Regeringskansliet

Fö2025/01117

Försvarsdepartementet
Ministern för civilt försvar

Till riksdagen

Svar på fråga 2024/25:1281 av Niels Paarup-Petersen (C)
Nationellt bug bounty-program

Niels Paarup-Petersen har frågat mig om jag tänker agera för att få till ett nationellt bug bounty-program för att stärka Sveriges cybersäkerhet och motståndskraften i den kritiska infrastrukturen.

Förmågan att hantera cyberhot och cyberangrepp som riktas mot kritisk infrastruktur är av fundamental betydelse för Sveriges säkerhet. Regeringen arbetar därför på bred front för att stärka skyddet av samhällskritiska system och för att öka beredskapen och förmågan att förhindra och hantera cyberhot.

Mot bakgrund av det försämrade säkerhetspolitiska läget i Sveriges närområde finns anledning att öka takten i det arbetet. Regeringen driver därför nu igenom en rad nya initiativ för att stärka Sveriges förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra IT-incidenter. Det handlar om förebyggande, strategiska och långsiktiga initiativ för att säkerställa att skyddet av kritisk infrastruktur är robust och

kontinuerligt anpassas utifrån behov och risker. Låt mig lista några exempel:

I mars i år beslutade regeringen om en ny nationell strategi för cybersäkerhet för åren 2025–2029. Strategin pekar ut regeringens inriktning för arbetet med Sveriges cybersäkerhet för kommande år och innehåller en rad konkreta mål som syftar till att stärka och effektivisera det nationella cybersäkerhetsarbetet.

I syfte att skapa ett mer ändamålsenligt och utåtriktat cybersäkerhetscenter har regeringen beslutat om att omstrukturera Nationellt cybersäkerhetscenter (NCSC). Från och med den 1 november 2024 leds centret av Försvarets radioanstalt (FRA). Satsningen speglas finansiellt genom regeringens beslut om att tillföra centret ytterligare 50 miljoner under 2025.

Regeringen har även tillskjutit substantiella medel för Sveriges Computer Security Incident Response Team (CERT-SE) vid Myndigheten för samhällsskydd och beredskap (MSB). Satsningen möjliggör ett mer effektivt stöd till samhällsaktörer för att förebygga, motstå och hantera cyberincidenter. De tillförda medlen möjliggör även stöd i arbetet med att omhänderta de operativa krav som ställs på Sverige genom NIS2-direktivet.

Vidare har regeringen uppdragit åt MSB att kartlägga kommunernas tekniska cybersäkerhetsförmåga. Målet med denna kartläggning är att identifiera kostnadseffektiva åtgärder som kommunerna själva kan genomföra, samt att stödja dem i att prioritera nödvändiga framtida investeringar inom cybersäkerhetsområdet.

Regeringen har alltså redan vidtagit ett antal åtgärder på området. Men vi fortsätter att noggrant följa omvärldsutvecklingen och de bedömningar som berörda myndigheter gör av säkerhetsläget. Vi överväger löpande behovet av ytterligare åtgärder på området och i det fall nya NCSC framgent föreslår initiativ i linje med ett så kallat bug bounty-program kommer ett sådant förslag noga beaktas.

Stockholm den 11 juli 2025

Carl-Oskar Bohlin