datenmissbrauch und die Verhinderung von Datenverlust, hohe Benutzerfreundlichkeit der OpenSecurity Software und einer einfachen Integration in ihre bestehende IT Infrastruktur fokussiert.

### *3.1.2 Sicherheitszonen*

Für eine bessere und genauere Beschreibung der Use Cases und Anforderungen empfehlen wir zwischen zwei Sicherheitszonen, die in der OpenSecurity Schicht verwendet werden, zu unterscheiden.

Sichere Zone/Safe Network: Geräte, Dateien und Workflows im jeweiligen Firmennetzwerk der Bedarfsträger. Hier befinden sich die sensiblen Informationen, die OpenSecurity vor Missbrauch und Manipulation schützen soll.
Diese Zone wird prinzipiell von den IT Departments der Institutionen gewartet und betreut und operiert innerhalb von klar definierten Betriebsparametern und Workflows.

Unsichere Zone/Unsafe Network: Alle Geräte, Dateien, Netzwerke und Workflows, die sich außerhalb der sicheren Zone befinden. Z.B. das Internet (und Internet-Anfragen), von Zuhause mitgebrachte, private UBS Sticks, sowie mobile Workstations, die bereits mit unbekannten und unsicheren Netzwerken verbunden waren gehören zu dieser Zone.
Die unsichere Zone wird von den IT-Abteilungen der Bedarfsträger nicht – oder nur minimal – überwacht, weswegen verschiedene unbekannte oder unerwartete Ereignisse sowie deren Auswirkungen eintreten können.

Eine der Hauptherausforderungen des OpenSecurity Projektes ist UserInnen zu ermöglichen innerhalb eines geschlossenen und sicheren, lokalen Netzwerks sicher mit externen Ressourcen zu arbeiten. Derzeit sind die UserInnen einerseits auf das institutionelle Netzwerk begrenzt, ein von der Außenwelt isoliertes sicheres Netzwerk, in dem sie mit sensiblen Informationen arbeiten. Andererseits können sie einfachen Zugang zu unsicheren Netzwerken und Ressourcen haben, was zu verschiedenen Sicherheitsbedrohungen für die sensiblen Informationen führt.

OpenSecurity versucht den Datenfluss zwischen diesen zwei Zonen zu kontrollieren und zu überwachen, um den UserInnen zu ermöglichen mit Ressourcen in beiden Zonen ohne Verlust des Schutzes sensibler Daten zu arbeiten und zu interagieren.

## 3.2 Use Cases

Nach einer detaillierten Diskussion unserer Ergebnisse glauben wir, dass die Architektur von OpenSecurity drei sicherheitsrelevante Use Cases unterscheiden soll[2].

- Interaktion mit Wechseldatenträgern (Import/Export von Daten)
- Sicherer Internetzugang
- Mobile Workstations (Notebooks)

Die nächsten Unterkapitel enthalten eine Übersicht über diese drei Use Cases und ihre Hauptbedrohungen, die den in Abschnitt 2.1 angeführten Risiken entsprechen. In Kapitel 4 sind Anforderungen an die OpenSecurity Architektur enthalten, um diese Bedrohungen zu vermeiden.

### *3.2.1 Interaktion mit Wechseldatenträgern (Import/Export von Daten)*

Workflow Beschreibung: Dieser Workflow behandelt Import und Export von Daten von und auf Wechseldatenträger wie USB Sticks, optische Medien (CD, DVD, Blu-Ray...) und so weiter. Typischerweise werden diese Geräte direkt an die Workstation/den Client PC der UserInnen angeschlossen, der sich in der sicheren Zone befindet. Jedoch befindet sich die Quelle (bei Datenimport) oder das Ziel (bei Datenexport) in der unsicheren Zone.

Hauptbedrohungen dieses Workflows sind:

- Aus Wechseldatenträgern importierte Daten können mit Malware infiziert sein, vor der die sichere Zone geschützt werden muss. Dies wird ein noch schwierigeres Unterfangen, wenn das Gerät oder Teile davon bereits verschlüsselt sind und dadurch nicht direkt auf Viren gescannt werden können.
- Durch den Datenexport auf externe Wechseldatenträger werden sensible Informationen unsicheren Zonen preisgegeben. Dadurch werden sie anfällig auf z.B. Verlust oder Diebstahl.

User Story: Der User/die Userin will auf eine Datei zugreifen, welche sich auf einem externen Speichergerät (z.B. USB Memory Stick) befindet, diese auf einem Computer innerhalb des Safe Networks bearbeiten und zurück auf dasselbe Gerät speichern, um sie zu einem lokalen Netzwerk-Share zu transportieren.

[2] Diese ähneln den drei Risiko-Szenarien in Abschnitt 2.1.

Die Datei kann – muss jedoch nicht zwingender Weise – sensible Informationen enthalten. Nehmen wir ersteres in Betracht, welches das heiklere Szenario ist, können einzelne Dateien oder der gesamte Inhalt des Massenspeichergerätes verschlüsselt sein. Zugleich könnte der Wechseldatenträger schadhaften Code enthalten, welcher identifiziert und, wenn möglich, entfernt werden sollte. Alternativ sollten die enthaltenen Dateien in Quarantäne gestellt werden.
Beim Speichern (Exportieren) der Daten auf ein externes Massenspeichergerät kann der User/die UserIn diese verschlüsseln.

### *3.2.2 Sicherer Internetzugang*

Workflow Beschreibung: Der zweite Workflow beinhaltet User-Anfragen ans Internet und damit verbundene Aktionen wie Dateien Down- und Uploads. Beim BMLVS geschieht dies derzeit über spezielle Workstations, die nicht mit dem Safe Network verbunden sind. Zukünftige Lösungen sollen UserInnen erlauben direkt ihre Firmen-Workstations zu verwenden, um die Benutzerfreundlichkeit zu steigern. Beim IKTL wird Internetzugang derzeit direkt über Firmen-Workstations innerhalb der sicheren Zone gewährt.

Hauptbedrohungen dieses Workflows sind:

- Die Verbindung der sicheren Zone mit unsicheren Zonen, wie dem Internet.
- Die Möglichkeit einer Malwareinfektion oder des Imports von ungewollten Dateien oder Programmen in die sichere Zone.
- Datenmissbrauch und Verlust durch den Export von sensiblen Informationen aus der sicheren Zone ins Internet (z.B. beim Upload oder Copy & Paste).
- Programme, die (im Hintergrund verborgen) kommunizieren und der dadurch entstehende nicht regulierte Datenfluss zu Dritten.

User Story: Der User/die Userin will eine Quelle vom unsicheren Netzwerk abrufen und diese im sicheren Netzwerk bearbeiten. Der User/die Userin muss einen Web-Browser verwenden können, um die Quelle zu finden, downzuloaden, zu speichern oder in die Zwischenablage zu kopieren.

### *3.2.3 Mobile Workstations (Notebooks)*

Workflow Beschreibung: Der dritte sicherheitsrelevante Use Case betrifft mobile Workstations. Diese Workstations (hauptsächlich Notebooks) werden von den Bedarfsträger-Angestellten sowohl innerhalb der sicheren Zone als auch in unsicheren Zonen verwendet (z.B. im Home Office, im Außendienst). Durch den mobilen Gebrauch und den Wechsel zwischen den Sicherheitszonen gibt es verschiedene Anforderungen, um den Zugang zu Internet und Speicher zu sichern.

Hauptbedrohungen dieses Workflows sind:

- Export sensibler Daten aus der sicheren Zone auf die mobile Workstation und in der Folge Verwendung/Transfer in unsichere Zonen.
- Import von vielleicht schädlichen Daten aus der unsicheren Zone auf die mobile Workstation. In der Folge werden die mobile Workstation und auch die darauf gespeicherten Daten (wieder) mit der sicheren Zone verbunden.
- Die mobile Workstation befindet sich, während diese in unsicheren Zonen verwendet wird, nicht unter Kontrolle und Aufsicht des IT Departments des Bedarfsträgers. Zusätzlich könnte es der OpenSecurity Lösung an Funktionalität mangeln, wenn diese auf zentrale Komponenten im Netzwerk des Bedarfsträgers angewiesen ist.

User Story: Nachdem das Notebook des Users/der Userin nach der Arbeit außerhalb der institutionellen Grenzen (mit nicht vertrauenswürdigen Netzwerken verbunden) verschiedenen Bedrohungen ausgesetzt wurde, verbindet es sich erneut mit dem Safe Network.

Aufgrund des hohen Risikos externer Netzwerke wird die Maschine als kompromittiert eingestuft und muss auf Malware überprüft werden. Bevor ihr Zugang zum Safe Network gewährt wird, muss sie als sicher deklariert werden.

## 3.3 Einschränkungen und Abgrenzung

Das OpenSecurity Projekt wird sich auf die drei oben erwähnten Use Cases beschränken. Deswegen können Risiken wie z.B. Screenshots, Manipulationen durch direkten physischen Zugang zur Workstation (z.B. Keylogger Geräte) und von Wechseldatenträgern bootende, schädliche Systeme nicht im Rahmen dieses Projektes angegangen werden. Die Meisten dieser Risiken können durch Zugangsbeschränkungen (z.B. BIOS Passwort) oder andere Policies verhindert werden.

Die Sicherheit von mobilen Geräten (Smartphones, Tablets, usw.) liegt nicht innerhalb des Projektrahmens, da diese Geräte eine Vielzahl an proprietärer Software verwenden und hierfür keine generische Lösung implementiert werden kann. Wir werden Smartphones jedoch als Speicher- oder Netzwerkgeräte in Betracht ziehen.

Usability und nichtfunktionale Anforderungen an Workflows und User Interfaces werden in diesem Dokument nur teilweise behandelt, da diese Teil des Arbeitspaketes 6 “Sozial-relevante Forschungsfragen” sind.

# 4 Anforderungen

## 4.1 Interaktion mit Wechseldatenträgern (Datenimport/Export)

| # | Beschreibung |
|---|---|
| **1** | **Interaktion mit Wechseldatenträgern** |
| 1.1 | Das Gerät darf nicht mit der sicheren Zone verbunden/für die sichere Zone (nativ) verfügbar sein, um die Ausführung oder die Infektion von/durch schädlichen Code zu verhindern. |
| 1.1.1 | Zu jeder Zeit ist es strikt verboten, dass ein User/eine Userin Zugang zum Gerät oder der innerhalb der sicheren Zone befindlichen Daten ohne die Verwendung eines OpenSecurity Clients und dessen Workflow erhält. |
| 1.1.2 | Die Geräte sollen mit einem System verbunden sein, welches im Idealfall auf dem Gerät befindlichen (Schad-)Code nicht nativ ausführen kann. |
| 1.2 | UserInnen sollen instruiert werden das Gerät mittels eines vordefinierten Workflows zu verbinden und den OpenSecurity Client für den Import/Export von Daten vom/zum Gerät zu verwenden. |

| | |
|---|---|
| **2** | **Datenimport vom Wechseldatenträger in die sichere Zone** |
| 2.1 | UserInnen sollten die Möglichkeit haben Gerät und Daten für den Import sowie, wenn erforderlich, Speicherziel für die importierten Dateien auszuwählen. |
| 2.1.1 | Die Auswahl des Speicherziels sollte sowohl vom lokalen Datensystem des Clients als auch von (verbundenen) Netzwerk-Shares innerhalb der sicheren Zone möglich sein. |
| 2.2 | Wenn ein Gerät oder bestimmte Daten auf demselben verschlüsselt zu sein scheinen, sollte der User/die Userin vor dem Start des Import Workflows aufgefordert werden die Daten zu entschlüsseln. |
| 2.2.1 | Wenn die Entschlüsselung nicht möglich ist oder der User/die Userin diese verweigert, sollten die verschlüsselten Daten nicht in die sichere Zone importiert werden. |
| 2.2.2 | Nicht entschlüsselte Daten sollten in Quarantäne gestellt und von einem Supervisor überprüft werden. |
| 2.3 | Vor dem Import müssen die Daten auf Viren überprüft werden. |
| 2.3.1 | Ein Virencheck sollte nach einer möglicherweise nötigen Entschlüsselung durchgeführt werden. |

| 2 | **Datenimport vom Wechseldatenträger in die sichere Zone** |
|---|---|
| 2.3.2 | Daten, die den Virencheck nicht bestehen, sollten in Quarantäne gestellt und von einem Supervisor überprüft werden. |
| 2.4 | Am Ende des Import Workflows sollten entschlüsselte und auf Viren überprüfte Daten an einen dem User/der Userin in der sicheren Zone zugänglichen Ort, oder an den von ihm/ihr gewählten Speicherort kopiert werden. |
| 2.4.1 | [Optional] Vor dem Kopieren der Daten an ihr Endziel sollten diese anhand der vom Bedarfsträger vordefinierten Methoden entschlüsselt werden. |

| 3 | **Datenexport aus der sicheren Zone auf einen Wechseldatenträger** |
|---|---|
| 3.1 | UserInnen sollten die zu exportierenden Daten sowie ihr Speicherziel (auf dem Gerät) auswählen können. |
| 3.1.1 | Die Auswahl der zu exportierenden Daten sollte sowohl vom lokalen Datensystem des Clients als auch von (verbundenen) Netzwerk-Shares innerhalb der sicheren Zone möglich sein. |
| 3.2 | [Optional] Die Daten sollten vor dem Export auf Viren überprüft werden. |
| 3.2.1 | Daten, die den Virencheck nicht bestehen sollten in Quarantäne gesetzt und von einem Supervisor überprüft werden. |
| 3.3 | Die Daten müssen vor dem Export entsprechend den von den Bedarfsträgern vordefinierten Methoden verschlüsselt werden. |
| 3.3.1 | Die Datenverschlüsselung muss nach dem (optionalen) Virencheck durchgeführt werden. |
| 3.3.2 | Der User/die Userin muss die nötigen Daten für die Entschlüsselung (z.B. Passwort oder Key) eingeben. |
| 3.4 | Der Datenexport sollte mit  mindestens Timestamp, User und Pfade der exportierten Daten zentral geloggt werden. |
| 3.5 | Am Ende des Export Workflows sollen Daten (optional) auf Viren überprüft werden. Die verschlüsselten Daten sollen auf das Gerät, welches aus der sicheren Zone hinaus gebracht werden wird, und ans Speicherziel, welches der User/die Userin ausgewählt hat, kopiert werden. |

## 4.2 Sicheren Internetzugang

| 4 | **Sicheren Internetzugang** |
|---|---|
| 4.1 | Da Internet und Internetzugang als unsicher eingestuft sind, müssen damit verbundene Workflows von der sicheren Zone getrennt werden. |
| 4.1.1 | Jedoch sollen User direkt von ihren Workstations Zugang zum Internet bekommen |

| | |
|---|---|
| | können. Also sollten sie keine andere Workstation in einer unsicheren Zone oder in einer Demilitarized Zone (DMZ) dazu verwenden müssen. |
| 4.1.2 | Unter “direkt von ihren Workstations” soll physisch verstanden werden, weswegen Lösungen wie VMs, Terminal Server Sessions, usw. nicht ausgeschlossen sind. |
| 4.1.3 | Datenflüsse zwischen Internet/unsicherer Zone und sicherer Zone, die nicht auf OpenSecurity Worksflows basieren, sind zu jeder Zeit strikt verboten. |
| 4.1.4 | Zugang zu und Arbeit mit Emails sind nicht zwingend Teil des sicheren Internetzugangs, da Emails innerhalb des Firmennetzwerks abgerufen werden. |
| 4.2 | Nach Kompromittierung durch z.B. Malware soll es möglich sein das sichere Internetzugangssystem leicht und schnell auf einen sauberen Zustand zurückzuversetzen. |
| 4.2.1 | Es sollte jedoch möglich sein im Internetzugangssystem Benutzereinstellungen (z.B. Bookmarks, Cookies) über eine Arbeitssitzung hinaus zu erhalten. |
| 4.3 | Andere verwendete Protokolle, die in Betracht gezogen werden sollten: FTP, SFTP, FTPS. |
| 4.4 | Der Umgang mit Firmenwebseiten sollte untersucht und beachtet werden. |
| 4.4.1 | Aus welcher Umgebung werden diese aufgerufen (Büroanwendungs- oder Internetumgebung)?<br>Falls diese Intranet-Seiten auf externe Webseiten verweisen/diese benutzen: Wie können sie bzw. der/die UserIn Zugriff auf das Internet bekommen? |

| **5** | **Datenimport/Export im sicheren Internetzugang** |
|---|---|
| 5.1 | User sollen Inhalte, Ressourcen oder Informationen aus dem Internet (unsichere Zone) finden und diese innerhalb der sicheren Zone verwenden und bearbeiten können. |
| 5.2 | User sollen Inhalte, Ressourcen oder Informationen aus der sicheren Zone ins Internet hochladen können. |
| 5.3 | Datenimport/Export vom/ins Internet kann und soll ähnlich wie in den in Absatz 4.1 beschriebenen Workflows durchgeführt werden. |
| 5.3.1 | Verschlüsselung bei Datenexport ins Internet sollte nicht obligatorisch sein. |
| 5.3.2 | Copy & Paste von der Internet- zur Büroanwendungsumgebung sollte möglich, jedoch eventuell nur eingeschränkt sein (z.B. auf eine geringe Datenmenge). |

## 4.3 Mobile Workstations (Notebooks)

| 6 | Mobile Workstations (Notebooks) |
|---|---|
| 6.1 | Prinzipiell sollten mobile Workstations und ihre Workflows wie normale User Workflows behandelt werden. Dies schließt sicheren Internetzugang und Interaktion mit Wechseldatenträgern mit ein. |
| 6.1.1 | Workflows des sicheren Internetzugangs und der Interaktion mit Wechseldatenträgern sollen auch funktionieren, wenn sich das Notebook außerhalb der institutionellen Grenzen/der sicheren Zone befindet (Offline-Verfügbarkeit). |
| 6.1.2 | Diese Offline-Verfügbarkeit könnte ein reduziertes Feature Set bieten. |
| 6.2 | Wenn ein Notebook in die sichere Zone zurückkehrt, nachdem es außerhalb der institutionellen Grenzen (mit unsicheren Netzwerken verbunden) war, wird es als kompromittiert eingestuft und muss daher einen OpenSecurity Check durchlaufen. |
| 6.2.1 | Dieser Check soll alle nötigen Schritte enthalten, z.B. Malwarescan, um ein sauberes und vertrauenswürdiges System zu gewährleisten, welches die sichere Zone nicht kompromittieren kann. |
| 6.2.2 | Vor dem Durchlaufen des OpenSecurity Checks ist kein Datentransfer zwischen Notebook und sicherer Zone erlaubt. |

## 4.4 Nichtfunktionale Anforderungen

| 7 | Nichtfunktionale Anforderungen |
|---|---|
| 7.1 | Die OpenSecurity Architektur soll ein modulares Konzept haben. |
| 7.1.1 | Malware Scanning soll von verschiedenen Scan-Engines ausgeführt werden können. |
| 7.1.2 | Malware Scanning sollte auf einem lokalen Client oder auf einem zentralen Server/Cluster ausgeführt werden. |
| 7.1.3 | Verschlüsselung sollte austauschbar sein, um verschiedene/mehr als einen Verschlüsselungsalgorithmus zuzulassen. |
| 7.2 | Die verwendeten Verschlüsselungsmethoden sollten standardisiert und weit verbreitet sein. |
| 7.3 | Alle OpenSecurity Workflows – mit Ausnahme von Fehlern und Sicherheitsverstößen – sollen automatisiert sein und keine Supervisor-Interaktionen erfordern. |
| 7.4 | Alle OpenSecurity Workflows sollen schnell und einfach zu verwenden sein. |
| 7.5 | Die OpenSecurity Schicht sollte sich einfach in bestehende IT Strukturen eingliedern lassen. |

[i] KIRAS_foerderungsansuchen_kooperative_fe-projekte_Open_Security_FINAL.pdf befinden sich auf http://www.opensecurity.at/projekt/antrag/KIRAS_foerderungsansuchen_kooperative_fe-projekte_Open_Security_FINAL.pdf

[ii] 20130122_Fragebogen_Bedarfserhebung.odt befinden sich auf http://www.opensecurity.at/arbeitspakte/ap2-bedarf-und-anwendung/bedarfserhebung/20130122_Fragebogen_Bedarfserhebung.odt

[iii] interviews_bedarfserhebung.pdf befinden sich auf http://www.opensecurity.at/arbeitspakte/ap2-bedarf-und-anwendung/bedarfserhebung/interviews_bedarfserhebung.pdf