Föreningen för digitala fri- och rättigheter

ORG.NR 802461-0852 – HTTPS://WWW.DFRI.SE – DFRI@DFRI.SE

DFRI
Box 3644
103 59 STOCKHOLM

Justitiedepartementet
103 33 STOCKHOLM

Stockholm 2018-03-05

Yttrande över delbetänkande av Utredningen om hemlig dataavläsning (SOU 2017:89)

Föreningen för digitala fri- och rättigheter (DFRI) är en ideell och partipolitiskt obunden förening som verkar för främjandet av digitala rättigheter. Vårt mål är ett samhälle med så lite övervakning, spårning och avlyssning som möjligt. Vi värnar om yttrandefrihet, transparens och informationsfrihet, personlig integritet och människors rätt att själva bestämma över sin personliga information och digitala fotspår.

Sammanfattning

DFRI avstyrker förslaget om att införa hemlig dataavläsning som ett hemligt tvångsmedel i Sverige. Ett sådant tvångsmedel skulle innebära ett synnerligen omfattande intrång i rätten till privatliv och skyddet av den personliga integriteten. Det har dessutom visat sig att de verktyg som används för hemlig dataavläsning medför stora risker för samtliga invånare, näringsliv, myndigheter och samhället i övrigt. De eventuella effektivitetsvinster som finns för brottsbekämpande myndigheter är inte tillräckligt stora för att motivera användandet av dessa riskabla metoder.

Privat kommunikation är en mänsklig rättighet

En stor och snabbt växande del av människors kommunikation sker numera digitalt. Säkra och effektiva sätt att kommunicera digitalt är en förutsättning för ett demokratiskt samhälle. Vi har alla rätt att föra privata konversationer med våra vänner, våra partikamrater, vår läkare, vår terapeut och andra, utan rädsla för att bli avlyssnade. Så länge vi inte kan misstänkas för något brottsligt så ska vi vara tillförsäkrade rätten att slippa avlyssning från staten.

Även myndigheter, företag och föreningar har legitima skäl till och behov av säker kommunikation utan risk för avlyssning.

Risken för brottslighet kan öka med hemlig dataavläsning

Målet med brottsbekämpning borde vara att göra tillvaron säkrare för landets invånare, inte att utsätta oskyldiga för större risker. Det riskerar dock att bli fallet eftersom de verktyg som utvecklas för att genomföra hemlig dataavläsning kan komma att användas för helt andra syften, om de kommer i händerna på exempelvis kriminella ligor eller utländska underrättelsetjänster.

Genom att aktivt söka efter eller köpa[1] sårbarheter i informationssystem och sedan bygga verktyg för att utnyttja dessa säkerhetsluckor utsätts allmänheten för stora risker. Om man väljer att inte rapportera dessa brister, för att istället kunna använda dem till hemlig dataavläsning av ett litet fåtal brottsmisstänkta individer, lämnas alla andra fortsatt allt mer sårbara för intrång.

Utredningen resonerar kring denna problematik[2] och konstaterar bland annat följande:

> Genom att inte underrätta tillverkaren om sårbarheten i dessa fall kommer denna stå öppen inte bara för den brottsbekämpande myndigheten utan också för andra, och därmed även illasinnade personer. På så vis kan det sägas att säkerhetshålen inte täpps igen så snart som de skulle kunna täppas igen. Det innebär i förlängningen att det finns risk för att kriminella skulle kunna utnyttja samma hål som den brottsbekämpande myndigheten. Detta kan i viss mån sägas tala för en rapporteringsskyldighet avseende den typen av sårbarheter och säkerhetsbrister.

Tyvärr visar utredningen sedan en betydande okunnighet om verkligheten när den gör följande bedömning:

> Dessutom kommer det endast vara en mycket begränsad mängd personer som har kännedom om de tekniker som används vid hemlig dataavläsning och därmed också om eventuella sårbarheter. Dessa personer kommer också att ha genomgått noggranna säkerhetskontroller varför risken för spridning utanför den skara personer som känner till sårbarheterna är synnerligen liten.

Verkligheten visar tvärtom att risken för spridning är uppenbar. Både amerikanska CIA[3] och NSA[4] har vid olika tillfällen tappat kontrollen över sina egna verktyg för hemlig dataavläsning. Dessa har sedan fått spridning och utnyttjats av kriminella som troligtvis

[1] https://www.svt.se/nyheter/vetenskap/stater-rustar-for-natattacker
[2] SOU 2017:89, s. 397-398
[3] https://en.wikipedia.org/wiki/Vault_7
[4] https://en.wikipedia.org/wiki/The_Shadow_Brokers

inte själva hade haft kapacitet att hitta och utnyttja de sårbarheter som dessa verktyg använde.

De senaste årens rapportering om IT-säkerhet hos Polisen och andra myndigheter visar tydligt att det saknas anledning att tro att svenska myndigheter skulle kunna skydda sina hemligheter bättre än sina amerikanska kollegor.

Stora risker och skador för samhället

Intrångsverktyg från NSA användes i maj 2017 till ett av historiens allvarligaste virusangrepp på datorer, under namnet WannaCry[5]. Det är ännu svårt att fullt ut analysera vilka konsekvenser detta har fått. Klart är att dock att minst 230.000 datorer runt om i hela världen drabbats. Enorma värden har gått förlorade för privatpersoner, företag och myndigheter. Exempelvis har sjukhus i flera länder lamslagits med ännu oklara följder för patienternas liv och hälsa.

Angreppet utnyttjade ett säkerhetshål som hade varit känt för amerikanska NSA en längre tid. Detta angrepp kunde ha undvikits om det hade rapporterats till tillverkaren, så att hålet hade kunnat täppas till i tid. Istället valde NSA att lämna miljontals datorer sårbara, för att själva kunna utnyttja säkerhetshålet till att i hemlighet spionera på innehållet i människors datorer.

Det är enligt DFRI:s bestämda uppfattning inte till gagn för alla laglydiga invånare i Sverige att deras myndigheter ägnar sig åt hemlig dataavläsning.

Föreningen för digitala fri- och rättigheter

Peter Michanek
Sekreterare

[5] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack