Myndigheten för
samhällsskydd
och beredskap

Det nya totalförsvaret – En hjälp på vägen!

Hantering av hemliga uppgifter i en fristående dator

Det nya totalförsvaret – En hjälp på vägen!

Hantering av hemliga uppgifter
i en fristående dator

Digital hantering av hemliga uppgifter

Myndigheten för samhällsskydd och beredskap (MSB)

Produktion: Advant
Tryck: DanagårdLitho

Publikationsnummer: MSB1309
ISBN: 978-91-7383-891-7

Förord

I Sverige så hanteras dagligen stora mängder med information, inom offentlig liksom privat verksamhet. Genom att informationshantering är ett centralt stöd för alla typer av verksamheter så krävs ett systematiskt informationssäkerhetsarbete. Till följd av detta så blir det allt viktigare för aktörer i samhället att säkerställa så informationen ges ett fullgott skydd, att den finns tillgänglig när man behöver den samt att informationen är korrekt när den väl ska användas.

Inom ramen för återuppbyggnaden av totalförsvaret finns ökade behov av att stärka aktörers förmåga att skydda och dela information som omfattas av sekretess, vilket även inkluderar att skydda information som omfattas av sekretess och rör rikets eller Sveriges säkerhet.

Informationen riktar sig till aktörer som hanterar eller kommer att hantera hemliga uppgifter. Avsikten är att dokumentet ska fungera som ett stöd i arbetet men inte ses som gränssättande eller uttömmande avseende på de säkerhetsåtgärder som kan komma att behövas. Alla organisationer har olika förutsättningar för att utforma fullgoda säkerhetsåtgärder för informationen vilket medför att anpassningar utifrån individuella förutsättningar krävs.

Den här informationen baseras på säkerhetsskyddslagen (1996:627), säkerhetsskyddsförordningen (1996:633), Säkerhetspolisens föreskrifter och allmänna råd om säkerhetsskydd (PMFS 2015:3) Försvarsmakten KSF Krav på IT-säkerhetsförmågor hos IT-system v3.1 och Försvarsmaktens handbok Säkerhetstjänst Informationssäkerhet. Detta medför att dokumentet kan komma att revideras under 2019 när den nya säkerhetsskyddslagen träder i kraft.

Myndigheten för samhällsskydd och beredskap (MSB) har även tagit fram annat stöd inom området som till exempel ”Riskreducerande åtgärder för lokal avsedd för delgivning av hemliga uppgifter” (Publikationsnummer: MSB1310, ISBN: 978-91-7383-889-4).

Innehåll

Inledning

1. Inledning

Information är en viktig och avgörande resurs för de flesta verksamheter och förekommer ständigt på ett eller annat sätt i olika informationskanaler. För att säkerställa att information hanteras korrekt behöver den först och främst värderas och klassas i syfte att ta reda på vilket nödvändigt skydd informationen behöver omgärdas av. Klassningen utgår ifrån den funktion och betydelse som informationen har och de konsekvenser det medför om den skulle hanteras felaktigt, försvinna eller komma i orätta händer.

Informationssäkerhet handlar i många fall om olika åtgärder, både tekniska och administrativa. Åtgärderna ska också anpassas till att möta aktuell hotbild. Genom att noggrant analysera, identifiera och prioritera verksamhetens informationstillgångar kan medvetna och adekvata skyddsåtgärder vidtas i syfte att skydda informationen. Målet är att informationen:

- Finns tillgänglig när den behövs,
- är och förblir riktig,
- är tillgänglig för endast dem som är behöriga att ta del av den, samt
- att hanteringen av informationen är spårbar.

Varje enskild organisation ansvarar för att verksamhetsanalyser och säkerhetsanalyser genomförs. Detta dokument ska ses som ett stöd i det fortsatta arbetet med att ta fram systemstöd för att kunna hantera hemliga uppgifter i digitalt format.

Hemliga uppgifter förekommer även i digitalt format som lagras permanent eller tillfälligt i exempelvis en fristående dator, USB-minne, CD/DVD-skiva, skrivare eller kopiator.

I det fall informationen omfattas av sekretess och som rör rikets säkerhet behöver uppgifterna omfattas av krav som benämns säkerhetsskydd enligt säkerhetsskyddslagstiftningen. Området säkerhetsskydd syftar till att skydda mot spioneri, sabotage och andra brott som kan hota rikets säkerhet. För mer information om säkerhetsskydd och hantering av hemliga uppgifter hänvisas till PMFS 2015:3.

Uppgifter som lagras i en fristående dator som är konfigurerad för arbete med hemliga uppgifter innebär inte per automatik att informationen hanteras säkert och på rätt sätt. Användaren behöver få utbildning, tydliga hanteringsregler och instruktioner för att säkerställa korrekt hantering.

Råden i detta dokument fokuserar på hantering av en fristående dator. Med fristående dator så avses en dator som inte är ansluten till ett nätverk, annan dator eller motsvarande. Den fristående datorn kan av verksamheten tillåtas kommunicera med godkänd lagringsmedia, exempelvis USB-minne och trådanslutna tillbehör så som CD/DVD-läsare, skrivare och scanner.

Avgränsningen att endast fokusera på ett enanvändarsystem baseras på att i de fall flera användare ska använda samma dator behöver man dels tänka på spårbarheten av händelser i systemet utifall det inträffar en incident/informationsförlust. Man behöver kunna ta reda på vem som har gjort vad och när.

Genom att tillåta fler användare att dela på samma dator måste man också säkerställa att alla är behöriga till all information som finns eller har funnits på datorn. Orsaken till detta är att alla har fysisk åtkomst till datorns innehåll och kan med enkla medel få åtkomst till all information.

Vid behov av en mer fördjupad teknisk beskrivning av säkerhetsfunktionerna hänvisas läsaren till Försvarsmaktens publikation KSF Krav på IT-säkerhetsförmågor hos IT-system v3.1.

1.1 Syfte och mål

Syftet med dokumentet är att ge stöd och praktiska råd för att möta de säkerhetskrav som kan ställas i samband med hantering av hemliga uppgifter i en fristående dator.

Målet är att sådana uppgifter i digitalt format ska bearbetas och hanteras säkert och korrekt. Genom adekvata och genomtänkta säkerhetsåtgärder minskas risken för att uppgifter obehörigen röjs, ändras eller förstörs.

1.2 Målgrupp

Dokumentet riktar sig till de som ansvarar för att ta fram interna bestämmelser, instruktioner och rutiner för hantering av hemliga uppgifter i digitalt format samt för systemtekniker som ska konfigurera utrustningen.

Hemliga uppgifter i digitalt format

2. Hemliga uppgifter i digitalt format

2.1 Allmänt

Det ökade informationsflödet inom viktiga samhällsfunktioner blir alltmer beroende av tillförlitliga och säkra it- system som kan garantera att informationen är korrekt och att sekretessen för uppgifterna upprätthålls. För att säkerställa att den digitala informationen har det skydd som krävs förutsätts en analys av, bland annat verksamhetens skyddsvärda informationstillgångar och framförallt förekomsten av hemliga uppgifter.

Säkerhetsarbetet bör utgå utifrån säkerhetsanalysen. Genom säkerhetsanalysen kan verksamheten avgöra vad som är skyddsvärt, ur vilket perspektiv det är skyddsvärt samt vilken maximal konsekvens som kan accepteras för det skyddsvärda.

Bedömningarna i säkerhetsanalysen motiverar sedan vilka förebyggande säkerhetsåtgärder inom områdena informationssäkerhet, tillträdesbegränsning och säkerhetsprövning som ska vidtas för att minska sårbarheterna.

Utbildning i informationssäkerhet och kontroll av säkerhetsarbetet är också viktiga delar i det förebyggande arbetet.

2.2 Behandling av hemliga uppgifter

Digitala uppgifter kan förekomma i många olika format och finnas i olika typer av informationstillgångar. Det kan exempelvis röra sig om, handlingar, minnesanteckningar, beslutsunderlag, risk- och sårbarhetsanalyser, rapporter, bilder, ljudfiler och databaser. För att veta vilken skyddsnivå den digitala informationen ska ha behöver informationen värderas och klassas. Verksamheten behöver med andra ord göra en bedömning innan man börjar hantera informationstillgången så att man använder ett systemstöd som uppfyller de säkerhetskrav som ställs för att hantera uppgifterna.

Arbetet med att bedöma vilka krav som behöver uppfyllas underlättas med en fastställd klassificeringsmodell som är ett stöd i bedömningen. Klassningen styr sedan direkt eller påverkar utformningen av exempelvis valet av IT-utrusning, vidare hantering och förvaring.

Något som man också behöver beakta i samband med värderingen är den totala mängden skyddsvärd information, så kallad aggregerad information som i vissa fall kan få ett högre skyddsvärde än den enskilda uppgiften.

Några rekommendationer:

- Klassa uppgifterna utifrån fastställd klassificeringsmodell. Stöd i framtagande av klassificeringsmodell finns på www.informationssäkerhet.se.
- Identifiera förekomsten av skyddsvärd information.
- Säkerställ att det i verksamheten finns förutsättningar att hantera uppgifterna korrekt:
  - » Att det för ändamålet finns adekvat framtagen och beslutad utrustning till exempel en fristående dator.
  - » Att det finns framtagna hanteringsregler.
  - » Att det finns kvittenslistor för utlämning och återlämning av en dator.
  - » Att personal är säkerhetsprövad (och registerkontrollerad) samt är inplacerad i säkerhetsklass.
  - » Att personalen är utbildad och införstådd i de hanteringsregler som gäller.
  - » Att det finns ändamålsenliga lokaler.

Det bör tas fram regler för den fristående datorn i sig och dess eventuella tillbehör avseende registrering, kvittering, hantering, förvaring, återlämning, destruktion etc. i enlighet med verksamhetens bestämmelser.

2.3 Överföring

Vid överföring av hemliga uppgifter krävs nationellt godkända kryptolösningar så kallade signalskyddssystem. Med signalskydd så avses system och åtgärder som syftar till att förhindra obehörig insyn i och påverkan av telekommunikations- och IT-system. Med hjälp av kryptolösningar och övriga signalskyddsåtgärder kan en säker överföring av informationen ske samtidigt som åtgärderna förhindrar att den hemliga informationen förvanskas eller röjs för obehöriga.

Hemliga uppgifter ska vid överföring krypteras med kryptosystem (signalskyddssystem) som har godkänts av Försvarsmakten enligt 13 § säkerhetsskyddsförordningen.

Ett signalskyddssystem består av tre samverkande enheter:

- signalskyddsmateriel (teknisk utrustning eller programvara)
- tillhörande signalskyddsnycklar och/eller aktiva kort
- en instruktion för hur signalskyddssystemet ska hanteras

Till de olika signalskyddsystemen finns det tillgång till användarstöd och anpassade utbildningar.

Vissa signalskyddssystem kan kopplas ihop med befintliga nätverk vilket gör att signalskyddet kan komma att bli en integrerad del i en kommunikationslösning.

Man ska göra en informationsanalys över verksamhetens informationstillgångar och i denna identifiera vilka samverkansvägar/informationsflöden man vid överföring av informationen är i behov av. Informationsanalysen påvisar vilka avsändare och mottagare man har behov av att kommunicera med, i vilken omfattning och i vilket format man kommunicerar (tal, data, digitalt eller via post).

Informationsanalysen ska ligga till grund för hur organisation och användningen av olika tekniska lösningar anpassas så att en organisations behov av informationsutbyte med andra parter blir tillgodosedda.

För mer information om när, hur och varför signalskydd kan användas, läs på informationssäkerhet.se/signalskydd.

2.4 Medförande

Samma hanteringsregler som gäller för medförande av hemliga handlingar i pappersformat bör tillämpas för handlingar i digitalt format. Det ska dokumenteras vad som gäller i de fall det föreligger behov av att medföra en dator som används för behandling av hemliga uppgifter från arbetsplatsen. Man bör också ha i åtanke hur skyddsvärd den fristående datorn blir med hänsyn till den aggregerade informationen som finns i datorn.

Med medförande menas när en person i sin tjänsteutövning exempelvis behöver transportera och förvara en fristående dator eller lagringsmedia utanför verksamhetens område och lokaler. Medförande bör beslutas av ansvarig chef.

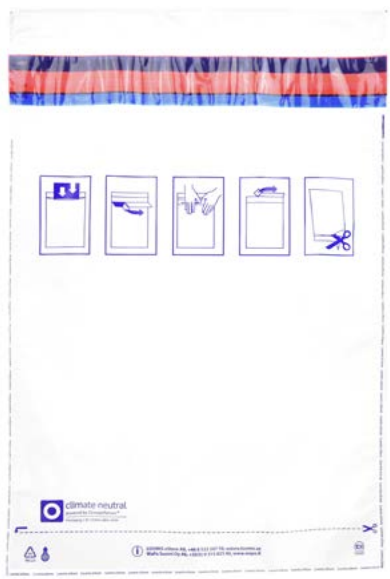
Beslut om medförande bör minst innehålla:

- för vilket ändamål den fristående datorn medförs
- till vilka platser den ska medföras
- när datorn ska återföras
- vem som är ansvarig för att säkerställa att datorn är återlämnad

Ett beslut om medförande kan vara generellt och utformas för att gälla ett visst specifikt behov.

I det fall en fristående dator avsedd för behandling av hemliga uppgifter tas med utanför verksamhetens lokaler ska den hållas under omedelbar uppsikt och ska förvaras på ett sätt som motsvarar den skyddsnivå som gäller för förvaringen av datorn inom verksamhetens lokaler. Vid medförande är det också lämpligt att:

- Någon form av dokumentation eller säkerhetskopiering av den fristående datorns innehåll har gjorts. Detta för att vid eventuell röjning eller förlust kunna redogöra för vilken information som den fristående datorn innehöll.
- När datorn inte används så bör den om det är möjligt förvaras i förseglat emballage så att eventuellt försök till intrång i emballaget kan uppmärksammas, förslagsvis i en säkerhetspåse.



Fristående dator

3. Fristående dator

Det här kapitlet beskriver bland annat vilka funktionella it-säkerhetskrav samt säkerhetskrav som kan appliceras på en fristående dator.

Beskrivningen avser en fristående dator som inte är ansluten till något nätverk eller motsvarande, här avses även ett enanvändarsystem. Med enanvändarsystem menas i det här fallet att endast en fysisk person tillåts ha behörigheter och åtkomst till den fristående datorn. Trots att datorn benämns som fristående så kan den av verksamheten tillåtas att kommunicera med godkänt lagringsmedia (USB-minne) och tillbehör så som skrivare eller kopiator.

Den fristående datorn kan i grunden utgöras av en valfri dator med både standard operativsystem och programvara, men som konfigurerats (härdats) utifrån de krav och behov som identifierats för att uppnå det säkerhetsskydd som informationen kräver.

I det fall säkerhetanalysen kommer fram till att den fristående datorn behöver skyddas mot röjande signaler, krävs en RÖS-skyddad dator alternativt en RÖS-skyddad lokal, se vidare i kapitel 3.2.6. Skydd mot röjande signaler.

Nedan tabell baseras på termer som används i Försvarsmaktens Krav på IT-säkerhetsförmågor hos IT-system v3.1 och är ett urval.

TERM	FÖRKLARING
Behörighets-kontroll	Administrativa eller tekniska åtgärder, eller både och som vidtas för att kontrollera en användares identitet, styra en användares behörighet att använda IT-systemet och dess resurser samt registrera användaren.
Objekt	Något som innehåller eller mottar information och som subjekt kan genomföra operationer på. Exempel filer, kataloger och enskilda data.
Röjande signaler (RÖS)	Inte önskvärda elektromagnetiska signaler som alstras i informationsbehandlande utrustning och som, om de kan tydas av obehöriga, kan bidra till att information röjs.
Skadlig kod	Programkod som är till för att ändra, röja, förstöra eller avlyssna ett IT-systems funktioner eller uppgifter.
Subjekt	En entitet i ett IT-system som kan utföra en åtgärd. Ett subjekt kan till exempel vara IT-systemet representation av en användare, en process eller en dator.
Säkerhetsfunktion	En eller flera funktioner i ett IT-system som upprätthåller säkerheten enligt regler om hur uppgifter i IT-systemet ska skyddas

Säkerhetsloggning	Manuell eller automatisk registrering eller både och, av händelser som är av betydelse för säkerheten i eller kring ett IT-system.
Lagringsmedia	Permanent minnesmedium som används för att kunna lagra och läsa, till exempel USB-minne, CD/DVD-skiva, extern hårddisk.

3.1 Allmänt

Den fristående datorn ska aldrig anslutas till någon kommunikation mot nätverk eller dylikt. Den fristående datorns förmåga att kommunicera mot annan aktiv eller passiv utrustning ska alltid vara avstängd (avser till exempel wifi, bluetooth och airdrop). Undantag gäller för lokalt anslutna enheter så som till exempel skrivare via USB-kabel.

3.1.1 Systemunderhåll

Rutiner för systemunderhåll som exempelvis uppdateringar av operativsystem, skydd mot skadlig kod behöver tas fram och fastställas innan den fristående datorn tas i bruk. Uppdateringar kan exempelvis ske genom att den fristående datorns hårddisk i sin helhet byts ut mot en ny konfigurerad hårddisk eller att uppdateringar görs via av verksamheten godkänt och dedikerat flyttbart lagringsmedia så som CD/DVD eller USB-minne. En kompletterande säkerhetsåtgärd är att alltid förstöra lagringsmediet efter genomförd uppdatering. Ansvaret för systemunderhåll kan ligga hos både användaren eller genom support av systemtekniker eller motsvarande. I båda fallen behöver rutiner för genomförande tas fram. Personal som använder eller administrerar den fristående datorn behöver vara inplacerad i säkerhetsklass (läs mer om detta i säkerhetspolisens vägledningar).

3.1.2 Systemförvaltning

Innan den fristående datorn konfigureras av systemtekniker eller motsvarande, så ska det säkerställas att systemteknikerna är placerade i säkerhetsklass. Detta för att systemteknikerna får en god uppfattning om den it-miljö som används för att bearbeta data. Systemteknikerna har även administrationsrättigheter och skulle kunna göra medvetna konfigurationsändringar som innebär en försämring av de skyddsåtgärder som identifierats som lämpliga.

Lokalen där konfiguration, uppdatering och anpassning av dessa datorer sker bör uppfylla ett antal säkerhetskrav. Kraven fås genom säkerhetsanalysen och kan avse till exempel inpassering, förvaring av utrustning, koder och rutiner.

3.1.3 Lagringsmedia

I de fall något lagringsmedia ansluts till den fristående datorn, ska lagringsmediet minst omgärdas av samma säkerhetskrav som den fristående datorn. Det vill säga, utformas så att den lagrade informationen inte kommer obehöriga till del, att eventuell förlust uppmärksammas samt att övriga säkerhetskrav upprätthålls gällande förvaring, hantering, medförande, märkning, arkivering, förstöring etc.

Lagringsmedia kan i vissa fall innehålla en stor mängd hemliga uppgifter samtidigt som det yttre utförandet kan vara mycket litet, exempelvis ett USB-minne. En förlust av ett sådant lagringsmedium kan medföra stora konsekvenser. Det är därför viktigt att så långt det är möjligt minimera användningen av lagringsmedia. I det fall det inte är möjligt behöver verksamheten ta fram tydliga rutiner för användandet av externa lagringsmedium.

3.1.4 Säkerhetskopiering

Säkerhetskopiering är en viktig åtgärd som säkerställer att uppgifterna i den fristående datorn går att återställa, oberoende om den eventuella förlusten av informationen sker uppsåtligen eller genom oaktsamhet. Rutiner för säkerhetskopiering behöver därför tas fram innan den fristående datorn tas i bruk. Säkerhetskopiering kan exempelvis genomföras av användaren via ett av verksamheten godkänt och dedikerat lagringsmedia. Lagringsmediet ska sedan hanteras och förvaras i samma skyddsnivå som den fristående datorn enligt framtagna rutiner. En ytterligare säkerhetsåtgärd som kan vidtas är att säkerhetskopian förvaras i ett separat utrymme, skilt från datorn men som uppfyller samma krav avseende förvaringen, till exempel godkänt säkerhetsskåp.

3.1.5 Skrivare, kopiator och andra tillbehör

Utskrift eller kopiering kan exempelvis ske via godkänd dedikerad skrivare eller kopiator utan något permanent lagringsmedia där utskrifter mellanlagras, alternativt kan skrivaren eller kopiatorn ha en löstagbar hårddisk som monteras bort och förvaras i godkänt säkerhetsskåp när den inte används. Ett ytterligare alternativ är att den dedikerade skrivaren eller kopiatorn förvaras i godkänt förvaringsutrymme.

Skrivare eller kopiator som används till den fristående datorn får inte vara ansluten till något nätverk eller motsvarande. Skrivare, kopiator och andra tillbehör, till exempel en projektor, bör inte användas tillsammans med den fristående datorn för att senare anslutas till annan utrustning.

Kopia av eller ett utdrag ur en hemlig handling ska i sig omfattas av samma skydd och ska hanteras likartat med hänsyn till eventuella krav på registrering, kvittering, hantering, förvaring, återlämning och destruktion i enlighet med verksamhetens interna bestämmelser.

I skrivare och kopiator kan stora mängder av uppgifter mellanlagras, när det rör sig om skrivare eller kopiator tillhörande den fristående datorn bör det finnas en dokumenterad rutin för hur underhåll och service ska genomföras (detta inkluderar regler för intern och extern servicepersonal) samt hur utrustningen skyddas mot manipulation och röjande signaler. Det bör också framgå på kopiatorn eller skrivaren vilka uppgifter den är godkänd för.

Kontrollera de tillbehör som avses anslutas till den fristående datorn så att den inte har inbyggda trådlösa funktioner som till exempel wifi eller bluetooth.

3.1.6 Märkning

I det fall en handling bedöms innehålla hemliga uppgifter ska detta framgå genom att handlingen förses med en hemligbeteckning. Även en fristående dator och eventuellt lagringsmedia ska så långt det är möjligt märkas. Detta gäller både allmänna och icke allmänna handlingar då det anger vilket skydd informationen i handlingen kräver.

3.1.7 Destruktion

Rutiner för destruktion av den fristående datorn, externt lagringsmedia och tillbehör (skrivare, kopiator) bör tas fram och fastställas av verksamheten innan utrustningen tas i bruk. Destruktion kan exempelvis genomföras genom bränning eller mekanisk bearbetning. I Sverige finns destruktionsanläggningar som genom bränning förstör materiel. En rekommendation är att alltid ha egen personal med som bevakar destruktionen.

3.1.8 Incident

En incident kan handla om uppsåtliga eller oavsiktliga händelser som medför störningar avseende konfidentialitet, riktighet eller tillgänglighet. En incident kan exempelvis vara dataintrång, olovlig avlyssning, stöld, spridning av skadlig kod eller manipulation av utrustning, kablage och lagringsmedia. Det kan också vara hård- eller mjukvarufel som uppstår utan någon yttre påverkan eller medvetet försök till sabotage.

En verksamhet ska ha fastställda och dokumenterade rutiner för hantering, rapportering och uppföljning av incidenter av betydelse för säkerheten.

När omständigheterna kring röjandet utreds kan följande frågeställningar användas:

- Vilka personer är inblandade?
- Vad har hänt?
- När hände det?
- När upptäcktes det?
- Hur hände det?
- När inventerades handlingarna eller lagringsmedierna senast?
- Vem har haft tillgång till uppgifterna?
- Vad finns det som tyder på att uppgifterna inte är röjda?

Svaren på ovanstående frågor kan sedan utgöra underlag för eventuella skyddsåtgärder för att förhindra ytterligare röjande och eliminera eller minska konsekvenserna av den röjda uppgiften. Skyddsåtgärder kan även behöva vidtas tidigt efter att röjandet har upptäckts.

3.1.9 Avveckling

Vid avveckling eller återlämnande av den fristående datorn ska användaren som nyttjat datorn få en kvittens på att datorn är återlämnad. Detta kan med fördel noteras på samma underlag som användes för att kvittera ut utrustningen.

3.2 Konfiguration av fristående dator

Nedanstående rekommendationer avser en lägstanivå av säkerhet som bör beaktas avseende säkerhetsfunktioner för den fristående datorn avsett för hemliga uppgifter. Säkerhetsfunktionerna ska dock inte ses som begränsande utan kan behöva kompletteras med ytterligare egna krav och åtgärder utifrån genomförd säkerhetsanalys. Syftet är att förebygga att hemliga uppgifter obehörigen röjs, ändras eller förstörs.

3.2.1 Konton och rättigheter

Den fristående datorn bör tilldelas två konton.

- Ett användarkonto som är begränsat och används för det dagliga arbetet.
- Ett administratörskonto som används vid administration av datorn (användaren får inte ha åtkomst till kontot).

3.2.2 Behörighetskontroll

Behörighetskontroll handlar om att kontrollera en användares identitet, styra en användares behörighet att använda datorn och dess resurser samt registrera användaren. Behörighetskontroll kan vara administrativa eller tekniska åtgärder, eller både administrativa och tekniska åtgärder som vidtas för, identifiering av användaren, verifiering av den föregivna identiteten, styrning av användarens åtkomsträttigheter till systemet samt registrering av användarens aktivitet.

Exempel:

- Lösenord
- Förstärkt inloggning (smart/aktivt-kort)
- Tvåfaktors-autentisering, både lösenord och förstärkt inloggning (smart/aktivt-kort)

Behörighetskontroll syftar till att förhindra obehörig åtkomst och dessutom säkerställa att det finns en spårbarhet över de aktiviteter som görs i datorn.

Rekommendation

Vid uppstart av den fristående datorn så bör det krävas två inloggningar, exempel:

1. Inloggning med PIN till Microsoft och exempelvis Bitlocker (eller annan motsvarande diskkryptering).
2. Inloggning med användarnamn och lösenordsfras till det användarkonto som ska användas vid tillfället.

Vid första inloggningstillfället ska användaren ersätta temporär PIN till exempelvis Bitlocker (eller annan motsvarande diskkryptering) samt de temporära lösenordsfraserna till användarkontot. Användarkonton bör ha lösenordsfraser som består av minst 14 tecken och att man använder gemener, versaler, siffror och specialtecken.

3.2.3 Säkerhetsloggning

Säkerhetsloggning handlar om att registrera händelser som är av betydelse för säkerheten i eller kring en dator. Detta kan ske manuellt eller automatiskt.

En säkerhetslogg bör visa av vem, var, när och hur en händelse inträffat. Kontroll och uppföljning av säkerhetsloggarna bör ske kontinuerligt enligt en framtagen loggrutin, som tydligt definierar vad som ska granskas. Säkerhetsloggar kan exempelvis användas i samband med utredningar om intrångsförsök, felaktig eller obehörig användning, spårning av missbruk eller försök till missbruk. En stor fördel är också om loggarna kan rekonstruera ett händelseförlopp.

Säkerhetsloggarna kan också behöva analyseras i extern miljö, loggarna kan därför behöva kunna exporteras, helt eller delvis. Med anledning av att säkerhetsloggar kan användas i till exempel utredningar av olika slag kan säkerhetsloggarna beroende på innehåll och omständigheter anses i vissa fall innehålla hemliga uppgifter, vilket behöver beaktas.

Kravställning av en dators säkerhetsloggning bör föregås av en analys som identifierar syftet med loggarna och hur dessa bör vara utformade för att uppfylla verksamhetens krav och behov. Möjligheten att analysera loggar är en grundläggande funktion för att kunna följa händelser och åtgärder genom systemets olika delar.

Rekommendation

Säkerhetsfunktionen för säkerhetsloggning ska minst omfatta:

- Konfigureringsförändringar i systemet främst händelser som har betydelse för säkerheten.
- In- respektive utläsning av information/data samt registrera tid och datum för händelsen, användarens eller subjektets identitet.
- Säkerhetsloggning ska kunna presenteras i läsbar form.
- Säkerhetsloggar sparas i enlighet med verksamhetens interna bestämmelser.
- Att registrerade händelser inte raderas, skrivs över eller på annat sätt förstörs.

3.2.4 Intrångsskydd

Intrångsskydd handlar om att på ett kontrollerat sätt ge åtkomst till olika tjänster som finns i datorn. Intrångsskydd kan utgöras genom administrativa, tekniska eller fysiska skyddsåtgärder, alternativt en kombination av dessa.

Exempel på tekniska åtgärder:

- Samtliga funktioner, program eller anslutningar som inte stödjer systemets primära syfte ska vara avstängda.
- Information som flödar ut ur systemet ska kontrolleras och vara möjlig att begränsa.

Exempel på administrativa åtgärder:

- Tydliga rutiner avseende hanteringsregler för datorn.
- Utbildning av användare.

Exempel på fysiska åtgärder:

- Lås in den fristående datorn i godkänt förvaringsutrymme (rekommenderat säkerhetsskåp som uppfyller kraven enligt standard SS3492) när den inte används.
- Lämna aldrig den fristående datorn obevakad.

3.2.5 Skydd mot skadlig kod

Funktionerna mot skadlig kod ska förhindra att datorn påverkas av, till exempel virus, trojaner, maskar och logiska bomber. Skyddsåtgärderna behöver anpassas beroende på vilka gränsytor och externa kopplingar som tillåts. Förekomsten av skadlig kod kopplas ofta ihop med internet och e-post, men även felaktig användning av flyttbart lagringsmedia som till exempel ett USB-minne kan innehålla skadlig kod. För att motverka skadlig kod via flyttbart lagringsmedia kan en så kallad ”tvättstation” upprättas som ett extra skydd. ”Tvättstationen” är en dedikerad dator framtagen enbart i syfte att spåra skadlig kod i flyttbara lagringsmedia. ”Tvättstationen” bör ha samma förvarings- och behörighetskrav som den fristående datorn.

Utöver den vanligaste skyddsåtgärden som är att installera antivirusprogramvara så kan även en dator och dess operativsystem låsas ner, ”härdas” för att ytterligare skydda datorn mot att skadlig kod kan exekvera på datorn. Sådana funktionella säkerhetskrav är till exempel:

- Rutin för säkerhetsuppdateringar av installerad programvara.
- Riktighetskontroll av filer och konfigurationer.

- Genom kontrollmekanismer reglera möjligheten att skriva, ändra, förstöra eller på annat sätt manipulera objekten i den fristående datorns program.
- Funktioner för att automatiskt kontrollera att installerad mjukvara överensstämmer med aktuell version.
- Automatisk detektering av skadlig kod samt kunna vidta åtgärder. Åtgärderna ska omfatta placering av smittat subjekt eller objekt i karantän samt visa en varning för den berörda användaren.
- Genomföra kontroller av subjekt och objekt under drift, vid uppstart och när så är påkallat.

Rekommendation

Datorn bör som minst vara försedd med ett virusskydd mot skadlig kod och som det finns en utpekad ansvarig för att hålla uppdaterat utifrån fastställda regler.

3.2.6 Skydd mot röjande signaler

Skydd mot röjande signaler handlar om att säkerställa att information som behandlas i en dator inte oavsiktligt röjs via elektromagnetiskstrålning och läckande signaler i kablage, som i värsta fall kan tydas av obehöriga. Skydd mot röjande signaler kan fås genom att använda en RÖS godkänd dator eller att använda en lokal som är RÖS godkänd eller båda i kombination.

Rekommendation

En analys avseende behov av RÖS-skydd bör alltid göras innan den fristående datorn tas i bruk.

3.2.7 Sammankopplade datorer (nätverk)

I de fall en fristående dator inte är tillräcklig för att tillgodose en verksamhets behov av digital bearbetning av information så kan en organisation välja att koppla samman datorer i ett nätverk. Samma skyddsfunktioner som rekommenderas för en fristående dator ska minst appliceras även vid sammankoppling av fler datorer. Då sammankoppling av datorer och säkerställande av fullgoda säkerhetsåtgärder i nätverk bedöms vara mer omfattande beskrivs inte det närmare här. De formella kraven på funktioner som ska upprätthållas finns i PMFS 2015:3 kap 4, IT-säkerhet. För ytterligare stöd hänvisas till Försvarsmaktens ”Handbok säkerhetstjänst informationssäkerhet” från 2013 med M-nr: M7739-352056 för mer tips och råd. Handboken finns tillgänglig via www.forsvarsmakten.se.

3.3 Övrigt

Kapitel 3.2 Konfiguration av fristående dator, beskriver säkerhetsfunktioner som avser en lägstanivå av säkerhet som bör beaktas. Nedanstående checklista ger ytterligare konkreta rekommendationer kring styrning och konfigurering av den fristående datorn som skulle kunna vara aktuella och ska ses som uppslag för kompletterande åtgärder utöver kap 3.2.

- Nätverksgränssnitt bör vara avaktiverade, exempelvis nedlåsning av bluetooth, firewire, HDMI, modem(3G/4G), BIOS nedlåsning (lösenord för åtkomst lagras hos systemadministratör som konfigurerar systemet). Användaren bör inte ha tillgång till detta lösenord.
- Bootning: användaren bör endast kunna starta systemet (med driftsatt hårddisk.) Det bör tydligt framgå vad som ska vara aktiverat, följ vitlistningsprincipen.
- In- och utförsel av information bör i första hand ske via CD/DVD-skiva alternativt dedikerat USB-minne.
- Lagringsmedia (ex USB-minne) som anslutits till den fristående datorn rekommenderas enbart användas i motsvarande system med samma klassning. Lagringsmedia som tidigare anslutits till den fristående datorn ska aldrig användas i system med en lägre klassning, exempelvis ett intranät.
- Den fristående datorns brandväggsregler bör konfigureras till att inte tillåta varken inkommande eller utgående kommunikation, detta för att minimera risken för att användaren själv ändrar i brandväggsreglerna.
- Uppdaterat operativsystem, det bör framgå hur och i vilken omfattning uppdatering ska genomföras.
- Installerad programvara enligt behov och efter en godkännandeprocess, all annan programvara bör avinstalleras.
- Funktionen för automatiska uppdateringar bör vara avslagen.
- Den fristående datorn får aldrig anslutas mot internet.
- WIFI och andra trådlösa funktioner samt nätverksportar bör, där det så är möjligt vara avslagna i BIOS, i det fall detta inte är möjligt behöver andra åtgärder vidtas så att dessa funktioner inte kan aktiveras av användaren.
- Krypterad hårddisk rekommenderas.
- Inställning av automatiskt skärmlås vid inaktivitet efter exempelvis fem minuter.
- Rutiner för all service av hårdvara som kan komma att innehålla hemliga uppgifter behöver vara fastställda och

dokumenterade innan service påbörjas, oavsett om det är intern eller extern personal som utför servicen. Vid nyttjande av extern personal kan behov föreligga att genomföra en säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA) av tjänsten.

- Uppdatering av antivirusprogram med aktuella konfigurationsfiler sker lämpligen via CD/DVD-skiva i andra hand USB-minne (bör endast användas en gång och där efter destrueras enligt fastställda rutiner).
- Systemloggning ska alltid vara påslaget.
- Det bör tydliggöras att användaren förstår och ansvarar för att säkerhetsbestämmelserna följs och att backuper genomförs på viktiga filer, och förvaras på ett tillförlitligt sätt så att de inte kommer någon obehörig till del.
- I de fall den fristående datorn ska användas av flera personer ska alla vara behöriga till all information, och alla ska ha egna inloggningskonton så lång det är möjligt. Datorn bör då förvaras i ett gemensamt godkänt förvaringsutrymme med samförvaringsbeslut.
- Ett alternativ är att varje användare tilldelas personliga diskar men en gemensam dator. Datorn bör då förvaras utan hårddisk i ett gemensamt godkänt förvaringsutrymme Respektive användare förvarar sedan sin egen hårddisk i ett godkänt förvaringsutrymme exempelvis innerfack i ett gemensamt säkerhetsskåp, ett samförvaringsbeslut behöver då upprättas för de som använder säkerhetsskåpet. Även om datorn är utan hårddisk så bör den förvaras så att ingen obehörig kan manipulera den.
- Det bör dokumenteras vilka som gemensamt använder en fristående dator, det bör också dokumenteras vilka fristående datorer som finns. Samtliga sammanställningar bör finnas hos exempelvis registratur där man kvitterat ut datorn.
- Används fler hårddiskar till en fristående dator, ska varje hårddisk personligen kvitteras av den som ska nyttja hårddisken. Kvitteringen ska ske på liknande sätt som vid kvittering av en hemlig handling.
- Det bör framgå i verksamhetens interna bestämmelser att den fristående datorn alltid när den inte används förvaras i godkänt förvaringsutrymme.
- Datorn bör plomberas, detta för att användaren lättare ska kunna uppmärksamma om den utsatts för åverkan. Plombering sker lämpligen med numrerade säkerhetsetiketter som går sönder då de tas bort.

Myndigheten för samhällsskydd och beredskap (MSB)
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB1309 - december 2018 ISBN 978-91-7383-891-7