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

Dataskydd.net Sverige
Alsnögatan 18
116 41 Stockholm

Justitiedepartementet
103 33 Stockholm

Falun 2017-07-23

Remissyttrande över SOU 2017:36 (Ju2017/03997/L4) – Informationssäkerhet för samhällsviktiga och digitala tjänster

Dataskydd.net är en svensk ideell, partipolitiskt obunden förening som verkar för bättre tekniskt och juridiskt dataskydd för privatpersoner i Sverige.

Förslag

Dataskydd.net avråder från genomförandet av nuvarande lagförslag eftersom det resulterar i kontraproduktiva effekter på samhällets dataskydd och IT-säkerhet. I korthet innebär det en ineffektiv byråkrati med tillsyn och incidentrapportering, samtidigt som effektiva åtgärder för dataskydd och IT-säkerhet uteblir och till och med undergrävs.

Följande förändringar efterfrågas:

- Det behövs tydliga krav på offentliggörande av sårbarheter och incidenter i informationssystem och tjänster, samt om tillsyn, för att skapa incitament till effektiv styrning och uppföljning för såväl myndigheter som företag.
- Det behövs tydliga krav på oberoende tillsyn av behöriga myndigheters informations- och incidenthantering för att försäkra marknaden och medborgare att gällande regelverk och rekommendationer för dataskydd även gäller säkerhetsmyndigheter.
- Post-och telestyrelsen (PTS), inte Myndigheten för samhällsskydd och beredskap (MSB), bör ansvara för incidentrapporter från näringslivet. PTS har bättre kompetens och är bättre rustad att hantera behovet av informationsdelning samt samordna med Datainspektionen.

Motiveringarna till dessa förslag är välkända för de som är bekanta med säkerhetsekonomiska överväganden. Här nöjer vi oss med en kort sammanfattning av relevans.

Insyn stärker säkerheten

Offentlig exponering av sårbarheter och it-incidenter, allmän säkerhetsinformation och kommunikation, bidrar till bättre säkerhet genom att skapa incitament

för förbyggande och effektiva säkerhetsåtgärder.[1] Risken för exponering och förlust i förtroendekapital på marknaden och bland konsumenter är en drivkraft till egenkontroll.[2] En rad studier stödjer det, till exempel en studie som nyligen publicerades och där det framgick att marknadskonkurrens och exponering av sårbarheter förkortar tiden till publicering av patchar med 50 dagar,[3] land flera andra studier som pekar på vikten av offentlig information.[4,5]

Offentlig information och kommunikation underlättar vidare ansvarsutkrävande, erfarenhets- och kunskapsåterföring, samt därmed till kunskaps- och kompetensutveckling.[6] I det syftet publicerar Storbritannien sedan 2016 officiell statistik om cybersäkerhet och incidenter. USA har sedan många år system för offentlig publicering av obligatoriska rapporter om dataintrång.

Situationen i Sverige är allt annat än transparent.

Sedan 1 april 2016 har MSB ansvaret för att samla in och sammanställa incidentrapporter från myndigheter. Sedan införandet har MSB tagit mot ett antal förfrågningar från journalister och medborgare om att få ta del av uppgifter i incidentrapporter. Det har genomgående besvarats med sekretess, även om och när uppgiftslämnaren själv inte anger att sekretess föreligger. Ingen information publiceras löpande. I början av 2017 publicerade MSB en första årsrapport om antal rapporter. I huvudsak var innehållet förenat med sekretess. MSB beskrev själv resultatet som att ”systemet är i sin linda”.[7] I opinionsinlägg menar att säkerhetsexperter att systemet är meningslöst så länge ingen erfarenhets- och kunskapsåterföring sker.[8]

Det aktuella lagförslaget andas samma kultur av sekretess som präglar incidentrapportering, nationell underrättelseverksamhet och rikets säkerhet. Marknadens aktörer ska delge information om säkerhetsåtgärder och incidenter till myndigheter, men inga krav ställs på myndigheter att delge allmän information till marknaden och medborgare om säkerhetsbrister och incidenter. Det är en fråga för myndigheterna att bedöma från fall till fall.

Även Datainspektionen (DI) har i en skrivelse till regeringen gått på säkerhetsmyndigheternas linje med behovet av högsta möjliga sekretess för incidentrapporter om dataintrång.[9] Med anledning av den nya dataskyddsförordningen ser DI säkerhetsrisker med att incidentrapporter begärs ut och offentliggörs. I likhet med MSB och andra säkerhetsmyndigheter nämner inte DI ett enda ord om de positiva effekter som transparens medför och de negativa

Amerikanska delstater med offentligt publicerade incidentrapporter:

Iowa
https://www.iowaattorneygeneral.gov/for-consumers/security-breach-notifications/

Kalifornien
https://oag.ca.gov/ecrime/databreach/list

Maryland
http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/breachnotices.aspx

Montana
https://dojmt.gov/consumer/consumers-known-data-breach-incidents/

New Hampshire
http://www.doj.nh.gov/consumer/security-breaches/

Oregon
https://justice.oregon.gov/consumer/databreach/

Vermont
http://ago.vermont.gov/focus/consumer-info/privacy-and-data-security1/data-security-breaches/archived-security-breaches.php

Washington
http://www.atg.wa.gov/data-breach-notifications

Incidentrapporterna publiceras på Attorney Generals webbplats och går att beskåda av både invånare i delstaten, forskare och andra företag. De öppna publiceringarna kartläggs också av *Privacy Clearing House*, en amerikansk civilsamhällesorganisation som hjälper invånare när de drabbats av en säkerhetsläcka och kontinuerligt utvärderar olika myndigheters och företags *privacy*-ansträngningar. Ytterligare 39 delstater kräver att företag och myndigheter skickar incidentrapporter direkt till berörda medborgare och konsumenter, när ett IT-säkerhetsfel inträffat.

[1] ENISA. 2008. Security Economics and the Internal Market. Författare: Ross Anderson, Rainer Boehme, Richard Clayton, Tyler Moore.

[2] Wahlund R, Dellham R, Åberg D och Lakomaa E. 2016. Anseenderisker och dataskydd. Kapitel 5, utdrag ur Risker och riskhantering i näringsliv och samhälle. Wahlund R (red.) Stockholm School of Economics Institute for Research.

[3] Jo, A. M. (2017). The effect of competition intensity on software security-An empirical analysis of security patch release on the web browser market. The Workshop on the Economics of Information Security (WEIS) 2017.

[4] Dingman, A. C., & Russo, G. (2015). Risk-Based Vulnerability Disclosure: Towards Optimal Policy.

[5] Sedenberg, Elaine M. and Mulligan, Deirdre K. 2016. “Public Health as a model for cybersecurity information sharing” Berkeley Technology Law Journal 30:3.

[6] Se ovan fotnot 1.

[7] Myndigheten för samhällsskydd och beredskap (15 mars 2017) Första årsrapporten inlämnad till regeringen om arbetet med allvarliga it-incidenter.

[8] SVT Opinion (19 juli 2017), Lars Mårelius, Patrik Fälström, Niels Paarup-Petersen: ”Sverige lär sig inget av alla IT-haverier”.

[9] Datainspektionen, Dnr. 1704-2017, Vissa frågor om sekretess med anledning av EU:s dataskyddsreform.

effekter som sekretess och mörkläggning av it-incidenter medför.

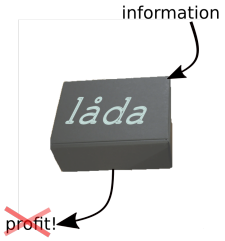
Att undanhålla information från marknaden innebär att sårbarheter och säkerhetsbrister mörkläggs istället för exponeras. Under våren 2017 fick vi erfara ett högst konkret exempel på det, WannaCry, ett verktyg utvecklat av Försvarets radioanstalts amerikanska motsvarighet, NSA.[10] Verktyget stals från NSA, men NSA delgav ingen information, vilket hade underlättat förebyggande arbete och mildrat effekterna av den globala it-attacken som följde.

Ett annat exempel på värdet av offentlig exponering av säkerhetsfrågor är sommarens nyhetsrapportering om Transportstyrelsens upphandling av utländska systemförvaltare, där grundläggande säkerhetskrav medvetet ignorerades. Rapporteringen bidrar till en radikalt högre medvetenhet om de säkerhetsvärden, risker och krav som står på spel. Det medför högre risk för exploatering av sårbarheter, men ytterst tjänar det säkerheten genom att alla myndigheter och organisationer åtgärdar gemensamma problem.

Införandet av obligatorisk incidentrapportering 2016 präglas tvärtom av låg exponering och rapportering, oklara mål och tolkningsproblem, till exempel när MSB ska återkoppla till andra myndigheter och vad som räknas allvarliga incidenter. NIS-direktivet kan förväntas ge en större mängd incidentrapporter från privata aktörer, vilket gör det än mer angeläget om explicita krav på återkoppling av tillsyn och incidenter. Annars lär regelverket bara skapa en resurskrävande byråkrati utan effektiv styrning och uppföljning.

Styrning och ledning

MSB har och får i lagförslaget en mer central roll i samordningen av samhällets informations- och cybersäkerhet. Det bör åtföljas av krav på styrning och uppföljning av myndighetens arbete på området, även med tanke på att myndigheten lägger stora ekonomiska resurser på det, i storleksordningen en halv miljard kronor per år. Hittills har ingen utvärdering gjorts av verksamheten. Inte heller innehåller lagförslaget några krav på tillsyn av MSB:s verksamhet, trots att myndigheten kommer att aggregera och hantera en stor mängd känslig information om samhällsviktiga system och tjänster hos privata aktörer.



En sluten process. Så här fungerar *inte* IT-säkerhet. Ingen blir klokare av att man stoppar en massa information i en svart låda som inte lämnar ifrån sig något vettigt resultat.

Lagförslaget lägger tonvikt på att utöva tillsyn på samhällsviktiga informationssystem och tjänster, men inget sägs om hur tillsynsresultat ska kommuniceras till samhället och marknaden, förutom informationsdelning mellan enskilda myndigheter och aktörer.

Bristen på krav på offentlig genomlysning och transparens innebär en brist på incitament att utveckla gemensamma ramverk för styrning och uppföljning av säkerhetsarbetet, ett centralt syfte med NIS-direktivet. Utan gemensamma ledningssystem finns en överhängande risk för målkonflikter och motstridiga tolkningar.

I NIS-direktivet, lagförslaget och även MSB:s nuvarande föreskrifter på området sägs att det är viktigt att beakta ledningssystem för säkerhetsarbetet. Trots det saknar MSB själv ett ledningssystem för sitt arbete med samhällets informations- och cybersäkerhet.

Myndigheten saknar till exempel riktlinjer eller rutiner för att hantera information, varningar och larm från andra myndigheter och organisationer. Det får

[10] Burgess, Matt. Wired (28 juni 2017) Everything you need to know about EternalBlue – the NSA exploit linked to Petya.

bland annat till följd att MSB larmar om vissa hot, till exempel Cloud Hopper, efter en rapport från konsultföretaget PWC och försvarsföretaget BAE system, men inte andra, till exempel cybervarningen för Hospiras infusionspumpar från Food and Drug Administration (FDA).[11]

I lagförslaget får MSB ytterligare mandat att hantera säkerhetsinformation från andra organisationer, men fortfarande utan några kvalitetskrav på den egna verksamheten, trots att myndigheten inte på förhand kan antas vara befriad från vare sig misstag eller missbruk av känsliga uppgifter. Mot bakgrund av upprepade fall av bristfälligt dataskydd i underrättelseorganisationer och säkerhetsmyndigheter är det anmärkningsvärt att lagförslaget inte innehåller några som helst krav på kontrollåtgärder.

För trovärdig incidenthantering och tillsyn av informationssystem och tjänster krävs tydligare krav på offentlig, aktuell och systematisk informationsdelning. Nuvarande lagförslag innehåller inga ambitioner alls i denna fråga och undergräver möjligheterna till genomlysning och insyn. Information till marknaden och allmänheten blir en förhandlingsfråga mellan MSB, tillsynsmyndigheter och leverantörer från fall till fall. Det bådar inte gott för vare sig konsumenternas, företagens eller samhällets dataskydd och säkerhet.

I NIS-direktivet finns ett krav på att samverka med Datainspektionen i fall som berör den nya dataskyddsförordningen. I det svenska lagförslaget åläggs tillsynsmyndigheterna att samverka MSB, men MSB åläggs inte med något motsvarande krav att samarbeta tillbaka, trots att det är MSB som är navet i samhällets samordning av incidenthantering och rapportering.

Med tanke på att MSB ska tilldelas denna senare roll är det rimligare att samråd med Datainspektionen sker när incidentrapporter delges. Annars finns det risk att myndigheter inleder utredningsarbete oberoende av varandra, eller att det går lång tid innan berörda medborgare delges den information som de har rätt till.

Mot bakgrund av de krav som bör ställas på offentlig genomlysning av incidenter och tillsyn, inte minst med tanke på att NIS-direktivet avser informationshantering, system och tjänster som i många fall berör enskilda medborgare och konsumenter, måste MSB som mottagare av incidentrapporter ifrågasättas. MSB agerar idag i hög grad som en underrättelseorganisation vid incidenthantering, snarare än genom att främja en bred och allmän erfarenhets- och kunskapsuppbyggnad på området.

Huvudansvaret för samordningen av incidentrapporter från den privata sektorn borde istället ligga på Post- och telestyrelsen (PTS). De har redan idag ansvaret för incidentrapporter från telekomföretagen och visar på mognad i säkerhetsrapportering och redovisning. Myndigheten balanserar behov och krav på både konfidentialitet och tillgänglighet i informationshantering. De publicerar också risk- och sårbarhetsanalyser av kvalitet där incidentstatistik redovisas.[12]

Post- och telestyrelsen har haft ett ledningssystem för sitt informationssäkerhetsarbete sedan 2006, ett system som omfattar informationshanteringen i sin helhet.

Tango kräver två. För att samarbete ska fungera mellan två parter, måste bägge parterna bidra till samarbetet. Den koordinerande rollen som föreslås för MSB förutsätter emellertid bara att den ena parten, den som inte är MSB, ska samarbeta, medan MSB är fria att bestämma om de vill vara med på tåget.

Bild: Public domain (kulturallmänning) från engelsk-språkiga Wikipedias artikel om tango.

Amelia Andersdotter
Ordförande, Dataskydd.net

[11] Dataskydd.net och Föreningen för digitala fri- och rättigheter (DFRI), Remissyttrande över promemorian Ju2017/02002/L4 om ett tekniskt sensorsystem hos MSB.

[12] Post- och telestyrelsen (PTS-ER-2016:23) Risk- och sårbarhetsanalys 2016.

Källhänvisningar med länkar där möjligt

1. Burgess, Matt. Wired (28 juni 2017) Everything you need to know about EternalBlue – the NSA exploit linked to Petya. http://www.wired.co.uk/article/what-is-eternal-blue-exploit-vulnerability-patch
2. Datainspektionen, Dnr. 1704-2017, Vissa frågor om sekretess med anledning av EU:s dataskyddsreform. http://www.datainspektionen.se/Documents/2017-07-13-skrivelse-sekretess.pdf
3. Dataskydd.net och Föreningen för digitala fri- och rättigheter (DFRI), Remissyttrande över promemorian Ju2017/02002/L4 om ett tekniskt sensorsystem hos MSB. https://dataskydd.net/sites/default/files/dfri_dataskyddnet_promemoriaju201702002l4_utan_sig.pdf
4. Dingman, A. C., & Russo, G. (2015). Risk-Based Vulnerability Disclosure: Towards Optimal Policy.
5. ENISA. 2008. Security Economics and the Internal Market. Författare: Ross Anderson, Rainer Boehme, Richard Clayton, Tyler Moore. https://www.enisa.europa.eu/publications/archive/economics-sec
6. Jo, A. M. (2017). The effect of competition intensity on software security-An empirical analysis of security patch release on the web browser market. The Workshop on the Economics of Information Security (WEIS) 2017. http://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/05/WEIS_2017_paper_10.pdf
7. Myndigheten för samhällsskydd och beredskap (15 mars 2017) Första årsrapporten inlämnad till regeringen om arbetet med allvarliga it-incidenter. https://www.msb.se/sv/Om-MSB/Nyheter-och-press/Nyheter/Nyheter-fran-MSB/Forsta-arsrapporten-inlamnad-till-regeringen-om-arbetet-med-allvarliga-it-incidenter/
8. Post- och telestyrelsen (PTS-ER-2016:23) Risk- och sårbarhetsanalys 2016. http://www.pts.se/sv/Dokument/Rapporter/Allmanna/2016/PTS-risk--och-sarbarhetsanalys-2016---PTS-ER-201623/
9. Sedenberg, Elaine M. and Mulligan, Deirdre K. 2016. "Public Health as a model for cybersecurity information sharing" Berkeley Technology Law Journal 30:3.
10. SVT Opinion (19 juli 2017), Lars Mårelius, Patrik Fälström, Niels Paarup-Petersen: "Sverige lär sig inget av alla IT-haverier". https://www.svt.se/opinion/it-haverikommission
11. Wahlund R, Dellham R, Åberg D och Lakomaa E. 2016. Anseenderisker och dataskydd. Kapitel 5, utdrag ur Risker och riskhantering i näringsliv och samhälle. Wahlund R (red.) Stockholm School of Economics Institute for Research.