Regeringskansliet
Försvarsdepartementet

Remissvar - Slutbetänkande av cybersäkerhetsutredningen (SOU 2021:63)

Åklagarmyndigheten har ombetts att lämna synpunkter på delbetänkandet *Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem*.

Sammanfattning

Åklagarmyndigheten avstyrker betänkandets förslag i sin nuvarande utformning vad avser möjliga krav på statliga myndigheters nyttjande av kommersiella certifierade IKT-produkter, -tjänster och -processer. Åklagarmyndigheten delar utredningens syn på behovet av en ökad medvetenhet och kunskap om säkerheten hos IKT-produkter, -tjänster och -processer, men ser problem med en möjlig mer tvingande begränsning.

Åklagarmyndigheten avstyrker även betänkandets förslag om en ny rätt för tillsynsmyndigheter att utan samtycke från verksamhetsutövaren genomföra teknisk tillsyn på aktiva informationssystem. Åklagarmyndigheten anser att förslaget kan innebära en icke obefintlig risk för skador vid tillsyn, vid vilka ansvarsförhållandet inte är tydligt. Åklagarmyndigheten anser även att det från utredningen inte framgår varför en ytterligare tvingande åtgärd skulle vara nödvändig för att stärka säkerheten i berörda informationssystem.

12.5.6 Det föreligger f.n. inte behov av en nationell särskild ordning för certifiering i säkerhetskänslig verksamhet

Utredningen redogör under detta avsnitt ett behov av ett ökat nyttjande av certifierade IKT-produkter, -tjänster och -processer. Åklagarmyndigheten instämmer med utredningens slutsats att säkerheten i berörda informationssystem behöver höjas, och att ytterligare åtgärder för att

säkerställa detta krävs. Åklagarmyndigheten instämmer även med utredningens bedömning om att certifierade IKT-produkter, -tjänster och -processer i regel bör kunna förutsättas vara att föredra ur säkerhetssynpunkt. Dock vänder sig Åklagarmyndigheten emot utredningens uppfattning att ett ökat nyttjande skulle kunna vara lämpligt att uppnå genom tvingande allmänna råd. Även om en sådan ordning skulle tillåta nyttjandet av icke certifierade IKT-produkter, -tjänster och -processer där alternativet skulle vara olämpligt eller omöjligt riskerar detta att innebära en olämplig ansvarsförskjutning från den enskilda myndigheten till den ansvariga tillsynsmyndigheten. Det är Åklagarmyndighetens uppfattning att bedömningar av vilka tekniska lösningar som nyttjas i möjligaste mån bör beslutas av den som är närmast det berörda systemet, så länge lösningarna ger ett adekvat skydd.

Säkerhetsnivån på en certifierad säkerhetsprodukt är till sin natur beroende av vilken certifiering som produkten innehar. Det finns idag, vilket även utredningen konstaterar, flertalet utfärdare av säkerhetscertifikat för IKT-produkter, -tjänster och -processer, vilka arbetar utifrån egna krav och certifieringsrutiner. Ett krav på certifiering av IKT-produkter, -tjänster och -processer skulle innebära en utmanande balansgång, där en begränsning av godkända certifikat måste ställas mot att verksamhetsutövare inte ska möta ett allt för begränsat utbud av säkerhetslösningar.

Åklagarmyndigheten har i tidigare remissvar förespråkat en reglering som ställer specifika funktionella och/eller tekniska krav. Detta kan möjliggöra ett större mångfald av leverantörer utan att negativt inverka på kravställningen. Vid en certifikatbaserad reglering av IKT-produkter, -tjänster och -processer, kommer utbudet av leverantörer i viss mån riskera att vara avhängigt marknadens ekonomiska incitament att söka efterfrågade certifieringar. Skulle leverantörer av IKT-produkter, -tjänster och -processer genom en och samma certifiering ges tillträde till exempelvis hela den Europeiska unionens inre marknad bör kunna förutsättas att incitamenten är väsentligen högre än om motsvarande förvarande endast skulle ge tillträde till den svenska marknaden.

14 Tillgång till informationssystem vid tillsyn

Utredningen föreslår en rätt för tillsynsmyndigheterna att vid tillsyn få tillgång till informationssystem i syfte att genomföra tekniska kontroller. Utredningen anser att vid genomförandet av teknisk tillsyn även ska vara möjligt att genomföra vad som benämns som teknisk säkerhetsgranskning, exempelvis

genom simulerade angreppsförsök. Åklagarmyndigheten saknar här från utredningen viktiga svar.

Åklagarmyndigheten saknar en tydligt angiven ansvarsfördelning vad avser skador som vid aktiva tekniska kontroller kan uppstå. Att simulera angreppsförsök på ett informationssystem kan innebära förlust av data, korruption av mjukvara eller fysiska skador på utrustning. Det bör kunna förutsättas att ett informationssystems säkerhet följer skyddsvärdet på den information som behandlas. Därmed bör mycket känsliga system i högre utsträckning vara föremål för den typ av teknisk säkerhetsgranskning som utredningen föreslår ska kunna genomföras utan samtycke från systemägaren.

Vidare framgår inte av utredningen på vilket sätt som den nuvarande ordningen, vilken innefattar en möjlighet att granska exempelvis systemdokumentation och incidenthantering, inte anses kunna ge ett tillräckligt underlag för att säkerställa ett adekvat skydd. Åklagarmyndighetens bedömning är att samrådsförfarande inför driftsättning även fortsatt bör vara tillräckligt, i kombination med en frivillig möjlighet för verksamhetsutövare att låta utföra sådana tekniska säkerhetsgranskningar som behandlas i förslaget.

Detta yttrande har beslutats av vice riksåklagaren Katarina Johansson Welin efter föredragning av it-direktören Anders Thoursie och it-juristen Ezra Hatt.

I den slutliga handläggningen av ärendet har också säkerhetschefen Mikael Svensson, tf. enhetschefen Stefan Forsberg, it-säkerhetsspecialisten Christian Rothman och it-säkerhetsspecialisten Anders Nilsson deltagit.

Katarina Johansson Welin

Anders Thoursie

Kopia till
Justitiedepartementet (Å)

Kommunikationsavdelningen
Rättsavdelningen
Biblioteket
Paula Ljunggren, chefssekreterare