Svar på skriftligt spörsmål om autentisering av statsförvaltningens e-post

Till riksdagens talman

I det syfte som anges i 27 § i riksdagens arbetsordning har Ni, ärade talman, till den minister som saken gäller översänt följande skriftliga spörsmål SS 292/2020 rd undertecknat av Atte Harjanne (De gröna):

> *Hur avser regeringen sköta om uppdateringen av sekretessinställningarna för statsförvaltningens domännamn så att det inte är möjligt att använda dem på ett obehörigt sätt?*

Som svar på detta spörsmål anför jag följande:

De e-posttjänster som används inom statsförvaltningen är sådana gemensamma IT-tjänster som avses i 2 § i lagen om anordnande av statens gemensamma informations- och kommunikationstekniska tjänster (1226/2013, härefter TORI-lagen) och sådana kommunikationstekniska tjänster som avses i 1 § 2 mom. i statsförvaltningens förordning om anordnande av statens gemensamma informations- och kommunikationstekniska tjänster (1226/2019, härefter TORI-förordningen). På motsvarande sätt är e-posttjänsterna även sådana informations- och kommunikationstekniska tjänster som avses i lagen om verksamhet i den offentliga förvaltningens säkerhetsnät (10/2015, härefter TUVE-lagen) och sådana gemensamma kommunikationstekniska tjänster i säkerhetsnätet som avses i 3 § 2 mom. i statsrådets förordning (1109/2015, härefter TUVE-förordningen).

Statens center för informations- och kommunikationsteknik, Valtori, som fungerar inom Finansministeriets förvaltningsområde, tar fram och utvecklar statens gemensamma informations- och kommunikationstekniska tjänster (IKT-tjänster) i enlighet med TORI-lagen samt gemensamma IKT-tjänster i säkerhetsnätet i enlighet med TUVE-lagen. Valtori producerar själv en del av e-posttjänsterna men skaffar en del från externa tjänsteleverantörer, och till vissa delar administrerar Valtori de avtal som statens ämbetsverk har ingått med externa tjänsteleverantörer.

Finansministeriet har i uppdrag att förbereda frågor som gäller styrning av statens gemensamma IKT-tjänster liksom styrningen och tillsynen av den informations- och kommunikationstekniska aktionsberedskapen, övriga beredskapen och säkerheten i fråga om säkerhetsnätets verksamhet. I enlighet med TORI-lagen måste de tjänster som Valtori producerar uppfylla de krav som ställs på informationssäkerhet och beredskap. Informationshanteringsenheten ska kartlägga relevanta risker som är förenade med informationsbehandlingen och dimensionera informationssäkerhetsåtgärderna utifrån riskbedömningen såsom avses i 13 § i lagen om informationshantering inom den offentliga förvaltningen (906/2019). Till Valtoris grundläggande uppgifter hör alltså att även be-

döma de risker som knyter an till e-posttjänsterna och dimensionera informationssäkerhetsåtgärderna utifrån riskbedömningen. Att samarbeta med de myndigheter inom statsförvaltningen som använder tjänsterna är en viktig del av riskbedömningen. E-posttjänstens säkerhetsåtgärder har skrivits in i tjänstebeskrivningarna eller överenskommits på annat sätt med varje kund.

Finansministeriet bedömer att ett okontrollerat missbruk av statliga domännamn i e-posttrafik åtminstone i viss mån kan störa myndigheternas verksamhet och i hög grad verksamhetens trovärdighet. Samtidigt kan e-post överlag inte ses som en pålitlig och huvudsaklig kanal när det gäller myndighetskommunikation. Därför utvecklas myndigheternas kommunikationskanaler och digitala tjänster så att ärenden ska kunna skötas på ett säkert sätt. Rent allmänt tar den offentliga förvaltningen modell av till exempel banksektorns sätt att kommunicera med sina kunder. Kunden kan läsa sina viktigaste meddelanden och sköta ärenden i en separat och tillförlitlig tjänst som bygger på stark identifiering och ett krypterat informationssystem.

Finansministeriet, som ansvarar för styrningen av statens IKT-tjänster, bad Valtori ta fram en utredning om nuläget när det gäller e-postens domänautentisering och utvecklingsplaner. Av Valtoris utredning framgår att flera olika tekniker och en kombination av dessa har använts för e-postens domänautentisering i de e-posttjänster som statsförvaltningen använder. Dessa funktioner inkluderar bland annat SPF (Sender Policy Framwork) som ger domänägaren möjlighet att styra vilka e-postservrar som får skicka e-post från ett visst domännamn och DKIM (DomainKeys Identified Mail) som bygger på att avsändarens e-postserver signerar det utgående meddelandet med krypteringscertifikat. Detta krypteringscertifikat tillåter den server som tar emot e-postmeddelandet att fråga domännamnsservern om avsändaren av e-postmeddelandet är rätt part medan DMARC (Domain-based Message Authentication, Reporting and Conformance) har i uppgift att meddela den mottagande servern att meddelandet använder SPF- och/eller DKIM-funktioner och informera vad mottagaren ska göra med e-postmeddelandet om autentiseringen misslyckas.

De ovan nämnda tekniska funktionerna används bara i viss mån i de e-posttjänster som Valtori producerar och tillhandahåller. När det gäller utgående e-postmeddelanden är funktionerna tillgängliga i cirka 14–50 procent av domänerna, beroende på e-posttjänst. I bara en del av inkommande e-postmeddelanden har funktionerna aktiverats. Enligt uppgifter från Valtori och andra ämbetsverk pågår emellertid flera utvecklingsprojekt när det gäller statsförvaltningens e-posttjänster som handlar om att utreda och ta i bruk ovan nämnda tekniker, liksom kombinationer av dessa, för att autentisera e-postdomäner.

Finansministeriet konstaterar att ovan nämnda tekniska metoder för att autentisera domännamn är en liten men viktig del av statsförvaltningens alla förvaltningsåtgärder när det gäller informations- och cybersäkerheten. Finansministeriet kommer att förutsätta att Valtori fortsätter det pågående förbättringsarbetet med informations- och cybersäkerheten när det gäller statens gemensamma tjänster liksom följer upp hur det framskrider som en del av utvecklingen av statsförvaltningens informations- och cybersäkerhet. Finansieringen av förbättringsåtgärderna i samband med utvecklingen av informations- och cybersäkerheten kommer att planeras som en separat del av ett utvecklingsprogram och dessutom som en del av utvecklingen av statens gemensamma

Svar på skriftligt spörsmål SSS 292/2020 rd

IKT-tjänster i sin helhet. I syfte att minimera obehörig användning av statens domännamn i kommande e-postlösningar förutsätter Finansministeriet, utöver ovan nämnda åtgärder, att Valtori sammanställer en riskbedömning och en handlingsplan inklusive finansieringsbehov som en del av utvecklingsarbetet för varje e-posttjänst.

Helsingfors 12.5.2020

Kommunminister Sirpa Paatero