Myndigheten för
samhällsskydd
och beredskap

Vägledning för säkrare hantering av mobila enheter

Sammanfattning

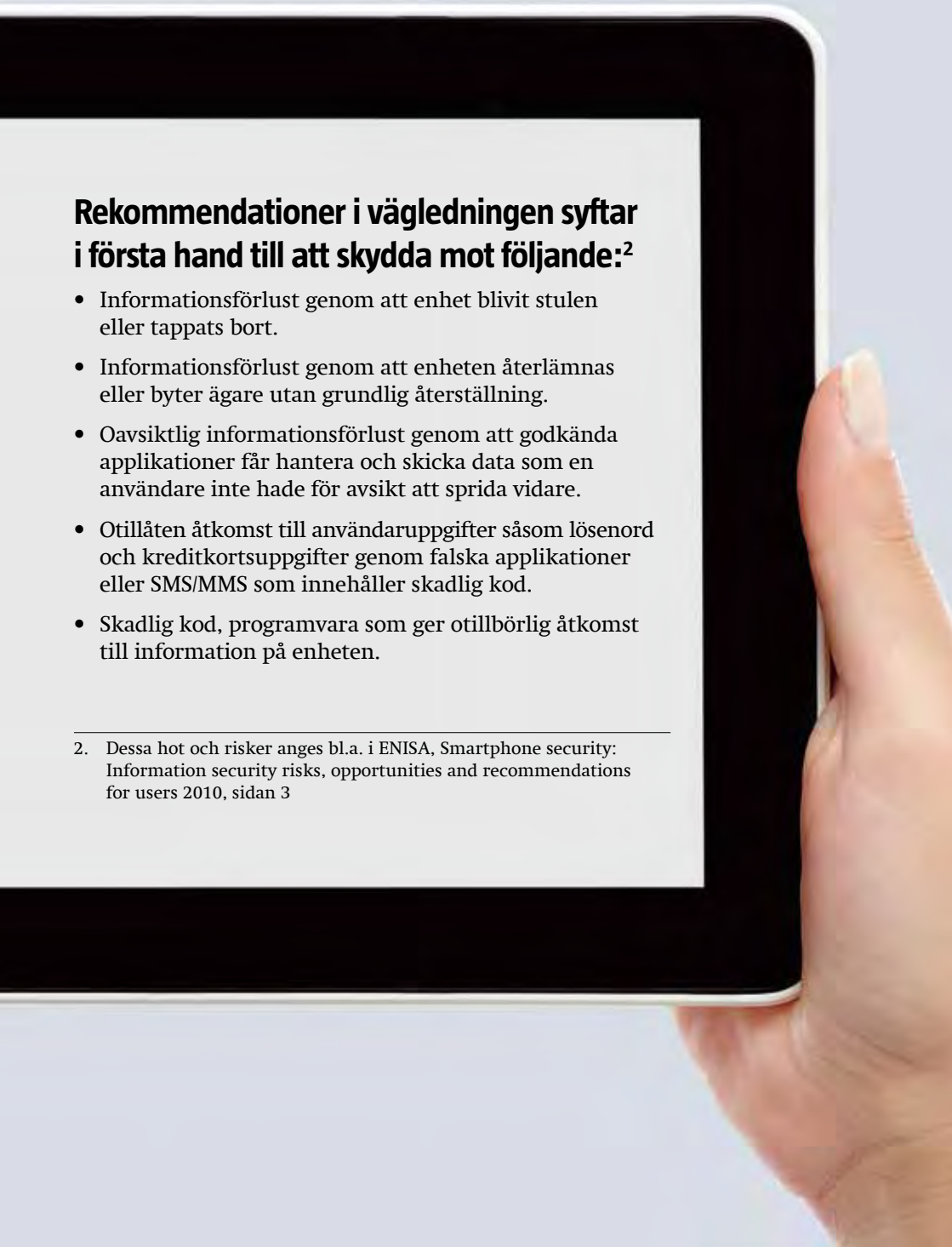
Smarta telefoner, surfplattor och andra liknande mobila enheter används i allt större utsträckning både privat och i organisationer. En annan växande trend är att användarna ges åtkomst till arbetsrelaterad information via mobila enheter. Den ökande användningen av smarta telefoner och surfplattor i kombination med att den privata och arbetsrelaterade sfären smälter alltmer samman innebär att verksamhetens information och informationstillgångar exponeras på ett nytt sätt genom de mobila enheterna. Utvecklingen ställer krav på organisationer som vill nyttja teknikens möjligheter på ett säkert sätt.

Denna vägledning ska utgöra ett stöd för organisationer som planerar att tillåta att smarta telefoner, surfplattor eller liknande mobila enheter ansluts till verksamhetens interna resurser och vill göra det på ett så säkert sätt som möjligt. Utmaningarna ligger i stor grad inom utbildning, management, regelverk och tekniska implementationer för skydd. I vägledningen finns rekommendationer för vad organisationen bör reglera i regelverk och rutiner, vilka krav som bör ställas på användarna samt vilka tekniska skydd som rekommenderas när mobila enheter får kopplas upp mot verksamhetens interna resurser.

Det finns många olika sorters mobila enheter. Smarta telefoner och surfplattor utgör de mer avancerade enheterna under begreppet mobila enheter och i vägledningen kommer samlingsnamnet i första hand användas även om rekommendationerna i de flesta fall är avsedda för att stödja hanteringen av just smarta telefoner och surfplattor.

Underlaget för val av rekommendationer utgörs av en sammanställning från de mest förekommande åtgärdspunkterna i interna regler som MSB har tagit del av från ett antal myndigheter och organisationer. Därtill har även rekommendationer från Europeiska byrån för nät- och informationssäkerhet (ENISA)[1] beaktats.

1. http://www.enisa.europa.eu/



Rekommendationer i vägledningen syftar i första hand till att skydda mot följande:[2]

- Informationsförlust genom att enhet blivit stulen eller tappats bort.
- Informationsförlust genom att enheten återlämnas eller byter ägare utan grundlig återställning.
- Oavsiktlig informationsförlust genom att godkända applikationer får hantera och skicka data som en användare inte hade för avsikt att sprida vidare.
- Otillåten åtkomst till användaruppgifter såsom lösenord och kreditkortsuppgifter genom falska applikationer eller SMS/MMS som innehåller skadlig kod.
- Skadlig kod, programvara som ger otillbörlig åtkomst till information på enheten.

---

2. Dessa hot och risker anges bl.a. i ENISA, Smartphone security: Information security risks, opportunities and recommendations for users 2010, sidan 3

Bakgrund

Användandet av mobila enheter har ökat starkt de senaste åren och förutspås fortsätta att öka[3] men det finns fortfarande en viss osäkerhet hur sådana enheter ska hanteras i organisationen och vilka säkerhetsåtgärder som bör vidtas.

Utvecklingen och designen av smarta telefoner, surfplattor och andra liknande mobila enheter har främst präglats av marknadens krav på funktionalitet, utan att i grunden ta sikte på och garantera säkerheten i enheterna. Sådana mobila enheter kan idag ofta innehålla personlig information om användaren, hans/hennes kontaktnät och inte sällan även användarnamn och lösenord till en rad olika tjänster. Vid bedömningen av behovet av säkerhetsåtgärder bör beaktas att de mer avancerade mobila enheterna kan spåras, övervakas och avlyssnas. Det går snabbt och lätt att installera spionprogram och annan skadlig kod, särskilt om enheterna vid ett obevakat tillfälle hamnar i fel händer.

Om information lagras på den mobila enheten är det viktigt att den ges adekvat skydd och att enheten hanteras på ett sådant sätt att exponeringen av informationen minskar. Information på den mobila enheten behöver skyddas så att den inte kommer i orätta händer, manipuleras eller förloras. Vid manipulation eller förlust av en mobil enhet som används i arbetet och som har möjlighet att kopplas upp mot organisationens interna nät kan den användas som språngbräda för vidare attacker in i organisationen. Genom att till exempel återanvända lagrad information för trådlösa nätverk kan en angripare ges åtkomst till organisationens interna resurser. Beroende på angriparens syfte kan detta leda till ytterligare allvarligare informationsförluster, tillgänglighetsproblem, förlust av förtroende hos samarbetspartners och kunder etc. Syftet med skyddsåtgärderna är att ge en tvåstegseffekt; om de mobila enheterna får

3. Se exempelvis – Gartner Reveals Top predictions for IT Organizations and Users for 2012 and Beyond, http://www.gartner.com/it/page.jsp?id=1862714

ett utökat skydd för att minska risken att angrepp ska lyckas, så minskas även risken för att organisationens informationstillgångar och resurser i övrigt blir åtkomliga för externa angripare via de mobila enheterna.

Syfte

Det finns ett stort antal olika typer av mobila enheter som alla har olika säkerhetsmässiga förutsättningar och risker. I vägledningen används genomgående begreppet *mobila enheter* men rekommendationerna är i de flesta fall avsedda för att stödja hanteringen av de mer avancerade enheterna, främst smarta telefoner och surfplattor.

Som underlag för valet av rekommendationer i denna vägledning har MSB bland annat utgått från en sammanställning av de vanligast förekommande åtgärdspunkterna i interna regler hos ett antal myndigheter och organisationer samt rekommendationer från ENISA. De rekommendationer som finns samlade i vägledningen bör ses som “good practice”, snarare än ”best practice” eftersom det finns en rad olika ändamålsenliga sätt att lösa hanteringen av mobila enheter på. För att underlätta användningen av rekommendationerna är dessa indelade i tre huvudgrupper baserat på vilket syfte de har och vilken målgrupp de vänder sig till:

- Rekommendationer för utformning av regelverk och rutiner.
- Rekommenderade krav som bör ställas på användare.
- Rekommendationer för utformning av tekniska skydd.

Att arbeta systematiskt med informationssäkerhet är en process där bland annat krav som ställs av verksamheten, andra aktörer eller i legala regelverk påverkar utformning och val av skyddsåtgärder. Innan rekommendationerna används är det av vikt att man noga analyserar vilka behov av skydd den egna organisationen har.[4]

4. På www.informationssäkerhet.se finns bland annat stöd för hur en organisation kan genomföra en riskanalys och andra åtgärder som är kopplade till ett systematiskt informationssäkerhetsarbete

En sådan analys bör utgöra en del i ett regelbundet återkommande arbete samt upprepas då kraven förändras. En organisation som till exempel idag inte tillåter uppkoppling av telefoner mot interna resurser behöver inte heller hantera detta i sina regler och kan givetvis bortse från vägledningens rekommendationer i dessa delar. Ändras förhållandena bör utformning av regelverk och rutiner, krav på användare samt tekniska skydd naturligtvis ses över.

När organisationen äger den mobila enheten kan organisationens regelverk rörande de mobila enheterna lättare upprätthållas. Organisationen kan kräva att den anställde följer fastställda regler avseende hanteringen av den mobila enheten men även installera programvara och göra fysiska begränsningar i enheten för att på det sättet öka säkerheten. Användaren har dock fortfarande ett stort ansvar för hanteringen av enheten. Mobiltelefoner och surfplattor uppfattas av många användare som en mer "privat" ägodel än t.ex. en bärbar dator, varför införandet av tekniska begränsningar för att upprätthålla regelverk kan väcka visst motstånd hos de anställda.

Rekommendationer angivna i vägledningen är främst avsedda att användas då organisationen äger den mobila enheten. Huvudrekommendationen är att inte tillåta privatägda enheter att ansluta sig till en organisations nätverk. Om detta ändå tillåts ges i slutet av vägledningen övergripande rekommendationer för vad man bör tänka på och hur man i ett sådant fall kan öka säkerheten.

När organisationen äger den mobila enheten

En process samt tre verktyg för ökad säkerhet

Att bygga upp säkerhet förutsätter i de allra flesta fall en kombination av åtgärder, både administrativa regler och tekniska lösningar. Som nämnts tidigare i vägledningen är säkerhetsarbete dessutom en process där de valda åtgärderna behöver utformas så att de motsvarar verksamhetens och omgivningens, ofta föränderliga, krav och önskemål. Det är även av vikt att se organisationens säkerhetsarbete som en helhet där säker hantering av mobila enheter utgör en del av flera sammanhängande pusselbitar.

På webbplatsen www.informationssäkerhet.se har MSB, tillsammans med andra myndigheter med särskilt ansvar för informationssäkerhet i samhället, samlat stöd för systematiskt informationssäkerhetsarbete i organisationer. Syftet är främst att underlätta för organisationer att leda och strukturera sitt informationssäkerhetsarbete genom att införa ett ledningssystem för informationssäkerhet (LIS). Arbetet med att säkra hanteringen av mobila enheter i organisationen bör utgöra en integrerad del av organisationens övergripande informationssäkerhetsarbete.

Informationsklassning är central aktivitet i säkerhetsarbetet för hanteringen av mobila enheter och har till syfte att bedöma informationens värde och känslighet. Bedömningen sker både utifrån den egna verksamhetens behov och utifrån externa krav. Avsikten är att varje informationstillgång (mobil enhet) ska omges med rätt skydd.

I alla delar av säkerhetsarbetet är det av vikt de som är berörda av olika åtgärder har tillräcklig kunskap om och insikt i vad som krävs av henne eller honom. Innan en användare kvitterar ut en mobil enhet, ska användaren ha tagit del av och bör även ha

undertecknat användarreglerna för den mobila enheten, detta för att tydliggöra att användaren förstår och är insatt i organisationens fastställda regler.

Nedan följer en sammanställning av rekommendationer som är är grupperade med utgångspunkt från det syfte och den målgrupp de har:

- *Rekommendationer för utformningen av organisationens regelverk och rutiner för hantering av mobila enheter* utgörs av en sammanställning av frågeställningar som organisationen behöver ta ställning till. Till exempel rekommenderas att organisationen fastställer vilka tjänster som ska vara åtkomliga från den mobila enheten. Valet av vilka tjänster som de facto görs tillgängliga bör grundas på en riskanalys.
- När det gäller *rekommendationer på krav som bör ställas på användare* ligger fokus på krav som enligt ”good practice” bör ställas på användarna. Det är av vikt att påpeka att dessa rekommenderade krav inte utgör en komplett uppsättning av användarregler. Efter att organisationen har tagit ställning till hur det mer övergripande regelverket och rutinerna ska utformas kommer användarreglerna att behöva kompletteras för att spegla dessa. För att underlätta för användarna att följa reglerna är det av vikt att dessa är samlade i ett eller ett fåtal dokument, tydliga och lättförståeliga.
- *Rekommendationerna för utformning av tekniska skydd* är konkreta och konsekvenserna av att göra avsteg från rekommendationerna bör analyseras noga. Införandet av tekniska skydd kan dock medföra kostnader vilka naturligtvis bör jämföras med förväntad nytta/effekt av investeringen.

Varje organisation utformar sina styrdokument och regler på ett sätt som passar den egna verksamheten. Syftet med indelningen ovan är främst att tydliggöra syftet med respektive typ av rekommendationer så att organisationen på ett enkelt sätt kan införliva rekommendationerna i sina egna styrdokument.

Rekommendationer för utformning av organisationens regelverk och rutiner för hantering av mobila enheter:

Fastställ i regelverk och rutiner:

Uppkoppling, installation

- Om användaren ska kvittera ut den mobila enheten för att förtydliga ägarförhållandena avseende enheten.
- På vilket sätt mobila enheter får koppla upp till organisationens resurser (trådlöst nätverk, via kabel, Bluetooth etc.).
- Vilka typer och modeller av mobila enheter som får kopplas upp till organisationens resurser (epost, nätverk etc.).
- Vilka tjänster (t.ex. e-post synkronisering och åtkomst till interna nätverksresurser) som ska vara åtkomliga från mobila enheter.
- Om beslut gällande uppkoppling av mobila enheter ska dokumenteras. Beslut bör användaren kvittera och beslutet bör innehålla vilka tjänster som avses, vem som avses och övriga ansvarsförhållanden.
- På vilket sätt inköp och eventuell ominstallation innan användning t.ex. återställning till fabriksinställningar ska hanteras. Detta för att minska risken med förinstallerad skadlig kod.

Användning och lagring

- Vilken typ information som får diskuteras i tal över mobila enheter.
- Hur de mobila enheterna får förvaras.
- Vilken typ av information som får lagras på den mobila enheten. Reglerna för vilken information som får lagras på mobila enheter bör kopplas till organisationens informationsklassificering[5] så att det blir enkelt för de anställda att ta till sig. En mobil enhet bör betraktas som ett osäkert media att lagra information på.

5. MSB har tillsammans med Swedish Standards Institute (SIS), publicerat en nationell modell för informationsklassificering som syftar till att stödja myndigheter och andra organisationer i deras arbete med att klassificera information på ett enhetligt sätt. Mer stöd kring informationsklassificering finns på https://www.msb.se/sv/Forebyggande/Informationssakerhet/Stod-fran-MSB/Stod--verktyg/.

- Om och i så fall hur externa lagringsutrymmen i den mobila enheten i form av t.ex. minneskort ska bytas ut och förstöras med viss regelbundenhet.
- Vad som gäller för användning av mobila enheter vid t.ex. möten eller samtal där känslig information hanteras. Vid sådana möten kanske sådana enheter inte får medföras in i möteslokalen överhuvudtaget då de kan fungera som avlyssningsutrustning utan användarens vetskap.
- Om internetsurfing får ske direkt från den mobila enheten eller om den måste gå via organisationens säkra uppkoppling för ökad möjlighet till kontroll och skydd av trafiken.
- Om användaren tillåts öppna SMS/MMS från okända avsändare eller klicka vidare på länkar som skickats från okända personer/avsändare.
- Om användaren ska avaktivera automatisk öppning av meddelanden.
- Om och hur användaren ska få installera applikationer (appar). En användare bör endast ladda ned applikationer som det finns behov av i tjänsten och från kända och välrenommerade bibliotek. En användare bör vara uppmärksam på vilken/vilka funktioner och information applikationer kräver tillgång till.
- Om användaren ska stänga av de tjänster som inte behövs i tjänsten, t.ex. allmänna lokaliseringstjänster, GPS positionering, WLAN, Bluetooth, GPS, Datatrafik etc. Detta minskar den mobila enhetens exponering och sparar dessutom batteri.
- Om användaren ska undvika att lägga upp bilder på internet tagna med den mobila enheten. Inbäddade metadata kan avslöja tid och plats som fotot togs.
- Om användaren regelbundet ska radera information som inte längre behövs.

Säkerhetsrutiner

- På vilket sätt backuper och synkronisering av enheter får ske och vilka skyddsåtgärder som ska gälla för backuperna.
- Om användaren ansvarar för att uppdatera den mobila enheten. Uppdateringar bör ske så fort tillgängliga uppdateringar finns.
- Om och i så fall hur loggning gällande användning av de mobila enheterna görs, samt att uppföljning kan förekomma om så är fallet.
- Vem som får besluta om installation av olika typer av programvara i enheten. Upprätta till detta beslut processer för att hantera godkännande av säkerhetsinställningar, applikationer, uppkopplingar etc. Om organisationen har en ”vitlista” över godkända applikationer kan användaren t.ex. installera dessa själv.
- Hur och i vilket intervall utbildning av användarna ska genomföras. Utbildning bör omfatta hantering av den mobila enheten samt de risker som finns förknippade med att använda dessa.
- Rutiner för säker hantering och radering av återlämnade enheter. En återlämnad enhet kan återanvändas inom organisationen, förmedlas vidare utanför organisationen för fortsatt användning eller kasseras. Enheter som inte längre ska användas bör raderas på innehåll eller återställas t.ex. till fabriksinställningar innan kassering.
- En process för anmälan av förlust eller om den mobila enheten har blivit manipulerad.
- En process för uppföljning av att organisationens interna regelverk och rutiner efterlevs. Uppföljning bör ske regelbundet och strukturerat genom interna kontroller.

Rekommendationer på krav som bör ställas på användarna

Fastställ i användarreglerna:

- Att användaren ska förpliktigas att ha fysisk kontroll över den mobila enheten och inte lämna den obevakad t.ex. på allmän plats, hotellrum eller synlig i bil.
- Hur användaren vid förlust av enhet ska anmäla detta till organisationen och om det bör göras skyndsamt.
- Att användaren ska lösenordskydda enheten så att den är låst när skärmsläckaren är aktiv. Det rekommenderas att undvika de mest uppenbara pinkoderna eller lösenorden t.ex. 1111, 1234 samt aktivering av tidsinställning för inaktivitet innan skärmsläckaren startas.
- Att användaren inte får manipulera den mobila enhetens grundfunktionalitet för att t.ex. få högre behörighet i enhetens interna filsystem.
- Att användaren ska undvika att exponera telefonnumret och jobbrelaterad epostadress i sammanhang som inte är arbetsrelaterade. Till exempel är det olämpligt att lägga upp telefonnummer och epostadress till användarens arbete på sociala medier som till exempel Facebook och Twitter om inte tjänsten kräver det.
- Att användaren bara använder den mobila enheten för internetsurfing i enlighet med organisationens regelverk.
- Att den mobila enheten i första hand ska anslutas mot kända trådlösa nätverk som har skydd i form av kryptering.
- Att användaren inte får byta SIM-kort i enheten för att använda den för privata ändamål som inte följer organisationens regelverk.
- Att användaren omedelbart ska byta lösenord på de tjänster som användaren tillåts att koppla upp emot om den mobila enheten blivit stulen eller förlorats.

Rekommendationer för utformning av tekniska skydd

- Tillåt endast skyddad uppkoppling och lagring för synkronisering av kalender, e-post, kontakter etc. samt implementera en säker uppkoppling (VPN) till organisationens interna resurser. Vid behov av extra skydd, överväg att implementera två-faktors-autentisering.
- Implementera kryptering för den mobila enheten om denna funktion bedöms nödvändig och de tekniska förutsättningarna hos den mobila enheten finns. Information som kan finnas lagrad och som kan behöva skydd i form av kryptering kan t.ex. utgöras av e-post, bilagor, dokument, fotografier, inloggningsuppgifter mm.
- Implementera kontrollfunktioner gällande kommunikationen som går till och från de synkroniseringspunkter den mobila enheten kan ansluta sig till. Applicera skydd mot skadlig kod där (e-postserver, interna nätverksresurser etc.).
- Implementera central styrning över organisationens mobila enheter, där uppdateringsstatus, efterlevnad av regelverk etc. kan följas och åtgärder kan vidtas vid t.ex. förlust av enhet.
- Implementera processer för att kunna hantera förlust av enhet så som distansradering av enhet och låsning av SIM-kort och IMEI-nummer hos operatör.
- Följ upp kostnaden för de mobila abonnemangen och ha beredskap för att reagera vid avvikelser.
- Implementera lösningar för detektering och skydd mot skadlig kod i den mobila enheten.
- Implementera processer för att återställa angripna mobila enheter till ett känt säkert läge, till exempel fabriksinställningar.
- Bevaka vilka uppdateringar som finns tillgängliga för de typer av mobila enheter och applikationer som organisationen använder.
- Implementera en rutin för att informera användarna om nya tillgängliga uppdateringar. Tiden för säkerhetsuppdateringar kan variera kraftigt för mobila enheter och sker betydligt mer sällan än för datorer.
- I de fall det är möjligt, begränsa åtkomsträttigheter på de mobila enheterna endast till behöriga användare.

När privatperson äger den mobila enheten

En mobil enhet som ägs av den anställde står helt utanför organisationens administrativa kontroll vilket innebär att organisationen har liten möjlighet att genomdriva regelverk och tekniska restriktioner. Den mobila enheten används sannolikt till många privata ändamål och är därmed exponerad på ett sätt som organisationen inte kan påverka annat än med en särskild överenskommelse. Möjligheten att följa upp huruvida den anställde följer överenskomna regler är begränsad. Rekommendationen är därför att som huvudregel inte tillåta privatägda mobila enheter att kopplas upp mot organisationens interna resurser och tjänster som e-post, kalender, lagringsytor för dokument etc.

Om man ändå gör det bör man beakta de rekommendationer som gäller för organisationsägda enheter men vara medveten om svårigheten att se till att reglerna följs. Ett beslut som tillåter privat uppkoppling mot organisationens resurser bör föregås av en grundlig riskanalys. Den anställde bör, för att få ta del av de tjänster som erbjuds av organisationen, även som privatperson förbinda sig att följa de regler som organisationen tar fram. God kunskap hos användaren om vilka risker som är förknippade med användningen är viktig.

En organisation bör även se över om det finns tekniska lösningar som kan underlätta i de fall privatägda mobila enheter får användas t.ex. applikationer som bygger på principen för tunna terminaler. Det finns till exempel lösningar där ingen information lagras på enheten utan informationen finns centralt och en användare kan ”titta” på informationen genom applikationen.

Avslutande reflektioner

Mobila enheter utgör idag ett viktigt arbetsredskap och är en stor informationskälla. Rätt använda kan smarta telefoner, surfplattor och andra mobila enheter med allt som denna nya teknik medför vara en viktig del i det dagliga arbetet utan att vara en säkerhetsrisk för en organisation och dess anställda.

Vägledningen för smarta telefoner, surfplattor och andra mobila enheter bör ses som ett stöd i det systematiska informationssäkerhetsarbetet i en organisation. Mer information och stöd för hur en organisation kan bedriva informationssäkerhetsarbete i sin verksamhet finns på www.informationssäkerhet.se.

Myndigheten för samhällsskydd och beredskap (MSB)
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ. nr MSB405 - juni 2012 ISBN 978-91-7383-234-2