

**MOTIVERINGSPROMEMORIA OM STATSRÅDETS PRINCIPBESLUT OM EN
NATIONELL INFORMATIONSSÄKERHETSSTRATEGI ”Trygg vardag i
informationssamhället – Inte med tur utan med kunskap”**

Bakgrunden för strategin

I den nationella informationssamhällsutvecklingen lever vi nu en fas där data- och kommunikationsteknologin som tidigare var en fristående verksamhetssektor har blivit en del av medborgarnas vardag. I vardagens informationssamhälle (det s.k. ubicompsamhället) blir de datatekniska lösningarna mångsidigare och blir med tanke på användarna en fast del av människornas och företagens normala verksamhet. På grund av detta är det väsentligt att medborgarna kan använda informationssamhällets tjänster enkelt och att de elektroniska tjänsterna upplevs som pålitliga. Alla har ansvar för detta och därför är kunnandet i och medvetenheten om informationssäkerheten väsentligt viktiga. Målet är en trygg vardag i informationssamhället, inte med tur utan med kunskap. Förtroendefullheten, integriteten och användbarheten av uppgifterna har en stor betydelse för vardagens informationssamhälle.

Statsrådets föregående principbeslut om en nationell strategi för informationssäkerheten antogs 2003 och den samlade på ett nästan unikt sätt aktörerna från den privata och den offentliga sektorn runt samma bord. Först och främst lyfte strategin fram informationssäkerheten till ett betydande tema i den samhälleliga debatten. Vår syn på och vårt förstånd om informationssäkerheten har vuxit och Finland har kunnat representera de främsta länderna i ärenden som gäller informationssäkerheten såväl i EU som på internationella forum. Informationssäkerhetsstrategin var den första i Europa och eventuellt den första i världen. Mandattiden för informationssäkerhetsstrategin och den nationella delegationen för informationssäkerhet som samordnade genomförandet av strategin löpte ut våren 2007. Arbetet utfördes mycket betydligt som samarbete mellan den offentliga och den privata sektorn. De största resultaten som informationssäkerhetsstrategin gav var en ökad kunskap om informationssäkerheten bl.a. med införande av en nationell informationssäkerhetsdag, bildande av en nationell lägesbild av informationssäkerheten och resultaten av utvecklingsprogrammet ”Förtroende och informationssäkerhet i elektroniska tjänster”.

Omvärlden förändras snabbt och därför finns det behov att uppdatera informationssäkerhetsstrategin. Det är viktigt att få en realistisk och fokuserad nationell informationssäkerhetsstrategi med några prioriterade mål. Informationssäkerheten ska göras till en väsentlig och naturlig del av det vardagliga livet. Därför skrivs strategin inte bara för sakkunniga inom branschen. Med strategin reagerar vi inte bara passivt utan vi påverkar aktivt framtiden, vågar vara aktiva och

modiga föregångare. Strategin påverkar inte ansvarsfördelningen som anknyter till informationssäkerheten och inte heller de existerande organisationsstrukturerna. Strategin och statsförvaltningens riktlinjer för informationssäkerheten som samordnas av finansministeriet stöder varandra. Strategin länkar också till det antagna handlingsprogrammet för den inre säkerheten.

Den nationella informationssäkerhetsstrategin är en central del av regeringens informationssamhällspolitik. I handlingsprogrammet för delegationen för vardagens informationssamhälle för 2008–2011 talas det om informationssäkerheten. Strategin skapades under 2008 i informationssäkerhetsgruppen som lyder under delegationen för vardagens informationssamhälle med hjälp av flera verkstäder, möten och en intervjurunda. Gruppen för informationssäkerheten i vardagens informationssamhälle har till uppgift att främja informationssäkerheten i informationssamhället, följa utvecklingen i fråga om informationssäkerhet och att ta initiativ till att förbättra informationssäkerheten.

Strategiska mål

Med hjälp av den nationella informationssäkerhetsstrategin strävas det efter att skapa finländarna (medborgare, företag, myndigheter och andra aktörer) en trygg vardag i informationssamhället. Strategin har den visionen att medborgarna och företagen kan lita på att deras uppgifter är säkra både på data- och kommunikationsnäten och i tjänsterna som hör till dem. Det allmänna informationssäkerhetskunnandet ska vara på en hög nivå och olika parter i samhället samarbetar skarvlöst i syfte att främja informationssäkerheten. Finland är föregångarlandet i informationssäkerheten i världen 2015.

Tyngdpunkt 1: Baskunskaper i vardagens informationssamhälle

Informationssäkerheten är också annat än teknik. I vardagens informationssamhälle behöver medborgarna nya baskunskaper som de inte tidigare har haft. Informationssäkerheten ses fortfarande för mycket som fristående del från utvecklingen av kommunikations- och datasystemen. Det finns olika slag av information och därför bör man fundera över vilka risker som hör samman med skyddet av information. Förtroendet för informationssamhället uppstår när både användarna och leverantörerna av tjänsterna förstår sitt ansvar, sina rättigheter och sina skyldigheter. Det är också viktigt att utveckla kunnandet hos dem som har hand om företagens och företagets informationssäkerhet.

Tyngdpunkt 2: Riskhantering som anknyter till uppgifterna och funktionssäkerhet

Elektroniska tjänster och den elektroniska ärendehanteringens bildar en allt centralare del av servicesystemet såväl på den offentliga som på den privata sektorn. Samtidigt gör beroendet av datatekniken tjänsterna sårbarare än tidigare. Medborgarna måste kunna lita på att det är tryggt att använda systemen och att konfidentiella uppgifter inte kommer i fel händer. Medborgarna och företagen måste garanteras tillräckligt stöd från myndigheterna om informationssäkerheten har kränkts t.ex. genom identitetsstöld.

Tyngdpunkt 3: Konkurrenskraft och internationellt nätverkssamarbete

Finland lever i en global informationsnätsekonomi och således riktas en betydande del av hoten och angreppen (bl.a. överbelastningsattacker) mot informationssäkerheten på oss utanför vårt lands gränser. Finland ska agera aktivt i det internationella myndighetssamarbetet för att nätbrottsligheten kan bekämpas på förhand och att skadorna som den orsakar kan minskas. Finland ska inte bara utveckla sin egen nationella reglering så att den blir enklare och mer förutsebar med tanke på företagen utan också sträva efter att aktivt påverka den internationella regleringen.

Åtgärder

1.1. Starkare medvetenhet om och kunnande i informationssäkerheten

En trygg verksamhet förutsätter baskunskaper av leverantörerna och användarna av tjänsterna. Med strategin försöker man säkerställa att medborgarna har sådant kunnande som kan likställas med 2000-talets medborgarfärdighet, m.a.o. kunskaper om informationssäkerheten när det handlar sig om användningen av nättjänsterna, förvaring av egna konfidentiella uppgifter (lösenord, kreditkort- och bankuppgifter, personuppgifter), identifieringen av allmänna fall av nätfiske samt översynen av att den egna terminalen är säker. Det bör utvecklas konkreta medel som kan stärka medborgarnas kunskaper och kunnande i informationssäkerheten.

1.2 Utbud av säkra elektroniska tjänster och säkerställande av förtroendefullheten

Målet är att göra de inhemska nättjänsterna så säkra som möjligt under tjänsternas hela livscykel (med början från planeringsfasen). På detta sätt blir informationssäkerheten en väsentlig del av tjänsternas kvalitet. Detta betyder i praktiken att informationssäkerhetsaspekterna beaktas också i samband med anskaffningsprocesserna och när serviceavtal ingås. Utvecklingen av informationssäkerheten får inte vara bara något som hör till IT-sakkunniga. Ledningens roll är ytterst viktig när informationssäkerheten integreras till en del av affärsverksamhets- och förvaltningsprocesser. Informationssäkerheten måste beaktas i utbildningen som hänför sig till hela tjänsteproduktionskedjan. Tjänsterna ska göras så att de är enkla, konkreta och lättförståeliga utan att ändå glömma skyddet av konfidentiella uppgifter. Enkelheten producerar i sig säkerhet.

2.1 Utveckling av riskhanteringen och funktionssäkerheten

Riskhanteringen utgör grunden för säkerställandet av informationssamhällets uppgifter och garanterar systemets funktionssäkerhet och kontinuiteten av företagens affärsverksamhet. Riskhanteringsaspekten ska alltid ingå i planeringen av nya produkter och tjänster. I företagen är riskhanteringen inte bara något som hör till it-sakkunniga utan den ska kunna integreras till en fast del av planeringen, ledningen och genomförandet av affärsverksamheten. Att skapa ett riskhanteringssystem för företagen hör till ledningen. Bedömning och minimering av riskerna hör till varje utvecklingsfas av tjänsterna. Strategin har till uppgift att främja användningen av

riskhanteringsförfaranden. Detta ska hända i skarvlöst samarbete med myndigheterna, företagen och medborgarna.

2.2 Tryggande av samhällets vitala funktioner i alla situationer

Samhällets beroende av data- och kommunikationssystemen är mycket genomgripande och blir allt djupare. Samtidigt kan ändå konkurrensen och strävan efter kostnadseffektiviteten minska säkerhetsinvesteringar inom användbarheten. En allt större utmaning i vardagens informationssamhälle blir funktionssäkerheten och riskhanteringen av de allt mer invecklade näten. Till och med styrningen av elektroniska apparater via internet (t.ex. att gatubelysningen och styrningen av trafikljusen överförs till internet) hänger samman med stora risker i störningssituationer. Med gemensamma övningar förbättras i normala förhållanden beredskapen för störningar och strävas efter att fortsätta verksamheten i undantagsförhållanden. Övningarna satsar på att skapa och testa samarbetsmodeller. Övningarna utvecklas så att de innehåller mer konkret verksamhet.

3.1 Att göra Finland mera lockande och att öka konkurrenskraften genom att öka förutsebarheten

Att regelverket är klart och kan förutses är en central faktor för företagen. Finland ska utveckla sin lagstiftning så att regleringen i frågor som gäller informationssäkerheten är så lätt som möjligt och samtidigt täckande. När lagstiftningen utvecklas ska myndigheterna kritiskt betrakta dess verkningar i företagens verksamhetsförutsättningar och medborgarnas/konsumenternas rättigheter (eventuella synpunkter på motstridigheter måste beaktas). Allt flera företag är mångnationella och verkar på globala marknader. Det som i praktiken har visat sig vara problematiskt är att de nationella bestämmelserna och verkställigheten av EU-direktiven i olika länder skiljer sig från varandra. Detta försvårar för sin del verksamhetsförutsättningarna också av de finländska företag som är verksamma i flera länder.

3.2 Skärpning av det förutseende och påverkande internationella samarbetet

En förutseende och påverkande internationell verksamhet behöver en god nationell samordning och prioritering av funktioner. Det är viktigt att det internationella påverkandet inleds i en tillräckligt tidig fas (t.ex. genom aktivt deltagande i beredande arbetsgrupper och inofficiella nätverk). Det är viktigt att kartlägga god internationell praxis och att kunna föra finländskt kunnande i informationssäkerheten till utlandet. Dessutom ska den finländska lagstiftningens och det finländska regelverkets reformvänlighet ”marknadsföras” tillräckligt i det internationella samarbetet. På detta sätt är det för Finland möjligt att påverka andra länders regleringspraxis på ett sätt som gynnar de finländska företagens verksamhet på globala marknader.

Framgång i det internationella samarbetet förutsätter också aktivt påverkande i riktlinjerna för EU:s informationssamhällspolitik och i de internationella organisationernas riktlinjer för informationssäkerheten. Att inrätta en fungerande och resultatrik NCSA-funktion (nationell myndighet för informationssäkerheten, National Communications Security Authority) som främjar Finlands deltagande i det internationella samarbetet och de finländska datateknikaktörernas deltagande i internationella anbuds-förfaranden. Rollen som myndigheten för

informationssäkerheten har i att främja internationellt samarbete ger synlighet för det finländska informationssäkerhetskunnandet med tanke på myndighets- och företagsvärlden.

Genomförande av strategin

Utgångspunkter

Enligt den nuvarande arbetsfördelningen hör informationssäkerheten och utvecklingen av den enligt den gällande lagstiftningen till flera aktörer; både till den privata sektorn och till den offentliga sektorn. I reglementet för statsrådet (262/2003, ändrat 1.1.2008) har nämnts arbetsfördelningen mellan ministerierna.

Organisering av genomförandet

Statsrådet bär helhetsansvaret för informationssäkerhetsstrategin och övervakar genomförandet av strategin och uppdaterar den efter behov. Gruppen för informationssäkerheten i vardagens informationssamhälle som tillsatts av kommunikationsministeriet stöder samordningen av åtgärderna som genomförandet av strategin kräver samt följer hur strategin verkställs. Gruppen för informationssäkerheten i vardagens informationssamhälle har flera aktörer från den privata sektorn och den offentliga sektorn. Arbetsgruppen ger årligen till statsrådet en berättelse om genomförandet av strategin och behovet att uppdatera den samt rapporterar till delegationen för vardagens informationssamhälle om hur arbetet framskrider.

Gruppen för informationssäkerheten i vardagens informationssamhälle inrättades den 31 augusti 2007 genom beslut av minister Suvi Lindén för tiden 1.9.2007–28.2.2011. Gruppen har till uppgift att främja informationssäkerheten i informationssamhället, följa utvecklingen av informationssäkerheten och att ta initiativ i syfte att förbättra informationssäkerheten. Gruppen behandlar stora frågor som gäller informationssäkerheten och som överskrider olika sektorer i ett nära samarbete med andra parter som främjar informationssäkerheten.

Ekonomiska och samhällliga verkningar

Målen som ställts i principbeslutet kan förverkligas inom ramen av rambesluten och de beslut som årligen fattas i samband med budgeten. Strategin ökar alla användarnas kunskap i och medvetenhet om informationssäkerheten. Strategin ökar och stärker det nationella samarbetet i fråga om informationssäkerheten.