Digital säkerhet inom den offentliga förvaltningen

Statsrådets principbeslut
UTKAST
24.1.2020

Sammandrag

Medborgare, företag och sammanslutningar ska kunna lita på att den offentliga förvaltningens tjänster är etiskt hållbara, stöder en öppen och transparent verksamhet och är säkra. Med säkerheten i den digitala verksamhetsmiljön, dvs. den digitala säkerheten, avses frågor som gäller riskhantering, kontinuitetshantering och beredskap, cybersäkerhet, informationssäkerhet och dataskydd. Målet för den digitala säkerheten är att inom referensramen för den övergripande säkerheten skydda medborgarna, sammanslutningarna och samhället mot de risker och hot som kan riktas mot personuppgifter och medborgarnas tjänster samt mot samhällets och myndigheternas processer, tjänster och informationsmaterial i en digital verksamhetsmiljö. Samtidigt möjliggör den digitala säkerheten utvecklandet av befintliga tjänster och även tjänster som utnyttjar ny teknik och deras säkerhet på 2020-talet.

Utifrån internationella bedömningar av digitaliseringen är Finland känt som en föregångare både när det gäller förutsättningarna för digitaliseringen i samhället1 och som tillhandahållare av digitala tjänster för medborgare och sammanslutningar2. I internationella bedömningar som gjorts av hanteringen av cybersäkerheten och beredskapen för den3 har Finland placerat sig nära toppländerna. Digitaliseringens snabba framfart samt hoten mot olaglig användning av uppgifter och påverkan med hjälp av felaktiga uppgifter har ökat samhällets sårbarhet och ställt nya krav på styrningen av den digitala säkerheten inom den offentliga förvaltningen och beaktandet av säkerhetsfaktorerna i ekosystem som består av olika aktörer. Därför är det motiverat att dra upp riktlinjer för utvecklingen av den digitala säkerheten.

I en internationell jämförelse granskades den digitala säkerheten i fråga om styrning, uppgifter, strukturer, risker och resurser i Nederländerna, Australien, Storbritannien, Israel, Sverige, Tyskland, Ryssland och Estland4. I jämförelsestaterna har man strävat efter att utveckla lagstiftningen så att den motsvarar de snabba förändringarna i den digitala verksamhetsmiljön. Ledningen av den digitala säkerheten koncentreras och ämbetsverk sammanförs till större helheter. Jämförelsen ger vid handen

[1] EU (2019) The Digital Economy and Society Index (DESI).
[2] United Nations (2018) E-Government Survey 2018, Gearing E-Government to Support Transformation Towards Sustainable and Resilient Societies. United Nations, Economic & Social Affairs.
[3] International Telecommunications Union (2019) Global Cybersecurity Index (GCI); e-Governance Academy (2019) National Cyber Security Index (NCSI).
[4] Internationell jämförelse av digital säkerhet, KPMG, januari 2020.

att Finland ska utvärdera ledningsstrukturerna, ansvaret och rollerna för den digitala säkerheten samt förnya dem så att de motsvarar den internationella utvecklingen.

I jämförelsestaterna betraktas den offentliga förvaltningen, näringslivet, högskolorna och forskningsinstituten samt medborgarna allmänt som aktiva aktörer inom den digitala säkerheten. Alla dessa samhällsaktörer ska ha en aktiv roll som aktörer inom den digitala säkerheten, och utvecklandet av färdigheterna inom den digitala säkerheten ska vara en strategisk prioritering i hela samhället. Förvaltningen, medborgarna och sammanslutningarna ska erbjudas stöd för identifierade störningar i den digitala säkerheten. Finland ska tydligt beskriva hoten mot den digitala säkerheten i en form som alla aktörer i samhället förstår.

I jämförelsestaterna ses den digitala infrastrukturen som en del av servicestrukturerna och den digitala säkerheten som en del av servicehelheten. Tjänsteleverantören ska svara mot kraven på digital säkerhet och garantera en trygg användning av tjänsten. I Finland ska det systematiskt förutsättas att internationella standarder för digital säkerhet tillämpas.

De utvecklingsprinciper som utarbetats utifrån en analys av nuläget för den digitala säkerheten inom den offentliga förvaltningen och utifrån den internationella jämförelsen är följande:

- Vi leder säkerheten i det digitala samhället tillsammans utifrån lägesinformation och riskbedömning.
- Vi planerar och följer upp effekterna av och kostnaderna för den digitala säkerheten inom den offentliga förvaltningen.
- Vi utvecklar medborgarnas och de anställdas förståelse för konsekvenserna av och ansvaret för riskerna i den digitala säkerheten.
- Vi främjar den digitala säkerheten i samarbete mellan den offentliga förvaltningen, sammanslutningarna och medborgarna.
- Vi påverkar den digitala säkerheten på EU-nivå och internationellt och utnyttjar resultaten av samarbetet.
- Vi förutsätter att tekniken och tjänsteproduktionen är säker.

De viktigaste tjänster som behöver utvecklas för den digitala säkerheten inom den offentliga förvaltningen i syfte att stödja verksamhetsprocesserna och tjänsterna är följande:

1) Nationell och internationell samarbetsmodell för digital säkerhet
2) Hantering av risker i samband med digital säkerhet
3) Gemensamma tjänster för kommunerna för främjande av den digitala säkerheten
4) Hantering av digital identitet
5) Utveckling av medborgarnas och de anställdas kompetens
6) Säker utveckling av autonoma och lärande system och tjänster
7) Bedömning av den digitala säkerheten hos tjänster och tjänsteproduktion
8) Skydd av den digitala infrastruktur som den offentliga förvaltningen behöver
9) Sakkunnigservice för den digitala säkerheten inom den offentliga förvaltningen

Samhällets verksamhet och tjänster samt samutnyttjandet av information baserar sig på ömsesidigt förtroende för säkerhetshanteringen. Säkerhetsproblem inom den offentliga förvaltningens digitala

tjänster kan undergräva medborgarnas och sammanslutningarnas förtroende för myndigheterna. Samhället måste därför satsa på att trygga digitala tjänster och funktioner på ett balanserat sätt jämfört med främjandet av digitaliseringen. De mål som sätts upp för utvecklingsprojekten för digital säkerhet ska gagna samhället och vara mätbara.