Ert datum	Er referens
	Ju2017/08898/Å
Datum	Vår referens
2018-03-05	Pär Nygårds

IT&Telekomföretagen
ALMEGA

Justitiedepartementet
103 33 Stockholm

Remissvar SOU 2017:89 – Hemlig dataavläsning

IT&Telekomföretagen tackar för möjligheten att inkomma med synpunkter på utredningen. De är samberedda med medlemsföretag verksamma i Datarådet vilket samlar företag engagerade i data- och innehållsrelaterade policyfrågor.[1]

Det ska inledningsvis framhållas att IT&Telekomföretagen stödjer utredningens målsättning att bekämpa allvarlig brottslighet. Vi är måna om att våra medlemsföretag bistår de brottsbekämpande myndigheterna i deras arbete. En central förutsättning är dock att det sker inom ramen för ett system som är proportionerligt i relation till de ingrepp som hemlig dataavläsning (HDA) innebär för användares och kunders integritet.

Utredningen föreslår en sk medverkansmöjlighet för teleoperatörer vid HDA. Med andra ord föreslås inget lagstadgat krav på operatörer att vare sig anpassa sin verksamhet eller sin utrustning eller medverka till verkställighet i det enskilda fallet. Däremot pekar utredningen tydligt ut teleoperatörer som instrumentella för brottsbekämpande myndigheters möjlighet att placera ut trojaner och spionprogram i utpekade kunders mobiltelefoner. Utredarna argumenterar för frivillighet för operatörer att medverka kopplat till det *”…samhällsansvar som följer med den bedrivna verksamheten”*. De slår också fast att *”Mot bakgrund av de regler som vi föreslår ska gälla till skydd för den personliga integriteten och informationssäkerheten finns [det] inte skäl för operatörer att vägra att medverka eller hjälpa den brottsbekämpande myndigheten”*.[2] Om brottsbekämpande myndigheter över tid inte är nöjda med utfallet av operatörernas frivilliga medverkansmöjlighet föreslår utredningen att en lagstadgad medverkansskyldighet bör införas.

Mot bakgrund av det möte IT&Telekomföretagen och berörda medlemsföretag haft med utredarna och de synpunkter som där framfördes är vi förvånade över att de tagit så lätt på frågan om teleoperatörers skyldigheter avseende driftsäkerhet och integritetsskydd. Dessa skyldigheter finns reglerade i lagar och föreskrifter.[3] Det finns även utifrån en kommersiell och varumärkesbaserad

[1] https://www.itot.se/radsverksamhet/dataradet/
[2] SOU 2017:89 s.428
[3] Lag (2003:389) om elektronisk kommunikation och exempelvis PTSFS 2014:1 *”Post- och telestyrelsens föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter”* i vilken krav ställs på operatörer att göra allt i sin makt för att förhindra spridning av skadlig kod, virus

utgångspunkt ett starkt kundvårdsincitament att begränsa spridningen av skadlig kod och virus. Till yttermera visso är operatörer enligt EU-förordning 611/2013 skyldiga att utan dröjsmål rapportera integritetsincidenter till såväl tillsynsmyndighet som till den berörda kunden.

Så som HDA är definierat i utredningen innebär det att brottsbekämpande myndigheter får starka incitament att avstå från att rapportera svagheter i exempelvis operativsystem, terminaler eller chipset som man blir medveten om till relevanta myndigheter, tillverkare och tjänsteleverantörer. Det är precis den typ av svagheter som utnyttjas för att exempelvis kunna placera en hemlig mjukvara på en mobiltelefon för att kunna ta del av dess information. Vilka konsekvenser förslaget om HDA har för informationssäkerheten har utredningen enligt egen utsaga svårt att bedöma. Att man ser det svårt att bedöma art eller omfattning av risker förknippade med HDA och ändå föreslå ett sådant kraftfullt redskap är klart otillfredsställande. Sådana risker kräver en betydligt mer utförlig analys och välgrundad intresseavvägning än vad utredningen presterar.

Ett illustrativt exempel på informationssäkerhetskonsekvenserna av att inte rapportera in svagheter i mjukvaror är ransomware-attacken WannaCry från 2017. Utpressare utnyttjade en svaghet i operativsystemet Microsoft Windows för att ta över och kryptera en mängd IT-system. Först mot ersättning fick de drabbade en krypteringsnyckel som åter gav dem kontroll över sina system. Uppskattningsvis 230 000 datorer drabbades världen över, däribland sjukhus, hamnar och andra samhällskritiska funktioner. I efterhand visade det sig att amerikanska signalspaningsmyndigheten NSA känt till svagheten men underlåtit sig att meddela Microsoft i syfte att själva kunna nyttja den.

Det är precis den här typen av samhälleliga risker som HDA öppnar upp för. Här finns en direkt och uppenbar motsättning mellan det förslag om HDA som utredningen föreslår och upprätthållandet av driftsäkerhet och informationssäkerhet. Mot bakgrund av ovanstående kan det med fog ifrågasättas att operatörer ska förväntas att aktivt medverka till att för dem okända virus och spionprogram släpps in i nät och kundutrustning. Utan närmre information om vilka åtgärder operatören ska medverka till och vilka säkerhets- och driftsmässiga konsekvenser som kan uppstå vore det direkt oansvarigt för operatören att medverka. Det framgår inte heller av utredningen vilka tekniker som kan bli aktuella och vad som närmre förväntas av operatören för att underlätta verkställighet av HDA. Utan sådan fakta kan operatörerna svårligen tänkas medverka till att virus och spionprogram placeras i deras och kundernas utrustning.

I sammanhanget är det värt att nämna några av de utländska exempel på HDA som utredningen tar upp. Danmark beskrivs som ett land där HDA använts under lång tid. Där finns dock ingen medverkansplikt och operatörerna har ingen som

---

och liknande mjukvara av precis det slag som utredningen föreslår aktivt ska placeras i kunders mobiltelefoner.

helst insyn i hur tvångsmedlet används och de medverkar inte på något sätt i verkställigheten så som utredningen förordar att svenska operatörer ska göra. I Norge har HDA nyligen införts. Där finns krav på operatören att tillhandahålla information som är nödvändig för verkställandet, men i övrigt har de ingen medverkansplikt. I praktiken har den norska polisen i några fall begärt att en operatör aktivt ska medverka till att spionprogram generellt ska släppas igenom via vissa utpekade kommunikationsvägar. Där har operatören med hänvisning till de tekniska och integritetsmässiga riskerna med de föreslagna åtgärderna vägrat att medverka. I detta fall har operatörens bedömning av riskerna fått stöd av den norska tillsynsmyndigheten NKOM.

I den utsträckning som svenska teleoperatörer kan förväntas medverka aktivt till verkställighet av HDA krävs att operatörerna ges tillräcklig insyn i den teknik som används i det enskilda fallet så att operatören självständigt kan bedöma riskerna för driftsäkerheten och integritetsskyddet i den egna verksamheten. Även på området relevanta myndigheter, såsom PTS och MSB, bör kopplas in för bedömning om de aktuella riskerna är godtagbar i förhållande till de lagkrav som gäller för operatörerna.

Såväl WannaCry som det norska exemplet visar dessutom tydligt på målkonflikten mellan brottsbekämpande myndigheters önskan om mer och bättre information och operatörernas, deras kunders och för den delen hela samhällets behov av robusta och säkra elektroniska kommunikationstjänster.

Även om utredningen förordar domstolsbeslut samt att Säkerhets- och Integritetsskyddsnämnden (SIN) föreslås som kontrollinstans är det, givet målkonflikterna och den ovan nämnda problematiken, tveksamt om utredningens förslag till fullo lever upp till kraven på nödvändighet, proportionalitet och rättssäkerhet.

Avslutningsvis vill vi understryka att IT&Telekomföretagen är måna om att våra medlemsföretag bistår brottsbekämpande myndigheter i deras verksamhet. Sådan samverkan existerar sedan länge, fungerar överlag väl (vilket utredningen också noterat) och sker där det bedöms förenligt med gällande lagkrav och föreskrifter samt då det inte utsätter branschens kunder för säkerhetsrisker eller omotiverat långtgående integritetsintrång.

Med vänlig hälsning

Pär Nygårds
Näringspolitisk expert