Insider Threat Report

Identified Elements

The most vulnerable BPMN elements are listed below and ordered according to the number of times the user has depicted the element as a potential attack target.

1. Secure storage (4)

Threats identified

Confidential data acquisition
Confidential data view
Unauthorized access to credentials
Data corruption

2. Process and forward (3)

Threats identified

Confidential data transfer
Data corruption
Malware installation

3. Prepare publication of results (2)

Threats identified

Data corruption
Malicious code modification

4. Collect voting envelope (1)

Threats identified

Confidential data view

5. Receive ballot envelope (1)

Threats identified

Confidential data view

6. Personally cast the vote at the urn of the municipality (1)

Threats identified

Data corruption

7. Cast voting envelope in letterbox (1)

Threats identified

Data corruption

8. Post voting envelope into letterbox of municipality (1)

Threats identified

Data corruption

9. Securely store voting envelopes (1)

Threats identified

Data corruption

10. Start tallying paper ballots (1)

Threats identified

Data corruption

Insider Threat Report

Identified Threats

In the part below you find a description for each threat that was found by the Insider Threat Modeler. As this prototype does not include any suggestions for controls or countermeasures, please discuss with a cyber security expert to decide if further measures are needed to mitigate the threats.

Confidentiality

Confidential data acquisition

Data that is being stolen or used inappropriately its in this category. The attack can target not only a computer system but also a web service when for instance a session is being hijacked.

Confidential data view

If sensitive data is being inspected apart from the normal usage, the attack belongs to confidential data view.

Confidential data transfer

The illegal distribution of confidential files such as password lists, financial information, and other sensitive material is a part of confidential data transfer.

Unauthorized access to credentials

Attacks in this category happen when an insider gets access to crypto keys and other credentials without authorization

Integrity

Data corruption

With data corruption, the fraudulent modification of data can be understood. It happens when information is manipulated within either an application or also a system. Incidents in the past have shown that tampering with cookies is a widely used technique to corrupt data in an unauthorized manner.

Malicious code modification

In software code programming small modifications can have a huge impact. Logic bombs, trojan horses, and other malicious code injections are examples of this attack group.

Malware installation

The installation of malware can originate from various sources. The use or download of illegal software or offensive material has a higher chance of containing trojan horses or trapdoors in order to compromise a computer system.