



Myndigheten för
samhällsskydd
och beredskap

Strategi för samhällets informationssäkerhet

2010 – 2015



Förord

I dagens informationssamhälle bearbetar, lagrar, kommunicerar och mångfaldigar vi information i större mängder än någonsin tidigare. Informationshantering utförs manuellt och i allt högre grad med stöd av IT – som till exempel det publika nätverket Internet.

Informationssäkerhet handlar om att information ska skyddas utifrån krav på dess konfidentialitet, riktighet och tillgänglighet. Det gäller både hos enskilda personer och hos organisationer.

Informationssäkerhet är med andra ord en angelägenhet för alla.

Information och dess hantering ska hålla en hög kvalitet i Sverige. Samtliga aktörer i samhället ska ha relevanta kunskaper om informationssäkerhet och kunna känna tillit till information och dess hantering på alla nivåer i samhället.

Brister i informationshantering kan leda till att tilliten till aktuella tjänster och bakomliggande aktörer sjunker. Allvarliga och upprepade störningar kan leda till förtroendekriser, som också kan sprida sig till flera aktörer och tjänster och även till andra sektorer i samhället.

För att lyckas med utmaningarna inom informationssäkerhet är det viktigt att det i samhället finns en gemensam uppfattning om informationssäkerhetsarbetet: en strategi.

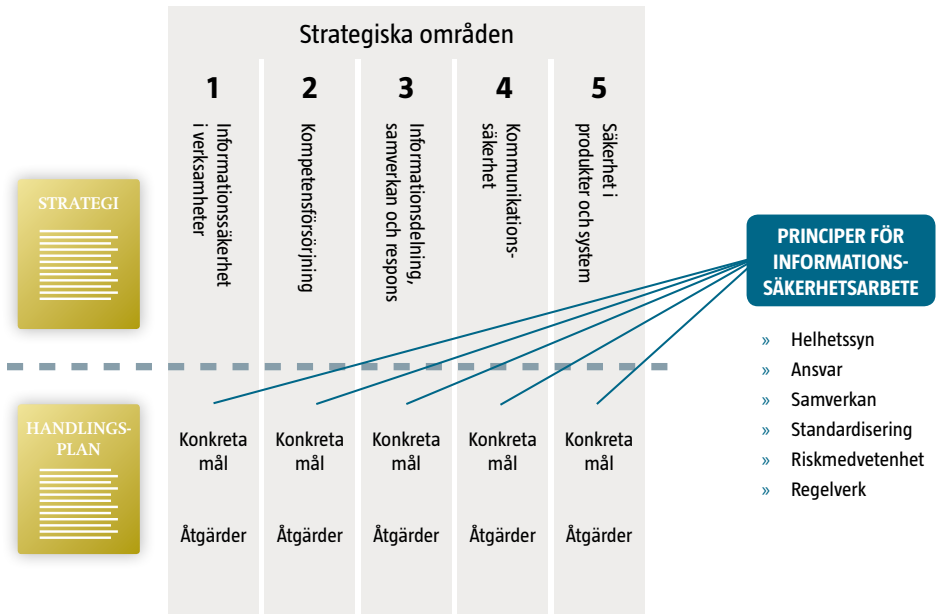
Mot denna bakgrund har MSB, i samverkan med Försvarmakten, Försvarets materielverk, Försvarets radioanstalt, Post- och telestyrelsen tagit fram denna strategi för samhällets informationssäkerhet. Utöver detta har Säkerhetspolisen lämnat synpunkter på föreliggande strategi.



Helena Lindberg, Generaldirektör

STRATEGISKA MÅL

- » Medborgares fri- och rättigheter samt personliga integritet.
- » Samhällets funktionalitet, effektivitet och kvalitet.
- » Samhällets brottsbekämpning.
- » Samhällets förmåga att förebygga och hantera allvarliga störningar och kriser.
- » Näringslivets tillväxt.
- » Medborgares och verksamheters kunskap om, och förtroende för informationshantering och IT-system.



Färdriktning för samhällets informationssäkerhet

Syftet med denna strategi är att ange långsiktiga målsättningar, färdriktningar och arbetssätt för informationssäkerhet i Sverige.

En mängd olika aktörer i samhället behöver en gemensam förståelse för informationssäkerhet, vad den syftar till och hur framtida säkerhetsinsatser ska inriktas och utformas. Främst berörda är de som arbetar med informationssäkerhet på olika nivåer, beslutsfattare i offentlig förvaltning och i näringslivet, de som arbetar med IT eller generell säkerhet, men också den enskilde medborgaren.

Strategin omfattar därmed hela samhället, det vill säga alla statliga myndigheter, kommuner och landsting, företag, organisationer och privatpersoner.

Denna strategi för samhällets informationssäkerhet anger tillsammans med den nationella handlingsplanen färdriktningen för Sveriges informationssäkerhet.

Strategin anger strategiska mål, strategiska områden samt principer för informationssäkerhetsarbete. Målen ska uppfyllas genom att arbeta inom de strategiska områdena på det sätt som principerna uttrycker.

I den nationella handlingsplanen återfinns de strategiska områdena i form av kapitel, som innehåller konkreta mål och åtgärder.

Strategin förvaltas av MSB. Tillsammans med berörda myndigheter kommer MSB att uppdatera strategin minst vart sjätte år.

*Informationssäkerhet är en
stödande verksamhet för att
öka kvaliteten hos samhällets
funktioner*

Strategiska mål

Informationssäkerhet är en stödjande verksamhet för att öka kvaliteten hos samhällets funktioner. Ytterst handlar det om att slå vakt om väsentliga värden och mål i samhället, som demokrati, personlig integritet, tillväxt samt ekonomisk och politisk stabilitet.

Den omfattande IT-användningen i samhället innebär att informationssäkerhet ibland också är en förutsättning för att nya företeelser i samhället som till exempel e-förvaltning ska kunna fungera.

Målet är att uppnå en god informationssäkerhet i samhället som främjar:

- medborgares fri- och rättigheter samt personliga integritet
- samhällets funktionalitet, effektivitet och kvalitet
- samhällets brottsbekämpning
- samhällets förmåga att förebygga och hantera allvarliga störningar och kriser
- näringslivets tillväxt
- medborgares och verksamheters kunskap om, och förtroende för informationshantering och IT-system

Strategiska områden

1. Informationssäkerhet i verksamheter
2. Kompetensförsörjning
3. Informationsdelning, samverkan och respons
4. Kommunikationssäkerhet
5. Säkerhet i produkter och system

1. Informationssäkerhet i verksamheter

Informationshantering sker i alla delar av samhället och samhällets informationsssäkerhet är följaktligen beroende av ett stort antal aktörer. Statliga myndigheter, kommuner, landsting, företag och andra organisationer har olika förutsättningar, och därmed olika behov och krav på informationsssäkerhet.

Verksamheter hanterar information som är mer eller mindre konfidentiell, riktighets- och tillgänglighetskritisk. Att ha en god informationsssäkerhet är en viktig intern fråga för de flesta verksamheter för att nå upp till deras kvalitets- och effektivitetskrav. Samtidigt kan informationsssäkerhet inte betraktas som enbart en verksamhetsintern angelägenhet. Flöden av tjänster och produkter sker i flera led, och bristande informationsssäkerhet kan därför få följdverkningar långt utanför den egna verksamhetens gränser.

Informationssäkerhet handlar om verksamhetens kvalitet. Att förbättra informationsssäkerheten innebär inte enbart att tillmötesgå externa krav, utan att förbättra verksamheten i sig. Att ha en god informationsssäkerhet ska därför ses som en kvalitetsaspekt, ett sätt att uppnå god intern kontroll, ordning och reda. En god informationsssäkerhet utgör också en förutsättning för en rad olika IT-baserade tjänster som i sig kan vara kostnadsbesparande eller inkomstbringande för verksamheten.

2. Kompetensförsörjning

Kunskaper om riskerna med IT och elektronisk kommunikation via exempelvis Internet måste läras in tidigt och vara en integrerad och naturlig del av den första IT-användningen. Därefter ska den följa med under hela skolgången och finnas med i högre utbildningar, inte minst som en integrerad del i utbildningar som leder till yrken med betydande inslag av informationshantering.

I många verksamheter är den mänskliga faktorn kritisk. Stora incidentkostnader kan härledas till brister i medvetenhet och kompetens hos ledning, användare och IT-personal. I olika verksamheter behövs olika typer av kunskap i en mängd olika roller. Det är människor som utvecklar, installerar, konfigurerar och använder tekniska system. Det är människor som formulerar, kommunicerar och efterföljer administrativa system. En särskilt viktig grupp ur ett informationssäkerhetsperspektiv är organisationsledningar, eftersom det är de som i slutändan ansvarar för verksamhetens kvalitet och säkerhet samt beslutar om skyddsåtgärder.

Ett så mångfacetterat område som informationssäkerhet behöver studeras djupare. Forskning och forskarutbildning är nödvändig för att upprätthålla såväl en generell kunskap som spetskompetens inom området. En nationell forskning och forskarutbildning förbättrar dessutom lärarkompetensen inom området, från grundskola till högskolor och universitet.



3. Informationsdelning, samverkan och respons

Att dela och sprida information är viktigt för att ta till vara och sprida kunskap och erfarenhet inom informationssäkerhetsområdet. Sådana kunskaper och erfarenheter återfinns överallt i samhället; både inom offentlig och privat sektor.

Det är därför viktigt att det finns väl fungerande nätverk inom och mellan den privata och offentliga sfären. Detta är särskilt tydligt när det gäller den kritiska svenska informationsinfrastrukturen som återfinns i såväl offentlig som privat ägo, och både offentlig sektor och näringsliv kan ha nytta av ett gott erfarenhetsutbyte.

En global värld med gränslösa hotbilder kräver även internationell samverkan. Sverige bör aktivt medverka i internationella samarbeten på flera plan: inom EU, med de nordiska länderna och med enskilda stater.

IT-baserade störningar och angrepp sprider sig inte sällan över organisationsgränser med hög hastighet. Samhället behöver ha en god förmåga att förebygga dessa och, om de ändå inträffar, kunna hantera sådana händelser på ett bra sätt.

Den traditionella brottsligheten som bedrägeri, utpressning, förtal och sabotage finns i dag även på Internet. Det är ett hot mot samhället, och dessa nya former av brottslighet måste motverkas.

4. Kommunikationssäkerhet

Informationshantering sker regelmässigt mellan fler aktörer vilket ställer krav på säker kommunikation över tele- och datanät. Exempelvis är Internet bärare av en stor andel av vårt informationsflöde.

Det är viktigt i detta sammanhang att ha robusta kritiska funktioner i infrastrukturen för elektronisk kommunikation och att det finns säkra kryptografiska funktioner och signalskydd. För förtroendefullt informationsutbyte är det också nödvändigt att elektroniska tjänster bygger på väl fungerande och säkra system.

5. Säkerhet i produkter och system

Långsiktig försörjning av säkra IT-produkter ställer krav på formella ramverk för evaluering och certifiering av säkerhetsegenskaper. Sådana ramverk bör vara nationellt och internationellt accepterade.

Inom området industriella kontrollsystem för samhällsviktiga verksamheter – exempelvis el- och vattendistribution samt spår-bunden trafik och petrokemisk industri – används IT-system för att styra och övervaka de centrala fysiska processerna. Det är av stor vikt att dessa system har en hög säkerhet.



Principer för informationssäkerhetsarbete

Helhetssyn

Ansvar

Samverkan

Standardisering

Riskmedvetenhet

Regelverk

Helhetssyn

För att informationshantering och IT-användning i samhället ska kunna utvecklas på ett tryggt och säkert sätt krävs att alla aktörer har en helhetssyn på informationssäkerhet. Informationssäkerhet är ett komplext och gränsöverskridande område som spänner över bland annat teknik, administration, ekonomi och juridik. När vi arbetar för att förbättra informationssäkerheten i organisationer och på nationell nivå, måste vi ta hänsyn till flera perspektiv.

Informationssäkerhet ska vara en självklar och integrerad del i allt IT- och informationsrelaterat arbete på alla nivåer i samhället; inom och mellan organisationer samt inom och mellan samhällets olika sektorer.

Säkerhetsåtgärder bör både syfta till att skapa en mer robust informationshantering vid samhällets normaltillstånd och att hantera mer allvarliga störningar och kriser. En väl fungerande vardags-säkerhet är ofta likställd med att vara förberedd på allvarligare händelser. Exempelvis kan en god intern kontroll i verksamheter, kompetens inom informationssäkerhet samt informationsutbyte med andra ge en betryggande förmåga att hantera en kris.

Ansvar

Allt arbete med informationssäkerhet ska utgå från det i samhället reglerade ansvaret, exempelvis ansvarsprincipen. Den säger, att ”Den som har ansvar för en verksamhet under normala förhållanden också ska ha motsvarande ansvar vid en kris- eller krigssituation”.

Informationssäkerhetsansvaret följer normalt verksamhetsansvaret och ska vara otvetydigt. För att bedriva ett framgångsrikt informationssäkerhetsarbete måste det vara tydligt vem eller vilka som har ansvar för det. Detta gäller på alla nivåer – både inom organisationer och i samhället i stort.

Samverkan

Informationssäkerhetens komplexitet, gränsöverskridande karaktär och snabba utvecklingstakt kräver en effektiv samverkan. En god samverkan kring informationssäkerhet i samhället är viktigt under ett normaltillstånd, men också en nödvändighet för att kunna skapa en god operativ förmåga att hantera allvarliga störningar. Det handlar om samverkan mellan olika aktörer i Sverige, som statliga myndigheter, kommuner och landsting, näringsliv och intresseorganisationer, men också om internationell samverkan.

Sverige bör vara aktivt i EU och internationellt, inom exempelvis forskning och teknikutveckling, och påverka utformningen av regelverk och andra styrmedel. Förutom samarbetet genom EU behövs också en samverkan med en rad andra länder, till exempel våra nordiska grannländer.



Standardisering

Standarder som gynnar informationssäkerhet bör tillämpas eftersom de bygger på erfarenhet och tar tillvara redan gjorda landvinningar. På så sätt kan en högre säkerhet uppnås och onödiga misstag undvikas. Standardisering förenklar utbildning och förbättrar alltså även kompetenser. Standarder ökar också transparensen mellan organisationer vilket gör det lättare att ställa krav och bedöma produkter, system och hela verksamheter.

Riskmedvetenhet

Det krävs resurser för att kunna nå en säker och trygg informationshantering i samhället. Säkerhetsaspekter ska inte ses som en ytterligare kostnadspost, utan som en självklar investering för att uppnå avsedd funktion och kvalitet.

Investeringar för att bygga in och förbättra säkerhet bör alltid jämföras med vad det kan kosta att inte göra detta. Målet är att hitta rätt säkerhetsnivåer och att de ansvariga är medvetna om vilka risker som finns, för att aktivt kunna besluta om att eliminera, reducera eller acceptera dessa risker. En sådan riskmedvetenhet utgör grunden för effektiva informationssäkerhetsinvesteringar.

Investeringar i informationshantering görs inte sällan i syfte att effektivisera och rationalisera tjänster i samhället. Det är därför rimligt att man satsar en del av besparingarna på att uppnå kvalitet och robusthet genom ökade säkerhetsinsatser.

Regelverk

En förutsättning för en god informationssäkerhet i samhället är att det finns regler som ligger i linje med modern informationshantering. Detta gäller för både verksamhetsnivå och samhällsnivå. Regelverk bör vara tydliga, kommunicerbara och, om så är möjligt, teknikerberoende för att fungera över tid. De bör heller inte verka konkurrensbegränsande.

MSB:s kontaktpersoner:

Richard Oehme

E-post: richard.oehme@msb.se

Per Oscarson

E-post: per.oscarson@msb.se

Wiggo Öberg

E-post: wiggo.oberg@msb.se

Myndigheten för samhällsskydd och beredskap (MSB)

651 81 Karlstad Tel 0771-240 240 www.msb.se

Publ.nr MSB 0171-10 ISBN 978-91-7383-081-2