Genomföra risk- och sårbarhetsanalys (RSA) samt upprätta en informationssäkerhetspolicy

Betygsnivåer. Denna uppgift bedöms på ett sätt som liknar ett examensarbete. Det går inte att sätta specifika gränser då den är mer öppen och kan se olika ut för varje student. För mer information se Teknisk/Akademisk bedömning av ditt arbete nedan.

Risk- och sårbarhetsanalyser är metoder för att upptäcka brister samt fastställa konsekvenser av en oönskad händelse. I metoden ingår också att bedöma sannolikheten att händelsen ska inträffa samt att åsätta en kostnad om händelsen inträffar.

Risk- och sårbarhetsanalys är en av åtgärderna som ingår i säkerhetsarbetet. Nya system ska alltid genomgå en risk- och sårbarhetsanalys och befintliga system bör revideras regelbundet. Riskbedömningen ska vara **dokumenterad** och **signerad/godkänd** av systemägaren för alla IT-resurser. I en risk- och sårbarhetsanalys ingår följande delar:

1. Beskriva hotbilder.
2. Kalkylera konsekvenser och skadekostnader.
3. Bedöma sannolikhet för att hoten ska inträffa.

Resultatet av analysen ska vara vägledande vid klassning av IT-resurser, t.ex. informationsklassning, som i sin tur leder till lämpliga skyddsåtgärder.
Källa ”Statskontorets Handbok i IT-säkerhet”

En informationssäkerhetspolicy formaliserar hur informationen säkerställs och behandlas inom organisationen.

Innan ni börjar så kan det vara en god ide att titta på filmer etc. från t.ex. Microsoft TechNet Webb TV: https://technet.microsoft.com/sv-se/dd883284 eller YouTube etc. om riskhantering i IT-miljön. Använd de vedertagna sökord som finns i detta dokument, t.ex. riskanalys, it-säkerhet, risk analysis, risk assessment, it-security, it-policy, information security, RA, RSA etc.

Ett sätt (av många) att arbeta med risk analys är Failure Modes and Effects Analysis (FMEA) metoden: https://en.wikipedia.org/wiki/Failure_mode_and_effects_analysis. Det finns en mall i laborationens mapp ”ISO27k_FMEA_spreadsheet.xlsx”.

Det kan vara bra att se exempel som t.ex. Falu kommuns informationssäkerhetspolicy dokument i laborationens mapp ”Informationssäkerhetspolicy - Falu Kommun.doc”.

Annars kan du läsa mer på nedanstående länkar vad gäller riskanalys och it-säkerhetspolicy:

- LIS på webbsidan Informationssakerhet.se: https://www.informationssakerhet.se/
- Myndigheten för samhällsskydd och beredskap (MSB): https://www.msb.se/rsa
- LIS - Ledningssystem för Informationssäkerhet - SIS/TK 318, http://www.sis.se/ledningssystem/ledningssystem-f%C3%B6r-informationss%C3%A4kerhet/sis-tk-318
- “Security Risk Analysis and Management”, a white paper by: B. D. Jenkins, Countermeasures, i laborationens mapp

- Ledningssystem för informationssäkerhet vid 24-timmarsmyndigheter - Vägledning och mallregelverk (OffLIS), Stadskontoret, publikation 2003:23, se länk interna resurser. *Innehåller mycket bra information om hur man genomför RSA och upprättar en informationssäkerhetspolicy!*
- CERT.SE: https://www.cert.se/ och deras incidenthanteringsprocess (CIHSP)
- The SANS Security Policy Project, har många mallar och dokument: https://www.sans.org/security-resources/policies
- CERT.org har en hel del resurser som kan användas. T.ex. en nedladdningsbar OCTAVE Method Implementation Guide, http://www.cert.org/octave/
- Skydd av data på bärbara datorer – examensarbete, se länk interna resurser.
- Microsoft Security Assesment Tool (MSAT). Risk assessment application. Sök!
- Sveriges universitet och högskolor - Handbok i Informations- och IT-säkerhet: https://itsakhandbok.irt.kth.se/ har bra information om lagar, förordningar och föreskrifter som är relevanta i samband med informationssäkerhet.

Välj de mallar och metoder som passar dig och ditt problem från ovanstående eller egna källor. Redovisa en RSA och upprätta en enklare informationssäkerhetspolicy utifrån analysen. Välj från något av nedanstående problem.

- Utgå ifrån ett realiserat nätverk från kursen hård infrastruktur. Lägg till någon eller några uppsäkrade tjänster till nätverket.
- Om du har tillgång till en organisation/företag så gör laborationen mot detta objekt.
- En tredje lösning är att ett påhittat konstruerat "problem" används som tex. webbutiken i detta dokumentets sista rubrik.

Du bör kontakta mig innan du påbörjar ditt arbete så vi kan stämma av lämpligheten i ditt upplägg.

Redovisning:

- Genomför RSA med ditt eget val av metod och ange varför du valde just denna metod. Exempel på rubriker i din rapport finns i RA_by_Jenkins.pdf.
- Försök kvantifiera riskerna i RSA.
- Planera motåtgärder för att säkra upp systemen. Försök att definiera värdet av den kvarvarande risken med realistiska belopp.
- Genomför så många RSA cykler som det behövs men tillåt dig att ha en acceptabel risknivå för realismens skull.
- Skriv en enkel informationssäkerhetspolicy (all indata som behövs finns troligen inte tillgänglig för dig). På sidorna 41-44 i ” Ledningssystem för informationssäkerhet vid 24-timmarsmyndigheter” finns angivet vad en policy bör innehålla.

Skriv en rapport där alla delar sammanförs och sammanställ den så att en muntlig presentation kan ges utifrån ditt material.

Teknisk bedömning av ditt arbete:
Du kommer i huvudsak att bedömas efter hur realistisk din riskanalys är. Om du kommer upp med ett fåtal risker (mindre än 20) och motåtgärder för riskerna så anses inte ditt arbete vara tillräckligt realistiskt.
Det är inte troligt att för varje risk bara ha en motåtgärd och sedan är risken borta, utan det behövs förmodligen göras en ny riskbedömning (RSA cykel) för varje ny motåtgärd.

Akademisk bedömning av ditt arbete:
Använd de metoder som förekommer i alla akademiska arbeten. Redovisa källor, referenser, metoder osv. Resultatet ska kunna läsas och presenteras för andra än experter inom området.

Påhittat problem

Du skall starta upp en webbutik där man kan köpa dataprogram. Mjukvaran är tillgänglig för direkt nedladdning och du får betalt direkt vid ett köp. För att få statistik om vad kunder köper skall en kunddatabas som innehåller personlig kunddata installeras.

Du antar att du kommer att tjäna omkring 300 000 SEK i vinst om året. Om du förlorar kunddata så kostar det dig 25 000 SEK. Om din försäljnings- och betalningsprocess avbryts på något sätt så förlorar du 100 000 SEK – därför behövs datasäkerhet.
Som du känner till finns det många fria verktyg (brandväggar, algoritmer, SSL servrar …) tillgängligt och du skall använda dessa. Hursomhelst glöm inte att varje implementation av säkerhet kostar pengar, försök ange hur mycket.

Du kan också anta att du hittar ett försäkringsbolag som vill sälja en försäkring till dig på 1500 SEK som garanterar dig 15 000 SEK vid en förlust. Du kan ta ut hur mycket du vill i försäkring men du vill helst inte förlora mer än max 10 000 SEK per år.
Du är tillåten att ändra villkoren i den påhittade uppgiften om du kontaktar mig och förklarar varför.