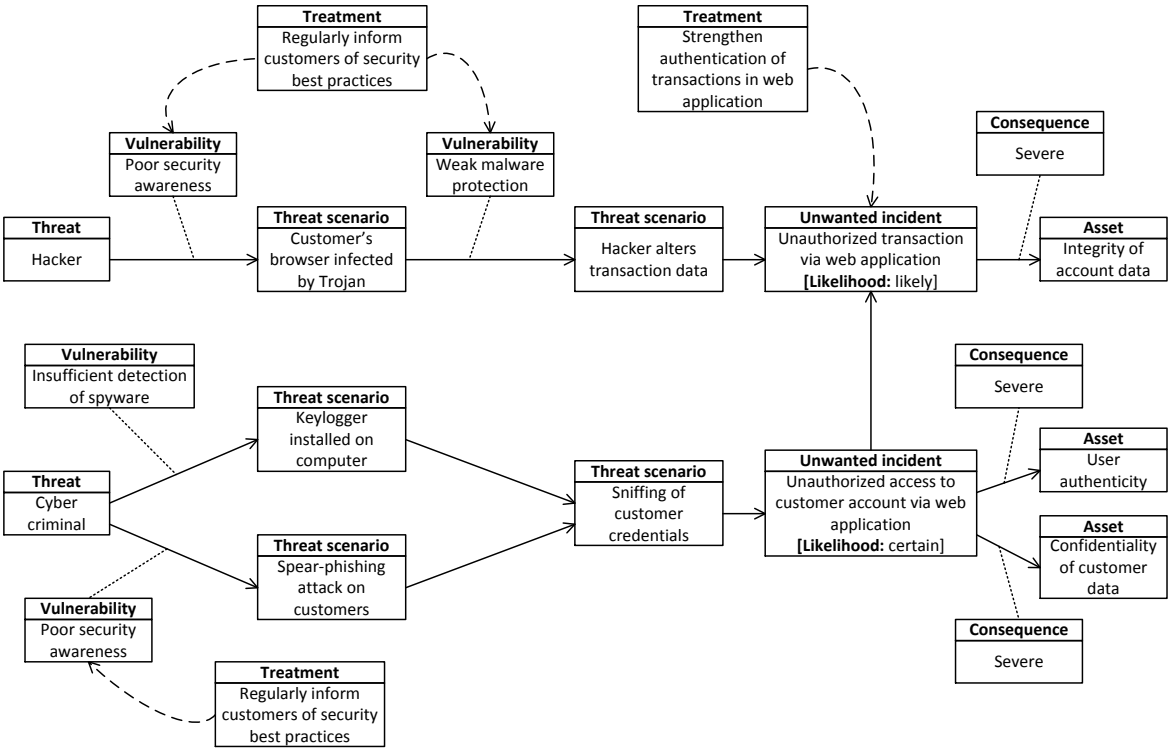
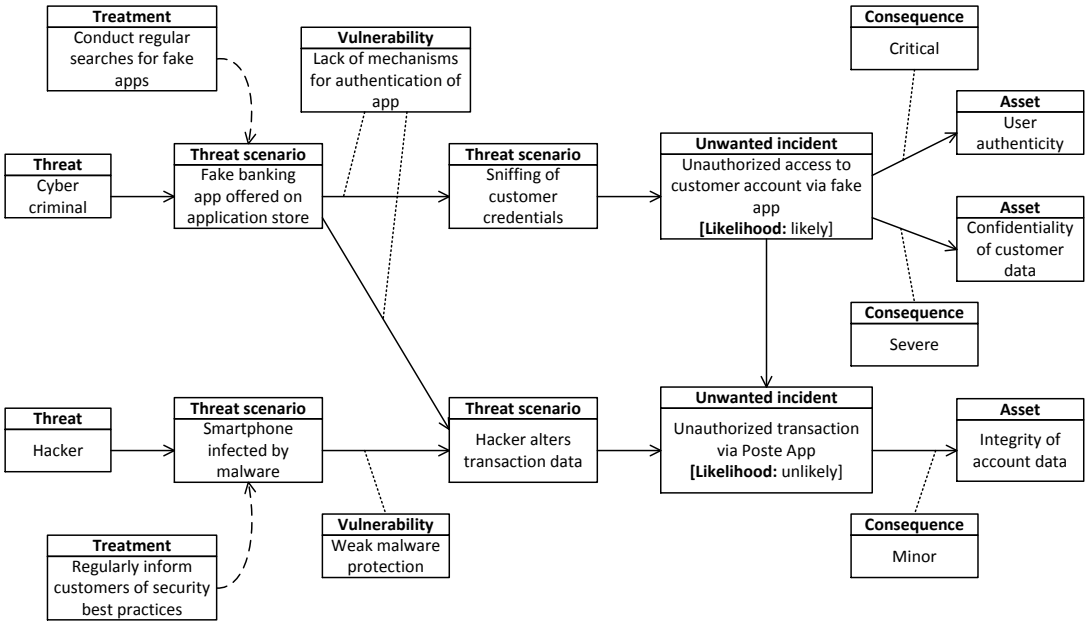
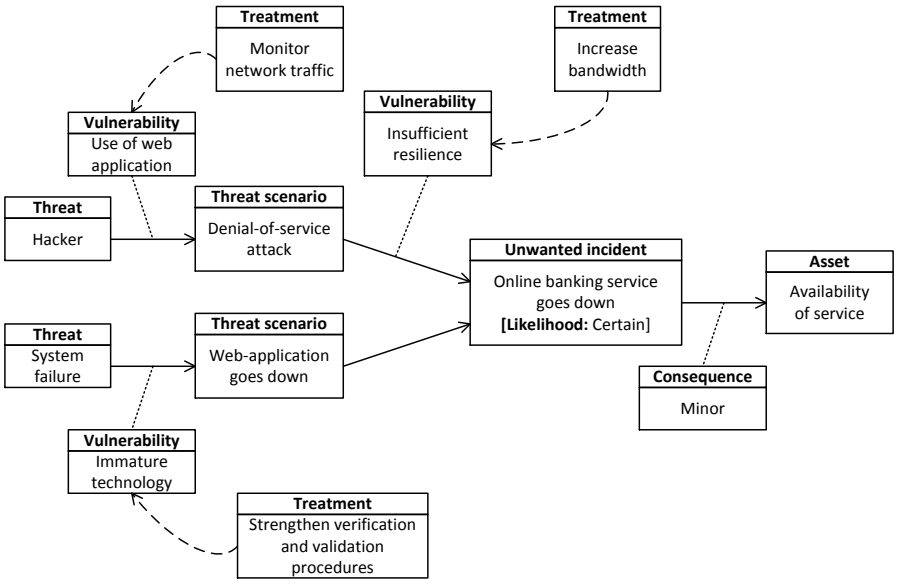

Treatment
Regularly inform customers of security best practices
Treatment
Strengthen authentication of transactions in web application
Vulnerability
Poor security awareness
Vulnerability
Weak malware protection
Consequence
Severe
Threat
Hacker
Threat scenario
Customer's browser infected by Trojan
Threat scenario
Hacker alters transaction data
Unwanted incident
Unauthorized transaction via web application
[Likelihood: likely]
Asset
Integrity of account data
Vulnerability
Insufficient detection of spyware
Threat scenario
Keylogger installed on computer
Consequence
Severe
Threat
Cyber criminal
Threat scenario
Sniffing of customer credentials
Unwanted incident
Unauthorized access to customer account via web application
[Likelihood: certain]
Asset
User authenticity
Asset
Confidentiality of customer data
Threat scenario
Spear-phishing attack on customers
Vulnerability
Poor security awareness
Consequence
Severe
Treatment
Regularly inform customers of security best practices


Treatment
Conduct regular searches for fake apps
Vulnerability
Lack of mechanisms for authentication of app
Consequence
Critical
Asset
User authenticity
Threat
Cyber criminal
Threat scenario
Fake banking app offered on application store
Threat scenario
Sniffing of customer credentials
Unwanted incident
Unauthorized access to customer account via fake app
[Likelihood: likely]
Asset
Confidentiality of customer data
Consequence
Severe
Threat
Hacker
Threat scenario
Smartphone infected by malware
Threat scenario
Hacker alters transaction data
Unwanted incident
Unauthorized transaction via Poste App
[Likelihood: unlikely]
Asset
Integrity of account data
Vulnerability
Weak malware protection
Consequence
Minor
Treatment
Regularly inform customers of security best practices


Treatment
Monitor network traffic
Treatment
Increase bandwidth
Vulnerability
Use of web application
Vulnerability
Insufficient resilience
Threat
Hacker
Threat scenario
Denial-of-service attack
Unwanted incident
Online banking service goes down
[Likelihood: Certain]
Asset
Availability of service
Threat
System failure
Threat scenario
Web-application goes down
Consequence
Minor
Vulnerability
Immature technology
Treatment
Strengthen verification and validation procedures