Svar på fråga 2020/21:3561 av Lars Hjälmered (M)
Inrapporterade it-incidenter

Lars Hjälmered har frågat mig om jag avser att vidta några åtgärder för att se över att skyldigheten att inrapportera it-incidenter fungerar som den ska och att alla med rapporteringsskyldighet lever upp till sitt uppdrag.

Rapportering av it-incidenter är viktig eftersom den ger information om hot och sårbarheter och underlag för att stärka förmågan att förebygga, upptäcka och hantera it-incidenter. It-incidenter utgör i sig ett hot mot de digitala grunder som Sveriges säkerhet, konkurrenskraft och välstånd vilar på. Rapporteringen av it-incidenter från såväl statliga myndigheter som leverantörer av samhällsviktiga och digitala tjänster, i enlighet med förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap respektive lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, är central. En förutsättning för att rapporteringen ska fungera är att statliga myndigheter och leverantörer av samhällsviktiga och digitala tjänster har rutiner och processer för identifiering och rapportering av it-incidenter. Mot bakgrund av detta gav därför regeringen i december 2020 ett antal myndigheter i uppdrag att redovisa detta.

Den granskning som Post- och telestyrelsen ska göra av hur leverantörer inom sektorn digital infrastruktur hanterar och rapporterar incidenter kan ge ytterligare underlag kring det potentiella mörkertalet i inrapporteringen. Den kan också säkerställa att leverantörerna har nödvändiga rutiner och processer för hantering och rapportering av säkerhetsincidenter.

Europeiska kommissionen har presenterat ett förslag till revidering av det EU-direktiv som lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster följer av. I förslaget finns bl.a. skärpta krav på incidentrapportering. Förhandlingar om förslaget pågår för närvarande inom EU.

Myndigheten för samhällsskydd och beredskap (MSB) inhämtar kontinuerligt information gällande sårbarheter, hot och risker och sprider den till både privata och offentliga aktörer. Av MSB:s reglerings­brev för 2021 framgår att myndigheten ska redovisa hur spridningen av råd och stöd i syfte att förebygga it-incidenter kan effektiviseras.

Målet med det nyinrättade nationella cybersäkerhetscentret är att stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot som utgör en av källorna till de it-incidenter som drabbar Sverige. Inom ramen för cybersäkerhetscentret ska även myndigheterna bl.a. koordinera arbetet för att förebygga, upptäcka och hantera cyberangrepp och andra it-incidenter samt förmedla råd och stöd avseende hot, sårbarheter och risker. Samverkan med privat och offentlig sektor utgör en central del av centrets uppdrag. Regeringen har en tät dialog med de ansvariga myndigheterna om verksamheten och den fortsatta inriktningen.

Regeringen kommer fortsatt att noggrant följa frågan om olika aktörers it-incidentrapportering och, om nödvändigt, vidta ytterligare åtgärder för att rapporteringen ska fungera tillfredsställande.

Stockholm den 8 september 2021

Mikael Damberg