eSam

Rapport

Klientsäkerhet

ES2025-26

oktober 2026

Innehållsförteckning

1. Inledning 4
   1.1 Syfte 4
   1.2 Målgrupp 4
   1.3 Avgränsning 4
   1.4 Medverkande 5
2. Klientsäkerhetskrav vid anskaffning 5
   2.1 Några aktuella regleringar kring en klienttjänst 5
   2.2 Säkerhetsrisker kopplade till tillverkningsland 7
   2.3 Krav på central klienthantering och policystyrning 9
   2.4 Krav på imagepåläggning 10
   2.5 Långsiktigt säkerhetsstöd 13
   2.6 Säkerhetskrav på användarstödet 13
   2.7 Säkerhetskrav vid avyttring av klienter 14
3. Klientinställningar 14
   3.1 Skyddsverktyg för klienter 14
   3.2 Windows Security baseline som grundkrav 15
   3.3 Linux Security baseline som grundkrav 16
   3.4 macOS Security baseline som grundkrav 18
   3.5 Lokal skanning på klienter 19
   3.6 Telemetri och diagnostikdata i Windows 23
   3.7 Lokal filsynkning och offline files 24
4. Alternativa klienter 24
   4.1 Lånedator 24
   4.2 Windows Subsystem for Linux 25
   4.3 Kioskdator 25
   4.4 Tunna klienter 26
5. Hårdvarukrav 26
   5.1 Fysisk säkerhet 27
   5.2 BIOS/UEFI-säkerhet 27
   5.3 Firmware-integritet 27
   5.4 Diskkryptering 28
   5.5 Kringutrustning och säkerhet 28
   5.6 Fjärrhantering på hårdvarunivå 30

6. Säkerhetsuppdateringar 30
6.1 Rekommenderad arbetsprocess 30
6.2 Windows 31
6.3 Linux 32
6.4 macOS 32
6.5 Säkerhetsuppdatering av övriga komponenter 33
7. Behörigheter 33
7.1 Lokala konton 33
7.2 Hantera lokala administratörsrättigheter på klienter 33
7.3 Olika konton för olika roller 34
8. Nätverk och klienter 34
8.1 Always-on VPN 34
8.2 Användaraktiverad VPN 35
8.3 Secure Access Service Edge (SASE) 36
8.4 Nolltillit och klientsäkerhet 36
8.5 Tvåfaktorsinloggning och smarta kort i myndigheters it-miljö 36
9. Mätning och övervakning 37
9.1 Mätning av klienter och behörigheter 37
9.2 Övervakning av klienter 38
10. Klienter utanför myndigheten 39
10.1 Klientsäkerhet utanför myndighetens nätverk 39
10.2 Privat användning av myndighetsdatorer 39
10.3 Klientsäkerhet vid arbete utomlands 40
11. Bilaga 1. Källor för omvärldsbevakning 41
12. Bilaga 2. Checklista för klientsäkerhet 42

1. Inledning

Klienterna är centrala för myndighetens säkerhet, eftersom nästan all myndighetsinformation hanteras i dem. De är också ett attraktivt mål för antagonister som söker sårbarheter.

När myndigheter använder molntjänster sker arbetet oftast från en och samma klient. Därför blir operativsystemens inbyggda funktioner för informationsinsamling en växande säkerhetsrisk, liksom den ökande mängden information som passerar myndighetens klienter. En enda exponerad dator kan ge insyn i myndighetens information, it-tjänster och infrastruktur.

Rapporten innehåller krav och praktiska råd som hjälper myndigheter att minska riskerna, skydda känslig information bättre och skapa en mer robust digital arbetsmiljö. Med klient avses i rapporten en fysisk enhet för verksamhetens användare, till exempel myndighetens standarddatorer, men inte program eller webbtjänster.

1.1 Syfte

Syftet med rapporten är att ge myndigheter råd om klientsäkerhet, både när klienttjänsten utkontrakteras och när myndigheten tar fram den själv, och löpande när tjänsten förvaltas eller byggs ut. En klienttjänst är ett tjänstepaket med den teknik, det stöd och den drift som behövs för myndighetens klienter. Myndigheter avgränsar klienttjänsten på olika sätt. Rapporten utgår från det som vanligtvis ingår i en standardklienttjänst: installation, flytt, tillägg, förnyelse och destruktion.

1.2 Målgrupp

Målgruppen för rapporten är beslutsfattare för myndighetens klienttjänst, klientarkitekter, anskaffningsprojekt, säkerhetsexperter, klientförvaltare och andra som berörs av klienttjänsten.

1.3 Avgränsning

Rapporten tar inte upp alla aspekter av klientsäkerhet. Arbetsgruppen har i stället valt ut de frågor som bedöms ge störst värde för medlemmarna. Rapporten behandlar inte klientkrav för myndigheter som arbetar med information som omfattas av säkerhetsskydd, EU-information eller Nato-information.

Säkerhetspolisen har tagit fram en vägledning[1] för upphandlingar där tjänsten omfattar säkerhetsskyddad information. Vägledningen kan även tillämpas på klienttjänster.

[1] Länk till Säkerhetspolisens sida (hämtad 2026-08-25): https://www.sakerhetspolisen.se/sakerhetsskydd/sakerhetsskyddsavtal-vid-upphandlingar-och-samarbeten.html

Rapporten ger stöd för att formulera krav på klientsäkerhet vid upphandling av en klienttjänst, men den är inte en fullständig upphandlingsguide. Hur stor del av klienttjänsten som upphandlas – hela, delar eller inget alls – varierar stort mellan myndigheter. Säkerhetskraven i rapporten ska därför inte ses som renodlade upphandlingskrav.

1.4 Medverkande

Rapporten har tagits fram av arbetsgruppen Cybersäkerhet.

2. Klientsäkerhetskrav vid anskaffning

Myndigheternas klienttjänster har förändrats över tid. Under en period var det vanligt att myndigheter upphandlade de kontorsnära klienttjänsterna, men i dag tar många myndigheter fram dem i egen regi. Klienttjänster för operativa klienter upphandlas mer sällan. Att myndigheter tar hem sin kontorsnära klienttjänst beror oftast på säkerhetsskäl, som beskrivs närmare i rapporten, och på att en egen klienttjänst ofta kan drivas till låg kostnad.

I det här kapitlet beskrivs de säkerhetskrav som myndigheten behöver ställa när den etablerar sin klienttjänst. Hur myndigheten utformar klienttjänsten avgör om kraven riktas till en extern leverantör eller till den egna it-organisationen. Den som vill veta mer om juridiken vid utkontraktering av it-tjänster kan läsa eSams *Vägledning Utkontraktering – sekretess och dataskydd*[2].

2.1 Några aktuella regleringar kring en klienttjänst

Det finns flera juridiska aspekter att beakta när det gäller myndigheters klienttjänster. Här redovisas några vanliga regleringar som är viktiga ur ett säkerhetsperspektiv. Översikten är inte heltäckande. Myndigheten behöver själv identifiera vilka lagar och föreskrifter som gäller för den egna klienttjänsten och bedöma hur tjänsten och anskaffningen uppfyller kraven.

Upphandlingstyp vid utkontraktering av en klienttjänst

Vid upphandling av klienttjänsten behöver myndigheten överväga hur tjänsten ska vara utformad. Leverantörens åtkomst till myndigheten bör styras genom tjänstens utformning, eftersom branschstandard är att leverantörer får full åtkomst till kundens it-miljö. Åtkomstens omfattning kan påverka bedömningen av upphandlingsform. Vissa myndigheter har bedömt att deras upphandling av klienttjänst faller under lagen om upphandling på försvars- och säkerhetsområdet (LUFS, 2011:1029), bland annat på grund av leverantörens samlade åtkomst till och insyn i eventuell känslig information i

[2] Länk till vägledningen (hämtad 2026-03-11): https://www.esamverka.se/publikationer/juridik/2025-04-15-es2023-06-vagledning-utkontraktering---sekretess-och-dataskydd.html

hela myndigheten. Oftast omfattas sådan anskaffning dock inom lagen om offentlig upphandling (LOU, 2016:1145), och inköp kan ske via ramavtal.

Vid upphandling kan lag (2023:560) om granskning av utländska direktinvesteringar samt MSBFS 2024:9, föreskrifter om vilka samhällsviktiga verksamheter som omfattas av lagen (2023:560) om granskning av utländska direktinvesteringar[3] kan göra det möjligt att vid upphandling ställa säkerhetskrav på leverantörers och tillverkares ursprungsland. Detta bör vägas samman med Säkerhetspolisens offentliga varningar till privat och offentlig sektor i Sverige[4]. En av eSams medlemmar har ställt ett sådant krav, och kravet har prövats i domstol (se avsnitt 2.2).

Föreskrifter med detaljerade krav på klienttjänsten

Myndigheter omfattas av flera krav på säkerhetsåtgärder i MSBFS 2020:7, *Föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter*[5]. Rapporten listar inte alla detaljerade säkerhetskrav, men exempel är krav på testförutsättningar, krav på programvara med leverantörsstöd, säkerhetsuppdateringar, kryptering och skydd av utrustning.

Myndigheter ska också följa ISO/IEC 27000-serien[6], och även där finns flera detaljerade säkerhetskrav som berör klienttjänsten, till exempel i standarden ISO/IEC 27002.

Ekonomistyrningsverkets föreskrifter och allmänna råd om myndigheters bokföring (ESVFA 2022:2[7]) och om intern styrning och kontroll (ESVFA 2022:8[8]) ställer krav på att utrustning och programvaror är korrekt inventerade, vilket även omfattar klienttjänsten.

2.1.1 Regler för klientsäkerhet är under förändring

När rapporten skrivs genomför Sverige flera EU-direktiv och anpassar svensk rätt till EU-förordningar som berör myndigheters klientsäkerhet. Ett exempel är NIS2-direktivet[9], som har genomförts genom cybersäkerhetslagen (2025:1506). Arbetsgruppen har ännu inte tolkat hur föreskrifterna till cybersäkerhetslagen och andra kommande regelverk påverkar myndigheterna, till exempel cyberresiliensförordningen, förordning (EU) 2024/2847 (Cyber Resilience Act, CRA)[10], och CER-direktivet om ökad

[3] Länk till föreskrift (hämtad 2026-02-26): https://www.mcf.se/sv/regler/gallande-regler/msbfs-20249/
[4] Länk till Säkerhetspolisens publika informationssida (hämtad 2025-09-11): https://www.sakerhetspolisen.se/ovriga-sidor/nyheter/nyheter/2024-02-21-allvarligt-omvarldslage-praglar-hoten-mot-sverige.html
[5] Länk till föreskrift (hämtad 2025-12-10): https://www.msb.se/sv/regler/gallande-regler/msbfs-20207/
[6] Länk till beskrivande artikel (hämtad 2025-12-10): https://www.sis.se/iso27001/dettariso27001/sakerhetsatgarder-enligt-iso-27000/
[7] Länk till föreskrift (hämtad 2025-12-10): https://www.esv.se/kunskapsstod-och-regler/regelverk/foreskrifter/esvfa-20222/
[8] Länk till föreskrift (hämtad 2025-12-10): https://www.esv.se/kunskapsstod-och-regler/regelverk/foreskrifter/esvfa-20228/
[9] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (Text av betydelse för EES)
[10] Länk till EU-förordningens sida (hämtad 2026-08-25): https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX%3A02024R2847-20241120

motståndskraft i samhällsviktig verksamhet[11]. Remissunderlagen tyder dock på att utvecklingen ligger i linje med rapportens innehåll.

Cybersäkerhetslagen kräver ett proportionerligt riskhanteringsarbete utifrån myndighetens klassning av sina informationsmängder. Det ska bedrivas som ett allriskarbete och dokumenteras, inklusive systemkonfiguration, skyddsåtgärder och förändringar i tjänsten över tid. Arbetsgruppen har i remissarbetet kunnat se att föreskrifterna till cybersäkerhetslagen och de uppdaterade föreskrifterna från Myndigheten för civilt försvar (föreskriftsarbete flyttades under sommaren 2026 till NCSC) sannolikt kommer att ställa krav på it-miljön, segmentering av klientnätverk, test och utveckling samt loggning och logghantering.

Krav kommer också att ställas på godkänd utrustning, kryptering och flerfaktorsautentisering vid inloggning i olika situationer och mot olika typer av tjänster. Dessutom kommer incidenter och betydande incidenter att definieras och hanteringen av dem att regleras i föreskrifter. Den här typen av krav finns oftast redan i dagens föreskrifter för myndigheter, men arbetsgruppen bedömer att kraven på klientsäkerheten kommer att skärpas något.

Myndigheten för civilt försvar kommer under 2026 att uppdatera sina föreskrifter med anledning av cybersäkerhetslagens bestämmelser. MSBFS 2020:7 kommer sannolikt att ersättas under 2026 av nya föreskrifter om säkerhetsåtgärder som meddelas med stöd av den nya lagstiftningen.

2.2 Säkerhetsrisker kopplade till tillverkningsland

Det kan i vissa fall finnas en säkerhetsrisk om både tillverkaren och datorleverantören kommer från samma land, eller om leverantören omfattas av lagkrav som till exempel ger en främmande stat full insyn i klienterna, informationen på dem eller själva installationsmiljön. Leverantören kan också omfattas av ett annat lands underrättelselagstiftning, som tvingar den att aktivt stödja underrättelsearbete i det landet.

Hot som byggs in redan i fabriken är svåra för myndigheter att hantera. Bland eSams medlemmar har det förekommit incidenter med skadlig kod i hårdvaran, riktad mot en dator som beställts till myndighetens generaldirektör eller någon annan nyckelperson. Hotet finns oavsett om myndigheten upphandlar klienttjänsten eller driver den i egen regi. De flesta datorer tillverkas i Kina, oavsett vilket land pc-leverantören kommer från. I dag kopplas datorbeställningen i många klienttjänster till en namngiven tjänsteperson hela vägen in i fabriken. I Kina finns lagkrav som innebär att företag i landet måste stödja underrättelsearbete, och andra lagkrav ger den kinesiska staten full åtkomst till och insyn i alla it-lösningar inom landets gränser. Säkerhetspolisen har dessutom under lång

[11] Länk till förklarande informationssida hos Myndigheten för civilt försvar (MCF) (hämtad 2026-08-25): https://www.mcf.se/sv/amnesomraden/beredskap-for-kris-och-krig/beredskap-for-aktorer/samhallsviktig-verksamhet/cer-direktivet/okad-motstandskraft-i-samhallsviktig-verksamhet-cer-direktivet/

tid varnat för Kinas omfattande industrispionage mot Sverige.[12] Varje myndighet måste själv bedöma hur stor risken är. Risken bör bedömas oavsett tillverkningsland och gäller alltså inte bara datorer som tillverkas i Kina.

Rekommenderade åtgärder

Myndigheter kan minska hotet genom att ställa upphandlingskrav på klienthårdvaran, till exempel genom att begränsa tillverkarens insyn i vilken tjänsteperson som ska få vilken dator. Mottagarnas namn kan anonymiseras som ett krav på klienttjänsten, så att endast myndigheten vet vilket installationsnummer som hör till vilken tjänsteperson. Myndigheten kan också ha möjlighet att i en upphandling ställa vissa krav på datorleverantörens nationella tillhörighet. En eSam-medlem har ställt ett sådant krav i en upphandling och fick 2025 bifall i kammarrätten[13], som bedömde att det inte hade visats att myndigheten i fråga hade överträtt någon upphandlingsrättslig bestämmelse eller de grundläggande upphandlingsrättsliga principerna genom att ställa det aktuella kravet. En bedömning måste dock göras i varje enskilt fall.

Ett sådant anskaffningskrav gör att myndigheten kan använda pc-leverantören som ett skyddande mellanled mot eventuell manipulation i fabriken, till exempel organiserad av kinesisk underrättelsetjänst, och mot tillverkare av potentiellt opålitliga drivrutiner och firmware. Detta kan ge ett extra skyddslager utöver de vanliga skyddsåtgärderna och kan också ge hårdvarutillverkaren något mindre insyn i myndighetens verksamhet via klienttjänsten.

Utifrån kammarrättens resonemang i domen skulle ett säkerhetskrav kunna utformas så här:

Anbudslämnaren ska vid upphandling av klienthårdvara säkerställa att ingen främmande makt, som av Säkerhetspolisen identifieras som ett hot mot Sverige, kan komma åt, manipulera, avlyssna eller på annat sätt påverka data, mjukvara eller hårdvara. Kravet består av två delar:

1. Anbudslämnare, tillverkare eller underleverantör får inte lyda under lagstiftning i ett land som Säkerhetspolisen har identifierat som ett hot om underrättelseverksamhet och säkerhetshotande verksamhet i och mot Sverige.
2. Om det bland ägarna till anbudslämnaren, tillverkaren eller underleverantören finns en representant[14] för ett land som Säkerhetspolisen har identifierat som ett hot om underrättelseverksamhet och säkerhetshotande verksamhet i och mot Sverige, får varken representantens ägarandel eller röstandel överstiga 10 procent. Detta gäller oavsett om ägandet är direkt eller indirekt genom ett eller flera led av bolag där en sådan representant finns bland ägarna.

[12] Länk till nyhet om Säkerhetspolisens varning kring Kinas spionage (hämtad 2025-12-10): https://www.svt.se/nyheter/inrikes/sapo-ett-hot-mot-sverige
[13] Kammarrätten i Stockholms dom 2025-10-08 i mål nr 4677-25. Artikel som analyserar domen: https://inkopsradet.se/ok-att-utestanga-svenska-bolag-med-utlandskt-agande/
[14] Med representant avses organisation, bolag eller person som står under direkt inflytande av land som identifierats av Säkerhetspolisen enligt ovan.

Upphandlingsreglerna för offentlig sektor håller också på att ändras när det gäller säkerhetskrav. Ett förslag till nya regler skulle göra det möjligt för myndigheter att utesluta företag från tredjeländer som saknar frihandelsavtal med EU. Myndigheter skulle då enklare än i dag kunna välja bort leverantörer som bedöms utgöra en risk för nationell säkerhet eller andra skyddsvärda intressen[15].

2.3 Krav på central klienthantering och policystyrning

Central klienthantering och policystyrning ska säkerställa att alla klienter inom myndigheten håller samma säkerhetsnivå, att systemen hålls uppdaterade och att endast godkända program används. Detta skapar en robust it-miljö och minskar risken för driftstörningar, informationsförlust och intrång. Myndigheten behöver säkerställa att klienttjänsten har dessa förmågor, antingen genom utkontraktering eller genom en egenproducerad tjänst.

Enligt MSBFS 2020:7, ESVFA 2022:2 och ESVFA 2022:8 ska myndigheter se till att inga klienter eller system används utan aktuella säkerhetsuppdateringar och att klienter och program är inventerade. Endast program som myndigheten har granskat och godkänt får användas i verksamheten.

Manuell kontroll av klienternas inställningar håller sällan tillräcklig kvalitet över tid. Central styrning bör därför vara ett krav på klienthanteringen.

Krav på centrala hanteringsverktyg

Myndigheten bör ställa krav på att all kommunikation mellan klienten och hanteringsplattformen är krypterad, att klienterna får säkerhetsuppdateringar automatiskt och i rätt tid och att endast behörig it-personal kan göra ändringar i systemen. Hanteringssystemet bör vara avskilt från andra system för att begränsa skadan vid ett eventuellt intrång. Vid policystyrning ska alla klienter följa samma grundkonfiguration för säkerhet, se kapitel 3 *Klientinställningar*. Att endast godkända program körs kan säkerställas med vitlistning av program och skript.

Säkerhetspolicys, till exempel för lösenord, skärmlås, kryptering och brandvägg, ska vara tvingande och får inte kunna kringgås av användarna. Alla ändringar, installationer och åtkomster ska loggas och kunna följas upp för att skapa spårbarhet.

2.3.1 Vanliga klientroller

Utöver standardklienten behöver myndigheter ofta särskilda klientroller för olika typer av användning. Syftet är att kombinera användbarhet och säkerhet och samtidigt minimera attackytan. Varje klientroll bör vara tydligt definierad och godkänd i myndighetens säkerhetsarkitektur. Myndigheten behöver besluta om en

[15] Regeringens information om ny bestämmelse efter genomförd utredning (hämtad 2026-02-26): https://www.regeringen.se/pressmeddelanden/2026/01/regeringen-gar-vidare-med-andrade-upphandlingsregler-for-att-skydda-sverige-fran-antagonistiska-stater/

säkerhetskonfiguration per roll och ställa den som krav på den som levererar klienttjänsten. Förslag på säkerhetskonfigurationer finns i kapitel 3.

Myndigheten bör begränsa antalet klientroller till ett fåtal väl motiverade varianter som kan styras och underhållas centralt.

Exempel på vanliga roller:

- Standardklient
  Grundnivån för de flesta användare, förkonfigurerad med myndighetens säkerhetspolicy, central uppdatering, full diskkryptering och applikationskontroll. Den ska användas som grund för alla andra roller.
- Administratörsklient (Privileged Access Workstation[16], PAW)
  Används av systemadministratörer och teknisk personal med förhöjda behörigheter. En isolerad miljö utan e-post, webbläsare eller andra användarprogram, med högsta skyddsnivå, strikt åtkomst, hårdvarubaserad kryptering och säker loggning.
- Utvecklarklient
  Anpassad för utvecklare som behöver till exempel kompilatorer, containerteknik eller virtualisering. Den ska vara separerad från produktionsmiljöer och aldrig ha administrativ åtkomst till myndighetens centrala system. Särskild nätverkssegmentering och kontinuerlig sårbarhetsskanning krävs.
- Operativ klient
  För användare som arbetar i fält eller i miljöer med begränsad uppkoppling. Klienten ska fungera säkert i begränsade nätverk, oftast utan internetåtkomst, och uppdateras automatiskt när den ansluts igen. Den behöver extra skydd mot fysisk åtkomst.
- Kiosk- eller lånedator
  En delad klient med tillfälliga användarsessioner. Den ska återställas automatiskt efter användning och ha strikt begränsad åtkomst till interna system. Lämplig för reception, testmiljöer och externa besökare (se även avsnitt 4.1 och 4.3).

Varje klientroll ska dokumenteras i myndighetens förvaltningsplan och omfattas av samma krav på spårbarhet, säkerhetsuppdateringar och revisionsbarhet som standardklienten.

2.4 Krav på imagepåläggning

Klienter installeras genom så kallad imagepåläggning. I den processen läggs de flesta av myndighetens centralt beslutade konfigurationsinställningar, uppdateringar och standardprogram in. Myndigheten kan upphandla den här delen av klienttjänsten eller utföra den i egen regi. Myndigheter bör kräva att imagepåläggning sker under strikt åtkomstkontroll, med säkra imagefiler, i ett krypterat nät och enligt fastställda

[16] Artikel som beskriver konceptet (hämtad 2025-12-10): https://learn.microsoft.com/sv-se/security/privileged-access-workstations/privileged-access-devices

säkerhetsprofiler. Om tjänsten är utkontrakterad behöver myndigheten granska leverantören, så att både sekretess och integritet kan garanteras i leveransen.

Ur ett säkerhetsperspektiv är det viktigt att bedöma om installationstjänsten (imagepåläggningen) får och bör ligga utanför myndighetens egen it-perimeter och om it-perimetern ska utökas till en utkontrakterad leverantörs it-miljö. Ett alternativ är att leverantören sätter upp installationstjänsten i myndighetens egna lokaler, vilket ger myndigheten bättre kontroll. En annan lösning är en så kallad installationsbur hos leverantören, där myndigheten styr och kontrollerar både nätverket (VPN) och den fysiska åtkomsten.

2.4.1 Hantering av installationsmedia och imagefiler

Imagefiler med operativsystem och standardprogram ska lagras säkert och skyddas mot manipulation, eftersom en angripare annars kan lägga in en sårbarhet redan vid installation eller ominstallation. Myndigheten bör kräva att endast behörig personal får skapa, ändra och distribuera imagefiler, och att filerna är versionshanterade och kontrolleras med kontrollsummor så att otillåtna ändringar upptäcks. Endast godkända och testade imageversioner får läggas på myndighetens skarpa datorer, det vill säga datorer som används utanför test- och pilotverksamhet.

2.4.2 Åtkomstkontroller

Om installationstjänsten är utkontrakterad måste leverantören ha stark åtkomstkontroll, till exempel flerfaktorsautentisering, för de system som används vid installationen. Driften av klienttjänsten bör ha rollbaserade behörigheter, så att teknikerna bara får åtkomst till de system de behöver. Uppgifter om vilken användare som får vilken dator, till exempel vilken dator generaldirektören har tilldelats, bör bara vara synliga för behöriga administratörsroller. Alla åtgärder ska loggas och loggarna ska skyddas mot manipulation.

2.4.3 Nätverks- och leveranssäkerhet

Imagepåläggning ska ske i ett skyddat nät, till exempel via VPN eller i ett dedikerat nätverkssegment. Om installationstjänsten är utkontrakterad måste nätverkstrafiken mellan myndigheten och leverantören vara krypterad. Inga obehöriga enheter får kunna ansluta till installationstjänsten eller till nätverksuttag hos leverantören, och åtkomststyrningen ska följa myndighetens krav.

2.4.4 Kontroll av leverantören

Leverantören ska vara skyldig att omedelbart rapportera avvikelser, incidenter och misstänkta intrång. Myndigheten ska ha rätt att granska leverantörens säkerhetsrutiner, till exempel genom revision och kontroll av säkerhetsklassning av personal. Båda delarna bör regleras i avtalet.

2.4.5 Härdning av operativsystem under installation

Installationerna ska följa myndighetens egna säkerhetsprofiler, till exempel baserade på CIS Benchmarks från Center for Internet Security (CIS)[17] eller på rekommendationer från Nationellt cybersäkerhetscenter (NCSC). Alla överenskomna säkerhetsinställningar ska om möjligt läggas in redan vid installationen. Själva installationstillfället är en svag länk i säkerhetskedjan och behöver skyddas. Efter installationen får inga standardlösenord eller otillåtna öppna portar finnas kvar, och säkerhetsuppdateringar ska ingå i imagefilen eller installeras direkt efteråt.

2.4.6 Spårbarhet och ansvar

Varje installation ska kunna spåras: vem som har beställt den, vem som har utfört den och vilken imageversion som har använts. Leverantören får inte kunna installera extra programvara eller bakdörrar utan behörighet. Klienttjänsten kan konfigureras så att alla förändringar loggas centralt och så att det är tydligt definierat vem som får göra ändringar. Hur kraven på spårbarhet följs upp avgör myndigheten utifrån hur klienttjänsten är definierad och levererad. Ansvaret vid incidenter ska regleras i avtal.

2.4.7 Leveranskedjesäkerhet

Myndigheten ska kräva att leverantören har tillräcklig kontroll över sin leverantörskedja, med spårbarhet, riskhantering, informationssäkerhet, säker personalhantering och rutiner för incidenter. Dessutom ska myndigheten ha rätt till insyn och revision, för att vid behov kunna säkerställa att kraven följs hela vägen ner i kedjan.

Leverantören ska verifiera att ingen obehörig firmware är installerad för att skydda mot attacker i leverantörskedjan.

Myndigheten kan till exempel ta ställning till följande krav på leverantören och underleverantörerna:

- Leverantören ska redovisa hela leverantörskedjan för hårdvara, mjukvara och tjänster.
- Kritiska underleverantörer ska identifieras och godkännas av myndigheten.
- Leverantören och dess underleverantörer ska följa etablerade säkerhetsstandarder, exempelvis ISO/IEC 27001[18].
- Åtkomst till system och data ska styras med principen ”minsta möjliga behörighet” och alltid loggas.

[17] Länk till förklaring av begreppet CIS Benchmarks (hämtad 2026-10-14): https://www.cyberquell.com/blog/cis-benchmarks-for-real-world-security-what-they-are-and-how-to-actually-use-them
[18] Länk till förklarande sida (hämtad 2026-08-25): https://en.wikipedia.org/wiki/ISO/IEC_27001

- Eventuell fjärråtkomst ska ske med flerfaktorsautentisering och via säkra förbindelser.
- Leverantören ska ha rutiner för kontinuitet och incidenthantering i hela leverantörskedjan.
- Myndigheten ska kunna kräva byte av underleverantör om allvarliga brister upptäcks.
- Det ska finnas en plan för leveranssäkerhet vid störningar, exempelvis geopolitiska risker eller cyberangrepp.

2.5 Långsiktigt säkerhetsstöd

Myndigheten behöver ställa krav på att leverantören tillhandahåller regelbundna och tillförlitliga säkerhetsuppdateringar så länge avtalet gäller. Det omfattar rättningar av kända sårbarheter, förbättringar av befintliga säkerhetsfunktioner och anpassningar till nya hot och branschstandarder under produktens hela livscykel.

2.6 Säkerhetskrav på användarstödet

Vissa myndigheter låter användarstödet ingå i klienttjänsten, medan andra hanterar det separat. På samma sätt utkontrakterar en del myndigheter användarstödet, medan andra driver det själva.

Användarstödet har ofta administrativa behörigheter med full åtkomst till myndighetens klienter och därmed stor möjlig insyn. Det är en viktig funktion i myndighetens dagliga verksamhet och behöver utföras på ett ansvarsfullt sätt.

Myndigheten kan till exempel ställa följande säkerhetskrav på användarstödet:

- Supportpersonalen ska ha personliga konton (inga delade inloggningar) och separata konton för administrativa uppgifter.
- Fjärradministration får endast utföras av godkänd personal, och användaren ska alltid meddelas när en fjärrstyrningssession pågår.
- Behörigheter ska ges enligt principen ”minsta möjliga behörighet” och ska tas bort direkt när behovet upphör.
- Flerfaktorsautentisering ska användas för åtkomst till myndighetens system och supportverktyg.
- All åtkomst och alla åtgärder i supportverktygen ska loggas.
- Loggar ska skyddas mot manipulation och regelbundet granskas.
- Supporten får bara ta del av känslig information i den utsträckning som är nödvändig för att lösa ärendet.
- Det ska vara förbjudet att kopiera, lagra eller sprida känslig information utanför godkända system.
- Sessioner får spelas in och skärmdumpar tas endast om myndigheten har godkänt det, i godkända stödverktyg och med rutiner för säker lagring och radering.

- Supportpersonal ska utbildas i dataskydd, sekretess och informationssäkerhet.
- Leverantören ska omedelbart rapportera incidenter eller avvikelser.

2.7 Säkerhetskrav vid avyttring av klienter

När klienter tas ur drift ska myndigheten säkerställa att all information raderas på ett sätt som förhindrar återställning. Avyttring av klienter är en kritisk del av livscykelhanteringen och omfattas av både säkerhets- och integritetskrav.

Krav och rekommendationer:

- Loggning och spårbarhet
  Avyttringen ska vara spårbar. Varje klient ska kunna följas i myndighetens inventariesystem från inköp till säker destruktion av informationen. Loggarna ska visa vem som har initierat och verifierat raderingen.
- Certifierad dataradering
  All lagrad data ska raderas med certifierade verktyg enligt standarder som NIST SP 800-88[19] eller motsvarande. För särskilt känslig information kan fysisk destruktion krävas. Leverantören ska kunna visa raderingsintyg.
- Säker transport och lagring
  Klienter som väntar på radering eller återvinning ska förvaras i låsta utrymmen med kontrollerad åtkomst. Transport till extern part ska ske med krypterad lagring (om enheten fortfarande är aktiv) eller med en obruten fysisk säkerhetskedja.

En tydlig avyttringsrutin minskar risken för dataläckage, obehörig återanvändning och förlust av myndighetsinformation.

3. Klientinställningar

Säkerhetsåtgärderna i det här kapitlet bör vara desamma oavsett operativsystem, så långt det är tekniskt möjligt.

3.1 Skyddsverktyg för klienter

De flesta angrepp börjar hos en enskild användare, genom nätfiske, stulna inloggningsuppgifter eller sårbarheter. Traditionella antivirusprogram räcker inte, eftersom angripare ofta använder legitima verktyg för att röra sig obemärkt i nätverket. Endpoint Detection and Response (EDR)[20] ger insyn i vad som händer på varje klient och gör det möjligt att snabbt isolera, stoppa och utreda ett angrepp. Extended Detection and Response (XDR)[21] kopplar dessutom ihop signaler från klienter, e-post, identiteter, nätverk och moln till en samlad bild.

Cybersäkerhetslagen, som trädde i kraft den 15 januari 2026, innebär bland annat skärpta krav, ett tydligare ansvar för ledningen och en skyldighet att rapportera betydande

[19] Artikel som förklarar standarden (hämtad 2025-12-10): https://blancco.com/resources/blog-what-is-nist-800-88-media-sanitization/
[20] Länk till förklarande sida (hämtad 2026-08-25): https://en.wikipedia.org/wiki/Endpoint_detection_and_response
[21] Länk till förklaring av begreppet (hämtad 2026-08-25): https://en.wikipedia.org/wiki/Extended_detection_and_response

incidenter. Därför ser många myndigheter det som avgörande att ha en EDR- eller XDR-förmåga i sin it-miljö.

Att tänka på vid införandet

- Data och lagring: Var hamnar telemetrin? Bedöm sekretess, dataskydd (GDPR) och risken för åtkomst från tredjeland.
- Säkerhetsskydd: Säkerhetsskyddsanalys och säkerhetsskyddsavtal kan krävas.
- Leverantörsberoende: Agenten körs med höga behörigheter, så granska leverantörens uppdateringsrutiner och avtalsvillkor.
- Förmåga: Någon måste agera på larmen, antingen ett eget Security Operations Center (SOC) eller en hanterad tjänst.
- Styrning: Bestäm vem som får isolera klienter och se insamlat data, och informera medarbetarna.

EDR och XDR kompletterar grundskyddet – till exempel patchning, flerfaktorsautentisering, behörighetsstyrning och säkerhetskopiering – men ersätter det inte.

3.2 Windows Security baseline som grundkrav

Myndigheten bör kräva att alla Windows-klienter konfigureras enligt Microsofts Windows Security Baselines[22] eller motsvarande, kompletterade med egna härdningskrav. Viktiga områden är stark autentisering (till exempel flerfaktorsautentisering eller Windows Hello[23]), kryptering (till exempel BitLocker[24]), patchning, applikationskontroll, skydd mot skadlig kod, avstängning av osäkra tjänster samt central loggning och revision. Nedan ges exempel inom varje område. Myndigheten behöver själv bedöma om exemplen räcker för de egna behoven.

1. Leverantörens rekommendationer: Microsoft Security Baselines

- Baselines bygger på Group Policy[25] eller MDM[26]-profiler och ger en säker grundnivå för bland annat kontohantering, nätverk, tjänster och applikationer.
- Eventuella avvikelser från baselinen ska dokumenteras och godkännas av myndigheten.

2. Autentisering och åtkomst

- Flerfaktorsautentisering (MFA)[27] ska användas för alla administratörskonton.

[22] Länk till stödverktyg där kunden kan utvärdera hur väl man möter säkerhetsgrundkraven från leverantör (hämtad 2025-12-10): https://www.microsoft.com/en-us/download/details.aspx?id=55319
[23] Artikel som förklarar tekniken Windows Hello (hämtad 2025-12-10): https://www.microsoft.com/en-us/windows/tips/windows-hello
[24] Länk till sida som förklarar tekniken (hämtad 2026-08-25): https://support.microsoft.com/sv-se/windows/security/encryption/bitlocker-overview
[25] Länk som beskriver konceptet hos Microsoft (hämtad 2026-08-25): https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-overview
[26] Länk som förklarar begreppet (hämtad 2026-08-25): https://sv.wikipedia.org/wiki/Mobil_enhetshantering
[27] Länk som förklarar begreppet (hämtad 2026-08-25): https://sv.wikipedia.org/wiki/Multifaktorautentisering

- Slutanvändare ska använda Windows Hello for Business eller annan stark autentisering i stället för lösenord.
- Administratörer ska använda Privileged Access Workstations (PAW)[28] eller motsvarande skyddade miljöer.
- Lokala administratörskonton ska inaktiveras eller skyddas med Local Administrator Password Solution (LAPS)[29].

3. Kryptering

- Som huvudregel bör myndighetens information inte lagras lokalt på klienterna. Åtminstone originalet bör lagras centralt på en godkänd plats, och lokal synkronisering bör bara tillåtas för information som inte är känslig (se avsnitt 3.7).
- All data på klienten ska krypteras med BitLocker (med TPM[30] 2.0 eller senare) eller motsvarande krypteringslösning.
- Återställningsnycklar ska säkerhetskopieras i en central och skyddad lösning, till exempel Active Directory eller motsvarande.

4. Applikations- och nätverkssäkerhet

- Skydd mot skadlig kod, till exempel antivirus eller EDR, ska vara aktiverat.
- Applikationskontroll, till exempel AppLocker eller Windows Defender Application Control, eller motsvarande ska begränsa körningen av otillåtna program.
- SmartScreen-filtret ska vara aktiverat både i Edge och på systemnivå.
- Brandväggen ska alltid vara aktiverad, och en policy ska förhindra att användaren stänger av den.
- Loggar ska skickas till central logghantering (till exempel syslog eller SIEM).

5. Härdning av system och tjänster

- Sårbara, onödiga och föråldrade tjänster, protokoll och portar ska inaktiveras, till exempel SMBv1 och gamla TLS-versioner.
- Automatisk körning av externa medier (autorun) ska blockeras.
- Klienten ska, utöver Microsofts baseline, följa myndighetens egen härdningsguide baserad på CIS Benchmarks eller NCSC:s rekommendationer.

3.3 Linux Security baseline som grundkrav

För Linux-klienter bör myndigheter kräva en baseline baserad på CIS Benchmarks för den aktuella distributionen. Viktiga områden är stark autentisering (MFA, SSH-nycklar och ingen root-inloggning), full diskkryptering, automatiska säkerhetsuppdateringar, applikationskontroll (AppArmor eller SELinux), brandvägg och loggning med auditd. Efterlevnaden av baselinen ska kunna verifieras och följas

[28] Länk som förklarar begreppet (hämtad 2026-08-25): https://www.ncsc.gov.uk/collection/principles-for-secure-paws
[29] Länk som beskriver konceptet hos Microsoft (hämtad 2026-08-25): https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-overview
[30] Länk som förklarar begreppet (hämtad 2026-08-25): https://en.wikipedia.org/wiki/Trusted_Platform_Module

upp centralt. Vissa centrala Linux-inställningar går också att styra med MDM-verktyg.

1. Utgångspunkt: standardiserad baseline

- Klienter ska konfigureras enligt en erkänd härdningsguide, exempelvis CIS Benchmark för vald Linux-distribution (Ubuntu, RHEL, Debian med flera).
- Eventuella avvikelser från baseline ska dokumenteras och godkännas av myndigheten.

2. Autentisering och åtkomst

- Flerfaktorsautentisering (MFA) ska användas för alla administratörskonton, via PAM-moduler eller federerad inloggning.
- SSH-nycklar[31] ska användas i stället för lösenord, och lösenordsinloggning via SSH ska vara avstängd.
- Alla administrativa rättigheter ska ges via sudo (inga direkta root-inloggningar).
- Principen ”minsta möjliga behörighet” ska tillämpas.

3. Kryptering

- Diskar ska krypteras med LUKS[32]/dm-crypt eller motsvarande.
- Swap-partitionen[33] ska vara krypterad. På känsliga system kan swap i stället inaktiveras.
- Hemkataloger och känsliga kataloger (exempelvis /etc/ssl, /var/log) bör krypteras eller skyddas med strikta behörigheter.

4. Uppdateringar och patchhantering

- Säkerhetsuppdateringar ska ske automatiskt (exempelvis med unattended-upgrades i Ubuntu eller dnf-automatic i RHEL).
- Hantering och rapportering ska ske centralt via konfigurationsverktyg, till exempel Ansible, Puppet, Landscape eller Red Hat Satellite.
- Kritiska säkerhetspatchar ska införas enligt rekommendationerna i kapitel 6 *Säkerhetsuppdateringar*.

5. Applikations- och nätverkssäkerhet

- AppArmor (Ubuntu/Debian) eller SELinux (RHEL/Fedora) ska vara aktiverat.
- Endast godkända program får installeras, och paket ska hämtas från betrodda paketkällor.
- Brandvägg (iptables/nftables, firewalld eller ufw) ska alltid vara aktiverad.

[31] Länk till beskrivande artikel (hämtad 2025-12-10): https://dbwebb.se/guide/kom-igang-med-ssh/kom-igang-med-ssh-nycklar
[32] Länk till beskrivande artikel (hämtad 2025-12-10): https://gitlab.com/cryptsetup/cryptsetup/-/blob/main/README.md
[33] Länk till beskrivande artikel (hämtad 2025-12-10): https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/7/html/storage_administration_guide/ch-swapspace

- Inga onödiga tjänster eller portar ska vara aktiva.

6. Systemhärdning

- Auditd eller motsvarande loggningsramverk ska vara aktiverat för att registrera säkerhetshändelser.
- Administrativa sessioner ska loggas ut automatiskt efter en viss tids inaktivitet (idle timeout).
- Onödiga kärnmoduler, till exempel för gamla nätverksprotokoll, ska inaktiveras.
- USB-åtkomst kan behöva begränsas på känsliga system.
- Konton ska låsas automatiskt efter upprepade misslyckade inloggningsförsök.

7. Spårbarhet och revision

- Loggar ska skickas till central logghantering (till exempel syslog eller SIEM).
- Efterlevnaden av baselinen ska kontrolleras regelbundet med verktyg som OpenSCAP eller CIS-CAT.
- Myndigheten ska kunna genomföra revisioner av konfigurationen.

3.4 macOS Security baseline som grundkrav

Myndigheten ska utgå från CIS Apple macOS Benchmark från Center for Internet Security, som innehåller detaljerade säkerhetsrekommendationer för systeminställningar i macOS. Efterlevnaden av baselinen ska kunna verifieras och följas upp centralt.

1. Utgångspunkt: standardiserad baseline

- Använd också macOS Security Compliance Project[34] som stöd för lämpliga säkerhetsinställningar.

2. Autentisering och åtkomst

- Starka lösenord eller inloggning med smart kort eller via en identitetsleverantör (IdP) ska krävas, och skärmlåset ska aktiveras automatiskt efter en kort tids inaktivitet.
- Ingen användare ska vara administratör. Administrativa rättigheter ska bara ges tillfälligt via MDM (Mobile Device Management).

3. Kryptering

- Diskkrypteringen FileVault ska alltid vara aktiverad, så att data skyddas om enheten förloras.

[34] Länk till Apples informationssida (hämtad 2026-02-26): https://support.apple.com/sv-se/guide/certifications/apc322685bb2/web

4. Uppdateringar och patchhantering

- Alla klienter ska vara registrerade i en MDM-lösning, så att efterlevnaden av policys kan säkerställas.
- Operativsystem och appar ska uppdateras automatiskt via MDM.
- Kritiska säkerhetspatchar ska införas enligt rekommendationerna i kapitel 6 *Säkerhetsuppdateringar*.

5. Applikations- och nätverkssäkerhet

- Endast godkända appar ska kunna installeras, via App Store eller MDM. Gatekeeper ska vara aktiverat så att bara betrodda program från App Store eller verifierade utvecklare kan köras, och användarna ska inte kunna stänga av det. Apples inbyggda skydd mot skadlig kod, XProtect och MRT, ska vara aktiverat och uppdaterat.
- Den inbyggda brandväggen ska vara aktiverad och konfigurerad. Delningstjänster, till exempel fildelning och fjärrinloggning, ska vara avstängda som standard.

6. Systemhärdning

- System Integrity Protection (SIP) ska vara aktiverat för att skydda systemfilerna.

7. Spårbarhet och revision

- Systemloggar ska vara aktiverade, och säkerhetsrelaterade händelser ska skickas till central logghantering.

3.5 Lokal skanning på klienter

De vanligaste operativsystemen (Android, iOS, macOS och Windows) har i dag inbyggda funktioner för lokal skanning av hur användaren använder klienten. Funktionerna har utvecklats under lång tid och använder numera avancerad lokal AI och särskilda beräkningschip i datorer och mobiler.

Skanningsfunktionen kan användas för att kartlägga användarens beteende och arbete. Den kan vara till nytta, till exempel genom att hjälpa användaren att minnas tidigare arbete eller viktiga möten, men innebär också en risk för otillåten delning av känslig myndighetsinformation. I ett större perspektiv medför den även att all personal kartläggs, vilket kan kräva en prövning enligt

integritetsskyddslagstiftningen. Problemet gäller inte bara offentliganställda utan även yrkesgrupper som politiker, journalister och forskare – alla som hanterar känslig eller hemlig information.

Eftersom lokal skanning som regel är aktiverad från början måste myndigheten aktivt välja bort funktionen. Detta kan skapa säkerhetsproblem om den centrala styrningen, till exempel via GPO:er, inte fungerar på alla klienter.

3.5.1 Windows Recall

Windows Recall[35] är en funktion som spelar in och analyserar användarens aktiviteter. Den kan användas för att svara på frågor som ”Vad arbetade jag med förra veckan och med vilka kollegor?”

För myndigheter innebär Windows Recall en risk. Funktionen kan lagra och analysera känslig information lokalt och i vissa fall dela den med leverantören. Koden går inte att ta bort från datorerna, även om funktionen stängs av, vilket i sig är en sårbarhet.

Det är inte bara ett problem att Windows Recall kan dela information med leverantören. Minst lika problematiskt är att den analyserade informationen lagras lokalt, där en antagonist kan dra nytta av den[36].

Microsoft utvecklar flera lokala AI-förmågor i Windows. Myndigheter bör också följa utvecklingen av Model Context Protocol (MCP)[37], en ny standard som låter AI-agenter samla in information och styra Windows-klienter.

3.5.2 Begränsad kontroll över Windows Recall

Windows-administratörer kan delvis konfigurera Windows Recall och definiera filter för känslig information och undantag. Filtret definieras dock av leverantören och inte av myndigheten. Det är alltså inte anpassat till myndighetens bedömning av vilken information som är känslig, och kritik har framförts mot att det inte tar tillräcklig hänsyn till nationella förhållanden, till exempel svenska personnummer eller vissa hälsodata. Filtret fungerar dessutom bara i produkter som Microsoft pekar ut, till exempel Edge och Microsoft Office. Myndigheter som använder andra webbläsare, till exempel Firefox, får därför inget skydd mot insyn. Tidiga

[35] Länk till förklaring av lösningen (hämtad 2026-08-25): https://en.wikipedia.org/wiki/Windows_Recall
[36] Artikel om faran att Windows Recall hackas (hämtad 2025-05-12): https://www.inc.com/kit-eaton/microsofts-ai-recall-feature-can-be-easily-hacked-security-researcher-finds.html
[37] Artikel om denna teknikutveckling från Microsoft (hämtad 2025-12-10): https://www.theregister.com/2025/12/08/microsoft_windows_insiders_agentic_future/

rapporter[38] och senare säkerhetstester[39] visar också att filtret inte har fungerat som utlovat. Viss egen mer anpassad filtering för myndighetens känsliga informationsmängder kan kunder som använder M365 molntjänsten och funktionen Microsoft Purview[40] skapa. Myndigheter som överväger denna tekniska lösning bör utreda lämpligheten då Microsoft Purview i sig är en molntjänst som är tänkt att lista kunden känsliga informationsmängder (samt var den är lagrad hos myndigheten) och därmed kan myndigheten dela otillåten information med leverantören genom denna tjänst.

Enligt en rapport[41] har Microsoft efter kritik från användare diskuterat att stoppa nya planerade integrationer av Copilot i Windows. Befintliga Copilot-integrationer, till exempel i det inbyggda programmet Anteckningar, finns dock kvar.

3.5.3 Apple Intelligence

Apple Intelligence är Apples lokala AI-lösning och motsvarar Microsofts Copilot och Windows Recall. Den finns i alla Apples klientoperativsystem och har som standard tillgång till klientens innehåll (kunddata). Enligt Apple sorterar lösningen ut känslig information, och till exempel personuppgifter anonymiseras innan data skickas över nätverket till Apples datacenter. Hur detta fungerar för myndigheters känsliga informationsmängder är oklart. Apple Intelligence är en inbyggd del av operativsystemet. Den går att stänga av eller konfigurera per program och operativsystemsfunktion, men inte att avinstallera.

3.5.4 Android Gemini

Gemini är Googles motsvarighet till Microsofts och Apples lokala AI-lösningar. Gemini byggs in i Googles olika klientoperativsystem och är, precis som hos Apple och Microsoft, en så kallad opt-out-lösning. Kunden måste alltså aktivt stänga av funktionen, och den går inte att avinstallera.

3.5.5 TV apparater och lokal skanning

En liknande utveckling har skett för tv-apparater, där en amerikansk delstat har stämt fem stora tv-tillverkare för spionage[42]. Det är standard bland TV tillverkare att samla in stora mängder information från miljön TV apparat befinner sig i, nätverket den är uppkopplad i och användarens nyttjande av TVn. I denna förändring av TV apparater finns en påtvingande utrullning av lokal AI lösning (bland annat MS copilot). För

[38] Artikel som beskriver brister i känslighetsfiltret i Windows Recall (hämtad 2025-05-12): https://www.tomshardware.com/software/windows/microsoft-recall-screenshots-credit-cards-and-social-security-numbers-even-with-the-sensitive-information-filter-enabled
[39] Artikel om nya säkerhetstester av Windows Recall (hämtad 2025-08-19): https://www.theregister.com/2025/08/01/microsoft_recall_captures_credit_card_info/
[40] Länk till funktionen Microsoft Purview (hämtad 2025-08-25): https://www.microsoft.com/sv-se/security/business/microsoft-purview
[41] Länk till artikel (hämtad 2026-02-26): https://wonderfulengineering.com/microsoft-quietly-pulls-back-on-windows-11-ai-after-user-backlash/
[42] Länk till information från delstatens informationssida (hämtad 2026-02-26): https://www.texasattorneygeneral.gov/news/releases/attorney-general-paxton-sues-five-major-tv-companies-including-some-ties-ccp-spying-texans

myndigheter som använder TV apparater i konferensrum är detta en säkerhetsfråga att utreda och hantera.

3.5.6 Mobiltelefoner och lokal skanning

Mobiltelefoner ingår i ekosystem där hårdvaran delvis finansieras genom att användardata samlas in. Till exempel används positionsdata från mobilens GPS-funktion för att skapa aktuella trafikprognoser: om en mobilanvändare hamnar i en bilkö loggas det, och de stora kartapparna varnar andra bilförare för köbildning i området. I priset för en mobiltelefon ingår alltså underförstått att tredje part får tjäna pengar på viss kundinformation.

Varken Android eller iOS ger ett fullständigt skydd mot denna insyn. Även om åtkomsten till informationen ibland kan begränsas med mobilens säkerhetsinställningar kan tillverkaren själv oftast komma åt informationen. Det gör även mobila sandbox-lösningar sårbara.

Detta skapar särskilda risker för myndigheter som hanterar känslig information i sina mobiltelefoner. Det finns också nya exempel på att trafik med totalsträckskryptering (end-to-end encryption, E2EE) medvetet spelas in genom lokal skanning i mobiltelefoner[43].

3.5.7 Mobila operativsystem som minimerar lokal skanning

Det finns flera mobila operativsystem som ersätter tillverkarens operativsystem och därmed den inbyggda insynen i hur mobilen används. Flera Linux-versioner har tagits fram särskilt för mobiler, med starkare säkerhet och med mindre eller ingen oönskad informationsinsamling. Flera myndigheter använder olika öppna Android-varianter för att minska den lokala skanningen. Arbetsgruppen har identifierat följande exempel, som inte ska ses som rekommendationer:

- Sailfish OS (https://sailfishos.org/): finsk lösning som utvecklas av bolaget Jolla. Jolla tillverkar även annan hård- och mjukvara med nordiska myndigheter som huvudsaklig målgrupp.
- Plasma Mobile (https://plasma-mobile.org/): tysk lösning
- /e/OS (https://e.foundation/e-os/): fransk lösning
- Ubuntu Touch (https://www.ubuntu-touch.io/): tysk lösning
- iodéOS (https://iode.tech/iodeos/): fransk lösning
- CopperheadOS (https://copperhead.co/android/): kanadensisk lösning
- GrapheneOS (https://grapheneos.org/): kanadensisk lösning

[43] Artikel som beskriver hur flera it-leverantörer spelar in information via klienten (hämtad 2025-09-11): https://www.forbes.com/sites/zakdoffman/2025/07/09/google-and-microsoft-start-reading-your-private-texts-act-now/

3.5.8 Rekommenderade åtgärder

- Windows Recall: Stäng av funktionen eller begränsa den så långt det går. Verifiera med trafikmätningar att ingen känslig information skickas vidare.
- Windows-klienter: Konfigurera centralt (via GPO) att alla nätverksanslutningar, till exempel trådlösa, mobila och trådbundna, behandlas som anslutningar med datapriser (metered connections). Det minskar mängden data som samlas in från klienten.
- Copilot: Utvärdera riskerna innan funktionen aktiveras. Testa och granska för att säkerställa att information inte delas otillåtet.
- Apple Intelligence: Stäng av funktionen eller konfigurera den per program och operativsystemsfunktion genom central hantering av Apple-klienterna.
- Gemini: Stäng av funktionen eller konfigurera den per program och operativsystemsfunktion genom central hantering av Android-klienterna.
- Lokala assistenter: Begränsa också den insyn som assistenter som Google Assistant, Siri och Cortana har i myndighetens information på klienterna.
- Linux: Överväg Linux som alternativt operativsystem för särskilt känsliga roller i myndigheten. Kontrollera dock att distributionen inte innehåller egna funktioner för lokal skanning eller tredjepartsprogram som skannar användaren på ett oönskat sätt.

3.6 Telemetri och diagnostikdata i Windows

Telemetri (fjärrmätning) och diagnostikdata (felsökningsdata) har länge varit en fråga som myndigheter behöver hantera, inte bara för klienter utan för all it-utrustning och alla program och tjänster. Microsoft har en informationssida[44] där kunderna kan läsa om hur känslig information och personuppgifter hanteras. Sidan uppdateras löpande och bör bevakas av myndigheter som använder Microsofts produkter och tjänster. Där beskrivs bland annat vad Windows, Copilot och Edge samlar in med olika inställningar. Det finns också en särskild guide[45] för Windows.

Rekommenderade åtgärder

Utred i samverkan med myndighetens dataskyddsombud vilken telemetri som är tillåten och vilken som inte är det. Granska om data innehåller uppgifter som omfattas av sekretess eller som kan kartlägga eller identifiera personer, och dokumentera alla beslut i en säkerhetsbedömning. Om myndigheten har flera klientroller med olika säkerhetsnivå kan olika filter för telemetri och diagnostikdata vara motiverade.

Begränsa insamlingen med centrala, tvingande inställningar, till exempel via GPO:er. Sätt telemetrinivån till ”Säkerhet” (finns endast i Enterprise-utgåvorna) och stäng av insamling av användardata där det är möjligt. Om det är tillåtet kan

[44] Länk till Microsofts informationssida (hämtad 2026-08-25): https://www.microsoft.com/en-us/privacy/privacystatement
[45] Länk till denna guide (hämtad 2026-08-25): https://learn.microsoft.com/en-us/windows/privacy/windows-privacy-compliance-guide

myndigheten också blockera kända telemetriadresser hos Microsoft med en avancerad brandväggskonfiguration. Kryptera all lagrad data, även lokala loggar och telemetrifiler.

Övervaka nätverkstrafiken för att upptäcka oönskad datadelning och säkerställ att loggningen inte leder till oavsiktliga läckor. Verifiera inställningarna i klienttestningen, både generellt och särskilt för roller med känsliga arbetsuppgifter.

3.7 Lokal filsynkning och offline files

Lokal filsynkning och funktionen Offline Files i operativsystem är användbara för att möjliggöra arbete utan internetuppkoppling, men innebär samtidigt säkerhetsrisker. Lokalt synkroniserade filer kan innehålla sekretessbelagd eller skyddsvärd information och blir då svårare att skydda enligt myndighetens centrala säkerhetskrav.

Arbetsgruppen rekommenderar att Offline Files bara används för dokument som inte innehåller känslig information. Myndigheten behöver utreda vilka grundläggande säkerhetskrav som gäller och om vissa roller behöver särskilda krav på lokal lagring och synkronisering. Centralt styrda policys bör se till att synkronisering bara sker mot godkända myndighetsresurser, och synkroniseringen bör loggas centralt. Lokalt lagrade filer ska alltid vara krypterade, till exempel med BitLocker, FileVault eller LUKS. Om molnlagring används, till exempel Dropbox, Google Drive, OneDrive eller Nextcloud, ska myndigheten dokumentera och godkänna vilken information som får synkroniseras.

4. Alternativa klienter

Det här kapitlet handlar om klienter som vanligtvis skiljer sig från standardklienten: lånedatorer, Windows Subsystem for Linux, kioskdatorer och tunna klienter. Fristående datorer används till exempel när vissa arbetsmoment eller informationsmängder behöver isoleras från myndighetens ordinarie nätverk.

4.1 Lånedator

Lånedatorer lånas ofta ut till tillfälliga användare, externa konsulter eller besökare. De bör ha en egen klientroll med kraftigt begränsade behörigheter (se avsnitt 2.3.1) och köras i nedlåst läge eller som tunna klienter. Alla sessioner ska raderas automatiskt efter användning. Lånedatorer får inte ha lokal lagring eller tillgång till interna system utöver det som är absolut nödvändigt. Om användaren behöver internetåtkomst ska ett separat gästnät användas. Av säkerhetsskäl bör myndigheten också överväga att inte ansluta lånedatorerna till domänen.

4.2 Windows Subsystem for Linux

Windows Subsystem for Linux (WSL)[46] är en funktion i Windows 11 som gör det möjligt att köra en fullständig Linux-kärna direkt i Windows. Det kan vara en fördel för till exempel utvecklare som behöver en Linux-miljö. Med WSL kan användaren utnyttja operativsystemsfunktioner som kräver Linux, köra Linux-program och skript, läsa filer i Linux-filsystem och använda grafikkortet för lokala AI-lösningar i Linux – utan att behöva en extra dator med Linux installerat. Ur ett säkerhetsperspektiv kan WSL dock bli ett problem för myndigheten.

Rekommendation

Myndighetens behov av Linux kan lösas tekniskt på flera sätt. WSL kan vara den lösning som ger störst säkerhetsproblem, om myndigheten inte har tillräcklig kontroll över miljön. Andra alternativ är en virtuell Linux-klient som delas av användare med tillfälliga behov, vilket kräver att myndigheten har förmåga till klientvirtualisering, eller en särskild Linux-dator för användare med permanenta behov.

4.3 Kioskdator

Kioskdatorer är kraftigt nedlåsta klienter som oftast står i allmänna utrymmen hos myndigheten. Exempel är självbetjäningsterminaler för e-tjänster i receptioner och kundtorg, informationsstationer på bibliotek, utställningar och i väntrum, terminaler för tidsbokning, utbildningssystem eller interna blanketter samt gästarbetsstationer för kortvariga besökare och externa parter. Rätt utformade kan kioskdatorer göra digitala tjänster mer tillgängliga utan att säkerheten försämras. De innebär dock ett hot, dels eftersom de kan användas som plattform för attacker mot myndigheten (de har ofta åtkomst till myndighetens nätverk), dels eftersom de ofta saknar god övervakning och tillräcklig spårbarhet. Kioskdatorer ska därför hanteras som särskilda säkerhetsobjekt, vara centralt hanterade och omfattas av samma krav på inventering, uppdatering och kontroll som myndighetens övriga klienter.

Arbetsgruppen rekommenderar tre huvudprinciper för kioskdatorer:

1. Minsta möjliga funktion – datorn ska endast kunna utföra det som är absolut nödvändigt för sitt ändamål.

2. Ingen kvarvarande information – när en användarsession avslutas får ingen data, inloggning eller historik sparas lokalt.

3. Fullständig isolering – kioskdatorn ska vara tekniskt och nätverksmässigt isolerad från myndighetens övriga system.

[46] Länk till förklaring av lösningen (hämtad 2026-08-25): https://learn.microsoft.com/en-us/windows/wsl/about

4.4 Tunna klienter

Tunna klienter kan ge högre säkerhet för en myndighet, men det beror på hur de används och i vilket sammanhang. Rätt utformade kan de kraftigt minska riskerna för dataläckage, manipulation och förlust av information. Samtidigt kräver de en tydlig arkitektur och robust servermiljö.

4.4.1 Vad är en tunn klient?

En tunn klient är en dator eller terminal utan egen lokal lagring av information. Den används enbart för att visa och interagera med en central servermiljö där all bearbetning och lagring sker. Användaren arbetar alltså i en fjärrskrivbordsmiljö (till exempel Citrix, Microsoft AVD eller annan VDI-lösning[47]), medan klienten i sig bara är ett gränssnitt.

4.4.2 Säkerhetsfördelar med tunna klienter

- Minskad risk för informationsförlust
  Eftersom ingen information lagras på den lokala enheten leder stöld eller förlust av klienten inte till att information hamnar i fel händer. Kryptering och central åtkomstkontroll räcker för att skydda informationen.
- Central säkerhetskontroll
  Alla uppdateringar, patchar och behörigheter hanteras i servermiljön. Detta minskar risken att en enskild användare missar en säkerhetsuppdatering eller installerar otillåten programvara.
- Mindre angreppsyta
  Den tunna klienten har ett begränsat operativsystem med få tjänster och applikationer. Detta gör den svårare att angripa jämfört med en fullvärdig pc med många installerade program.
- Skydd mot dataexfiltration
  Eftersom användaren inte har tillgång till filsystemet lokalt kan information inte enkelt kopieras till USB-enheter eller laddas upp till externa molntjänster (förutsatt att policys är korrekt inställda i servermiljön).
- Lättare revision och spårbarhet
  All aktivitet sker i den centrala miljön, vilket gör det enklare att logga, övervaka och analysera användarbeteende utan att behöva hantera lokala loggar på varje klient.

5. Hårdvarukrav

Hårdvaran i klienttjänsten omfattar både själva klienten och kringutrustningen. Båda delarna behöver skyddsåtgärder.

[47] Länk som förklarar begreppet (hämtad 2026-08-25):
https://en.wikipedia.org/wiki/Virtual_Desktop_Infrastructure

5.1 Fysisk säkerhet

Myndigheter bör ställa krav på ett grundläggande fysiskt skydd för sina klientdatorer, till exempel följande:

- Låsbarhet: Datorn ska kunna fästas med säkerhetslås (till exempel Kensington-lås) eller monteras i låsbara skåp eller vagnar.
- Skydd mot stöld: Bärbara datorer ska alltid förvaras säkert, till exempel i ett låsbart skåp när de inte används. På arbetsplatser med hög risk för obehörig åtkomst ska det finnas rutiner för att låsa in alla datorer.
- Portsäkerhet: USB-portar och andra anslutningar ska kunna spärras, så att obehöriga inte kan koppla in utrustning.
- Skydd mot manipulering: Känsliga klienter bör ha chassin med intrångsskydd som larmar eller loggar om datorn öppnas.
- Krypterad hårddisk: Om en dator trots allt stjäls ska all data vara skyddad med stark kryptering (se avsnitt 5.4).

5.2 BIOS/UEFI-säkerhet

Myndigheter bör ställa krav på att datorernas BIOS/UEFI[48] är skyddat mot obehöriga ändringar. Följande fem krav är viktiga:

1. Lösenordsskydd: Alla datorer ska ha ett starkt BIOS/UEFI-lösenord som inte är lätt att gissa.
2. Secure Boot: Funktionen Secure Boot ska vara aktiverad för att förhindra att skadlig kod startar innan operativsystemet har laddats.
3. Uppdateringar: Leverantören ska tillhandahålla säkerhetsuppdateringar för BIOS/UEFI under datorns hela livslängd. Uppdateringarna ska kunna installeras via en säker kanal, och BIOS/UEFI ska stödja TPM-baserad attestering, som skyddar mot firmware-attacker och rootkits.
4. Åtkomstkontroll: Endast behöriga administratörer ska kunna ändra inställningar i BIOS/UEFI.
5. Loggning: Försök att ändra i BIOS/UEFI ska loggas så att intrång kan upptäckas.

5.3 Firmware-integritet

Firmware är programvara på låg nivå som kommunicerar med viss kringutrustning eller vissa komponenter i datorn. All firmware ska vara signerad, och endast verifierad kod ska kunna laddas in, så att firmware inte kan manipuleras.

[48] Länk till förklaring av begreppen (hämtad 2026-08-25): https://en.wikipedia.org/wiki/UEFI

5.4 Diskkryptering

Myndigheter bör ställa krav på att alla klientdatorer har fullständig diskkryptering. Det innebär att hela hårddisken skyddas, inte bara vissa mappar eller filer. Centrala krav är följande:

- Obligatorisk kryptering
  Alla klienter, både stationära och bärbara, ska vara krypterade med en stark algoritm (till exempel AES-256).
- Stöd i hårdvara
  Krypteringen ska utnyttja datorns inbyggda säkerhetsmodul, till exempel Trusted Platform Module (TPM), för att skydda nycklarna. Självkrypterande diskar (SED) kan ge ytterligare skydd vid stöld eller förlust.
- Automatiskt skydd
  Krypteringen ska starta automatiskt utan att användaren behöver slå på den manuellt.
- Prestanda och stabilitet
  Krypteringen får inte försämra datorns funktion på ett sätt som gör den svår att använda i vardagen.
- Återställningsnycklar
  Myndigheten ska ha rutiner för säker hantering av återställningsnycklar. De får inte lagras tillsammans med datorn.
- Säker start
  Diskkryptering ska kombineras med Secure Boot eller liknande skydd för att hindra manipulation innan operativsystemet laddas (se avsnitt 5.2).
- Radering vid stöld
  Om en dator blir stulen bör det finnas möjlighet till fjärrlåsning eller radering.

5.5 Kringutrustning och säkerhet

Till klienterna hör kringutrustning som gör dem mer användbara, till exempel headset för möten eller dockningsstationer som snabbt gör en bärbar dator till en bra stationär arbetsplats.

5.5.1 USB och Bluetooth

Myndigheter bör ha en samlad strategi för säkerheten kring USB- och Bluetooth-utrustning. Åtgärderna behöver utvärderas och uppdateras löpande för att möta nya hot.

Åtkomstkontroll. Begränsa användningen av USB- och Bluetooth-enheter till behörig personal, till exempel med rollbaserad åtkomstkontroll (Role-Based Access Control, RBAC). Inför också en process för att registrera alla USB- och Bluetooth-enheter som används i myndigheten, så att användningen kan spåras och övervakas.

USB-enheter. Kryptera data som lagras på USB-enheter, så att informationen är skyddad om enheten förloras eller stjäls. Alla datorer som kan anslutas till USB-enheter ska ha uppdaterat skydd mot skadlig kod. Överväg att inaktivera USB-portar på datorer

som inte behöver dem, eller använd programvara som styr vilka enheter som får anslutas.

Bluetooth-enheter. Konfigurera Bluetooth-enheter med starka säkerhetsinställningar, inklusive autentisering och kryptering. Håll enheterna i osynligt läge när de inte används, begränsa parkoppling till betrodda enheter och håll firmware och programvara uppdaterade.

Utbildning och medvetenhet. Utbilda medarbetarna om riskerna med USB- och Bluetooth-enheter och om hur enheterna används säkert. Ta fram och kommunicera en tydlig rutin för hur medarbetarna ska rapportera säkerhetsincidenter som rör enheterna.

Övervakning och granskning. Logga alla anslutningar och aktiviteter som rör USB- och Bluetooth-enheter, så att säkerhetsincidenter kan spåras. Granska regelbundet att policys och rutiner är aktuella och effektiva.

5.5.2 HDMI och DisplayPort

HDMI och DisplayPort används för att ansluta skärmar, projektorer och annan bildutrustning. Dessa portar är i första hand avsedda för visning av bild, men de kan också överföra ljud, styrsignaler och i vissa fall nätverksinformation. På senare år har hotbilden breddats, då vissa enheter kan utnyttja dessa portar för att föra in eller ut information utan att det är avsikten. Det gäller särskilt i miljöer där skyddsvärd information hanteras.

Hotbild

HDMI- och DisplayPort-anslutningar kan innebära flera typer av risker:

- Otillåten informationspåverkan: Vissa typer av bildskärmar, adaptrar eller KVM-switchar (Keyboard, Video, Mouse[49]) kan fungera som en brygga och överföra data tillbaka till klienten via kanaler som inte övervakas.
- Inbyggda komponenter: Skärmar eller dockningsstationer kan innehålla integrerade mikroprocessorer eller nätverksgränssnitt som kan manipuleras eller fjärrstyras.
- Dolda USB-funktioner: Enheter som kopplas via HDMI- eller DisplayPort-adaptrar kan även presentera sig som USB-enheter (så kallad HID[50]-spoofing), vilket kan användas för att installera skadlig kod.
- El- och signalavlyssning: Vid arbete med hemliga uppgifter kan elektromagnetiska läckor via bildkablar utgöra en signalspaningsrisk.

Rekommenderade åtgärder

Myndigheter bör tillämpa en kombination av tekniska och administrativa skyddsåtgärder:

[49] Länk till beskrivning (hämtad 2026-08-25): https://en.wikipedia.org/wiki/KVM_switch
[50] Artikel som beskriver HID-attacker och tips för åtgärder (hämtad 2025-12-10): https://www.startupdefense.io/cyberattacks/hid-based-attack

1. Inventering och godkännande:
   Alla bildskärmar, adaptrar, KVM-lösningar och dockningsstationer ska omfattas av myndighetens inventering och godkännandeprocess, på samma sätt som annan kringutrustning. Endast granskade och godkända modeller får användas.
2. Fysisk styrning av portar:
   HDMI- och DisplayPort-utgångar som inte används ska inaktiveras i BIOS eller operativsystem, eller fysiskt spärras med portblockerare. På stationära datorer i känsliga miljöer kan myndigheten helt ta bort portarna.
3. Separata visningsmiljöer:
   Datorer som hanterar skyddsvärd information bör inte användas för att visa presentationer eller bild på externa enheter i öppna miljöer. Använd i stället särskilda visningsdatorer eller tunna klienter utan åtkomst till känsliga system.
4. Krav på ”snälla skärmar”:
   Vid upphandling av bildskärmar och projektorer ska krav ställas på att enheterna inte har aktiv lagring, inbyggd mjukvara med nätverksanslutning, Bluetooth eller annan trådlös kommunikation.

5.5.3 eSATA

eSATA-portar kan, likt USB, användas för att ansluta lagringsenheter med hög överföringshastighet. Detta innebär risk för otillåten dataexport eller införsel av skadlig kod.

Inaktivera eSATA-portar i BIOS/UEFI eller via central policy om de inte behövs. Om portarna används krävs samma skydd som för USB-portar, det vill säga kryptering, loggning av åtkomst och godkännande av enheter.

5.6 Fjärrhantering på hårdvarunivå

Företagsdatorer har i dag inbyggd teknik i hårdvaran för fjärrstyrning, till exempel Intel vPro och AMD DASH. Tekniken gör det möjligt att hantera enheter centralt och agera snabbt vid incidenter, även när klienten inte startar korrekt och stöd på plats är svårt eller oönskat. Samtidigt kan en antagonist utnyttja tekniken. Myndigheten behöver därför styra och kontrollera den.

6. Säkerhetsuppdateringar

För att kunna hantera säkerhetsuppdateringar på klienterna behöver myndigheten lämpliga centrala verktyg för klienthantering. Med verktygen kan myndigheten schemalägga säkerhetsuppdateringar för alla klienter och följa upp dem.

6.1 Rekommenderad arbetsprocess

En bra arbetsprocess bygger på regelbundenhet, prioritering och spårbarhet. Myndigheten bör ha en tydlig plan där kritiska säkerhetsuppdateringar installeras omedelbart, ofta inom 24 timmar från publiceringen. Mindre viktiga uppdateringar kan samlas och rullas ut veckovis eller månadsvis, beroende på verksamhetens behov.

Processen bör omfatta följande steg:

- **Övervakning**: Bevaka kontinuerligt nya säkerhetspatchar via leverantörernas säkerhetskanaler.
- **Prioritering**: Bedöm vilka uppdateringar som är kritiska och vilka som kan vänta.
- **Testning**: Testa uppdateringarna i en begränsad miljö för att se att de inte skapar driftproblem.
- **Utrullning**: Installera uppdateringarna automatiskt och centralt på alla klienter.
- **Uppföljning**: Kontrollera att uppdateringarna verkligen har installerats och skapa rapporter för spårbarhet och revision.

Eftersom antalet kritiska sårbarheter ökar och de sprids allt snabbare har tiden för test och införande av säkerhetsuppdateringar minskat drastiskt.

6.2 Windows

Det finns olika typer av säkerhetsuppdateringar för Windows. Microsoft släpper månatliga säkerhetsuppdateringar den andra tisdagen varje månad. För att säkerställa kvaliteten rekommenderar arbetsgruppen att uppdateringarna först installeras hos pilotgrupper.

Rekommenderad tidslinje för utrullning

Följ processen i avsnitt 6.1. Bedöm hur allvarlig sårbarheten är och hur kritisk den är för den egna verksamheten, och rulla ut uppdateringen inom den tid som tabellen anger[51]. Tabellen visar föreslagna hanteringstider per allvarlighetsgrad enligt CVSS.

Allvarlighetsgrad (CVSS)	Föreslagna hanteringstider
Kritisk (CVSS 9,0–10,0)	24–72 timmar för externt exponerade it-system, 7 dagar för interna system
Hög (CVSS 7,0–8,9)	7 dagar för externt exponerade it-system, 14 dagar för interna system
Medel (CVSS 4,0–6,9)	30 dagar
Låg (CVSS 0,1–3,9)	90 dagar eller valfritt

Exempel på patchhantering i praktiken

Dagen efter Microsofts release, det vill säga på onsdagen, skickas uppdateringarna till en liten pilotgrupp inom it-avdelningen, till exempel fem personer eller cirka 2 procent av it-personalen. En vecka efter releasen skickas de till ett större antal piloter i hela myndigheten, till exempel ett trettiotal personer eller cirka 5 procent av medarbetarna, fördelade på olika delar av verksamheten. Två veckor efter releasen skickas de till alla

[51] Länk till artikel som förklarar sårbarhetsnivå (hämtad 2025-12-10): https://www.paloaltonetworks.co.uk/cyberpedia/patch-management

medarbetare i tre omgångar: tisdag, onsdag och torsdag. Exemplet förutsätter att pilotgrupperna inte har hittat några problem.

Definitionsuppdateringar med nya virusdefinitioner släpps regelbundet, ibland flera gånger om dagen. De bör hämtas varannan timme.

Microsoft rekommenderar själv att Windows-uppdateringar hämtas så snart de är tillgängliga[52].

6.3 Linux

Myndigheter kan använda flera typer av verktyg för att hantera säkerhetsuppdateringar på Linux-klienter. Vanliga lösningar är konfigurations- och automatiseringsverktyg, till exempel Ansible, Puppet, Chef eller SaltStack, som gör det möjligt att styra uppdateringar centralt och samtidigt på många Linux-datorer. För miljöer med blandade operativsystem kan även plattformar som Red Hat Satellite, SUSE Manager eller Canonical Landscape användas. De är anpassade för Linux och ger patchhantering, rapportering och efterlevnadskontroller.

För distributioner som bygger på Debian eller Ubuntu finns inbyggda paketkällor med stöd för automatiska uppdateringar. För Red Hat-baserade system finns motsvarande stöd via yum/dnf. Genom att kombinera dessa med centrala administrationsverktyg får myndigheten både enkelhet för användaren och kontroll för it-avdelningen.

För att skydda myndighetens information är det avgörande att Linux-klienter hålls uppdaterade. Angrepp utnyttjar ofta kända säkerhetshål, och en dator som inte uppdateras regelbundet blir snabbt en svag punkt i it-miljön.

Myndigheten bör ha en central och automatiserad rutin för uppdateringar, där klienterna regelbundet kontrollerar om det finns nya säkerhetspatchar. Patcharna bör sedan rullas ut med samma metodiska upplägg som för Windows (se avsnitt 6.1 och 6.2).

Användarna bör inte själva ha ansvar för att uppdatera sina Linux-klienter. I stället ska uppdateringsprocessen vara centralstyrd och ske i bakgrunden, så att klienterna alltid är skyddade utan att det kräver aktivt arbete från personalen. Myndigheten bör dessutom ha en övervakning som visar vilka datorer som inte är uppdaterade, och rutiner för att åtgärda det.

6.4 macOS

Även för macOS rekommenderar arbetsgruppen att säkerhetsuppdateringar först installeras hos pilotgrupper, med samma upplägg som för Windows (se avsnitt 6.2).

[52] Länk till sida med Microsofts rekommendation (hämtad 2026-02-26): https://support.microsoft.com/sv-se/windows/h%C3%A4mta-windows-uppdateringar-s%C3%A5-snart-de-%C3%A4r-tillg%C3%A4ngliga-f%C3%B6r-din-enhet-cad7b32b-001e-435b-9110-f18309b54168

Apple släpper säkerhetsuppdateringar oregelbundet. Myndigheten bör därför ha en rutin kopplad till Apples betaprogram för macOS[53].

Om myndigheten inte hittar några problem i testerna kan uppdateringen installeras när Apple har släppt den.

6.5 Säkerhetsuppdatering av övriga komponenter

Myndighetens arbete med säkerhetsuppdateringar ska också omfatta andra komponenter, till exempel program, drivrutiner, firmware och BIOS/UEFI. Säkerhetsbehovet, brådskan och uppdateringsmetoden varierar så mycket mellan komponenterna att det inte går att ge en allmän rekommendation för hur arbetet ska utföras.

7. Behörigheter

Behörigheter till och på klienterna är en viktig säkerhetsfråga. När en klient har hackats har antagonisten oftast tagit över dess behörigheter och kan då styra både klienten och delar av det nätverk som den är ansluten till.

7.1 Lokala konton

Lokala konton på klienterna bör ses som en säkerhetsrisk, eftersom de kan utnyttjas vid cyberattacker och försvårar central spårbarhet. Myndigheten bör därför begränsa användningen av och tillgången till lokala konton, vilket också är ett krav enligt MSBFS 2020:7.

Arbetsgruppen rekommenderar att både det lokala administratörskontot och gästkontot tas bort vid installationen. Om ett lokalt administratörskonto behövs bör ett nytt konto skapas med en ny, unik identitet och helst utan ”admin” i namnet, så att kontots syfte blir svårare att gissa.

7.2 Hantera lokala administratörsrättigheter på klienter

Endast de som behöver lokala administratörsrättigheter bör få dem, och bara när behovet uppstår. Permanenta och brett utdelade administratörsrättigheter är ett omedelbart och allvarligt säkerhetsproblem. Även detta regleras i MSBFS 2020:7.

Om myndigheten ansluter klienterna till Entra ID (tidigare Azure AD) kan Windows LAPS tekniskt användas för att hantera lokala administratörsrättigheter. Om detta är juridiskt eller säkerhetsmässigt lämpligt behöver sannolikt prövas.

Det finns flera verktyg på marknaden för tidsbegränsad administratörsåtkomst, så kallad Just-in-Time (JIT)[54] privileged access, som ofta ingår i en lösning för Privileged Identity

[53] Länk till Apples betaprogram för macOS (hämtad 2025-12-10): https://beta.apple.com/
[54] Artikel som förklarar konceptet (hämtad 2025-12-10): https://www.crowdstrike.com/en-us/cybersecurity-101/identity-protection/just-in-time-access/

Management (PIM)[55]. I sådana lösningar är det standard att arbeta enligt en skiktmodell (tier-modell), där vissa administratörskonton bara finns i vissa skikt. Säkerställ att endast de konton som behövs på klienterna kan logga in på dem.

Gör en egen informationssäkerhetsbedömning av om administrativa kontonamn och lösenord får delas mellan myndigheten och leverantören, till exempel via en molntjänst. Ett säkrare alternativ kan vara att skapa särskilda konton i tjänsten för leverantören.

7.3 Olika konton för olika roller

För att minska risken för fel och intrång bör myndigheter separera konton utifrån användarens roll och uppgift. Samma konto bör inte användas för administrativa, operativa och vanliga arbetsuppgifter.

Arbetsgruppen rekommenderar att myndigheten inför principen om åtskillnad av arbetsuppgifter (Separation of Duties, SoD)[56]. Administratörer ska ha ett separat administratörskonto utan tillgång till e-post eller internet, och vanliga användarkonton ska sakna lokala administratörsrättigheter. Privilegierade konton bör hanteras med PIM- eller JIT-lösningar. Alla konton bör vara personliga och spårbara och inaktiveras direkt vid rollbyte eller när anställningen upphör.

8. Nätverk och klienter

Nätverksuppkopplingen är en central del av klientdatorsäkerheten. Den avgör hur enheten kommunicerar med interna resurser och tjänster, och har stor påverkan på både säkerhet och användarupplevelse. I kapitlet beskrivs tre vanliga modeller för säker anslutning till myndighetens nätverk: Always-on VPN, användaraktiverad VPN och Secure Access Service Edge (SASE).

8.1 Always-on VPN

Always-on VPN innebär att klienten automatiskt upprättar en VPN-anslutning så snart enheten har internetuppkoppling. Denna lösning kräver ingen användarinteraktion och säkerställer att klientdatorn alltid befinner sig på myndighetens nätverk och att all nätverkstrafik till och från klienten alltid passerar myndighetens säkerhetsmekanismer.

Fördelar

- Hög säkerhet genom konstant skyddad anslutning.
- Centraliserad kontroll och insyn i nätverkstrafik.
- Skydd även på osäkra nätverk (till exempel publika trådlösa nätverk).

[55] Artikel som förklarar konceptet (hämtad 2025-12-10): https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure
[56] Länk som förklarar begreppet (hämtad 2025-12-10): https://csrc.nist.gov/glossary/term/separation_of_duty

- Lämplig för hårt reglerade verksamheter eller vid hantering av känslig information.
- Traditionella verktyg för klienthantering och övervakning kan användas.

Nackdelar

- Kan påverka prestanda, särskilt för geografiskt avlägsna användare eller användare med sämre uppkoppling.
- Kräver stabil VPN-infrastruktur och redundans.
- Kräver gedigna processer för kvalitetssäkring eftersom en felaktig uppdatering kan få stora konsekvenser gällande tillgängligheten för distansanslutna medarbetare.

Användningsområden

- Organisationer med höga krav på säkerhet och dataskydd.
- Verksamheter som följer regelverk som NIS2 eller GDPR och där datatrafiken måste hållas inom en kontrollerad zon.

8.2 Användaraktiverad VPN

Med användaraktiverad VPN ansvarar användaren själv för att ansluta till VPN-tjänsten vid behov, till exempel när tillgång till interna resurser krävs. VPN-klienten installeras på klientdatorn och ger användaren möjlighet att initiera och avsluta anslutningen.

Fördelar

- Mindre belastning på nätverksinfrastrukturen när VPN inte behövs.
- Mer flexibel för användare som arbetar med både interna och externa system.
- Lägre krav på alltid tillgänglig VPN-infrastruktur.

Nackdelar

- Klienterna växlar mellan okända nätverk och myndighetens interna nätverk.
- Kommunikationen är mer utsatt, vilket är ett problem vid användning av publika trådlösa nätverk.
- Ingen garanti att nätverkstrafik passerar myndighetens säkerhetsfilter.
- Svårare att upprätthålla konsekvent säkerhetsnivå.
- Klienthantering och övervakning behöver ske med internetbaserade tjänster.

Användningsområden

- Miljöer med lägre krav på ständig anslutning till interna resurser.

- Personal som arbetar mycket mobilt eller främst använder molnbaserade tjänster.

8.3 Secure Access Service Edge (SASE)

SASE är en molnbaserad arkitektur som kombinerar nätverks- och säkerhetstjänster såsom identitetsbaserad åtkomstkontroll, brandväggar, webbsäkerhet och dataskydd i ett globalt distribuerat ramverk. I stället för att all trafik går via myndighetens nätverk går den via SASE-leverantörens närmaste anslutningspunkt.

Fördelar

- Möjliggör direkt, säker åtkomst till internet och molntjänster utan att gå via myndighetens datacenter.
- Förbättrad prestanda genom lokal ”breakout” och optimerad routing.
- Centraliserad säkerhetspolicy även i distribuerade miljöer.
- Skalbar och framtidssäker lösning för hybridarbete.

Nackdelar

- Kräver integration med identitets- och enhetshanteringslösningar.
- Kan vara tekniskt och organisatoriskt komplext att införa.
- Beroende av tredjepartsleverantörens tillgänglighet och säkerhetsnivå.

Användningsområden

- Organisationer med hög grad av distansarbete eller molnbaserade arbetsverktyg.
- Verksamheter som eftersträvar en arkitektur enligt principen om nolltillit (zero trust)[57] och snabb anpassning till förändrade behov.

8.4 Nolltillit och klientsäkerhet

Vissa myndigheter använder nolltillit (zero trust) för att skydda nätverk, informationsmängder och tjänster. Det ger ofta en hög säkerhetsnivå som kan anpassas efter myndighetens behov och lagkrav. I en sådan arkitektur är klienterna ofta en av de komponenter som separeras säkerhetsmässigt.

8.5 Tvåfaktorsinloggning och smarta kort i myndigheters it-miljö

För att skydda känsliga system och uppgifter bör myndigheter använda tvåfaktorsinloggning i alla sina it-tjänster. Tvåfaktorsinloggning innebär att inloggningen kräver både något användaren vet, som ett lösenord, och något användaren har, till

[57] Länk till förklarande artikel (hämtad 2026-09-04): https://it-ord.computersweden.se/ord/nolltillit/

exempel ett smart kort (med ett hanterat certifikat) eller en mobilapplikation. Denna kombination gör det betydligt svårare för obehöriga att få tillgång till myndighetens resurser, även om ett lösenord skulle komma på avvägar.

Smarta kort kan fungera som en gemensam nyckel för flera tjänster. De kan användas både för fysisk passage i myndighetens lokaler och för digital åtkomst till datorer, nätverk och skrivartjänster. På så sätt förenklas hanteringen för användaren samtidigt som säkerhetsnivån höjs.

Det är viktigt att korten och inloggningslösningarna används konsekvent i hela myndigheten. Samma krav bör gälla för klienter, som bärbara datorer, och för alla it-tjänster, från e-post och fildelning till utskrifter. Myndigheten bör också ha tydliga rutiner för hur kort utfärdas, spärras och ersätts, så att risken för missbruk minskar vid förlust eller stöld.

8.5.1 EFOS-kunder bland eSams medlemmar

Sommaren 2025 använde 24 av eSams medlemmar identitetstjänsten EFOS från Försäkringskassan, och ytterligare 5 medlemmar testade tjänsten inför ett eget, större införande. Flera av de övriga 11 medlemmarna har också visat stort intresse. EFOS väntas bli en viktig tjänst inom NITIS (säker statlig it-drift) och är en av de tolv första tjänster som ska levereras när NITIS startar sin driftleverans. EFOS är dock inte en beslutad standard bland eSams medlemmar. I dag saknas en gemensam standard, något som hade kunnat göra säker digital samverkan enklare, även inom medlemmarnas klienttjänster.

9. Mätning och övervakning

Mätning och övervakning av klienterna behövs för att upptäcka både försök till incidenter och pågående incidenter.

9.1 Mätning av klienter och behörigheter

Ett sätt att stärka säkerheten i klienterna, och även i andra it-system och komponenter, är att arbeta metodiskt med härdning enligt en etablerad metod (se kapitel 3 *Klientinställningar*) och sedan följa upp resultatet med automatiserade mätverktyg (benchmarks). På så sätt får myndigheten jämförbara mätvärden med jämna mellanrum, som visar om säkerhetsarbetet går framåt och kan användas i den långsiktiga planeringen. Myndigheten kan välja ambitionsnivå utifrån verksamhetens övergripande säkerhetskrav.

Beroende på verktyg kan myndigheten till exempel mäta kända sårbarheter i Active Directory, förekomsten av vanliga felkonfigurationer, klientsäkerhet, brister i säkerhets- och granskningsloggar samt otillåten nätverkstrafik från klienterna.

9.1.1 Enklare metod för mätning

Med enkla verktyg med öppen källkod kan myndigheten snabbt undersöka hur väl ett behörighetssystem baserat på Active Directory är konfigurerat för att undvika sårbarheter. Det finns verktyg som stöder rapportering enligt ramverk som MITRE ATT&CK och ANSSI:s rekommendationer.[58]

Fynden redovisas i följande huvudkategorier: brister i lösenord och autentisering, problem med behörigheter och åtkomsthantering, föråldrade system och sårbarheter, brister i kontohanteringen, sårbarheter i nätverk och protokoll, problem med domäntillit och infrastruktur samt luckor i granskning och övervakning. Dessutom görs specifika sårbarhetskontroller. Resultatet poängsätts och redovisas i grafiska rapporter.

9.1.2 Mer omfattande metod enligt CIS Benchmarks[59]

En mer ambitiös satsning på att höja säkerheten kan genomföras som ett projekt eller program enligt CIS Benchmarks.

Arbetet delas lämpligen upp i faser, som i sin tur består av flera arbetsmoment: förberedelse och bedömning, planering och pilot, implementeringsstrategi, test och validering, utrullning i produktion och avslut samt löpande förvaltning efter avslutet. Tidsåtgången för en medelstor organisation bedöms till 10–20 veckor.

Arbetet med CIS Benchmarks kan kompletteras med andra standarder och ramverk, till exempel ramverk från NIST[60] eller uppföljning mot ISO/IEC 27000-serien[61].

9.2 Övervakning av klienter

Klientplattformen ska stödja centraliserad och strukturerad logghantering. Systemet ska generera säkerhetsloggar för alla väsentliga händelser såsom inloggningar, autentiseringsförsök, systemändringar, nätverksanslutningar, applikationskörningar och policyavvikelser. Loggarna ska ha ett format som möjliggör spårbarhet, analys och forensik.

Loggarna ska vara skyddade mot obehörig åtkomst och manipulation, samt lagras i en SIEM-lösning (Security Information and Event Management) för realtidsövervakning, händelsekorrelation och upptäckt av avvikelser. Loggdata ska vara tillgänglig för både incidenthantering och revision.

Logghanteringen ska uppfylla kraven i ISO/IEC 27001, MSBFS 2020:7, MSBFS 2020:8 och cybersäkerhetslagen. Krav på loggning, lagringstid, format och tillgänglighet ska också ställas vid upphandling av system som hanterar klientdata.

[58] Se https://www.netwrix.com/active-directory-risk-assessment.html
[59] Se beskrivande artikel (hämtad 2025-12-10): https://www.cisecurity.org/cis-benchmarks
[60] Se beskrivande artikel (hämtad 2025-12-10): https://en.wikipedia.org/wiki/Security_Technical_Implementation_Guide
[61] Se beskrivande artikel (hämtad 2025-12-10): https://en.wikipedia.org/wiki/ISO/IEC_27000_family

För utformning av logghantering, SOC-funktion och integration i incidentprocesser hänvisas till *ES2024-16 Vägledning Ransomware*[62], särskilt avsnitt 4.1 och 5.2.

10. Klienter utanför myndigheten

Framför allt bärbara klienter används på tjänsteresor och vid arbete på andra platser än kontoret. Hur bör en myndighet skydda en klient som befinner sig på en okänd plats, är uppkopplad mot okända nätverk eller kanske används till mer än arbete?

10.1 Klientsäkerhet utanför myndighetens nätverk

När en myndighetsdator används utanför det egna nätverket, till exempel vid besök hos andra myndigheter eller på allmänna platser som hotell och flygplatser, ökar risken för intrång och dataläckor. Myndigheten behöver därför tydliga riktlinjer för klientsäkerhet. All trafik bör gå genom en säker VPN-tunnel, så att den passerar myndighetens skydd, och datorn måste hållas uppdaterad med de senaste säkerhetspatcharna. Delad tunnel (split tunneling) ger visserligen bättre prestanda men ses oftast som en säkerhetsrisk. Myndigheten behöver också ta ställning till om användaren ska kunna stänga av VPN-anslutningen. Inloggning ska ske med flerfaktorsautentisering, till exempel en kombination av lösenord och mobilapp eller säkerhetsdosa. Användaren ska bara ha tillgång till den information och de system som behövs för arbetsuppgifterna.

Brandväggen och klientskyddet (till exempel EDR) ska vara aktiverade på klienten. Datorn bör inte anslutas direkt till öppna trådlösa nätverk utan skydd; internetdelning via tjänstemobilen är att föredra. Datorn får inte lämnas obevakad, och skärmen ska alltid låsas när användaren går ifrån den.

10.2 Privat användning av myndighetsdatorer

Notera: All privat användning av myndighetens utrustning kan bli föremål för både myndighetens incidentutredningar och begäranden om utlämnande av handlingar. Det behöver vara tydligt för medarbetarna.

Frågan om privat användning av myndighetsdatorer är känslig. Grundprincipen bör vara att datorn används för arbete, men det kan finnas praktiska skäl att tillåta viss privat användning, till exempel för att boka vårdbesök eller sköta enklare bankärenden. För att det ska vara säkert behöver privat och arbetsrelaterad användning vara tydligt avgränsade. Myndigheten kan till exempel överväga att tillhandahålla en särskilt konfigurerad webbläsare för privat användning. Myndigheten behöver också klargöra vad som är tillåtet och vad som är förbjudet. Då kan den erbjuda användarna en viss flexibilitet utan att ge avkall på informationssäkerheten. Arbetsgruppen rekommenderar att myndigheten förbjuder följande privata användning och informerar tydligt om det:

[62] Länk till eSams publikation (hämtad 2025-12-10): https://www.esamverka.se/publikationer/sakerhet/2025-04-15-vagledning-ransomware.html

- Att läsa privat e-post. Det är ett känt och historiskt stort hot, och risken för myndigheten är för stor för att det ska kunna tillåtas.
- Att installera egna program. Det ökar säkerhetsrisken och försvårar dessutom myndighetens centrala licenshantering.
- Att använda strömningstjänster. De kan belasta myndighetens nätverk orimligt mycket, framför allt vid stora populära sändningar, och att tillåta dem kan signalera att bredare privat användning av klienterna är godkänd. Reglerna skiljer sig ofta mellan dator och mobil.
- Att ansluta kringutrustning som inte är godkänd till tjänstedatorn. Hur stort problemet är varierar, men för beredskapsmyndigheter är det inte tillåtet enligt MSBFS 2020:7.

Arbetsgruppen rekommenderar att myndigheten bara tillåter privat användning som bedöms medföra ett lågt hot, till exempel besök på säkra och seriösa webbplatser.

10.3 Klientsäkerhet vid arbete utomlands

När myndighetsanställda arbetar utanför landet ställs särskilda krav på klientsäkerheten. Risken för avlyssning, intrång och dataläckor ökar, särskilt när datorer eller mobiltelefoner används i miljöer där myndigheten inte har kontroll över nätverk och infrastruktur.

Myndigheten kan ha olika säkerhetsregler för olika länder eller regioner. Det kan till exempel innebära att tjänsteutrustning inte får tas med alls vid tjänsteresor till Ryssland, men att den är tillåten vid tjänsteresor inom EU. Myndigheten kan också ge särskilda instruktioner inför resor till högriskområden.

Grundskyddet är detsamma som vid annat arbete utanför myndighetens nätverk (se avsnitt 10.1). Utomlands är det särskilt viktigt att personalen känner till riskerna med publika trådlösa nätverk, till exempel på hotell, flygplatser och kaféer, eftersom de kan vara manipulerade för att fånga upp trafik.

Även säkerheten kring SIM-kort är viktig. Kort kan bytas ut eller klonas utan att användaren märker det, vilket kan ge obehöriga tillgång till samtal eller meddelanden. Myndigheten bör därför använda SIM-kort med hög säkerhetsnivå och ha rutiner för att snabbt upptäcka och hantera misstänkta incidenter.

Säker laddning med USB-datablockerare

Laddning av tjänsteutrustning kan också vara ett problem vid vissa utlandsresor. Laddning via USB i till exempel hyrbilar eller på hotellrum kan föra över skadlig kod till datorn eller mobilen. Ett enkelt skydd är att alltid använda en USB-datablockerare[63].

[63] Länk till artikel som förklarar begreppet (hämtad 2025-09-12): https://en.wiktionary.org/wiki/USB_data_blocker

11. Bilaga 1. Källor för omvärldsbevakning

Rekommenderade källor:

- Myndigheten för civilt försvars (MCF) publikationer
- Nationellt cybersäkerhetscenter (NCSC) vid FRA, där CERT-SE ingår sedan den 1 juli 2026
- Säkerhetspolisens öppna rapporter om hotbilden mot Sverige
- EU:s cybersäkerhetsbyrå ENISA – rekommendationer och rapporter
- NIST:s uppdateringar (till exempel SP 800-serien)
- Nationella och internationella CVE-databaser
- Leverantörernas säkerhetsbulletiner (Microsoft, Apple, Canonical, Dell, HP med flera)

12. Bilaga 2. Checklista för klientsäkerhet

1. Upphandling och leverantörskrav

- Ställ juridiska krav relaterade till klientsäkerhet, inklusive dataskydd och informationssäkerhet.
- Ta ställning till risker kopplade till tillverkningsland, hårdvarutillverkare och leverantörskedja, och ställ krav på skydd utifrån behov.
- Ställ krav på långsiktigt säkerhetsstöd från leverantören.
- Ställ säkerhetskrav på användarstödet, inklusive dess åtkomst till klienterna.
- Ställ krav på säker avyttring av klienter.

2. Central hantering och policy

- Ha central klienthantering med policystyrning.
- Säkerställ en säker och spårbar imagepåläggning vid klientinstallationer.

3. Klientinställningar

- Använd Windows Security Baselines och motsvarande baselines för Linux och macOS som grundkrav på myndighetens datorer.
- Bedöm riskerna med lokal skanning, till exempel lokala AI-funktioner, och begränsa eller stäng av funktionerna centralt.
- Begränsa telemetri och diagnostikdata i Windows.
- Hantera lokal filsynkning och offlinefiler enligt rekommendationerna i avsnitt 3.7.

4. Alternativa klienter

- Ha särskilda säkerhetskrav för lånedatorer.
- Bedöm risker med Windows Subsystem for Linux (WSL2).
- Säkra kioskdatorer med låsta behörigheter.
- Ställ krav på tunna klienter utifrån driftsmiljö och hotbild.

5. Hårdvarukrav

- Se över de fysiska säkerhetskraven för klienterna.
- Säkerställ integriteten hos firmware och drivrutiner i klientmiljön, till exempel genom kontroller och uppdateringar.
- Säkerställ en säker BIOS/UEFI-konfiguration, till exempel lösenordsskydd och Secure Boot.
- Använd diskkryptering som standard.

- Hantera kringutrustning säkert, till exempel USB-enheter, dockningsstationer och andra tillbehör. Bara godkänd utrustning får anslutas till klienten.
- Styr och kontrollera fjärrhantering på hårdvarunivå, till exempel Intel vPro och AMD DASH.

6. Säkerhetsuppdateringar

- Följ rekommenderad arbetsprocess och riskbedömning för säkerhetspatchning.
- Säkerställ uppdateringsprocesser för Windows, Linux och macOS.
- Dokumentera och följ upp patchnivåer och utrullning av patchar.

7. Behörigheter

- Tillämpa principen om minsta möjliga behörighet.
- Använd flerfaktorsautentisering vid inloggning på klienten, till exempel med smarta kort.
- Begränsa lokala administratörsbehörigheter.
- Inför en strukturerad roll- och behörighetsstyrning.

8. Nätverk och anslutning

- Använd VPN för allt arbete utanför myndighetens nätverk. Bedöm om VPN ska vara tvingande (always-on) för att uppnå rätt säkerhetsnivå.
- Säkerställ rutiner och kontroller om användaraktiverad VPN används.
- Överväg Secure Access Service Edge (SASE) vid molncentrerade arbetssätt.

9. Mätning och övervakning

- Mät status på klienter, beteenden, uppdateringar och behörigheter regelbundet.
- Övervaka klienter för avvikande beteenden eller hot.
- Koppla övervakningen till myndighetens SOC eller motsvarande funktion.

10. Klienter utanför myndigheten

- Följ särskilda säkerhetsrutiner för klienter utanför myndighetens nätverk.
- Ha riktlinjer för privat användning av myndighetsdatorer.
- Hantera de särskilda riskerna vid arbete utomlands, till exempel genom att använda USB-datablockerare vid laddning och vara försiktig med nätverk och fysisk exponering.

eSamverkansprogrammets syfte är att genom frivillig samverkan mellan myndigheter, underlätta och driva på medlemmarnas digitala transformation.

Tillsammans bidrar vi med hållbara och rättssäkra lösningar till nytta för såväl medlemmar som samhälle.

Alla publikationer finns på esamverka.se

I eSam ingår Arbetsförmedlingen, Arbetsmiljöverket, Bolagsverket, Boverket, Centrala Studiestödsnämnden, Domstolsverket, E-hälsomyndigheten, Ekonomistyrningsverket, Finansinspektionen, Folkhälsomyndigheten, Försäkringskassan, Havs- och vattenmyndigheten, Inspektionen för vård och omsorg, Jordbruksverket, Kemikalieinspektionen, Kronofogdemyndigheten, Kustbevakningen, Lantmäteriet, Livsmedelsverket, Läkemedelsverket, Länsstyrelserna, Migrationsverket, Naturvårdsverket, Pensionsmyndigheten, Riksantikvarieämbetet, Riksarkivet, Rättsmedicinalverket, Sida, Skatteverket, Skogsstyrelsen, Skolverket, Statens institutionsstyrelse, Statens servicecenter, Statens tjänstepensionsverk, Statens veterinärmedicinska anstalt, Statistiska centralbyrån, Tillväxtverket, Trafikverket, Transportstyrelsen, Tullverket, Universitets- och högskolerådet samt Utbetalningsmyndigheten. (juli 2026.)