System Description and Risk Analysis

Cyrill Krhenbhl   Silvan Egli   Lukas Bischofberger

. . .

Page limit: 30 pages.

Contents

1 System Characterization

1.1 System Overview

20 points

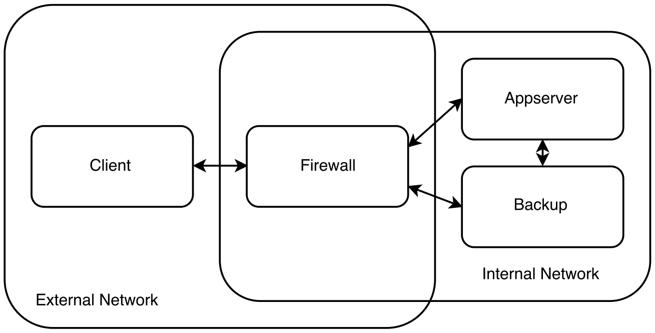

Figure 1: System overview

Describe the system's mission, the system boundaries, and the overall system architecture, including the main subsystems and their relationships. This description should provide a high-level overview of the system, e.g., suitable for managers, that complements the more technical description that follows.

1.2 System Functionality

Describe the system's functions.

1.3 Security Design

Describe the system's security design, including key and session management and security of data at rest and in transit.

1.4 Components

List all system components and their interfaces, subdivided, for example, into categories such as platforms, applications, data records, etc. For each component, state its relevant properties.

1.5 Backdoors

Describe the implemented backdoors.

Hide this subsection in the version handed over to the reviewing team by setting the flag `showbackdoors` at the top of this document to `false`.

1.6 Additional Material

You may have additional sections according to your needs.

2 Risk Analysis and Security Measures

2.1 Assets

3 points

Describe the relevant assets and their required security properties. For example, data objects, access restrictions, configurations, etc.

2.2 Threat Sources

3 points

Name and describe potential threat sources including their motivation.

2.3 Risks Definitions

2 points

Define likelihood, impact and risk level using the following three tables.

Likelihood	
Likelihood	Description
High	...
Medium	...
Low	...

Impact	
Impact	Description
High	...
Medium	...
Low	...

Risk Level			
Likelihood	**Impact**		
	Low	Medium	High
High	Low	Medium	High
Medium	Low	Medium	Medium
Low	Low	Low	Low

2.4 Risk Evaluation

7 points

List all potential threats and the corresponding countermeasures. Estimate the risk based on the information about the threat, the threat sources and the corresponding countermeasure. Adhere to the risk definitions you have given above.

2.4.1 *Evaluation Asset X*

Evaluate the likelihood, impact and the resulting risk, *after implementation of the corresponding countermeasures.* For each threat, clearly name the threat source and the the threat action.

No.	Threat	Countermeasure(s)	L	I	Risk
1	...	...	*Low*	*Low*	*Low*
2	...	...	*Medium*	*High*	*Medium*

2.4.2 *Evaluation Asset y*

No.	Threat	Countermeasure(s)	L	I	Risk
1	...	...	*Low*	*Low*	*Low*
2	...	...	*Medium*	*High*	*Medium*

2.4.3 Detailed Description of Selected Countermeasures

Optionally explain the details of the countermeasures mentioned above.

2.4.4 Risk Acceptance

List all medium and high risks, according to the evaluation above. For each risk, propose additional countermeasures that could be implemented to further reduce the risks.

No. of threat	Proposed additional countermeasure including expected impact
...	...
...	...