# Exempel Utkast TSIT01 Datasäkerhetsmetoder

### Detta är ett fiktivt exempel, där förutsättningen är följande uppgift:

"Litterati är ett postorderföretag, som förmedlar antikvariska böcker samt har diskussionsforum för bokmalar. Den antikvariska delen är öppen som vilken nät-handel som helst, medan diskussionsfora bara är till för registrerade medlemmar, som först måste ha köpt något av Litterati. Hemsidan ger självfallet möjlighet för kunderna att söka i basen av böcker på lager, att fråga efter särskilda böcker, att samla på sig flera böcker till en beställning med en fraktavgift och annat, som är standard i denna typ av system. Böckerna betalas i förskott inklusive frakt. Datorsystemet är en enkel Windowsbaserad server, och kundernas betalningar skickas vidare till kortföretag via rutiner som bestäms av kortföretagen själva, varför ni inte behöver bry er om den delen av systemet. Ge rekommendationer för säkerheten för övriga systemdelar!"

# Studenternas inskickade dokument

### Bakgrund

Uppgiften gäller att studera en kombination av internet-bokhandel och diskussionsklubb. Pengar överförs via transaktioner mot kortkonton, vilket ger extra känslighet åt systemet. Själva kommunikationen mot kortbolagen ingår dock inte i uppgiften.

## Sårbarhet och hot.

### Sekretesskrav:

Kundernas kontonummer måste behandlas med full sekretess. Lösenord (som vi förutsätter är lagom nivå för användarautentisering i diskussionsdelen) kräver också sekretesskydd. Troligen vill kunderna inte heller avslöja sina bokinköp för andra utöver vad de själva skriver i diskussionsdelen.

### Dataintegritet:

Kundernas beställningar måste bli helt korrekta, så de får det de beställt och inget annat. Ingen ska kunna beställa i någon annans namn. Ingen ska heller kunna lämna in diskussionsinlägg under någon annans identitet, eller förvanska andras lagrade inlägg. Bokdatabasen över lager och beställningar måste vara korrekt. Hemsidorna får inte kunna förvanskas.

### Tillgänglighet:

Hemsidorna får inte vara nere för ofta eller för länge. Bokdatabasen måste alltid vara uppe, om hemsidan är det. Kunderna ska kunna se vad de beställt. Man måste alltid kunna nå ansvarig person via någon kanal.

### Tänkbara hotagenter:

Rena hårdvaru-olyckor, som hårddiskkrasch, vattenskada, längre strömavbrott, avgrävd telelinje och andra hot mot fysisk säkerhet (brand, stöld m m). Allmänt nätsabotage, som att göra servern till nod för illegalt material eller deltagare i bot-net, eller destruktiva virus, eller attacker på måfå för att testa nyupptäckta säkerhetshål. Konkurrent med skumma metoder. Attackerare, som insett att kontokortsinformation finns här.

### Attackmetoder att beakta:

Falsk inloggning
Kända säkerhetshål
Virus/maskar
Nätavlyssning

### Att göra till slutversion:

Detaljbeskriva hot, koppla hotagenter till tänkbara attackmetoder och prioritera hoten efter kombinationen av sannolikhet och skadans storlek. Göra lista över vilka verktyg och metoder som måste införas för rimligt skydd och detaljbeskriva hur de kan sättas upp/användas i just detta fall.

# Lärarkommentar:

Hotanalysen är OK, men lite kort. Till exempel saknar ni två inte helt osannolika hotagenter: "Missnöjda kunder" samt "Insider, som smyger in kostnad för egna köp i större kundbeställningar". Notera att i synnerhet den sistnämnda är extra intressant, eftersom skydd mot rena nätattacker inte hjälper på den punkten. Er lista över "Att göra" är mycket kortfattad, men innehåller alla väsentliga punkter. Se bara till att er prioritering klargör hur allvarligt ni bedömer varje typ av eventuell skada och skälet till denna bedömning, eftersom ni inte antytt detta i ert utkast.