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. business case file (4)

Threats identified

Confidential data acquisition
Confidential data view
Confidential data transfer
Data deletion

2. business case file with clarification document (4)

Threats identified

Confidential data acquisition
Confidential data view
Confidential data transfer
Data deletion

3. personal register (4)

Threats identified

Confidential data acquisition
Confidential data view
Data corruption
Data deletion

4. citizens platform (4)

Threats identified

Confidential data acquisition
Confidential data view
Data corruption
Data deletion

5. check further clarifications (3)

Threats identified

Data corruption
System control manipulation
Data deletion

6. check answer (3)

Threats identified

Data corruption

System control manipulation
Data deletion

7. check employee in system (3)

Threats identified

Data corruption
System control manipulation
Data deletion

8. check responsibility (3)

Threats identified

Data corruption
System control manipulation
Data deletion

9. process returned correspondence (2)

Threats identified

Confidential data view
Malware installation

10. sign up insured (2)

Threats identified

Confidential data view
Malware installation

11. order insurance number (2)

Threats identified

Confidential data transfer
Data corruption

12. send insurance card (1)

Threats identified

Confidential data transfer

13. write a letter or message (1)

Threats identified

Data corruption

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.

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.

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.

System control manipulation

When default configurations are being modified or the protection of components gets disabled attackers manipulate system controls.

Availability

Data deletion

The loss of data because of its destruction by an insider is labeled as data deletion.