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 2015-09-13

Remissyttrande över SOU 2015:25 – En ny säkerhetsskyddslag

Dataskydd.net avstyrker utredningens förslag i sin helhet. Särskilt

- utredningens problemformulering i kap. 9.
- utredningens förslag och analys att civila verksamheter ska anses kritiska för rikets säkerhet i kap. 11.2.
- utredningens förslag att det skyddsvärda området inte ska avgränsas genom regleringen om skyddsobjekt utan ska även kunna innefatta annat slag av säkerhetskänslig verksamhet, t.ex. verksamheter som innefattar hantering av it-system eller av sammanställningar av uppgifter som är av central betydelse för ett fungerande samhälle i kap. 12.
- utredningens förslag om säkerhetsskyddsanalys i kap. 13.
- utredningens förslag om administration av säkerhetsskyddsanalys i kap. 14.
- utredningens förslag om informationssäkerhet i kap. 16.
- utredningens förslag om säkerhetsskyddade upphandlingar i kap. 19.
- utredningens förslag om tillsyn, föreskrifter och rapportering i kap. 21.

Introduktion

Utredningens uppdrag och utförande exemplifierar på ett olyckligt sätt den kompetenskonflikt som för närvarande finns mellan brottsbekämpande myndigheter och krisberedande myndigheter på IT-säkerhetsområdet. Dataskydd.net har tidigare lyft problemet i vårt remissyttrande på utredningen SOU 2015:23. Denna kompetenskonflikt underblåses av regeringens oförmåga att visa ledarskap i IT-säkerhetsfrågor (bland annat genom regeringens terroriststrategi från 28 augusti 2015, som okritiskt stödjer både SOU 2015:23 och SOU 2015:25 samtidigt). Att regeringen förvärrar, snarare än reder ut, kompetensstrider mellan myndigheter riskerar dessutom att viktiga intressen i IT-säkerheten, så som individers och konsumenters rättigheter, eftersätts.

Den föreslagna informationssäkerhetsmodellen är byråkratisk och långsam, tvärtemot de dynamiska och snabbt utvecklande system den försöker reglera. Framför allt åsidosätter den de privatpersoner som behöver interagera med de samhällskritiska system utredningen identifierar. Det finns starka skäl, både från

Dataskydd.net, Remissyttrande över SOU 2015 :23 – Informations- och cybersäkerhet i Sverige, s. 13. Tillgänglig på https://dataskydd.net/sites/default/files/sou201523_remissyttrande_dataskyddnet.pdf

Skrivelse 2014/15:146, Förebygga, förhindra och försvåra – den svenska strategin mot terrorism, s. 25-26

forskning om IT-säkerhet och från den rättsfilosofi vi hoppas genomsyrar vårt demokratiska samhälle, att göra en annan slutsats än den utredningen har valt.

Utredarens uppdrag har varit att ”föreslå hur reglerna om informationssäkerhet, som en del av säkerhetsskyddet, bör vara utformade”. Förslagen som läggs fram innebär en kraftig ökning Säkerhetspolisens och Försvarsmaktens möjligheter att via administrativa åtgärder och direkt kontroll utöva inflytande över informationsteknologiska system i privat och offentlig sektor. Utredningen stödjer sina förslag på lösryckta, anekdotiska påståenden från myndigheterna vars befogenheter ökas i och med utredningens förslag. Inget kvantitativt eller kvalitativt stöd för dessa anekdoter anförs. Vid åtminstone ett tillfälle anför utredningen ett direkt felaktigt, och lätteligen motbevisat, påstående som stöd för sina slutsatser.

Kommittédirektiv 2011:94

SOU 2015:25, s. 237. Se också nedan.

Forskning visar att näringspolitiska åtgärder så som konsumentskydd, dataskydd och bättre ansvars- och riskfördelning är det som behövs för bättre IT-säkerhet[1] snarare än ökad och centraliserad kravställning. Det finns en överväldigande mängd forskning och tidigare utredningar på området som indikerar att ett näringspolitiskt fokus på informationssäkerhet skulle hjälpa hela samhället, inklusive de intressen som utredningen givits i uppdrag att skydda.[2]

I uppdraget till utredningen står bland annat ”[s]äkerhetsskyddslagstiftningen måste vara utformad på ett sådant sätt att den ger utrymme för att vidta de åtgärder som krävs för att möta utvecklingen på it-området”. Det är mot denna bakgrund otillfredsställande att utredningen har låtit sig begränsas av partsinlagor och politiska missförstånd. Det kan inte vara så att ett område som upplevs som absolut kritiskt för nationens fortlevnad ska styras av felaktig information, partsintressen och skrönor.

Kommittédirektiv 2011:94

Felaktigheter i utredningen

Utredningen påstår felaktigt att ”[ö]ppenhet kring skyddsåtgärder är i regel kontraproduktivt. Att öppet tala om sårbarheter kan få oönskad påverkan”. Metoden att skapa bättre IT-säkerhet genom transparens tillämpas tvärtemot utredningens påstående flitigt i privat sektor.[3] Fördelarna med öppenhet som säkerhetsförbättrande metod är väl befästa i modern IT-säkerhetsforskning.[4] En tydlig och stark konsumenträtt har visat sig ge bättre IT-säkerhet till ett lägre

SOU 2015:25, s. 237

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

[2] Från myndigheter, se t.ex.: 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 (2010). *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*.

[3] Ett kortfattat urval: Google Project Zero. http://googleprojectzero.blogspot.se/ ; Pwnie Awards. http://pwnies.com/about/; Pwn2Own https://cansecwest.com/post/2015-03-08-14:42:30_PWN2OWN_2015; Man kan hitta en sammanställning av befintliga *bug bounty awards* – priser för den som hittar och avslöjar säkerhetsfel – på https://bugcrowd.com/list-of-bug-bounty-programs

[4] Ross Anderson, Rainer Böhme, Richard Clayton, och Tyler Moore. *Security, Economics, and the Internal Market*. ENISA 2008. Tillgänglig på http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf; Jay Pil Choi, Chaim Fershtman och Neil Gandal. *Network Security: Vulnerabilities and Disclosure Policy*., WEIS 2007. Tillgänglig på http://weis2007.econinfosec.org/papers/68.doc.

pris för tjänsteleverantörerna.[5] Utredningen stödjer sig alltså på ett felaktigt och grundlöst antagande.

Utredningen om säkerhetsskydd anför som stöd för sina förslag bara anekdotiska hänvisningar à la ”angrepp i form av elektroniska attacker på samhällsviktiga informationssystem är ett av de allvarligaste hoten mot rikets säkerhet”. Utredningens ensidiga informationsintag verkar ha medfört en orealistisk uppfattning om begreppen ”kris” och ”allvarliga hot”.

SOU 2015:25, s. (227) 565

> Det kanske tydligaste exemplet på en oförväntad IT-incident vi har i Sverige är när Skatteverkets SPAR-register hackades 2009.[6] Trots osannolikheten i händelsen kan den dock varken beskrivas som allvarlig eller kris: 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.[7]

Dataskydd.net, Remissyttrande över SOU 2015 :23 – Informations- och cybersäkerhet i Sverige, s. 3

Här hade det behövts bättre perspektiv kring vad ”kris” och ”allvarlig samhällspåverkan” innebär. Det är en sak att någon på Säkerhetspolisen blir orolig. Det är en annan sak att statens grundvalar rämnar. Det är obehagligt och förargande att datorer ibland har säkerhetsproblem. Det är emellertid fel att tro att säkerhetsproblemen löser sig av att man döljer dem eller försvårar öppna och transparenta utredningar om dem.[8]

> Vid ett annat tillfälle har Myndigheten för samhällsskydd och beredskap kartlagt Tietos serveruppgraderingar 2011.[9] Trots oförväntade störningar till följd av uppgraderingen, kan dessa störningar inte rimligen beskrivas som ”kris”: Bilprovningen var stängd i en dag, flera landsbygdsapotek fick arbeta med pappersrecept, vissa företag lyckades åtgärda störningarna på mindre än fyra timmar, och ett par kommuner fick administrativa merkostnader som utgör en bråkdel av deras förväntade överskott under ett givet budgetår.

Dataskydd.net, Remissyttrande över SOU 2015 :23 – Informations- och cybersäkerhet i Sverige, s. 3

Vi *vill* att företag ska hålla sina servrar uppgraderade, och *vill inte* straffa beteendet att uppgradera med onödig rapportskrivning och dyra revisionsåtgärder. Utredningens brist på exempel – även fiktiva exempel! – på när utredningens förslag kan tänkas vara bra gör att det är svårt att veta om Tietos serveruppgradering skulle falla inom ramen för säkerhetsskyddet eller inte (eller delvis?). Den sannolika konsekvensen av säkerhetsskydd på Tietos servrar är dock att de under säkerhetsskydd uppgraderas mer sällan, eftersom varje uppgradering kommer att bli mer besvärlig.

Risker med utredningens förslag

Utredningen diskuterar inga särskilda exempel på när utredningens åtgärder är önskvärda. Mot bakgrund av de åtgärder, särskilt den starka maktcentralisering-

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

[6] ”Skatteverkets folkbokföring hackad”, *Dagens Nyheter*, 29 mars 2012.

[7] 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

[8] Jfr Datatilsynet (Danmark). 31 juli 2015. Journalnummer: 2013-632-0050 ”*Uvedkommendes 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/

[9] 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.*

en, som föreslås i kapitel 14-16, samt 19-21, borde utredningen ha presterat bättre indikationer på att de föreslagna åtgärderna motsvarar ett existerande behov.

Omfattande statlig inblandning i informationssäkerhetsåtgärder riskerar leda till att privat sektor lastar över kostnader för vanligt underhåll av IT-system på skattebetalarna. Privat sektor kan också antas lockas att lasta över kostnaden för att inte åtgärda säkerhetsproblem i deras infrastruktur på skattebetalarna. Utredningens förslag riskerar alltså förta fördelarna av en marknadsekonomisk regim för viktiga basmarknader (el, vatten, gas, telekom). Utredningens förslag riskerar att försvåra och försena utarbetandet av lämpliga konsumentskyddande åtgärder på dessa marknader och öppna, grundliga granskningar av offentlig sektors och privata företags investeringar i nya digitala teknologier.

I tidigare svenska utredningar om IT-brott har det anförts att ”[t]illiten till och förtroendet för elektroniska kommunikationstjänster och internet är /.../ av betydande vikt”. Det kan då vara lockande att med hänvisningar till Skatteverkets SPAR-registerincident hävda att allmänhetens förtroende för myndigheter inte rubbas så länge myndigheterna undanhåller information från allmänheten om uppkomna säkerhetsproblem.

Medborgare har redan idag inte någon rättighet att få veta att en myndighet, eller en myndighets underleverantör, inte har lyckats med informationssäkerheten. Inte ens människor med skyddade eller fingerade personuppgifter har en rätt att veta om myndigheten misslyckats med informationssäkerhet. Men det liggande förslaget kan innebära även att journalister och media inte får skriva om när myndigheter är dåliga på informationssäkerhet.

Regeringen och lagstiftaren bör vara klokare än att inom informationssäkerheten låta ”tillit och förtroende” översättas till ”ignorance is bliss”.

SOU 2013:39. *Europarådets konvention om it-relaterad brottslighet*. Tillgänglig på http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2013/06/sou-201339/

Förslag

Dataskydd.net föreslår att lagstiftaren tillsätter en utredning om konsument- och kundorienterad lagstiftning, med emfas på transparens och tydlig riskfördelning mellan olika aktörer på den öppna marknaden för informationssystem och tillhörande säkerhetsfunktionaliteter. Post- och telestyrelsen (PTS) har eftersökt en sådan utredning sedan 2006.[10] En utförligare utredning i samma anda genomfördes 2008 vid Europeiska byrån för nätverks- och informationssäkerhet (ENISA).[11] Även amerikanska nationella standardinstitutets (NIST) har utarbetat förslag på riktlinjer för god informationssäkerhet i organisationer[12] som följer denna linje.

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

[11] Ross Anderson, Rainer Böhme, Richard Clayton, och Tyler Moore. *Security, Economics, and the Internal Market*. ENISA 2008. Tillgänglig på http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf; Se också Panagiotis Trimintzios, Chris Hall, Richard Clayton, Ross Anderson och Evangelos Ouzounis. *Resilience of the Internet Interconnection Ecosystem*. ENISA 2011. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter-x/interx/report/interx-report

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

Individ-centrisk incidentrapportering

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.[13] Forskning visar också att konsumenter är mer benägna att ställa sådana aktörer till svars, som utredningen framhåller att det är extra viktigt att medborgarna har förtroende för (t.ex. vård- och finansaktörer). Dataskydd.net hänvisar till sitt remissyttrande på SOU 2015:23 för en mer substantiell behandling av frågan.

IT-haverikommission

Dataskydd.net föreslår en IT-haverikommissionen som går igenom statliga IT-upphandlingar och genom öppen, parlamentarisk debatt och diskussion ser efter vilka organisatoriska och tekniska aspekter som kan förbättras vid upphandling och underhåll av IT-system. Nederländernas riksdag lät genomföra en sådan utredning redan 2014, med mycket gott resultat.[14]

Bygg på existerande modeller i privat sektor

Metoden att skapa bättre IT-säkerhet genom transparens tillämpas tvärtemot utredningens påstående flitigt i privat sektor.[15] Fördelarna med öppenhet som säkerhetsförbättrande metod är väl befästa i modern IT-säkerhetsforskning.[16]

Starkare konsumentskydd

Starkare konsumenträtt ger mer säkerhet i vanligt använda elektroniska system för samma mängd pengar som annars skulle leda till sämre säkerhet, och detta har varit känt i snart 30 år.[17] 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.[18]

Typiska problem för IT-säkerhet är att den som utvecklat systemet inte

---

[13] För forskning på området se t.ex. Sasha Romanosky, David Hoffman, Alessandro Acquisti *Empirical Analysis of Data Breach Litigation* i WEIS 2010 Tillgänglig på http://weis2012.econinfosec.org/papers/Romanosky_WEIS2012.pdf; David Solove, ”Are People Really Harmed By a Data Security Breach?”, Concurring Opinions, 22 september 2010 Tillgänglig på http://concurringopinions.com/archives/2010/09/are-people-really-harmed-by-a-data-security-breach.html

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

[15] Se ovan fotnot 3.

[16] Jay Pil Choi, Chaim Fershtman och Neil Gandal. *Network Security: Vulnerabilities and Disclosure Policy*. i WEIS 2007. Tillgänglig på http://weis2007.econinfosec.org/papers/68.doc; Ashish Arora, Rahul Telang och Hao Xu. *Optimal Policy for Software Vulnerability Disclosure*. Tillgänglig på http://www.dtc.umn.edu/weis2004/xu.pdf; Ashish Arora, Ramayya Krishnan, Anand Nandkumar, Rahul Telang och Yubao Yang. *Impact of Vulnerability Disclosure and Patch Availability – An Empirical Analysis*. Tillgänglig på http://www.dtc.umn.edu/weis2004/telang.pdf

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

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

har tillräckligt starka incitament för att säkerställa att systemet fungerar.[19] Konsumenter och kunder bär ofta bevisbördan för att produkten inte fungerat så som föreskrivet.[20] Jur. Dr. Lennart Johansson skrev 2006 en avhandling om den avtalsrättsliga förflyttningen av risk och ansvar från banker till konsumenter på marknaden för kredittransaktioner riktade mot slutkonsumenter.[21]

Att man politiskt inte agerat på det dåliga konsumentskyddet i digitala miljöer är upprörande och skamligt.

Rätt ansvars- och riskfördelning

Privata företag i konsumentinriktade marknader (det vill säga, som får stå till svars gentemot konsumenterna för säkerhetsfel) lägger i regel mycket mer pengar på brottsförebyggande åtgärder i IT-system än vad stater gör.[22] Om målet med säkerhetsskyddet är en högre integritet och tillförlitlighet i IT-systemen tjänar man alltså på att ytterligare förstärka konsumenträttigheter.

Sammantaget finner Dataskydd.net att så pass stora delar av utredningen är dåligt underbyggda att utredningen i sin helhet måste avstyrkas.

Dataskydd.net

Amelia Andersdotter
Ordförande

[19] Ross Anderson och Tyler Moore. *Economics and Internet Security: A Survey of Recent Analytical, Empirical and Behavioral Research*. TR-03-11. Computer Science Group, Harvard University, Cambridge, Massachusetts. Tillgänglig på ftp://ftp.deas.harvard.edu/techreports/tr-03-11.pdf

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

[21] Lennart Johansson, *Banker och internet*, Iustus förlag (Stockholm) 2006.

[22] Ross Anderson, 24 november 2014: ”Britain spends less on fighting online crime than Facebook does, and only about a fifth of what either Google or Microsoft spends[.]”. https://www.lightbluetouchpaper.org/2014/11/27/spooks-behaving-badly/