**GDC-EDaSA-IDS**

**Lastenheft**

**Version 0.1**

Historie der Dokumentversionen

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Datum | Autor | Änderungsgrund / Bemerkungen |
| 0.1 | 2014/07 | Bernd Landgraf | Ersterstellung |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Historie der Dokumentversionen 2](#_Toc394492091)

[Inhaltsverzeichnis 2](#_Toc394492092)

[1 Introduction 4](#_Toc394492093)

[1.1 General 4](#_Toc394492094)

[1.1.1 Purpose of this document 4](#_Toc394492095)

[1.1.2 Product Scope 4](#_Toc394492096)

[1.1.3 Abkürzungen 4](#_Toc394492097)

[1.1.4 Ablage, Gültigkeit und Bezüge zu anderen Dokumenten 4](#_Toc394492098)

[1.2 Verteiler und Freigabe 4](#_Toc394492099)

[1.2.1 Verteiler für dieses Lastenheft 4](#_Toc394492100)

[1.3 Reviewvermerke und Meeting-Protokolle 4](#_Toc394492101)

[1.3.1 Erstes bis n-tes Review 4](#_Toc394492102)

[2 Product Perspective 5](#_Toc394492103)

[2.1 Product Goals and Benefits 5](#_Toc394492104)

[2.2 User Types 6](#_Toc394492105)

[2.3 User-Devices 6](#_Toc394492106)

[2.4 Deployment-Scenarios 6](#_Toc394492107)

[2.4.1 U1: Individual users 6](#_Toc394492108)

[2.4.2 U2: Companies 7](#_Toc394492109)

[2.5 Resources 7](#_Toc394492110)

[3 Attack-Detection Functions (AD) 8](#_Toc394492111)

[3.1 Intercept http/1.1 Traffic 8](#_Toc394492112)

[3.1.1 Description 8](#_Toc394492113)

[3.1.2 Dependencies 8](#_Toc394492114)

[3.1.3 Risks 8](#_Toc394492115)

[3.2 Intercept http/1.1 + SSL/TLS (https) Traffic 8](#_Toc394492116)

[3.2.1 Description 8](#_Toc394492117)

[3.2.2 Dependencies 8](#_Toc394492118)

[3.2.3 Risks 8](#_Toc394492119)

[3.3 Intercept websocket Traffic 8](#_Toc394492120)

[3.3.1 Description 8](#_Toc394492121)

[3.3.2 Dependencies 8](#_Toc394492122)

[3.3.3 Risks 9](#_Toc394492123)

[3.4 Intercept http/2 (spdy) Traffic 9](#_Toc394492124)

[3.4.1 Description 9](#_Toc394492125)

[3.4.2 Dependencies 9](#_Toc394492126)

[3.4.3 Risks 9](#_Toc394492127)

[3.5 Determine the content type 9](#_Toc394492128)

[3.5.1 Description 9](#_Toc394492129)

[3.5.2 Dependencies 9](#_Toc394492130)

[3.5.3 Risks 9](#_Toc394492131)

[3.6 Perform signature based analysis of the transferred content 9](#_Toc394492132)

[3.6.1 Description 10](#_Toc394492133)

[3.6.2 Dependencies 10](#_Toc394492134)

[3.6.3 Risks 10](#_Toc394492135)

[3.7 Perform anomaly based analysis of the transferred content 10](#_Toc394492136)

[3.7.1 Description 10](#_Toc394492137)

[3.7.2 Dependencies 10](#_Toc394492138)

[3.7.3 Risks 10](#_Toc394492139)

[3.8 Determine content danger-level 10](#_Toc394492140)

[3.8.1 Description 10](#_Toc394492141)

[3.8.2 Dependencies 10](#_Toc394492142)

[3.8.3 Risks 10](#_Toc394492143)

[4 User Management Functions (UM) 10](#_Toc394492144)

[4.1 Register a user 11](#_Toc394492145)

[4.1.1 Description 11](#_Toc394492146)

[4.1.2 Dependencies 11](#_Toc394492147)

[4.1.3 Risks 11](#_Toc394492148)

[4.2 Authenticate a user 11](#_Toc394492149)

[4.2.1 Description 11](#_Toc394492150)

[4.2.2 Dependencies 11](#_Toc394492151)

[4.2.3 Risks 11](#_Toc394492152)

[4.3 Modify user details 11](#_Toc394492153)

[4.3.1 Description 11](#_Toc394492154)

[4.3.2 Dependencies 12](#_Toc394492155)

[4.3.3 Risks 12](#_Toc394492156)

[5 Appliance Management Functions (AM) 12](#_Toc394492157)

[5.1 Manage Appliance Settings 12](#_Toc394492158)

[5.1.1 Description 12](#_Toc394492159)

[5.1.2 Dependencies 12](#_Toc394492160)

[5.1.3 Risks 12](#_Toc394492161)

[6 Non-Functional Requirements 13](#_Toc394492162)

[6.1 Availability 13](#_Toc394492163)

[6.2 Security 13](#_Toc394492164)

[6.3 Testability 13](#_Toc394492165)

[6.4 Usability 13](#_Toc394492166)

[6.5 Modifiability 13](#_Toc394492167)

[6.6 Scalability 13](#_Toc394492168)

# Introduction

## General

### Purpose of this document

This document describes the requirements of the planned product GDC-EDaSA-IDS (Green Danube Cloud Early-Detection and Self-Adaption Intrusion Detection System). This document aims to define which goals should be achieved by the product.

### Product Scope

The product will be developed as a stand-alone product in terms of an FFG-project.

### Abkürzungen

-

### Ablage, Gültigkeit und Bezüge zu anderen Dokumenten

-

## Verteiler und Freigabe

### Verteiler für dieses Lastenheft

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Rolle / Rollen | Name | Telefon | E-Mail | Bemerkungen |
| Projektleiter |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

<Ihr Text>

## Reviewvermerke und Meeting-Protokolle

### Erstes bis n-tes Review

<Ihr Text>

# Product Perspective

## Product Goals and Benefits

This product should increase endpoint security of mobile devices as well as personal computers when using web- and cloud-applications. Our approach is based on the assumption that attacks generated by infected web- or cloud-applications can be detected by analyzing the response of the application before it even reaches the endpoint (e.g. the browser on a user’s device).

To allow a high detection rate as well as the possibility to detect yet unknown attacks – so called 0-day-attacks – the product will use signature-based as well as anomaly-based detection algorithms.

Additionally, the product will intercept the line of attack in an very early phase of the attack cycle (see Illustration 1). Therefore it will help not only to detect malicious changes or infections but will have the ability to prevent infections on endpoints before they actually happen.



Illustration 1: Position of the product in the line of attack

Illustration 1 decribes a typical process of a modern attack:

1. The attacker exploits an, otherwise legitimate, Web-Application or Website and injects a so-called redirect.
2. A users visits the Web-Application e.g. with his browser
3. The Web-Application handles the user’s request and sends the infected source-code to the user’s browser.
4. The user’s browser interprets the source-code, including the malicious part, and is redirected to the so-called exploit service.
5. Tbe exploit service generates a custom exploit for the user’s browser (by analyzing the browser-type, version, exensions, etc.) and sends it back to the browser.
6. The custom exploit uses vulnerabilities of the browser or its extensions to force him to load and install malware from a malware-provider.
7. The installed can take over the user’s device and has access to its computing capabilities, to sensitive information stored on the user’s device etc.

Most existing products try to intercept this cycle at later stages:

* Revers Firewalls (RFW) will try to detect when data from an already infected devices is sent to illegitimate sources in the internet or when the installed malware requests command-signals from a so called Command-and-Control-Server.
* Firewalls (FW) try to detect the receiving of the actual malware, e.g. by scanning for specific patterns.

Our product aims to intercept the attack-cycle in a very early stage by detecting malicious changes in otherwise legitimate websites or web-applications. This should be done using signature-based detection algorithms and, in addition, the product should provide a self-learning, self-adapting anomaly detection algorithm, which allows the product to detect and prevent so-called 0-day-attacks where no signature-based detection algorithms are available yet.

## User Types

The product is intended for 2 different user types:

* U1: Individual users using the product to secure their private devices
* U2: Companies that want to protect their network infrastructure by securing the devices of their employees.

## User-Devices

The product shall be usable with both mobile- as well as desktop-devices. If possible, a platform-independent implementation should be preferred. If a platform-independent implementation is impossible, Android- and IOS-Mobile-Devices will be the first target-platform for the product.

## Deployment-Scenarios

The 2 different user types implicitly define 2 different deployment scenarios:

### U1: Individual users

Individual users will directly communicate with our product, all functions will be performed there.

### U2: Companies

Companies aiming to secure the devices in their network might want individual control over which attack-detection algorithms to apply and might prefer to have the product physically situated at their company site.

In this deployment scenario, the client devices will communicate with an appliance situated direct in the company network. This appliance will perform most of the functionality and will only communicate with the Green Danube Cloud to request updated data (e.g. parameters) for attack-detection.

## Resources

<Ihr Text>

# Attack-Detection Functions (AD)

This chapter describes the requirements that concern

## Intercept http/1.1 Traffic

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Nr. / ID** | AD-01 | **Nichttechnischer Titel** | | Intercept http/1.1 Traffic | | |
| **Quelle** | U1, U2 | | **Verweise** |  | **Priorität** | Critical |

### Description

The product has to intercept all incoming and preferably also outgoing traffic sent over the http/1.1-protocol. The content will be available in plain form and can be directly analyzed for attack-vectors

### Dependencies

<Ihr Text>

### Risks

<Ihr Text>

## Intercept http/1.1 + SSL/TLS (https) Traffic

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Nr. / ID** | AD-02 | **Nichttechnischer Titel** | | Intercept http/1.1 + SSL/TLS (https) Traffic | | |
| **Quelle** | U1, U2 | | **Verweise** |  | **Priorität** | Critical |

### Description

The product has to intercept all incoming and preferably also outgoing traffic sent over the http/1.1-protocol, encrypted by SSL/TLS. The content transferred will have to be decrypted before it can be analyzed for attack vectors.

### Dependencies

<Ihr Text>

### Risks

A suiting architecture that allows access to the plain content will have to be found.

Decrypting an otherwise encrypted transmission makes the product a high-value target for attackers as the data will – at least for a short time – will be available in plain text in our application

## Intercept websocket Traffic

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Nr. / ID** | AD-03 | **Nichttechnischer Titel** | | Intercept websocket Traffic | | |
| **Quelle** | U1, U2 | | **Verweise** |  | **Priorität** | Critical |

### Description

The product has to intercept all incoming and preferably also outgoing traffic sent over the websocket-protocol. The content transferred via this protocol might be encrypted by TLS/SSL and in that case will have to be decrypted before it can be analyzed for attack vectors.

### Dependencies

<Ihr Text>

### Risks

A suiting architecture that allows access to the plain content will have to be found.

Decrypting an otherwise encrypted transmission makes the product a high-value target for attackers as the data will – at least for a short time – will be available in plain text in our application

## Intercept http/2 (spdy) Traffic

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Nr. / ID** | AD-04 | **Nichttechnischer Titel** | | Intercept http/2 (spdy) Traffic | | |
| **Quelle** | U1, U2 | | **Verweise** |  | **Priorität** | Important |

### Description

The product has to intercept all incoming and preferably also outgoing traffic sent over the upcoming http/2-protocol. This protocol will adapt Google’s spdy-protocol which will have to be supported in order to ensure that the product will be to protect user-devices in the future.

The content transferred via this protocol will always be encrypted and will have to be decrypted before it can be analyzed for attack vectors.

### Dependencies

<Ihr Text>

### Risks

A suiting architecture that allows access to the plain content will have to be found.

Decrypting an otherwise encrypted transmission makes the product a high-value target for attackers as the data will – at least for a short time – will be available in plain text in our application

## Determine the content type

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Nr. / ID** | AD-05 | **Nichttechnischer Titel** | | Determine the content type | | |
| **Quelle** | U1, U2 | | **Verweise** |  | **Priorität** | Critical |

### Description

To be able to determine which attack-detection algorithms apply to the plain content received from a website or web-application, the product has to be able to determine the content type of the transferred data. The product thereby cannot only rely on the content-type specified e.g. in the http-header but has to perform its own checks as the specified content-type is often wrong or might have been modified by an attacker.

### Dependencies

To perform this function, the transferred content has to be available in plain form.

### Risks

<Ihr Text>

## Perform signature based analysis of the transferred content

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Nr. / ID** | AD-06 | **Nichttechnischer Titel** | | Perform signature based analysis of the transferred content | | |
| **Quelle** | U1, U2 | | **Verweise** |  | **Priorität** | Critical |

### Description

The product should perform signature based analysis, based on the content-type of the transferred data to detect possible attacks.

### Dependencies

To perform this function, the transferred content has to be available in plain form and its content-type has to be known

### Risks

<Ihr Text>

## Perform anomaly based analysis of the transferred content

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Nr. / ID** | AD-07 | **Nichttechnischer Titel** | | Perform anomaly based analysis of the transferred content | | |
| **Quelle** | U1, U2 | | **Verweise** |  | **Priorität** | Critical |

### Description

The product should perform anomaly based analysis, based on the content-type of the transferred data to detect possible attacks.

### Dependencies

To perform this function, the transferred content has to be available in plain form and its content-type has to be known

### Risks

<Ihr Text>

## Determine content danger-level

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Nr. / ID** | AD-08 | **Nichttechnischer Titel** | | Determine content risk | | |
| **Quelle** | U1, U2 | | **Verweise** |  | **Priorität** | Critical |

### Description

The product should combine the results of anomaly- and signature based analysis to decide the danger-level of the transferred content.

### Dependencies

To perform this function, the transferred content has to be available in plain form, its content-type has to be known and the results of the signature- and anomaly-based analysis have to be available.

### Risks

Too high false positive rate -> Negative impact on usability

Too high false negative rate -> Negative impact on security

# User Management Functions (UM)

This chapter describes the requirements that concern

## Register a user

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Nr. / ID** | UM-01 | **Nichttechnischer Titel** | | Register a user | | |
| **Quelle** | U1 | | **Verweise** |  | **Priorität** | Critical |

### Description

The user management has to provide methods to register a user. The user will have to provide at least:

* a username to identify the user
* a password to authenticate the user

Additional necessary user-details will have to be determined.

### Dependencies

<Ihr Text>

### Risks

<Ihr Text>

## Authenticate a user

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Nr. / ID** | UM-02 | **Nichttechnischer Titel** | | Authenticate a user | | |
| **Quelle** | U1 | | **Verweise** |  | **Priorität** | Critical |

### Description

The user management has to provide methods to authenticate a registered user by providing

* the user’s username
* the user’s password

This authentication is necessary to:

* use the product
* change the user’s details

### Dependencies

A user has to be registered to authenticate

### Risks

<Ihr Text>

## Modify user details

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Nr. / ID** | UM-03 | **Nichttechnischer Titel** | | Modify user details | | |
| **Quelle** | U1 | | **Verweise** |  | **Priorität** | Important |

### Description

The user management has to provide methods to change the details of an authenticated user. This includes at least:

* the user’s password
* the decision if encrypted transmissions should be analyzed as well

### Dependencies

A user has to be registered and authenticated to change his/her details

### Risks

<Ihr Text>

# Appliance Management Functions (AM)

This chapter describes the requirements that concern

## Manage Appliance Settings

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Nr. / ID** | AM-01 | **Nichttechnischer Titel** | | Manage Appliance Settings | | |
| **Quelle** | U2 | | **Verweise** |  | **Priorität** | Important |

### Description

Administrators have to be able to manage the settings of the appliance. The exact scope of customization options will have to be evaluated. They MIGHT include:

* which protocols should be inspected
* the decision if encrypted transmissions should be analyzed as well
* the attack detection methods that should be applied

### Dependencies

<Ihr Text>

### Risks

<Ihr Text>

# Non-Functional Requirements

## Availability

Availability is a basic quality-requirement of our product as when our product is unavailable, the user cannot be protected

## Security

*A*lthough our product will enhance the security of clients regarding malicious responses, it also increases the attack surface and presents itself as a high value target for attackers as even encrypted communication will be available in plain form and as attacking our product will simplify attacking clients afterwards.

DoS attacks could severely affect the usability of our product or make it even unusable if they are not handled correctly

Therefore, the product has to be thoroughly secured against attacks and thoroughly tested itself.

We will have to develop or adapt existing secure-development-, review- and testing-guidelines and continuously enforce these activities during the software-development-cycle.

## Testability

Due to the high security risks of the product, functional as well as penetration testing will need to be an integral part of our development cycle. Therefore, Testability has to be carefully considered in the software-architecture and design.

## Usability

The acceptance of our product will – apart from its ability to detect attacks- highly depend on its usability. There are 2 factors that have to be especially considered:

**Performance:**

If our product introduces too much latency, it might not get used anymore. Therefore Performance has to be considered as a key aspect for the Usability of our Product.

**False-Alarm-Rates**:

To ensure the usability of our product, the false-alarm-rate has to be extremely low. A high number of false-alarms will also lead to users abandoning the use of our product. Axelsson recommends a false-alarm-rate of < 10-5 to ensure the usability of an intrusion-detection-system.

## Modifiability

The internet and its protocols are a very changeable, constantly evolving environment. Therefore it should be easily possible to add support for new protocols.

The changeability is even greater concerning attacks on internet-users. This implies, that it should be easily possible to adapt or extend the existing attack-detection algorithms. Adding new attack-detection algorithms will be frequent changes in the future and should be easily possible.