Exempelsystem i kursen ETE352 Cybersäkerhet - grunder och medvetenhet

Owner:
Reviewer:
Contributors: ,
Date Generated: Mon Oct 14 2024

Executive Summary

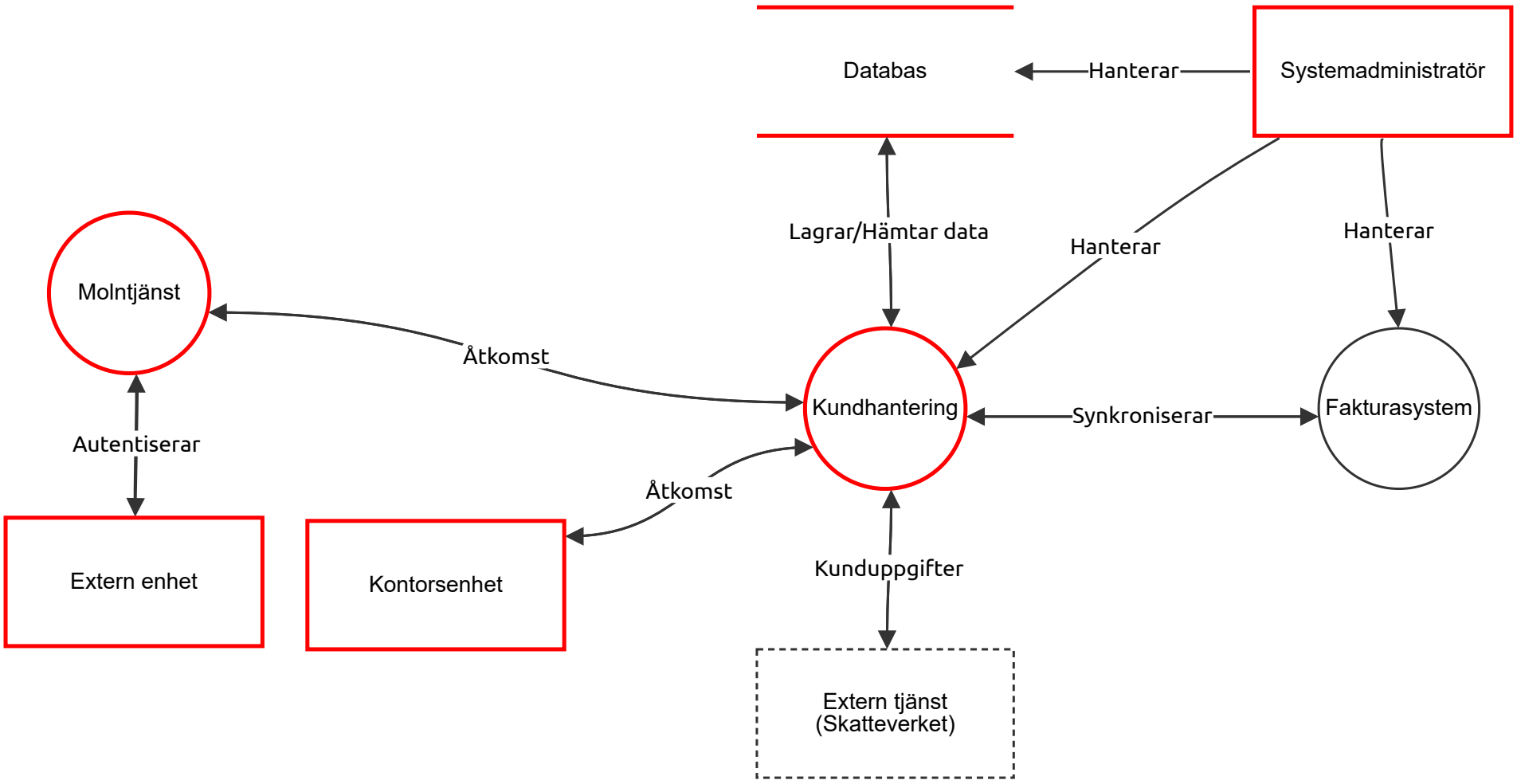
High level system description

Not provided

Summary

Total Threats	10
Total Mitigated	3
Not Mitigated	7
Open / High Priority	4
Open / Medium Priority	1
Open / Low Priority	2
Open / Unknown Priority	0

Exempelsystem



Exempelsystem

Databas (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
101	Läckta lösenord	Confidentiality	High	Mitigated		En angripare som har åtkomst till databasen har tillgång till lösenord som är lagrade i klartext vilket resulterar i läckta lösenord.	Lagra inte lösenord i klartext. Lagra istället utdatan från saltade hash-funktioner.
102	Misstag av systemadministratör	Integrity	Medium	Open		En systemadministratör råkar av misstag vid en manuell uppdatering av en användare i databasen radera information om en användare från databasen.	Skapa regelbundet backups av databasen och se till att databasen enkelt går att återställa.
117	SQL injection	Confidentiality	High	Open		En angripare genomför en SQL-injektion på databasen som saknar funktionalitet för prepared-statements eller character escaping vilket resulterar i läckta kunduppgifter.	Provide remediation for this threat or a reason if status is N/A

Systemadministratör (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
112	Bedräglig mirror	Confidentiality	Low	Open		En angripare har skapat en mirror för en nedlaggning av en programvara. En oaktsam systemadminstratör kontrollerar inte hash/checksum eller den pgp-signaturen av den nedladdade programvaran med hash/checksum eller publicerad av programvarans skapare. Detta möjliggör för en angripare att få kontroll över kundsystemet	Provide remediation for this threat or a reason if status is N/A

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

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Hanterar (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Hanterar (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Hanterar (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

flow 11 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Synkroniserar (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

(Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

(Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

(Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

(Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

(Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Lagrar/Hämtar data (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Åtkomst (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Åtkomst (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Autentiserar (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
110	Återanvändande av lösenord	Confidentiality	High	Mitigated		En angripare har fått tillgång till en användares lösenord som denne använder för flera tjänster vilket resulterar i att angriparen får tillgång till systemet.	2FA

Kontorsenhet (Actor)

Dator

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Molntjänst (Process)

Autentisering, Access control av externa enheter

Number	Title	Type	Priority	Status	Score	Description	Mitigations
114	Denial of Service Attack	Availability	Low	Open		En angripare överbelastar molnsystemet genom en distributed denial-of-service attack vilket gör systemet otillgängligt för användare att logga in på externa enheter.	Provide remediation for this threat or a reason if status is N/A

Kundhantering (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
109	Denial-of-Service	Availability	High	Open		En angripare överbelastar systemet genom en distributed denial-of-service attack vilket gör systemet otillgängligt för användare och systemadministratörer så länge attacken pågår.	Provide remediation for this threat or a reason if status is N/A

Fakturasystem (Process)

Fakturahantering

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Extern enhet (Actor)

Mobil

Dator

Number	Title	Type	Priority	Status	Score	Description	Mitigations
111	Läckta inloggningsuppgifter	Confidentiality	High	Open		En angripare får en oaktsam användare att ladda ned och köra skadlig kod på sin externa enhet vilket möjliggör för en angripare att installera övervaka kommunikationen mellan den externa enheten och kundhanteringssystemet.	Provide remediation for this threat or a reason if status is N/A

Kontorsenhet (Actor)

Dator

Number	Title	Type	Priority	Status	Score	Description	Mitigations
105	Externt USB-minne	Confidentiality	High	Mitigated		En angripare har planterat skadlig kod på ett USB-minne som en oaktsam användare pluggar in i sin jobbdator vilket möjliggör dataläckage, fjärrstyrning, installation av kryptovirus etc.	Tillåt inte användare att använda externa USB-minnen
115	Phishing	Confidentiality	High	Open		En användare får ett mejl där denne uppmanas att (brådskande) logga in via en länk som bifogats i mejlet av vad som ser ut att vara en kollega. Detta resulterar i läckta inloggningsuppgifter.	2FA, phishing-övningar.