Justitiedepartementet
Enheten för lagstiftning om allmän ordning och säkerhet och samhällets krisberedskap
Att: Rättssakkunnig Katarina Bilge
103 33 Stockholm

Tillhandahållande av tekniska sensorsystem – ett sätt att förbättra samhällets informationssäkerhet - Ju2017/02002/L4

Regeringen har skickat ut rubricerade skrivelse från Justitiedepartementet på remiss. Stiftelsen för Internetinfrastruktur (IIS) ber att få framföra sina synpunkter på skrivelsen. Synpunkterna inkommer tyvärr efter sista svarsdatum då vi blev varse om skrivelsen sent eftersom vi uppenbarligen inte längre finns med på Justitiedepartementets lista över relevanta remissinstanser (vilket vi har gjort tidigare).

Skrivelsen innehåller förslag om att ge Myndigheten för samhällsskydd och beredskap (MSB) rätt att tillhandahålla sensorsystem för att bevaka internettrafik till och från myndigheter och andra organisationer utanför den offentliga sektorn, det vill säga sådana som betecknas vara skyddsvärda verksamheter. Syftet är att spåra och larma om skadlig trafik. Anslutning till sensorsystemet ska vara frivillig.

MSB har begärt att regeringen bör prioritera tillhandahållandet av sensorsystem på grund av dess angelägenhet, vilket innebär att denna del av förslagen som lämnats i betänkandet SOU 2015:23 Informations- och cybersäkerhet i Sverige bryts ut och särbehandlas trots att arbetet med en sammanhållen nationell strategi för stärkt informations- och cybersäkerhet i samhället pågår inom regeringskansliet. Skälet till denna brådska har inte redovisats.

IIS anser det inte vara tillräckligt redovisat huruvida denna isolerade åtgärd är tillräcklig, lämplig eller verkningsfull. Försvarets radioanstalt har redan till uppgift att på begäran kunna

placera ut liknande system vid de mest skyddsvärda verksamheterna bland statliga myndigheter och statligt ägda bolag i samverkan med Säkerhetspolisen. Någon analys av effektivitet och verkan av det systemet har inte redovisats.

Allt arbete med åtgärder för att uppnå ökad informationssäkerhet ska ske systematiskt. Systematiken ska utgå från den ansvariga ledningens styrning och ställer krav på att en verksamhet ska vidta åtgärder som står i proportion till de risker som den är utsatt för. För att kunna hantera riskerna krävs att verksamheten genomför en riskbedömning som är ändamålsenlig och verksamhetsanpassad. Verksamheten ska identifiera, förstå och bedöma riskerna för händelser som innebär till exempel förlust eller röjande av skyddsvärd information. Beskrivning av **hur** informationssäkerhet ska uppnås måste ingå vid både utveckling och upphandling av it-lösningar.

IIS är kritisk mot att man i det nu aktuella förslaget i princip har bortsett från behovet av kravställning och till och med förutsätter att MSB kan erbjuda en bättre och mer ändamålsenlig lösning än kommersiella aktörer på en öppen marknad.

IIS är även av uppfattningen att integritets- och demokratiaspekterna är både svepande och otillräckligt hanterade i skrivelsen. Det ursprungliga förslag som lades fram av NISU mötte också kritik hos remissinstanserna ifråga om integritetsaspekterna. I det tidigare förslaget var tanken att det skulle vara obligatoriskt för statliga myndigheter. I det nuvarande förslaget är anslutning frivillig men gäller för alla organisationer, alltså även verksamheter utanför den statliga sektorn.

IIS anser att de grundläggande riskerna med förslaget kvarstår och kanske till och med ökar i och med att det är öppet för all "samhällsviktig verksamhet" att ansluta sig. Om förslaget går igenom ger regeringen MSB "carte blanche" för att upprätta och utveckla en lista signaler och digitala spår som MSB ska bevaka, den så kallade "förteckningen". I skrivelsen står det att det "främst" handlar om ip-adresser och skadlig kod, att det "inte sannolikt" förekommer personuppgifter, men att det kan bli aktuellt bland annat i syfte att upptäcka falsklarm. Att ip-adresser ofta kan vara personuppgifter är i stort sett klargjort i EU-praxis.

Regeringen gör i sin tur bedömningen att det inte bryter mot proportionalitetsprincipen eller innebär "betydande intrång". Detta trots att det inte är möjligt att inhämta samtycke av den registrerade, ett avsteg som man rättfärdigar med att behandlingen är nödvändig för en arbetsuppgift av allmänt intresse ska kunna utföras. Dessutom är bedömningen gjord i skrivelsen att det är särskilt föreskrivet i lag att uppgifter inte får lämnas ut till den registrerade (s. 19). Låt oss anta att en individ får sin ip-adress blockerad av sensorsystemet på felaktiga grunder, ska denne då inte kunna få del av de uppgifter som ligger till grund för blockeringen?

I princip kan vilka digitala spår som helst hamna i förteckningen. Det finns inget i skrivelsen som sätter stopp för det. Andra integritetsfrågor är till exempel hanteringen av inspelningar av misstänkt trafik. Det berör inte bara enskilda individer, utan potentiellt organisationer i sin helhet. Upprepade larm kan innebära omfattande material om enskilda organisationer. Eftersom allt blir förenat med sekretess kommer ingen att få insyn i vad som registreras och hur det görs.

MSB ska kunna läsa e-post, bilagor, filer och meddelanden, trots att dessa går mellan medborgare och mellan aktuella myndigheter och andra berörda verksamheter utanför den offentliga sektorn. Vem ska kontrollera MSB:s arbete i dessa delar? Vart kan en individ vända sig med klagomål eller misstanke om missbruk av information?

Taget som en enskild företeelse kanske det inte ter sig så allvarligt att MSB ska tillhandahålla ett sensorsystem, men IIS vill erinra om att MSB numera också får incidentrapporter från statliga myndigheter. Att en myndighet i sin verksamhet ska vara både stödjande och samordnande, samtidigt som man ska utöva tillsyn är oftast ingen bra kombination. Utredningen om genomförande av NIS-direktivet (Ju 2016:11) ska inom den närmaste tiden föreslå hur EU-direktivet om åtgärder för en hög gemensam nivå av säkerhet i nätverk och informationssystem ska genomföras i svensk rätt. Utredaren ska bl.a. föreslå hur direktivets krav på utpekande av myndigheter med ansvar för vissa funktioner ska genomföras, med inriktningen att Myndigheten för samhällsskydd och beredskap (MSB) ges en samordnande roll på området men att andra myndigheters ansvar för tillsyn inom särskilda sektorer ska fortsätta att gälla.

Vidare arbetar man i regeringskansliet för närvarande med att ta fram en nationell strategi för informations- och cybersäkerhet, som tar sin utgångspunkt i det förslag som lades fram i betänkandet Informations- och cybersäkerhet i Sverige (SOU 2015:23). I dagsläget är planen att strategin ska presenteras i maj 2017. Även här pekas på MSB som den centrala punkten genom att MSB ges i uppgift att bedriva tillsyn över statliga myndigheters arbete med informationssäkerhet.

Det är en knivskarp balansgång mellan behovet att förebygga it-attacker och att skydda individers personliga integritet, alltså upprätthålla och värna om mänskliga rättigheter.

Utvecklingen inom svensk lagstiftning går alltmer mot ett ökat utnyttjande av tvångsmedel med nya typer av integritetskänslig insamling, övervakning och lagring av information. När ett sensor- eller övervakningssystem väl är infört är förslag om breddning och utökning på olika sätt inte långt borta och ändamålsglidningen kan vara ett faktum.

Regeringen har i sitt förslag att ge MSB rättsligt mandat att stödja vissa offentliga och enskilda verksamhetsutövare inom samhällsviktig verksamhet med informationssäkerheten genom att på deras begäran tillhandahålla sensorsystem inte lyckats visa att åtgärden har en klar och tydlig nytta. Trenden är dessutom att angripare finner nya metoder som går under radarn för både svartlistor och signaturbaserade filter av den typ som förslaget innefattar.

Stockholm den 8 maj 2017

Stiftelsen för Internetinfrastruktur

Danny Aerts, vd