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

Dataskydd.net Sverige
Alsnögatan 18
116 41 Stockholm

Justitiedepartementet
103 33 Stockholm

Malmö 2017-05-03

Remissyttrande över Ds 2017:7 – Kommunikation för vår gemensamma säkerhet

Vi avstyrker i huvudsak promemorians förslag som onödigt, dyrt och riskabelt. Förslaget är dåligt förankrat i befintlig kunskap om vad som har rimliga förutsättningar att förverkliga promemorians och regeringens ambition om en robust, säker och tillförlitlig kommunikationsinfrastruktur för samhällets kritiska tjänster och allmänheten. Vi har sammanställt några alternativ för säker, mobil kommunikation som vi tror att Justitiedepartementet bör begrunda istället för de lösningar som tas upp av utredningen.

Förslag

1. Regeringen förlikar sig med att den redan innevarande, marknadsdrivna modellen för utbyggnad av mobilnätet i Sverige varit den europeiskt sett mest framgångsrika. Förslaget i promemorian läggs åt sidan till fördel för den handlingsplan som Post- och telestyrelsen utarbetade under 2016.

2. Regeringen förlikar sig med omständigheten att vanliga kommunikationsappar tillgängliga för slutkonsumenter på den öppna marknaden för kommunikationsappar redan uppnår den säkerhetsnivå som de samhällskritiska tjänsterna rimligen kan vara i behov av. Det finns starka ekonomiska skäl för staten att inte använda skattemedel för att skapa vad som riskerar att ändå bli en undermålig konkurrent till de redan befintliga alternativen från privat sektor.

3. Regeringen förlikar sig med att bara för att man en gång misslyckats med en dyr, statlig kommunikationslösning för PPDR (det vill säga Rakel), så betyder inte det att man måste testa igen.

4. När det gäller till exempel motorfordon förstår regeringen intuitivt att polisen kan köra Mercedes eller Volvo, istället för att utveckla en egen polisbil. Samma resonemang bör tillämpas på telekommunikation: det finns inget egenvärde i att utveckla och äga en egen statlig infrastruktur eller kommuikationsapp när privat sektor visar sig vara tillräckligt bra på att utveckla användarvänliga, funktionsdugliga, säkra tjänster.

✻ Informationssäkerhet ✻

"*Because of its military and technical origin, information security is sometimes reduced to "the techniques employed to maintain security within a computer system" (Gollmann, 1999). However, information security in the context of organisational governance is much broader. /.../*
The predominance of the command-and-control approach has a serious consequence when working with employees' information security behaviours. Employees are still seen as the biggest obstacle to information security. In many cases, their security behaviours are directed by poorly designed information security policies (Stahl et al., 2012). Moreover, most methods focus on changing employees' behaviours because they consider these behaviours to be irrational and wrong, while the information security policies themselves are "correct" and unchangeable. However, various studies (e.g. Mattia and Dhillon, 2003; Corbin, 2013) have shown that the inability of policy to reflect current work practices is one of the biggest reasons for non-compliance."

– Ella Kolkowska m.fl., 2017 (se även fotnot 8).

Batmobile

Inget för polisen. Polisen köper in bilar från kommersiella aktörer eftersom nyttan av att utveckla helt egna fordon är låg. Bildkälla: Bagera3005 på DeviantArt.

Befintlig förekomst av säker kommunikation för mobiltelefoner

En drivande tes i promemorian är att behovet av informationssäkerhet för samhällets kritiska tjänster är så stort att bara ett statligt ägt och kontrollerat nät kan uppfylla säkerhetskraven. En sådan tes måste emellertid vara felaktig, eftersom redan befintliga, kommersiellt tillgängliga appar för slutkonsumenter i flertalet rapporter från bland andra Totalförsvarets forskningsinstitut[1], Finansinspektionen[2] och EU:s ministerråd[3] bedömts vara så säkra att de till och med utgör ett terroristhot och ett hinder för polisiära utredningar. Även svenska polismyndigheten har haft ett aktivt kommunikationsarbete för att påtala svårigheterna i att hantera just de höga säkerhetsnivåer som uppnås vanligt tillgängliga, kostnadsfria konsumentappar vid brottsutredningar och spaningsuppdrag.[4]

Om det behövs särskild lagstiftning, till exempel nya tvångsmedel av typen hemlig dataavläsning[5] eller generösare regler för digital husrannsakan,[6] för att hantera den starka utvecklingen mot bättre säkerhet i konsumentappar, är det svårt att förstå varför sådan bättre säkerhet ändå är otillräcklig för samhällets kritiska tjänster. Tvärtom finns stora synergivinster att hämta genom att även samhällets kritiska tjänster börjar använda de redan befintliga, mycket säkra och kommersiella alternativen.

Dessa synergier uppstår på två olika sätt:

1) Sannolikheten är hög att personalen i samhällskritiska verksamheter redan använder säkra kommunikationsappar på sin fritid, vilket ökar deras möjlighet att använda samma appar i tjänsten på ett ändamålsenligt sätt. Så undviker man problemet att de statligt utvecklade systemen för säker kommunikation blir så svåranvända att personalen ändå inte ids nyttja dem. För att hjälpa personalen hålla isär sina privata och professionella identiteter kan man tilldela dem jobbtelefon – något som enligt promemorian ändå i praktiken ofta sker.[7]

Svenska studier på myndighetspersonals benägenhet att följa informationssäkerhetspolicys bekräftar med all önskvärd tydlighet att en informationssäkerhetspolicy måste vara anpassad till redan befintliga arbetsmetoder hos personalen.[8] Om detta inte görs, finns en risk att de anställda kommer att välja att genomföra sitt jobb på ett annat sätt. I princip är det detta senare beteende som promemorian redan upplever sig ha bekräftat vid användningen av Rakel.[9] Det bör man dra lärdomar av.

2) De samhällskritiska tjänsterna kan också dra nytta av den snabba utvecklingen inom användarvänlig säkerhet och framför allt bättre säkerhet som för närvarande sker på marknaden för kommunikationsappar riktade mot privat-

Urval av mer eller mindre populära kommunikationsappar som marknadsför sig med en mycket hög säkerhetsnivå för slutanvändarna (samtlig produktinformation är hämtad från företagens egna webbplatser, media eller Wikipedia):

Wire. Öppen källkodsapplikation för säker (krypterad) text-, ljud- och videokommunikation samt filöverföringar i mobila miljöer. Utvecklas av Wire, ett schweiziskt bolag.

Signal. Öppen källkodsapplikation för säker (krypterad) text-, ljud- och videokommunikation samt filöverföringar i mobila miljöer. Utvecklas av Open Whisper Systems, ett amerikanskt företag.

Whatsapp. Mycket populärt alternativ för säker (krypterad) text-, ljud- och videokommunikation samt filöverföringar. Ägs och utvecklas av Facebook. Har på grund av den utbredda användningen av appen varit fokus i en rad rättskonflikter internationellt, bland annat i Brasilien och Belgien.

[1] *Se t. ex.* Hatbudskap och våldsbejakande extremism i digitala miljöer (FOI-R–4392–SE), s. 20.

[2] SEDU nr 46/2015, Understanding Terrorist Finance Modus Operandi and National CTF Regimes, s. 21–22.

[3] Council of the European Union (14711/16) Encryption: Challenges for criminal justice in relation to the use of encryption - future steps - progress report *samt* Council Response to Parliamentary Question E-009129/2016.

[4] NyTeknik, *Krypterade appar försvårar för polisen*, 28 mars 2017; Omni, *Finansvärlden trotsar regler med krypterade appar*, 2 april 2017; DN, *Löfvens statliga trojaner väcker frågor*, 19 november 2015.

[5] *Jfr* Kommittédirektiv 2016:36 Hemlig dataavläsning.

[6] Kommittédirektiv 2016:20 Moderna regler om beslag och husrannsakan.

[7] Ds 2017:7, s. 77.

[8] Ella Kolkowska och Gurpreet Dhillon, *Organizational power and information security rule compliance*, Computers & Security 33:3-11, 2012; Ella Kolkowska *m. fl.*, *Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method*, Journal of strategic information systems, 6(1) p. 39-57, 2017.

[9] Ds 2017:7, s. 19.

personer. Kryptering av text-, ljud- och videokommunikation var för inte så länge sedan besvärligt och svårt att implementera. De senaste åren har det dock skett stora forskningsinsatser på området att göra krypterade kommunikationer användbart och enkelt.[10] Eftersom en statligt utvecklad tjänst bara med stor svårighet kan antas uppnå samma förbättringstakt som de privata alternativen, kommer de samhällskritiska tjänsterna kunna åtnjuta bättre fungerande och bättre uppgdaterade kommunikationsverktyg om de förutsätts få använda kommersiella lösningar istället för att låsas in till en statligt handhaven tjänst.

För att öka användningen och nyttan av säker mobil kommunikation för samhällets kritiska verksamheter, måste de valda lösningarna vara förankrade i verkligheten. Med det menas inte bara att de ska förankras i hypotetiska hotbilder från en hårdnande geopolitisk verklighet, utan framför allt att de behöver förankras i den ansvariga personalens faktiska arbetssituation och beteende samt det marknadsläge som redan råder.

Nackdelarna med en roaminglösning enligt promemorian

Promemorian har identifierat två säkerhetsnackdelar med en roaminglösning:[11]

- Operatörer som ingår i samarbetet kommer att ha tillgång till trafik- och positionsuppgifter.
- Utvecklingen av nya PPDR-tjänster och kontroll över befintliga tjänster minskar jämfört med en virtuell operatörslösning (MOCN).

Den andra nackdelen, att nya PPDR-tjänster inte kan utvecklas lika lätt, anser vi redan bemött i ovanstående avsnitt.

Vad gäller den första invändningen kan man konstatera att de privata aktörerna kommer att ha möjlighet att spåra personal i kritiska verksamheter så länge dessa har med sig antingen en privat smart telefon eller en arbetstelefon. Eftersom det är sannolikt att personal i kritiska verksamheter även fortsättningsvis kommer att behöva komplettera en statlig kommunikationsinfrastruktur med privata abonnemang – om inte annat så på grund av den överlägsna tjänstekvaliteten och mångfalden av tjänster som finns tillgängliga i den kommersiella sektorn – kommer det vara svårt att undvika att bli således spårad.

Det är emellertid också så att de kritiska verksamheternas möjligheter att inte bli spårade av kommersiella mobiloperatörer är avhängig att de kommersiella mobiloperatörerna har incitament att utveckla effektiva tekniska metoder för slutanvändare att bli spårade. Det kan till exempel åstadkommas genom en stark, progressiv dataskyddslagstiftning till privatkonsumenters fördel, med tillräckliga tillsynsmöjligheter allokerade för att bevaka privatkonsumenternas intressen i Sverige. En möjlighet i närtid att bevaka ett sådant starkare skydd är EU-förhandlingarna om den så kallade e-Dataskyddsförordningen.[12]

Fler exempel på kommunikationsappar som inte nödvändigtvis sparar användaruppgifter, har krypteringsfunktionalitet för den användare som efterfrågar/vill ha sådan och som blivit väldigt populära bland slutkonsumenter, bland annat för att de är lätta att använda. Nedanstående appar har också ådragit sig mycket negativ kritik från brottsbekämpande myndigheter i olika delar av världen (produktinformationen kommer från företagens egna webbplatser och medier):

Kik. Krypterad video-, bild-, och textkommunikation. Lagrar inte data och kräver inga särskilda identifikationsåtgärder från sina användare när man skapar ett konto.

Snapchat. Marknadsför sig specifikt med att de inte sparar data över tid, för att därigenom bättre skydda sina användares data och privatliv.

Telegram. Har fått kritik för att den bland annat lagrar kommunikation i klartext om inte användaren specifikt begär något annat, och att den vill ha tillgång till adressböcker på mobiltelefoner.

[10] *Se t. ex.* Adrienne Porter Felt, Why is usable security hard, and what should we do about it?, USENIX Enigma Conference, januari 2016.

[11] Ds 2017:7, s. 143.

[12] Se Dataskydd.net:s kommentarer till Näringsdepartementet om densamma, daterade 2017-03-03. https://dataskydd.net/vara-remissvar

Svenska mobilnät i en europeisk kontext

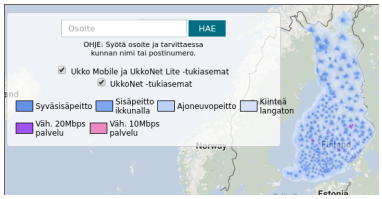
Sverige är idag en apart fågel i den europeiska mobilnätsutvecklingen. Medan många medlemsländer har tre eller fyra konkurrerande mobila nät, har Sverige fem. Sverige har atypiskt bra konkurrens, och en, i europeisk kontext, atypiskt hög täckningsgrad[13] – trots att Sverige är glesbefolkat.

Post- och telestyrelsen har tillsammans med länsstyrelserna[14] genomfört gedigna mätningar av mobil täckningsgrad i Sverige, både med avseende på yta och befolkning, och Post- och telestyrelsen identifierar lågfrekvensband, så som 450Mhz-bandet, 700MHz-bandet, 800MHz-bandet och 900MHz-bandet, som viktiga komponenter i bra, tillförlitlig tillgång till mobila kommunikationer och datatjänster på landsbygden.[15] Den lägsta täckningssiffran som uppmäts av Post- och telestyrelsen i något län är 99, 8% av befolkningen (Jämtland, täckningsgraden är dock på väg upp).[16] Relevansen av lågfrekvensband för bra täckning inses lätt av att titta på det finska företaget Ukkovarkots täckningskarta – med hjälp av sin 450MHz-licens tar de pålitligt trådlöst bredband till den nordöstfinska landsbygden.

På grund av att de privata nätägarnas infrastruktur har en så hög täckningsgrad har också konsumenter i Sverige – oavsett i vilken landsände de bor och hur glesbefolkad eller tätbefolkad denna landsände är – goda förutsättningar att hålla sig själva informerade i kristider genom att till exempel besöka statliga myndigheters webbplatser via sina smarta telefoner eller annan uppkopplad utrustning. Teleoperatörernas goda täckning ger möjligheter att ringa vanliga telefonsamtal, i de fall en konsument fortfarande inte är digitalt delaktig. Konsumenter i Sverige har gynnats väldigt mycket av den marknadsorienterade politiken regeringen hittills har drivit, och de positiva effekterna för konsumenter av god täckning och hög tjänstekvalitet kan spilla över på samhällets krishanterande tjänster, om dessa senare är villiga att låta sig dra nytta av utvecklingen.

Terrordådet i Stockholm den 7 april 2017 understryker vidare tillräckligheten och kvaliteten i de nät som redan upprättats av privata aktörer. Datatrafik fortsatte att fungera under hela den krissituation som uppstod efter dåden – och samtliga krypterade, säkra kommunikationsappar vi har nämnt ovan använder datatrafik:

> *”Tele2 skrev på sin hemsida att deras nät blev överbelastat: ”Det kan vara svårt att ringa och ta emot samtal”. Operatören uppmanar folk att prova med appar som WhatsApp, Viber, Facebook och Messenger istället.*
>
> */.../*
>
> *Just nu är nätet överbelastat i de delarna av Stockholm. Det innebär att bara hälften av alla Telenorsamtal går igenom. Vi rekommenderar därför våra kunder att använda sociala medier för att kontakta sina sociala medier, och kan också se att dataanvändningen ökar i nuläget, säger Niclas Bergervik, pressinformatör.”*
>
> – NyTeknik, 7 april 2017.[17]



Heltäckande. Täckningskarta där ljusblått indikerar täckning för trådlöst bredband och mörkblått indikerar täckning även om man befinner sig i ett hus med tjocka väggar. Tagen från http://www.ukkoverkot.fi

✻ Terrordådet i Stockholm ✻

Terrordådet i Stockholm den 7 april 2017 understryker vidare tillräckligheten och kvaliteten i de nät som redan upprättats av privata aktörer. Datatrafik fortsatte att fungera under hela den krissituation som uppstod efter dåden – och samtliga krypterade, säkra kommunikationsappar vi har nämnt ovan använder datatrafik. Flera stora teleoperatörer uppmuntrade sina kunder, via webbplatsen och via allmänna medier, att använda datatrafik istället för att ringa eller skicka sms.

[13] Se t. ex. EU-kommissionens *Digital Score Board - Sweden (Country Specific Report 2016)* eller Post- och telestyrelsens rapport Mobiltäckning 2015 (PTS-ER-2016:11) s. 20–21.

[14] *Jfr t. ex.* Täckningskollen. http://tackningskollen.se/

[15] PTS, Flera trådlösa alternativ till fast bredband. http://www.pts.se/sv/Privat/Internet/Flera-tradlosa-alternativ-till-fast-bredband/

[16] *Se ovan* PTS-ER-2016:11.

[17] NyTeknik, *Telefonnäten överbelastade efter dådet*, 7 april 2017.

Ett viktigt komplement till promemorians befintliga observationer om andra europeiska länder, vore att till exempel svårigheterna i Belgien att klara täckningskrav och robusthet har att göra med att den belgiska telekommunikationsmarknaden under lång tid fungerat mycket dåligt. Konkurrensen är låg och det har funnits misstankar om att statliga myndigheter favoriserar det gamla telemonopolet vid tilldelningen av spektrumlicenser.[18] Under en tvåårsperiod kunde Belgien till följd av utebliven regeringsbildning inte aktivt arbeta med problemen på telekommarknaden, eftersom dessa regleras på federal nivå. Det gjorde att viktiga reformer av Belgiens motsvarighet till Post- och telestyrelsen, BIPT, uteblev.

På en så dåligt fungerande marknad kan det säkert vara svårt att föreställa sig någon annan lösning än ett dedicerat statligt nät, men den svenska marknaden fungerar inte dåligt. Tvärtom fungerar den svenska marknaden bra och det kan staten dra nytta av även vid planeringen av kriskommunikation.

I både Frankrike och Tyskland har arbetsmarknadspolitiska betänkligheter länge vägt tyngre i telekompolitiken än konsumentfrämjande betänkligheter. De tidigare statliga monopolen, numera Orange och Deutsche Telekom, ses som viktiga för att de antingen har ett stort antal befintliga anställda, är ansvariga för ett stort antal tidigare anställdas pensionsfonder eller har potential att öka respektive lands exportbalans. Det gör att både Frankrike och Tyskland har dragits med en relativt långsammare utveckling av allmänna elektroniska kommunikationsnät och -tjänster än vad till exempel Sverige har, och därför finns ett annat behov av att även fortsättningsvis förlita sig på dedicerade, statliga kommunikationslösningar.

Storbritannien ska, istället för att betecknas som ett ”högriskprojekt”,[19] snarare ses som en förebild på området: trots att även Storbritanniens tidigare statsmonopol, British Telecom, ansvarar för stora pensionsfonder och höga anställningstal, lyckas den brittiska regeringen och de brittiska myndigheterna balansera de arbetsmarknadspolitiska intressena med det allmännas kriskommunikationsintressen och allmänhetens intresse av en väl fungerande kommunikationsinfrastruktur. I Sverige är förutsättningarna att lyckas med den brittiska modellen än högre, eftersom Telia inte har samma *legacy*-problem som BT i personalfrågor.

Amelia Andersdotter
Ordförande, Dataskydd.net

[18] Tweakers.net, *Belgacom krijgt gsm-licentie vijf jaar lang gratis*, 23 september 2009.
[19] Ds 2017:7, s. 118.

Källförteckning

1. Adrienne Porter Felt, Why is usable security hard, and what should we do about it?, USENIX Enigma Conference, januari 2016. https://www.usenix.org/conference/enigma2016/conference-program/presentation/porter-felt
2. Council of the European Union (14711/16) Encryption: Challenges for criminal justice in relation to the use of encryption - future steps - progress report. http://data.consilium.europa.eu/doc/document/ST-14711-2016-INIT/en/pdf
3. Council of the European Union, Response to Parliamentary Question E-009129/2016. http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2016-009129&language=EN
4. Ella Kolkowska m. fl., *Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method* Journal of strategic information systems, 6(1) p. 39-57, 2017. http://oru.diva-portal.org/smash/get/diva2:1058091/FULLTEXT01.pdf
5. Ella Kolkowska och Gurpreet Dhillon, *Organizational power and information security rule compliance*, Computers & Security 33:3-11, 2012. https://www.researchgate.net/publication/299135936_Organizational_power_and_information_security_rule_compliance
6. EU-kommissionen, *Digital Score Board - Sweden (Country Specific Report 2016).* https://ec.europa.eu/digital-single-market/en/scoreboard/sweden
7. Finansinspektionen (SEDU nr 46/2015) Understanding Terrorist Finance Modus Operandi and National CTF Regimes. http://www.fi.se/contentassets/733cb77e383d49a98aa060a16d011392/understanding_terrorist_finance_160315.pdf
8. Kommittédirektiv 2016:20 Moderna regler om beslag och husrannsakan. http://www.regeringen.se/rattsdokument/kommittedirektiv/2016/03/dir.-201620/
9. Kommittédirektiv 2016:36 Hemlig dataavläsning. http://www.regeringen.se/rattsdokument/kommittedirektiv/2016/05/dir.-201636/
10. NyTeknik, *Krypterade appar försvårar för polisen*, 28 mars 2017. http://www.nyteknik.se/digitalisering/krypterade-appar-forsvarar-for-polisen-6836085
11. Post- och telestyrelsen, Mobiltäckning 2015 (PTS-ER-2016:11). pts.se/upload/Rapporter/Radio/2016/Mobiltackning-2015.pdf
12. Totalförsvarets forskningsinstitut, Hatbudskap och våldsbejakande extremism i digitala miljöer (FOI-R–4392–SE). https://foi.se/rapportsammanfattning?reportNo=FOI-R--4392--SE
13. Tweakers.net, *Belgacom krijgt gsm-licentie vijf jaar lang gratis*, 23 september 2009. https://tweakers.net/nieuws/62667/belgacom-krijgt-gsm-licentie-vijf-jaar-lang-gratis.html