Exempelsystem i kursen ETE352 Cybersäkerhet - grunder och medvetenhet

Owner:
Reviewer:
Contributors: ,
Date Generated: Thu Apr 10 2025

Executive Summary

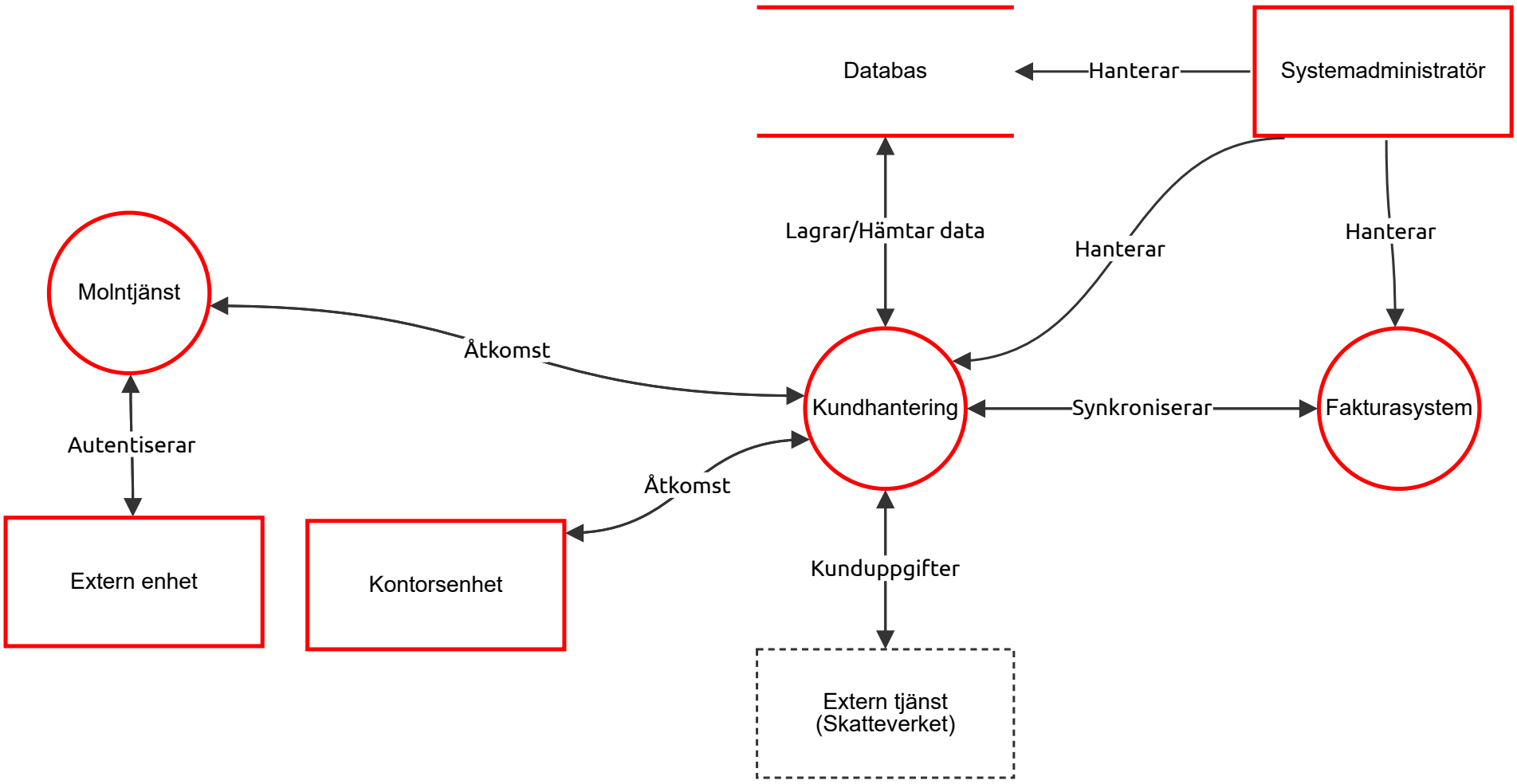
High level system description

Not provided

Summary

Total Threats	8
Total Mitigated	0
Not Mitigated	8
Open / High Priority	1
Open / Medium Priority	3
Open / Low Priority	2
Open / Unknown Priority	0

Exempelsystem



Exempelsystem

Databas (Store)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
106	Data Corruption During Synchronization	Integrity	Medium	Open		The asset is the data flow between Kundhantering and Fakturasystem, but threats cannot be directly added to data flows in Threat Dragon. There is a risk of a man-in-the-middle attack if data flows over unsecured channels. If the database is hosted remotely, the absence of encryption or authentication mechanisms could lead to data corruption during synchronization.	Encryption in Transit: Use encrypted channels for data synchronization (e.g., HTTPS, TLS). Authentication: Validate both systems before data exchange to prevent unauthorized access. API keys: Unique keys assigned to each system for secure communication. Mutual TLS: Certificates required from both systems to establish trust. OAuth or Token-Based Authentication: Ensuring only authenticated requests are processed. Monitoring: Implement logs and alerts to detect abnormal synchronization activity.

Systemadministratör (Actor)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
103	New CIA threat	Confidentiality	Medium	Open		Brute Force Attack: Repeated login attempts targeting the administrator account could compromise admin credentials, exposing sensitive system controls.	Account lock outs: After a defined number of incorrect password attempts, lock account. Passwords: Thorny issue, either have complex password, or better yet a security-key like Google Titan or Yubikey. MFA: If it's the regular password route, then MFA is a must. XDR: Have an enterprise defense suite that monitors accounts and login attempts.
104	New CIA threat	Integrity	TBD	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A

Extern tjänst (Skatteverket) (Actor) - *Out of Scope*

Reason for out of scope: Externt

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Hanterar (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Hanterar (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Hanterar (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

flow 11 (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Synkroniserar (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

(Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

(Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

(Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

(Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

(Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Lagrar/Hämtar data (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Åtkomst (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Åtkomst (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Autentiserar (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Kontorsenhet (Data Flow)

Description: Dator

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Molntjänst (Process)

Description: Autentisering, Access control av externa enheter

Number	Title	Type	Priority	Status	Score	Description	Mitigations
107	DDos Attack on Molntjänst	Availability	Low	Open		A Distributed Denial-of-Service (DDoS) attack targeting the cloud service (Molntjänst) could render the system inaccessible to external devices and office units. If the Molntjänst is provided by an external cloud provider, the risk level for a DDoS attack may be low, as major providers typically have robust defenses against such attacks (e.g., DDoS mitigation services, traffic filtering).	Cloud Provider's DDoS Protection: Built-in DDoS mitigation (e.g., AWS Shield, Azure DDoS Protection). Backup and Recovery Plan: Maintain regular backups of critical data and ensure the ability to quickly restore operations if the service becomes unavailable.

Kundhantering (Process)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
102	New CIA threat	Confidentiality	High	Open		Sensitive customer data (personal details, payment info) being leaked, exposed, stolen.	Encrypt data: Strong encryption (AES-256) for databases and backups, both at rest and in transit. So even if the data is stolen, it cannot be read without decryption keys. Least privilege access controls: Only users who need access to customer data should have it. In the same vein, use role-based access control (RBAC) and regularly review permissions. MFA: Required for sensitive systems, admin accounts. Network segmentation: Isolate customer databases from the rest of the network. Intrusion Detection and Monitoring: Use tools to monitor and detect unauthorized access or unusual behavior in the system.

Fakturasystem (Process)

Description: Fakturahantering

Number	Title	Type	Priority	Status	Score	Description	Mitigations
101	New CIA threat	Availability	Critical	Open		Third-party supply chain attack (like the 2021 Kaseya attack).	Update Software Regularly: Ensure the system and all dependencies are patched. Vendor Due Diligence: Verify that third-party providers follow strict security practices. Zero Trust Approach: Assume breach. Limit trust in third-party software. Backup Data: Regularly back up invoices and customer data offline.

Extern enhet (Actor)

Description: Mobil
Dator

Number	Title	Type	Priority	Status	Score	Description	Mitigations
105	Rogue External Device	Confidentiality	Medium	Open		This threat affects all 3 parts of the CIA triad: Confidentiality: Data theft. Integrity: Data tampering. Availability: Unauthorized actions disrupting services.	Authorized Devices: Ensure only onboarded, authorized devices are able to access the cloud service. XDR (Extended Detection and Response): Monitor suspicious activity related to the cloud service to detect and respond to threats. Vendor Risk Management: Continuously assess and mitigate risks from third-party cloud vendors.

Kontorsenhet (Actor)

Description: Dator

Number	Title	Type	Priority	Status	Score	Description	Mitigations
108	Hardware Failure in Kontorsenhet	Availability	Low	Open		A breakdown in the office unit could prevent employees from accessing the business system and handling orders/fakturas. In case of theft, ensure laptops are encrypted . This is a Confidentiality measure to to prevent unauthorized access to stored data. There might be phishing attacks to trick users into authenticating malicious systems. And general phishing attacks that risk credential leaks.	Backup laptops: Ensure backup laptops are available, onboarded, updated, and patched for temporary use to maintain business continuity. Encryption: E.g. Bitlocker encryption on the laptops. Hardware-based authentication tokens: E.g. YubiKeys with multi-factor authentication (PIN + token). Employee training: Train employees to recognize phishing attempts targeting YubiKey usage and email/login info.