Myndigheten för samhällsskydd och beredskap

VÄGLEDNING

Säkerhetsåtgärder i informationssystem

Vägledning säkerhetsåtgärder i informationssystem

© Myndigheten för samhällsskydd och beredskap (MSB)

Foto omslag: iStock
Produktion: Advant

Publikationsnummer: MSB2032 – reviderad november 2023
ISBN: 978-91-7927-446-7

Vägledning säkerhetsåtgärder i informationssystem

Denna vägledning utgör ett stöd vid tillämpningen av *Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd (MSBFS 2020:7) om säkerhetsåtgärder i informationssystem för statliga myndigheter*, men kan med fördel användas av alla organisationer[1], till exempel regioner, kommuner eller företag, som stöd i it-säkerhetsarbetet. Vägledningen riktar sig i första hand till de personer som utvecklar, hanterar och förvaltar en organisations it-miljö, till exempel CIO[2], it-chefer, it-säkerhetsansvariga, it-säkerhetsarkitekter samt CISO[3] i sin roll att samordna organisationens informationssäkerhetsarbete. Föreskrifternas krav på säkerhetsåtgärder motsvarar vad MSB bedömer att en statlig myndighet *minst* behöver göra för att nå en godtagbar nivå av säkerhet i sin it-miljö. Vilka ytterligare säkerhetsåtgärder som behöver vidtas identifierar organisationen genom sitt systematiska och riskbaserade informationssäkerhetsarbete. Annan reglering kan också ställa högre krav på säkerhet, exempelvis dataskyddsförordningen[4] eller säkerhetsskyddslagen[5].

Vägledningen kommer vid behov att uppdateras. Förändringsförslag, kommentarer och synpunkter skickas till informationssakerhet@informationssakerhet.se

Läsanvisning

Vägledningen består av ett antal avsnitt. Varje avsnitt beskriver ett område som är viktigt att arbeta med för att skydda informationssystem.

Varje avsnitt inleds med ett syfte som beskriver varför området är viktigt. Därefter följer ett antal ska-krav, ibland även bör-krav, samt stöd för att uppfylla kraven. Ska- och bör-krav är hämtade från Myndigheten för samhällsskydd och beredskaps (MSB) föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter men ibland uttryckta på ett något mer lättillgängligt sätt. Efter varje ska- och bör-krav finns en hänvisning till motsvarande krav i föreskrifterna. Kraven i vägledningen är inte tänkta att ha något annat syfte eller annan innebörd än föreskriftskraven. I vägledningen används även begreppet ”behöver” där föreskrifterna saknar uttryckliga krav men där MSB ändå vill betona vikten av att vidta en viss säkerhetsåtgärd.

---

1. För att ytterligare tydliggöra detta så används genomgående begreppet organisation i vägledningen.
2. Chief Information Officer.
3. Chief Information Security Officer.
4. Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG(allmän dataskyddsförordning).
5. Säkerhetsskyddslag (2018:585).

I de fall MSB vill lyfta fram en säkerhetsåtgärd men har bedömt att den inte är av samma vikt att vidta som en säkerhetsåtgärd som organisationen ”behöver” vidta så används skrivningen att säkerhetsåtgärden är ”lämplig”.

Eftersom vägledningen är tänkt att ha en bredare målgrupp än de statliga myndigheterna har, med undantag för kapitel 5, ”myndighet” ersatts med ”organisation” i vägledningen. Anledningen till att ”myndighet” har behållits i kapitel 5 är att kraven där riktar sig specifikt till beredskapsmyndigheter.[6] Som en följd av att vägledningen har en bredare målgrupp har dessutom föreskrifternas skrivningar om ”myndighetens uppdrag” ersatts med ”organisationens verksamhet”. Några skillnader avseende omfattning avses inte, utan begreppen används här på ett likvärdigt sätt.

Vägledningen täcker samtliga områden som en organisation enligt avsnitt 3.1.2. behöver ta fram krav på men har inte specifika avsnitt för områdena kontinuitetshantering under fredstida krissituationer och inför och vid höjdberedskap, arkivering och avveckling.[7] För ytterligare stöd rörande dessa områden hänvisas till bilaga A. I bilaga A har vi samlat hänvisningar till andra råd och stöd, både generella och sådana som ger stöd att uppfylla en viss säkerhetsåtgärd.

I bilaga B beskrivs kopplingen mellan vägledningens säkerhetsåtgärder och vad vi bedömer är motsvarande säkerhetsåtgärder i SS EN-ISO ISO 27002:2017 och SS EN-ISO ISO 27002:2022.

Rättigheter

Handböcker, lagkommentarer och upplysande skrifter och publikationer (såsom denna vägledning) som har upprättats hos en myndighet omfattas av begränsad upphovsrätt. Detta innebär att man får kopiera, översätta, visa och framföra materialet om man anger källa och upphovsmannens namn i den utsträckning som god sed kräver (26a § andra stycket upphovsrättslagen).

6. Förordning (2022:524 om statliga myndigheters beredskap

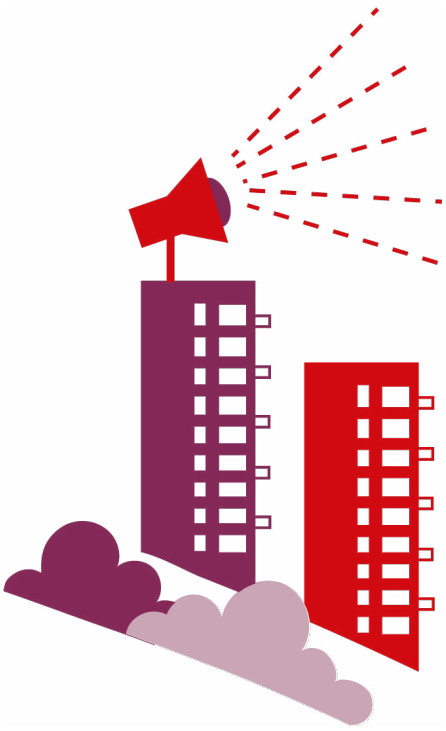
7. Stöd för kontinuitetshantering och avveckling behandlas exempelvis i kapitel 4.14 Redundans och återställning och kapitel 4.13.6 Radera och kassera it-utrustning. För krav och stöd avseende arkivering hänvisas till Riksarkivet.

Innehåll

Inledning

1. Inledning

Digitalisering ger många fördelar, men leder också till nya risker genom att komplexiteten i it-miljön och behovet av kontinuerlig uppkoppling till internet ökar. Detta medför större exponering av information och informationssystem mot andra organisationer och deras informationssystem. Bristande it-säkerhet kan medföra att organisationer inte har åtkomst till sin information, att information kan komma obehöriga till del eller att informationen blir förvanskad eller förstörd. It-säkerhet handlar om att införa säkerhetsåtgärder för att skydda information i informationssystem. Tillräckliga säkerhetsåtgärder för informationssystemen är en förutsättning för att digitaliseringens möjligheter ska kunna tas tillvara.



Informationssystem kan se olika ut. De kan exempelvis användas som stöd för kontorsarbete (kontors-it), men även för att interagera med maskiner, fordon och annan utrustning[8] (cyberfysiska system). I vägledningen görs ingen skillnad mellan de olika typerna av informationssystem, utan vägledningen kan med fördel användas som stöd för att införa, förvalta, följa upp och utvärdera säkerhetsåtgärder för alla informationssystem oavsett användningsområde. När det gäller cyberfysiska system kan dock ytterligare överväganden behöva göras.

Både ett enskilt informationssystem och informationssystem samlade i en it-miljö behöver skydd mot olika typer av risker. Rena handhavandefel och systemfel står för de flesta it-incidenter som rapporteras in till MSB, men även risken för avsiktliga angrepp och naturhändelser behöver hanteras. Vägledningen utgår från ett allriskperspektiv, det vill säga att alla olika typer av risker ska beaktas.

8. Exempelvis sensorer som kan inhämta data från omgivningen.

1.1 Begreppsförklaringar

I denna vägledning ges följande begrepp nedanstående betydelse:[9]

Begrepp	Förklaring
behandling	En åtgärd eller kombination av åtgärder beträffande information, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.
extern aktör[10]	Annan organisation, inhyrd personal eller motsvarande som behandlar organisationens information, exempelvis leverantör.
informationssystem	Applikationer, tjänster eller andra komponenter som hanterar information. I begreppet ingår också nätverk och infrastruktur. Informationssystem omfattar till exempel datorprogram, appar, datorer, skrivare, hårddiskar, mobiltelefoner, wifi och vissa delar i styr- och reglersystem.
informationssäkerhet	Bevarande av konfidentialitet, riktighet och tillgänglighet hos information.
informationsägare	Befattning som ansvarar för att säkerställa att information har tillräckligt skydd.
it-miljö	Den samlade mängden informationssystem som används för att behandla information som organisationen ansvarar för. It-miljö omfattar både informationssystem som hanteras internt och som är utkontrakterade.
it-säkerhet	It-relaterade tekniska säkerhetsåtgärder för att upprätthålla informationssäkerhet.
medarbetare	Egen och inhyrd personal.
produktionsmiljö	Den del av it-miljön som organisationen använder för att bedriva sin verksamhet.
redundant funktion	Två eller flera, identiska eller olika, funktioner som oberoende av varandra uppfyller samma syfte.
riskbedömning	Arbetssätt för att identifiera, analysera och värdera risker.
systemadministrativ behörighet	Behörighet med priviligierade rättigheter som ger möjlighet att förändra grundläggande funktioner och säkerhetsfunktioner i ett informationssystem.
systemägare	Befattning som ansvarar för att införa, förvalta, följa upp och utvärdera säkerhets-åtgärderna i ett informationssystem.
sårbarhet	Brist i eller avsaknad av säkerhetsåtgärd som möjliggör att ett eller flera hot kan realiseras.
säkerhetsfunktion	Teknisk funktion som svarar för viss del av säkerheten, såsom behörighetskontrollsystem, säkerhetsloggning, intrångsdetektering, intrångsskydd eller skydd mot skadlig kod.
säkerhetsloggning	Automatisk eller manuell registrering av säkerhetsrelaterade händelser.
testmiljö	En från produktionsmiljön avskild del av it-miljön som används för att testa informations-system innan användning i produktionsmiljön.

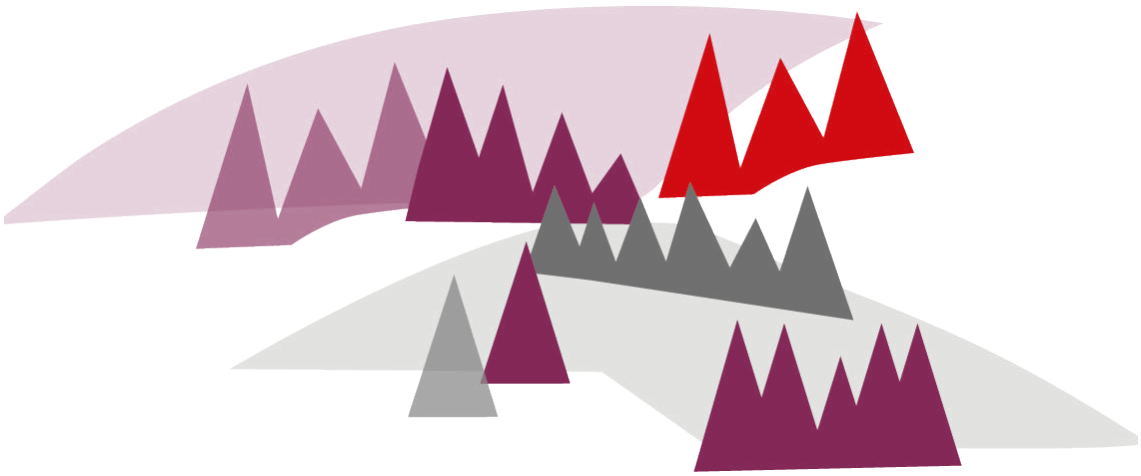
9. Underlag för begreppsförklaringarna är främst hämtade från MSB:s föreskrifter om säkerhetsåtgärder i informations-system för statliga myndigheter (MSBFS 2020:7) och MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

10. För statliga myndigheter finns begreppsdefinition i 3 § MSB:s föreskrifter om säkerhetsåtgärder i informationssystem (MSBFS 2020:7): Extern aktör – Leverantör som inte omfattas av dessa föreskrifter, inhyrd personal eller motsvarande.

Begrepp	Förklaring
utkontraktera	Att lägga ut en del av organisationens information, tjänster eller verksamhet till en extern aktör, till exempel en leverantör av it-drift.
utbildningsmiljö	En från produktionsmiljön avskild del av it-miljön där användare ges möjlighet att öva på att använda funktionerna i ett informationssystem.
utvecklingsmiljö	En från produktionsmiljön avskild del av it-miljön som används för att utveckla nya och förbättra befintliga informationssystem innan systemen testas i en från produktionsmiljön avskild del av it-miljön.

1.2 Koppling till systematiskt informationssäkerhetsarbete

Säkerhetsåtgärderna i denna vägledning utgör en del av de säkerhetsåtgärder som en organisation behöver införa för att skydda sin information och sina informationssystem. Arbetet med att införa vägledningens säkerhetsåtgärder är en del av organisationens systematiskt och riskbaserade informationssäkerhetsarbetet. MSB:s metodstöd för systematiskt och riskbaserat informationssäkerhetsarbete[11] är utformat för att stödja olika typer av organisationer i olika typer av organisationer i att utforma, förbättra och följa upp ett systematiskt och riskbaserat informationssäkerhetsarbete, bland annat gällande ansvar, informationsklassning, riskbedömning, incidenthantering och kontinuitetshantering. Ytterligare stöd för att följa upp sitt systematiska informationssäkerhetsarbete tillhandahålls i MSB:s verktyg Infosäkkollen.



11. www.informationssakerhet.se/metodstodet/.

Grundläggande förutsättningar

2. Grundläggande förutsättningar

2.1 Ansvar

2.1.1 Syfte

Det behöver vara tydligt i organisationen vem som ska se till att tillräckliga säkerhetsåtgärder införs i ett informationssystem, och att det finns resurser för att anpassa säkerhetsåtgärderna när organisationens behov eller förhållanden i omvärlden förändras.

2.1.2 Krav

Organisationen ska se till att

1. varje informationssystem har en systemägare[12]
2. systemägaren ansvarar för att införa, förvalta, följa upp och utvärdera säkerhetsåtgärder[13]
3. systemägaren har resurser för att införa och förvalta tillräckliga säkerhetsåtgärder i informationssystemen[14].

2.1.3 Ansvar för informationssäkerhetsarbete

Ledningen har det övergripande ansvaret att styra och inrikta informationssäkerhetsarbetet samt säkerställa att det finns tillräckliga resurser och mandat. En vanlig ansvarsfördelning i övrigt är följande:

- CISO ansvarar för att leda och samordna informationssäkerhetsarbetet.
- Informationsägaren ansvarar för att genomföra informationsklassning och riskbedömning för den information som hanteras i dennes verksamhet.
- Systemägaren ansvarar för att informationssystemet har de tekniska säkerhetsåtgärder som behövs för att skydda informationen som hanteras där, och att det finns arbetssätt för att utvärdera och uppdatera säkerhetsåtgärder så att de ger ett tillräckligt skydd för informationssystemet.

Det ska framgå av ledningens styrning och inriktning av informationssäkerhetsarbetet vilka som är systemägare för organisationens olika informationssystem samt vem som har ett övergripande ansvar för hela respektive delar av it-miljön, exempelvis utvecklings- och testmiljö.

12. Myndigheten ska, för varje informationssystem, tydliggöra vilken befattning som ansvarar för att införa, förvalta, följa upp och utvärdera säkerhetsåtgärder (systemägare). MSBFS 2020:7 2 kap. 1 §.

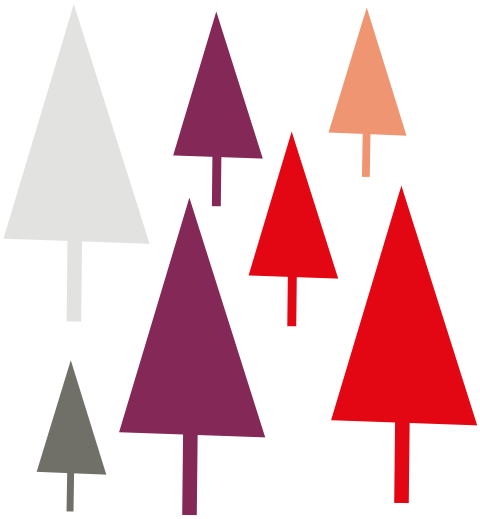
13. Myndigheten ska, för varje informationssystem, tydliggöra vilken befattning som ansvarar för att införa, förvalta, följa upp och utvärdera säkerhetsåtgärder (systemägare). MSBFS 2020:7 2 kap. 1 §.

14. När myndigheten utformar informationssäkerhetsarbetet ska den säkerställa att informationssäkerhetsarbetet tilldelas nödvändiga resurser, MSBFS 2020:6 5 § 3 p.

2.1.4 Varje informationssystem har en systemägare

En organisation har i regel ett stort antal olika informationssystem. Det är lämpligt att en systemägare har ansvar för flera informationssystem av samma typ. Exempelvis kan en systemägare ges ansvar för organisationens administrativa system (ekonomi, personal), en annan för fastighetsautomation (el, kyla, hissar och liknande), en tredje för it-miljöns nätverk (routrar, switchar, DNS, DHCP och liknande), en fjärde för databaser, en femte för webbmiljö etcetera. En systemägare kan även ges ansvar för hela eller delar av en it-miljö, exempelvis produktionsmiljö, utvecklingsmiljö, testmiljö eller utbildningsmiljö. Det är lämpligt att att organisationens storlek och it-miljöns utformning avgör hur ansvaret fördelas.

Systemägarna i en organisation behöver gemensamt och regelbundet, både sinsemellan och med berörd informationsägare, diskutera framtida förändringsbehov i sina informationssystem, till exempel utifrån nya risker, verksamhetsförändringar, ny teknik eller identifierade sårbarheter.



2.1.5 Införa, förvalta, följa upp och utvärdera

Systemägaransvaret innebär att införa, förvalta, följa upp och utvärdera att de införda säkerhetsåtgärderna är tillräckliga över tid. Uppföljning och utvärdering bör göras regelbundet. Om brister upptäcks i skyddet av informationen, behöver systemägaren se till att dessa blir åtgärdade och informera CISO och berörda informationsägare. Behov av ytterligare säkerhetsåtgärder under fredstida krissituation samt inför och vid höjd beredskap behöver också beaktas.

För att kunna ta sitt ansvar behöver systemägaren bland annat veta

- vilken information som behandlas i informationssystemet och hur den är klassad
- vem eller vilka som är informationsägare
- vilken hård- och mjukvara som informationssystemet består av
- vilka beroenden som finns av andra interna och externa informationssystem, samt
- vilka säkerhetsåtgärder som är införda.

Systemägaren behöver också se till att det finns arbetssätt för att införa, förvalta, följa upp och utvärdera säkerhetsåtgärder i informationssystemet och informera ledningen att det finns tillräckligt med resurser så att systemägaren kan utföra sin uppgift.

2.1.6 Resurser, kompetens och kunskap

Som stöd för systemägarnas löpande arbete kan det behöva tillsättas ytterligare resurser för teknisk förvaltning och drift. Systemägaren behöver också utse en förvaltningsorganisation för informationssystemet, exempelvis en teknisk förvaltare som stöd för det operativa arbetet. Vid budgetering och resurssättning behöver systemägaren ta hänsyn till att det behövs bemanning med rätt kompetens. I detta ligger även att kunna bidra med resurser till incidentorganisationen

när incidenter inträffar. Det finns organisationer som stänger ned informationssystem under vissa tider när det saknas resurser för att arbeta med eventuella incidenter.

Systemägaren och dennes medarbetare behöver förstå hur informationssystemet är utformat, dess syfte, begränsningar och hur det är integrerat med övriga system. Behovet av kompetens kan skifta över informationssystemets livscykel, från arbetet med utveckling och anskaffning till driftsättning, uppdatering, uppgradering respektive avställning och avveckling. Systemägaren behöver kartlägga och planera för hur behovet av kompetens för att utveckla, drifta och förvalta informationssystemet ska lösas.

Brister i kompetens kan hanteras med hjälp av utbildning eller genom att anlita externa aktörer (konsulter). Externa aktörer kan anlitas för att få extra stöd med den egna driften eller stötta med beställarkompetens inför anskaffning och utveckling. En organisation som gör sig beroende av externa resurser för tidskritiska arbetsuppgifter behöver hantera risken att resurserna inte finns tillgängliga när organisationen behöver dem. Att helt förlita sig på externa resurser för beställarkompetens vid anskaffning och utveckling kan också innebära risker, eftersom organisationen kan ha svårt förstå vad som är anskaffat eller utvecklat och hur det svarar mot organisationens behov. Organisationen behöver även ställa krav som minskar risken för inlåsningseffekter, det vill säga svårigheter att avsluta en leverantörrelation utan att riskera oförutsedda kostnader.

2.1.7 Dialog med informationsägare

Systemägaren behöver ha en dialog med berörda informationsägare inom organisationens olika verksamheter för att införa de säkerhetsåtgärder som ger rätt nivå av skydd för informationssystemet. Behovet av säkerhetsåtgärder identifieras utifrån de informationsklassningar och riskbedömningar som informationsägaren har genomfört, samt systemägarens egna riskbedömningar för informationssystemet.

2.2 Omvärldsbevakning

2.2.1 Syfte

Organisationen behöver bedriva omvärldsbevakning för att kunna identifiera och hantera hot mot och sårbarheter i organisationens informationssystem.

2.2.2 Krav

Organisationen ska se till att bedriva omvärldsbevakning för att[15]

1. identifiera potentiella hot mot sina informationssystem
2. identifiera potentiella sårbarheter i sina informationssystem
3. hitta stöd för hanteringen av hot mot och sårbarheter i sina informationssystem.

2.2.3 Lämpliga källor

En organisation behöver följa utvecklingen på informations- och cybersäkerhetsområdet för att hålla sig uppdaterad om nya hot, sårbarheter och teknisk utveckling. Organisationen behöver välja relevanta källor för sin omvärldsbevakning, exempelvis

- det nationella cybersäkerhetscentret (Försvarets Radioanstalt, Försvarsmakten, MSB och Säkerhetspolisen) gällande cyberangrepp
- expertmyndigheter, exempelvis
  - Integritetsskyddsmyndigheten (IMY) gällande personuppgiftsbehandling
  - MSB inklusive CERT-SE gällande informations- och it-säkerhet
  - Säkerhetspolisen gällande säkerhetsskydd
  - Post- och telestyrelsen (PTS) gällande elektronisk kommunikation
  - Försvarets materielverk (FMV) gällande certifiering av it-säkerhet i produkter och system
- branschorganisationer
- internationella aktörer på cybersäkerhetsområdet, såsom ENISA[16], NIST[17], CISA[18], CIS[19], OWASP[20].

Vilken information som är relevant beror på vilka informationssystem som organisationen använder i sin verksamhet. Systemägaren bör ta del av de hotbilder och hotkataloger som är relevanta.

När det gäller sårbarheter så är det lämpligt att systemägaren prenumererar på nyhetsbrev och varningar från bland annat:

- leverantörerna av organisationens informationssystem och it-produkter
- CERT-SE – Sveriges nationella CSIRT (Computer Security Incident Response Team)[21] – hos MSB.

Den tekniska utvecklingen kan lämpligtvis följas genom att organisationen håller sig uppdaterad rörande vilka produktförändringar som organisationens leverantörer planerar. Även den övergripande utvecklingen av ny teknik behöver följas, exempelvis genom facktidningar på it-området.

Underlagen från omvärldsbevakningen underlättar arbetet med att hantera potentiella hot och sårbarheter i informationssystem genom att systemägaren enklare kan identifiera vilka åtgärder som behöver genomföras direkt (exempelvis säkerhetsuppdateringar) respektive vilka som behöver hanteras mer långsiktigt (exempelvis att support kommer att upphöra för äldre versioner).

15. Myndigheten ska bedriva omvärldsbevakning för att underlätta identifiering och hantering av hot mot och sårbarheter i myndighetens informationssystem. MSBFS 2020:7 2 kap. 2 §.

16. European Union Agency for Cyber Security.
17. National Institute of Standards and Technology (USA).
18. Cyber Security and Infrastructure Security Agency.
19. Center for Internet Security.
20. Open Web Application Security Project.
21. www.cert.se.

2.3 Riskbedömning

2.3.1 Syfte

Organisationen behöver identifiera, analysera och värdera risker för att kunna vidta ändamålsenliga och proportionerliga säkerhetsåtgärder för sina informationssystem.

2.3.2 Krav

Organisationen ska

1. se till att det finns ett arbetssätt för att identifiera, analysera och värdera risker[22]
2. genomföra riskbedömning av produktionsmiljön i sin helhet[23]
3. genomföra riskbedömning av enskilda informationssystem var för sig eller samlat för informationssystem i produktionsmiljön med liknande funktion, uppbyggnad och användningsområde.[24]

Organisationen bör

1. se till att det även genomförs en riskbedömning för organisationens[25]
   a. utvecklingsmiljö
   b. testmiljö
   c. utbildningsmiljö.
2. ge systemägaren i uppgift att säkerställa att riskbedömningen genomförs för de informationssystem som systemägaren ansvarar för.[26]

22. MSBFS 2020:6 6 § 2 p Myndigheten ska säkerställa att informationssäkerhetsarbetet är systematiskt och riskbaserat genom att identifiera, analysera och värdera risker för sin information (riskbedömning).

23. MSBFS 2020:7 2 kap. 3 § Myndigheten ska genomföra riskbedömning för enskilda informationssystem och myndighetens produktionsmiljö i sin helhet.

24. MSBFS 2020:7 2 kap. 3 § Myndigheten ska genomföra riskbedömning för enskilda informationssystem och myndighetens produktionsmiljö i sin helhet.

25. Allmänt råd till MSBFS 2020:7 2 kap. 3 § Riskbedömningar bör även genomföras för myndighetens utvecklings-, test- respektive utbildningsmiljö.

26. Allmänt råd till MSBFS 2020:7 2 kap. 3 § Myndigheten bör överväga att ge systemägaren för berört informationssystem i uppgift att säkerställa att riskbedömning genomförs.

2.3.3 Att bedöma risker

Arbetet med att bedöma risker ger ett underlag för beslut om vilka säkerhetsåtgärder som behöver införas. Riskbedömningar höjer riskmedvetenheten och ökar kunskapen om hot mot och sårbarheter i organisationens it-miljö samt vilka konsekvenser de kan få för organisationen.

Riskbedömningen går förenklat ut på att besvara de fyra frågorna ”Vad kan hända?”, ”Varför kan det hända?”, ”Vad blir konsekvenserna?” och ”Hur sannolikt är det att det inträffar?”. Underlag för att i riskbedömningen identifiera hot och sårbarheter samt bedöma konsekvens och sannolikhet kommer bland annat från omvärldsbevakningen. Konsekvenser kan till exempel bestå av merarbete, ekonomisk förlust, förlorade möjligheter, försämrad hälsa (i värsta fall dödsfall) samt ekonomiska kostnader för återställning och skadat förtroende.

Målsättningen med riskbedömning är att beskriva samtliga relevanta hot och sårbarheter som kan leda till negativ påverkan på informationssystemens funktion. Det är viktigt att lägga resurser och tid på arbetet med riskbedömning för att säkerställa att så många relevanta risker som möjligt identifieras. Systemägaren behöver vid sin riskbedömning för informationssystem och it-miljö exempelvis beakta:

- informationen – behovet av skydd för den information som hanteras i informationssystemet (bedöms utifrån informationsägarens informationsklassning och riskbedömning)
- informationssystemen – hur och till vad de används
- utrustningen – klienter, servrar, mobiltelefoner, skrivare, nätverkskomponenter, usb-minnen
- mjukvaran – operativsystem, drivrutiner, firmware och applikationer
- de fysiska förutsättningarna – tillträde, serverrum, brandskydd, elförsörjning och kyla/värme

- arbetssätten – regler och stöd för säker drift och förvaltning
- resurserna – tillgång till personal med rätt kompetens
- beroendena – av leverantörer och tjänster.

Information om hot, sårbarheter och risker är ofta känslig. Den behöver hanteras på ett säkert sätt och endast delas med de som behöver ha kunskap om den.

2.3.4 Arbetssätt för att identifiera, analysera och värdera risker

I organisationen ska det finnas ett beslutat arbetssätt för att identifiera, analysera och värdera risker (riskbedömning). För att arbetet med riskbedömning ska bedrivas på ett enhetligt sätt behöver alla systemägare använda organisationens arbetssätt. Arbetssättet bör visa vilka befattningar som ansvarar för att riskbedömning genomförs, när och i vilka situationer riskbedömning ska genomföras, och vilka kriterier och nivåer som ska användas för att bedöma konsekvens och sannolikhet. De som genomför riskbedömningarna behöver dokumentera resultatet. I arbetet ingår att ge systemägaren förslag på åtgärder som minskar riskerna. Det är lämpligt att använda resultatet från riskbedömningarna för att både ta fram organisationens samlade riskbild och se om riskbilden ändras över tiden.

Som underlag för sin riskbedömning behöver systemägaren ha en dialog med informationsägaren för att få kunskap om de risker som informationsägaren har identifierat och som är relevanta för systemägarens riskbedömning av informationssystem och it-miljö.

För mer information om arbetssätt för bedömning av risker, se Metodstödet för systematiskt informationssäkerhetsarbete på Informationssakerhet.se/metodstodet.

2.3.5 Riskbedömning av it-miljö, produktionsmiljö och enskilda informationssystem

Riskbedömningar behöver göras för enskilda informationssystem och produktionsmiljön, både dess delar och i sin helhet. Organisationen behöver ha ett arbetssätt för att löpande identifiera och bedöma de tekniska riskerna som är kopplade till organisationens it-miljö och dess ingående delar, så att riskerna kan åtgärdas med hjälp av olika typer av säkerhetsåtgärder. Många organisationer har utöver produktionsmiljön även andra miljöer som också bör riskbedömas. Det är vanligt med en:

- miljö för utveckling av informationssystem där utvecklare kan programmera och enhetstesta ny eller förändrad programkod med stöd av utvecklingsprogram (utvecklingsmiljö)
- miljö för funktions-, system- och användartestning av informationssystem där testare kan säkerställa att de funktioner som utvecklats i utvecklingsmiljön motsvarar kravställningen och att informationssystemet kommer att fungera på avsett sätt vid driftsättning (testmiljö)
- miljö för utbildning av användare där de ges möjlighet att öva på att använda funktionerna i ett informationssystem utan att riskera att påverka information och funktion i produktionsmiljön (utbildningsmiljö).

I de fall organisationen, som del av sin verksamhet, erbjuder externa aktörer tjänster inom utveckling, testning eller utbildning, ska den delen av it-miljön som används för detta betraktas som produktionsmiljö. Detta gäller exempelvis organisationer som tillhandahåller tjänster för utveckling och testning men även skolor och lärosätens utbildningsverksamhet. De informationssystem som utvecklas eller testas av den externa aktören i en sådan miljö hanterar inte organisationens information och ska därför inte ses som en del av organisationens egen

informationsbehandling.[27] Riskerna för att tillåta externa aktörer att på detta sätt behandla sin information[28] i organisationens produktionsmiljö behöver bedömas och hanteras.

Olika risker kan identifieras för enskilda it-system och för produktionsmiljön som helhet. Att bara sammanställa riskerna för varje informationssystem räcker inte som underlag för att bedöma risken i produktionsmiljön. När enskilda informationssystem kopplas samman i en it-miljö kan riskerna samverka och förändras, till och med förstärkas. Detta gör att riskerna för produktionsmiljö, utvecklingsmiljö, testmiljö, utbildningsmiljö samt it-miljön i sin helhet behöver bedömas särskilt. Riskerna som identifierats för de informationssystem som ingår i respektive miljö utgör ett av flera underlag för den riskbedömningen.

Nedan följer exempel på förhållanden, hot och sårbarheter som de flesta organisationer behöver beakta vid riskbedömning för it-miljön:

- Sårbarheter i autentiseringsfunktioner kan utnyttjas.
- Bristande konto- och behörighetshantering.
- Svagheter i it-miljöns arkitektur, till exempel brister i segmentering, filtrering och virtualisering.
- Bristande underhålls- och uppdateringsrutiner.
- Leverantörer eller andra externa aktörer ges åtkomst till hela eller delar av organisationens interna it-miljö.
- Behov av att byta leverantör av hårdvara, mjukvara eller tjänster.
- Otillräcklig förvaltning av äldre informationssystem.
- Bristande härdning av utrustning så att onödiga tjänster och protokoll är aktiva.
- Det saknas kontroll eller begränsning av vilken mjukvara som får köras eller installeras.
- Utrustning som inte är sanktionerad kan anslutas till nätverket.
- Privat utrustning, som inte kan eller får förvaltas av organisationen, kan anslutas till organisationens interna it-miljö.
- Bristande loggning och kunskap om hur man upptäcker och hanterar incidenter.
- Bristande förmåga att kunna återställa information från säkerhetskopior.
- Bristande fysisk säkerhet som kan medföra ökad risk för brand, översvämning eller inbrott.
- Avsaknad av tillräcklig kompetens som ger beroenden av nyckelpersoner eller externa experter.
- Felaktig hantering av krypteringsnycklar vilket kan medföra informationsläckage.
- Avsaknad av, eller felaktig, dokumentation om informationssystem och beroenden.
- Avsaknad av tillräcklig redundans i viktiga informationssystem.
- Mjukvara utan skydd mot enkla handhavandefel av användare eller administratörer.
- Leverantören för en utkontrakterad tjänst utsätts för en överbelastningsattack.
- Problem hos nätverksoperatören medför att internet är oåtkomligt.
- Kabel för elektricitet eller tele- och datakommunikation grävs av.
- Alla rättsliga krav är inte omhändertagna.
- Bristande kapacitet i vpn-lösning som försvårar vid hög belasting – exempelvis vid behov av distansarbete.

27. Sådan informationssystem omfattas därför inte av kraven i MSB:s föreskrifter om säkerhetsåtgärder i informationssystem (MSBFS 2020:7).

28. Exempelvis programkod, skript eller tester i form av kartläggningar av it-miljön, angreppsmetoder med mera.

2.3.6 Riskbedömning av utvecklingsmiljö, testmiljö och utbildningsmiljö

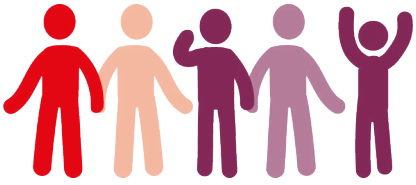
Utöver produktionsmiljön bör organisationen riskbedöma sin utvecklingsmiljö, testmiljö och utbildningsmiljö om de har sådana. Beroende på vilken information och vilka informationssystem som finns i dessa miljöer kan det vara aktuellt att, utöver de risker som nämns ovan, även beakta risker som är speciella för dessa miljöer utifrån vilken information som hanteras och vilka säkerhetsåtgärder som finns på plats.

2.3.7 Att åtgärda risker

Det som framkommer i riskbedömningen behöver dokumenteras i form av en uppställning över identifierade risker, med tillhörande riskbedömning. Arbete med att åtgärda risker inkluderar att ta fram en åtgärdsplan som beskriver:

- vem som ska införa en säkerhetsåtgärd
- när den senast ska vara införd
- hur kontroll ska ske av att den är införd och att den ger avsett skydd.

Säkerhetsåtgärder som behöver införas tas fram i dialog mellan systemägare och informationsägare. Val och utformning av säkerhetsåtgärder behöver baseras på den informationsklassning och riskbedömning informationsägaren gjort utifrån sin verksamhet, men också de riskbedömningar som systemägaren gjort utifrån sin kunskap om it-miljön i sin helhet. Dialog behöver även hållas med andra stödfunktioner (till exempel juridik) för att systemägaren ska kunna skaffa sig en uppfattning om vilka faktiska risker som behöver åtgärdas.



2.4 Dokumentation av it-miljön

2.4.1 Syfte

Organisationen behöver dokumentera sin it-miljö, dess olika delar, ingående informationssystem, beroenden samt den hård- och mjukvara som används i it-miljön för att kunna bedriva säker drift och förvaltning.

2.4.2 Krav

Organisationen ska för samtliga informationssystem ha uppdaterad dokumentation om[29]

1. vilken hård- och mjukvara som används i varje informationssystem
2. vilka beroenden som finns till andra interna informationssystem
3. vilka beroenden som finns till informationssystem hos externa aktörer
4. om informationssystemet behandlar information i behov av utökat skydd
5. om informationssystemet är särskilt viktigt för organisationens möjlighet att bedriva sin verksamhet.

Organisationen bör

1. använda tekniskt stöd för att säkerställa att dokumentation om exempelvis informationssystemets hård- och mjukvara samt beroenden är uppdaterad[30]
2. beskriva beroenden mellan informationssystem i en systemkarta eller motsvarande[31]
3. använda informationsklassning för att identifiera vilka informationssystem som behandlar information i behov av utökat skydd.[32]

29. MSBFS 2020:7 2 kap. 4 § Myndigheten ska upprätthålla uppdaterad dokumentation över 1. hård- och mjukvara som används i varje enskilt informationssystem, 2. beroenden mellan olika interna informationssystem respektive beroenden av informationssystem hos externa aktörer, 3. vilka informationssystem som behandlar information som har behov av utökat skydd, och 4. vilka informationssystem som är centrala för myndighetens förmåga att utföra sitt uppdrag.

30. Allmänt råd till MSBFS 2020:7 2 kap. 4 § Tekniskt stöd bör användas för att upprätthålla uppdaterad dokumentation.

31. Allmänt råd till MSBFS 2020:7 2 kap. 4 § Beroenden bör tydliggöras i en systemkarta eller motsvarande.

32. Allmänt råd till MSBFS 2020:7 2 kap. 4 § Information som är i behov av utökat skydd bör identifieras med stöd av informationsklassning enligt 6 § MSBFS 2020:6.

2.4.3 Dokumentera it-miljö och informationssystem

Systemägaransvaret innebär att införa, förvalta, följa upp och utvärdera att införda säkerhetsåtgärder är tillräckliga över tid. För att kunna göra detta behöver systemägaren säkerställa att det finns tillräcklig dokumentation om de informationssystem eller den del av it-miljön som hen ansvarar för.

Dokumentationen behöver visa hur it-miljön ser ut, bland annat vilka produkter och tjänster som används för att bedriva verksamheten. Det är även viktigt att kartlägga beroenden mellan informationssystem i den egna it-miljön och beroenden till informationssystem hos externa aktörer, exempelvis samarbetspartner, tjänsteleverantörer och underleverantörer. Organisationen behöver även dokumentera övrig information som krävs för att drift och förvaltning av it-miljö och informationssystem ska kunna bedrivas på ett säkert sätt. Det är därför lämpligt att dokumentera mer än vad som kravställs i föreskrifterna. För att få nödvändig överblick över sin it-miljö är det lämpligt att organisationen minst dokumenterar följande för varje informationssystem:

1. informationssystemets syfte, bland annat inom vilken verksamhet det används
2. vilken information som behandlas i informationssystemet
3. vem eller vilka som är informationsägare för informationen i informationssystemet
4. informationsägarens klassning av informationen som behandlas i informationssystemet:
    - om informationssystemet behandlar personuppgifter
    - om informationssystemet behandlar information som omfattas av sekretess
    - om informationen i övrigt, efter informationsklassning, behöver utökat skydd avseende konfidentialitet, riktighet eller tillgänglighet
5. vilken hård- och mjukvara som informationssystemet består av
6. vilka beroenden, inklusive integrationer, som finns till andra interna informationssystem
7. vilka beroenden, inklusive integrationer, som finns till informationssystem hos externa aktörer
8. vem eller vilka som har behörighet att få tillgång till informationssystemet och i vilket syfte
9. vilka säkerhetsåtgärder som är införda
10. hur prioriterat informationssystemet är utifrån dess betydelse för organisationen att bedriva sin verksamhet
11. systemägarens riskbedömning för informationssystemet
12. kontaktuppgifter till leverantörer och myndigheter som stöd vid incidenter.

När en systemägare sammanställer dokumentationen för ett informationssystem behöver hen ta fram vissa delar själv medan andra underlag hämtas från olika källor. Tekniskt stöd för kartläggning av it-miljöer kan ge ett bra stöd i dokumentationsarbetet. Det är lämpligt att också hämta in underlag från CISO, berörda informationsägare och den som leder och samordnar organisationens kontinuitetshantering.

Systemägaren bör, som en del av dokumentationen, ta fram systemkartor som beskriver informationssystemens logiska och fysiska placering i it-miljön. Systemkartorna behöver inte göras komplicerade. Målet är att visuellt beskriva it-miljön så att förvaltning, felsökning och dokumentation underlättas. Systemkartorna kan även tas fram med hjälp av tekniskt stöd.

Är informationsbehandling utkontrakterad ska det framgå av dokumentationen. Detta gäller oavsett om det är en myndighet som anlitar en annan myndighet eller om en organisation anlitar en leverantör för exempelvis drift och förvaltning av informationssystem.

Det är lämpligt att dokumentation som behöver vara åtkomlig för flera olika roller, exempelvis driftpersonal, CISO och dataskyddsombud, lagras i gemensamma förteckningar. Eftersom förteckningen kommer att innehålla detaljerad information om många informationssystem behöver organisationen vidta lämpliga säkerhetsåtgärder utifrån informationsklassning och riskbedömning. Det är lämpligt att särskilt beakta ökade risker orsakade av att information aggregeras. Exempelvis kan det vara nödvändigt att begränsa vilka som har åtkomst till olika delar av förteckningen.

2.4.4 Hårdvara, mjukvara och beroenden

Hårdvara kan exempelvis utgöras av stationära och bärbara klienter, servrar, nätverksutrustning (såsom routrar, switchar, brandväggar och accesspunkter), skrivare, lagringsnätverk, IP-telefoner, mobiltelefoner, läsplattor och IoT-enheter[33]. Det är lämpligt att det i förteckningen, för varje hårdvara, åtminstone framgår

- typ av hårdvara inklusive modellnummer
- identifierare, exempelvis maskinnamn, mac-adress, nätverksadress och ip-adress
- till vilket informationssystem hårdvaran hör.

Det är lämpligt att det i förteckningen, för all typ av mjukvara, inklusive operativsystem, drivrutiner, firmware och applikationer som är installerad på hårdvaran, åtminstone framgår

- vilken version mjukvaran har
- när mjukvaran installerades
- när mjukvaran senast uppdaterades.

När det gäller dokumentation av nätverkstrafik till och från andra interna och externa informationssystem, är det lämpligt att det i förteckningen åtminstone framgår

- mellan vilka nätverkssegment nätverkstrafiken går
- mellan vilka informationssystem (interna och externa) nätverkstrafiken går
- berörd information
- protokoll, både för kommunikation och kryptering
- portar
- trafikens riktningar, inklusive var den initeras och termineras.

2.4.5 Tekniskt stöd för dokumentation

Dokumentationen måste hållas uppdaterad för att kunna stödja säker drift och förvaltning av organisationens it-miljö. Mjukvara som används i it-miljöns olika informationssystem ändras vid uppdateringar, nyinstallation eller avinstallation, och hårdvara flyttas ibland mellan olika delar i it-miljön eller mellan olika informationssystem. Detta gör att uppdateringar kan behöva göras ofta. Arbetet med att dokumentera förändringarna, särskilt i en mer omfattande it-miljö, underlättas betydligt av tillgången till tekniskt stöd.

Den som är ansvarig för drift och förvaltning av organisationens it-miljö bör använda automatiserade verktyg för att aktivt identifiera och upprätthålla en sammanställning över

- den hårdvara (nätverks- och användarutrustning) som är inkopplad i it-miljön
- den mjukvara (operativsystem, drivrutiner, firmware och applikationer) som används i it-miljön
- nätverkstrafik (både intern och extern) i it-miljön.

Sammanställningen kan användas för att kontrollera att ingen obehörig hård- eller mjukvara har anslutits till it-miljön samt att all mjukvara som kräver programvarulicens också har en sådan.

33. Internet of Things-enheter eller ”sakernas internet”.

Använd gärna it-stöd för att skapa systemkartor som kan visualisera informationssystemens logiska och fysiska placering i it-miljön inklusive dataflöden. Systemkartor underlättar förvaltning av och felsökning i it-miljön.

Mobila enheter, som mobiltelefoner, är normalt inte direkt anslutna till nätverket utan synkroniserar data via någon typ av tjänst. En sammanställning över dessa enheter kan med fördel göras via en programvara för Mobile Device Management (MDM).

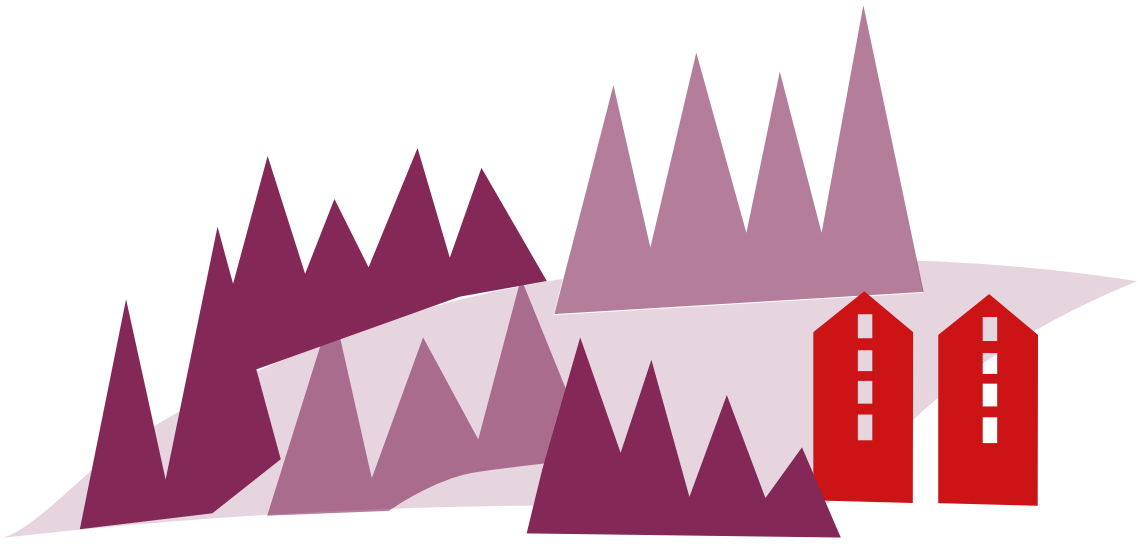
2.4.6 Information i behov av utökat skydd

Både information och informationssystem kan behöva utökat skydd utifrån ett eller flera av de tre informationssäkerhetsperspektiven: konfidentialitet, riktighet och tillgänglighet. Behovet av utökat skydd identifieras genom informationsägarens klassning av information. Bedömningen av informationssystemens behov av skydd utgår från vilken information som behandlas där och hur den har klassats. Förutom informationsklassning ska resultat från riskbedömning också användas vid val av säkerhetsåtgärder. Alla informationssystem ska skyddas med tillräckliga säkerhetsåtgärder. Om information i behov av utökat skydd behandlas, behöver informationssystemets säkerhetsåtgärder motsvara det ökade skyddsbehovet.

2.4.7 Informationssystem som är särskilt viktiga för organisationen

Organisationen behöver identifiera vilka informationssystem som är särskilt viktiga för organisationens förmåga att bedriva sin verksamhet. Underlag för att identifiera sådana informationssystem kan hämtas från kontinuitetsplaneringen och informationsklassningen. Vid avvikelser, incidenter, fredstida kris eller höjd beredskap är det viktigt för organisationen att på förhand ha prioriterat vilka informationssystem som behöver fungera.

Prioriteringsordningen mellan informationssystemen utifrån interna och externa krav behöver fastställas av organisationens ledning som ett led i ansvaret för organisationens verksamhet.



Utveckling, anskaffning och utkontraktering

3. Utveckling, anskaffning och utkontraktering

3.1 Kravställning

3.1.1 Syfte

Inför utveckling eller anskaffning av informationssystem respektive utkontraktering av informationsbehandling, behöver organisationen identifiera vilka krav på säkerhetsåtgärder som ska ställas för att kunna ge information och informationssystem ett tillräckligt skydd.

3.1.2 Krav

Organisationen ska[34]

1. vid utveckling, anskaffning eller utkontraktering av informationssystem, identifiera krav på säkerhet avseende
   a. uppdelning i nätverkssegment
   b. filtrering av nätverkstrafik
   c. behörigheter, digitala identiteter och autentisering
   d. kryptering
   e. säkerhetskonfigurering
   f. säkerhetstester och granskningar
   g. ändringshantering, uppgradering och uppdatering
   h. robust och korrekt tid
   i. säkerhetskopiering
   j. säkerhetsloggning och tillhörande analys
   k. övervakning av nätverkstrafik
   l. övervakning av informationssystem inklusive säkerhetsfunktioner
   m. skydd mot skadlig kod
   n. skydd av utrustning
   o. redundans och återställning
   p. kontinuitet under fredstida krissituation samt inför och vid höjd beredskap
   q. arkivering
   r. avveckling
2. dokumentera vilka säkerhetsåtgärder som valts för att möta respektive krav.[35]

Organisationen bör

1. vid val av säkerhetsåtgärder kombinera organisatoriska, administrativa, fysiska och tekniska åtgärder[36]
2. gruppera beslutade säkerhetsåtgärder i olika skyddsnivåer, som bör motsvara de olika konsekvensnivåerna som används vid informationsklassningen[37]
3. vid anskaffning av informationssystem överväga att välja produkter som är certifierade genom tredjepartsgranskning mot etablerad standard.[38]

34. MSBFS 2020:7 3 kap. 1 § Myndigheten ska, vid utveckling, anskaffning eller utkontraktering av informationssystem, identifiera krav på säkerhet avseende 1. uppdelning i nätverkssegment, 2. filtrering av nätverkstrafik, 3. behörigheter, digitala identiteter och autentisering, 4. kryptering, 5. säkerhetskonfigurering, 6. säkerhetstester och granskningar, 7. ändringshantering, uppgradering och uppdatering, 8. robust och korrekt tid, 9. säkerhetskopiering, 10. säkerhetsloggning och tillhörande analys, 11. övervakning av nätverkstrafik, 12. övervakning av informationssystem inklusive säkerhetsfunktioner, 13. skydd mot skadlig kod, 14. skydd av utrustning, 15. redundans och återställning, 16. kontinuitet under fredstida krissituation samt inför och vid höjd beredskap, 17. arkivering, och 18. avveckling.

35. MSBFS 2020:7 3 kap. 1 § Myndigheten ska dokumentera vilka säkerhetsåtgärder som valts för att möta respektive krav.

36. Allmänt råd till MSBFS 2020:6 6 § Vid val av ändamålsenliga och proportionella säkerhetsåtgärder bör myndigheten kombinera organisatoriska, administrativa, fysiska och tekniska åtgärder.

37. Allmänt råd till MSBFS 2020:6 6 § För att underlätta informationssäkerhetsarbetet bör myndigheten gruppera beslutade säkerhetsåtgärder i skyddsnivåer och koppla dem till informationsklassningens konsekvensnivåer.

38. Allmänt råd till MSBFS 2020:7 3 kap. 1 § Vid anskaffning av informationssystem bör myndigheten överväga att välja produkter som är certifierade genom tredjepartsgranskning mot etablerad standard.

3.1.3 Att ställa krav på en säker it-miljö

Arbetet med att identifiera krav på säkerhet behöver utgå från organisationens verksamhetsbehov, resultatet av informationsklassningen och relevanta riskanalyser samt externa krav på informationsbehandlingen och dess skydd i exempelvis författningar, standarder och branschnormer. Dessutom kan ytterligare krav på säkerhetsåtgärder finnas i avtal och överenskommelser.

Kraven på säkerhet kan uppfyllas med hjälp av olika säkerhetsåtgärder, och här bör organisatoriska, administrativa, fysiska och tekniska åtgärder ofta kombineras för att uppnå tillräckligt skydd. Vilken roll som ställer krav respektive uppfyller kraven beror på ansvarsfördelningen i organisationen.

I många organisationer ansvarar informationsägaren för att ta fram krav på informationsbehandlingen samt se till att organisatoriska och administrativa åtgärder införs för att verksamheten ska kunna bedrivas på ett effektivt och säkert sätt. Systemägaren har sedan ett ansvar att införa lämpliga tekniska säkerhetsåtgärder utifrån informationsägarens kravställning på it-miljön och informationssystemen. Systemägaren ansvarar också för att införa de organisatoriska och administrativa säkerhetsåtgärder som krävs för att de informationssystem systemägaren ansvarar för kan driftas på ett effektivt och säkert sätt. Systemägaren och informationsägaren ställer i sin tur krav på den som ansvarar för den fysiska miljön att införa tillräckliga fysiska säkerhetsåtgärder. Den som ansvarar för den fysiska miljön ska införa de organisatoriska och administrativa säkerhetsåtgärder som krävs för att upprätthålla det fysiska skyddet.

De olika säkerhetsåtgärderna som införs i it-miljön ska kunna skydda mot såväl angrepp som andra oönskade händelser, exempelvis handhavandefel. I detta ingår att identifiera krav på säkerhetsåtgärder såsom behörighetshantering, kryptering, säkerhetskopiering, loggning, övervakning, test och granskning.

De olika säkerhetsåtgärderna behöver även ta höjd för att organisationens olika typer av information har olika skyddsbehov. Skyddsbehovet framgår av informationsklassning och riskbedömning. Den som ansvarar för it-miljön bör gruppera de beslutade tekniska säkerhetsåtgärderna i olika skyddsnivåer som motsvarar behovet av skydd för olika typer av information. Genom att organisationen i första hand använder de säkerhetsåtgärder som är godkända på respektive skyddsnivå, kan antalet produkter som används för att upprätthålla en viss säkerhetsfunktion (exempelvis skydd mot skadlig kod) begränsas. Detta underlättar säker förvaltning genom att komplexiteten i it-miljön kan hållas nere och tillgängliga resurser kan användas effektivare när ett mer begränsat antal produkter används.

3.1.4 Anskaffning av informationssystem

En organisation måste ställa rätt säkerhetskrav vid anskaffning av hård- och mjukvara till sin it-miljö. Säkerhetskraven ska utformas utifrån informationsklassning och riskbedömning och omhänderta organisationens behov.

Vid anskaffning av informationssystem ska den som ansvarar för it-miljön säkerställa att organisationen använder modern och uppdaterad hård- och mjukvara med aktuella säkerhetsuppdateringar installerade eller tillgängliga. Många av dagens produkter har dessutom inbyggda funktioner som för över information om till exempel funktionalitet och användning till leverantören. Säkerställ att det går att blockera sådana informationsflöden som organisationen, utifrån informationsklassning och riskbedömning, bedömer vara olämpliga utan att de funktioner hos informationssystem som organisationen behöver inte påverkas.

Innan man anskaffar informationssystem som ska användas för att upprätthålla en säkerhetsfunktion, behöver man kontrollera om sådana funktioner redan finns i existerande hård- och mjukvara men inte är aktiverade.

Om sådana funktioner finns behöver man bedöma om användningen av dessa är tillräckliga för att nå den önskade skyddsnivån, antingen i sig själva eller i samverkan med andra säkerhetsfunktioner. Vid val av säkerhetsfunktioner som ska samverka kan det vara lämpligt att välja produkter som använder olika tekniker till exempel olika operativsystem eller programmeringsspråk. Syftet är att om det finns en sårbarhet i en produkt så kan skyddet som finns i andra produkter fortfarande vara opåverkat. Anskaffningen behöver göras med ett livscykelperspektiv, där man kontrollerar om leverantörens plan för support, uppdateringar och uppgraderingar av informationssystemet stämmer överens med organisationens behov.

Vid anskaffning av informationssystem bör den som ansvarar för it-miljön överväga att välja produkter som är certifierade genom tredjepartsgranskning mot lämplig etablerad standard. Granskningen syftar till att kontrollera att säkerhetskraven är uppfyllda på ett tillfredsställande sätt. Granskningen kan ha olika syften. Det är viktigt att kontrollera att de säkerhetskrav och de konfigurationer som granskningen omfattat är relevanta för organisationen samt att resultatet av granskningen visar att informationen är tillräckligt skyddad.

Resurssättning inför anskaffning av nya informationssystem behöver göras långsiktigt. Utöver anskaffningskostnaden tillkommer kostnader för underhåll, förvaltning och avveckling samt utbyte. Anskaffningskostnaden utgör ofta en mindre del av totalkostnaden.

3.1.5 Utveckling av informationssystem

En organisation måste ställa krav på både funktionalitet och säkerhet vid utveckling av informationssystem till sin it-miljö. Säkerhetskraven ska utformas utifrån informationsklassning och riskbedömning och omhänderta organisationens behov.

Med utveckling av informationssystem avses här att ta fram och förändra mjukvara för att fylla ett verksamhetsbehov av både funktionalitet och säkerhet. Utveckling omfattar både kodning och sammanfogning av färdigkodade moduler för att uppnå vad som efterfrågas.

Lite förenklat kan sägas att det finns två olika huvudmodeller för att utveckla mjukvara. I den ena huvudmodellen, ofta kallad *vattenfallsmodellen*, är tanken att samtliga krav tas fram i början av projektet och därefter påbörjas programmeringsarbetet. I den andra huvudmodellen, ofta kallad *agil utveckling*, bedrivs utvecklingsarbetet genom att kraven och funktionerna tas fram för en del i taget. Arbetet behöver ske i nära samverkan med informationsägaren. Informationsägaren prioriterar utifrån riskbedömning vilken del av informationssystemet som ska kravställas och programmeras i nästa steg.

Oavsett vilken modell som används är det centralt att resultatet av utvecklingsarbetet löpande dokumenteras och testas för att kunna upptäcka brister i säkerheten. I detta ingår även att kontinuerligt bedöma förekomsten av nya eller förändrade risker. Det är centralt att kraven på säkerhet omhändertas så tidigt som möjligt i utvecklingsarbetet, och valet av modell kan påverka hur detta kan göras. Att följa upp säkerheten enbart i slutet, innan driftsättning, medför risker för att kostnaderna för att åtgärda bristerna på detta sena stadium blir mycket större än om de hanterats i inledningsfasen. Säkerhetsarbete behöver bedrivas under hela utvecklingsarbetet. Detta innebär exempelvis att utvecklarna behöver utbildas i att skapa säker kod och kunna omhänderta krav på säkerhet tidigt i arbetet. Behov av snabba förändringar av mjukvara ställer nya krav på säkerhetsarbetet. Att manuellt kodgranska varje förändring innan den driftsätts är i princip ogörligt, eftersom det skulle bli mycket tidskrävande och försena driftsättningen. Många delar av test- och säkerhetsarbetet inom utveckling kan därför behöva automatiseras.

Vid utveckling av mjukvara enligt *vattenfallsmodellen* finns det en risk att säkerhetsbrister (till exempel sårbarheter och funktionsfel) identifieras sent. Bristerna kan då bli svårare att åtgärda, om det krävs att tidigare slutfört arbete med kravställning och utveckling görs om eller justeras. Eftersom detta kan bli både kostsamt och tidsödande finns en risk att den som är ansvarig för utvecklingsarbetet och berörda informationsägare får acceptera de upptäckta bristerna eller försöka lösa dem genom extra tillägg som avviker från informationssystemets ursprungliga design. Inget av dessa alternativ är lämpliga. Därför är det viktigt att göra en grundlig riskanalys för att identifiera möjliga problem innan kravställningen fastställs.

Vid utveckling av mjukvara enligt den *agila metoden* finns möjlighet att hela tiden förtydliga kravställningen, testa samt åtgärda upptäckta brister. Till skillnad från vattenfallsmetoden ligger risken i att projektet ofta levereras i små delar och detaljerna i kravbilden hela tiden förändras, vilket kan göra det svårt att se och riskbedöma helheten. Detta kan delvis hanteras genom att löpande identifiera risker och hantera de största riskerna först. Även här är det centralt med en grundlig riskanalys av både helheten och delarna som underlag för kravställningen.

Följande ingångsvärden behöver beaktas i riskanalysen inför kravställningen:

- rättsliga krav
- verksamhetens behov av funktionalitet i informationssystemet
- informationsägarens informationsklassning och riskbedömning för den information som ska hanteras i informationssystemet
- val av hård- och mjukvara som ska ingå i informationssystemet, inklusive hur länge hård- och mjukvaran kommer att kunna uppdateras och ge tillräcklig funktionalitet
- val av säkerhetsfunktioner som ska skydda informationssystemet
- informationssystemets funktioner och placering i it-miljön
- utvecklingsmiljöns verktyg för utveckling och test
- tillgång till ändamålsenliga testdata avseende mängd och innehåll
- drift och förvaltning avseende val av programmeringsspråk, kompetens, applikationer, tjänster och andra komponenter
- arkivering och avveckling.

Riskanalysen genomförs lämpligen i nära samverkan mellan utvecklare och de som kommer att ansvara för drift och förvaltning.[39]

3.1.6 Utkontraktering

Det som kännetecknar utkontraktering är att en organisation anlitar en leverantör för att utföra en del av den egna verksamheten. En organisation kan välja att utkontraktera sin informationsbehandling i olika omfattning. Det kan exempelvis handla om it-utveckling, it-support, eller drift av informationssystem. Motivet till utkontrakteringen kan exempelvis vara att dra ned på kostnader[40], öka effektiviteten eller förbättra tillgången till kompetens eller hård- och mjukvaruresurser. Ansvaret för att organisationens information hanteras och driften sker säkert kan inte utkontrakteras, det är endast arbetsuppgifter som kan utkontrakteras. Organisationen ansvarar för sin information oavsett var den behandlas.

39. För att minska avståndet mellan utvecklarna (”developers”, som vill se sin kod snabbt i produktion) och de som driftsätter mjukvara (”operations”, som vill ha stabila tjänster utan förändringar) har DevOps blivit en metod. Utvecklare och driftansvariga har täta kontakter och mycket av installationen och uppdateringar av mjukvara sker med hjälp av automatiska metoder.

40. Utkontraktering behöver inte alltid medföra lägre kostnader. En organisation som utkontrakterar drift behöver, istället för att ha en egen driftenhet, lägga mer resurser på kravställning och uppföljning av hur leverantören uppfyller ställda krav, exempelvis skyddet av organisationens information. Vid utkontraktering av it-utveckling tillkommer kostnader för att kontrollera att säkerhetskraven uppfylls av den part som det är utkontrakterat till över tid. Exempelvis behöver organisationen ha en egen testmiljö som kan användas för att kontrollera att mjukvaran är tillräckligt säker för att kunna installeras i produktionsmiljön.

Innan organisationen utkontrakterar informationsbehandling är det viktigt att som första steg kontrollera att en eventuell utkontraktering uppfyller relevanta rättsliga krav[41]. En sådan analys förutsätter att organisationen specificerar

- vilken information som omfattas
- vilken informationsbehandling som leverantören är tänkt att utföra
- vilka leverantörer som skulle kunna komma att behandla informationen, inklusive eventuella underleverantörer
- var informationen kommer att behandlas.

Nästa steg är att kontrollera att det är lämpligt, ur organisationens eget perspektiv, att utkontraktera informationsbehandling. Vid bedömningen behöver organisationen förstå vilka utmaningar och risker det medför att en extern aktör kan få åtkomst till och kontroll över hela, eller delar av, den information som behandlas i it-miljön.

Många risker kan hanteras genom tydlig och relevant kravställning och uppföljning. Organisationen kan inte utgå från att vissa krav är underförstådda, utan behöver säkerställa att avtalet är så heltäckande som möjligt. Genom att organisationen ställer funktionskrav (vad som ska uppnås) istället för detaljkrav (hur kravet ska uppnås), ges leverantören möjlighet att uppfylla organisationens behov även om den inte använder exakt samma säkerhetsåtgärder som organisationen skulle ha använt. Kraven på säkerhet för den utkontrakterade informationsbehandlingen behöver vara desamma som om organisationen själv hade behandlat informationen. Det medför att de säkerhetskrav som organisationen ställer på sin egen informationsbehandling även ska ställas på leverantören. Dessutom kan ytterligare krav behöva ställas på leverantören för att kompensera organisationens minskade kontroll av informationen.

I många fall kommer organisationen att behöva jämföra sina säkerhetskrav mot de säkerhetsåtgärder som erbjuds i standardleveranser och standardavtal av leverantörer. För att få större leverantörer att möta organisationens krav genom tillägg till och justeringar av kraven i standardavtalet, kan det krävas mycket arbete av organisationen. I vissa fall är det inte ens möjligt att få till stånd sådana ändringar. Det kan också vara svårt att själv kunna kontrollera eller säkerställa en oberoende verifiering av att informationsbehandlingen hos leverantören överensstämmer med organisationens krav. Om organisationens krav inte beaktas eller det inte går att kontrollera att säkerhetsåtgärderna som leverantören infört är tillräckliga behöver organisationen överväga att välja en annan leverantör eller bedriva verksamheten i egen regi.

Grundkrav vid utkontraktering

I avtalet är det lämpligt att som minimum ställa följande krav på leverantörens verksamhet:

- Leverantören ska uppfylla tillämpliga regulatoriska krav, exempelvis rörande dataskydd.
- Det ska finnas ett etablerat systematiskt och riskbaserat informationssäkerhetsarbete.
- Det ska genomföras riskanalyser av den it-miljö som ska användas för att behandla organisationens information i enlighet med dokumenterade arbetssätt.
- Leverantören ska identifiera och hantera den hotbild som den egna och kundernas verksamhet skapar.
- Säkerhetsåtgärder som ska skydda information och informationssystem utifrån konfidentialitet, riktighet och tillgänglighet ska följa den tekniska utvecklingen och svara upp mot förändringar i hotbilden.
- Det ska finnas säkerhetsåtgärder i form av exempelvis åtkomst- och behörighetsstyrning, kryptering, loggning, filtrering, säkerhetskopiering, övervakning samt skydd mot skadlig kod.

41. Exempelvis avseende säkerhetsskydd, sekretess och dataskydd.

- Det ska finnas dokumenterade arbetssätt för ändringshantering som inkluderar att informationen informeras om kommande ändringar.
- Det ska finnas dokumenterade arbetssätt för avvikelse- och incidenthantering. Detta inkluderar när och hur informationen ska delas med organisationen samt hur krav på extern incidentrapportering ska uppfyllas.
- Det ska finnas dokumenterade arbetssätt för kontinuitetshantering, inklusive kris- och beredskapsplaner eller motsvarande. I detta ska ingå att leverantören har identifierat vilka underleverantörer den är beroende av för att behandla organisationens information under avtalsperioden.
- Det ska finnas ett fysiskt skydd som svarar mot den identifierade hotbilden.
- Det ska genomföras kontroller av säkerhetsåtgärder i den it-miljö som ska användas för att behandla organisationens information.

I avtalet är det lämpligt att som minimum ställa följande krav på hur relationen mellan organisationen och leverantören utformas:

- Leverantören ska tillhandahålla underlag för att organisationen ska kunna bedöma om utformningen av arkitekturen, inklusive säkerhetsarkitekturen, som används för att leverera avtalad tjänst uppfyller ställda säkerhetskrav.
- Leverantören ska tillhandahålla underlag för att organisationen ska kunna bedöma förutsättningarna för att informationssystemen ska kunna driftas och förvaltas på ett säkert sätt under avtalsperioden.
- Leverantören ska redovisa hur de hanterar och informerar om ändringar som kan påverka organisationens informationssystem.
- Leverantören ska redovisa vem eller vilka som får tillgång till organisationens information, var och hur informationen ska behandlas och lagras samt beskriva hur det säkerställs att den hålls åtskild från andra kunders information.
- Leverantören ska redovisa i vilka länder informationsbehandlingen kommer att bedrivas så att organisationen kan bedöma risker, lämplighet och förekomsten av rättsliga hinder.
- Leverantören ska redovisa vilka underleverantörer i samtliga led som är tänkta att anlitas. Underleverantörerna ska godkännas av organisationen innan de får åtkomst till information eller annan kännedom om informationsbehandlingen.
- Det ska vara tydligt vad, hur och när leverantören ska rapportera till organisationen om avvikelser och incidenter, identifierade risker, resultat av kontroller av säkerhetsåtgärder samt vilka säkerhetsåtgärder som vidtagits för att hantera brister.
- Organisationen, eller tredje part, ska regelbundet och vid behov få möjlighet att säkerhetstesta, granska och verifiera den del av leverantörens it-miljö som används för informationsbehandlingen.
- Organisationen och leverantören ska vara överens om vilka aktiviteter som ska utföras vid avslutande av kontrakten för att skyndsamt kunna återföra, flytta eller radera organisationens information, inklusive säkerhetskopior.

Att kraven är uppfyllda behöver kontrolleras innan kontrakt skrivs. Uppföljning och kontroll av att skyddet upprätthålls över tid behöver också göras under hela kontraktstiden. Om kraven inte uppfylls löper organisationen en risk och behöver själv införa kompenserande åtgärder, byta leverantör eller avsluta utkontrakteringen för att behandla informationen internt.

Vid utkontraktering tillkommer kostnader för att kontrollera att säkerhetskraven uppfylls av leverantören över tid. Det kan innebära kontroll av arbetssätten för att förebygga problem, att uppdateringar testas i testmiljö innan de installeras i produktionsmiljön och att incidenthanteringen fungerar.

Särskilt vid utkontraktering av it-utveckling

Om utvecklingen sker utanför organisationen kan det utöver ovanstående också behöva ställas krav på att leverantören utför utvecklingen på ett säkert sätt. I detta ingår att

- genomföra utvecklingsarbetet i en avskild och skyddad it-miljö
- skydda information, såsom kod, kravställning/beställningsunderlag och kommunikation såsom leverans och felrättning av kod.

För att skydda sin produktionsmiljö vid driftsättning av ny- eller uppdaterad programvara är det lämpligt att organisationen har en egen förmåga att testa funktion och säkerhet innan driftsättning. Organisationen behöver, oavsett sådan egen förmåga, säkerställa att de tester som leverantören genomfört och godkänt är tillräckliga och kan verifieras av organisationen.

Särskilt vid utkontraktering av it-support

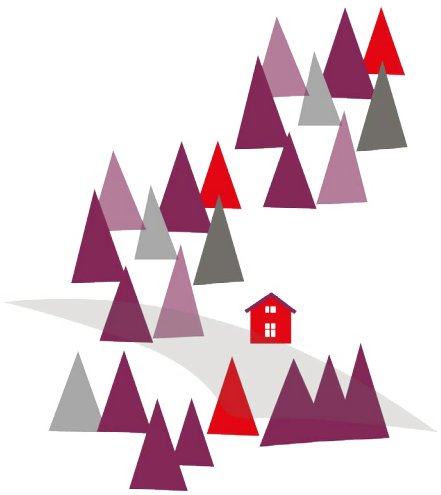
Vid utkontrakteringen av it-support där informationen fortfarande behandlas i organisationens it-miljö behöver leverantören få åtkomst dit. I praktiken innebär det ofta att leverantören då har tillgång till all information i it-miljön. Konsekvenserna av sådan tillgång behöver riskbedömas innan organisationen väljer att utkontraktera.

Extern it-support till den interna it-miljön förutsätter ofta att leverantören ges möjlighet till fjärråtkomst. Detta kan antingen ske till hela it-miljön eller till en begränsad del. Rätt till fjärråtkomst kan ges till leverantören i sin helhet eller till specifika medarbetare hos leverantören. Möjligheten att utföra support kan begränsas till en viss tidpunkt eller till specifika situationer där organisationen godkänner tillgång till it-miljön vid varje enskilt tillfälle. Om fjärråtkomst tillåts behöver den utformas utifrån organisationens verksamhetsbehov och riskbedömning.

Riskbedömning behöver även göras om leverantörens medarbetare utför sina arbetsuppgifter på plats hos organisationen och använder organisationens it-miljö.

3.1.7 Dokumentation om säkerhetsåtgärder för att möta krav

Genom att dokumentera vilka krav som uppfylls av vilka säkerhetsåtgärder blir det enklare att kontrollera att samtliga krav är omhändertagna och på vilket sätt detta har gjorts. Många organisationer väljer att lägga dokumentationen på en övergripande nivå och hänvisar till detaljerad systeminformation såsom arkitekturbeskrivningar. Om uppföljningen av införda säkerhetsåtgärder visar på brister ger en sådan dokumentation även stöd vid bedömningen av vilka risker som bristerna kan innebära. Dokumentationen underlättar även systemägarens kontroll av om säkerhetsåtgärderna är tillräckliga för säker drift och förvaltning. Vid utkontraktering behöver organisationen bedöma vilken dokumentation de själva ska upprätta respektive vilken dokumentation leverantören ska ansvara för.



3.2 Kontroller

3.2.1 Syfte

För att kunna bedriva säker drift och förvaltning behöver organisationen, innan driftsättning och inför förändringar som kan påverka säkerheten i informationssystemen, kontrollera att valda säkerhetsåtgärder är införda och ger tillräckligt skydd.

3.2.2 Krav

Organisationen ska, innan driftsättning och inför förändring som kan påverka säkerheten i informationssystemen,[42]

1. genom säkerhetstester och granskning kontrollera att valda säkerhetsåtgärder är tillräckliga för att möta identifierade krav på säkerhet
2. verifiera att det finns nödvändig dokumentation för drift och förvaltning
3. genomföra riskbedömning och hantera brister som identifierats genom säkerhetstester och granskning samt vid verifiering av dokumentationen.

Organisationen bör se till att dokumentation för drift och förvaltning av informationssystem omfattar[43]

1. arkitektur, ingående komponenter, konfiguration, dataflöden och övrig relevant systeminformation
2. vem som är systemägare
3. om och till vilken extern aktör utkontraktering har skett.

42. MSBFS 2020:7 3 kap. 2 § Myndigheten ska, innan driftsättning och inför förändring som kan påverka säkerheten i informationssystemen, 1. genom säkerhetstester och granskning kontrollera att valda säkerhetsåtgärder är tillräckliga för att möta identifierade krav på säkerhet, och 2. verifiera att det finns nödvändig dokumentation för drift och förvaltning. I de fall brister identifieras ska myndigheten riskbedöma och hantera dessa brister innan driftsättning eller inför förändring som kan påverka säkerheten i informationssystemen.

43. Allmänt råd till MSBFS 2020:7 3 kap. 2 § Nödvändig dokumentation för drift och förvaltning bör omfatta arkitektur, ingående komponenter, konfiguration, dataflöden och övrig relevant systeminformation. Av dokumentationen bör även framgå vem som är systemägare samt om och till vilken extern aktör informationssystemet är utkontrakterat.

3.2.3 Utforma och genomföra kontroller innan driftsättning

Även om den utvecklade hård- och mjukvaran genomgått gedigna tester kan sårbarheter upptäckas i efterhand. Dessa kan ha sitt ursprung i misstag, felaktig arkitektur, nyutvecklad teknik eller brister i förvaltningen. I allvarliga fall kan även sårbarheter avsiktligt ha lagts in i hård- eller mjukvaran av angripare, antingen vid tillverkningen eller vid senare uppdateringar.

Innan organisationen driftsätter ny hårdvara eller ny/förändrad mjukvara behöver det därför göras en kontroll för att upptäcka eventuella brister som kan påverka säkerheten i it-miljön. Sådana kontroller kan göras på olika sätt, exempelvis genom säkerhetstester, granskning eller verifiering av dokumentation. Detta kan exempelvis göras genom att uppdateringar testas i testmiljö innan de installeras i produktionsmiljön, samt att nyinköpt hård- och mjukvara alltid kontrolleras för att säkerställa att de är uppdaterade till senaste version innan de installeras i it-miljön.

Det är lämpligt att organisationen har fastställda arbetssätt för hur de olika typerna av kontroller ska genomföras och kombineras, eftersom de kan vara resurskrävande. Arbetssättet behöver också ta höjd för skyddsbehovet genom att säkerställa att ett stort skyddsbehov för information och informationssystem samt hög risk även innebär mer omfattande kontroll av säkerhetsåtgärderna.

Vid utveckling genomförs tester, granskningar och verifiering av dokumentation i första hand av utvecklingsorganisationen. I samband med utvecklingsarbete behöver det tas fram en testplan som beskriver behovet av tester under utvecklingsarbetet så att fel och brister upptäcks och kan rättas till före driftsättning. Det är lämpligt att testplanen beskriver vilka tester som ska utföras samt när och hur testerna ska genomföras, exempelvis enhetstest, systemtest, integrationstest, stresstest, acceptanstest, pilottest och säkerhetstester

såsom konfigurationstester av klienter, servrar och nätverk samt penetrationstester. Tester som kan påverka it-miljön behöver utföras av personer med specifik kompetens och erfarenhet. Ibland kan externt stöd behöva engageras för att genomföra testerna.

Utöver tester behöver även organisationen åtminstone i slutet av utvecklingsarbetet genomföra granskningar. Sådana granskningar behöver göras innan ny hårdvara eller ny/förändrad mjukvara installeras i it-miljön. En säkerhetsgranskning innebär att organisationen kontrollerar att säkerhetskraven är uppfyllda, avseende både skyddsnivå och vald lösning. Det kan handla om att kontrollera säkerheten hos utvecklad kod eller att säkerhetsåtgärder implementerats på rätt sätt genom att granska exempelvis konfigurationer och testresultat. Granskningar görs i många fall fortfarande manuellt, men tillgången till automatiserade stöd för granskning har ökat de senaste åren. Granskningen kompletteras genom att verifiera att det finns nödvändig dokumentation för att drift och förvaltning samt användare ska kunna behandla information och informationssystem på ett säkert sätt.

Det är lämpligt att granskning innan driftsättning utförs av medarbetare utanför utvecklingsorganisationen. Det är fördelaktigt att sätta samman en grupp av medarbetare med olika relevanta kompetenser för granskningen, exempelvis representanter för drift och förvaltning, informations- och it-säkerhet, juridik, informationsägare och systemägare. Det är lämpligt att organisationen bedömer behovet av att anlita en extern part med särskild kompetens för granskningen, särskilt i samband med större och känsligare utvecklingsarbeten eller när organisationen själv saknar nödvändig kompetens.

Innan informationssystemet godkänns och förs över till produktionsmiljön, ska valda säkerhetsåtgärder inklusive säkerhetsfunktioner vara aktiverade samt brister som upptäcks i samband med tester, granskningar och verifiering av dokumentation ska vara åtgärdade. Om det finns brister som det inte går att göra något åt behöver dessa riskbedömas.

Se även **avsnitt 4.6** för mer information om hur säkerhetstester och granskningar kan genomföras.

3.3 Utvecklings-, test- och utbildningsmiljöer

3.3.1 Syfte

För att skydda organisationens produktionsmiljö från incidenter som kan uppstå i organisationens utvecklings-, test- och utbildningsmiljöer behöver organisationen skilja produktionsmiljön från dessa miljöer.

3.3.2 Krav

Organisationen ska

1. bedriva sitt arbete med utveckling och tester som kan påverka säkerheten i en it-miljö som är avskild från produktionsmiljön[44]
2. identifiera och hantera behovet av en utbildningsmiljö som är avskild från produktionsmiljön.[45]

3.3.3 Utvecklings- och testmiljöer

En organisation ska använda avskilda miljöer för utveckling och testning så att den informationsbehandling som sker i organisationens produktionsmiljö inte påverkas vid problem i samband med utveckling och test. Bristande säkerhet i utvecklings- och testmiljöer kan användas av en angripare för att få åtkomst till organisationens produktionsmiljö och informationen som hanteras där.

En miljö kan ha olika omfattning och utformning. Utifrån behov kan en organisation exempelvis använda sig av virtuella utvecklings- och testmiljöer eller bygga upp dessa på en enskild klient. För att en it-miljö ska räknas som avskild från produktionsmiljön får det inte finnas några dataflöden eller andra integrationer mellan dem, förutom de som krävs för att flytta testad och godkänd hård- och mjukvara från testmiljön till produktionsmiljön. Organisationen behöver också identifiera lämpliga och säkra sätt att flytta färdigutvecklad kod från utvecklings- till testmiljön. Arkitekturen behöver stödja utformningen av miljöerna genom tydlig segmentering. Det är lämpligt att varje avskild it-miljö har en utpekad systemägare som ansvarar för att där införa, förvalta, följa upp och utvärdera säkerhetsåtgärder. Systemägaren godkänner vilken information och vilka informationssystem som it-miljön får innehålla.

De organisationer som själva utvecklar och förändrar hård- och mjukvara ska ha en avskild miljö för utvecklingsarbetet och en testmiljö för att kunna genomföra tester utan att påverka säkerheten i produktionsmiljön. Det är lämpligt att organisationer som inte bedriver utvecklingsarbete ändå har en miljö för tester där de kan kontrollerar säkerheten hos anskaffad hård- och mjukvara innan den tas i drift. Organisationer som har utkontrakterat driften av sin it-miljö ska i sin kravställning och kontroll av uppfyllnad av kraven säkerställa att leverantören håller organisationens produktionsmiljö avskild från leverantörens utvecklings- och testmiljö.

Särskilt om utvecklingsmiljö

Utvecklingsmiljön ska hållas åtskild från produktionsmiljön eftersom utvecklingsarbetet ofta innebär att vissa säkerhetsfunktioner behöver vara avstängda för att underlätta eller till och med möjliggöra utvecklingen. Information och informationssystem i utvecklingsmiljön behöver dock skyddas mot exempelvis obehörig åtkomst och obehörig förändring. Detta gäller exempelvis information såsom källkod och autentiseringsuppgifter till utvecklingsmiljön och externt hämtade kodbibliotek som används i utvecklingsarbetet samt de informationssystem som används vid utveckling.

44. MSBFS 2020:7 3 kap. 3 § Myndighetens arbete med utveckling och tester som kan påverka informationssäkerheten i produktionsmiljön ska ske i en från produktionsmiljön avskild del av it-miljön.

45. MSBFS 2020:7 3 kap. 4 § Myndigheten ska identifiera och hantera behovet av en utbildningsmiljö som är avskild från produktionsmiljön.

Vid utveckling av informationssystem är det viktigt att ha tydliga arbetssätt som beskriver hur testade och godkända programdelar/koder ska paketeras. Detta för att ha kontroll över vilka versioner av programkod som är under utveckling, testning respektive godkända för driftsättning.

Särskilt om testmiljö

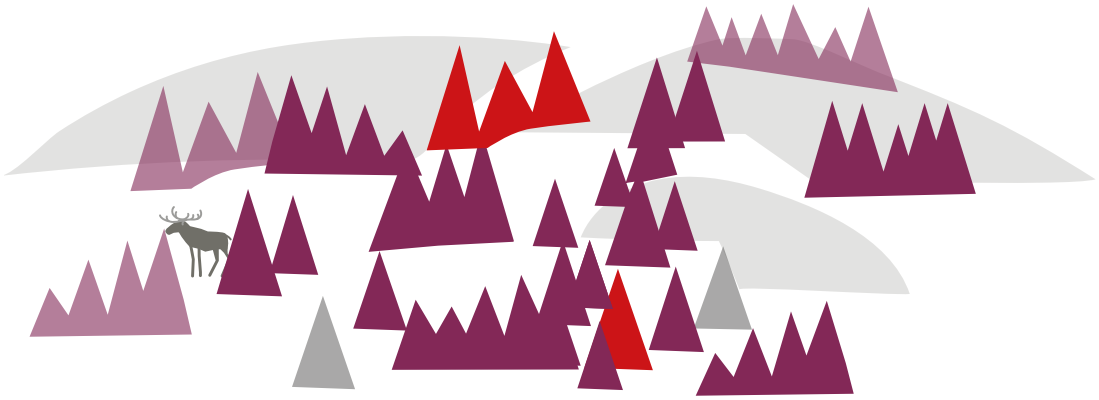
Innan nyutvecklad eller förändrad hård- eller mjukvara driftsätts i produktionsmiljön ska säkerhetstester genomföras för att kontrollera att säkerhetsåtgärderna är tillräckliga för att möta kraven på säkerhet och att hård- och mjukvaran inte har någon oönskad funktionalitet. Testerna ska göras i en miljö (testmiljö) avskild från produktionsmiljön för att undvika att eventuella säkerhetsbrister i hård- och mjukvaran inte påverkar produktionsmiljön och den verksamhetsinformation som hanteras där. Att genomföra tester i produktionsmiljön kan orsaka allvarliga störningar. Ibland är det dock nödvändigt att i produktionsmiljön verifiera att informationssystemet är korrekt uppsatt. Detta ska inte likställas med testning utan räknas, om det görs utan att påverka säkerheten, som en del av säker drift och förvaltning.

Testning kan ha olika syften och det styr hur och i vilken miljö den bör genomföras. I en utvecklingsmiljö kan exempelvis tester göras av att utvecklad eller förändrad kod har avsedd funktionalitet (enhetstestning).

Testmiljön är avsedd att användas för exempelvis systemtester och integrationstester. För att skapa goda förutsättningar för integrationstester behöver testmiljön efterlikna produktionsmiljön så mycket som möjligt eller kunna simulera de delar i produktionsmiljön som den testade hård- och mjukvaran kommer att ha utbyte med i produktionsmiljön. Även säkerhetstester där syftet är att upptäcka sårbarheter och kontrollera att införda säkerhetsåtgärder är på plats behöver göras i en testmiljö som är så lik produktionsmiljön som möjligt. Ju mer lika de är, desto enklare blir det att vara säker på att alla sårbarheter upptäcks.

System-, integrations- och säkerhetstester förutsätter att organisationen har tillgång till en uppsättning av informationssystem i testmiljön som kan användas för att simulera samma dataflöden som finns i produktionsmiljön. Detta för att kunna testa funktionaliteten fullt ut, men samtidigt undvika att använda verksamhetsinformation och riskera att påverka drift och säkerhet i produktionsmiljön.

Vissa organisationer använder två exakt likadana avgränsade miljöer för varje informationssystem med identisk hård- och mjukvara – en för produktion och en för testning. När informationssystemet i den avskilda testmiljön är testat och systemägaren godkänt det för driftsättning, pekas adresseringen om så att informationssystemets testmiljö blir dess produktionsmiljö och den tidigare produktionsmiljön blir ny testmiljö.

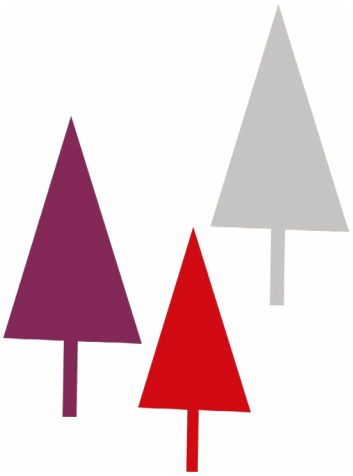


3.3.4 Utbildningsmiljöer

För att utbilda medarbetarna i hur ett informationssystem fungerar bör det finnas en utbildningsmiljö där det är tillåtet att göra fel utan att verksamheten påverkas i produktionsmiljön. När en organisation bedömer behovet av att en sådan utbildningsmiljö hålls avskild från produktionsmiljön bör minst följande risker beaktas:

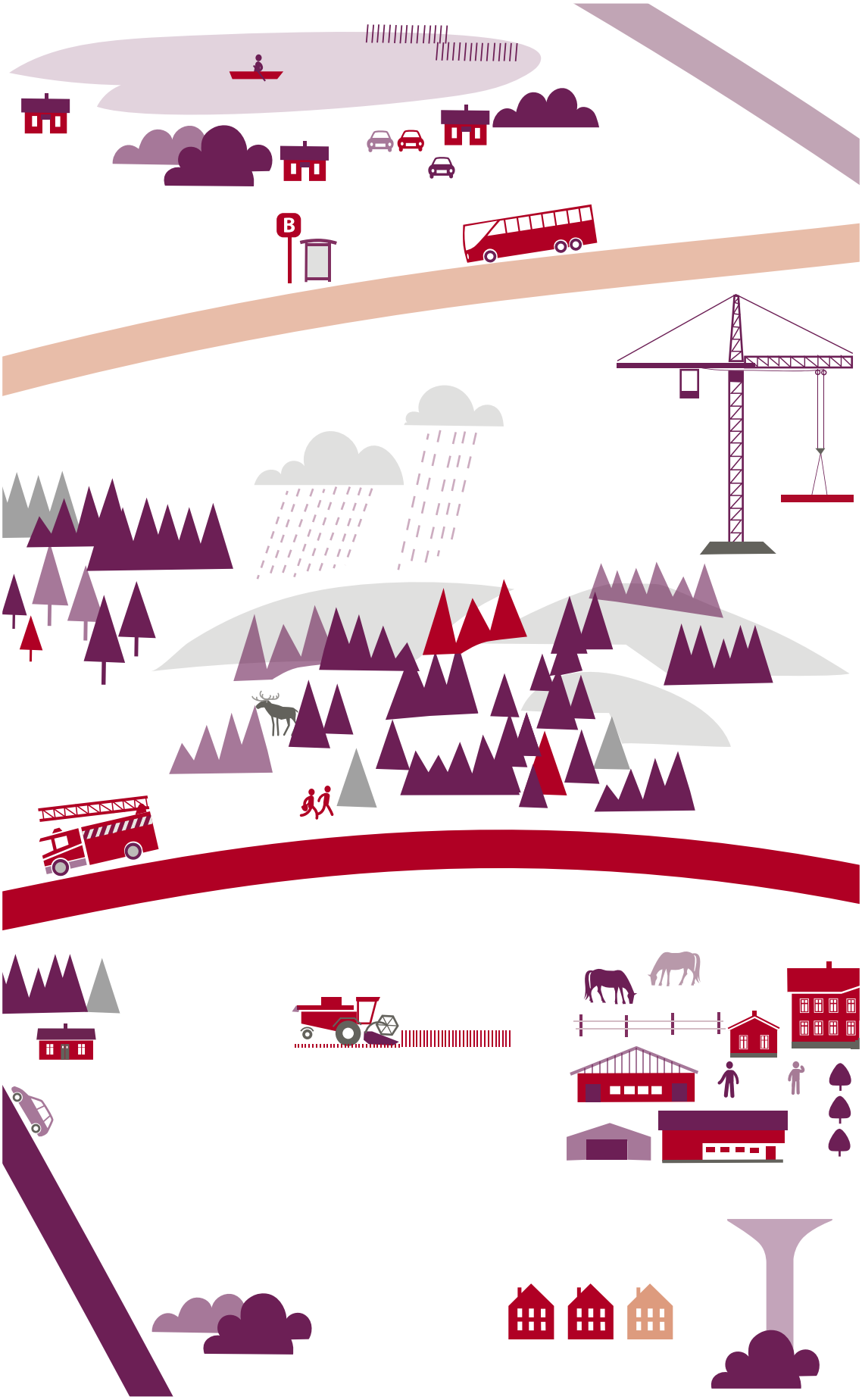
- obehörig åtkomst till information i produktionsmiljön, exempelvis personuppgifter
- obehörig förändring av information som används i produktionsmiljön
- informationssystem som används i produktionsmiljön kopplas samman med informationssystem i utbildningsmiljön, exempelvis för att kunna demonstrera hela arbetsflödet.

För att utbildningsmiljön ska ses som avskild från produktionsmiljön får det inte finnas några dataflöden eller andra integrationer mellan de båda miljöerna. För att utbildningen ska kunna vara så realistisk som möjligt är det dock lämpligt att informationssystemen i utbildningsmiljön är så lika informationssystemen i produktionsmiljön som möjligt i de delar som medarbetarna ska utbildas i. Det kan även vara lämpligt att, precis som i testmiljön, ha möjlighet att simulera de dataflöden som behövs för att få en realistisk utbildningsmiljö.



Informationen som används i informationssystemen vid utbildningen bör i första hand bestå av testdata. Om organisationen behöver använda verksamhetsinformation, det vill säga information från produktionsmiljön, i utbildningsmiljön är det viktigt att säkerställa att det inte finns rättsliga regler eller verksamhetskrav som förhindrar sådan behandling, exempelvis dataskyddsförordningen. Systemägaren behöver godkänna att sådan informationsbehandling sker och säkerställa att informationssystemet i utbildningsmiljön har ett skydd som motsvarar skyddet för informationssystemet i produktionsmiljön. De medarbetare som genomgår utbildning behöver informeras om vilken information som används vid utbildningen, särskilt när verksamhetsinformation (produktionsdata) används, samt vilka hanteringsregler som gäller.

Den utbildningsmiljö som avses här har endast som syfte att användas för intern utbildning av medarbetare i de informationssystem som används i verksamheten. Organisationer som bedriver verksamhet i form av undervisning använder inte en avskild utbildningsmiljö utan sin produktionsmiljö för detta syfte. Detta eftersom undervisningen är den verksamhet som organisationen bedriver. För den här typen av organisationer, exempelvis högskolor och universitet, är det lämpligt att dela upp sin produktionsmiljö så att undervisning sker i en miljö som är avskild från den del av produktionsmiljön som används för administrativa uppgifter såsom ekonomi, betygssättning, ärendehantering och studievägledning. Beroende på undervisningens inriktning och moment kan det finnas anledning att även dela in undervisningsdelen i produktionsmiljön i ytterligare segment, exempelvis om det tillhandahålls informationssystem som kan användas för kodutveckling, penetrationstester eller motsvarande. Bristande säkerhet i utbildningsmiljön kan användas av en angripare för att få åtkomst till organisationens produktionsmiljö och informationen som hanteras där.


B

Drift och förvaltning

4. Drift och förvaltning

4.1 Nätverkssegment och filtrering

4.1.1 Syfte

För att förhindra spridning och konsekvenser av inträffade incidenter behöver organisationen dela upp sin it-miljö i olika nätverkssegment och filtrera trafiken så att endast nödvändiga dataflöden förekommer.

4.1.2 Krav

Organisationen ska

1. placera informationssystem med olika funktioner i separata nätverkssegment i sin produktionsmiljö[46]
2. filtrera nätverkstrafiken så att endast nödvändiga dataflöden förekommer mellan olika nätverkssegment.[47]

Organisationen bör placera följande funktioner i separata nätverkssegment:[48]

1. klienter för användare
2. klienter för administration
3. servrar
4. centrala systemsäkerhetsfunktioner i form av behörighetskontrollsystem, säkerhetsloggning, filtrering och liknande
5. centrala stödfunktioner i form av skrivare, scanner och liknande
6. trådlösa nätverk
7. gästnätverk
8. externt åtkomliga tjänster
9. informationssystem som sammankopplas med informationssystem hos extern aktör
10. industriella informations- och styrsystem
11. system som innehåller sårbarheter som inte kan hanteras.

46. MSBFS 2020:7 4 kap. 1 § Myndigheten ska förhindra spridning av incidenter och minska konsekvenser av angrepp genom att placera informationssystem med olika funktioner i separata nätverkssegment i sin produktionsmiljö.

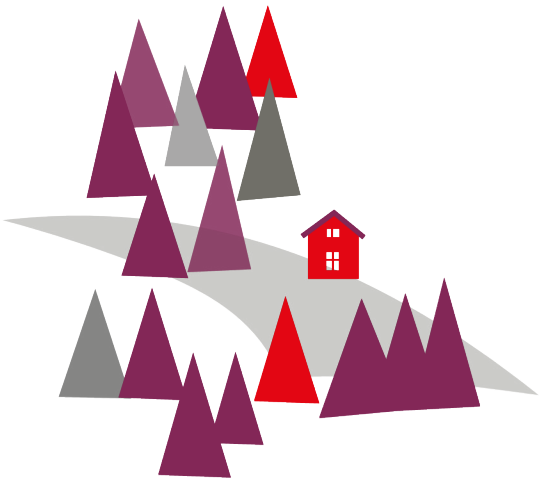
47. MSBFS 2020:7 4 kap. 2 § Myndigheten ska filtrera nätverkstrafiken så att endast nödvändiga dataflöden förekommer mellan olika nätverkssegment.

48. Allmänt råd till MSBFS 2020:7 4 kap. 1 § Följande funktioner i produktionsmiljön bör placeras i separata nätverkssegment: 1. Klienter för användare. 2. Klienter för administration. 3. Servrar. 4. Centrala systemsäkerhetsfunktioner i form av behörighetskontrollsystem, säkerhetsloggning, filtrering och liknande. 5. Centrala stödfunktioner i form av skrivare, scanner och liknande. 6. Trådlösa nätverk. 7. Gästnätverk. 8. Externt åtkomliga tjänster. 9. Informationssystem som sammankopplas med informationssystem hos extern aktör. 10. Industriella informations- och styrsystem. 11. System som innehåller sårbarheter som inte kan hanteras.

4.1.3 Behov av separata nätverkssegment

Nätverket är en viktig del av organisationens it-miljö. Organisationens nätverk sträcker sig många gånger långt utanför den fysiska kontorslokalen genom att tjänster är utkontrakterade, trådlösa nätverk[49] används, partnernätverk kopplas samman eller tjänster görs tillgängliga att nås av medarbetare hemifrån eller på resa. Det går inte längre att tala om en fysisk avgränsning av nätverket.

Nätverk måste skyddas mot såväl interna och externa som avsiktliga och oavsiktliga hot. Organisationen behöver utgå från att alla informationssystem i it-miljön innehåller kända och okända[50] sårbarheter. Dessa kan bero på brister i design, implementering och konfigurering av hård- och mjukvara. För att motverka konsekvenserna av brister behöver organisationen se till att inträffade incidenter inte sprider sig i nätverket och att konsekvenserna begränsas till en mindre del av it-miljön. Detta görs bland annat genom att dela in nätverket i mindre nätverkssegment.



Nätverkssegmenten behöver i sin tur skyddas med olika säkerhetsåtgärder. Det kan exempelvis handla om filtrering av nätverkstrafik, behörigheter, kryptering, säkerhetskonfiguration, säkerhetskopiering, loggning, övervakning, skydd mot skadlig kod och redundans. Hur säkerhetsåtgärderna utformas och vilken nivå av skydd de behöver ge beror på respektive nätverkssegments skyddsbehov, användningsområde och syfte.

En riskbedömning visar om vissa nätverkssegment kan behöva avskiljas fysiskt från övrig it-miljö. Ett fysiskt avskilt nätverkssegment har inte någon koppling till andra nätverkssegment och inget dataflöde till eller från nätverkssegmentet via en nätverksförbindelse.

4.1.4 Indelning i zoner

Arbetet med att dela in nätverket i olika segment underlättas om organisationen, lämpligen systemägaren för nätverket, dessförinnan har beskrivit designen i nätverket på övergripande nivå. Designen kan illustreras med hjälp av en zonmodell. De olika zonerna i en sådan modell kan skilja sig åt, exempelvis avseende användningsområde, skyddsbehov och möjlighet till extern kommunikation.

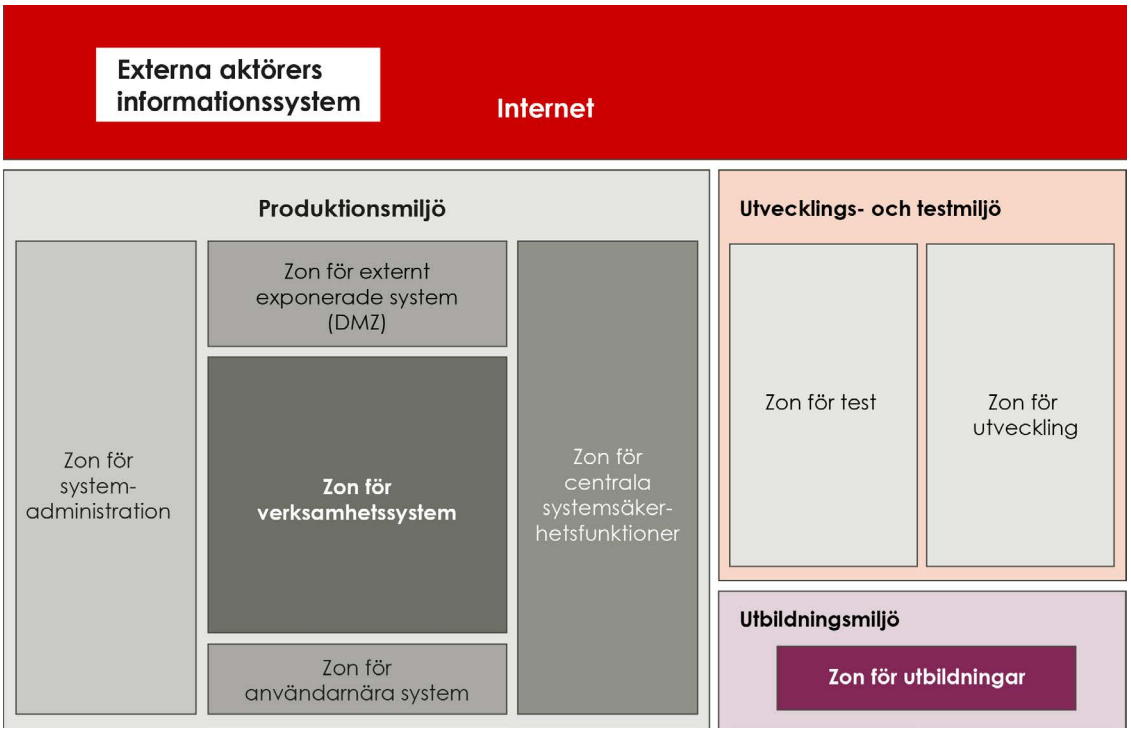
Zonerna avgränsas från varandra genom att nätverkstrafiken mellan zonerna filtreras, exempelvis med hjälp av brandväggar. En zon kan bestå av ett eller flera nätverkssegment. Nätverkstrafiken mellan segmenten, även om de finns i en och samma zon, behöver skiljas åt genom filtrering.

Nedan illustreras hur en zonmodell kan utformas i en organisation som utöver sin produktionsmiljö även har it-miljöer för utveckling, test och utbildning. Produktionsmiljön består här av zonerna för

- användarsystem
- verksamhetssystem
- systemadministration
- centrala systemsäkerhetsfunktioner
- externt exponerade system.

49. Med trådlöst nätverk avses här inte enbart wifi som baseras på 802.11-standarden, utan även trådlösa nätverk för t.ex. IoT-enheter (såsom Zigbee, LoRaWAN, Z-wave), Bluetooth, mobiltelefoninät (GSM, 3G, 4G och 5G) m.fl.

50. Med okända sårbarheter avses här sådana sårbarheter som ännu inte upptäckts av någon, exempelvis leverantör, hackergrupp, säkerhetsforskare eller myndighet.



Figur 1. Exempel på en organisations omgivning samt övergripande indelning av it-miljöer och zoner.

De olika zonerna har olika användningsområden, skyddsbehov och möjlighet till extern kommunikation. Nedan följer exempel på zoner och vilka informationssystem som placeras där.

- **Produktionsmiljö**
  - **Zon för användarnära system:** användarklienter och användarapplikationer.
  - **Zon för verksamhetssystem:** servrar, databaser, katalogtjänster och nätverksutrustning.
  - **Zon för systemadministration:** tjänster och klienter som används för systemadministrativa åtgärder.
  - **Zon för centrala systemsäkerhetsfunktioner:** behörighetskontrollsystem och säkerhetslogg.
  - **Zon för externt exponerade system (även kallad DMZ):** tjänster som exponeras mot internet, till exempel publika webbservrar, vpn-koncentrator och e-postgateway.
- **Utvecklings- och testmiljö**[51]
  - **Zon för utveckling.**
  - **Zon för test.**
- **Utbildningsmiljö**
  - **Zon för utbildningar.** Informationssystem som exempelvis används för utbildning av användare eller systemadministratörer i samband med att ett nytt informationssystem implementeras.

Informationssystemen i respektive zon ska i sin tur grupperas i olika nätverkssegment. Ovanstående zonmodell är bara ett exempel på hur it-miljön schematiskt kan delas in – en organisation behöver utforma nätverket i sin it-miljö utifrån sina behov. Exempelvis kan det finnas behov av att dela in utvecklings-, test- respektive utbildningsmiljön i ytterligare nätverkssegment.

51. Utvecklings- och testmiljön behöver inte vara en miljö med två olika zoner. Organisationen kan även välja att ha en separat utvecklingsmiljö respektive en separat testmiljö som i sin tur delas in i olika zoner.

Utformningen av nätverkets design påverkas av hur komplex organisationens it-miljö är. Komplexiteten kan exempelvis bestå i att hela eller delar av informationsbehandligen är kontrakterad, andra organisationer ges direktåtkomst till delar av it-miljö eller allmänheten ges tillgång till olika e-tjänster. Ett sätt att hantera sådana utmaningar är att bygga in säkerhet på flera nivåer i nätverket.

4.1.5 Indelning i nätverkssegment

En zon kan bestå av ett eller flera nätverkssegment. Systemägaren för nätverket behöver se till att uppdelningen av nätverkssegment reflekterar behovet av att separera:

- information med olika känslighet
- information med olika krav på tillgänglighet
- information med olika krav på kommunikationssätt
- informationssystem med olika nivå av exponering
- informationssystem med olika funktion
- informationssystem som används av specifika roller.

Uppdelningen kan göras med stöd av logiska åtgärder, exempelvis VLAN (Virtual Local Area Network). Segmentering kan även göras med hjälp av fysisk separation där ett nätverk inte har några fysiska sammankopplingar med ett annat nätverk.

På samma sätt som mellan zonerna regleras kommunikationen mellan nätverkssegmenten genom att trafiken filtreras utifrån ett strikt behov av vilka dataflöden som behövs. Systemägarna för de olika informationssystemen behöver analysera vilka dataflöden som krävs för att informationssystemet ska kunna möta verksamhetens behov och vilka dataflöden som utgör risker. Systemägaren för nätverket kan sedan placera informationssystemet i lämpligt nätverkssegment som motsvarar behoven. Vissa organisationer placerar alla sina informationssystem i egna nätverkssegment för att fullt ut kunna filtrera utifrån behoven hos respektive informationssystem. Som stöd för drift och förvaltning av de olika nätverkssegmenten kan till exempel verktyg som SDN (Software Defined Networking) användas för att ha en bild av nätverkets olika delar.

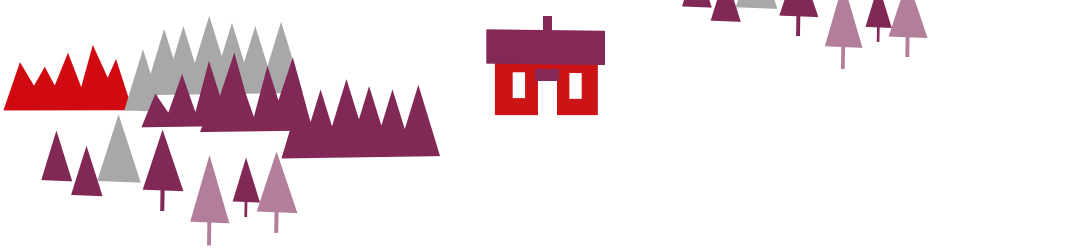
Vissa funktioner i produktionsmiljön bör alltid placeras i separata nätverkssegment. Följande lista över sådana funktioner kan behöva utökas beroende på organisationens behov, riskbedömning och tekniska förutsättningar.

- klienter för användare
- klienter för administration
- servrar
- centrala systemsäkerhetsfunktioner
- centrala stödfunktioner
- trådlösa nätverk
- gästnätverk
- externt åtkomliga tjänster
- informationssystem som sammankopplas med informationssystem hos extern aktör
- industriella informations- och styrsystem
- system som innehåller sårbarheter som inte kan hanteras.

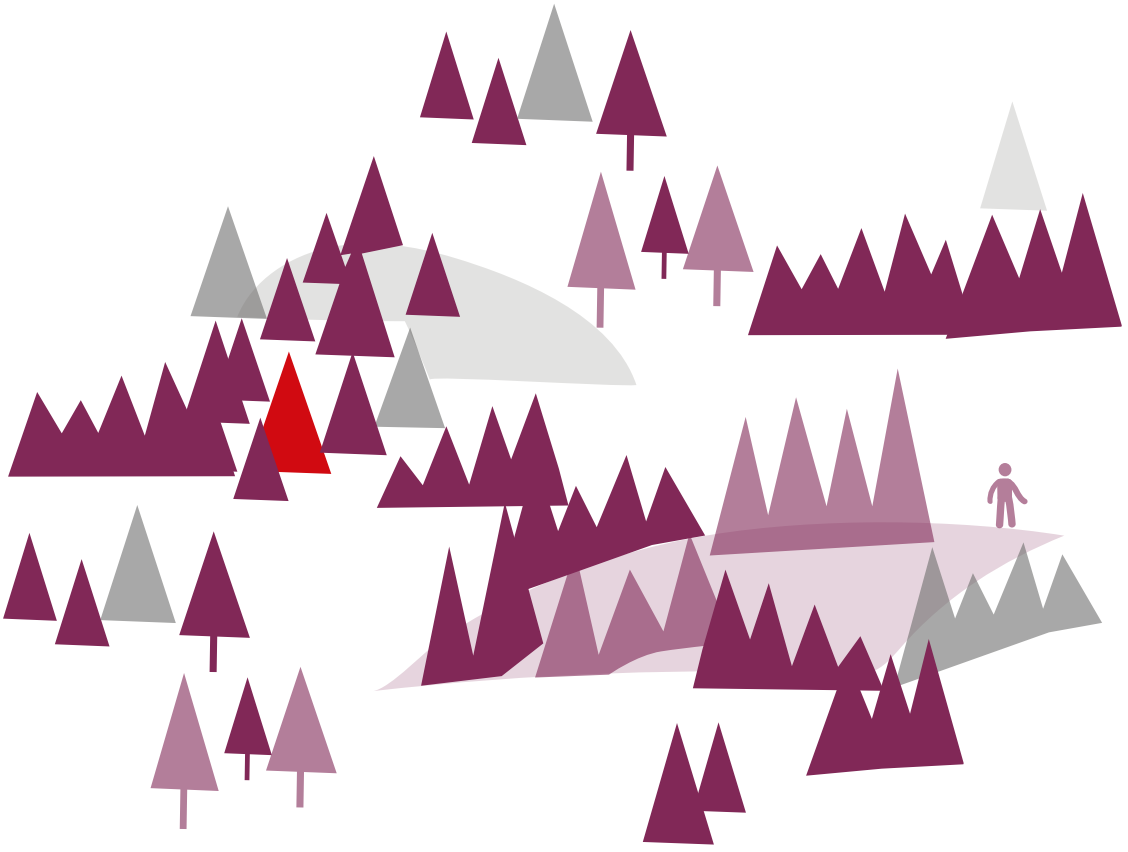
Det finns olika orsaker till att ovan nämnda funktioner bör placeras i olika nätverkssegment.

- **Klienter för användare:** Organisationens medarbetare behöver i regel ges tillgång till internet samtidigt som de behöver ha åtkomst till den interna miljön. För att skydda övriga delar av organisationens it-miljö mot eventuella incidenter som orsakas av användarklienternas exponering mot internet, bör dessa placeras i ett eller flera egna nätverkssegment. Det är lämpligt att inte placera alltför många klienter för användare i samma nätverkssegment.

- **Klienter för administration:** Systemadministratörerna behöver ha hög behörighet för att utföra sina arbetsuppgifter och kan därigenom påverka säkerheten i it-miljön. Obehörig åtkomst till it-miljön via klienter som används för systemadministration kan få stora negativa konsekvenser. Systemägaren behöver därför se till att sådana klienter placeras i ett eller flera nätverkssegment där de aldrig ges åtkomst till internet eller andra externa nätverk.
- **Servrar:** I servrarna behandlas en av organisationens främsta tillgångar, det vill säga dess information. För att kunna ge både informationen och informationssystemen tillräckligt skydd bör dessa placeras i ett eller flera separata nätverkssegment. Exempelvis är det lämpligt att placera servrar som efter informationsklassning och riskbedömning bedömts ha ett behov av utökat skydd, exempelvis avseende tillgänglighet, övervakning, konfidentialitet eller redundans, i ett särskilt nätverkssegment som kan tillhandahålla den extra nivån av skydd.
- **Centrala systemsäkerhetsfunktioner** i form av behörighetskontrollsystem, säkerhetsloggning, filtrering och liknande. Funktionen hos centrala systemsäkerhetsfunktioner är avgörande för att en organisation ska kunna behandla information på ett sätt som motsvarar verksamhetens behov av konfidentialitet, riktighet och tillgänglighet. De bör därför placeras i en särskild zon med höga säkerhetskrav. För att säkerställa att de olika systemsäkerhetsfunktionerna får det skydd de behöver, behöver zonen sannolikt delas upp i flera olika nätverkssegment som motsvarar respektive funktions skyddsbehov.
- **Centrala stödfunktioner** i form av skrivare, scanner och liknande. Den här typen av informationssystem har som huvudsyfte att underlätta för användarna, vilket gör att de behöver vara lättillgängliga och enkla att använda. Detta gör att användarnytta ibland sätts före säkerhet, vilket kan kompenseras genom att placera dem i ett eget nätverkssegment, avskilt från organisationens övriga informationssystem.
- **Trådlösa nätverk.** Användningen av trådlösa nätverk ökar möjligheterna för utomstående att skaffa sig tillgång till organisationens information genom att nätverkssignalen ofta kan nås av andra än organisationens medarbetare, både i och utanför de egna lokalerna. Genom att placera dem i ett särskilt nätverkssegment förenklas kontrollen av och det administrativa arbetet med att säkerställa att samtliga trådlösa nätverk hanteras på ett säkert sätt.
- **Gästnätverk.** Gästnätverk erbjuder organisationens besökare möjlighet att få tillgång till internet. Det är centralt att denna service till besökarna inte samtidigt innebär att de kan få åtkomst till organisationens interna it-miljö. Gästnätverk bör därför placeras i ett eget nätverkssegment. I det fall organisationen tillåter medarbetare att ansluta egen utrustning till organisationens nätverk (till exempel privata mobiltelefoner) ska den utrustningen bara kunna anslutas till gästnätverket, eftersom det behöver vara helt separerat från andra interna nätverk och inte ha någon åtkomst till den övriga it-miljön.



- **Externt åtkomliga tjänster.** Tjänster som exponeras mot internet, till exempel publik webbserver, vpn-koncentrator och e-postgateway, är synliga för andra aktörer på internet och därmed ofta utsatta för angreppsförsök. Syftet är i de flesta fall att skaffa sig tillgång till organisationens interna it-miljö. Externt åtkomliga tjänster bör placeras i ett eller flera nätverkssegment som kan ges ett extra högt skydd i form av säkerhetsåtgärder som upptäcker och hanterar konsekvenserna av ett angrepp.
- **Informationssystem som sammankopplas med informationssystem hos extern aktör.** För att förhindra att it-incidenter som inträffar hos den externa aktören får konsekvenser hos den egna organisationen, behöver informationssystem som är sammankopplade med informationssystem hos en extern aktör placeras i ett eller flera separata nätverkssegment.
- **Industriella informations- och styrsystem.** Den här typen av informationssystem är extra sårbara, eftersom de ofta saknar möjlighet att nyttja sådana säkerhetsåtgärder som informationssystem i kontors-it använder. Sårbarheten behöver därför kompenseras genom andra typer av åtgärder, vilket förenklas när de är placerade i nätverkssegment avskilda från övrig it-miljö.
- **System som innehåller sårbarheter som inte kan hanteras.** Vissa informationssystem är på grund av ålder, utformning, användning eller annan orsak inte möjliga att skydda med ändamålsenliga och proportionella säkerhetsåtgärder. För att kvarvarande sårbarheter inte ska påverka andra informationssystem i it-miljön, alternativt kunna utnyttjas av angripare i syfte att få åtkomst till organisationens it-miljö, behöver dessa placeras i ett eller flera separata nätverkssegment.



4.1.6 Filtrering av dataflöden

Filtrering av dataflöden sker företrädesvis genom det som i vanligt tal kallas brandvägg. Filtreringsfunktionen kan också vara implementerad i andra informationssystem eller annan typ av nätverksutrustning, exempelvis proxy-tjänster eller datadioder.

Brandväggar kan vara både hårdvaru- och mjukvarubaserade. Utformningen av brandväggarna skiljer sig även utifrån vilket syfte de har, exempelvis nätverksbrandvägg och applikationsbrandvägg. I många operativsystem ingår en klient/serverbrandvägg[52] som har till syfte att skydda informationssystemet mot angrepp genom att filtrera på både portar, typ av program och användarkonton med behörighet att initiera trafik.

Nätverksbrandväggen filtrerar inkommande och utgående nätverkstrafik utifrån exempelvis protokoll, portnummer och ip-adress, i vissa fall även innehåll. Nästa generations brandvägg kan filtrera informationsflöden från datalagret upp till applikationslagret i OSI-modellen.

Överväg användning av proxy-tjänster för att styra vissa typer av dataflöden, exempelvis webbtrafik så att organisationens klienter inte går att identifiera vid kommunikation på internet. Proxy-tjänster kan användas för att terminera trafiken så att externa dataflöden inte tillåts gå rakt in i informationssystemen i de interna nätverkszonerna. De interna systemen får istället hämta informationen i proxy-tjänsten. Proxy-tjänsten kan även begränsa vilka webbplatser som dataflödet får gå till och tillhandahålla viss övervakningsfunktionalitet. Internt kan proxyservrar användas för att reglera dataflöden mellan olika interna zoner.

Datadioder används för att förhindra tvåvägskommunikation. En sådan hårdvarukomponent tillåter kommunikation endast i en riktning och därmed blir det omöjligt att information överförs i motsatt riktning.

52. Kallas även hostbrandvägg.

Regler för filtrering

Organisationen behöver regelbundet se över de regler som den trafikfiltrerande utrustningen följer för att kontrollera att filtreringen endast tillåter sådan trafik som informationssystemen som placerats i nätverkssegmentet behöver. Om dataflöden endast ska tillåtas under en begränsad tid bör öppningen som tillåter dataflödet inaktiveras automatiskt när tidsperioden är över.

Dataflöden till fysiskt avskilda nätverkssegment[53] ska ske kontrollerat genom att till exempel flytta information på externa hårddiskar, usb-minnen eller cd-skivor. Alltså behöver även denna typ av fysiska dataflöden regleras. Organisationer som tar emot information från externa aktörer på till exempel cd, dvd och usb-minnen behöver även ha regler för hur innehållet i sådana fysiska dataflöden kontrolleras och godkänns innan de förs över till det fysiskt avskilda nätverkssegmentet. Det är lämpligt att kontrollen görs i en avskild it-miljö.

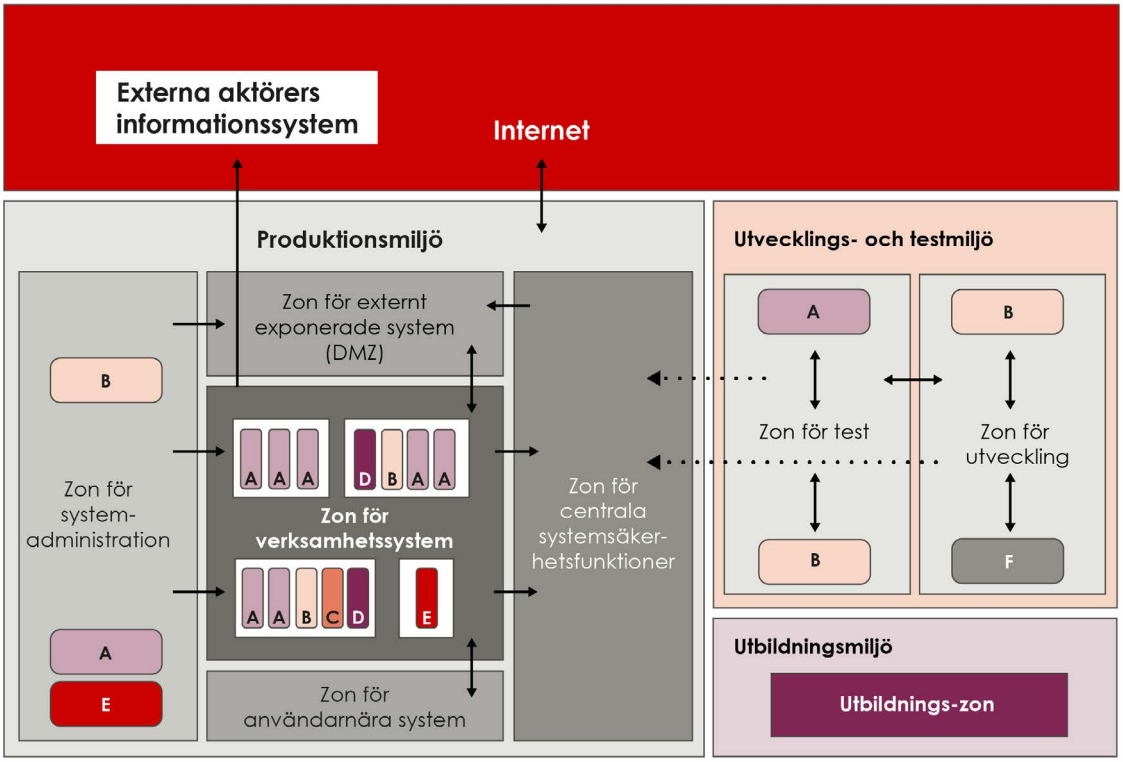
Filtrering mellan zoner

En organisation som delat in sitt nätverk i olika zoner behöver säkerställa att de regler för filtrering som gäller för respektive zon stödjer zonens syfte. Vilken riktning nätverkstrafiken tillåts ha inklusive var den får initieras respektive termineras har stor betydelse för organisationens möjlighet att skydda informationssystemen i de olika zonerna. Exempelvis behöver organisationen se till att nätverkstrafik från internet termineras i zonen för externt exponerade system och inte går direkt till ett informationssystem i en intern zon. Även nätverkstrafik från informationssystem som är sammankopplade med informationssystem hos en extern aktör bör om möjligt termineras i zonen för externt exponerade system och sedan hämtas därifrån av organisationens eget motsvarande informationssystem.

53. Kan i vissa fall kallas ”air gapping”, dvs. det finns bara luft mellan nätverken och ingen koppling (kablage, trådlös överföring m.m.) mellan det avskilda nätverket och övriga nätverk.

Det är också särskilt viktigt med ytterligare segmentering (sub- eller mikrosegmentering) av de zoner som har kopplingar till mer än en annan zon, särskilt när dessa zoner inte har någon inbördes koppling. Det finns annars risk för att en zon kan bli en brygga mellan de andra zonerna.

Zonmodellen har i figur 2 kompletterats med ytterligare segment och pilar för att illustrera lämplig riktning hos dataflöden.



Figur 2. Exempel på en organisations zoner, segment och kommunikationsvägar internt och mot omgivningen. A-F symboliserar informationssystem med olika funktioner och/eller som behandlar information med olika skyddsbehov.

4.2 Behörigheter och digitala identiteter

4.2.1 Syfte

För att kunna styra vilka användare och informationssystem som får agera i it-miljön behöver organisationen tilldela dessa digitala identiteter. För att också säkerställa att respektive digitala identitet endast får den åtkomst till information och informationssystem i it-miljön som den ska ha, behöver organisationen tilldela behörigheter till de digitala identiteterna.

4.2.2 Krav

Organisationen ska

1. säkerställa att endast behöriga användare och informationssystem har åtkomst till it-miljön[54]
2. utforma sin behörighetshantering på ett sätt som garanterar att varje digital identitet inte har mer åtkomst till information och informationssystem än vad den behöver[55]
3. se till att digitala identiteter som ger systemadministrativ behörighet endast används för systemadministration[56]
4. se till att systemaministrativa behörigheter tilldelas restriktivt.[57]

Organisationen bör

1. genom behörighetshantering säkerställa att[58]
   a. digitala identiteter i produktionsmiljön är unika
   b. digitala identiteter och behörigheter är godkända innan de kopplas till en användare eller ett informationssystem
   c. tilldelade behörigheter är tidsbegränsade och kontrolleras en gång per år
   d. behovet av att använda olika kataloger för digitala identiteter och behörigheter är identifierat och hanterat
   e. olika digitala identiteter används vid åtkomst till utvecklings- och testmiljö respektive produktionsmiljö.
2. säkerställa att en digital identitet endast kan användas av en individ[59]
3. hantera digitala identiteter och behörigheter som ger tillgång till externt åtkomliga informationssystem i kataloger skilda från kataloger för produktionsmiljön[60]
4. hantera digitala identiteter och behörigheter som ger tillgång till utvecklings-, test- och utbildningsmiljö i kataloger skilda från kataloger för produktionsmiljön[61]
5. säkerställa att en digital identitet med systemadministrativ behörighet endast ges åtkomst till en begränsad del av produktionsmiljön.[62]

54. MSBFS 2020:7 4 kap. 3 § Myndigheten ska säkerställa att endast behöriga användare och informationssystem har åtkomst till it-miljön och …

55. MSBFS 2020:7 4 kap. 3 § Myndigheten ska … utforma sin behörighetshantering på ett sådant sätt att varje digital identitet inte har mer åtkomst till information och informationssystem än vad den behöver.

56. MSBFS 2020:7 4 kap. 4 § Digitala identiteter som ger systemadministrativ behörighet ska endast användas för systemadministration och …

57. MSBFS 2020:7 4 kap. 4 § Digitala identiteter som ger systemadministrativ behörighet ska… tilldelas restriktivt.

58. Allmänt råd till MSBFS 2020:7 4 kap. 3 § Behörighetshanteringen bör säkerställa att 1. digitala identiteter i produktionsmiljön är unika, 2. digitala identiteter och behörigheter är godkända innan de kopplas till en användare eller ett informationssystem, 3. tilldelade behörigheter är tidsbegränsade och kontrolleras en gång per år, 4. behovet av att använda olika kataloger för digitala identiteter och behörigheter är identifierat och hanterat, och 5. olika digitala identiteter används vid åtkomst till utvecklings- och testmiljö respektive produktionsmiljö.

59. Allmänt råd till MSBFS 2020:7 4 kap. 3 § En digital identitet bör endast användas av en individ.

60. Allmänt råd till MSBFS 2020:7 4 kap. 3 § Digitala identiteter och behörigheter som ger tillgång till externt åtkomliga informationssystem samt utvecklings-, test- och utbildningsmiljö bör hanteras i olika kataloger skilda från kataloger för produktionsmiljön.

61. Allmänt råd till MSBFS 2020:7 4 kap. 3 § Digitala identiteter och behörigheter som ger tillgång till externt åtkomliga informationssystem samt utvecklings-, test- och utbildningsmiljö bör hanteras i olika kataloger skilda från kataloger för produktionsmiljön.

62. Allmänt råd till MSBFS 2020:7 4 kap. 4 § En digital identitet med systemadministrativ behörighet bör endast ges åtkomst till en begränsad del av produktionsmiljön.

4.2.3 Digitala identiteter

En digital identitet identifierar en person eller ett visst informationssystem i form av ett användarnamn eller systembeteckning. Det är vanligt att istället för digital identitet använda begreppet ”konto”, det vill säga att personen eller informationssystemet får ett ”konto” i it-miljön som är unikt för denne. En digital identitet bör endast användas av en person. Alla organisationer har ofta åtminstone tre olika typer av konton: användarkonton, systemadministrativa konton och systemkonton (för informationssystem). En digital identitet som ska användas för systemadministration ska tilldelas restriktivt.

När en organisation tilldelar en viss person en digital identitet behöver organisationen i de allra flesta fall kontrollera identiteten på personen innan den får en digital identitet och tilldelas ett konto i it-miljön. Det kan göras på olika sätt beroende på vilken nivå av tillit till att det är rätt person som behövs. Nivån av tillit till de digitala identiteterna för personer är beroende av hur identifieringen sker. Jämför med att vid en legitimationskontroll visa upp ett pass (ansökt och uthämtat på en polisstation), med ett körkort (ansökt på Trafikverket och uthämtat per rekommenderad post) och en hemmagjord identitetsbricka (oklar tillverkning och utgivningsprocess). I detta exempel skulle tilliten till passet vara högst, därefter körkortet och lägst till den egentillverkade identitetsbrickan. Om personen ska ha åtkomst till it-miljön behöver organisationen säkerställa identiteten, exempelvis genom ett fysiskt besök där personen får uppvisa giltig och verifierbar legitimation.

För att uppnå avsedd tillit till de digitala identiteterna, både internt och vid kommunikation med externa aktörer, behöver organisationen se till att de digitala identiteterna hanteras på ett säkert sätt avseende tilldelning, aktivering och inaktivering. Dessutom behöver organisationen se till att autentiserings-uppgifter skyddas och att det finns förmåga att upptäcka och hantera incidenter med koppling till digitala identiteter. Det är lämpligt att använda tekniskt stöd för hanteringen av digitala identiteter.

4.2.4 Behörighetshantering

Organisationen ska kunna hantera de digitala identiteternas behörigheter på ett sätt som garanterar att rätt behörighet knyts till rätt digital identitet. En behörighet kan utformas på olika sätt. Behörigheten kan exempelvis ge rätt att läsa, söka, skriva, radera och skapa information samt exekvera kod i ett informationssystem, men behörigheten kan även begränsas till en eller flera dessa rättigheter.

För att underlätta arbetet med att koppla rätt behörighet till respektive digital identitet behöver organisationen kartlägga och definiera vilka olika användargrupper, av både personal och informationssystem, som finns i organisationen. Exempel på sådana användargrupper är

- all egen personal
- inhyrd personal
- utifrån verksamheten anpassade grupper för personal utifrån arbetsuppgift, till exempel ekonomi, forskning
- individuellt anpassade behörigheter, exempelvis vid behov av utökad behörighet att utföra vissa arbetsuppgifter
- personal med systemadministrativa behörigheter
- digitala identiteter för informationssystem och tjänster
- digitala identiteter för utvecklings- och testmiljö
- temporära digitala identiteter.

Förvaltning av behörigheter

En digital identitet behöver förvaltas över hela dess livscykel, och det är viktigt att ha kontroll över digitala identiteter för både användare och informationssystem inklusive tjänster. Behörigheter som tilldelas en digital identitet behöver ofta ändras över tid. Exempelvis kan användaren med den digitala identiteten byta arbetsuppgift eller avsluta sin anställning. Det är lämpligt att alla behörigheter är tidsbegränsade. Detta kräver en aktiv behörighetshantering som bland annat inne-

fattar påminnelser om att tidsbegränsningen är på väg att gå ut. Påminnelserna behöver fungera på ett sådant sätt att de digitala identiteter som ska behålla sin behörighet får den förlängd utan störning. Organisationen behöver genom sin behörighetshantering ha förmåga att beställa, godkänna och förändra behörigheten hos en digital identitet eller en grupp av digitala identiteter på ett korrekt, snabbt och spårbart sätt. Behörigheter behöver tilldelas efter beslut av den ansvariga, ofta informationsägaren för berörda informationssystem. Se till att beslut om förändringar av behörigheter kan kopplas till en ansvarig person samt samt visa vid vilken tidpunkt beslutet fattades. Organisationen behöver tilldela behörigheter som ger åtkomst till information av högt skyddsvärde på ett restriktivt sätt.

Det arbetssätt som organisationen använder för sin behörighetshantering behöver innehålla regler för att omedelbart inaktivera digitala identiteter efter att en anställning (fast eller tillfällig) eller ett uppdrag avslutas. Det är betydligt bättre att inaktivera digitala identiteter som inte används än att radera dem. Detta för att vid behov, exempelvis vid behörighetsrevision eller loggkontroller, kunna gå tillbaka och se vem som haft den digitala identiteten. Det behöver även finnas regler till stöd för regelbunden kontroll och revidering av att behörighetstilldelningen är korrekt. Kontroll behöver också i samband med att personal börjar, byter tjänst, är tjänstlediga eller slutar. Bedöm möjligheten att aktivera de digitala identiteter leverantörer använder för åtkomst till it-miljön under den tidsperiod som behövs för att leverantören ska utföra det uppdrag organisationen gett dem, och, om möjligt, inaktivera den digitala identiteten per automatik efter en given tidsgräns. Vid revision är det särskilt viktigt att gå igenom alla digitala identiteter för informationssystem inklusive tjänster, både interna och externa, exempelvis molntjänster. Inaktivera digitala identiteter som inte kan knytas till ett verksamhetsbehov eller som inte har en informationsägare som kan visa på verksamhetsbehovet. Det är också viktigt att genomföra revision av de systemadministrativa behörigheterna.

Rollseparering

När behörigheter delas ut till användarna behöver organisationen säkerställa att samma person inte har i uppgift (och behörighet) att både utföra en åtgärd och granska den. Exempelvis ska inte den som ansvarar för analysen av loggarna ha behörighet att ändra i, eller radera, loggarna. Motsvarande uppdelning (rollseparering) är sedan länge standard inom de företagsekonomiska processerna, till exempel genom att separera rollen som har åtkomst till kontot för in- och utbetalningar (kassör) från rollen som kontrollerar att bankutdragen är korrekt gjorda (revisor)

respektive den som lämnar in kvitton från den som godkänner utgiften (attestant). Om det inte finns tillräckligt med medarbetare för att införa behövd rollseparering, se till att samma person har olika konton för olika uppgifter och kompensera med extra kontroller. Det gäller särskilt arbetsuppgifter som kräver höga behörigheter.

Hantering av högre behörigheter

I de fall användandet av ett informationssystem förutsätter att en användare ges behörighet att konfigurera funktioner som kan påverka säkerheten, behöver detta riskbedömas och kompenserande säkerhetsåtgärder införas såsom extra övervakning och logganalys.

Det bästa ur en angripares synvinkel är att få kontroll över digitala identiteter med systemadministrativa behörigheter, eftersom det i många fall ger en mycket omfattande åtkomst till it-miljön. Tilldelning av systemadministrativa behörigheter ska därför göras restriktivt och sådana behörigheter ska endast användas för systemadministration. För att minska konsekvenserna av misstag, exempelvis vid konfigurering i it-miljön bör en systemadministrativ behörighet inte omfatta hela it-miljön, utan endast en del denna. Det minskar även konsekvenserna av ett angrepp. Använd olika digitala identiteter för olika funktioner, till exempel för systemadministration av klienter, servrar, nätverk och olika säkerhetsfunktioner.

För att underlätta installation och drift levereras många mjukvaror med höga behörigheter förinställda. Exakt vilka behörigheter som behövs för att mjukvaran ska fungera kan vara dåligt dokumenterat av leverantören. Det kan i sin tur leda till att många organisationer behåller de förinställda höga behörigheterna. För att säkerställa att organisationen endast har aktiverat de behörigheter som motsvarar verksamhetens behov behöver organisationen ställa krav på leverantören att tillhandahålla underlag om vilka behörigheter som behövs för olika funktioner.

En god behörighetshantering minskar risken för att en extern eller intern angripare kan komma åt it-miljön genom att exempelvis använda digitala identiteter som borde ha varit inaktiverade eller digitala identiteter med onödigt höga behörigheter. När en angripare fått tillgång till ett informationssystem är nästa steg ofta att skaffa sig åtkomst till ännu fler delar av it-miljön. Detta görs antingen genom att ta över fler digitala identiteter för användare eller informationssystem, eller genom att försöka höja behörigheterna hos den digitala identiteten som angriparen kommit över.

4.2.5 Katalogtjänster och andra verktyg

Med katalogtjänst avses här ett informationssystem (databas) som samlar och hanterar digitala identiteter och behörigheter, ett så kallat IAM-system (Identity and Access Management). För de flesta organisationer förutsätter en fungerande hantering av digitala identiteter och behörigheter användning av katalogtjänster. För att underlätta behörighetsrevisioner och enklare kunna säkerställa rollseparering är det lämpligt att undvika att hantera identiteter lokalt för enskilda informationssystem. Genom katalogtjänsten kan alla digitala identiteter och deras behörigheter hållas samlade och enkelt uppdateras. I en katalogtjänst (till exempel Microsoft Active Directory) förekommer normalt digitala identiteter för användare, systemadministratörer och informationssystem (exempelvis klienter, servrar och nätverk) inklusive tjänster.

Alla förändringar i katalogtjänsten ska vara spårbara. Använd katalogtjänster som inte bara kan hantera de digitala identiteterna på individnivå, utan även ger stöd vid organisatoriska förändringar. Som grund vid uppdatering av de digitala identiteterna och behörigheterna är det lämpligt att ha en pålitlig datakälla, exempelvis organisationens personaladministrativa system. Att ha olika separerade katalogtjänster medför en högre säkerhet, så att inte ett konto som används av en obehörig kan ge alltför stor åtkomst till

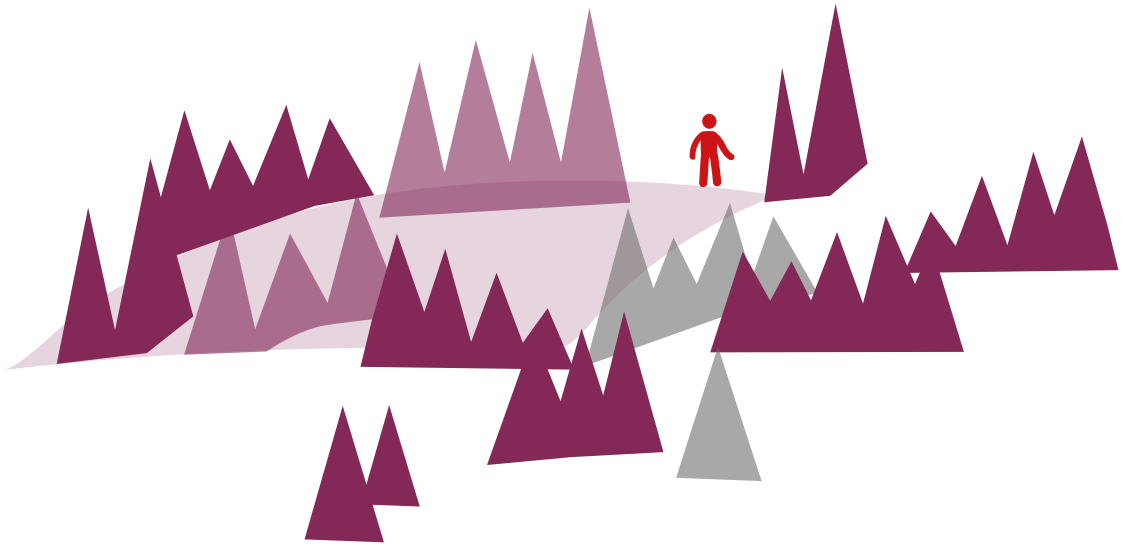
it-miljön. Det är viktigt att ha ett arbetssätt som säkerställer att de som administrerar katalogtjänsterna hanterar de risker det innebär att de olika katalogtjänsterna litar på varandra. Säkerställ inför upphandling av nya informationssystemen att de kan använda befintlig katalogtjänst.

Om en obehörig person får åtkomst till en digital identitet med systemadministrativ-behörighet i en katalog kan den användas för att skaffa åtkomst till övriga digitala identiteter i katalogen. Om bara en katalog används innebär det att angriparen kan få åtkomst till hela it-miljön. Om olika digitala identiteter hanteras i olika kataloger minskar denna risk. När man skapar kataloger kan till exempel organisationens zonindelning ligga till grund. Organisationen bör minst hantera digitala identiteter och behörigheter som ger tillgång till externt åtkomliga informationssystem samt utvecklings-, test- och utbildningsmiljö i kataloger skilda från kataloger för produktionsmiljön.

I it-miljön kan det ibland finnas behov av att sätta upp lokala och ibland temporära digitala identiteter i exempelvis databaser och operativsystem. Även dessa digitala identiteter kan utnyttjas av angripare för att skaffa sig tillgång till värdefull information, utökade behörigheter eller åtkomst till andra kritiska system, och de behöver därför ges ett motsvarande skydd.

4.2.6 Särskilt om utvecklings- och testmiljöer

Organisationen bör inte låta medarbetarna använda samma digitala identitet och autentiseringsuppgifter i utvecklings- och testmiljöerna som i produktionsmiljön. Detta för att it-miljöerna för utveckling och test ofta är mindre skyddade än produktionsmiljön. Om samma digitala identitet används i både dessa miljöer och produktionsmiljön, finns risk att information om den digitala identiteten och dess autentiseringsuppgifter blir lättare åtkomliga vid ett angrepp i de ofta mindre skyddade utvecklings- och testmiljöerna. Ett exempel på detta är när en digitala identitet och dess autentiseringsuppgifter som används i utvecklings- och testmiljöer skrivs in och lagras oskyddade i källkod och mjukvara som obehöriga kan få åtkomst till.



4.3 Autentisering

4.3.1 Syfte

För att skydda organisationens informationssystem mot obehörig åtkomst behöver organisationen ha interna regler för att skydda sina autentiseringsuppgifter och i vissa fall använda flerfaktorsautentisering.

4.3.2 Krav

Organisationen ska

1. använda flerfaktorsautentisering vid[63]
   a. egen och inhyrd personals åtkomst till produktionsmiljön via externt nätverk
   b. systemadministrativ åtkomst till informationssystem
   c. åtkomst till informationssystem som behandlar information som bedömts ha behov av utökat skydd
2. ha interna regler för hantering av autentiseringsuppgifter med krav på[64]
   a. längd och komplexitet
   b. när byte ska ske
   c. hur distribution ska ske
   d. hur autentiseringsuppgifterna ska skyddas.

Organisationen bör använda tekniska system för att stödja efterlevnaden av reglerna avseende autentiseringsuppgifternas längd, komplexitet och byte.[65]

63. MSBFS 2020:7 4 kap. 5 § Flerfaktorsautentisering ska användas vid 1. egen och inhyrd personals åtkomst till produktionsmiljön via externt nätverk, 2. systemadministrativ åtkomst till informationssystem, och 3. åtkomst till informationssystem som behandlar information som bedömts ha behov av utökat skydd.

64. MSBFS 2020:7 4 kap. 6 § Myndigheten ska ha interna regler för hantering av autentiseringsuppgifter med krav på 1. längd och komplexitet, 2. när byte ska ske, 3. hur distribution ska ske, och 4. hur autentiseringsuppgifterna ska skyddas.

65. Allmänt råd till MSBFS 2020:7 4 kap. 6 § Tekniska system bör användas för att stödja efterlevnaden av reglerna avseende längd, komplexitet och byte.

4.3.3 Autentisering

I en it-miljö behöver organisationen kunna verifiera att en person eller ett informationssystem som använder en viss digital identitet är den de utger sig för att vara. Detta sker genom autentisering.[66] Autentisering används exempelvis när en användare loggar in i en it-miljö eller ett informationssystem respektive när ett informationssystem ska verifiera sin identitet gentemot ett annat informationssystem. Vanliga autentiseringsuppgifter är lösenord, lösenordsfraser och pinkoder (alla tre något du vet), fingeravtryck (något du är) och kort med mikrochip (något du har). Det traditionella sättet att autentisera en uppgiven digital identitet är att användaren uppger sitt användarnamn och lösenord, vilket sedan kontrolleras mot organisationens register över digitala identiteter, lösenord och behörigheter. Att endast använda lösenord för autentisering är ofta inte tillräckligt säkert. Detta gäller särskilt om längden och komplexitet hos lösenordet inte är tillräcklig, om de är enkla att gissa eller om de inte omgärdas av tillräckligt högt skydd när de distribueras eller lagras. De tekniker som används av angripare för att hitta svaga lösenord blir också bättre och bättre.

Brister i hur lösenord skapas, distribueras och lagras samt hanteras av användaren möjliggör för angripare att exempelvis

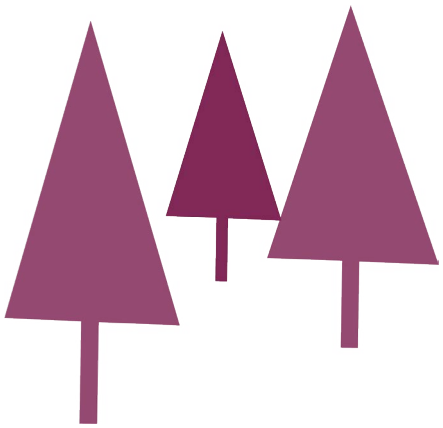
- gissa lösenord
- ta del av lösenord genom att hitta dem när de distribueras eller lagras i klartext
- forcera krypterade lösenord genom att använda datorkraft
- lura användaren att ange sitt lösenord (till exempel genom phishing).

66. I engelsk text används i huvudsak begreppet ”authenticate” och ”authentication”, vilket försvenskat alltså blir ”autentisera” och ”autentisering”. I eSAM:s vägledning *Juridisk vägledning för införande av e-legitimering och e-underskrifter* (utgåva 1.1, juni 2018) anges att ”autentisering” och ”e-identifiering” är samma sak.

Om samma lösenord används till flera olika digitala identiteter blir konsekvenserna för organisationen av att obehöriga får tillgång till lösenordet allvarligare eftersom fler informationssystem berörs vilket kräver en mer omfattande incidenthantering.

Behovet av tillgång till säkra sätt att autentisera sig i olika digitala miljöer ökar. Ett exempel är att i sin yrkesroll kunna legitimera sig i digital miljö utanför organisationen. Utvecklingen av särskilda autentiseringslösningar som är avsedda att användas i yrkesrollen sker både på nationell och EU-nivå.[67] Möjligheten att autentisera sig som privatperson har funnits under en längre tid.

Organisationer som idag utbyter information med varandra använder ofta olika federativa autentiseringslösningar. Vid användning av federativa autentiseringslösningar tillkommer ytterligare en dimension som behöver skyddas, nämligen hanteringen och kommunikationen av de certifikat som skickas mellan det informationssystem som utför autentiseringskontrollen och det informationssystem som kräver intyg för att ge åtkomst.



67. Mer om utvecklingen av digitala tjänstelegitimationer finns på https://www.digg.se/digitala-tjanster/e-legitimering.

4.3.4 Flerfaktorsautentisering

På grund av de säkerhetsbrister som är förknippade med att endast använda användarnamn och lösenord som autentiseringsmetod går många organisationer över till flerfaktorsautentisering. Med det menas autentisering baserad på flera olika typer av autentiseringsuppgifter (något man vet, något man är respektive något man har). Inloggning med till exempel två lösenord (båda något man vet) är sålunda inte en flerfaktorsautentisering. Flerfaktorsautentisering kan även kallas stark autentisering.

Några exempel på flerfaktorsautentisering med två olika faktorer (tvåfaktorsautentisering):

- Ett kort med mikrochip tillsammans med användarens pinkod (något man **har** kombinerat med något man **vet**).
- Ett kort med mikrochip tillsammans med ett fingeravtryck (något man **har** kombinerat med något man **är**).
- En pinkod för en lösenordsdosa som genererar en engångskod (något man **vet** kombinerat med något man **har**).

Genom flerfaktorsautentisering minskar risken för obehörig autentisering, eftersom det inte räcker för en angripare att skaffa sig tillgång till en autentiseringsuppgift. Angriparen måste exempelvis komma över både kortet med mikrochip (genom att stjäla eller hitta det) och tillhörande pinkod (via dataintrång eller genom att lura användaren att uppge det) för att kunna använda den digitala identitetens behörigheter.

Säkerheten i en flerfaktorsautentiseringslösning förutsätter att både administrativa rutiner och tekniska säkerhetsfunktioner är korrekt införda. Exempelvis behöver de administrativa rutinerna säkerställa att:

- tilldelningen av autentiseringsuppgifter (exempelvis lösenord, lösenordsfras eller pinkod) sker på ett korrekt sätt
- användare byter tilldelade autentiseringsuppgifter innan användning

- hjälpmedel för autentiseringsuppgifter (så som lösenordsdosa, eller kort med microchip) tilldelas rätt användare på ett korrekt sätt

Det behöver dessutom finnas rutiner för hur en förlust av hjälpmedel för autentisering, exempelvis en lösenordsdosa, ska hanteras. Den tekniska lösningen behöver installeras och förvaltas så att kravet på flerfaktorsautentisering inte går att kringgå.[68]

Vissa informationssystem tillåter inte användning av lösningar för flerfaktorsautentisering direkt mot systemet. Sådana system ska inte användas för information i behov av utökat skydd eller för systemadministration.

4.3.5 Krav på flerfaktorsautentisering

En organisation väljer utifrån informationsklassning och riskbedömning i vilka situationer flerfaktorsautentisering behöver användas. I nedanstående tre fall ska organisationen alltid använda flerfaktorsautentisering.

Egen och inhyrd personals åtkomst till produktionsmiljön via externt nätverk

Personal som arbetar på distans har ofta behov av att få åtkomst till organisationens produktionsmiljö. För att skydda produktionsmiljön mot angrepp räcker det inte att endast kräva användarnamn och lösenord vid inloggning via ett externt nätverk. Flerfaktorsautentiseringen kan sättas upp på olika sätt men krävs oavsett om personalen loggar in via organisationens egna klienter eller egen utrustning. Det räknas inte som flerfaktorsautentisering om personalen loggar in på en klient med endast användarnamn och lösenord, även om klienten är kopplad med certifikat via en vpn-tunnel till produktionsmiljön.[69] Anledningen är att certifikaten endast används för att identifiera utrustning inte personer.

Det är lämpligt att endast tillåta inloggning via klienter som organisationen tillhandahållit och konfigurerat så att organisationens säkerhetskrav uppfylls. En organisation som ändå tillåter personal att logga in i produktionsmiljön via egen utrustning behöver hantera de risker detta innebär, exempelvis att inte kunna kontrollera om den privata utrustningen har tillräckliga säkerhetsåtgärder och inte heller kunna åtgärda eventuella brister. Ett sätt att skydda produktionsmiljön vid åtkomst via externt nätverk är att endast ge åtkomst till en virtuell kopia av produktionsmiljöns informationssystem så kallad Virtual desktop infratructure (VDI).

Organisationer kan behöva tillåta andra än personalen att få tillgång till vissa delar av produktionsmiljön. Det handlar exempelvis om externa webbplatser eller motsvarande dit allmänheten ges tillgång.[70] Vissa organisationer erbjuder olika tjänster för andra än personalen, vilket också innebär att den valda målgruppen ges tillgång till vissa delar av produktionsmiljön. Organisationen behöver då, utifrån informationsklassning och riskbedömning, bedöma vilka autentiseringssätt och övriga säkerhetsåtgärder, exempelvis nätverkssegmentering och filtrering, som behövs för att hantera identifierade risker. Tjänster som innebär åtkomst till information i behov av utökat skydd ska alltid skyddas med flerfaktorsautentisering.

Systemadministrativ åtkomst till informationssystem

För att kunna utföra systemadministrativa uppgifter behövs i de flesta fall en hög behörighet, det vill säga den digitala identiteten som systemadministratören använder

68. Om ett informationssystem parallellt med flerfaktorsautentiseringen accepterar åtkomst med enbart lösenord så finns det från en angripares perspektiv ingen flerfaktorsautentisering, utan säkerheten är i slutändan baserad på lösenord. Exempel: om en webbtjänst kräver inloggning med eID för medborgarna, samtidigt som webbtjänstens administrationsgränssnitt enbart skyddas med användarnamn och lösenord, så anses inte systemet vara skyddat med flerfaktorsautentisering.

69. Eftersom certifikatet endast autentiserar klienten, identifieras användaren i detta fall endast genom en autentiseringsuppgift – användarnamn och lösenord.

70. I de fall egen eller inhyrd personal använder externa webbplatser eller motsvarande likställs de med allmänheten.

ges behörighet att utföra en rad åtgärder som användare inte ska ha rättigheter till. Exempel på sådana åtgärder är att ändra konfigurationer, förändra loggsystem, ändra behörigheter och konfigurera om brandväggar. Eftersom sådana åtgärder kan få stor påverkan på säkerheten i informationssystemen och it-miljön i sin helhet, ska digitala identiteter med systemadministrativ åtkomst skyddas genom flerfaktorsautentisering.

Åtkomst till information i behov av utökat skydd

Vissa informationssystem hanterar information som behöver ett utökat skydd med hänsyn till behov av konfidentialitet, riktighet eller tillgänglighet. Vilken information som behöver ett sådant skydd framgår av organisationens informationsklassning.[71] Exempel på information som med hänsyn till behov av konfidentialitet ofta bedöms vara i behov av utökat skydd är information som skulle kunna omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) eller definieras i dataskyddsförordningen[72] som särskilda kategorier av personuppgifter, så kallade ”känsliga personuppgifter”.

4.3.6 Hantering av autentiseringsuppgifter

Autentiseringsuppgifter behöver ha den längd och komplexitet som krävs för att ge avsett skydd. Dessutom behöver de hanteras på ett säkert sätt. Det handlar om att säkerställa att autentiseringsuppgifterna tilldelas rätt användare och informationssystem, att överföringen av dem sker på ett skyddat sätt samt att de förvaras säkert. Det behöver vara tydligt för alla berörda hur detta ska uppnås. Organisationen ska därför ha interna regler som ställer krav på autentiseringsuppgifternas längd och komplexitet, när de ska bytas och hur de ska distribueras och skyddas. Samtliga krav behöver utformas utifrån organisationens riskbedömning.

Följande behöver omhändertas:

- Autentiseringsuppgifter som enbart används tillsammans med användarnamn behöver vara långa och helst i form av en lösenordsfras, medan det ofta räcker med en kortare pinkod för att låsa upp ett kort med microchip eller en engångslösenordsdosa.
- Distribution av nya autentiseringsuppgifter (exempelvis lösenord) behöver ske på ett sätt som garanterar att det är rätt användare som får tillgång till uppgifterna. Säker distribution kan underlättas när organisationen använder flerfaktorsautentisering.
- Autentiseringsuppgifter, åtminstone i produktionsmiljön, behöver skyddas genom att inte skickas eller lagras okrypterade.

4.3.7 Tekniska system för hantering av autentiseringsuppgifter

Hantering av autentiseringsuppgifter och behörigheter underlättas genom att använda centraliserat systemstöd. Med hjälp av informationssystem för att hantera användarnamn, lösenord och behörigheter på ett samlat sätt, så kallade Identity and Access Management system (IAM), kan de personer i organisationen som arbetar med behörighetshantering enkelt lägga till, ta bort eller ändra både digitala identiteter och behörigheter. Med hjälp av IAM kan organisationen lätt få en överblick över alla användares behörigheter. Ett IAM-system kan även användas för att säkerställa efterlevnad av organisationens krav på lösenord avseende längd, komplexitet och byten. Det kan även användas för att säkerställa att lösenorden är unika och inte återanvänds.

71. Krav på att klassa sin information avseende konfidentialitet, riktighet och tillgänglighet i olika nivåer framgår av MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6) 6 § p. 1.

72. Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Om organisationen tillåter användarna att skapa och lagra sina lösenord och koder med stöd av lösenordshanterare, behöver organisationen kravställa och granska detta informationssystem på motsvarande sätt som övriga informationssystem i behov av utökat skydd. Lösenordshanterare som hanterar användarnas lösenord på internet är inte lämpliga att använda, eftersom det kan vara svårt (eller omöjligt) att garantera att lösenorden hanteras säkert hos leverantören.

4.3.8 Vanliga angreppssätt

Ett vanligt tillvägagångssätt för en angripare att få tag på autentiseringsuppgifter är att skicka ut e-post med en uppmaning att gå till en webbsida som liknar inloggning till webbmejlen eller en organisations egna tjänster. Om en användare luras att skriva in sina autentiseringsuppgifter på en sådan webbsida, fångas dessa upp av angriparen.

Angriparen använder sedan autentiseringsuppgifterna för att ta sig in i organisationens it-miljö. Riskerna för att drabbas av denna typ av angrepp minskas när organisationen använder flerfaktorsautentisering vid inloggning till sin it-miljö. Organisationen behöver dock vara uppmärksam på risken för så kallad ”man in the middle attack”[73] eftersom den även kan användas mot vissa flerfaktorsautentiseringslösningar, exempelvis vid användning av lösenordsdosa som genererar engångskoder.

Flerfaktorsautentisering baserad på att en engångskod skickas ut över sms via mobiloperatörsnät är sårbar, eftersom sms kan manipuleras av en angripare. Vid autentisering via sms-tjänster behöver man även beakta risken med bristfällig mobiltäckning eller otillräcklig leveranssäkerhet, vilket kan ge problem när organisationens användare behöver en engångskod för att kunna logga in.

73. Vid en ”man in the middle attack” där en angripare genom aktiv inkoppling i en kommunikation mellan två parter samtidigt simulerar respektive parts identitet mot den andre och därvid kan avlyssna eller förändra överförd information.

4.4 Kryptering

4.4.1 Syfte

För att skydda organisationens information mot obehörig åtkomst och obehörig förändring, både vid överföring och lagring, behöver organisationen använda kryptering på ett sätt som motsvarar behoven.

4.4.2 Krav

Organisationen ska

1. identifiera och hantera behovet av kryptering för att skydda informationen mot[74]
   a. obehörig åtkomst vid överföring och lagring
   b. obehörig förändring vid överföring och lagring
2. ha interna regler för kryptering med krav på[75]
   a. hantering av krypteringsnycklar
   b. godkännande och förvaltning av krypteringslösningar
   c. val av krypteringsalgoritmer, krypteringsprotokoll och nyckellängder
3. använda Domain Name System Security Extensions (DNSSEC) för domännamn som är registrerade i domännamnssystemet (DNS).[76]

Organisationen bör[77]

1. använda kryptering för att skydda
   a. säkerhetsloggar mot obehörig åtkomst och obehörig förändring
   b. autentiseringsuppgifter mot obehörig åtkomst och obehörig förändring
   c. information i behov av utökat skydd mot obehörig åtkomst och obehörig förändring vid överföring till informationssystem utanför organisationens kontroll
2. införa möjlighet att verifiera organisationen som avsändare respektive mottagare av e-post
3. identifiera behovet av att kryptera e-post på transportlagret.

Statliga myndigheter bör därutöver införa möjlighet att kryptera e-post på transportlagret vid överföring till och från andra statliga myndigheter.

4.4.3 Skydd mot obehörig åtkomst och förändring

Kryptering är en viktig säkerhetsåtgärd för att skydda information när den lagras eller överförs. Genom att använda kryptering på rätt sätt kan organisationen skydda sin information mot att obehöriga tar del av den (konfidentialitet) eller obehörigt förändrar den (riktighet).

Genom kryptering går det också att verifiera att den information som en avsändare skickat är densamma som mottagaren tar emot (autenticitet avseende innehåll). Det går även att verifiera att meddelandet kommer från den avsändare som uppgivits (autenticitet avseende ursprung).

74. MSBFS 2020:7 4 kap. 7 § Myndigheten ska identifiera och hantera behovet av kryptering för att skydda information mot obehörig åtkomst och obehörig förändring vid överföring och lagring.

75. MSBFS 2020:7 4 kap. 9 § Myndigheten ska ha interna regler för kryptering med krav på 1. hantering av krypteringsnycklar, 2. godkännande och förvaltning av krypteringslösningar, och 3. hur krypteringsalgoritmer, krypteringsprotokoll och nyckellängder ska väljas.

76. MSBFS 2020:7 4 kap. 8 § Myndigheten ska använda Domain Name System Security Extensions (DNSSEC) avseende samtliga domännamn som myndigheten registrerat i domännamnssystemet (DNS).

77. Allmänt råd till MSBFS 2020:7 4 kap. 7 § Kryptering bör användas för att skydda 1. säkerhetsloggar mot obehörig åtkomst och obehörig förändring, 2. autentiseringsuppgifter mot obehörig åtkomst och obehörig förändring, och 3. information i behov av utökat skydd mot obehörig åtkomst och obehörig förändring vid överföring till informationssystem utanför myndighetens kontroll. Myndigheten bör identifiera behovet av att kryptera e-post på transportlagret i enlighet med OSI-modellen (Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model, ISO/IEC 7498-1) eller motsvarande. Myndigheten bör också införa möjlighet att använda sådan kryptering vid överföring av e-post till och från andra statliga myndigheter. Myndigheten bör införa möjlighet att verifiera myndigheten som avsändare respektive mottagare av e-post.

Det finns två huvudtyper av kryptering, symmetrisk och asymmetrisk. Vid symmetrisk kryptering används samma krypteringsnyckel vid både kryptering och dekryptering, vilket förutsätter att avsändare och mottagare har identiska nycklar. Skyddet vid symmetrisk kryptering förutsätter att ingen annan har fått tillgång till nycklarna vilket gör att överlämningen av nyckeln till motparten är ett kritiskt moment. Vid användning av asymmetrisk kryptering används istället ett nyckelpar. Det som *krypteras* med den ena nyckeln i nyckelparet kan endast *dekrypteras* med den andra nyckeln i nyckelparet och vice versa. Varje användare av asymmetrisk kryptering har ett eget nyckelpar. Den ena nyckeln behöver skyddas mot obehörig åtkomst (privat nyckel) medan den andra nyckeln (publik nyckel) tillhandahålls till alla som önskar kommunicera krypterat med användaren.

Hashfunktioner är en vanlig tillämpning av asymmetrisk kryptering, med ett specifikt användningsområde. Hashfunktioner använder inga nycklar utan endast en krypteringsalgoritm för att göra en beräkning på utvald information och därigenom skapa en för informationen unik hashsumma (digitalt fingeravtryck). Hashsumman går inte, och är inte heller avsedd att kunna, dekrypteras (envägskryptering).

- *Symmetrisk kryptering* är snabbare och mindre resurskrävande än asymmetrisk kryptering, vilket gör att den ofta används vid kryptering av, särskilt stora, informationsmängder för att uppnå konfidentialitet.
- *Asymmetrisk kryptering* används främst för att uppnå riktighet men kan även säkerställa konfidentialitet. Den är mer tekniskt avancerad och kräver mer datorkraft än symmetrisk kryptering, vilket ofta gör den långsammare. Asymmetrisk kryptering används bland annat för att kunna överlämna en symmetrisk nyckel på ett säkert sätt till motparten och skapa digitala signaturer i PKI-lösningar (public key infrastructure). Genom att använda digitala signaturer kan en avsändare med sin privata nyckel *signera* ett meddelande[78], och mottagaren kontrollera att meddelandet verkligen kommer från avsändaren genom att *verifiera* meddelandets signatur med avsändarens publika nyckel.
- *Hashfunktioner:* Hashfunktioner används främst till att upptäcka obehörig förändring av information. Om hashsumman som avsändaren beräknar för ett meddelandes information, och bifogar meddelandet, inte överensstämmer med den hashsumma som mottagaren räknar fram på samma meddelande, har informationen förändrats. Hashfunktioner (envägskryptering) ingår som en del i digital signering av meddelanden. Detta för att kunna både säkerställa att innehållet inte förändrats (hashfunktionen) och verifiera avsändaren (genom asymmetrisk kryptering).

Kryptering kan behövas både när information överförs och när den lagras. Överföring av information sker både till andra aktörer och i organisationens egna nätverk. Vid överföring av information till informationssystem utanför organisationens kontroll, ska organisationen alltid överväga behovet av kryptering. I de fall information som enligt informationsklassningen är i behov av utökat skydd överförs bör organisationen alltid använda kryptering. Det kan även finnas anledning att använda kryptering vid överföring internt mellan olika nätverkssegment, särskilt om informationen är i behov av utökat skydd.

Vid lagring av information finns det i huvudsak två sätt att kryptera. Antingen krypteras informationen innan den lagras eller så krypteras informationen när den kommer till lagringsytan (hårddiskkryptering). Vilken lösning som ska användas beror på organisationens behov. Exempelvis är det lämpligt att loggar och lösenord krypteras direkt när de samlas in och förs över till lagringsytan i redan krypterad form. Hårddiskkryptering

78. Oftast signeras inte hela meddelandet utan endast meddelandets hashsumma som avsändaren tagit fram med hjälp av en hashfunktion.

används inte sällan på klienter för att skydda informationen när klienten är avstängd. Säkerhetsloggar bör alltid skyddas mot obehörig åtkomst och obehörig förändring genom kryptering. Detsamma gäller autentiseringsuppgifter såsom lösenord, lösenordsfraser, pinkoder, fingeravtryck och autentiseringsuppgifter som lagras på kort med mikrochip.

Det finns många olika sätt att lösa en organisations behov av kryptering. Krypteringslösningar ingår ofta i andra produkter och tjänster där kryptering kan behövas, exempelvis webbläsare eller e-postsystem. Organisationen kan även skaffa krypteringsfunktionalitet genom fristående produkter, i form av både hårdvara och mjukvara. Valet av krypteringslösningar behöver även beakta om det handlar om att skydda lagrad information eller information som överförs mellan informationssystem. Styrkan i krypteringen behöver motsvara skyddsbehovet både avseende nivå och tidsperiod. Skyddsbehovet behöver därför styra hur krypteringslösningen behöver konfigureras avseende krypteringsalgoritm, krypteringsprotokoll och nyckelängder samt hur krypteringsnycklarna hanteras.

4.4.4 Interna regler för kryptering

Kryptering är en viktig säkerhetsåtgärd, men förutsätter att den införs och förvaltas på rätt sätt för att ge avsett skydd för organisationens information. Om krypteringsnycklar inte hanteras korrekt eller felaktiga konfigurationer av krypteringsprodukter sker, kan organisationen få stora problem. Brister i skyddet av krypteringsnycklar kan medföra att obehöriga får tillgång till skyddad information. Bristande rutiner kring uppdatering av organisationens krypteringsnycklar kan resultera i att den skyddsvärda informationen blir otillgänglig för organisationen. Felaktig eller utebliven konfiguration av krypteringsprodukter kan få till konsekvens att organisationens bild av skyddet inte överensstämmer med det skydd som har införts. De krypteringslösningar som erbjuds i kommersiella produkter är ofta lätta att komma igång med, men de förinställningar som är gjorda av leverantören behöver inte vara de som passar organisationens behov.

De medarbetare som konfigurerar och förvaltar krypteringslösningar måste ha rätt utbildning och kompetens för sin uppgift. Det ska också finnas interna regler för hur krypteringsnycklar hanteras, hur krypteringslösningar godkänns och förvaltas samt hur krypteringsalgoritmer, krypteringsprotokoll och nyckellängder ska väljas. Det behöver finnas dokumentation för varje krypteringslösning där vald konfiguration beskrivs.

De interna reglerna för kryptering bör tas fram av en it-säkerhetsspecialist i samverkan med den som leder och samordnar informationssäkerhetsarbetet och den som är ansvarig för it-driften i organisationen.

Hantering av krypteringsnycklar

För att kryptering ska kunna ge avsett skydd behöver organisationen hantera krypteringsnycklar på ett säkert sätt. Nyckelhantering omfattar alla nödvändiga åtgärder för att skapa, skydda, kontrollera användandet av och slutligen avaktivera eller förstöra krypteringsnyckeln.[79] Detta gäller både nycklar som används vid symmetrisk kryptering och den privata nyckeln i ett asymmetriskt nyckelpar. Genom interna regler kan organisationen säkerställa att nycklarna hanteras på ett säkert sätt. Det handlar bland annat om att omhänderta följande risker:

- Krypteringsnycklar görs åtkomliga för obehöriga individer eller informationssystem. Vanliga exempel på detta är när krypteringsnycklar läggs in i källkodbasen (ofta av bekvämlighetsskäl), när de skickas öppet per e-post eller när de ligger oskyddade på filservern.

79. Hela processen från att en krypteringsnyckel skapas tills den ska förstöras kallas för nyckelns livscykel (eng. *key management life cycle*).

- Krypteringsnycklar förstörs eller förloras vilket gör att krypterad information inte kan göras läsbar. Detta kan exempelvis ske genom att lagringsmedia där nycklar eller lösenord till nycklarna förvaras, blir förstörda eller tappas bort.
- Krypteringsnycklar som skapas är för svaga vilket gör att obehöriga relativt enkelt kan skapa en ny likadan nyckel. Svagheter kan exempelvis orsakas av att inte tillräckligt bra slumptal används när nycklarna skapas eller att organisationen inte ställer krav på att nycklarna ska vara tillräckligt långa eller att en säker algoritm används.

De interna reglerna för kryptografiska nycklar behöver omfatta deras hela livscykel. Reglerna behöver även inkludera hur man ska hantera nyckelincidenter, såsom röjda eller förlorade krypteringsnycklar.

Reglerna behöver säkerställa att krypteringsnycklarna ges minst samma och helst högre skyddsnivå som den information de ska skydda genom kryptering. Oavsett hur krypteringsnycklarna skapas och lagras behöver skyddet av nyckeln upprätthållas under hela nyckelns livslängd[80], givet att skyddsbehovet hos informationen den skyddar består. När nyckeln inte längre ska användas behöver den även förstöras på ett säkert sätt.

Krypteringsnycklar kan skapas på flera olika sätt. Exempelvis skapas symmetriska och asymmetriska nycklar med olika algoritmer. I många av de kommersiella produkter som innehåller krypteringslösningar ingår möjlighet att skapa egna krypteringsnycklar. De interna reglerna behöver tydliggöra hur starka krypteringsnycklarna behöver vara för att svara mot organisationens behov. Olika användningsområden kan ha olika behov. Vissa leverantörer erbjuder kryptering som tjänst.

Detta innebär i de flesta fall att leverantören även har tillgång till nyckeln och därmed möjlighet att dekryptera informationen. Organisationen behöver bedöma om en sådan lösning är lämplig och i så fall omhänderta de risker detta kan innebära.

Krypteringsnycklar kan lagras på olika sätt, exempelvis i ett filsystem, i smarta kort, usb-minnen, trusted platform module chip (TPM-chip) eller i kryptografiska hårdvarumoduler (HSM). Att lagra krypteringsnycklar i mjukvara är vanligt i många krypteringslösningar. Möjligheterna att skydda krypteringsnycklar är här begränsat till mjukvarans förutsättningar och vilka säkerhetsåtgärder som är införda i informationssystemet. En HSM lagrar nyckelinformationen på ett säkert sätt och skyddar den mot direkt åtkomst. Istället för att låta krypteringslösningen ha åtkomst till krypteringsnyckeln så skickas informationen som ska krypteras till HSM:en och krypteras där. HSM:er ger generellt sett ett högre skydd än mjukvarulösningar. Det är därför lämpligt att använda HSM för lagring av krypteringsnycklar som har ett stort skyddsbehov eller sådana som ska användas under längre tid. Vilken lösning som ska väljas för nyckellagring måste beslutas efter riskbedömningen. Oavsett lösning måste krypteringsnycklar skyddas mot obehörig åtkomst eller förändring.

Godkännande och förvaltning av krypteringslösningar

Som med annan hård- och mjukvara så hittas sårbarheter och brister även i krypteringslösningar. Det är av stor vikt att inte använda svaga krypteringsalgoritmer eller krypteringsprotokoll, och att tillräcklig nyckellängd väljs. Det är också viktigt att ta ställning till om krypteringsnycklar ska få återskapas respektive säkerhetskopieras. Riskerna med återskapande och säkerhetskopiering behöver vägas mot riskerna att förlora en krypteringsnyckel och därmed möjligheten att använda informationen.

80. En krypteringsnyckel kan ha olika livslängd, från sekunder till år. Det är lämpligt att vid valet av skydd beakta om det handlar om långtidsnycklar eller sessionsnycklar, eftersom konsekvenserna vid eventuell förlust ofta skiljer sig åt.

Det är viktigt att organisationen har interna regler för både godkännande och förvaltning av krypteringslösningarna innan de implementeras i it-miljön. Godkännandet behöver omfatta både vilka krypteringslösningar som får användas i organisationens it-miljö och vilket behov av kryptering respektive lösning kan omhänderta. Dessutom behöver det finnas interna regler som ställer krav på att varje implementation av krypteringslösningar testas och godkänns innan användning. Tester behöver utföras av personal med nödvändig kompetens, och godkännande görs av systemägaren som en del av driftgodkännandet.

Organisationens interna regler för kryptering behöver ställa krav på vilka krypteringsalgoritmer, protokoll och nyckellängder som ska användas för att svara upp mot organisationens olika krypteringsbehov. Detta skapar förutsättningar för en effektiv förvaltning av krypteringsskyddet som ger organisationen möjlighet att hantera algoritmer som inte är tillräckligt starka, upptäcka sårbarheter i protokollen och behov av att öka nyckellängder. Förvaltningen av krypteringslösningar förutsätter att organisationen bedriver omvärldsbevakning för att i tid kunna identifiera kommande behov av att byta ut algoritmer, upptäcka sårbarheter i protokoll och förbereda för utökade nyckellängder. De interna reglerna behöver också innehålla krav på dokumentation av vilka informationssystem som använder vilka krypteringslösningar. Dokumentationen underlättar för organisationen att omhänderta sårbarheter som upptäcks vid omvärldsbevakningen.

Det finns leverantörer som argumenterar för att deras egenutvecklade krypteringslösningar är bättre eller snabbare än etablerade lösningar på marknaden. Så är ofta inte fallet. Styrkan i de etablerade lösningarna är att de baseras på allmänt tillgängliga algoritmer och protokoll som kontinuerligt granskas och testas för att upptäcka brister. Den faktiska skyddsnivån som en krypteringslösning ger beror på tillverkarens kompetens och leverantörens förmåga att skydda produkten mot manipulation i samband med leverans. Allt detta behöver beaktas vid valet av krypteringslösning.

För att minska riskerna med sårbarheter i kommersiell hård- och mjukvara som används för krypteringslösningar, är det lämpligt att låta lösningarna granskas helt, eller delvis, av ett certifieringsorgan eller en annan pålitlig tredjepartsaktör.

Krypteringsalgoritmer, protokoll och nyckellängder

Olika krypteringslösningar använder olika protokoll, och dessa protokoll baseras på en krypteringsalgoritm. För att kunna bedöma om en viss krypteringslösning är lämplig för ett visst syfte är det viktigt att veta

- vilka protokoll som kan användas
- vilka algoritmer som protokollen baseras på
- hur långa krypteringsnycklar som kan skapas.

Dessutom behöver organisationen genom omvärldsbevakning få underlag till en löpande bedömning av om valda protokoll innehåller sårbarheter som behöver hanteras, om valda algoritmer har blivit för svaga för att kunna användas eller vilka nyckellängder som krävs för att ge en säker krypteringslösning. Den bedömning organisationen gör ska ligga till grund för de interna krypteringsregler som tas fram.

4.4.5 Domännamnsservrar

All internettrafik är beroende av möjligheten att på ett korrekt och tillförlitligt sätt göra DNS[81]-uppslag. Domännamnssystemet (DNS) översätter webbadressen (hostnamnet) i textform till för datorn läsbara ip-adresser i sifferform och vice versa. DNS är dock sårbart för ett antal olika attacker vilka kan manipulera svar på DNS-frågor. En sådan attack kan

81. Domain Name System, DNS.

innebära att man dirigeras till fel webbserver (host) utan att veta om det. Domain Name System Security Extensions (DNSSEC) är ett tillägg till DNS-systemet som syftar till att öka säkerheten i DNS med hjälp av kryptografiska signaturer. DNSSEC säkerställer att DNS-svaret kommer från rätt källa och att data inte har manipulerats under överföringen. Detta kan förhindra missbruk där man lurar DNS-systemet med falsk information.

De flesta DNS-produkter på marknaden innehåller numera stöd för DNSSEC. Likaså är det vanligt att DNS-tjänsteleverantörer tillhandahåller DNSSEC. DNSSEC är också ofta en förutsättning för att autentiseringsmetoder för webbtjänster och e-post ska fungera på avsett sätt. Den DNS-tjänst som ska hantera externa förfrågningar till organisationens domännamn bör, utöver att stödja DNSSEC, också väljas utifrån robusthet.

En organisation har ofta flera domännamn. Vissa vänder sig till externa användare eller externa informationssystem medan andra har endast ett internt syfte.

Om organisationen har ett informationssystem som ska vara externt åtkomligt, exempelvis en webbtjänst, webbsida eller e-postserver, behöver det registreras i DNS för att externa användare eller externa informationssystem ska kunna hitta dit. Organisationen ska aktivera DNSSEC i namnservrarna för samtliga domännamn som organisationen registrerat i DNS. Den namnuppslagstjänst (resolver) som organisationen använder för uppslag av externa namnuppslag behöver också ha stöd för och kunna validera DNSSEC.

Interna informationssystem är nåbara via organisationens interna nät. För att hålla ordning på informationssystem och ip-adresser i det interna nätverket behövs ofta motsvarande funktionalitet som DNS ger på internet. Organisationen behöver dock se till att de interna informationssystemen inte är nåbara externt och inte registrerade i DNS. Om sådan registrering görs, vilket också innebär att informationssystemen går att slå upp och därmed blir synliga externt, krävs DNSSEC.

4.4.6 Säkerhetsloggar

Organisationen bör använda kryptering för att skydda sina säkerhetsloggar. När krypteringsskyddet för säkerhetsloggarna utformas är det viktigt att ta hänsyn till var loggarna skapas, var de lagras och hur de överförs däremellan. Krypteringsskyddet ska användas tillsammans med andra säkerhetsåtgärder för att skydda säkerhetsloggarna, exempelvis nätverkssegmentering, behörighetskontroll, övervakning och fysiskt åtkomstskydd.

För att skydda mot både obehörig åtkomst och obehörig förändring behöver säkerhetsloggarna krypteras så snart som möjligt efter att de skapats och så nära källan det går. Genom att använda hashsummor och signeringsfunktion kan obehörig förändring av innehållet i säkerhetsloggarna upptäckas. Lösningar för att verifiera riktighet går också att skapa genom att använda blockkedjeteknik.

Krypteringsskyddet behöver upprätthållas under överföring och lagring. Konsekvenserna av ett bristfälligt skydd av säkerhetsloggar är att organisationen inte kan lita på dess innehåll vilket försvårar organisationens säkerhetsarbete. Exempelvis kan det bli svårt att både upptäcka och utreda misstankar om obehörigt intrång, tekniska fel eller andra säkerhetsbrister.

Eftersom organisationen som en del i sitt säkerhetsarbete ska analysera säkerhetsloggarna behöver krypteringsskyddet utformas på ett sådant sätt att detta blir möjligt samtidigt som skyddsnivån upprätthålls. Detta underlättas i de allra flesta fall genom att säkerhetsloggarna samlas i ett för ändamålet avsett informationssystem (central säkerhetslogg).

4.4.7 Autentiseringsuppgifter

Organisationen bör använda kryptering för att skydda autentiseringsuppgifter. Det gäller både lösenordsdatabasen i sig och de enskilda autentiseringsuppgifterna som används för att identifiera en användare eller ett informationssystem. För att skydda autentiseringsuppgifter med kryptering i lösenordsdatabasen behöver de lagras där både ”saltade”[82] och hashade. Konsekvenserna för en organisation vid obehörig åtkomst till okrypterade autentiseringsuppgifter kan bli omfattande.

När en användare eller ett informationssystem autentiserar sig, exempelvis via en inloggningsruta på en webbsida eller annat gränssnitt, behöver krypteringsskydd finnas både i gränssnittet och vid överföringen till lösenordsdatabasen. Krypteringsskyddet syftar till att skydda autentiseringsuppgifterna mot obehörig åtkomst. Det är i de flesta fall inte lämpligt att skicka autentiseringsuppgifter i klartext mellan inmatning och verifiering.

4.4.8 Information i behov av utökat skydd

Den information som organisationen i sin informationsklassning[83] bedömt vara i behov av utökat skydd bör skyddas mot obehörig åtkomst och obehörig förändring när den förs över till informationssystem utanför organisationens kontroll. Detta gäller oavsett om behovet av det utökade skyddet handlar om konfidentialitet, riktighet eller tillgänglighet, eller kombinationer av dessa.

Med informationssystem utanför organisationens kontroll avses här alla informationssystem som inte fysiskt befinner sig i de egna lokalerna[84] eller andra utrymmen som organisationen disponerar, exempelvis vid samlokalisering. Om en organisation har flera lokaler på olika fysiska platser, alternativt anlitar en driftleverantör med lokal på en annan fysisk plats, ska behovet av kryptering för att skydda informationen identifieras och hanteras. Detta kan exempelvis ske genom att sätta upp ett virtuellt privat nätverk (vpn) mellan de olika lokalerna. Behovet av kryptering ska också identifieras och hanteras när organisationen tillåter att medarbetare vid distansarbete kopplar upp sig mot organisationens it-miljö.

När en organisation har en webbplats som exempelvis hanterar autentiseringsuppgifter ska behovet av kryptering identifieras och hanteras. Kryptering bör användas, eftersom sådan information generellt sett bedöms vara i behov av utökat skydd. De allra flesta tillämpningar för webbtjänster har inbyggt stöd för kryptering, inklusive stöd för användning av olika autentiseringsmetoder, för att besökare ska kunna verifiera att de är på rätt webbplats. Exempelvis är det lämpligt att använda HTTPS på samtliga webbtjänster som standard för applikationsnivån. Transport Layer Security (TLS) används ofta som krypteringsprotokoll på transportlagret.

En förutsättning för att TLS ska fungera som det är tänkt är att det på serversidan finns ett digitalt certifikat. Det digitala certifikatet behöver innehålla uppgifter om innehavaren av webbtjänsten på serversidan motsvarande det som kallas för Fully Qualified Domain Name (FQDN), det vill säga formatet ”www.statligmyndighet.se”. Klienten, en webbläsare eller ett annat informationssystem, kontrollerar om en webbtjänst är pålitlig genom att jämföra namnet på innehavaren i certifikatet med webbtjänstens adress. Matchar inte namn och adress varandra så har webbtjänsten inte något giltigt certifikat och kan vara osäker. För att minska risken för att adressen till organisationens webbtjänst förfalskas genom att byta ut domännamnsinformation i DNS, behöver organisationen aktivera DNSSEC.

82. Saltning innebär att lösenorden kompletteras med ett slumpmässigt valt tillägg som gör lösenorden längre och svårare för en angripare att knäcka.

83. För mer information om informationsklassning, se metodstödet ”utforma klassningsmodell” på www.informationssäkerhet.se.

84. Exempelvis organisationens bärbara datorer som används av personal vid distansarbete.

En organisation ska alltid bedöma behovet av kryptering för att skydda information mot obehörig åtkomst och obehörig förändring vid både överföring och lagring.

4.4.9 E-post

En organisation bör införa möjlighet för mottagare av ett e-postmeddelande att kunna verifiera att det är organisationen som är avsändare. Detta görs i syfte att minska risken för att organisationen och de som organisationen kommunicerar med råkar ut för ”spoofing” via e-post, det vill säga att någon annan felaktigt utger sig för att skicka meddelanden från organisationen. Beroende vad som kommuniceras och hur väl det falska e-postmeddelandet är utformat kan konsekvenserna bli påtagliga för organisationen och de mottagare som litar på e-postmeddelandets innehåll. De som använder den här tekniken för att skicka falska e-postmeddelanden blir allt skickligare på att härma andras sätt att kommunicera.

För att så långt som möjligt undvika att den egna organisationens personal luras, av både falska externa och interna meddelanden, behöver organisationen införa tekniskt skydd för e-post. Se exempelvis till att e-postkonton som inte är avsedda för extern kommunikation endast kan ta emot e-post från den egna organisationen. Organisationen behöver använda autentiseringsmetoder[85] för att mottagare ska kunna validera e-post som skickas från eller till organisationen. Den valda metoden behöver konfigureras så att skyddet inte kan kringgås. För att autentiseringsmetoderna även ska ge den egna organisationen stöd att själv identifiera falska meddelanden, är det lämpligt att kontakta de organisationer med vilka det finns en omfattande kommunikation och uppmana dem att aktivera motsvarande tekniskt skydd.

E-post är ett flexibelt sätt att kommunicera på och kan användas för många olika typer av information. En organisation behöver därför identifiera behovet av att skydda e-post mot obehörig åtkomst. Om hela eller delar av e-posttjänsten är utkontrakterad är det viktigt att se hur e-postkommunikationen skyddas fram till e-posttjänsten och från e-posttjänsten in till organisationen.

Skydd av informationen som skickas via e-post kan förenklat ske på något av dessa sätt:

- skydd av transporten mellan servrarna som överför e-post
- skydd av informationen i enskilda e-postmeddelanden.

I det första fallet används oftast Transport Layer Security (TLS), eller en vpn-lösning, mellan servrarna. Att få ett fullt utbyggt skydd mot obehörig åtkomst genom TLS eller vpn, kryptering på transportlagret[86], för sin e-postkommunikation förutsätter dock att både mottagare och avsändare av e-postmeddelandet har den funktionaliteten på plats.[87] Organisationen bör därför identifiera med vilka andra organisationer sådan skyddad kommunikation behöver ske, och sedan tillsammans med den organisationen bestämma vilken lösning som passar bäst.[88] Statliga myndigheter bör införa möjlighet att kryptera e-post på transportlagret vid kommunikation med andra statliga myndigheter.

85. Exempelvis DNS based Authentication of Name Entities (DANE), Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC). DANE, SPF, DKIM och DMARC bygger alla på att mottagaren slår upp information knuten till ett domännamn i DNS, vilket är en ytterligare anledning till att en organisation ska aktivera DNSSEC.

86. Transportlagret i enlighet med OSI-modellen (Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model, ISO/IEC 7498-1) eller motsvarande.

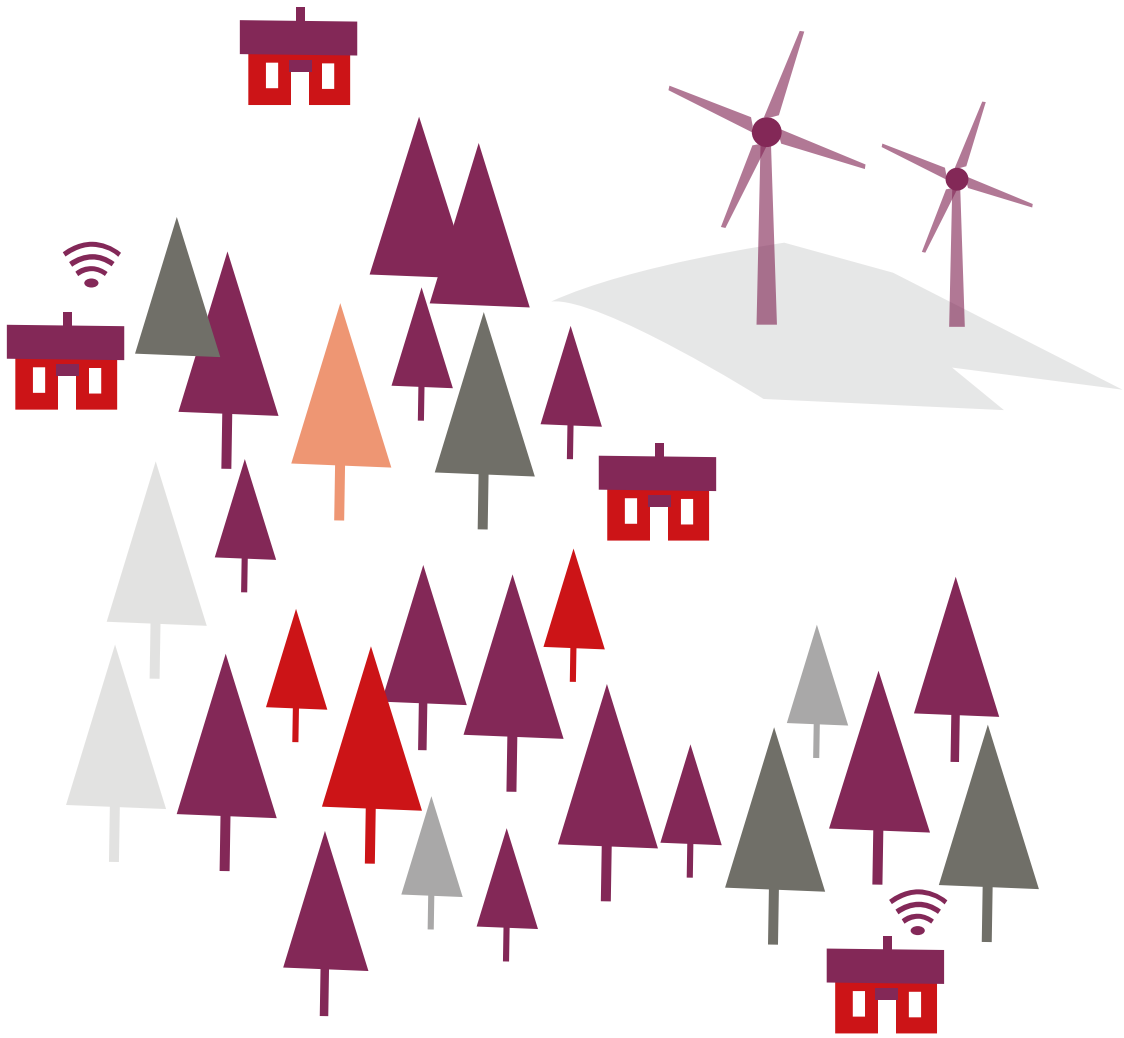
87. Om bara den mottagande organisationen använder TLS riskerar trafiken ändå att bli okrypterad, såvida inte den mottagande organisationen kräver att avsändaren använder TLS, så kallad enforced TLS. I det sistnämnda fallet kommer e-postmeddelandet, istället för att skickas okrypterat, inte skickas alls.

88. Oavsett vilken lösning som används är det viktigt att ha en genomtänkt certifikatanvändning.

Om organisationen bedömer att informationen i enskilda e-postmeddelanden, utifrån informationsklassningen och riskbedömningen, behöver skyddas på meddelandenivå vid överföring och lagring används oftast någon av dessa lösningar:

- krypteringslösning baserad på Pretty Good Privacy (PGP) eller Gnu Privacy Guard (GPG)
- krypteringslösning baserad på Secure/ Multipurpose Internet Mail Extensions (S/MIME)

Ovan lösningar baseras på att mottagare och avsändare har kommit överens om lösningen, att medarbetarna har tillgång till dessa och att nyckelutbyte kan ske på ett korrekt och säkert sätt. Om detta inte har skett är det istället möjligt att skydda informationen i meddelandet genom att meddelandet inte skickas direkt till mottagaren utan lagras på en för ändamålet godkänd server, och endast en notifiering går till mottagaren som ges möjlighet att logga in på servern (till exempel via en webbläsare) och där ta del av informationen.



4.5 Säkerhets-konfigurering

4.5.1 Syfte

För att skydda sin it-miljö mot obehörig åtkomst behöver organisationen byta ut förinställda autentiseringsuppgifter och konfigurera informationssystemen genom att endast tillåta nödvändiga systemfunktioner.

4.5.2 Krav

Organisationen ska, för att skydda informationssystem mot obehörig åtkomst,[89]

1. byta ut förinställda autentiserings-uppgifter
2. stänga av, ta bort eller blockera systemfunktioner som inte behövs
3. i övrigt anpassa konfigurationer för att uppnå avsedd säkerhet.

4.5.3 Att säkerhetskonfigurera

Informationssystem som är felaktigt konfigurerade, inte uppdaterade eller använder sig av standardinställningar kan utgöra en väg in för angripare. Alla informationssystem i organisationens it-miljö behöver därför säkerhetskonfigureras, exempelvis mobiltelefoner, nätverksenheter, servrar, klienter, skrivare, e-post, molntjänster och säkerhetsfunktioner. Detta gäller särskilt informationssystem med koppling till externa nätverk, så som e-post, webbsidor, webbtjänster och DNS-servrar.

Innan applikationer, tjänster och andra komponenter som behandlar information i informationssystemet installeras, ska standardinställningarna ses över och informationssystemet konfigureras så att endast de funktioner som organisationen behöver är aktiverade. Övriga funktioner ska stängas av, tas bort eller blockeras. De systemfunktioner som behöver vara aktiverade ska i sin tur konfigureras så att avsedd säkerhetsnivå uppnås. Dessutom ska organisationen byta ut förinställda autentiseringsuppgifter. Konfigurationen görs lämpligen av it-tekniker utifrån verksamhetens behov och kunskap om informationssystemet, risker, best practice och den it-miljö där informationssystemet ska användas.

4.5.4 Byta ut autentiserings-uppgifter

En organisation ska byta ut alla förinställda autentiseringsuppgifter i informationssystem innan de driftsätts. Sådana förinställda autentiseringsuppgifter, såsom standardlösenord/fabriksinställda lösenord, finns exempelvis i applikationer, operativsystem, brandväggar och nätverksutrustning. De förinställda autentiseringsuppgifterna kan vara kopplade till flera olika typer av digitala identiteter (konton) för användare, informationssystem och systemadministratörer.

Valet av nya autentiseringsuppgifter behöver göras enligt de interna reglerna för hantering av autentiseringsregler, så att behovet av längd och komplexitet tillgodoses.

4.5.5 Anpassa system-konfigurationer

De flesta informationssystem levereras med en standardkonfiguration utformad av antingen tillverkaren eller återförsäljaren. Den är vanligen utformad för att förenkla installation och användning samt möjliggöra bakåtkompatibilitet till äldre versioner, inte för att erbjuda god säkerhet. Vid leverans är det vanligt att produkterna inte är uppdaterade till senaste version och att fler tjänster och protokoll är aktiverade än vad organisationen behöver för att få avsedd funktion av informationssystemet. Om inte sådana brister hanteras innan driftsättning

89. MSBFS 2020:7 4 kap. 10 § Myndigheten ska, för att skydda informationssystem mot obehörig åtkomst, 1. byta ut förinställda autentiseringsuppgifter, 2. stänga av, ta bort eller blockera systemfunktioner som inte behövs, och 3. i övrigt anpassa konfigurationer för att uppnå avsedd säkerhet.

och nätverksanslutning[90], ökar risken för att angripare skaffar sig åtkomst till organisationens it-miljö. För att säkerställa att organisationen har stängt av, tagit bort eller blockerat systemfunktioner som inte behövs och i övrigt anpassa konfigurationer för att uppnå avsedd säkerhet, är det lämpligt att vidta följande steg:

- *Uppdatera och uppgradera*

  Det är lämpligt att inleda förberedelserna inför driftsättning av nya informationssystem med att uppdatera all mjukvara och, vid behov, uppgradera hård- och mjukvara till den senaste versionen, för att säkerställa att alla tillgängliga säkerhetsuppdateringar är införda. Äldre protokoll och inaktuell förinstallerad mjukvara kan innehålla sårbarheter.
- *Koppla loss nätverkskablar*

  Minimera antalet möjliga angreppspunkter genom att inaktivera och fysiskt koppla ifrån nätverkskablar från oanvända nätverksportar och nätverkskort.
- *Stäng ned onödig funktionalitet*

  Hård- och mjukvara har ofta fler funktioner, exempelvis nätverksprotokoll och nätverksapplikationer, än vad organisationen behöver. Dessa funktioner är i allmänhet aktiverade vid leverans. Konfigurera informationssystem med enbart nödvändig funktionalitet (least functionality) för att organisationens verksamhet ska fungera. Om det finns funktioner, exempelvis nätverksprotokoll och nätverksapplikationer, som organisationen inte behöver bör de i första hand tas bort. Om det inte är möjligt bör de stängas av. De funktioner som inte kan stängas av behöver blockeras, ibland med hjälp av andra säkerhetsåtgärder såsom brandväggsregler[91]. De funktioner som används behöver uppdateras för att ta bort sårbarheter och övervakas för att upptäcka om ohanterade sårbarheter används av obehöriga.
- *Ta bort för höga behörigheter*

  För att underlätta installation och drift levereras många mjukvaror med höga behörigheter förinställda. Det är viktigt att veta vilka behörigheter som behövs för att informationssystemet ska kunna fungera på det sätt som organisationen har behov av. Om det inte finns tillräcklig dokumentation över vilka behörigheter som krävs, behöver organisationen ställa krav på leverantören om att få sådan information. Annars kan organisationen behöva lägga ned mycket tid på att genom tester utreda vilka behörigheter som är nödvändiga. Det är inte lämpligt att behålla de förinställda höga behörigheterna då de kan förenkla för angripare.
- *Anpassa konfigurationen*

  Efter att ha stängt ned onödig funktionalitet behöver organisationen anpassa konfigurationen för den funktionalitet som organisationen behöver, så att den både svarar mot verksamhetens behov och uppnår avsedd säkerhet. Exempelvis, välj de säkraste protokollen, tillåt endast att trafik initieras i den ena riktningen, använd kryptering, använd certifikat, begränsa fysisk och logisk åtkomst, och konfigurera loggning och övervakning. Undersök om de säkerhetsfunktioner som redan finns inbyggda i produkterna uppfyller organisationens krav och använd i så fall dessa för att minska komplexiteten. Stäng inte av kodskydd som försvårar att programvara kan köras utanför tilldelat utrymme i processor och internminne.

90. Om viss konfigurering kräver nätverksanslutning är det viktigt att se till att informationssystemet inte innehåller någon information och att endast de nätverksportar och -tjänster som krävs för konfigureringen är öppna.

91. Exempel på brandväggsregler är att inte tillåta anslutningar till eller från andra informationssystem och att fjärrinloggning enbart får ske från specifikt utpekade informationssystem eller nätverkssegment.

- *Nyttja befintliga säkerhetsåtgärder i it-miljön*
  Utöver konfigurationen av själva informationssystemet är det lämpligt att öka säkerheten genom att placera informationssystemet på rätt ställe i it-miljön. Det handlar exempelvis om att välja rätt nätverkssegment och nyttja det skydd brandväggen ger för att minimera attackmöjligheter.

För att effektivisera arbetet är det lämpligt att ta fram mallar för säkerkonfigurationer som kan återanvändas på alla liknande informationssystem i it-miljön. Dessa kan exempelvis bestå av Group Policy Objects (GPO)[92], uppstartsskript och konfigurationsfiler som installeras i informationssystemen. Säkerhetskonfigurationen används vid nyinstallation av informationssystem. Det är lämpligt att informationssystem i drift automatiskt uppdateras med nya säkerhetskonfigurationer när sådana finns tillgängliga. När det exempelvis gäller informationssystem som är mycket känsliga för driftstörningar eller har ovanlig konfiguration kan det dock vara lämpligare att göra uppdateringar manuellt efter att tester är genomförda med godkänt resultat. Valet mellan automatisk eller manuell uppdatering av olika informationssystem grundas på riskbedömningen.

Förvaltning

Organisationens säkerhetskonfigurationer behöver förvaltas på ett tillförlitligt sätt. Genom att ha en samlad dokumenterad och versionshanterad säkerhetskonfiguration, underlättas arbetet med att kontinuerligt hålla säkerhetskonfigurationerna aktuella och uppdaterade. Det är lämpligt att använda verktyg som underlättar arbetet med att ha kontroll över vilka säkerhetskonfigurationer som är installerade i it-miljön. Sådana verktyg ger bland annat stöd för att automatiskt och regelbundet kontrollera att de senaste godkända säkerhetskonfigurationerna är införda i it-miljön. Det är lämpligt att använda verktyg som larmar om säkerhetskonfigurationen på någon enhet inte stämmer överens med gällande säkerhetskonfiguration.

Se över och uppdatera säkerhetskonfigurationerna med jämna mellanrum, så att de är uppdaterade i förhållande till de nyaste sårbarheterna och angreppssätten. Konfigurationen behöver ses över periodiskt eller vid behov, till exempel när

- mjuk- eller hårdvara uppgraderas eller uppdateras
- andra säkerhetsuppdateringar installeras
- nya sårbarheter har upptäckts
- verksamheten kräver ett nytt arbetssätt
- nya informationssystem införs.

Se också till att de nya säkerhetskonfigurationerna installeras i informationssystemen så snart som möjligt, i enlighet med organisationens ändringshantering. Att bestämma och distribuera säkerhetskonfiguration är en komplex uppgift, eftersom det ibland kan innebära att tusentals möjliga inställningar behöver utvärderas. Att ta fram och förvalta en säker konfiguration kräver därför teknisk kompetens för de komponenter som ska säkerhetskonfigureras, vilket innebär att vissa organisationer måste ta hjälp av externa specialister för att säkerhetskonfigurera respektive informationssystem i it-miljön.

De säkerhetskonfigurationer som används behöver skyddas mot obehörig åtkomst och förändring, minst på motsvarande nivå som skyddet för den information som ska behandlas i informationssystemet. En angripare som kan ta del av säkerhetskonfigurationen kan finna sårbarheter som går att utnyttja, eller göra förändringar i befintlig säkerhetskonfiguration för att på så sätt underlätta kommande angrepp. Kontrollera automatiskt och regelbundet att inte säkerhetskonfigurationerna har förändrats på ett obehörigt sätt.

92. Group Policy Object, GPO (grupprincip), ett sätt i Windowsmiljöer att från katalogtjänsten meddela klienter och servrar ett antal konfigurationsinställningar.

4.6 Säkerhetstester och granskning

4.6.1 Syfte

För att identifiera och hantera sårbarheter i enskilda informationssystem och it-miljön i sin helhet, behöver organisationen kontrollera att informationssystemen är uppdaterade samt att valda säkerhetsåtgärder och säkerhetskonfigurationer är införda och tillräckliga.

4.6.2 Krav

Organisationen ska[93]

1. säkerställa att säkerhetstester och granskningar möjliggör identifiering av sårbarheter
2. ha interna regler för hur kontroll görs av att
   a. informationssystemen är uppdaterade
   b. valda säkerhetsåtgärder är införda på korrekt sätt
   c. genomförda säkerhetskonfigurationer är tillräckliga.

Organisationen bör kombinera automatiserade säkerhetstester och manuella granskningar vid kontroll av säkerheten i informationssystemen.[94]

4.6.3 Kontroll av säkerhet i informationssystem och it-miljö

Organisationen ska regelbundet säkerhetstesta och granska sin förmåga att skydda sina informationssystem. Målet är att hitta fel och sårbarheter så att dessa kan korrigeras.

Säkerhetstester och granskningar kan göras på olika sätt, med olika syften och omfattning. Huvudsyftet är att upptäcka brister avseende skyddet för konfidentialitet, riktighet och tillgänglighet. Säkerhetstester och säkerhetsgranskningar kompletterar varandra.

Organisationen ska ha interna regler för hur kontroller ska genomföras. Eftersom säkerhetstester och granskningar tar tid och resurser är det lämpligt att ta fram och använda ett standardiserat arbetssätt för säkerhetstester och granskningar som alltid utförs. De standardiserade säkerhetstesterna och granskningarna behöver anpassas utifrån vad som ska kontrolleras och hur skyddsvärt det som ska kontrolleras är utifrån informationsklassning och riskbedömning.

De flesta organisationer utför säkerhetstester och granskningar av enskilda informationssystem, men det kan även finnas behov av att kontrollera såväl hela it-miljön som enskilda komponenter. För att säkerställa tillräckligt skydd i informationssystem som behandlar särskilt känslig information kan till och med kvaliteten i mjukvaran behöva kontrolleras, exempelvis genom kodtester och kodgranskningar. Många av de kontroller som behöver göras kräver särskild kompetens.

4.6.4 Säkerhetstester

Säkerhetstester syftar till att finna tekniska sårbarheter och genomförs i huvudsak genom sårbarhetsskanningar och intrångstester (penetrationstester eller pentest).

Sårbarhetsskanning

Sårbarhetsskanningar genomförs med stöd av automatiserade verktyg som, exempelvis utifrån en på förhand uppsatt lista över sårbarheter, kontrollerar om informationssystemet har brister. Genom sårbarhetsskanningen kan man upptäcka exempelvis saknade patchar, osäkra protokoll och utgångna certifikat. I ett skanningsverktyg går det att ställa in vilka informationssystem eller delar av it-miljön som ska skannas. Det går också att ge skanningsverktyget olika behörighetsnivåer. En högre behörighet, exempelvis motsvarande vad en systemadministratör

93. MSBFS 2020:7 4 kap. 11 § Myndigheten ska säkerställa att säkerhetstester och granskningar möjliggör identifiering av sårbarheter. Myndigheten ska ha interna regler för hur kontroll görs av att 1. informationssystemen är uppdaterade, 2. valda säkerhetsåtgärder är införda på korrekt sätt, och 3. genomförda säkerhetskonfigurationer är tillräckliga.

94. Allmänt råd till MSBFS 2020:7 4 kap. 11 §.

kan se, ger skanningsverktyget möjlighet att gå in i informationssystemet och upptäcka sårbarheter som svaga lösenord, konfigurationsproblem, otillåtet installerad programvara och skadlig kod. Behörighet som endast medger skanningar från utsidan av informationssystemet ger en bild av hur åtkomligt informationssystemet är för en angripare. Organisationen behöver regelbundet genomföra skanningar efter sårbarheter. Intervallet bör bestämmas utifrån informationsklassningen och riskbedömningen. Sårbarhetsskanning behöver alltid göras innan nya eller förändrade informationssystem driftsätts. Var uppmärksam på att det finns skanningsverktyg som lagrar resultatet i molntjänster där det kan vara svårt att bedöma vem som har åtkomst till uppgifterna om sårbarheterna.

Intrångstester

Intrångstester syftar till att identifiera sårbarheter och sätt som en angripare skulle kunna använda för att få åtkomst till organisationens informationssystem och it-miljö. Den som utför ett intrångstest behöver ha en hög teknisk kompetens och erfarenhet, eftersom testet syftar till att identifiera sårbarheter och ingångar som inte nödvändigtvis är kända sedan tidigare. Den som utför intrångstestet behöver både på ett realistiskt sätt kunna agera som en angripare och samtidigt inte riskera att organisationens informationssystem eller it-miljö utsätts för oacceptabla risker, exempelvis driftstörningar. Det är lämpligt genomföra testerna i testmiljö som är konfigurerat på samma sätt som produktionsmiljön men inte innehåller någon verksamhetsinformation.

Ett intrångstest är en avancerad säkerhetskontroll, och för att användas resurseffektivt bör organisationen förbereda sig genom att först kontrollera med sårbarhetsskanning att it-miljön är säkerhetskonfigurerad. Intrångstester behöver generellt sett inte utföras lika ofta som sårbarhetsskanningar. Det är inte heller alltid nödvändigt att genomföra intrångstester på samtliga informationssystem. Lämpligtvis prioriteras sådana informationssystem som är åtkomliga från externa nätverk.

Innan organisationen beslutar om att genomföra intrångstester behöver en riskbedömning göras, där synpunkter från berörda systemägare och verksamheter beaktas. Riskbedömningen kan resultera i att vissa delar av it-miljön undantas från intrångstestet, exempelvis för att konsekvenserna av om de påverkas blir för stora. Det är i sådana fall lämpligt att istället göra en skrivbordsövning där de undantagna informationssystemen säkerhetsgranskas utifrån beskrivna konfigurationer, integrationer och annan relevant dokumentation.

Om det finns resurser är det lämpligt att organisationen också nyttjar intrångstesterna för att kontrollera om övervakningssystemen upptäcker en pågående ”attack”. Det ger möjlighet att vid behov utveckla övervakningsfunktionaliteten och på så sätt förbättra förmågan att upptäcka incidenter. Det är även lämpligt att i samband med intrångstestet öva organisationens hantering av incidenter.

Konton som används för säkerhetstester, både sårbarhetsskanningar och intrångstester, behöver övervakas för att kontrollera att de bara används på avsett sätt och inaktiveras efter säkerhetstestet. Verktygen som används för säkerhetstester behöver uppdateras regelbundet, för att säkerställa att de inte själva innehåller sårbarheter samt att de upptäcker de senaste sårbarheterna.

4.6.5 Granskning

Säkerhetsgranskning innebär en manuell granskning av dokumentation i syfte att hitta fel och brister. Det kan exempelvis handla om att granska kod, konfigurationer, arkitektur och brandväggsregler. Det innefattar också kontroll av att den dokumentation som beskriver it-miljön och informationssystemen är tillräcklig för att drift och förvaltning ska kunna bedrivas på ett säkert sätt.

Säkerhetsgranskningar bör göras inför driftsättning och vid förändringar i informationssystemen eller it-miljön som kan påverka säkerheten.

4.7 Ändringshantering, uppgradering och uppdatering

4.7.1 Syfte

För att genomföra ändringar i informationssystem utan att påverka säkerheten i it-miljön, behöver organisationen ha en strukturerad och spårbar ändringshantering.

4.7.2 Krav

Organisationen ska[95]

1. säkerställa att ändringar i informationssystem genomförs på ett strukturerat och spårbart sätt
2. ha interna regler för ändringshantering med krav på
   a. kriterier för att godkänna hård- och mjukvara innan installation eller användning
   b. hur risker för incidenter och avvikelser i samband med förändring i produktionsmiljön ska identifieras och hanteras
   c. hur mjukvara, utan onödigt dröjsmål, ska uppdateras till senaste version
   d. hur hård- och mjukvara som inte längre uppdateras eller stöds av leverantören ska bytas ut eller uppgraderas utan onödigt dröjsmål
   e. hur risker ska hanteras när uppdatering eller uppgradering enligt c) och d) inte kan genomföras.

Organisationen bör[96]

1. skyndsamt införa säkerhetsuppdateringar
2. överväga behovet av att automatisera säkerhetsuppdateringar
3. i sina interna regler tydliggöra hur risker för incidenter och avvikelser i samband med förändringar i utvecklings-, test- och utbildningsmiljö identifieras och hanteras
4. för att undvika störning vid förändring, genomföra tester och ta fram en plan för återställning innan förändringen genomförs.[97]

4.7.3 Ändringshantering

Det är vanligt att organisationens it-miljö behöver ändras, för många organisationer till och med ofta. Orsakerna kan exempelvis vara driftsättning av nya informationssystem, uppdateringar och uppgraderingar av hård- och mjukvara samt felrättningar. För att ändringarna ska genomföras på ett strukturerat och spårbart sätt ska organisationen ha interna regler för ändringshantering[98]. Reglerna ska innehålla kriterier för vad som behöver göras innan it-miljön ändras, exempelvis genom att hård- och mjukvara installeras eller används. Kriterierna kan utformas såsom krav på följande:

- Godkänt resultat vid test av ändringen i testmiljön.
- Identifiering och hantering av risker för att incidenter och avvikelser inträffar i samband med ändring i produktionsmiljön, inklusive konsekvenser för verksamhet och andra informationssystem.

95. MSBFS 2020:7 4 kap. 12 § Myndigheten ska säkerställa att förändringar i informationssystem genomförs på ett strukturerat och spårbart sätt. Myndigheten ska ha interna regler för ändringshantering med krav på 1. vilka kriterier som ska användas för att godkänna hård- och mjukvara innan installation eller användning, 2. hur risker för incidenter och avvikelser i samband med förändring i produktionsmiljön ska identifieras och hanteras, 3. hur mjukvara, utan onödigt dröjsmål, ska uppdateras till senaste version, 4. hur utbyte eller uppgradering av hård- och mjukvara som inte längre uppdateras eller stöds av leverantören ska säkerställas utan onödigt dröjsmål, och 5. hur risker ska hanteras när uppdatering eller uppgradering enligt punkt 3 och 4 inte kan genomföras.

96. Allmänt råd till MSBFS 2020:7 4 kap. 12 § Säkerhetsuppdateringar bör införas skyndsamt och behovet av att automatisera uppdateringar bör övervägas. De interna reglerna bör tydliggöra hur risker för incidenter och avvikelser i samband med förändringar i utvecklings-, test- och utbildningsmiljö identifieras och hanteras.

97. Allmänt råd till MSBFS 2020:7 4 kap. 12 § För att undvika störning vid förändring bör myndigheten genomföra tester och ta fram en plan för återställning innan förändringen genomförs.

98. En mer detaljerad beskrivning av ändringshantering är beskriven i t.ex. Information Technology Infrastructure Library (ITIL) Change Management.

- Identifiering av lämplig tidpunkt för genomförande av ändringen i syfte att minimera påverkan på verksamhet och andra informationssystem.
- Dokumentation för drift och förvaltning har uppdaterats utifrån ändringen.
- Upprättad och godkänd återställningsplan till senast fungerande version om uppdateringen eller uppgraderingen helt eller delvis misslyckas.
- Hur beslut om att genomföra ändringen fattas.

Reglerna ska innehålla krav på att mjukvara uppdateras till senaste version utan onödigt dröjsmål. Det behöver finnas ett arbetssätt i organisationen som säkerställer att bevakningen av säkerhetsuppdateringar och andra nödvändiga uppdateringar är heltäckande samt att uppdateringarna införs i informationssystemet.

Den senaste versionen innehåller inte bara uppdatering med ny funktion eller liknande utan även de senaste säkerhetsuppdateringarna som leverantören skickat ut. Krav ska också ställas på att hård- och mjukvara som inte längre uppdateras eller stöds av leverantören ska bytas ut eller uppgraderas utan onödigt dröjsmål. Om det inte finns lämpliga it-produkter att byta till, eller om en riskbedömning har visat att uppdatering eller uppgradering inte kan genomföras utan onödigt dröjsmål på grund av att konsekvenserna för verksamhet eller andra informationssystem bedöms bli för höga, ska reglerna tydliggöra hur de risker som uppstår i samband med det ska hanteras. Det kan exempelvis handla om att införa kompenserande säkerhetsåtgärder, till exempel genom ytterligare nätverkssegmentering. Organisationen bör i sina interna regler även tydliggöra hur risker för incidenter och avvikelser i samband med ändringar i utvecklings-, test- och utbildningsmiljö identifieras och hanteras.

Det är lämpligt att de interna reglerna för ändringshantering även omhändertar situationer där ändringshantering behöver ske under en pågående incident. Ett sådant ändringsarbete sker ofta under tidspress där riskbedömningar, planering och genomförande av ändringar behöver ske skyndsamt. Det är lämpligt att genomföra övningar där både ändringsorganisationen och incidentorganisationen deltar.

Arbetssätt för ändringshantering

Organisationens ändringshantering samordnas lämpligen av en särskild utpekad roll på it-avdelningen. Ändringshanteringen behöver inkludera följande steg:

1. Identifiera vilken typ av ändring som behövs, exempelvis driftsättning av ett nytt informationssystem, uppgradering eller felrättning.
2. Planera i samverkan med informationsägaren och systemägaren hur ändringen ska genomföras, exempelvis tidpunkt, omfattning och med vilka resurser samt hur de som påverkas av ändringen informeras
3. Kontrollera att nödvändig dokumentation finns, exempelvis riskbedömning, återställningsplan samt uppdaterad dokumentation för drift och förvaltning.
4. Identifiera och hantera eventuell påverkan på införda säkerhetsåtgärder under genomförandet av ändringen.
5. Besluta om ändring och genomför den.
6. Följ upp att ändringen har avsedd effekt inklusive att den inte medför nya sårbarheter.
7. Utvärdera regelbundet ändringshanteringen i syfte att förbättra interna regler och arbetssätt.

För att öka effektiviteten i ändringshanteringen kan vissa typer av ändringar som ofta återkommer hanteras i särskilda snabbspår, där punkt 2–5 kan göras i en enklare form. Exempelvis genom att återanvända riskbedömningar och att ändringsorganisationen överlåter till utpekade medarbetare att hantera rutinbetonade ändringar med låg risk. Det kan även vara nödvändigt att använda snabbspår för särskilt tidskritiska uppdateringar

såsom säkerhetsuppdateringar. Besluta om förhandsgodkännanden för säkerhetsuppdateringar och frekventa ändringar med låg risk, så att organisationens resurser främst används för att hantera mer omfattande, komplexa och riskfyllda ändringar. Det behöver framgå av de interna reglerna i vilka situationer snabbspår kan respektive ska användas. Det finns också verktyg som automatiskt inför godkända ändringar i organisationens it-miljö. Användningen av sådana verktyg gör det enklare för organisationen att exempelvis skyndsamt införa säkerhetsuppdateringar.

4.7.4 Uppdatering

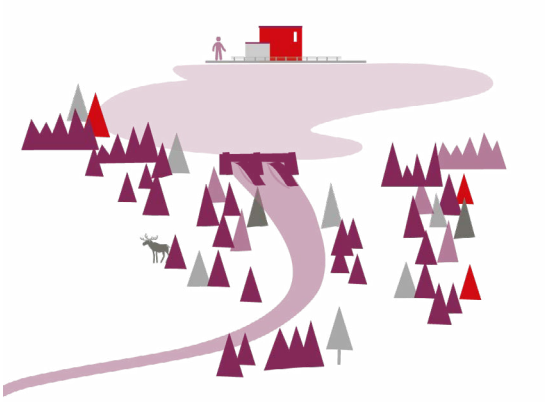
Med uppdatering avses en installation av leverantörens senaste version av en mjukvara som redan finns i informationssystemet. Det är viktigt att utan dröjsmål uppdatera till senaste version, eftersom nyare versioner i de flesta fall innehåller färre sårbarheter samt ofta flera och bättre säkerhetsfunktioner än äldre versioner. Detta gäller all mjukvara, såsom operativsystem, firmware, drivrutiner och applikationer. En uppdatering kan innehålla nya funktioner, vilket gör att säkerhetskonfigurationen kan behöva ses över för att motsvara organisationens behov.

Säkerhetsuppdateringar är en särskild typ av uppdateringar. För att en it-miljö ska vara så säker som möjligt behöver organisationen alltid ha den senaste säkerhetsuppdateringen installerad på varje enskilt informationssystem. Sådana installationer bör dessutom göras skyndsamt. Ibland tar det bara några timmar från det att en säkerhetsuppdatering släppts från en leverantör tills att den kända sårbarheten används i större skala och angrepp mot organisationer som inte hunnit säkerhetsuppdatera genomförs. Organisationen bör därför överväga behovet av att automatisera införandet av säkerhetsuppdateringar. I vissa fall utnyttjas sårbarheten också innan leverantören har haft möjlighet att ta fram en säkerhetsuppdatering, så kallad zero-day-sårbarhet. Det är därför viktigt att ha säkerhetsåtgärder i flera lager och ett arbetssätt för att snabbt kunna införa ytterligare säkerhetsåtgärder när sårbarhetens omfattning och karaktär blir känd. Det kan bli nödvändigt att helt stänga ned sårbara informationssystem i väntan på uppdateringar.

4.7.5 Uppgradering

Hård- och mjukvara blir med tiden mindre säkra. Det kan bero på att det har upptäckts nya sårbarheter som inte kan hanteras med den äldre tekniken som informationssystemet är byggt av, eller att leverantören inte längre tillhandahåller uppdateringar och support. Det är viktigt att utan onödigt dröjsmål uppgradera hård- och mjukvara där uppdateringar inte längre tillhandahålls av leverantören. Organisationen kan också välja att helt byta ut den äldre hård- och mjukvaran mot en ny lösning.

Det kan vara en utmaning för organisationer att få resurser till att uppgradera informationssystem genom att byta ut äldre hård- och mjukvara. Inled arbetet med att uppgradera informationssystem genom att ta fram en plan för hur ny hård- och mjukvara ska anskaffas och hanteras under sin livstid, och hur och när den ska ersättas. Som underlag till planen behöver beroenden till andra informationssystem och hur de påverkas av en uppgradering analyseras. Att inte i tid planera för att uppgradera hård- och mjukvara medför en risk att sitta med föråldrade informationssystem i vilka en angripare kan utnyttja kända sårbarheter.



4.8 Korrekt och spårbar tid

4.8.1 Syfte

För att kunna jämföra loggar mellan olika informationssystem och använda funktioner som ökar säkerheten vid kommunikation med andra, behöver organisationen[99] använda den officiella svenska normaltiden hämtad från en robust tidstjänst.

4.8.2 Krav

Organisationen *ska* använda robust och korrekt tid spårbar till den svenska tillämpningen av koordinerad universell tid, UTC(SP), i sin produktionsmiljö.[100]

Organisationen bör[101]

1. använda tidstjänsten Swedish Distributed Time Service på www.ntp.se
2. identifiera och hantera behovet av att använda robust och korrekt tid spårbar till den svenska tillämpningen av koordinerad universell tid, UTC(SP), i utvecklings-, test- och utbildningsmiljö.

4.8.3 Robust och korrekt tid

Med korrekt tid avses här tid som är spårbar till Universal Time Coordinated (UTC). UTC baseras på den internationella atomtiden och används för exakta tidsangivelser i hela världen. Den svenska motsvarigheten, den officiella svenska normaltiden, kallas UTC(SP). Post- och telestyrelsen erbjuder en robust tidtjänst[102] som är fritt tillgänglig och spårbar mot den officiella svenska normaltiden UTC(SP).

Robust och korrekt tid är en förutsättning för att kunna utreda olika händelser i it-miljön. När loggar från olika informationssystem behöver jämföras för att upptäcka fel (systemloggar) eller säkerhetsincidenter (säkerhetsloggar) underlättar det avsevärt om informationssystemen använder samma tid. Om olika tider används blir det svårt eller ibland omöjligt att veta i vilken ordning olika händelser inträffade. Vissa sätt att kommunicera med andra organisationer förutsätter också användningen av korrekt tid.[103] Detta skapar behov av att olika organisationer använder samma tid och gärna samma tidstjänst.

Organisationens it-avdelning ska därför säkerställa att organisationen använder en robust och korrekt tid spårbar till den svenska tillämpningen av koordinerad universell tid, UTC(SP), i sin produktionsmiljö.[104] Organisationen bör också identifiera behovet av att använda sådan tid i sin utvecklings-, test- och utbildningsmiljö.

Det är ofta lämpligt att organisationen installerar en central tidskälla i sin egen it-miljö som i sin tur kontinuerligt hämtar tid från tidstjänsten. Organisationen behöver identifiera och hantera konsekvenser av att den centrala tidskällan inte kan upprätthålla kontakt med den valda tidstjänsten samt att se över behovet av reservtidstjänster.

Vissa informationssystem i organisationens produktionsmiljö kan sakna möjlighet att hämta tid från organisationens centrala tidskälla, exempelvis på grund av ålder eller geografisk placering. I dessa fall är det bättre att använda någon tidskälla än ingen tidskälla alls. Ett alternativ är att organisationen kan låta informationssystemen synkronisera med på förhand valda reservtidstjänster.[105]

99. Eftersom vägledningen har som huvudsyfte att underlätta tillämpningen av föreskriftskrav på säkerhetsåtgärder i informationssystem för svenska myndigheter hänvisas till den officiella svenska normaltiden. Andra organisationer med internationell anknytning kan av olika skäl ha anledning att använda en annan nationell normaltid.

100. MSBFS 2020:7 4 kap. 13 § Myndigheten ska använda robust och korrekt tid spårbar till den svenska tillämpningen av koordinerad universell tid, UTC(SP), i sin produktionsmiljö.

101. Allmänt råd till MSBFS 2020:7 4 kap. 13 § Myndigheten bör använda tidstjänsten Swedish Distributed Time Service på www.ntp.se. Behovet av att använda robust och korrekt tid spårbar till den svenska tillämpningen av koordinerad universell tid, UTC (SP) i utvecklings-, test- och utbildningsmiljö bör identifieras och hanteras.

102. Network Time Protocol, NTP. För mer information om PTS NTP-tjänst, se www.ntp.se som beskriver tjänsten.

103. Det gäller exempelvis vid användning av TLS-förbindelser[102], DNSSEC[102], SAML[102] och Kerberos.

104. Nyttjas externa tjänster behöver organisationen kravställa att UTC (SP) används, detta gäller även molntjänster.

105. Till exempel Global Navigation Satellite System (GNSS).

4.9 Säkerhetskopiering

4.9.1 Syfte

För att kunna återskapa information som obehörigt eller av misstag har förstörts eller ändrats, behöver organisationen säkerhetskopiera sin information och skydda sina säkerhetskopior.

4.9.2 Krav

Organisationen ska

1. regelbundet säkerhetskopiera sin information, för att kunna återställa information som förlorats eller förvanskats[106]
2. förvara säkerhetskopior skilda från produktionsmiljön och skydda dessa mot skada, obehörig åtkomst och obehörig förändring.[107]

Organisationen bör[108]

1. en gång per dygn säkerhetskopiera information som behövs för organisationens förmåga att bedriva sin verksamhet
2. en gång per år, eller vid större förändringar av produktionsmiljön, verifiera sin förmåga att, inom en godtagbar tidsperiod, återställa information från säkerhetskopior
3. hantera programvara, konfiguration respektive information separat vid bedömningen av säkerhetskopieringens omfattning och intervall
4. identifiera och hantera behovet av säkerhetskopiering och förmågan till återställning av information i utvecklings-, test- och utbildningsmiljö.

106. MSBFS 2020:7 4 kap. 14 § Myndigheten ska, för att kunna återställa information som förlorats eller förvanskats, regelbundet säkerhetskopiera sin information.

107. MSBFS 2020:7 4 kap. 15 § Säkerhetskopior ska förvaras skilda från produktionsmiljön och skyddas mot skada, obehörig åtkomst och obehörig förändring.

108. Allmänt råd till MSBFS 2020:7 4 kap. 14 § Myndigheten bör 1. en gång per dygn säkerhetskopiera information som behövs för myndighetens förmåga att utföra sitt uppdrag, och 2. en gång per år, eller vid större förändringar av produktionsmiljön, verifiera förmågan att, inom för myndigheten godtagbar tidsperiod, återställa information från säkerhetskopior. Vid bedömning av säkerhetskopieringens omfattning och intervall, bör programvara, konfiguration respektive information hanteras separat. Behovet av säkerhetskopiering och förmåga till återställning av information i utvecklings-, test- och utbildningsmiljö bör identifieras och hanteras.

4.9.3 Säkerhetskopiering

Information som obehörigt eller av misstag förlorats eller förvanskats behöver kunna återställas. Vid säkerhetskopiering skapas en kopia av informationen i ett informationssystem vid en viss tidpunkt. Organisationen behöver regelbundet säkerhetskopiera all relevant information, det vill säga

- verksamhetsinformation
- konfiguration
- programvara.

It-avdelningen behöver genomföra säkerhetskopieringen utifrån verksamhetens behov, avseende både tillgång till verksamhetsinformation och funktionalitet i it-miljön.

Med vilket intervall en säkerhetskopia behöver tas beror på vilken information och funktionalitet i it-miljön som verksamheten kan acceptera att förlora. För viss tidskritisk verksamhet kan det innebära att säkerhetskopior behöver tas oftare än en gång i minuten. Organisationen bör dock minst en gång per dygn säkerhetskopiera information som behövs för förmågan att bedriva sin verksamhet. Hur ofta säkerhetskopior behöver tas kan styra vilken teknik för säkerhetskopiering som kan användas.

Även omfattningen av säkerhetskopiering behöver utgå från verksamhetens behov. En organisation ska kunna återställa information som förlorats eller förvanskats. Man behöver inte säkerhetskopiera information som inte riskerar att förloras eller förvanskas, antingen på grund av att den enkelt kan återskapas genom andra medel än säkerhetskopiering eller att den är av ett så ringa värde för organisationen att den kan mista informationen utan några konsekvenser.

Behovet av att kunnat återskapa funktionalitet i it-miljön kan kräva tillgång till säkerhetskopior av konfigurationer och programvara. Säkerhetskopieringar av konfigurationer och programvara behöver säkerställa att den senaste versionen finns tillgänglig.

I utvecklings-, test- och utbildningsmiljö behöver organisationen fastställa omfattning och intervall av säkerhetskopiering inklusive återställning i utifrån verksamhetsbehovet i respektive miljö.

Två exempel på incidenter som kräver att det finns säkerhetskopior för återställning:

- Ett utpressningsprogram (ransomware) orsakar att delar av, eller hela, informationssystemet krypteras så att informationen blir otillgänglig.
- Filsystemet blir korrupt och informationen blir otillgänglig.

Eftersom vissa incidenter kan vara svåra att upptäcka är det lämpligt att inte bara spara den senast tagna säkerhetskopian utan även säkerhetskopior några versioner tillbaka. Då kan informationssystemet återställas även om den senaste säkerhetskopian innehåller fel eller skadlig kod. Det är också lämpligt att använda lösningar som förhindrar att säkerhetskopian oavsiktligt skrivs över.[109]

Det är lämpligt att i drifts-och förvaltningsdokumenationen för ett informationssystem inkludera hur säkerhetskopieringen ska bedrivas genom att beskriva följande:

- vilken information som ska säkerhetskopieras
- hur ofta säkerhetskopiering ska genomföras och hur ändringar som gjorts efter säkerhetskopiering ska hanteras
- hur snabbt återställning behöver kunna göras
- på vilket sätt återställning ska göras
- hur länge säkerhetskopiorna ska lagras
- hur säkerhetskopiorna ska skyddas.

4.9.4 Återställa information

Brister vid säkerhetskopiering kan medföra att återläsningen tar lång tid, eller i vissa fall till och med är omöjlig. Organisationen behöver kontrollera följande för de säkerhetskopior som tagits:

- att de innehåller rätt information
- att informationen är i rätt format
- att informationen kan återställas inom den tidsperiod som verksamheten definierat.

Återställning kan göras på olika sätt. Ibland behöver hela eller delar av verksamhetsinformationen återställas, ibland behöver därutöver även konfigurationen och programvaran i informationssystemet återställas. I vissa fall behöver informationssystemet återskapas helt från grunden inklusive installation av ny hårdvara.

Organisationen bör en gång per år, eller vid större förändringar av produktionsmiljön, verifiera sin förmåga att, inom en godtagbar tidsperiod, återställa information från säkerhetskopior enligt informationssystemets återställningsrutin. Det är dock lämpligt att genomföra sådan verifiering oftare när det gäller verksamhetsinformation och funktionalitet i it-miljön som är central för organisationens förmåga att bedriva sin verksamhet.

4.9.5 Förvara säkerhetskopior

Säkerhetskopior kan lagras digitalt på interna eller externa hårddiskar, databand och ibland cd eller dvd. Organisationen ska förvara minst en säkerhetskopia skild från produktionsmiljön och skydda samtliga säkerhetskopior mot skada, obehörig åtkomst och obehörig förändring. Informationen på säkerhetskopiorna behöver skyddas vid både överföring och lagring.

109. Write Once Read Many (WORM).

Det är lämpligt att tillämpa 3-2-1-regeln vid säkerhetskopiering:

- Skapa tre (3) säkerhetskopior av informationen: en primär och två extra.
- Förvara informationen på två (2) olika lagringsmedia för att skydda mot olika typer av hot.
- Förvara ett (1) exemplar av säkerhetskopiorna fysiskt åtskilt från produktionsmiljön på en annan geografisk plats.

Skyddet av säkerhetskopiorna behöver vara på motsvarande nivå som skyddet för informationen som säkerhetskopierats. När det gäller förvaringen av olika exemplar av säkerhetskopiorna är det lämpligt att placera en i närheten av produktionsmiljön för att underlätta en snabb återställning och en på en geografiskt åtskild plats för att skydda säkerhetskopian från miljörelaterade händelser (till exempel brand eller översvämning) som påverkar produktionsmiljön. Det är också lämpligt att förvara olika versioner av säkerhetskopior åtskilda från varandra. Förvaras flera säkerhetskopior på samma plats behöver nivån på skyddet omhänderta den aggregerade mängden information som säkerhetskopierats.

Säkerhetskopior som lagras på hårddiskar och som går att nå via nätverket är sårbara för skadlig kod, till exempel krypteringsvirus. Lagras säkerhetskopior på en sådan hårddisk, är det lämpligt att lagra ytterligare en kopia logiskt åtskilt, en off-linekopia. Databand tar man normalt ur sin bandstation eller bandrobot och förvarar på en plats som är skild från it-utrymmet, vanligtvis ett säkerhetsskåp. Även bandstationen eller bandroboten behöver skyddas på motsvarande nivå som informationen de kopierar.

4.10 Säkerhetsloggning

4.10.1 Syfte

För att i efterhand kunna upptäcka och hantera incidenter och avvikelser som kan påverka säkerheten i informationssystemen, behöver organisationen logga säkerhetsrelaterade händelser.

4.10.2 Krav

Organisationen ska

1. säkerställa spårbarhet i informationssystem genom att logga följande säkerhetsrelaterade händelser:[110]
   a. obehörig åtkomst och försök till obehörig åtkomst till it-miljö och enskilda informationssystem
   b. förändringar av konfigurationer och säkerhetsfunktioner som förutsätter priviligierade rättigheter
   c. förändringar av behörighet för användare och informationssystem
   d. åtkomst till information som bedömts ha behov av utökat skydd
2. analysera innehållet i säkerhetsloggarna för att upptäcka och hantera incidenter och avvikelser, och säkerhetsloggarna ska[111]
   a. möjliggöra utredning av intrång, tekniska fel och brister i säkerheten
   b. utformas på ett sätt som möjliggör jämförbarhet mellan olika loggar
   c. vara tillgängliga för analys under fastställd bevarandetid.
3. dokumentera[112]
   a. hur säkerhetsloggarna ska användas
   b. varifrån loggningsuppgifter hämtas
   c. var säkerhetsloggarna lagras
   d. hur de skyddas
   e. hur länge de ska bevaras.

Organisationen bör[113]

1. säkerställa att en säkerhetslogg innehåller uppgifter om
   a. vem eller vad som har agerat
   b. vad som har skett
   c. vid vilken tidpunkt
2. skapa jämförbarhet genom att använda organisationens tidstjänst för samtliga säkerhetsloggar
3. samla säkerhetsloggar i ett för ändamålet avsett informationssystem.

4.10.3 Att säkerhetslogga

Genom loggning registreras olika händelser i ett informationssystem. Vid säkerhetsloggning registreras sådana händelser som på förhand har identifierats som viktiga ur ett säkerhetsperspektiv, så kallade säkerhetsrelaterade händelser. Säkerhetsloggar är viktiga för att kunna upptäcka och hantera incidenter och avvikelser i informationssystem. Organisationen bör se till att säkerhetsloggarna innehåller de loggningsuppgifter som krävs för att organisationen ska kunna förstå händelseförloppet. Att samtliga informationssystem sammanställer sina logguppgifter i ett standardiserat format samt hämtar logguppgifternas tid från organisationens tidstjänst är i princip nödvändigt för att kunna jämföra säkerhetsloggar från olika informationssystem och därmed förstå händelseförloppet.

110. MSBFS 2020:7 4 kap. 16 § Myndigheten ska, för att säkerställa spårbarhet i informationssystem, logga följande säkerhetsrelaterade händelser: 1. Obehörig åtkomst och försök till obehörig åtkomst till it-miljö och enskilda informationssystem. 2. Förändringar av konfigurationer och säkerhetsfunktioner som förutsätter priviligierade rättigheter. 3. Förändringar av behörighet för användare och informationssystem. 4. Åtkomst till information som bedömts ha behov av utökat skydd.

111. MSBFS 2020:7 4 kap. 17 § Myndigheten ska analysera innehållet i säkerhetsloggarna för att upptäcka och hantera incidenter och avvikelser. Säkerhetsloggarna ska 1. möjliggöra utredning av intrång, tekniska fel och brister i säkerheten, 2. utformas på ett sätt som möjliggör jämförbarhet mellan olika loggar, och 3. vara tillgängliga för analys under fastställd bevarandetid.

112. MSBFS 2020:7 4 kap. 17 § Myndigheten ska dokumentera hur säkerhetsloggarna ska användas samt var loggningsuppgifter hämtas och lagras, hur de skyddas och hur länge de ska bevaras.

113. Allmänt råd till MSBFS 2020:7 4 kap. 17 § En säkerhetslogg bör innehålla uppgift om vem eller vad som agerat, vad som har skett och vid vilken tidpunkt. För att skapa jämförbarhet bör myndigheten använda myndighetens tidstjänst för samtliga säkerhetsloggar. Säkerhetsloggar bör samlas i ett för ändamålet avsett informationssystem.

Organisationen ska alltid säkerhetslogga

- obehörig åtkomst och försök till obehörig åtkomst till it-miljö och enskilda informationssystem
- förändringar av konfigurationer och säkerhetsfunktioner som förutsätter priviligierade rättigheter
- förändringar av behörighet för användare och informationssystem
- åtkomst till information som bedömts ha behov av utökat skydd.

Utformning av säkerhetsloggning

Vid utformningen av säkerhetsloggningen behöver följande ingångsvärden användas:

- vilka informationssystem som behandlar information i behov av utökat skydd (konfidentialitet, riktighet, tillgänglighet)
- vilka informationssystem som är nödvändiga för att organisationen ska kunna bedriva sin verksamhet
- vilka digitala identiteter som har systemadministrativ behörighet
- vilka digitala identiteter som har tilldelats åtkomst till information i behov av utökat skydd
- vilka digitala identiteter som har utökad behörighet för att kunna utföra vissa arbetsuppgifter
- genom vilka trafikfiltrerande utrustningar som information passerar.

Vad som i övrigt behöver säkerhetsloggas beror på organisationens behov av ytterligare spårbarhet i sin it-miljö. Organisationen behöver, för respektive informationssystem, analysera vilka ytterligare säkerhetsrelaterade händelser som behöver samlas in och vilka logganalyser som behöver kunna genomföras för att förstå ett händelseförlopp. Säkerhetsloggar behöver skapas i nästan alla informationssystem. Det som skiljer olika informationssystem åt är snarare vad som behöver säkerhetsloggas och hur länge detta behöver lagras.

Även om organisationen själv har en begränsad förmåga att analysera säkerhetsloggarna, är det viktigt att samla in alla logguppgifter som behövs för att förstå ett händelseförlopp. Om en incident inträffar kan organisationen då tillhandahålla säkerhetsloggarna till rättsvårdande myndigheter eller till externt stöd för hjälp med att hantera incidenten.

Säkerhetsloggar innehåller ofta känslig information om enskilda medarbetare. Därför måste organisationens intresse av att samla in loggar som innehåller personuppgifter alltid vägas mot behovet av att skydda den personliga integriteten. Loggarna får också enbart användas på ett i förväg beslutat sätt. Av dataskyddsförordningen framgår att uppgifter endast får behandlas om det är såväl nödvändigt som proportionerligt med hänsyn till den enskildes integritet. Säkerhetsloggning kan även utgöra ett skydd för den enskildes integritet eftersom det bidrar till spårbarhet rörande vem som har gjort vad med personuppgifterna. Säkerhetsloggning kan även utgöra ett skydd för den enskildes integritet eftersom det bidrar till spårbarhet rörande vem som har gjort vad med personuppgifterna och är således ofta en viktig del i efterlevnaden av dataskyddsförordningen.

Utformningen av säkerhetsloggningen ska dokumenteras. Av dokumentationen ska följande framgå:

- syftet med insamlingen av säkerhetsloggar, det vill säga vad man behöver kunna upptäcka
- hur säkerhetsloggarna ska användas, det vill säga när och på vilket sätt de ska analyseras
- vilken information säkerhetsloggarna innehåller
- varifrån loggningsuppgifter hämtas, det vill säga från vilka informationssystem
- var säkerhetsloggarna lagras, det vill säga både temporär och varaktig lagring
- hur de skyddas, det vill säga mot skada, obehörig åtkomst och obehörig förändring vid överföring och lagring
- hur länge de ska bevaras och kunna användas för analys.

I dokumentationen över hur säkerhetsloggarna ska användas respektive hur länge de ska bevaras, behöver organisationen beskriva syftet med behandlingen av personuppgifter.

För att kunna säkerställa spårbarheten i informationssystem ska organisationen regelbundet kontrollera att rätt säkerhetsrelaterade händelser samlas in, såsom vem eller vad som har agerat, vad som har skett[114] inklusive vid vilken tidpunkt. Analysen av innehållet ska ge stöd för att upptäcka och hantera incidenter och avvikelser.

Skydda säkerhetslogga

Säkerhetsloggarna behöver skyddas mot obehörig åtkomst och obehörig förändring.

- En angripare som har fått åtkomst till ett informationssystem försöker ofta utplåna eventuella spår. Detta kan ofta bara göras genom att förändra säkerhetsloggarna.
- Loggarna innehåller ofta personuppgifter och dessa behöver skyddas enligt kraven i dataskyddsförordningen.
- För att loggarna ska vara användbara i analysarbetet behöver det säkerställas att ingen har förändrat dem sedan de samlades in.
- Loggar kan också innehålla annan kritisk information, exempelvis känslig verksamhetsinformation eller information om systemkonfigurationer och sårbarheter.

Organisationen behöver se till att det finns tillräcklig behörighetsstyrning för att förhindra att obehöriga tar del av innehållet i loggar. Det är lämpligt att logga åtkomst, förändring och radering av loggar. För att kunna upptäcka obehörig förändring av loggarna behöver krypteringslösningar användas.[115]

Logguppgifter som har skapats i ett informationssystem kan antingen föras över till ett informationssystem som används för lagring av säkerhetsloggar eller lagras i det informationssystem där de skapats. För att göra det enklare att skydda och analysera säkerhetsloggarna bör organisationen samla dessa i ett för ändamålet avsett informationssystem, exempelvis ett loggsystem med central lagring.[116] Att aktivera säkerhetsloggning på alla informationssystem kan generera stora mängder information. Oavsett var säkerhetsloggarna lagras behöver organisationen kontrollera att det finns tillräckligt med lagringsutrymme för att undvika risken att nya logguppgifter inte längre skrivs in alternativt skriver över äldre uppgifter som ska sparas.

4.10.4 Analys av säkerhetsloggar

Både bristande insamling av logguppgifter och bristande analys av säkerhetsloggarna kan göra att incidenter och avvikelser inte kan upptäckas eller utredas. Det kan exempelvis leda till att en angripares närvaro i organisationens it-miljö inte upptäcks. Bristerna kan också leda till att det inte finns någon möjlighet att förstå händelseförloppet, även om en organisation upptäcker att någon har skaffat sig obehörig åtkomst till organisationens informationssystem.

Analys av säkerhetsloggar krävs för att kunna upptäcka och förstå händelser som avviker från normal och tillåten användning av organisationens informationssystem. För att kunna utreda intrång, tekniska fel och brister i säkerheten behöver organisationen kunna återskapa ett händelseförlopp med ofta flera inblandade informationssystem. Det är viktigt att ha säkerställt jämförbarhet mellan logguppgifter hämtade från olika informationssystem. Om organisationen vid analysen av en incident eller avvikelse upptäcker brister i säkerhetsloggarnas innehåll eller utformning behöver dessa åtgärdas, exempelvis genom att samla in fler logguppgifter, se över logguppgifternas format eller utföra säkerhetsloggning i fler informationssystem.

114. Exempelvis händelser som innebär att någon läst, sökt, skrivit, raderat eller skapat information.

115. Se vidare avsnitt 4.4.6 Säkerhetsloggar.

116. Logg Management System, (LMS).

Logganalysen behöver genomföras på ett strukturerat sätt. Organisationens arbetssätt för analys av säkerhetsloggar behöver därför tydliggöra

- vilka som får hantera respektive utföra analys av säkerhetsloggar, exempelvis kan logguppgifter från ett informationssystem behöva hämtas ut manuellt av den tekniska systemförvaltaren medan analysen av säkerhetsloggar genomförs av utpekad logganalytiker
- när analys ska genomföras för respektive informationssystem, exempelvis regelbundet, genom stickprovskontroller eller på förekommen anledning
- hur analys av säkerhetsloggar ska genomföras, exempelvis om det ska ske automatiskt, manuellt eller en kombination och med vilka tekniska stöd
- vilka åtgärder som ska vidtas och vilka som ska kontaktas om en incident eller avvikelse upptäcks
- vilka sammanställningar av händelser och vilken statistik som ska tas fram för att kunna informera om inträffade avvikelser och incidenter samt förbättra arbetssättet för säkerhetsloggning.

Misstankar om brister i säkerheten behöver skyndsamt utredas för att kunna bekräftas eller avfärdas. Det kan exempelvis handla om misstankar om att personal inte följt interna regler om hantering av personuppgifter i ett visst informationssystem, eller att en angripare försökt få åtkomst till it-miljön.

Det är oftast nödvändigt att analysen av säkerhetsloggar görs med stöd av automatiserade verktyg, eftersom det ofta handlar om stora mängder logguppgifter som behöver jämföras med varandra. Vilket verktyg som är lämpligt att använda beror på syftet med analysen. Analysverktyget behöver kontinuerligt anpassas och kalibreras för att kunna upptäcka intrång, tekniska fel och brister i säkerheten i organisationens säkerhetsloggar.

4.11 Övervakning

4.11.1 Syfte

För att upptäcka och hantera intrång och avvikelser som kan påverka säkerheten, behöver organisationen övervaka säkerhetsrelaterade händelser i sina informationssystem.

4.11.2 Krav

Organisationen ska identifiera och hantera behovet av

1. intrångsdetektering[117]
2. intrångsskydd[118]
3. realtidsövervakning av informationssystem.[119]

Organisationen bör bedöma behovet av intrångsdetektering och intrångsskydd för[120]

1. enskilda informationssystem
2. organisationens produktionsmiljö i sin helhet
3. organisationens utvecklings-, test- respektive utbildningsmiljö.

4.11.3 Intrångsdetektering och intrångsskydd

Intrångsdetektering syftar till att upptäcka försök till och genomförda intrång. Intrångsdetekteringssystemet kan kompletteras med intrångsskydd som ger möjlighet att även agera på upptäckta försök till intrång, exempelvis genom att direkt blockera angreppet. Intrång som kan antas ha en brottslig grund polisanmäls.

Ett intrångsdetekteringssystem kan övervaka både nätverkstrafik och aktiviteter i enskilda informationssystem. Övervakning är särskilt viktig i produktionsmiljön men beroende på hur utvecklings-, test- respektive utbildningsmiljön används kan det vara nödvändigt även där. Vilka informationssystem som behöver övervakning är beroende av deras placering, vilken information som behandlas och dess betydelse för organisationens möjlighet att bedriva sin verksamhet. Övervakning är särskilt viktig i informationssystem med koppling till externa nätverk, exempelvis e-post, webbsidor, webbtjänster och DNS-servrar.

Det är lämpligt att övervaka

- nätverkstrafik
- säkerhetsfunktioner
- konfigurationer
- informationssystem som behandlar information i behov av utökat skydd
- informationssystem som av andra skäl bedöms ha behov av övervakning.

Konfigurera intrångsdetekteringssystemet för att undersöka både ingående och utgående nätverkstrafik (både internettrafik och system till systemkommunikation med en annan organisation) samt nätverkstrafiken i särskilt utsatta nätverkssegment mot kända sårbarheter och angreppsmetoder. Intrångsdetekteringen ska även omfatta trafik till och från särskilt värdefulla informationssystem, exempelvis informationssystem som behandlar information i behov av utökat skydd samt säkerhetsfunktioner såsom katalogtjänster, säkerhetsloggar och säkerhetskopiering. Implementeringen av intrångsdetekteringssystem och annan övervakning tar tid eftersom verktyget behöver anpassas till en nivå där de händelser som kan tyda på intrång uppmärksammas och övriga ignoreras.

117. MSBFS 2020:7 4 kap. 18 § Myndigheten ska identifiera och hantera behovet av intrångsdetektering och intrångsskydd.

118. MSBFS 2020:7 4 kap. 18 § Myndigheten ska identifiera och hantera behovet av intrångsdetektering och intrångsskydd.

119. MSBFS 2020:7 4 kap. 19 § Myndigheten ska identifiera och hantera behovet av realtidsövervakning av informationssystem.

120. Allmänt råd till MSBFS 2020:7 4 kap. 18 § Behovet av intrångsdetektering och intrångsskydd bör bedömas för enskilda informationssystem och för myndighetens produktionsmiljö i sin helhet. Behovet bör även bedömas för myndighetens utvecklings- test- och utbildningsmiljö.

Om ett angrepp upptäcks behöver organisationen hantera det i enlighet med sitt arbetssätt för incidenthantering. Det vanligaste är att blockera angriparen. I vissa fall kan det, om det inte finns någon risk för ytterligare skada, finnas anledning att istället låta angreppet fortsätta under noggrann övervakning för att få fram ytterligare underlag om hur intrånget genomförts i syfte att kunna förhindra framtida intrång. Intrångsdetekteringssystemet som används i nätverkens yttre skydd och de som används för att skydda interna nätverk behöver vara olika för att uppfylla sina respektive interna och externa syften. Att ha olika interna och externa intrångsdetekteringssystem bidrar även till att minska risken för att båda systemen påverkas vid ett angrepp.

De på it-enheten som arbetar med intrångsdetektering behöver ha kunskap om intrångsmetoder och hantering av skadlig kod. Det är också lämpligt att de har erfarenhet av att hantera och utreda incidenter.

4.11.4 Realtidsövervakning

Organisationen ska identifiera och hantera behovet av realtidsövervakning. Med hjälp av realtidsövervakning kan organisationen bevaka status på informationssystemens funktionalitet i realtid. De verktyg som används för realtidsövervakning kan konfigureras för att larma vid incidenter och avvikelser, exempelvis när fastställda tröskelvärden överskrids. Det är lämpligt att använda realtidsövervakning för att upptäcka

- om otillåten utrustning ansluts till it-miljön
- exekvering eller försök av exekvering av otillåten mjukvara
- om otillåtna kommandon körs i kommandogränssnitt
- fel i mjukvara
- problem med lagringsutrymme
- onormalt utnyttjande av systemresurser
- obehörig användning av systemadministrativa behörigheter
- obehörig åtkomst eller försök till obehörig åtkomst
- onormal nätverkstrafik, exempelvis med hänsyn till tidpunkten
- otillåten nätverkstrafik mellan nätverkssegment
- upptäckt av skadlig kod.

Realtidsövervakning är ofta resurskrävande initialt. Realtidsövervakning förutsätter inte alltid bemanning dygnet runt. En organisation kan välja att ha egen bemanning på plats under dagtid och att larm som inkommer övrig tid hanteras av jourpersonal. Under förutsättning att organisationen bedömer att samtliga larm som inkommer utanför ordinarie arbetstid kan, med bibehållen säkerhet, hanteras genom intrångsskydd som blockerar angrepp och sedan omhändertas påföljande arbetsdag även välja en sådan lösning. Behovet och utformningen av övervakning behöver utgå från verksamhetens behov och rådande hotbild.

4.12 Skydd mot skadlig kod

4.12.1 Syfte

För att förhindra installation, spridning och exekvering av virus, maskar, trojaner, spionprogram, utpressningsprogram och liknande i sin it-miljö, behöver organisationen skydda sig mot skadlig kod.

4.12.2 Krav

Organisationen ska

1. använda mjukvara som ger skydd mot skadlig kod.

För informationssystem där sådan mjukvara inte finns tillgänglig ska andra åtgärder vidtas.[121]

4.12.3 Skadlig kod

Skadlig kod är ett konstant hot mot it-miljön. Utöver att orsaka skada är koden ofta utformad för att undgå, inaktivera eller angripa säkerhetsfunktioner.

Skadlig kod kan sprida sig snabbt, vid behov förändra sig och kan bland annat ta sig in via e-post, webbsidor och flyttbara lagringsmedier. Den skadliga koden kan resultera i olika typer av skada, exempelvis ger den en angripare möjlighet att

- få en ingång till it-miljön för att kartlägga bästa angreppsmetod, exempelvis i syfte att ta över hela it-miljön
- få åtkomst till information inklusive förstöra eller ändra information
- utnyttja organisationens informationssystem för att beräkna kryptovalutor eller skicka ut skräppost
- kryptera organisationens information för att sedan bedriva utpressning.

Det är vanligt att få in skadlig kod i it-miljön genom att användare luras att klicka på länkar eller öppna e-postbilagor med makron. Organisationen kan även få skadlig kod genom informationsdelning med andra organisationer. Vid bedömningen av risken för att drabbas av skadlig kod behöver därför olika ingångsvägar till och spridningsmöjligheter i it-miljön beaktas.

Sättet som den skadliga koden sprids, vilka konsekvenser den får och vilka informationssystem som är mer utsatta ändras kontinuerligt. Därför är det viktigt med omvärldsbevakning avseende utveckling av skadlig kod och vilka informationssystem den angriper.

4.12.4 Mjukvara mot skadlig kod (antivirusprogram)

En organisation måste ha skydd mot känd skadlig kod och mot kända metoder att sprida koden. Men det behöver också finnas beredskap för att hantera nyutvecklad skadlig kod. Det finns två olika sätt att skydda sig mot skadlig kod med hjälp av mjukvara (antivirusprogram[122]) – svartlistning och vitlistning.

Svartlistning är en vanlig funktion i antivirusprogram, men för att ge god effekt är det viktigt att leverantören av programmet är snabb att tillhandahålla uppdateringar så fort ny skadlig kod upptäcks. Innan sådan uppdatering har skett är organisationen oskyddad mot den nya skadliga koden.

Skyddet förbättras genom att införa vitlistningsfunktioner. Vitlistning kräver dock ett strukturerat arbetssätt. Detta för att säkerställa att de mjukvaror som organisationen behöver för sin verksamhet tillåts samtidigt som skadlig kod utestängs. För att inte användarna ska påverkas i onödan när vitlistning börjar användas är det lämpligt att använda funktionens inlärningsläge under en övergångsperiod.

121. MSBFS 2020:7 4 kap. 20 § Myndigheten ska använda mjukvara som ger skydd mot skadlig kod. För informationssystem där sådan mjukvara inte finns tillgänglig ska andra åtgärder vidtas som ger motsvarande skydd.

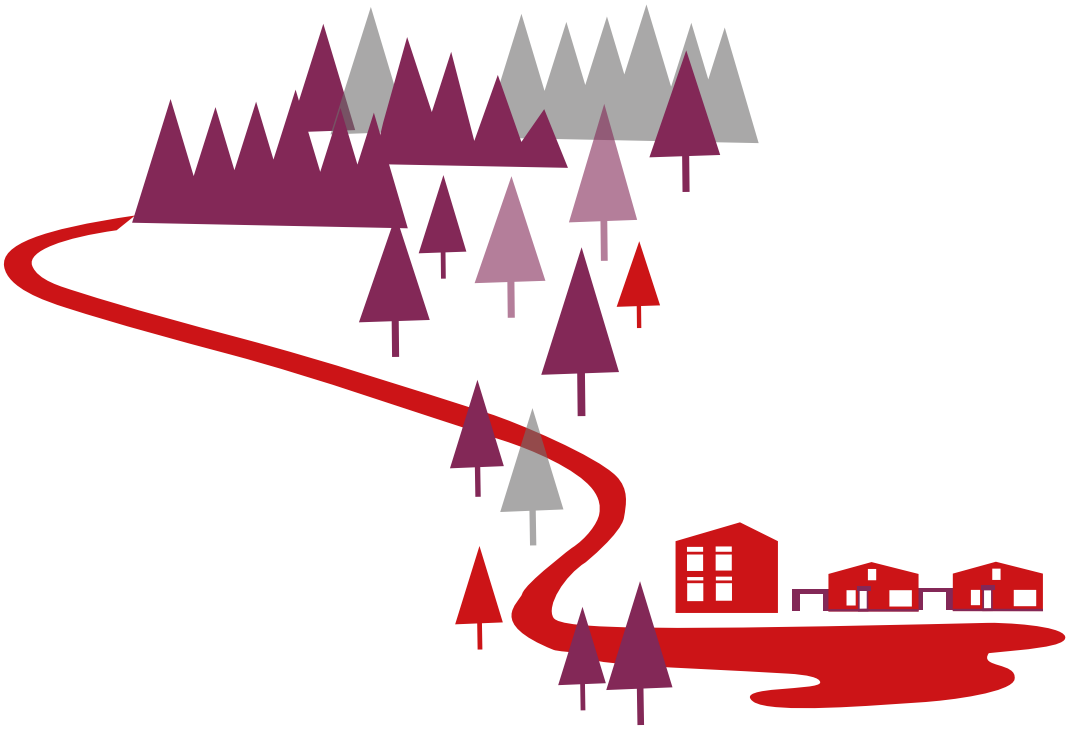
122. Antivirusprogram används både i dagligt tal och här som en beskrivning av mjukvara som skyddar mot alla typer av skadlig kod.

För att få ett mer heltäckande skydd behöver organisationen kombinera svartlistning och vitlistning.

Antivirusprogram behöver finnas på både klienter och servrar, särskilt sådana som behandlar information från externa nätverk. Det är lämpligt att använda ett särskilt informationssystem för att hantera installation, uppdateringar och larm från antivirusprogram på ett samlat sätt. Organisationen behöver ha ett arbetssätt som tydliggör hur larm om skadlig kod ska hanteras utifrån kodens allvarlighetsgrad, det vill säga risk för spridning och skada. I vissa fall är det viktigt att agera snabbt och kraftfullt för att kunna stoppa angreppet.

4.12.5 Om antivirusprogram inte finns tillgängliga

För vissa typer av informationssystem tillhandahåller leverantören inte några antivirusprogram. Det kan bero på att utformningen av tekniken anses omöjliggöra angrepp av skadlig kod eller att funktionaliteten i informationssystemet inte kan upprätthållas om antivirusprogram körs. Det senare lyfts ofta fram när det gäller industriella informations- och styrsystem. Eftersom det inte går att utesluta att sådana informationssystem ändå drabbas av skadlig kod i någon form, ska organisationen vidta kompenserande åtgärder. Vid riskbedömningen av dessa informationssystem behöver organisationen omhänderta den högre risk som avsaknaden av antivirusskydd innebär. Detta påverkar utformningen av säkerhetsåtgärder såsom nätverkssegmentering, filtrering, behörighetstilldelning, säkerhetskonfigurering, övervakning och skydd av utrustning. Exempelvis är det lämpligt att placera sådana informationssystem i ett eller flera egna nätverkssegment med omfattande övervakning och strikt behörighetstilldelning.



4.13 Skydd av utrustning

4.13.1 Syfte

För att förhindra skador på och obehörig åtkomst till it-utrustning, behöver organisationen säkerställa ett tillräckligt fysiskt skydd.

4.13.2 Krav

Organisationen ska skydda den utrustning som informationssystem består av mot skador och obehörig åtkomst, genom att[123]

1. placera centrala servrar och central nätverksutrustning i särskilda it-utrymmen
2. tilldela behörighet till särskilda it-utrymmen restriktivt
3. identifiera och hantera behovet av övervakning och larm i särskilda it-utrymmen
4. registrera tillträde till särskilda it-utrymmen på individnivå och spara dokumentationen under fastställd bevarandetid
5. ha interna regler för hur mobil utrustning ska skyddas.

4.13.3 Fysiskt skydd

Skydd mot obehörig åtkomst och störningar i informationssystemens funktionalitet kan inte uppnås med enbart organisatoriska, administrativa och tekniska säkerhetsåtgärder, även fysiskt skydd behövs. Fysiskt skydd byggs upp med hjälp av säkerhetsåtgärder som

- yttre säkerhet, exempelvis stängsel, betongsuggor och påkörningsskydd, planteringar, belysning och ronderande väktare
- skalskydd som försvårar obehörigt tillträde till organisationens byggnad eller kontor, exempelvis lås på dörrar och fönster, bemannad reception, krav på behörighetsbrickor, passersystem och kameraövervakning
- larmsystem vid obehörigt tillträde[124]
- brandskydd, inklusive larm och utrymningsvägar
- sektorsindelning av inre miljö, exempelvis besökszon, zoner för ordinarie verksamhet, zoner för hantering av känslig information samt särskilda it-utrymmen
- skyddad förvaring, exempelvis säkerhetsskåp, brandskåp[125], låsbara utrymmen[126] och arkivutrymmen.

Åtgärderna behöver väljas och utformas utifrån organisationens behov. Arbetet med utformning och förvaltning av det fysiska skyddet leds och samordnas av organisationens säkerhetsorganisation. Ett vanligt arbetssätt är att CISO bidrar i arbetet genom att förmedla skyddsbehovet för information och informationssystemen så att fastighetsägaren kan införa säkerhetsåtgärder. Om lokalerna hyrs behöver organisationen reglera säkerhetsåtgärderna i avtal och ha en nära dialog med fastighetsägaren eller dennes representant om det fysiska skyddet.

4.13.4 Särskilda it-utrymmen

Med särskilda it-utrymmen avses här avgränsade it-utrymmen – datorhallar, datorrum, korskopplingsrum, skåp eller motsvarande – som är anpassade för enstaka skyddsvärd it-utrustning, en större mängd it-utrustning eller där organisationen placerar centrala servrar och centrala nätverksutrustning.

123. MSBFS 2020:7 4 kap. 21 § Myndigheten ska skydda den utrustning som informationssystem består av mot skador och obehörig åtkomst, genom att 1. placera centrala servrar och central nätverksutrustning i särskilda itutrymmen, 2. tilldela behörighet till särskilda it-utrymmen restriktivt, 3. identifiera och hantera behovet av övervakning och larm i särskilda it-utrymmen, 4. registrera tillträde till särskilda it-utrymmen på individnivå och spara dokumentationen under fastställd bevarandetid, och 5. ha interna regler för hur mobil utrustning ska skyddas.

124. I Svenska stöldskyddsföreningens (SSF) standard SSF 130 beskrivs fyra larmklasser utifrån skyddsbehov.

125. Vid förvaring av säkerhetskopior är det viktigt att använda skåp som är brandklassade enligt standarden SS-EN 1047-1 som är lämpliga för sådan användning, exempelvis S60 DIS eller S120 DIS.

126. 123 Förvaringen ska vara inbrottsklassad, exempelvis enligt kraven i SSF 3492.

Var ett särskilt it-utrymme placeras i en byggnad och hur skyddet för det utformas behöver vara väl genomtänkt för att kunna skydda it-utrustning som placerats där mot skador och obehörig åtkomst. Vid utformning av särskilda it-utrymmen behöver organisationen minst identifiera och hantera risker för

- brand och översvämning, i och utanför det särskilda it-utrymmet samt i närområdet
- störningar i el, fjärrkyla och ventilation
- skadegörelse och inbrott.

Organisationen ska säkerställa att it-utrustning som hanterar information som är central för att organisationen ska kunna bedriva sin verksamhet ges ett tillräckligt skydd mot skada och obehörig åtkomst. Sådana servrar, databaser, routrar, switchar och liknande ska därför placeras i särskilda it-utrymmen.

Organisationen ska alltid tilldela behörighet till dessa utrymmen restriktivt, registrera tillträdet på individnivå och spara dokumentationen under fastställd bevarandetid. Organisationen ska identifiera och hantera behovet av övervakning och larm i sina särskilda it-utrymmen och behöver dessutom, utifrån informationsklassning och riskbedömning, identifiera och hantera behovet av

- förstärkta väggar, dörrar, fönster och lås
- bevakning
- intern zonindelning och låsta skåp
- redundans i el, kommunikation och klimatbevarande åtgärder såsom ventilation och temperaturreglering
- brand och översvämningsskydd.

Vid utformningen av särskilda it-utrymmen och dess skydd behöver säkerhetsorganisationen inklusive CISO samverka med ansvariga för it-drift och fastighet.

4.13.5 Mobil utrustning

Mobil utrustning såsom bärbara klienter, mobiltelefoner och usb-minnen, behöver skydd främst mot obehörig åtkomst till information eller informationsförlust genom att enheten blivit stulen eller tappats bort[127]. Skyddet behöver ta höjd för att utrustningen ofta ska kunna användas för att hantera organisationens information utanför organisationens egna lokaler.

Organisationen ska ha interna regler för hur mobil utrustning ska skyddas. Reglerna behöver både omhänderta tekniska och administrativa säkerhetsåtgärder. Det är lämpligt att minst ställa krav på tekniska säkerhetsåtgärder såsom

- krypterad lagring
- säkerhetskonfigurering, exempelvis begränsa möjligheter att starta upp datorn från ett usb-minne
- flerfaktorsautentisering
- möjligheten att radera information på distans
- skärmlås och skärmskydd
- kvittens av mobil utrustning
- stöldskyddsmärkning[128] och eventuell fjärrlokalisering[129].

Säkerheten för mobil utrustning är även beroende av hur utrustningen hanteras av användarna utanför organisationens lokaler. Det är därför lämpligt att minst reglera

- i vilka situationer och miljöer som den mobila enheten får tas med (exempelvis resor eller hotellrum)
- i vilka situationer den mobila utrustningen får användas

127. Se även *Vägledning för säkrare hantering av mobila enheter*, MSB405 (juni 2012).

128. Avsikten med en stöldskyddsmärkning är att göra det svårare att sälja vidare stulen utrustning, eftersom märkningen gör att ursprunget inte går att utplåna. Därmed blir utrustningen mindre eftertraktad att stjäla.

129. Ett beslut om att införa fjärrlokalisering behöver föregås av riskbedömning och avstämning med organisationens dataskyddsombud.

- vilka usb-minnen och motsvarande som får anslutas till organisationens informationssystem
- hur den mobila utrustningen ska laddas på ett säkert sätt (exempelvis datablockerare)
- hur den mobila utrustningen får förvaras
- hur användaren ska bete sig för att minska risken för att obehöriga ser eller överhör information.

De interna reglerna behöver utformas utifrån organisationens informationsklassning och riskbedömning, samt anpassas till det sätt som organisationen bedriver sin verksamhet. Det kan exempelvis behövas regler om huruvida mobila enheter får tas med på utlandsresor. Sådana regler kan behöva se olika ut beroende på vilket land det gäller. Vissa länder kan ha rättslig reglering som ger deras rättsväsende befogenhet att beslagta utrustning, kräva att information kan kopieras och kräva att tillhandahålla koder eller nycklar för åtkomst till krypterad information. Ett sätt att hantera sådana reglering är att tillhandahålla särskilda reseutrustning där endast den information som behövs tas med.

4.13.6 Radera och kassera it-utrustning

Den information som finns på it-utrustning behöver raderas innan utrustningen lämnas in på service, återanvänds eller kasseras, för att obehöriga inte ska kunna ta del av organisationens information. Informationen kan raderas på olika sätt. Vilket sätt som är lämpligast beror på vilken sorts it-utrustning det är, om it-utrustningen ska återanvändas, hur informationen som behandlats i it-utrustningen klassats och vad riskbedömningen kommit fram till. Det är viktigt att identifiera all den it-utrustning där det går att hitta information. Det kan till exempel vara skrivare som har hårddiskar där det finns kvar utskriftsunderlag, telefoner med telefonlistor och mer avancerade skärmar som hanterar kalenderbokningar.

Om utrustningen ska återanvändas inom organisationen, behöver i regel all tidigare information raderas med hjälp av ett dataraderingsprogram. Dataraderingsprogrammen skriver över ursprunglig information med meningslös information innan utrustningen återanvänds. För viss it-utrustning, exempelvis hårddiskar av solid-state-typ[130], räcker inte dataraderingsprogram för att helt radera information. Organisationen behöver alltid överväga om it-utrustning som lagrat information som har behov av utökat skydd avseende konfidentialitet ska kasseras istället för att återanvändas.

För att säkerställa att information som finns på it-utrustning som ska kasseras inte går att återskapa, kan organisationen exempelvis använda förbränning, avmagnetisering eller mala sönder de delar av it-utrustningen som innehåller information. Det kan vara lämpligt att anlita en leverantör som är specialiserad på destruktion. Destruktionstjänster kan ofta erbjudas på plats hos organisationen, eller så får organisationens representant följa med till destruktionsanläggningen för att verifiera att destruktionen sker på ett säkert sätt.

Säkerställ i avtal att organisationen även kan radera information som behandlats i utrustning som tillhör en leverantör (till exempel genom lån, hyra eller leasing), samt vid behov även kunna ställa krav på att utrustningen kasseras på ett säkert sätt när utrustningen återtas.

130. Lagringsmedia som inte behöver elförsörjning för att behålla information intakt.

4.14 Redundans och återställning

4.14.1 Syfte

För att vid incidenter och avvikelser kunna bedriva sin verksamhet utan mer störning än vad som kan accepteras behöver organisationen säkerställa tillräcklig redundans och förmåga till återställning av informationssystem i it-miljön.

4.14.2 Krav

Organisationen ska, för att säkerställa tillgänglighet till information och informationssystem vid incidenter och avvikelser,[131]

1. ha interna regler för återställning av produktionsmiljön i sin helhet och för enskilda informationssystem
2. öva återställning av informationssystem som är centrala för organisationens förmåga att bedriva sin verksamhet
3. placera centrala servrar och central nätverksutrustning som skapar redundant funktion i olika särskilda it-utrymmen.

Organisationen bör öva återställning regelbundet och utifrån identifierat behov av tillgänglighet.[132]

4.14.3 Återställning

Om verksamhetsinformation, konfiguration och programvara obehörigt eller av misstag förlorats eller förvanskats, behöver organisationen kunna återställa den. I vanliga fall återställs information som behandlas i digital form från en säkerhetskopia. De informationssystem som hanterar säkerhetskopior ger ofta stöd för återläsning av allt från enskilda filer till hela informationssystem. Även it-utrustning kan skadas, vilket kan medföra ett behov av att återställa hela eller delar av it-miljön. Detta förutsätter tillgång till ersättningsutrustning[133] och dokumentation över hur informationssystemen ska konfigureras.

Det är lämpligt att organisationens interna regler för återställning av produktionsmiljön i sin helhet innehåller anvisningar om prioriteringsordning mellan olika informationssystem utifrån funktion och beroenden. Det är också lämpligt att de interna reglerna, för respektive informationssystem, även beskriver vilka kompetenser som behövs för återställning och hur snabbt återställning behöver kunna ske, hur återställning ska övas samt var i dokumentationen för drift och förvaltning som information om återställning finns.

Öva återställning

Att återställa enskilda filer brukar inte vara komplicerat, men att återställa ett helt informationssystem från grunden kan vara svårare. Därför är det viktigt att öva. Efter en incident, exempelvis efter ett angrepp genom ett utpressningsprogram (ransomware) eller om it-utrustning gått sönder, kan det finnas behov att snabbt kunna återställa all information och ibland även informationssystemets konfiguration från grunden. Driftorganisationen ska öva återställning av informationssystem som är centrala för organisationens förmåga att bedriva sin verksamhet. Sådan övning bör ske regelbundet och utgå från organisationens behov av tillgänglighet till sin information och sina informationssystem. Ett lämpligt intervall för övning kan vara

131. MSBFS 2020:7 4 kap. 22 § Myndigheten ska, för att säkerställa tillgänglighet till information och informationssystem vid incidenter och avvikelser, 1. ha interna regler för återställning av produktionsmiljön i sin helhet och för enskilda informationssystem, 2. öva återställning av informationssystem som är centrala för myndighetens förmåga att utföra sitt uppdrag, och 3. placera centrala servrar och central nätverksutrustning som skapar redundant funktion i olika särskilda it-utrymmen.

132. Allmänt råd till MSBFS 2020:7 4 kap. 22 § Övning av återställning bör ske regelbundet och utifrån identifierat behov av tillgänglighet.

133. För att säkerställa tillgång till ersättningsutrustning behöver organisationen identifiera och hantera sina beroenden av externa leverantörer för att trygga sina digitala leveranskedjor.

mellan var tredje månad upp till en gång per år. Övningen behöver utformas för att så långt som möjligt motsvara ett realistiskt scenario utan att säkerheten i produktionsmiljön äventyras. I vissa fall kan hela eller delar av övningen utgöras av en skrivbordsövning. Det är en fördel om organisationens testmiljö är utformad och godkänd för att kunna öva hel eller delvis återställning av informationssystem.

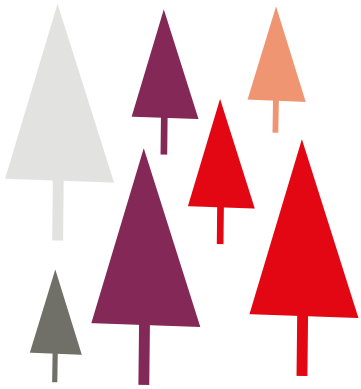
4.14.4 Redundans

Syftet med att ha redundans är att kunna upprätthålla tillgänglighet även om ett informationssystem eller en funktion i ett informationssystem slutar fungera. Detta uppnås genom att säkerställa tillgång till två eller flera, identiska eller olika, informationssystem eller funktioner som oberoende av varandra levererar samma resultat.

Organisationen ska placera centrala servrar och central nätverksutrustning som skapar redundant funktion i olika särskilda it-utrymmen. Därutöver behöver organisationen, utifrån informationsklassning och riskbedömning, identifiera och hantera ytterligare behov av redundanta funktioner som helt eller delvis tillhandahåller ursprunglig funktionalitet. För att möta olika behov av tillgänglighet kan redundans uppnås på olika sätt, exempelvis genom att:

- dela in personal som har samma kompetens i olika grupper så att om ena gruppen inte kan tjänstgöra på grund av sjukdomsutbrott kan den andra gruppen ta över
- spegla (kopiera) information så att samma information finns på fler än en hårddisk för att minska risken för informationsförlust vid skador på it-utrustning, exempelvis diskkrasch[134]
- använda olika mjukvara som utför samma funktion, alternativt samma mjukvara på olika informationssystem, vilket ska möjliggöra att funktionen kan tillhandahållas även om den ena mjukvaran eller ena informationssystemet drabbas av en incident, exempelvis skadlig kod
- installera en dubblett av ett informationssystem som är redo att omedelbart ta över funktionalitet om det primära informationssystemet drabbas av driftstörning
- förse särskilda it-utrymmen med dubblerade kraftaggregat vilka i sin tur är kopplade till olika säkringsgrupper för att minska konsekvenserna av störningar i elförsörjningen
- använda två skilda nätverksanslutningar för att minska risken att datakommunikationen slutar fungera vid nätverksavbrott
- etablera en reservdriftplats som möjliggör drift av organisationens informationssystem när ordinarie driftplats inte kan användas.

Olika åtgärder behöver ofta kombineras för att skapa tillräcklig redundans för organisationens it-miljö. Det är lämpligt att testa de redundanta funktionerna regelbundet och vid behov, exempelvis efter en förändring i it-miljön.



134. Redundant Array of Independent Disks, RAID. En uppsättning av lösningar där man kan använda flera hårddiskar för att minska risken för dataförlust om en av hårddiskarna går sönder. Den enklaste formen är att spegla (kopiera) informationen på den ena hårddisken till den andra (kallas RAID 1). En mer avancerad form är att använda sig av tre (eller fler) hårddiskar, där informationen sprids på alla hårddiskar (utom den sista) och där en checksumma skrivs in på den sista hårddisken (RAID 5). Om en av diskarna går sönder kan informationen återskapas av det som finns på de övriga tre hårddiskarna.

För myndigheter med särskilt ansvar för kris-beredskapen

5. För myndigheter med särskilt ansvar för krisberedskapen

5.1 Krav på högre säkerhet

5.1.1 Syfte

Beredskapsmyndigheter ska, enligt 18 § förordningen (2022:524) om statliga myndigheters beredskap, på grund av sitt uppdrag ha en högre säkerhet än vad kraven på säkerhetsåtgärder i kapitel 2–4 innebär.

5.1.2 Krav

Myndigheten ska skydda den utrustning som informationssystemet består av mot skador och obehörig åtkomst, genom att

1. använda flerfaktorsautentisering för informationssystem som är centrala för myndighetens förmåga att utföra sitt uppdrag[135]
2. använda realtidsövervakning för informationssystem som är centrala för myndighetens förmåga att utföra sitt uppdrag[136]
3. en gång per kvartal verifiera förmågan till återställning av dessa informationssystem[137]
4. en gång per kvartal kontrollera funktionen hos informationssystem som ska användas för informationsdelning under fredstida krissituationer.[138]

Myndigheten bör, som stöd för informationsdelning under fredstida krissituationer, använda[139]

1. Swedish Government Secure Intranet (SGSI)
2. Radiokommunikation för effektiv ledning (RAKEL).

135. MSBFS 2020:7 5 kap. 1 § De myndigheter som har ett särskilt ansvar för krisberedskapen enligt 10 § förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap ska, utöver vad som framgår av kapitel 2–4 i dessa föreskrifter, 1. använda flerfaktorsautentisering och realtidsövervakning för informationssystem som är centrala för myndighetens förmåga att utföra sitt uppdrag, och 2. en gång per kvartal verifiera förmågan till återställning av dessa system.
Anmärkning – ”Myndigheter som har ett särskilt ansvar för krisberedskapen” motsvaras av ”beredskapsmyndigheter” i förordning (2022:524) om statliga myndigheters beredskap.

136. MSBFS 2020:7 5 kap. 1 § De myndigheter som har ett särskilt ansvar för krisberedskapen enligt 10 § förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap ska, utöver vad som framgår av kapitel 2 – 4 i dessa föreskrifter, 1. använda flerfaktorsautentisering och realtidsövervakning för informationssystem som är centrala för myndighetens förmåga att utföra sitt uppdrag, och 2. en gång per kvartal verifiera förmågan till återställning av dessa system.
Anmärkning – ”Myndigheter som har ett särskilt ansvar för krisberedskapen” motsvaras av ”beredskapsmyndigheter” i förordning (2022:524) om statliga myndigheters beredskap.

137. MSBFS 2020:7 5 kap. 1 § De myndigheter som har ett särskilt ansvar för krisberedskapen enligt 10 § förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap ska, utöver vad som framgår av kapitel 2 – 4 i dessa föreskrifter, 1. använda flerfaktorsautentisering och realtidsövervakning för informationssystem som är centrala för myndighetens förmåga att utföra sitt uppdrag, och 2. en gång per kvartal verifiera förmågan till återställning av dessa system.
Anmärkning – ”Myndigheter som har ett särskilt ansvar för krisberedskapen” motsvaras av ”beredskapsmyndigheter” i förordning (2022:524) om statliga myndigheters beredskap.

138. MSBFS 2020:7 5 kap. 2 § Myndigheten ska, en gång per kvartal, kontrollera funktionen hos informationssystem som ska användas för informationsdelning under fredstida krissituationer.
Anmärkning – ”Myndigheter som har ett särskilt ansvar för krisberedskapen” motsvaras av ”beredskapsmyndigheter” i förordning (2022:524) om statliga myndigheters beredskap.

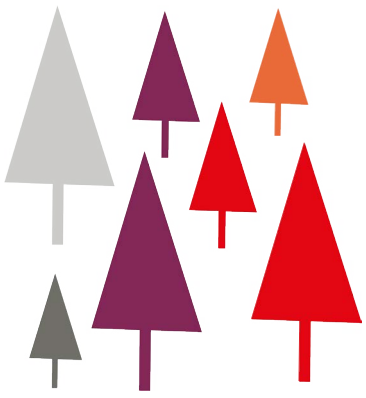
139. Allmänt råd till MSBFS 2020:7 5 kap. 2 § Myndigheten bör använda Swedish Government Secure Intranet (SGSI) och Radiokommunikation för effektiv ledning (RAKEL) som stöd för informationsdelning under fredstida krissituationer.
Anmärkning – ”Myndigheter som har ett särskilt ansvar för krisberedskapen” motsvaras av ”beredskapsmyndigheter” i förordning (2022:524) om statliga myndigheters beredskap.

5.1.3 Utökade krav på säkerhetsåtgärder

Beredskapsmyndigheterna ska ha god förmåga att motstå hot och risker, förebygga sårbarheter, hantera fredstida krissituationer och genomföra sina uppgifter vid höjd beredskap.[140] De ska på grund av sitt uppdrag vidta ytterligare säkerhetsåtgärder. Det handlar om att använda flerfaktorsautentisering och realtidsövervakning för de informationssystem som är centrala för myndighetens förmåga att utföra sitt uppdrag. Myndigheterna ska också minst en gång per kvartal verifiera förmågan att återställa dessa system.

När det gäller informationssystem som ska användas för informationsdelning under fredstida krissituationer behöver funktionen i dessa också kontrolleras minst en gång per kvartal. Som exempel på informationssystem som ska användas för informationsdelning under fredstida krissituationer kan nämnas informationssystem som möjliggör

- intern kommunikation som krävs för att kunna utföra sitt uppdrag
- kommunikation som krävs för samverkan med andra myndigheter eller andra organisationer
- informationsspridning till allmänheten.



Det är lämpligt att funktionen i ovan nämnda informationssystem kontrolleras genom att exempelvis

- verifiera att informationssystemen fungerar som de ska
- se till att rätt personer har behörighet och åtkomst till informationssystemet
- verifiera att det finns rätt kompetens för drift och förvaltning av informationssystemen
- öva personalens förmåga att använda informationssystemen
- verifiera att informationssystemen är rätt konfigurerade
- öva återställning av informationssystemen och kontrollera att behovet av redundanta funktioner kan uppfyllas, exempelvis genom genomföra skrivbordsövningar som gäller hanteringen av störningar i elförsörjningen eller nätverksavbrott
- kontrollera att informationssystemen är uppdaterade
- kontrollera att dokumentationen är tillräcklig för säker drift och förvaltning.

Kontrollerna planeras och genomförs lämpligtvis i samverkan mellan systemägare, myndighetens krisberedskapsorganisation och it-driftsorganisation. Kontrollen av funktioner i informationssystem som krävs för kommunikation med andra myndigheter eller andra organisationer planeras och genomförs med fördel tillsammans med andra berörda myndigheter eller organisationer.

140. 20 § förordning (2022:524) om statliga myndigheters beredskap. *Anmärkning – ”Myndigheter som har ett särskilt ansvar för krisberedskapen” motsvaras av ”beredskapsmyndigheter” i förordning (2022:524) om statliga myndigheters beredskap.*

5.1.4 Om SGSI och RAKEL

För att öka tillgången till kommunikationstjänster vid fredstida krissituationer tillhandahåller MSB idag två tjänster:

- **SGSI** (Swedish Government Secure Intranet)[141] är ett intranät, skiljt från internet, för säker och krypterad kommunikation mellan användare inom Sverige och i Europa. Nätet är utformat för att klara höga krav på tillgänglighet och driftsäkerhet. Med SGSI kan anslutna organisationer få åtkomst till andra anslutna tjänster, skicka skyddad e-post och ha skyddade videokonferenser. För att få ansluta till SGSI ställs krav på organisationens informationssäkerhetsarbete.
- **Rakel** (RAdioKommunikation för Effektiv Ledning)[142] är ett digitalt radiokommunikationssystem för trygg och säker kommunikation mellan personal i organisationer som bedriver samhällsviktig verksamhet. Rakel används bland annat av polis, räddningstjänst, sjukvård och Försvarsmakten, men också av ett stort antal andra myndigheter, energibolag, kollektivtrafikmyndigheter och organisationer som exempelvis hanterar farliga ämnen. Alla landets länsstyrelser, kommuner och regioner är anslutna till Rakel. Rakel är byggt för att klara svåra väderförhållanden och långa störningar i elförsörjningen. Rakel fungerar när andra system ligger nere, till exempel vid överbelastningar eller andra störningar i mobiltelefoni- och nätverkskommunikation.

Dessa tjänster kan användas för att nå ut med information när normala kommunikationskanaler inte fungerar.

141. Mer information om SGSI på MSB:s webbplats: https://www.msb.se/sv/verktyg--tjanster/sgsi/om-sgsi/ *Anmärkning – ”Myndigheter som har ett särskilt ansvar för krisberedskapen” motsvaras av ”beredskapsmyndigheter” i förordning (2022:524) om statliga myndigheters beredskap.*

142. Mer information om Rakel på MSB:s webbplats: https://www.msb.se/sv/verktyg--tjanster/rakel/.

Bilagor

Bilaga A – Referenser till ytterligare stöd och fördjupning

Standarder och övergripande vägledningar

Utöver det stöd för val och utformning av säkerhetsåtgärder som finns i standarderna SS-EN ISO/IEC 27001 och 27002[143] finns ytterligare standarder och vägledningar som kan användas, exempel på sådana ges nedan.

Standarder

- **ISO/IEC 27000-serien** – internationell standard för informationssäkerhet.
  - **SS-ISO/IEC 27004** Informationsteknik – säkerhetstekniker – styrning av informationssäkerhet – mätning
  - **SS-ISO/IEC 27005** Informationsteknik – säkerhetstekniker- riskhantering för informationssäkerhet
- **ISO/IEC 20000-serien** – internationell standard om tillhandahållande av it-tjänster
- **Information Technology Infrastructure Library** (ITIL)
- **IEC 62443-serien** – internationell standard för säkerhetsåtgärder inom industriella informations- och styrsystem (ICS/SCADA).
- **NIST SP 800-53** – amerikansk standard med vägledning och katalog över informations- och it-säkerhetsfunktioner. https://www.nist.gov/privacy-framework/nist-sp-800-53

Vägledningar

- **MSB:s metodstöd för systematiskt informationssäkerhetarbete.** https://www.informationssakerhet.se/metodstodet/
- **MSB, Vägledning till ökad säkerhet i industriella informations- och styrsystem.** https://rib.msb.se/dok.aspx?Tab=2&dokid=29984
- **MSB, Grundläggande säkerhet i cyberfysiska system: Vägledning.** https://rib.msb.se/dok.aspx?Tab=2&-dokid=29983
- **Säkerhetspolisen, Vägledning i Säkerhetsskydd – informationssäkerhet.** https://sakerhetspolisen.se/download/18.3752daf918b497112712b/1698133722307/Informationssa%CC%88kerhet_anpassad.pdf
- **Försvarsmaktens handbok hsäk/infosäk.** https://www.forsvarsmakten.se/siteassets/2-om-forsvarsmakten/dokument/handbocker/handbok-sak-infosak-andring-2.pdf
- **CIS CSC Top 20 Security controls** – vägledning med tjugo grundläggande informations- och it-säkerhetsåtgärder från Center for Internet Security (tidigare SANS Institute). https://www.cisecurity.org/controls
- **OWASP SAAM Software Assurance Maturity Model (SAMM).** https://owaspsamm.org/model/
- **NSM Grunnprinsipper for IKT-sikkerhet 2.0 – vägledning för it-säkerhet.** https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/

143. SS-EN ISO/IEC 27001:2017 & 2022 Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Krav och SS-EN ISO/IEC 27002:2017 & 2022 Informationsteknik – Säkerhetstekniker – Riktlinjer för informationssäkerhetsåtgärder.

- **BSI IT-Grundschutz** – tysk motsvarighet till MSB:s metodstöd för systematiskt informationssäkerhetsarbete (finns tillgänglig på engelska). https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html
- **ANSSI Recommendations to secure administration of IT Systems** – fransk vägledning för systemadministration (finns tillgänglig på engelska).
- **NCSC-UK Cyber Assessment Framework** – engelsk vägledning för införande av säkerhetsåtgärder i samhällsviktiga tjänster.
- **MITRE ATT&CK** – stöd för utformning av hotmodeller avseende antagonistiska hot mot it-miljöer.
- **NIST Cyber Security Framework** https://www.nist.gov/cyberframework

Fördjupat stöd till respektive kapitel

Här följer en lista med exempel på fördjupning inom vägledningens olika områden. Organisationen behöver göra en egen bedömning av om och hur fördjupningsdokumenten ska användas i det egna arbetet. Listan är inte uttömmande. Det kan finnas andra dokument som är mer relevanta för organisationens verksamhet.

Kapitel	Referenser
Kapitel 2	
2.1 Ansvar	MSB, *Ledningens roll inom informationssäkerhet, 2021* https://www.informationssakerhet.se/siteassets/metodstod-for-lis/ledningens-roll-inom-informationssakerhet---ett-stod-for-dig-med-en-ledande-funktion.pdf MSB:s metodstöd för systematiskt informationssäkerhetsarbete, *Utforma – Organisation* https://www.informationssakerhet.se/metodstodet/utforma/#organisation-anchor Finska transport- och kommunikationsverket TRAFICOM, *Cybersäkerhet och styrelsens ansvar*, 2020 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_SWEdigi_auk280120.pdf ACSC, *Information security manual- guidelines for cybersecurity roles*, 2022 https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-roles
2.2 Omvärldsbevakning	MSB:s metodstöd för systematiskt informationssäkerhetsarbete, *Analysera – Omvärldsanalys* https://www.informationssakerhet.se/metodstodet/analysera/#omv%C3%A4rldsanalys ENISA, ENISA *Cybersecurity threat landscape methodology*, 2022 https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology Se även källor med regelbundna uppdateringar likt CERT-SE:s *veckobrev* eller CISA *Alerts* https://www.cert.se/nyckelord/Veckobrev/ https://www.cisa.gov/uscert/ncas/alerts
2.3 Riskbedömning	MSB:s metodstöd för systematiskt informationssäkerhetsarbete, *Utforma – Om behovet av riskbedömning* https://www.informationssakerhet.se/metodstodet/utforma/#om-behovet-av-riskbed%C3%B6mning Samverkande myndigheter i det nationella cybersäkerhetscentret, *Cybersäkerhet i Sverige – Hot, metoder, brister och beroenden*, 2022 https://www.ncsc.se/siteassets/publikationer/ncsc-rappor-1-cybersakerhet-i-sverige-2022-hot-metoder-brister-och-beroenden.pdf National institute of standards and technology, NIST SP 800-30 – *Guide for conducting risk assessment*. Se särskilt kapitel 3. SS-ISO 31000:2018 *Riskhantering – Vägledning* SS-ISO/IEC 27005:2018 *Informationsteknik – Säkerhetstekniker – Riskhantering för informationssäkerhet*

Kapitel	Referenser
2.4 Dokumentation av it-miljön	MSB:s metodstöd för systematiskt informationssäkerhetsarbete, *Styrdokument* https://www.informationssakerhet.se/metodstodet/utforma/#styrdokument-anchor NSM, Grunnprinsipper for IKT-sikkerhet 2.0 – *Kartlegg styringsstrukturer, leveranser og understøttende systemer* https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/identifisere-og-kartlegge/kartlegg-styringsstrukturer-leveranser-og-understottende-systemer/ ASCS, Information security Manual – *Guidelines for security documentation*, 2022 https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-security-documentation
Kapitel 3	
3.1 Kravställning	MSB, *Upphandla informationssäkerhet – en vägledning*, 2018 https://www.msb.se/RibData/Filer/pdf/28742.pdf SS-ISO/IEC 27036-1:2014 Informationsteknik – Säkerhetstekniker – Informationssäkerhet vid leverantörsrelationer ENISA:s *Indispensable baseline security requirements for the procurement of secure ICT products and services*, 2017 https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and-services CSEC – Sveriges certifieringsorgan för IT-säkerhet https://www.fmv.se/verksamhet/ovrig-verksamhet/csec/
3.2 Kontroller	Säkerhetspolisen, *Vägledning i säkerhetsskydd – informationssäkerhet*, 2020. Avsnitt 7.7 om åtgärder som bör vidtas inför driftsättning samt 7.6 om funktionstester och säkerhetsgranskning https://sakerhetspolisen.se/download/18.310a187117da376c6601d43/1636446528314/Vagledning-Informationssakerhet_2020.pdf
3.3 Utvecklings- test och utbildningsmiljöer	NCSC-UK, *Secure development and deployment guideline* https://www.ncsc.gov.uk/collection/developers-collection/principles/secure-your-development-environment NCSC-UK, *Secure design and development* https://www.ncsc.gov.uk/section/advice-guidance/all-topics?allTopics=true&topics=secure%20design%20and%20development&sort=date%2Bdesc
Kapitel 4	
4.1 Nätverkssegment och filtrering (Segment och Zoner)	Samverkande myndigheter i det nationella cybersäkerhetscentret, Cybersäkerhet i Sverige – rekommenderade säkerhetsåtgärder (2020) Kapitel 8. Segmentera nätverken och filtrera trafiken mellan nätverken Se Säkerhetspolisens *Vägledning i säkerhetsskydd – informationssäkerhet*, 2020. Avsnitt 7.4 om Arkitektur NSA, *Segment networks and deploy application-aware defenses* https://media.defense.gov/2019/Sep/09/2002180325/-1/-1/0/Segment%20Networks%20and%20Deploy%20Application%20Aware%20Defenses%20-%20Copy.pdf MSB och FOI om *Fjärranslutningstekniker för industriella information- och styrsystem*, 2019 https://www.msb.se/contentassets/6840a9f762184a869b39954f670c8e77/ncs3---fjarranslutning.pdf

Kapitel	Referenser
4.2 Behörigheter och digitala identiteter	Säkerhetspolisen, *Vägledning i säkerhetsskydd – informationssäkerhet*, 2020. Avsnitt 7.4.5 om Identitets- och behörighetshantering NIST 800-63 Digital Identity Guidelines, avsnitt 5.1.1.2 “Memorized Secret Verifiers” NCSC-UK, *Introduction to identity and access management* https://www.ncsc.gov.uk/guidance/introduction-identity-and-access-management ANSSI, *Recommendations to secure administration of IT systems*, 2015, Avsnitt 7. Identification, authentication and administration privileges https://www.ssi.gouv.fr/guide/secure-admin-is/ NSA, *Defend privileges and accounts*, 2019 https://media.defense.gov/2019/Sep/09/2002180330/-1/-1/0/Defend%20Privileges%20and%20Accounts%20-%20Copy.pdf
4.3 Autenticering	ENISA, *Authentication methods* https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/authentication-methods NSCS-UK om behovet av en policy för autentiseringslösningar https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/enterprise-authentication-policy
4.4 Kryptering	Mer detaljerade beskrivning av DNSSEC-tjänster finns beskrivna i *Rekommendationer för införande av DNSSEC i kommuner och motsvarande verksamheter* utgiven 2014 av .SE/ Internetstiftelsen samt på https://internetstiftelsen.se/domaner/domannamnsbranschen/teknik/dnssec/ (hämtad 2020-08-25). Ett publikt verktyg att använda för att kontrollera konfiguration och status hos sina domäner och DNS-servrar är ZoneMaster (tidigare kallad DNSCheck), som tillhandahålls av Internetstiftelsen, på https://zonemaster.iis.se/. Kontrollera periodiskt att de registrerade domänerna är korrekt uppsatta gällande DNSSEC, t.ex. genom att använda ZoneMaster från Internetstiftelsen, https://zonemaster.iis.se/ NSM, *NSM cryptographic recommendations* https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/nsm-cryptographic-recommendations/ Informationssäkerhet.se om kryptolösningar https://www.informationssakerhet.se/kryptolosningar/
4.5 Säkerhetskonfigurering	Samverkande myndigheter i det nationella cybersäkerhetscentret, *Cybersäkerhet i Sverige – rekommenderade säkerhetsåtgärder*, 2020. Se avsnitt 4, 6 samt 7 Se också MITRE ATT&CK:s exempel på säkerhetskonfigureringar https://attack.mitre.org/mitigations/M0942/
4.6 Säkerhetstester och granskningar	MSB:s metodstöd för systematiskt informationssäkerhetsarbete, *Följ upp och förbättra* https://www.informationssakerhet.se/metodstodet/folja-upp-och-forbattra/#m%C3%A5luppfyllelse-av-informationss%C3%A4kerhetsm%C3%A5l-och-strategisk-inriktning ENISA, *Proactive detection – good practices gap analysis recommendations*, 2020. Kapitel 2 Good practices and gap analysis https://www.enisa.europa.eu/publications/proactive-detection-good-practices-gap-analysis-recommendations Se också NSCS-UK information om *Vulnerability scanning och Penetration testing* https://www.ncsc.gov.uk/guidance/vulnerability-scanning-tools-and-services https://www.ncsc.gov.uk/guidance/penetration-testing

Kapitel	Referenser
4.7 Ändringshantering, uppgradering och uppdatering Ändringshantering, uppgradering och uppdatering	Säkerhetspolisen, *Vägledning i säkerhetsskydd – informationssäkerhet*, 2020. Avsnitt 8.3–4 om Förändringshantering och Uppdatering ITIL, *Change management* https://www.itsm-docs.com/blogs/news/itil-change-management-process NCSC-UK, *Keeping devices and software up to date* https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/keeping-devices-and-software-up-to-date
4.8 Korrekt och spårbar tid	PTS, *Korrekt spårbar tid och takt* https://pts.se/sv/bransch/internet/Om-robust-kommunikation/robusthetshojande-atgarder/korrekt-och-sparbar-tid-och-takt/ Netnod, *Swedish distributed time service* https://www.netnod.se/swedish-distributed-time-service
4.9 Säkerhetskopiering	Samverkande myndigheter i det nationella cybersäkerhetscentret, *Cybersäkerhet i Sverige – rekommenderade säkerhetsåtgärder*, 2020. Kap. 3 Gör säkerhetskopior och testa om information går att läsa tillbaka. NSM, *Grunnprinsipper for IKT-sikkerhet 2.0 – Etabler evne til gjenoppretting av data* https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/beskytte-og-opprettholde/etabler-evne-til-gjenoppretting-av-data/ ACSC, *Backups* https://www.cyber.gov.au/backups
4.10 Säkerhetsloggning	NCSC-UK, *Logging and protective monitoring* https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/logging-and-protective-monitoring TRAFICOM, *Så här samlar du in och använder loggdata* https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/anvisningar-och-guider/sa-har-samlar-du-och-anvander-loggdata
4.11 Övervakning	MSB:s metodstöd för systematiskt informationssäkerhetsarbete, *följ upp och förbättra – övervaka och mäta* https://www.informationssakerhet.se/metodstodet/folja-upp-och-forbattra/#%C3%B6vervaka-och-m%C3%A4ta ENISA, *Proactive detection – measures and information sources*, 2020 https://www.enisa.europa.eu/publications/proactive-detection-measures-and-information-sources Informationssakerhet.se, Skyddspaket ICS/SCADA https://www.informationssakerhet.se/stod--vagledning/saker-it-infrastruktur/skyddspaket-icss-cada/
4.12 Skydd mot skadlig kod	ENISA, *Malware* https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/malware NCSC-UK *mitgating malware and ransomware* https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

Kapitel	Referenser
4.13 Skydd av utrustning	MSB, *Vägledning för fysisk informationssäkerhet i it-utrymmen*, 2013 (publ.nr: MSB629) https://www.msb.se/sv/publikationer/vagledning-for-fysisk-informationssakerhet-i-it-utrymmen/ Försvarsmaktens handbok H säk Fysisk säkerhet, utgiven 2015, inkluderar beskrivning av hur it-utrustning kan skyddas https://www.forsvarsmakten.se/siteassets/2-om-forsvarsmakten/dokument/handbocker/hand-bok-sakerhetstjanst-fysisk-sakerhet.pdf Säkerhetspolisen, *Vägledning i säkerhetsskydd – informationssäkerhet*, 2020. Avsnitt 8.6 om Avveckling
4.14 Redundans och återställning	NSM, *Håndbok i kartleggning og vurdering av avhengigheter* https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/handbok-i-kart-legging-og-vurdering-av-avhengigheter/prosess-og-metode/steg-2-vurdering-av-avhengighe-ter/vurdering-av-beskyttelse-og-resiliens/ FSPOS, *Regelverk för kontinuitet I it-verksamhet – Beskrivning av innehåll och tillämpning*, 2020 https://www.fspos.se/siteassets/fspos/rapporter/2020/regelverk-kontinuitet-it-verksamhet.pdf MSB:s metodstöd för systematiskt informationssäkerhetsarbete, *Utforma – Kontinuitetshantering för informationstillgångar* https://www.informationssakerhet.se/metodstodet/utforma/#kontinuitetshante-ring-f%C3%B6r-informationstillg%C3%A5ngar-anchor FOI om Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) https://www.foi.se/forskning/informationssakerhet/ncs3.html
Kapitel 5	
5.1 Krav på högre säkerhet	Säkerhetspolisens *Vägledning i säkerhetsskydd – informationssäkerhet, 2020 säkerhets-åtgärder som krävs vid högre säkerhetskrav* MSB, *Säkra kommunikationer* https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommu-nikationer/sakra-kommunikationer/

Bilaga B – koppling mellan vägledningens kapitel, föreskriftskrav samt avsnitt i SS-EN ISO/IEC 27002

Vägledningens kapitel	Föreskriftskrav MSBFS 2020:7	Avsnitt i SS-EN ISO/IEC 27002:2017	Avsnitt i SS-EN ISO/IEC 27002:2022
2 .1 Ansvar	2 kap 1 §	• 6.1.1 Informationssäkerhetsroller och ansvar • 8.1.2 Ägarskap av tillgångar • 18.2.3 Granskning av teknisk efterlevnad	• 5.2 Information security roles and responsibilities • 5.10 Acceptable use of information and other associated assets • 5.9 Inventory of information and other associated assets
2.2 Omvärldsbevakning	2 kap 2 §	• 6.1.4 Kontakt med särskilda intressegrupper • 12.6.1 Hantering av tekniska sårbarheter	• 5.5 Contact with authorities • 5.6 Contact with special interest groups • 5.7 Threat intelligence • 8.8 Management of technical vulnerabilities
2.3 Riskbedömning	2 kap 3 §	• 6.1.1 Informationssäkerhetsroller och ansvar	• 5.7 Threat intelligence • 5.13 Labelling of information • 5.2 Information security roles and responsibilities • 8.8 Management of technical vulnerabilities
2.4 Dokumentation av it-miljön	2 kap 4 §	• 8.1.1 Inventering av tillgångar • 8.2.1 Klassning av information	• 5.9 Inventory of information and other associated assets • 5.12 Classification of information • 5.13 Labelling of information • 5.37 Documented operating procedures • 8.8 Management of technical vulnerabilities
3.1 Kravställning	3 kap 1 §	• 14.1.1 Analys och specifikation av informationssäkerhetskrav	• 5.8 Information security in project management • 5.19 Information security in supplier relationships • 5.20 Addressing information security within supplier agreements • 5.21 Managing information security in the ICT supply chain • 5.22 Monitoring, review and change management of supplier services • 5.23 Information security for use of cloud services • 5.31 Legal, statutory, regulatory and contractual requirements • 8.26 Application security requirements • 8.28 Secure coding • 8.30 Outsourced development

Vägledningens kapitel	Föreskriftskrav MSBFS 2020:7	Avsnitt i SS-EN ISO/IEC 27002:2017	Avsnitt i SS-EN ISO/IEC 27002:2022
3.2 Kontroller	3 kap 2 §	• 12.1.1 Dokumenterade drifts-rutiner • 12.6.1 Hantering av tekniska sårbarheter • 13.1.2 Säkerhet hos nätverk-stjänster • 14.2.3 Teknisk granskning av tillämpningar efter ändringar i driftsmiljö • 14.2.8 Säkerhetstestning • 15.1.1 Informationssäkerhets-regler för leverantörsrelationer • 15.1.2 Hantering av säkerhet inom leverantörsavtal • 15.1.3 Försörjningskedja för informations- och kommuni-kationsteknologi • 18.2.3 Granskning av teknisk efterlevnad	• 5.22 Monitoring, review and change management of supplier services • 5.19 Information security in supplier relationships • 5.20 Addressing information security within supplier agre-ements • 5.21 Managing information security in the ICT supply chain • 5.36 Compliance with policies, rules and standards for information security • 5.37 Documented operating procedures • 8.8 Management of technical vulnerabilities • 8.21 Security of network services • 8.32 Change management • 8.29 Security testing in develop-ment and acceptance • 8.33 Test information
3.3 Utvecklings-test och utbild-ningsmiljöer	3 kap 3 – 4 §§	• 12.1.4 Separation av utveck-lings-, test och driftmiljöer • 14.2.6 Säker utvecklingsmiljö • 14.2.7 Outsourcad utveckling	• 8.25 Secure development life cycle • 8.27 Secure system architecture and engineering principles • 8.28 Secure coding • 8.30 Outsourced development • 8.31 Separation of development, test and production environments
4.1 Nätverks-segment och filtrering	4 kap 1 – 2 §§	• 13.1.3 Separation av nätverk • 13.1.1 Säkerhetsåtgärder för nätverk	• 6.7 Remote working • 8.20 Network security • 8.22 Segregation of networks • 8.23 Web filtering • 8.31 Separation of development, test and production environments • 5.14 Information transfer
4.2 Behörig-heter och digitala identiteter	4 kap 3 – 4 §§	• 6.1.2 Uppdelning av arbets-uppgifter • 9.1.1 Regler för styrning av åtkomst • 9.2.1 Registrering och avregist-rering av användare • 9.2.2 Tilldelning av användar-åtkomst • 9.2.5 Granskning av användares åtkomsträttigheter • 9.2.6 Borttagning eller justering av åtkomsträttigheter • 9.4.1 Begränsning av åtkomst till information • 9.2.3 Hantering av privilegie-rade åtkomsträttigheter • 9.4.4 Användning av privile-gierade verktygsprogram	• 5.3 Segregation of duties • 5.15 Access control • 5.16 Identity management • 5.18 Access rights • 8.2 Privileged access rights • 8.3 Information access restriction • 8.4 Access to source code • 8.18 Use of privileged utility programs

Vägledningens kapitel	Föreskriftskrav MSBFS 2020:7	Avsnitt i SS-EN ISO/IEC 27002:2017	Avsnitt i SS-EN ISO/IEC 27002:2022
4.3 Autenticering	4 kap 5 – 6 §§	• 9.4.2 Säkra inloggningsrutiner • 9.2.4 Hantering av användares konfidentiella autentiseringsinformation • 9.3.1 Användning av konfidentiell autentiseringsinformation • 9.4.3 System för lösenordshantering	• 5.17Authentication information • 8.5 Secure authentication
4.4 Kryptering	4 kap 7 – 9 §§	• 10.1.1 Regler för användning av kryptografiska säkerhetsåtgärder • 10.1.2 Nyckelhantering	• 8.24 Use of cryptography
4.5 Säkerhetskonfigurering	4 kap 10 §	• 12.1.1 Dokumenterade driftsrutiner • 12.2.1 Säkerhetsåtgärder mot skadlig kod • 12.5.1 Installation av program på driftsystem • 12.6.1 Hantering av tekniska sårbarheter • 12.6.2 Restriktioner för installation av program	• 5.37 Documented operating procedures • 8.7 Protection against malware • 8.8 Management of technical vulnerabilities • 8.9 Configuration management • 8.19 Installation of software on operational systems
4.6 Säkerhetstester och granskningar	4 kap 11 §	• 12.6.1 Hantering av tekniska sårbarheter • 14.2.8 Säkerhetstestning • 16.1.3 Rapportering av svagheter gällande informationssäkerhet	• 5.27 Learning from information security incidents • 5.35 Independent review of information security • 5.36 Compliance with policies, rules and standards for information security • 6.8 Information security event reporting • 8.8 Management of technical vulnerabilities • 8.29 Security testing in development and acceptance • 8.33 Test information • 8.34 Protection of information systems during audit testing
4.7 Ändringshantering, uppgradering och uppdatering	4 kap 12 §	• 12.1.2 Ändringshantering • 12.6.1 Hantering av tekniska sårbarheter • 14.2.4 Restriktioner för ändringar av programpaket	• 8.8 Management of technical vulnerabilities • 8.32 Change management • 8.19 Installation of software on operational systems
4.8 Korrekt och spårbar tid	4 kap 13 §	• 12.4.4 Synkronisering av tid	• 8.17 Clock synchronization
4.9 Säkerhetskopiering	4 kap 14 – 15 §§	• 12.3.1 Säkerhetskopior av information	• 5.33 Protection of records • 8.13 Information backup

Vägledningens kapitel	Föreskriftskrav MSBFS 2020:7	Avsnitt i SS-EN ISO/IEC 27002:2017	Avsnitt i SS-EN ISO/IEC 27002:2022
4.10 Säkerhetsloggning	4 kap 16 – 17 §§	• 12.4.1 Loggning av händelser • 12.4.3 Administratörs- och operatörsloggar • 12.4.2 Skydd av logginformation • 16.1.1 Ansvar och rutiner (Hantering av informationssäkerhetsincidenter och förbättringar)	• 5.24 Information security incident management planning and preparation • 5.28 Collection of evidence • 8.15 Logging
4.11 Övervakning	4 kap 18 – 19 §§	• 16.1.1 Ansvar och rutiner (Hantering av informationssäkerhetsincidenter och förbättringar) • 16.1.5 Hantering av informationssäkerhetsincidenter	• 5.24 Information security incident management planning and preparation • 5.26 • 5.28 Collection of evidence • 8.12 Data leakage prevention • 8.15 Logging • 8.16 Monitoring activites
4.12 Skydd mot skadlig kod	4 kap 20 §	• 12.2.1 Säkerhetsåtgärder mot skadlig kod	• 8.7 Protection against malware
4.13 Skydd av utrustning	4 kap 21 §	• 6.2.1 Regler för mobila enheter • 11.1.1 Fysiska säkerhetsavgränsningar • 11.1.2 Fysiska tillträdesbegränsningar • 11.1.3 Säkerställande av kontor, rum och anläggningar • 11.1.4 Skydd mot yttre och miljörelaterade hot • 11.1.5 Arbeta i säkra utrymmen • 11.2.1 Placering och skydd av utrustning • 11.2.6 Säkerhet för utrustning och tillgångar utanför organisationens lokaler • 11.2.7 Säker kassering eller återanvändning av utrustning	• 5.11 Return of assets • 7.1 Physical security perimeters • 7.2 Physical entry • 7.3 Security offices, rooms and facilities • 7.4 Physical security monitoring • 7.5 Protecting against physical and environmental threats • 7.6 Working in secure areas • 7.8 Equipment siting and protection • 7.9 Security of assets off-premises • 7.10 Storage media • 7.11 Supporting utilities • 7.13 Equipment maintenance • 7.14 Secure disposal or re-use of equipment • 8.1 User endpoint devices • 8.10 Information deletion
4.14 Redundans och återställning	4 kap 22 §	• 17.2.1 Tillgänglighet till informationsbehandlingsresurser	• 5.29 Information security during disruption • 8.14 Redundancy of information processing facilities • 5.30 ICT readiness for business continuity
5.1 Krav på högre säkerhet	5 kap 1 – 2 §§	• Se referenser för avsnitt 4.3, 4.6, 4.11 och 4.14	• 5.31 Legal, statutory, regulatory and contractual requirements

Myndigheten för
samhällsskydd
och beredskap

© Myndigheten för samhällsskydd och beredskap (MSB)
651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publ.nr MSB2032 – reviderad november 2023 ISBN 978-91-7927-446-7