dataskydd.net

ORG.NR 802495-4797 – HTTPS://DATASKYDD.NET – INFO@DATASKYDD.NET

Dataskydd.net Sverige
c/o Anders Lundquist
Eningebölevägen 44
749 61 Örsundsbro

Justitiedepartementet
103 33 Stockholm

Lund 2015-09-11

Remissyttrande över SOU 2015:23 – Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten

Dataskydd.net avstyrker utredningens förslag till förordning om statliga myndigheters informationssäkerhet. Dataskydd.net avstyrker utredningens förslag till förordning om ändring i säkerhetsskyddsförordningen.
Dataskydd.net lämnar särskilda kommentarer på följande stycken i utredningen:

- Kapitel 5: Dataskydd.net avstyrker utredningens genomgång av det rådande rättsläget. *s. 4*
- Kapitel 9.1: Dataskydd.net avstyrker utredningens förslag om en nationell strategi för informations- och cybersäkerhet så som presenterad i Bilaga 5. *s. 5*
- Kapitel 9.2: Dataskydd.net avstyrker utredningens förslag om ansvar, styrning, samordning och tillsyn. *s. 8*
- Kapitel 9.3: Dataskydd.net avstyrker utredningens förslag om staten som tydlig kravställare. *s. 10*
- Kapitel 9.5: Dataskydd.net avstyrker utredningens förslag om incidentrapportering. *s. 12*
- Kapitel 9.6: Dataskydd.net avstyrker utredningens förslag om brottsbekämpning. *s. 14*

Introduktion

Utredningens har genom det ensidiga valet av underlag kommit att i hög grad baseras på partsinlagor. Detta i kombination med att man inte beaktat forskning och befintlig praktik i näringslivet innebär att man ger rekommendationer som är mer ägnade att tjäna vissa myndigheters egna intressen snarare än allmänintresset.[1] En strategi för ett säkrare internet utarbetad av Post- och telestyrelsen 2006[2] förefaller ha legat i linje med åtgärder som i forskning och praktik i näringslivet då visat sig ge säkerhetshöjande resultat. Redan i början av 1990-talet drogs slutsatsen att starkare konsumenträtt ger mer säkerhet i vanligt använda

[1] Se utförliga underlag i fotnot 15, 16 och 43. För en lite äldre sammanställning, se Jay Pil Choi, Chaim Fershtman och Neil Gandal. *Network Security: Vulnerabilities and Disclosure Policy*. WEIS 2007.

[2] Post- och telestyrelsen. *Strategi för ett säkrare Internet i Sverige*. PTS-ER-2006:12.

elektroniska system för samma mängd pengar som annars skulle leda till sämre säkerhet.[3] Forskning visar att medvetna åtgärder för att ge privatpersoner och konsumenter bättre tillgång till information om säkerhetsproblem i IT-system hjälper dem att utkräva ansvar.[4]

Utredningen borde ha undersökt varför åtgärder med starkt stöd i forskning och näringsliv inte genomförts, och vad som kunnat förbättras givet det nya kunskapsläget. Utredningen verkar dock ha bortsett från all kunskap om informationssäkerhet som har näringspolitisk, konsumenträttslig eller människorättslig anknytning, och även från merparten av tidigare svenska IT-säkerhetsstrategier som utarbetats av myndigheter med ansvar för för sådana områden.

Utredningen tillsattes under svårbegripliga förhållanden: utredningen annonserades av en näringsminister,[5] men uppdraget och kravställaren är försvarsdepartementet. Uppdraget och utförandet ger ett rörigt intryck.

Dataskydd.net föreslår en ”individ-centrisk” incident- och sårbarhetsrapportering. I flera amerikanska delstater har man infört obligatorisk incidentrapportering för företag och myndigheter som riktar sig till de privatpersoner som berörs av incidenten. Först ut var Kalifornien 2002. Det finns mycket forskning kring hur konsumenter ställer företag till svars för att inte ha åtgärdat säkerhetsproblem.[6] Forskningen visar också att konsumenter är mer benägna att ställa sådana aktörer till svars, som också MSB i sina utredningar håller med om att det är extra viktigt att medborgarna har förtroende för.

Ur Dataskydd.net:s perspektiv är det mest allvarligt att utredningen bortsett från privatpersoners rättigheter. Det mest uppenbara exemplet på detta är formuleringen ”mänskliga rättigheter *samt* personlig integritet” i utredningens föreslagna strategi i bilaga 5. Personlig integritet är inte någonting som staten har åtagit sig att skydda *utöver* de egentliga mänskliga rättigheterna som staten egentligen skyddar, utan är en viktig och prioriterad del av de konventioner om mänskliga rättigheter som staten åtagit sig att upprätthålla. Det är oroväckande att utredaren lägger sig till med en semantik som ger intrycket av att utredaren inte anser att staten ska fortsätta stödja de rättighetskataloger som är etablerade internationellt.

SOU 2015:23, bilaga 5, *Strategi för statens informations- och cybersäkerhet*, s. 330.

Normaltillstånd och kris

En samhällskris är enligt Myndigheten för samhällsskydd och beredskap en kris som drabbar många människor och stora delar av samhället samt hotar grundläggande värden och funktioner. Den är oväntad, utanför det vanliga och vardagliga och hotar liv, hälsa, säkerhet och grundläggande värden.[7] Exempel från närtiden är branden i Västmanland, då människor drevs från hus och hem, förlorade vattenförsörjning och runt 14 000 hektar värdefulla skogsarealer ödela-

[3] Ross Anderson. *Why Cryptosystems Fail*. ACM. 1st Conf. – Computer and Communication Security 1993.

[4] Sasha Romanosky, David Hoffman, Alessandro Acquisti. *Empirical Analysis of Data Breach Litigation*. WEIS 2010.

[5] Pressmeddelande från näringsdepartementet om infosäkerhetsutredning.

[6] Sasha Romanosky, David Hoffman, Alessandro Acquisti. *Empirical Analysis of Data Breach Litigation*, WEIS 2010; David Solove, *Are People Really Harmed By a Data Security Breach?*, Concurring Opinions, 22 september 2010; m. fl.

[7] Myndigheten för samhällsskydd och beredskap. *Pedagogik för samverkan i samhällskriser*.

des.[8] Stormen Gudrun förstörde stora skogsarealer, påverkade elförsörjning och telefoni för ett stort antal människor och drev människor från hus och hem.[9]

Utredningens föreslagna lösningar verkar anta att alla former av IT-problem automatiskt är kriser, och lägger över en stor del av ansvaret för motverkande av IT-problem på den krishanterande och krisberedande myndigheten MSB. Utredningen blandar därmed ihop ”normaltillstånd” med ”kris”.

NORMALTILLSTÅND: när det inte är kris.
KRIS: sbst., r. (l. f.); best. -en; pl. -er; Av lat. crisis, av gr. κρίσις, avgörande prövning, dom, till κρίνειν, frånskilja utgallra m. m.
1) brydsam situation (i vilken ett avgörande är att vänta); kritiskt stadium l. ödesdiger rubbning i ngts utveckling l. fortbestånd o. d.; (med själslig strid, oro o. d. förbunden) avgörande l. genomgripande vändning i ngns liv.
a) i uttr. vara i sin kris, befinna sig i en kris genomgå en kris.
b) avgörande vändning (till det bättre) i en akut sjukdoms förlopp;
c) kritisk situation i affärs- l. näringsliv,,stagnation l. förlamning av det ekonomiska livet.
d) polit. brydsam politisk situation som kan tvinga en regering att avgå.
2) medvetslöshet, dvala; trans; äv. om hysteriskt anfall o. d.; särsk. i uttr. falla i kris, gripas av hysteri, få ett hysteriskt anfall.

Det är ingen samhällskris att företaget Tieto uppgraderar sina serverhallar.[10] Även om flera landsbygdsapotek fått hantera pappersrecept, två kommuner fått jämförelsevis små administrativa merkostnader, Bilprovningen har stängt i en dag och två företag löser sina IT-problem inom ett fåtal timmar är det fortfarande ingen samhällskris. Tvärtom är det önskvärt och bra att företag uppgraderar sina serverhallar, och vi vill inte bygga en IT-säkerhetsstrategi som förutsätter att kontinuerliga uppgraderingar av hård- och mjukvara ska göras svårare och mer byråkratiskt.

Det var ingen samhällskris att Skatteverkets SPAR-register blev hackat 2009:[11] skatteindrivningen påverkades inte, majoriteten av de drabbade medborgarna informerades inte, inga skulder förblev obetalda till följd av tilltaget och ingen myndighetsutövning i övrigt upphörde (så vitt allmänheten kunnat erfara). Ej heller minskade medborgarnas förtroende för de berörda myndigheterna[12] – trots att detta hade varit väl förtjänt.[13]

Vi har inga indikationer på att denna sorts kriser drabbar samhället vid användning av informationsteknologiska system. Forskning stödjer att vi inte heller kan förvänta oss att drabbas av sådana kriser.[14] Vad vi däremot har vid användning av informationsteknologiska system är ett stort antal vardagliga, normala problem som inte behandlas: blåa skärmar, onödiga säkerhetsåtgärder, programkrascher som förstör människors arbetsdagar, storskalig och osäker insamling av en mängd personuppgifter från det att vi går i skolan, till att vi besöker vården, tills dess vi arbetar och betalar skatt och tills vi blir pensionärer.

Om Sverige, så som hävdas av försvarsmyndigheterna i utredningens fjärde bilaga, ”är en exportnation och det är viktigt för Sveriges industri att inte vår export onödigtvis hindras av andra länders regleringar” och därför ska ”föregå med gott exempel” genom att ”beakta handelsaspekten” då man försöker ”upprätthålla säkerhet och integritet i samhällsviktig it-infrastruktur” måste utgångspunkten vara att man hanterar normala förfaranden inom IT-branschen som normala, inte som kriser. Man kan göra detta i enlighet med redan befintlig forskning[15] och befintliga myndighetsutredningar från myndigheter som an-

SOU 2015:23, bilaga 4, ”Förslag till nationell strategi och åtgärdsplan för säkra kryptografiska funktioner”, s. 310–311.

FN:s expertgrupp på telekomfrågor har uttalat att ”States must not use proxies to commit internationally wrongful acts.” och ”States should encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs, including supply chain security for ICT products and services” i en rapport från 68:e sessionen 2013.

[8] Se t.ex. Wikipedia: https://sv.wikipedia.org/wiki/Skogsbranden_i_Västmanland_2014

[9] Se t.ex. Wikipedia: https://sv.wikipedia.org/wiki/Orkanen_Gudrun

[10] Myndigheten för samhällsskydd och beredskap, *Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter – En studie av konsekvenserna i samhället efter driftstörningen hos Tieto i november 2011*, februari 2012.

[11] Rebecca Haimi, ”Skatteverkets folkbokföring hackad”, *Dagens Nyheter*, 29 mars 2012.

[12] Svenska folkets bedömning av offentliga myndigheters verksamhet, SOM-rapport nr 2014:11; Svenskars bedömning av offentliga myndigheters verksamhet, SOM-rapport nr 2012:10; Förtroendet för myndigheter Riks-SOM-undersökningen 1986-2007. SOM-rapport nr 2008:25.

[13] Jämför danska Datatilsynets skarpa kritik mot danska polismyndigheten i det liknande ärendet ”Uvedkommendes adgang til personoplysninger i systemer, som Rigspolitiet er dataansvarlig for”, Journalnummer: 2013-632-0050. 31 juli 2015.

[14] Thomas Rid, *Cyber War Will Not Take Place*, London: Hurst/Oxford University Press, 2013.

[15] Se en längre lista relaterade forskningsartiklar på https://www.cl.cam.ac.uk/~rja14/econsec.html

svarar för näringslivsfrågor.[16] Svenska myndigheter bör sluta överdriva vanliga och normala problem som uppstår i IT-system. Det som behövs är normaltillståndsrutiner, inte krisrutiner.

Utredningen borde ha övervägt ett förbud för brottsbekämpande och försvarsrelaterade myndigheter att förvärra problemen med dataintrång och antagonistiska hot mot IT-system.[17] Polisen och åklagarmyndigheten har i närtid uttryckt önskemål om att få bidra till marknaden för ”[p]rogramvara särskilt utvecklad för it-angrepp” som utredaren flaggar som ”antagonistiskt hot” i kapitel 4.[18] Även underrättelsetjänsten[19] och försvarsmakten[20] verkar antyda att de vill ha tillgång till sådana produkter som utredaren beskriver som ”antagonistiska hot”.

SOU 2015:23, s. 70

Kapitel 5: Dataskydd.net avstyrker utredningens sammanfattning av den nu rådande regleringen som bristfällig.

I utredningens uppdrag står följande:

SOU 2015:23, s. 292

> Informationssäkerhetsområdet är tvärsektoriellt och omfattar många aktörer i samhället på lokal, regional och central nivå. Även näringslivet har en stor roll i detta arbete. /.../ Nuvarande ansvarsförhållanden och åtaganden ska beaktas men inte begränsa utredningen, som ska utgå från ansvarsprincipen och gällande ekonomiska ramar.

Utredningen missar att utreda konsumenträttigheter, trots att bristen på konsumenträttigheter i digitala miljöer är någonting som uppenbarligen påverkar näringslivets incitament att leverera fungerande, säkra tjänster. Att konsumenträttsliga frågeställningar tidigare inte framgångsrikt har lyfts politiskt – trots att de rönt stor uppmärksamhet bland till exempel IT-säkerhetsexperter och forskare – borde inte ha begränsat utredningen, men verkar ändå ha gjort det.

Omständigheten att bördan för att bevisa produktfel faller på konsumenten i digitala miljöer, men på leverantören i icke-digitala miljöer, är en nackdel för konsumenten i digitala miljöer. En enskild konsument har sällan möjlighet att påvisa säkerhetsfel i en produkt. Det är inte ens säkert att en enskild konsument har möjlighet att få kännedom om säkerhetsfel som är allmänt kända bland utvecklare av digitala produkter. Även då en konsument drabbats negativt av ett säkerhetsfel i en digital produkt, är det inte säkert att konsumenten har möjlighet att koppla den negativa verkan till säkerhetsfelet. Det kan till exempel röra en digital tjänst som orättfärdigt läcker kreditkortsinformation: en konsument kan rimligen antas upptäcka att konsumenten förlorat delar av sina privata tillgångar, men kan inte rimligen antas tekniskt spåra förlusten tillbaka till den felaktiga digitala tjänsten.

De flesta säkerhetsproblem vid användning av informationsteknologiska system vardagliga, normala problem som bortses ifrån av lagstiftare, utredare och krisberedskapsmyndigheter: blåa skärmar, onödiga säkerhetsåtgärder, programkrascher som förstör människors arbetsdagar, storskalig och osäker

[16] Post- och telestyrelsen (2006). *Strategi för ett säkrare Internet i Sverige*. PTS-ER-2006:12; ENISA (2008). Ross Anderson, Rainer Böhme, Richard Clayton, och Tyler Moore. *Security, Economics, and the Internal Market*; ENISA (2011). Panagiotis Trimintzios, Chris Hall, Richard Clayton, Ross Anderson och Evangelos Ouzounis. *Resilience of the Internet Interconnection Ecosystem*; Post- och telestyrelsen/Datainspektionen, *Användning av trafikuppgifter i mobila innehållstjänster. Rapport efter avslutad tillsyn*. PTS-ER-2010:01/Datainspektionen 2010:1; Datainspektionens allmänna råd, *Säkerhet för personuppgifter*, reviderad november 2008; Datainspektionen, vägledning, *Inbyggd integritet – Privacy by design*, januari 2012.

[17] För tydliga översikter av problem som uppstår när stater ägnar sig åt antagonistiska åtgärder i nätmiljöer se t.ex. Ronald Deibert, *Black Code: Inside the Battle for Cyberspace*, Signal, 2013; Claudio Garnieri, ”Everything we know of NSA and Five Eyes malware”, blogginlägg, 2015; se även ovan, fotnot 18, 19 och 20; se även Förenta nationernas generalförsamling, ”Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security”, rapport A/68/98 av 24 juni 2013; samt för en översikt av de ekonomiska incitament som styr huruvida sårbarheter och IT-problem åtgärdar, se Rainer Böhme, *Vulnerability Markets – What is the economic value of a zero-day exploit?*, Chaos Communication Congress 2007

[18] SOU 2012:44 Hemliga tvångsmedel, kapitel 14.2 om hemlig dataavläsning; ”Åklagare och Säpo vill införa nytt tvångsmedel – hemliga ”spiontrojaner” i datorer”, *Dagens Juridik*, 24 april 2014.

[19] ”FRA hackar datorer – topphemligt projekt med NSA”, *Sveriges television*, 11 december 2013.

[20] Mikael Holmström, ”Försvarsministern: Vi ska kunna genomföra cyberattacker”, *Dagens Nyheter*, 18 mars 2015.

insamling av en massa personuppgifter från det att vi går i skolan, till att vi besöker vården, tills dess vi arbetar och betalar skatt.

Konsumenters rättigheter på digitala marknader är betydligt svagare än motsvarande rättigheter för konsumenter på icke-digitala marknader. De många mellanhänderna gör att det konsumenträttsliga skydd som normalt skulle vara gällande vid produktköp och tjänstköp avtalsrättsligt försvinner.[21] Det här problemet blir ännu större när konsumenten är en privatperson som har kontakt med en myndighet. Då är det myndigheten som är kund och ansvarig för avtalen, och privatpersonen har inga möjligheter att utkräva något ansvar alls.

Det har gjorts försök att åtgärda detta i den europeiska utvecklingen på området:

- EU-kommissionen utredde 2006 om digitala tjänster och produkter bör likställas med fysiska tjänster och produkter,[22] i syfte att ta reda på om konsumenter bör ges samma rättigheter på digitala marknader som de har på icke-digitala marknader.
- Sommaren 2015 har EU-kommissionen öppnat för möjligheten att lägga bevisbördan för fel i digitala system på tjänste- och produktleverantörer istället för på slutkonsumenter.[23]

Kapitel 9.1: Dataskydd.net avstyrker utredningens förslag om en nationell strategi för informations- och cybersäkerhet så som presenterad i Bilaga 5.

Sverige lider redan idag av ett stort antal ogenomförda strategier och åtgärdsprogram för bättre IT-säkerhet i allmänna och privata IT-system.

Givet forskningsläget[24] verkar Post- och telestyrelsen ha varit helt rätt ute i sin strategi för ett säkrare internet i Sverige från 2006.[25] Tyvärr har strategin inte följts upp eller utvärderats.

De flesta tidigare strategier har aldrig utvärderats. Det har aldrig konstaterats att de är dåliga. Det har aldrig undersökts varför de knappt eller inte alls har genomförts. En utvärdering och uppföljning av dessa strategier känns angelägen, eftersom åtgärderna de föreslår sammanfaller väldigt väl med det som etablerats fungera säkerhetshöjande i forskning.[26]

Utredningens enda hänvisning till tidigare handlingsplaner för informationssäkerhet utgörs av ett direkt citat från en regeringsskrivelse från 2009:

En ej uttömmande lista över tidigare svenska säkerhetsstrategier:
PM 1:2001, IT-kommissionen, *Grundskydd i datorer och programvaror*
PM 39:2001, IT-kommissionen, *Hantering av IT-incidenter, vem gör vad och hur?*
PTS-ER-2006:12 *Strategi för ett säkrare Internet i Sverige.*
Datainspektionens allmänna råd. *Säkerhet för personuppgifter*. Reviderad november 2008.

SOU 2015:23, s. 205/Samhällets krisberedskap – stärkt samverkan för ökad säkerhet (skr. 2009/10:124), s. 66.

[21] För en svensk behandling av avtalsrättsligt flyttad skuldbörda, se Lennart Johansson, *Banker och internet*, Iustus förlag (Stockholm) 2006.

[22] EU-kommissionen (2006). COM (2006) 744 final. *Green Paper on the Review of the Consumer Acquis.*; EU-kommissionen (2007) *Detailed analysis of responses to the European Com mission Green Paper on Consumer Rights Reform.*

[23] EU-kommissionen (2015). *Public consultation on contract rules for online purchases of digital content and tangible goods*.

[24] Se t.ex. angivna referenser i fotnot 15, men också det mer utförliga urvalet av myndighetsreferenser i fotnot 16. Se emellertid särskilt Sasha Romanosky, David Hoffman, Alessandro Acquisti *Empirical Analysis of Data Breach Litigation* i WEIS 2010, för en omfattande behandling av rättsliga konsekvenser för aktörer som hanterar personuppgifter dåligt, när man ger privatpersoner möjligheten att stämma dessa aktörer.

[25] Se fotnot 73.

[26] Se särskilt ENISA (2008). Ross Anderson, Rainer Böhme, Richard Clayton, och Tyler Moore. *Security, Economics, and the Internal Market* och vidare forskning med angivna referenser i 42.

> I dåvarande Krisberedskapsmyndighetens regleringsbrev för budgetåret 2007 gav regeringen myndigheten i uppdrag att ta fram en nationell handlingsplan för samhällets informationssäkerhet (Fö2009/2566/SSK). Handlingsplanen redovisades till regeringen i april 2008. Enligt handlingsplanens tredje åtgärdsförslag skulle den nationella strategin som hade redovisats av InfoSäkutredningens delbetänkande uppdateras.

Utredaren avfärdar sedan citatet från regeringsskrivelsen:

SOU 2015:23, s. 206

> Utredningen menar att den av regeringen tidigare redovisade strategin (prop. 2001/02:158) liksom den i betänkandet SOU 2005:42 föreslagna i grunden var riktiga. Utredningen anser dock att de båda har sökt åtgärda samtliga problem och utmaningar i hela samhället i ett sammanhang, något som ställer genomföranden inför överväldigande utmaningar.

Det här är otillfredsställande. Det enda som förefaller ”överväldigande” är utredarens oförmåga att leta fram och utvärdera IT-säkerhetsstrategier.

Alternativ

Krav från sakkunniga svenska experter på en IT-haverikommission (”Så avslöjar du it-projekten som riskerar att haverera”, *Dagens Nyheter*, 20 maj 2015) har inte hörsammats, vare sig av innevarande utredning eller tidigare. Erfarenheten från Nederländerna av den stora IT-haveriutredning landets riksdag färdigställde 2014 är dock goda. Det finns anledning för Sverige att överväga en liknande insats.
SOU 2015:23, s. 292

Utredningen har haft i uppdrag att ”föreslå övergripande mål för samhällets informationssäkerhetsarbete, och hur Sverige ska upprätthålla säkerhet och integritet i samhällsviktig it-infrastruktur”. Teknisk standardisering för bättre IT-säkerhet för enskilda har fått fäste i flera betydelsefulla standardiseringsorgan[27] och lyfts av tidigare svenska statliga utredningar.[28] Internationella organisationer som verkar för mänskliga rättigheter har lyft den tekniska standardiseringens roll för individers säkerhet – då särskilt när stater påverkar standardisering av teknologi i negativ riktning (vilket det med avseende på bland annat Europarådets och Förenta nationernas observationer kan anses finnas en betydande risk för i Sverige).[29]

Datainspektionens rekommendationer om inbyggt integritetsskydd[30] och säkerhet vid personuppgiftsbehandling[31] ligger i linje med det amerikanska standardiseringsinstitutet NIST:s föreslagna rekommendationer för informationssäkerhet[32] men har i praktiken inte tilldelats någon uppmärksamhet, vare sig i denna utredning eller annorstädes.

Detta framgår inte minst av Justitiedepartementets utredning om inbyggt integritetsskydd i socialförsäkringen – som föreslår ändra lagen för att passa IT-systemen, istället för att göra IT-systemen integritetsfrämjande[33] (se bland andra Datainspektionens remissvar på utredningen[34]). Datainspektionens råd om

[27] Bland annat Internet Engineering Taskforce (IETF) och World Wide Web Consortium (W3C), men se till exempel också CEN/CENELEC/ETSI: Cyber Security Coordination Group (CSCG) White Paper No. 01, ”Recommendations for a Strategy on European Cyber Security Standardisation”

[28] SOU 2007:47 Den osynliga infrastrukturen – om förbättrad samordning av offentlig IT-standardisering.

[29] CommDH/IssuePaper(2014) 1. 8 december 2014. *The rule of law on the Internet and in the wider digital world. Issue Paper published by the Council of Europe Commissioner for Human Rights*; FN:s kammare för mänskliga rättigheter, 27 sessionen. Rapport A/HRC/27/37 av den 30 juni 2014; Rapporter om mänskliga rättigheter till FN:s generalförsamling, 69 sessionen. Rapport A/69/397 av 23 september 2014.

[30] Datainspektionen, vägledning, *Inbyggd integritet – Privacy by design*, januari 2012.

[31] Datainspektionens allmänna råd, *Säkerhet för personuppgifter*, reviderad november 2008.

[32] Recommendations of the National Institute of Standards and Technology. Special Publication 800-122. *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*.

[33] SOU 2014:67. Inbyggd integritet inom Inspektionen för socialförsäkringen

[34] Datainspektionens remissyttrande till SOU 2014:67, *Inbyggd integritet inom Inspektionen för socialförsäkringen*, februari 2015.

bättre säkerhet och integritet vid personuppgiftsbehandling har inte heller följts upp i utredningen om en ny myndighetsdatalag,[35] i Energimarknadsinspektionens arbete med smarta elmätare,[36] i utarbetningen av strategier för framtidens e-Hälsa,[37] eller vid utformningen av ett nytt e-legitimationssystem för Sverige.[38] Datainspektionens råd om bättre säkerhet och integritetsskydd förefaller inte ha varit ledande för vare sig Myndigheten för samhällsskydd och beredskaps arbete, eller E-delegationens arbete, eller Digitaliseringskommissionens arbete, eller Sveriges kommuner och landstings arbete. Givet att Datainspektionens råd är både kortfattade och konkreta, hade det – om utredningen så som den påstår identifierat att tidigare strategier varit alltför ”överväldigande utmaningar”’ – varit på sin plats för utredningen att lyfta dessa som goda exempel.

Det grundläggande problemet – som är välkänt, etablerat och diskuterat i IT-säkerhetsforskningen sedan 1990-talet – är att det saknas anledningar för både företag och myndigheter att investera i bättre IT-säkerhet.[39] Det är helt enkelt billigare och enklare att tillhandahålla osäkra och icke-fungerande tjänster än att bygga säkra och fungerande tjänster.

Ett problem för privatpersoner och konsumenter i IT-miljöer är att komplexa värdekedjor ibland gör det svårt att koppla orsak med verkan. En medborgare som utsätts för besvärande reklam, identitetsstöld eller i värsta fall utpressning kommer inte i första hand att koppla besväret till en informationsläcka på en myndighet. Inte heller är det alltid uppenbart vilken av IT-tjänsterna i värdekedjan som brustit i ansvar när en konsument drabbas av obehagligheter.

Det är för det första svårt för privatpersoner att få reda på när saker går fel. Även om information om säkerhetsbrister rapporteras i medier finns det begränsade möjligheter för privatpersoner och konsumenter att agera på informationen. Bevisbördan för att någonting gått fel ligger i normalfallet på konsumenten eller medborgaren,[40] och i konsumentsammanhang saknas möjligheter att kräva tillräckligt stora skadestånd för att tjänsteleverantören ska få anledning att ändra sig.

Redan i början av 1990-talet drogs slutsatsen att starkare konsumenträtt ger mer säkerhet i vanligt använda elektroniska system för samma mängd pengar som annars skulle leda till sämre säkerhet.[41] Forskning stödjer att medvetna åtgärder för att ge privatpersoner och konsumenter bättre tillgång till information om säkerhetsproblem i IT-system hjälper dem att utkräva ansvar.[42]

Det har också uppstått en omfattande verksamhet i privat sektor kring att prata öppet om säkerhetsproblem i syfte att få dem åtgärdade snabbare (”responsible disclosure”).[43] Denna verksamhet har byggts upp samtidigt som

[35] SOU 2015:39, Myndighetsdatalag.

[36] Energimarknadsinspektionen, *Funktionskrav på framtidens elmätare*, Ei R2015-09

[37] SOU 2014:23 Rätt information på rätt plats vid rätt tid; SOU 2015:32 *Nästa fas i e-hälsoarbetet*

[38] SOU 2010:104 E-legitimationsnämnden och Svensk e-legitimation; jämför emellertid också material på E-legitimationsnämnden egen hemsida: http://www.elegnamnden.se/4.3aa8c78a1466c584587112e.html

[39] Se den pedagogiska och kortfattade framställningen i introduktionen till Rainer Böhme, *Vulnerability Markets – What is the economic value of a zero-day exploit?*

[40] Nicholas Bohm et al, ”Electronic Commerce: Who Carries the Risk of Fraud?”, 2000 (3) The Journal of Information, Law and Technology (JILT); jfr också behandlingen av bevisbördesfrågor i Lennart Johansson, *Banker och internet*, Iustus förlag (Stockholm) 2006; Jean-Francois Blanchette, *Burdens of Proof: Cryptographic Culture and Evidence Law in the Age of Electronic Documents*, MIT Press, 2012

[41] Se fotnot 3.

[42] Sasha Romanosky, David Hoffman, Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation* i WEIS 2010.

[43] Google Project Zero innebär att ett antal säkerhetsexperter får i uppdrag att leta efter buggar och säkerhetshål i mjukvaror som dels tillhör Google själva, men också sådana buggar och säkerhetshål som kan upptäckas i andra företags mjukvaror. http://googleprojectzero.blogspot.se/; Pwnie Awards är en årlig tävling för den som avslöjat ett särskilt värdefullt och signifikant säkerhetsproblem i någon kommersiell eller offentlig IT-lösning. http://pwnies.com/about/; Pwn2Own är en årlig tävling som syftar till att ge säkerhetsforskare möjligheter att avslöja och uppdagar säkerhetsfel så att dessa kan åtgärdas. https://cansecwest.com/post/2015-03-08-14:42:30_PWN2OWN_2015; Jämför emellertid också öppna diskussioner om nya

många amerikanska delstater har antagit lagstiftning om incidentrapportering direkt till privatpersoner i syfte att stärka deras möjligheter att utkräva ansvar.

Att stärka konsumentmakten är inte nödvändigtvis tillräckligt. Nederländernas riksdag lät 2014 genomföra en storskalig utredning av statliga IT-projekt[44] och utarbetade därigenom rekommendationer för hur den statliga upphandlingen kan förbättras både med avseende på medborgarnas upplevelser och med avseende på statens egna funktioner. Sverige bör överväga att följa Nederländernas exempel med en IT-haverikommission.

Redan år 2001 utarbetade IT-kommissionen flera rekommendationer för bättre IT-säkerhet i Sverige.[45] Utredningen återknyter varken till IT-kommissionens rekommendationer eller hur de har följts upp sedan de tillkom.

2008 utfärdade Datainspektionen rekommendationer om säkerhet vid personuppgiftsbehandling[46] och 2012 utfärdade Datainspektionen vidare rekommendationer om inbyggt integritetsskydd.[47] Utredningen återknyter inte till Datainspektionens rekommendationer eller hur de har följts upp.

Utredaren har bara genom ett direktkopierat citat från regeringsskrivelsen om stärkt samverkan från 2009 berört tidigare erfarenheter av strategiska insatser för bättre IT-säkerhet:

SOU 2015:23, s. 205/Samhällets krisberedskap – stärkt samverkan för ökad säkerhet (skr. 2009/10:124), s. 66

> I dåvarande Krisberedskapsmyndighetens regleringsbrev för budgetåret 2007 gav regeringen myndigheten i uppdrag att ta fram en nationell handlingsplan för samhällets informationssäkerhet (Fö2009/2566/SSK). Handlingsplanen redovisades till regeringen i april 2008. Enligt handlingsplanens tredje åtgärdsförslag skulle den nationella strategin som hade redovisats av InfoSäkutredningens delbetänkande uppdateras.

Regeringsskrivelsen avfärdas sedan så här:

SOU 2015:23, s. 206

> Utredningen menar att den av regeringen tidigare redovisade strategin (prop. 2001/02:158) liksom den i betänkandet SOU 2005:42 föreslagna i grunden var riktiga. Utredningen anser dock att de båda har sökt åtgärda samtliga problem och utmaningar i hela samhället i ett sammanhang, något som ställer genomförandena inför överväldigande utmaningar.

Det enda som förefaller ”överväldigande” är emellertid utredarens oförmåga att leta fram och utvärdera IT-säkerhetsstrategier. Sverige borde låta sig inspireras av andra EU-länder som haft liknande problem med genomförandeunderskott i IT-säkerhetsstrategierna.

Kapitel 9.2: Dataskydd.net avstyrker utredningens förslag om ansvar, styrning, samordning och tillsyn.

Myndigheter som Datainspektionen, Post- och telestyrelsen, Konsumentverket, Statskontoret, Konsumentombudsmannen, samt Konkurrensverket tillmäts

säkerhetsbrister på branschkonferenser så som DefCon eller BlackHat, eller den europeiska konferensen Chaos Communication Congress, m. fl.; Ett väl utrett och undersökt område är också så kallade *bug bounty awards*. Man kan hitta en sammanställning av befintliga *bug bounty awards* på den här hemsidan: https://bugcrowd.com/list-of-bug-bounty-programs

[44] Tweede kamer. Temporary Committee on Government ICT Projects Final Report. 13 oktober 2014

[45] IT-kommissionen, Observatoriet för Informationssäkerhet. PM 1:2001, ”Grundskydd i datorer och programvaror”; IT-kommissionen, Observatoriet för informationssäkerhet. PM 39:2001, ”Hantering av IT-incidenter, vem gör vad och hur?”

[46] Datainspektionens allmänna råd, *Säkerhet för personuppgifter*, reviderad november 2008.

[47] Datainspektionen, vägledning, *Inbyggd integritet – Privacy by design*, januari 2012.

ingen relevans alls. Detta trots att dessa myndigheter är *de facto* standardsättare och föreskriftsamordnare för de aktörer i näringslivet som utredningen själv identifierat som mest relevanta för bättre IT-säkerhet i utredningens kapitel 4.

Utredningen blandar istället ihop ”kris” med ”normaltillstånd”. Utredningens förslag förvärrar begreppsförvirringen mellan ”krig” och ”fred” som gör sig gällande i allt för många diskussioner om informationssäkerhet. Utredningen förslag vilar sig uteslutande på krishanterande myndigheters, som Myndigheten för samhällsskydd och beredskap, och försvarsrelaterade myndigheters, som Försvarsmakten, utsagor och observationer.

Detta trots att myndigheterna som utredningen bortser från tidigare har utarbetat bra, tydliga rekommendationer som ligger i linje med tillgänglig forskning.[48] Märk särskilt att Datainspektionens riktlinjer för inbyggt integritetsstöd[49] får medhåll i amerikanska tekniska standardinstitutets (NIST) rekommendationer för IT-säkerhet.[50]

I kontexten av tillsyn är det också tveksamt om utredningen kan antas göra rätt val genom att ignorera det mesta av det arbete som hittills skett på området.

En av utredningens mer besvärande brister vid val av tillsynsmyndigheter är att vissa av myndigheterna själva aspirerar på att verka i enlighet med det som utredaren i kapitel 4 beskriver som ”antagonistiska hot”. Polisen och åklagarmyndigheten har i närtid uttryckt önskemål om att få bidra till marknaden för ”programvara särskilt utvecklad för it-angrepp.”[51] Även underrättelsetjänsten[52] och försvarsmakten[53] antyder att de vill ha tillgång till sådana produkter.

SOU 2015:23, s. 70

Bortsett från att de brottsbekämpande myndigheterna i samhället inte ska utgöra ”antagonistiska hot” mot viktiga funktioner i samhället, finns även internationell doktrin som talar för att utredaren borde ha granskat denna utveckling noggrannare.[54]

Oligopol

I kapitel 4 tar utredaren upp de särskilda svårigheter som uppstår när värdekedjorna i elektronikbranschen blir mer komplexa. Utredaren tar också upp problemet med att ett fåtal marknadsaktörer dominerar tjänsteleveranserna och produktutvecklingen. Den amerikanske IT-rättsjuristen Tim Wu har beskrivit problemet i termer av vertikal integration och oligopol.[55] Han drar slutsatsen att även vertikal integration kan leda till horisontell dominans, och att starkt marknadsinflytande på en viss nivå i värdekedjan kan översättas till ett starkt inflytande även på andra nivåer i värdekedjan.

---

[48] En ej uttömmande lista över tidigare svenska säkerhetsstrategier: PM 1:2001, IT-kommissionen, *Grundskydd i datorer och programvaror*; PM 39:2001, IT-kommissionen, *Hantering av IT-incidenter, vem gör vad och hur?*; PTS-ER-2006:12 *Strategi för ett säkrare Internet i Sverige*; Datainspektionens allmänna råd, *Säkerhet för personuppgifter*, reviderad november 2008

[49] Datainspektionen, vägledning, *Inbyggd integritet – Privacy by design*, januari 2012.

[50] Recommendations of the National Institute of Standards and Technology. Special Publication 800-122. *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*.

[51] SOU 2012:44 *Hemliga tvångsmedel*, kapitel 14.2 om hemlig dataavläsning; Åklagare och Säpo vill införa nytt tvångsmedel – hemliga ”spiontrojaner” i datorer”, *Dagens Juridik*, 24 april 2014.

[52] ”FRA hackar datorer – topphemligt projekt med NSA”, *Sveriges television* 11 december 2013.

[53] ”Försvarsministern: Vi ska kunna genomföra cyberattacker”, *Dagens Nyheter*, 18 mars 2015.

[54] Förenta nationernas generalförsamling . ”Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security” Rapport A/68/98 av 24 juni 2013.

[55] Tim Wu. *The Master Switch: The Rise and Fall of Information Empires*. Random House, november 2010, är en trevlig och populärjuridisk introduktion till ämnet.

För att undvika oligopolisering av viktiga marknader kan man hoppas på att det sker en utveckling av oligopolhanteringen i konkurrensrätten.[56] EU-kommissionens strategi på 1990-talet var att hantera oligopolisering av marknader genom rigorös tillämpning av sammanslagningsförordningen.[57] Denna strategi övergavs emellertid i början av 2000-talet.[58]

Kopplingen mellan oligopolisering och informationssäkerhet är enbart indirekt, men som utredningen lyfter i sin genomgång av marknadsläget är den ändå relevant. Ju färre aktörer som kämpar om marknadsfördelar, och ju mer inlåsta dessa aktörers kunder är till aktörernas specifika lösningar, desto sämre möjligheter har man att få en dynamisk utveckling mot bättre säkerhet.

Fenomenet med oligopol syns i dag lättast på konkurrensrättens oförmåga att hantera konkurrensbegränsningar på mobiloperatörsmarknaden, Googles och Apples plattformar för mobila applikationer, men går igen i Intels dominans för datachip eller på marknaderna för IT-tjänster. EU-kommissionens databaser över tidigare sammanslagningsavgöranden[59] är en lärorik källa till information, både om de olika branschernas nuvarande sammansättning och om konkurrensrättens tillkortakommanden. Den pågående oförmågan från lagstiftare och utredare att betrakta de näringspolitiska aspekterna av IT, digitalisering och telekom leder till en förvärring av många av de problem samma lagstiftare och utredare säger sig undvika.

Klok sektorsreglering skulle ställa oligopolproblemen till rätta. Det har skett flera större diskussioner om konkurrensupprätthållande sektorsreglering i EU de senaste åren, den mest betydelsefulla varandes nätneutralitetsdiskussionerna, men av olika anledningar har det inte blivit uppenbart för vare sig lagstiftaren eller medborgarna att det i mångt och mycket handlar om konkurrensstärkande åtgärder. Från utredningens uppdrag framgår att även regeringen tänkt sig att utredaren skulle ta ett helhetsgrepp – trots det har viktiga frågor om marknadsdynamik och konkurrens fallit bort, på ett sätt som skadar regeringens målsättningar med utredningar.

I Kungliga vetenskapsakademien, *Scientific Background on the Sveriges Riksbank Prize in Economic Sciences in Memory of Alfred Nobel 2014. Jean Tirole: Market power och regulation. Compiled by the Economic Sciences Prize Committee of the Royal Swedish Academy of Sciences* beskrivs att den europeiska konkurrensrätten varit långsammare på att anpassa sig till insikten att vertikal integration kan vara lika konkurrenshämmande som horisontell integration (särskilt på marknader med starka nätverkseffekter) än de amerikanska motsvarigheterna

Kapitel 9.3: Dataskydd.net avstyrker utredningens förslag om staten som tydlig kravställare.

Utredningens förslag att låta centrala myndigheter agera ”tydliga kravställare” har redan prövats och misslyckats i fyra decennier.

I utredningarna ADB och samordning[60] och ADB och sårbarhet[61] som utfördes på 1970-talet identifierade både lagstiftare och utredare liknande problem som de som utredningen om informationssäkerhet har identifierat. Man föreslog – och genomförde – därför en förflyttning av makten att kravställa från landets myndigheter till Statskontoret, i förhoppningen om att en central myndighet skulle ha bättre möjligheter att ställa tydliga krav och förbättra möjligheterna till standardisering av ofta använda produkter. Hänvisningar till central kravställning för bättre informationssäkerhet har sedan återkommit

[56] Se bl.a. Nicolas Petit, ”The Oligopoly Problem in EU Competition Law”, 5 februari 2012.

[57] Juan F. Briones Alonso. ”Economic assessment of oligopolies under the Community Merger Control Regulation”, European Competition law Review (Vol 4, Issue 3)”, 5 juni 1993.

[58] Rådets förordning (EG) nr 1/2003 av den 16 december 2002 om tillämpning av konkurrensreglerna i artiklarna 81 och 82 i fördraget (Text av betydelse för EES.)

[59] http://ec.europa.eu/competition/sectors/ICT/cases.html

[60] SOU 1976:58, ADB och samordning.

[61] SOU 1979:93. ADB och samhällets sårbarhet.

regelbundet.[62]

Utredningen borde givet de tidigare erfarenheterna ha utforskat alternativ, till exempel genom att konsultera forskningsläget[63] och myndighetsrapporter[64] om problem för IT-säkerhet ur en ekonomisk och konsumenträttslig synvinkel.

Utredningen påtalar att det är ett problem när allt för få företag kontrollerar en allt för stor del av marknaden. Det här problemet är också känt sedan ungefär fyrtio år tillbaka då det undersöktes grundligt i utredningarna *Data och näring I*[65] och *Data och näring II*.[66]

I de tidigaste utredningarna om datasystem framgår kopplingarna mellan central kravställning och höga marknadskoncentrationer tydligt. Ett alternativ för att öka konkurrensen och få in fler aktörer på marknaden presenteras dock i utredningen *Den osynliga infrastrukturen* från 2007: förslaget om en strategi för öppna standarder i offentlig verksamhet har dock inte följts upp.

SOU 2007:47 Den osynliga infrastrukturen – om förbättrad samordning av offentlig IT-standardisering

I utredningsuppdraget ingick det att granska svenskt IT-säkerhetsarbete i förhållande till EU-kommissionens nya dataskyddsförslag. EU-kommissionens dataskyddsförslag från 2012 är inriktat på att ställa enhetliga, tydliga krav på myndigheter och privat sektor. Sveriges regering har motarbetat dessa enhetliga, tydliga krav, bland annat i syfte ”ge [myndigheterna] likartade förutsättningar att utföra sitt uppdrag [som de har idag] och att det i övrigt lämnas åt medlemsstaterna att reglera den nationella förvaltningen.”[67]

Samtliga marknader som utredningen behandlar regleras inte bara ekonomiskt utan också i sin administrativa utformning.[68] Staten ställer redan *de facto* krav på alla verksamheter som hanterar personuppgifter genom särregleringar, förordningar och myndighetsspecifika föreskrifter. Dessa begränsar myndigheternas handlingsutrymme att tänka på IT-säkerhet när de upphandlar IT-system. Detaljregleringen begränsar den privata sektorns möjligheter att utforma IT-system enligt eget säkerhetsomdöme: det är inte säkert att lagstiftaren bäst kan förutse vilka hot och komplikationer som kan uppstå i en databas. Den svenska särregisterregleringen har kallats ”splittrande och föråldrad” av en svensk offentlig utredning 2012.[69] Den IT-haverikommission som Nederländernas riksdag lät genomföra 2014 uppmärksammade precis den sorts problem som uppstår när man förlitar sig för mycket på detaljreglering uppifrån[70] och lyckades föreslå åtgärder. Sverige bör också överväga att genomföra en liknande utredning.

Utredningen borde ha granskat dessa politiska omständigheter i förhållande till teknisk standardisering för bättre IT-säkerhet. Det finns goda anledningar att tro att lagstiftaren inte har den snabbhet och insikt som krävs för att på bäst sätt garantera datasäkerhet i myndigheternas dagliga verksamhet, och att

[62] Se bl.a. PM 1:2001, IT-kommissionen, Observatoriet för Informationssäkerhet, ”Grundskydd i datorer och programvaror”.

[63] Se ovan fotnot 15.

[64] Se ovan fotnot 73; se också ENISA (2008). Ross Anderson, Rainer Böhme, Richard Clayton, och Tyler Moore. *Security, Economics, and the Internal Market.*

[65] SOU 1973:6 Data och näringspolitik

[66] SOU 1974:10 Data och näringspolitik 74

[67] Faktapromemoria till riksdagen, 27 februari 2012; Rådspromemoria framställd till riksdagen 2 mars 2015

[68] Se t.ex. angivna referenser i fotnot 36, 37 och 38.

[69] SOU 2012:90. Överskottssinformation vid direktåtkomst.

[70] Tweede kamer. *Temporary Committee on Government ICT Projects Final Report* 13 oktober 2014.

tydliga, enkla och bindande principer för myndigheterna (utformade t.ex. efter Datainspektionens skrift om inbyggt integritetsskydd[71] från 2012) vore att föredra. Datainspektionens råd om inbyggt integritetsskydd ligger nära amerikanska standardiseringsinstitutet National Institute of Standards and Technology:s (NIST) föreslagna rekommendationer för informationssäkerhet.[72]

Utredningen föreslår certifiering som en möjlig framkomlig väg till bättre IT-säkerhet. Myndigheten för samhällsskydd och beredskap samt Försvarets materielverk ska ansvara för att produkter som används inom statlig förvaltning uppfyller vissa förutbestämda mål.

Certifiering är emellertid ett intuitivt olämpligt instrument att förlita sig på inom marknader med korta produktcykler och snabba utvecklingscykler: för att en viss mjukvara eller ett visst system ska certifieras, måste det befinna sig i ett visst tillstånd kring vilket certifieringstesterna kan genomföras. Det innebär att man efter certifieringsprocessens start inte kan laga säkerhetshål och förbättra upptäckta brister, utan att behöva ta om certifieringsproceduren från början. På en marknad där nya hot och säkerhetsproblem upptäcks varje vecka är detta olyckligt.

Certifieringskrav försenar också införande och lansering av nya lösningar, tjänster och produkter. Eftersom testerna för certifiering med nödvändighet tar tid finns en risk att de färdigcertifierade produkterna redan är otidsenliga när de får börja användas.

Det är ett säkert recept för att tappa tid, pengar, flexibilitet och säkerhet. Utredaren borde ha insett detta. En alternativ modell är självcertifiering i kombination med tillsyn och kraftiga viten då felaktigheter upptäcks. Incidentrapportering direkt till berörda privatpersoner kan också tänkas vara effektivt, eftersom det för både privat och offentlig sektor då blir en fråga om att minimera *goodwill*-förluster när bristande säkerhetsåtgärder inte åtgärdas. De huvudsakliga linjerna i varje hållbar lösning är förmåga till snabb och kontinuerlig förbättring, oavsett i hur små steg. Transparens mot privatpersoner som byggsten är ett tacksamt hjälpmedel eftersom överföringskostnader för information till privatpersoner genom internets intåg i hushållen blivit i stort sett gratis, för både offentlig sektor och marknadens aktörer, samtidigt som ett gott anseende blivit viktigare för alla samhällets aktörer.

Ett första utkast till ett bättre system: rapportering av sårbarheter i IT-system till berörda medborgare (då det gäller myndigheters IT-system) och konsumenter (då det gäller kommersiella IT-system), samt viten vid utebliven transparens och uteblivet åtgärdande av upptäckta problem. Fördelen med transparens som grund för ett säkerhetssystem är att det aldrig är omöjligt att öppet deklarera en sårbarhet som är känd. Transparensen innebär i sig ett incitament att åtgärda problemet. Vid särskilt komplicerade fall där åtgärdandet tar tid, kan man införa en karenstid som får tillses av en ansvarig myndighet (till exempel Post- och telestyrelsen eller Datainspektionen). Om företaget eller myndigheten misslyckas med transparens gentemot berörda privatpersoner kan vite utdömas. Om källkoden redan är öppen och tillgänglig, och sårbarheter redan regelbundet publiceras via kanaler som privatpersoner enkelt har tillgång till, så utdöms inget vite.

På detta sätt påverkas marknadens nuvarande funktion minimalt, man behåller flexibiliteten i systemet, ger konsumenter och privatpersoner mer makt och inflytande över de IT-system som påverkar dem och får samtidigt ett incitament på både marknaden och myndigheter för självförbättring. Forskningen talar inte emot denna modell och de huvudsakliga åtgärderna i rätt riktning har redan föreslagits i Sverige av PTS 2006.

Kapitel 9.5: Dataskydd.net avstyrker utredningens förslag om incidentrapportering.

Dataskydd.net föreslår istället en ”individ-centrisk” incident- och sårbarhetsrapportering.

Utredningens föreslagna incidentrapportering är byråkratisk och tungrodd, och kan inte antas effektivt uppnå målsättningarna med systemet att skapa bättre IT-säkerhet. Givet forskningsläget och den långsiktiga utvecklingen i amerikanska delstater, verkar istället Post- och telestyrelsen ha varit helt rätt ute i sin strategi för ett säkrare internet i Sverige från 2006.[73] Tyvärr har PTS

[71] Datainspektionen, vägledning, *Inbyggd integritet – Privacy by design*, januari 2012.

[72] Recommendations of the National Institute of Standards and Technology. Special Publication 800-122. *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*.

[73] Post- och telestyrelsen. *Strategi för ett säkrare Internet i Sverige*. PTS-ER-2006:12

strategi från 2006 inte följts upp eller utvärderats, vare sig av denna utredning eller någon av utredningarna utredningen hänvisar till.

Utredaren förlitar sig i utformningen av sitt förslag på incidentrapportering fullständigt på Myndigheten för samhällsskydd och beredskaps (MSB) rapporter. MSB:s rapporter är dåligt utförda och ovetenskapliga. MSB har som ”grundläggande utgångspunkt för förslaget /…/ att inrapporteringen ska ske till MSB” eftersom att MSB har fått ett ”utvidga[t] mandat”. Denna dåliga motivering gav upphov till en kompetensstrid mellan flera brotts- och krisbekämpande myndigheter, varför MSB:s andra utredning föreslår en ”arbetsgrupp bestående av representanter för MSB, Säkerhetspolisen och Rikskriminalpolisen”. Vidare ägnas hela avdelning 5.2 i MSB:s andra rapport åt att diskutera vad som ska rapporteras.

s. 15, Myndigheten för samhällsskydd och beredskap (2011). *System för obligatorisk IT-incidentrapportering för statliga myndigheter.*

s. 16, Myndigheten för samhällsskydd och beredskap (2012). *Nationellt system för it-incidentrapportering.*

MSB och övriga myndigheter har bortsett från erkänd IT-säkerhetsforskning som menar att det är möjligheter för de som drabbas att ställa ansvariga till svars som gör skillnad.[74] Att sätta individen i centrum för incidentrapporteringen har många fördelar som uppenbarligen inte manifesterar sig i det föreslagna systemet: 1) Användare får en möjlighet att parera negativa konsekvenser mot dem själva av att en säkerhetsrisk har uppstått; 2) Användare ges en möjlighet att utkräva ansvar – antingen genom att kräva skadestånd (till exempel av en myndighet), eller genom att byta leverantör – om en viss leverantör inte visar sig leva upp till vad som utlovats, eller genom att anmäla brott; 3) Användare får på sikt en bättre förståelse för vilka aktörer den interagerar med.

Utredaren borde ha bedömt arbetsinsatsen för incidentrapporteringen i förhållande samhällsnyttan. Att skriva incidentrapporter kommer att vara ett tråkigt och tidskrävande uppdrag för de myndigheter som sammanställer dem. Det kommer att vara tråkigt och tidskrävande att sammanställa incidentrapporterna hos MSB. Varken rapporterna eller diagrammen kommer att nå de konsumenter som använder IT-systemen, eller de medborgare som interagerar med myndigheter som använder IT-system. Få personer kommer att läsa MSB:s sammanställningar av incidentrapporterna, och för att se till att någon dragen slutsats efterlevs kommer det att krävas ytterligare administration, kontroll och byråkrati. Kostnaden för detta system är högt, och nyttan är otydlig.

Frågan om vilken information som ska rapporteras till privatpersoner som berörs av IT-systemen är enklare än motsvarande fråga för rapporter mellan myndigheter. Privatpersonerna behöver sådan information som ger dem möjlighet att gå vidare med ansvarsutkrävande. Erfarenheten av dataskydd, skadestånd, offentlig rätt och konsumenträtt är i praktiken idag så stora att man på förhand kan förutse vilken sorts information privatpersoner skulle behöva.

I flera amerikanska delstater har man infört obligatorisk incidentrapportering för företag och myndigheter som riktar sig till de privatpersoner som berörs av incidenten. Först ut var Kalifornien 2002. Det finns mycket forskning kring hur konsumenter ställer företag till svars för att inte ha åtgärdat säkerhetsproblem.[75] Forskningen också att konsumenter är mer benägna att ställa sådana aktörer till svars, som också MSB i sina utredningar håller med om att det är extra viktigt att medborgarna har förtroende för.

Kaliforniens incidentrapporteringsplikt gör undantag för företag som på ett adekvat sätt skyddar informationen som läcks. Det har bland annat haft effekten att flera av de största IT-företagen i världen har infört bättre säkerhetsåtgärder (till exempel kryptering) vid till exempel inloggning. Det går att dra många viktiga slutsatser av de amerikanska delstatslagarna och de effekter de har haft på näringslivet och IT-säkerheten, men utredningen lämnar allt detta åt sidan. För att IT-säkerhet ska bli ett realistiskt mål för Sverige behöver även incidentrapporteringen vara smart, och i vilket fall inte helt utesluta medborgare och konsumenter.

Ett exempel på utfall av incidentrapportering till konsumenter är *Privacy Rights Clearinghouse*, en amerikansk konsument-inriktad hemsida om dataläckor och IT-incidenter. Se https://www.privacyrights.org/data-breach, Se också sidan ”*Have I been pwned?*”, som dock inte ger meningsfulla sätt att aggregera data eller ställa ansvariga aktörer till ansvar. https://haveibeenpwned.com/

MSB hade kunnat utreda incidentrapportering, men valde att exkludera alla erfarenheter från sitt faktaunderlag som inte stödjer att specifikt krisberedande och brottsbekämpande myndigheter ska ges ensamrätt till information. Mönstret följer en ”europeisk tradition” av att inte lita på privatpersoners förmåga att aktivt engagera sig för bättre IT-infrastruktur. Också EU har varit tveksamma inför att införa incidentrapportering direkt till privatpersoner – både i direktivet om integritet och elektronisk kommunikation,[76] och i den allmänna förord-

[74] Se referenser i fotnot 15 och 16, men särskilt ENISA (2008). Ross Anderson, Rainer Böhme, Richard Clayton, och Tyler Moore. *Security, Economics, and the Internal Market* och Rainer Böhme, *Vulnerability Markets – What is the economic value of a zero-day exploit?*.

[75] Sasha Romanosky, David Hoffman, Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation*, WEIS 2010; David Solove, ”Are People Really Harmed By a Data Security Breach?”, Concurring Opinions, 22 september 2010; m. fl.

[76] Direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation som ändrad av direktiv 2009/136/EG

ningen om uppgiftsskydd[77] har man istället låtit incidentrapporter filtreras genom en ansvarig statlig myndighet (Post- och telestyrelsen, respektive Datainspektionen) innan den drabbade privatpersonen ges möjlighet att agera på incidenten.

Någon plikt att rapportera sårbarheter finns inte i USA, men flera större IT-företag har skapat initiativ för så kallade *bug bounties* eller *responsible disclosure*.[78] Målsättningen med dessa är att få säkerhetsproblem kända och åtgärdade så snabbt som möjligt. Åtgärderna är inte identiska med, men verkar likna den sårbarhetsrapportering som Post- och telestyrelsen föreslog redan 2006.[79] Om utredningen inte hade kört fast på MSB:s rapporter hade den kunnat undersöka möjligheterna att vidareutveckla detta inom ramen för konsumentskydd och dataskydd.

Kapitel 9.6: Dataskydd.net avstyrker utredningens förslag om ratificering av Europarådets IT-brottskonvention och förslaget om översyn av bestämmelser om tvångsmedels [sic] i den digitala miljön.

Angående utredningens förslag att se över informationsutbyte och tvångsmedels kan nämnas att regeringen de senaste åren har utrett brottsbekämpning i och på digitala miljöer i SOU 2012:44,[80] SOU 2012:85,[81] SOU 2012:95,[82] SOU 2013:39,[83] och SOU 2015:31.[84] Till detta kan läggas flertalet utredningar från 2000-talets tidiga år[85] samt utredningen om överskottsinformation vid direktåtkomst.[86] Det är begråtansvärt att man efter fler än 2 000 sidors utredningstext på bara tre år fortfarande upplever ”stora kunskapsluckor och svarta fält avseende hur de existerande tvångsmedlen kan, får och ska användas i den digitala miljön”. För många och för långa utredningar minskar transparensen i beslutsfattandet. I det här fallet framstår kravet på vidare utredningar mer som en fiskeexpedition för att få återlyfta förslag som redan avfärdats av lagstiftaren.

SOU 2015:23, s. 265

Särskilt om Europarådets IT-brottskonvention

De länder i EU som inte har implementerat Europarådets konvention om IT-brottslighet (”IT-brottskonventionen”) är de medlemsländer som har en framgångsrik IT-industri: Sverige och Irland.[87] Svenska politiker bör dra lärdom av det sällskap de befinner sig i.

Både Europarådet och FN har varnat för att informationssamhällets infrastruktur efter krav från brottsbekämpande myndigheter anpassas för kränkning-

Organisationen OSCE:s forum för unga ledare efterfrågade våren 2015 en omförhandling av IT-brottskonventionen i sin helhet, så att nya uttryck för politiskt engagemang så som hacktivism otvetydigt ska falla utanför straffrättens område (OSCE Office for Democratic Institutions and Human Rights. *Promoting and Increasing Youth Political Participation and Civic Engagement in the OSCE Region*. Youth Leadership Forums, Warsaw 16-17 June and 13-14 November 2014).

[77] Förslag till Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning) – 2012/0011 (COD)

[78] Se fotnot 43.

[79] Se ovan fotnot 73.

[80] SOU 2012:44 Hemliga tvångsmedel mot allvarliga brott

[81] SOU 2012:85, Avlyssning mot grova vapenbrott?

[82] SOU 2012:95 Spionerі och annan olovlig underrättelseverksamhet

[83] SOU 2013:39 Europarådets konvention om it-relaterad brottslighet. Utredningen om it-brottskonventionen.

[84] SOU 2015:31 Datalagring och integritet

[85] SOU 2005:38. Tillgång till elektronisk kommunikation i brottsutredningar m.m.; SOU 2006:98, Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel, m.m.; SOU 2007:76. Lagring av trafikuppgifter för brottsbekämpning

[86] SOU 2012:90 Överskottsinformation vid direktåtkomst

[87] Se listan över stater som undertecknat och ratificerat IT-brottskonventionen på http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG

ar av mänskliga rättigheter.[88] Det borde vara uppenbart att även de tvångsmedel som ingår i IT-brottskonventionen kan utgöra sådana krav.

Den tidigare utredning som gjorts om Europarådets IT-brottskonvention[89] fick stark kritik.[90] Det var delvis för att utredningen gick längre än vad konventionen kräver. IT-brottskonventionen är dock i sig själv bristfällig. Tvångsmedel och tvångsåtgärder i digitala miljöer är inte ekonomiskt neutrala: processrätten definierar på vilka sätt det är gynnsamt och vinstgivande att utveckla IT-plattformar.[91] Vi hamnar i situationen att IT-infrastrukturen och alla tillhörande affärsmodeller anpassas till de brottsbekämpande myndigheternas önskan om enkla och kravlösa utredningar, istället för att de brottsbekämpande myndigheterna anpassar sig till samhällets behov av rättssäkerhet och tröghet i deras myndighetsutövning.

Utredningen har delvis rätt i att de tidigare utredningsmassorna inte har åstadkommit annat än att förespråka de brottsbekämpande myndigheternas egenupplevda behov.[92] En förutsättningslös diskussion om hur hemliga tvångsmedel kan utformas för att inte bli *de facto* marknadsstyrande och standardsättande vore önskvärt, men utredningens förslag leder inte dit.

”Under krigsåren hade vi en polis för vilken ingen tog det politiska ansvaret,” skrev Tage Erlander i sin dagbok 1952.[93] ”Vi vill inte ha den tiden tillbaka.”

Förslag

Förslag till förordning för statliga myndigheters informationssäkerhet

Dataskydd.net efterlyser en individ-centrisk lagstiftning som gör det enklare för privatpersoner, både i sin roll som konsumenter och sin roll som medborgare, att utkräva ansvar vid bristande IT-säkerhet. Dataskydd.net har redovisat i det ovanstående att denna modell redan är framgångsrik (se ovan avsnitten om utredningens kapitel 5 och 9.5).

Förslag till förordning om ändring i säkerhetsskyddsförordningen (1996:633)

Dataskydd.net har ingenting emot att försvarsrelaterade myndigheter hjälper varandra att skapa administration.

---

[88] CommDH/IssuePaper(2014)1. 8 december 2014. *The rule of law on the Internet and in the wider digital world. Issue Paper published by the Council of Europe Commissioner for Human Rights*; FN:s kammare för mänskliga rättigheter, 27 sessionen. Rapport A/HRC/27/37 av den 30 juni 2014; Rapporter om mänskliga rättigheter till FN:s generalförsamling, 69 sessionen. Rapport A/69/397 av 23 september 2014.

[89] SOU 2013:39 Europarådets konvention om it-relaterad brottslighet

[90] Se t.ex. Datainspektionen Dnr 936-2013: Remiss av betänkandet Europarådets konvention om it-relaterad brottslighet (SOU 2013:39); Journalistförbundet Dnr 2013/92810: Remissyttrande Europarådets konvention om IT-relaterad brottslighet. Betänkande av utredningen om IT-brottskonventionen SOU 2013:39; Advokatsamfundet avstyrker förslag om IT-brottslighet, 24 september 2013; Justitieombudsmannen Dnr R 73-2013: Yttrande över betänkandet (SOU 2013:39) Europarådets konvention om it-relaterad brottslighet, m.fl.

[91] Se t.ex. James Boyle, *Foucault In Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors*, 1997, men jämför också resonemangen kring marknadsutveckling i SOU 2007:76 *Lagring av trafikuppgifter för brottsbekämpning*, då särskilt avsnitten som behandlar småföretagens möjligheter att uppfylla de brottsbekämpande myndigheternas krav.

[92] För en strukturerad och längre genomgång, se Naarttijärvi, Markus. *För din och andras säkerhet: Konstitutionella proportionalitetskrav och Säkerhetspolisens preventiva tvångsmedel*, Doktorsavhandling, Umeå universitet, 2013.

[93] Tage Erlander, *Dagböcker 1952*, Gidlunds förslag, 2002

Förslag till nationell strategi och åtgärdsplan för säkra kryptografiska funktioner

Dataskydd.net efterlyser en marknadsorienterad strategi som är bättre anpassad för de civila och näringsrelaterade verksamheter där strategin förväntas tillämpas. Dataskydd.net har redovisat i det ovanstående varför en sådan modell har bättre förutsättningar att vara framgångsrik än den föreslagna strategin (se ovan avsnitten om utredningens kapitel 9.1, 9.2 och 9.3).

Strategi för statens informations- och cybersäkerhet

Dataskydd.net efterlyser en individ-centrerad och marknadsorienterad strategi som är bättre anpassad för de civila och näringsrelaterade verksamheter där strategin förväntas tillämpas. Dataskydd.net efterlyser också politisk handling mot att både utredaren och dennes referensmyndigheter verkar exkludera den personliga integriteten från den vanliga rättighetskatalogen. Dataskydd.net har i avsnitten introduktion och avsnitten om utredningens kapitel 5, 9.1, 9.3 och 9.5 redogjort för anledningarna.

Dataskydd.net

Amelia Andersdotter
Ordförande

Källförteckning med webblänkar, där tillgängligt

De dokument som återfinns här nedan är de referenser från fotnoter eller marginalnoter som finns tillgängliga på nätet. Tyvärr gäller det inte alla remissyttrandets källdokument. Länkarna återfinns här nedan av estetiska skäl: det hade blivit plottrigt att istället föra in dem direkt i fotnoter.

Myndighetskällor

Datainspektionens allmänna råd. *Säkerhet för personuppgifter*. Reviderad november 2008. http://www.datainspektionen.se/Documents/faktabroschyr-allmannarad-sakerhet.pdf

Datainspektionen/Post- och telestyrelsen (2010). *Användning av trafikuppgifter i mobila innehållstjänster. Rapport efter avslutad tillsyn.* Datainspektionen 2010:1/PTS-ER-2010:01. https://www.pts.se/upload/Rapporter/Tele/2010/2010-1-mobila-innehallstjanster-100119.pdf

Datainspektionen, vägledning. *Inbyggd integritet – Privacy by design*. Januari 2012. http://www.datainspektionen.se/Documents/faktablad-inbyggd-integritet.pdf

Datatilsynet (Danmark). 31 juli 2015. Journalnummer: 2013-632-0050 ”Vedkommendes adgang til personoplysninger i systemer, som Rigspolitiet er dataansvarlig for” http://www.datatilsynet.dk/afgoerelser/seneste-afgoerelser/artikel/vedroerende-uvedkommendes-adgang-til-personoplysninger-rigspolitiets-jnr-2013-079-76/

Energimarknadsinspektionen, *Funktionskrav på framtidens elmätare* Ei R2015-09. ei.se/Documents/Publikationer/rapporter_och_pm/Rapporter%202015/Ei_R2015_09.pdf

ENISA (2008). Ross Anderson, Rainer Böhme, Richard Clayton, och Tyler Moore. *Security, Economics, and the Internal Market*. http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf

ENISA (2011). Panagiotis Trimintzios, Chris Hall, Richard Clayton, Ross Anderson och Evangelos Ouzounis. *Resilience of the Internet Interconnection Ecosystem*. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter-x/interx/report/interx-report

Europarådet. CommDH/IssuePaper(2014)1. 8 december 2014. *The rule of law on the Internet and in the wider digital world. Issue Paper published by the Council of Europe Commissioner for Human Rights* https://wcd.coe.int/ViewDoc.jsp?id=2268589&Site=COE

Europeiska datatillsynsmannens skrivelse om molntjänster och ansvarsfördelning för dataskydd mellan små och stora marknadsaktörer. ”Opinion of the European Data Protection Supervisor on the Commission’s Communication on ”Unleashing the potential of Cloud Computing in Europe””, 16 november 2012. https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf

EU-kommissionen. Sammanslagningsfall inom IKT-sektorn med vidare hänvisningar. http://ec.europa.eu/competition/sectors/ICT/cases.html

EU-kommissionen (2006). COM (2006) 744 final. Green Paper on the Review of the Consumer Acquis. http://ec.europa.eu/consumers/archive/cons_int/safe_shop/acquis/green-paper_cons_acquis_en.pdf

EU-kommissionen (2007) *Detailed analysis of responses to the European Commission Green Paper on Consumer Rights Reform* http://ec.europa.eu/consumers/archive/rights/detailed_analysis_en.pdf

EU-kommissionen (2012). Data Protection Reform. Se http://ec.europa.eu/justice/data-protection/

EU-kommissionen (2015). *Public consultation on contract rules for online purchases of digital content and tangible goods* http://ec.europa.eu/justice/newsroom/contract/opinion/150609_en.htm

Förenta nationernas generalförsamling . "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" Rapport A/68/98 av 24 juni 2013. http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-th pdf

Förenta nationerna. Tredje kammaren för mänskliga rättigheter, 27 sessionen. Rapport A/HRC/27/37 av den 30 juni 2014. http://ap.ohchr.org/documents/alldocs.aspx?doc_id=23880

Förenta nationernas generalförsamling. Rapporter om mänskliga rättigheter till FN:s generalförsamling, 69 sessionen. Rapport A/69/397 av 23 september 2014. http://www.ohchr.org/EN/newyork/Pages/HRreportstothe69thsessionGA.aspx

IT-kommissionen, Observatoriet för Informationssäkerhet. PM 1:2001 "Grundskydd i datorer och programvaror" http://www.itkommissionen.se/doc/24.html

IT-kommissionen, Observatoriet för informationssäkerhet. PM 39:2001 "Hantering av IT-incidenter, vem gör vad och hur?" http://www.itkommissionen.se/doc/94.html

Myndigheten för samhällsskydd och beredskap. *Pedagogik för samverkan i samhällskriser* https://www.msb.se/Upload/Insats_och_beredskap/Ledning_och_samordning/pedagogik%20f%c3%b6r%20samverkan%20i%20samh%c3%a4llskriser.pdf?epslanguage=sv

Myndigheten för samhällsskydd och beredskap (2011). *System för obligatorisk IT-incidentrapportering för statliga myndigheter*. https://www.msb.se/Upload/Nyheter_press/System_for_obligatorisk_IT-incidentrapportering_for_statliga_myndigheter.pdf

Myndigheten för samhällsskydd och beredskap. Februari 2012. "Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter – En studie av konsekvenserna i samhället efter driftstörningen hos Tieto i november 2011" https://www.msb.se/RibData/Filer/pdf/26170.pdf

Myndigheten för samhällsskydd och beredskap (2012). *Nationellt system för it-incidentrapportering* https://www.msb.se/Upload/Forebyggande/Informationssakerhet/MSB_uppdragsredovisning_it-incidentrapportering.pdf

National Institute of Standards and Technology. Special Publication 800-122. *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

OSCE Office for Democratic Institutions and Human Rights. *Promoting and Increasing Youth Political Participation and Civic Engagement in the OSCE Region*. Youth Leadership Forums, Warsaw 16-17 June and 13-14 November 2014. Tillgänglig på http://www.osce.org/odihr/155691?download=true

Post- och telestyrelsen. *Strategi för ett säkrare Internet i Sverige*. PTS-ER-2006:12. https://www.pts.se/sv/Dokument/Rapporter/Internet/2006/Strategi-for-ett-sakrare-Internet-i-Sverige---PTS-ER-200612/

Post- och telestyrelsen/Datainspektionen (2010). *Användning av trafikuppgifter i mobila innehållstjänster. Rapport efter avslutad tillsyn.* PTS-ER-2010:01/Datainspektionen 2010:1. Tillgänglig på https://www.pts.se/upload/Rapporter/Tele/2010/2010-1-mobila-innehallstjanster-100119.pdf

SOU 1973:6 Data och näringspolitik http://urn.kb.se/resolve?urn=urn:nbn:se:kb:sou-7257496

SOU 1974:10 Data och näringspolitik 74 http://urn.kb.se/resolve?urn=urn:nbn:se:kb:sou-7257651

SOU 1976:58 ADB och samordning http://urn.kb.se/resolve?urn=urn:nbn:se:kb:sou-7258376

SOU 1979:93 ADB och samhällets sårbarhet http://urn.kb.se/resolve?urn=urn:nbn:se:kb:sou-8350833

SOU 2007:47 Den osynliga infrastrukturen – om förbättrad samordning av offentlig IT-standardisering http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2007/06/sou-200747/

SOU 2007:76 Lagring av trafikuppgifter för brottsbekämpning http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2007/11/sou-200776/

SOU 2010:104 E-legitimationsnämnden och Svensk e-legitimation http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2010/12/sou-2010104/

SOU 2012:44 Hemliga tvångsmedel mot allvarliga brott http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2012/06/sou-201244/

SOU 2012:90 Överskottsinformation vid direktåtkomst http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2013/01/sou-201290/

SOU 2012:95 Spioneri och annan olovlig underrättelseverksamhet http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2013/02/sou-201295/

SOU 2013:39 Europarådets konvention om it-relaterad brottslighet. Utredningen om it-brottskonventionen. http://www.regeringen.se/rattsdokument/

statens-offentliga-utredningar/2013/06/sou-201339/

SOU 2014:23 Rätt information på rätt plats vid rätt tid http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2014/04/sou-201423/

SOU 2014:67 Inbyggd integritet inom Inspektionen för socialförsäkringen http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2014/09/sou-201467/

SOU 2015:31 Datalagring och integritet http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2015/03/sou-201531/

SOU 2015:32 Nästa fas i e-hälsoarbetet http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2015/03/sou-201532/

SOU 2015:39 Myndighetsdatalag http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2015/04/sou-201539/

Tweede kamer. *Temporary Committee on Government ICT Projects Final Report* 13 oktober 2014. http://www.houseofrepresentatives.nl/news/committee-presents-report-failures-government-ict-projects

Akademiska källor

Ross Anderson, ”Why Cryptosystems Fail”. ACM. 1st Conf.- Computer and Comm. Security ’93. http://www.cl.cam.ac.uk/users/rja14/wcf.html

Nicholas Bohm et al, ”Electronic Commerce: Who Carries the Risk of Fraud?” 2000 (3) The Journal of Information, Law and Technology (JILT). http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/bohm/

James Boyle, *Foucault In Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors*, 1997 http://james-boyle.com/foucault.htm

Juan F. Briones Alonso. ”Economic assessment of oligopolies under the Community Merger Control Regulation”, European Competition law Review (Vol 4, Issue 3), 5 juni 1993. http://ec.europa.eu/competition/speeches/text/sp1995_033_en.html

Rainer Böhme, *Vulnerability Markets – What is the economic value of a zero-day exploit?* https://events.ccc.de/congress/2005/fahrplan/attachments/542-Boehme2005_22C3_VulnerabilityMarkets.pdf

Jay Pil Choi, Chaim Fershtman och Neil Gandal. *Network Security: Vulnerabilities and Disclosure Policy.*, WEIS 2007 http://weis2007.econinfosec.org/papers/68.doc

Claudio Garnieri, ”Everything we know of NSA and Five Eyes malware”. https://nex.sx/blog/2015-01-27-everything-we-know-of-nsa-and-five-eyes-malware.html

Kungliga vetenskapsakademien, *Scientific Background on the Sveriges Riksbank Prize in Economic Sciences in Memory of Alfred Nobel 2014. Jean Tirole: Market power and regulation. Compiled by the Economic Sciences Prize Committee of the Royal Swedish Academy of Sciences*. http://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/2014/advanced-economicsciences2014.

pdf

Nicolas Petit ”The Oligopoly Problem in EU Competition Law”, 5 februari 2012. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1999829

Sasha Romanosky, David Hoffman, Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation*, WEIS 2010 http://weis2012.econinfosec.org/papers/Romanosky_WEIS2012.pdf

David Solove, ”Are People Really Harmed By a Data Security Breach?”, Concurring Opinions, 22 september 2010. http://concurringopinions.com/archives/2010/09/are-people-really-harmed-by-a-data-security-breach.html

SOM-rapport nr 2008:25. *Förtroendet för myndigheter Riks-SOM-undersökningen 1986-2007*. http://som.gu.se/digitalAssets/1275/1275004_2008_fortroende-for-myndigheter.pdf

SOM-rapport nr 2012:10. *Svenskars bedömning av offentliga myndigheters verksamhet*. http://som.gu.se/digitalAssets/1373/1373436_svenskars-bed--mning-av-offentliga-myndigheters-verksamhet.pdf

SOM-rapport nr 2014:11 *Svenska folkets bedömning av offentliga myndigheters verksamhet*. http://som.gu.se/digitalAssets/1488/1488151_svenska-folkets-bed--mning-av-offentliga-myndigheters-verksamhet.pdf

Dagstidningar

Computer Sweden, 29 april 2013. ”Så hackades Logica” http://computersweden.idg.se/2.2683/1.505012/sa-hackades-logica

Dagens Juridik, 24 april 2014. ”Åklagare och Säpo vill införa nytt tvångsmedel – hemliga ”spiontrojaner” i datorer” http://www.dagensjuridik.se/2014/04/aklagare-och-sapo-vill-infora-nytt-tvangsmedel

Dagens Nyheter, 29 mars 2013 ”Skatteverkets folkbokföring hackad” http://www.dn.se/nyheter/sverige/skatteverkets-folkbokforing-hackad/

Dagens Nyheter, 5 december 2013. ”En halv miljon känsliga uppgifter stals från Kronofogden” http://www.dn.se/ekonomi/en-halv-miljon-kansliga-uppgifter-stals-fran-kronofogden/

Dagens Nyheter, 20 maj 2014. ”Så avslöjar du it-projekten som riskerar att haverera” http://www.dn.se/debatt/sa-avslojar-du-it-projekten-som-riskerar-att-haverera/

Dagens Nyheter 18 mars 2015. ”Försvarsministern: Vi ska kunna genomföra cyberattacker” http://www.dn.se/nyheter/sverige/forsvarsministern-vi-ska-kunna-genomfora-cyberattacker/

Sveriges Television 11 december 2013. ”FRA hackar datorer – topphemligt projekt med NSA” http://www.svt.se/ug/fra-hackar-datorer