Stockholm 2021-05-06

Infrastrukturdepartementet
Enheten för samhällets digitalisering

Er referens: I2021/00342
Vår referens: 21-004

Netnod fick den 2 februari 2021 från Infrastrukturdepartementet möjlighet att komma med synpunkter på It-driftsutredningens delbetänkande *Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering*, SOU 2021:1.

Sammanfattning av Netnods synpunkter:

1. Netnod håller **inte** med utredaren om dess definition av termen *röjd*. Information kan inte anses vara röjd vid utlämning till annan part. Information anses vara röjd när information inte kan anses vara tillräckligt skyddad. Fortfarande oavsett om det är känt eller inte om någon verkligen tagit del av informationen.
2. Netnod håller **inte** med utredarens bedömning att det ska göras en liknande bedömning av överföring av information oberoende av om sådana metoder som kryptering används eller inte. Tvärtom, Netnod anser att kryptering är en god metod för att skydda information. Dessutom bör kryptering användas oavsett om hanteringen av informationen görs av underleverantör eller inte. Rutiner och processer kan och måste anpassas till vilket skyddsvärde informationen har, och detta oberoende av vem som hanterar den. Organisationen själv eller underleverantörer.
3. Netnod anser att ett **övergripande problem** med It-driftsutredningens delbetänkande är att utredningen utgår från befintlig lagstiftning som helt styrande när de egentliga behoven är ny lagstiftning som bygger på dagens tekniska miljöer. Ett exempel är de föreslagna förändringarna i Offentlighets- och sekretesslagen som vi anser resonerar sig runt problematiken istället för att sätta tydliga krav och regler.
4. Netnod noterar att utredaren inte anser det vara utkontraktering i det fall tjänster som faller under lagen (2003:389) om elektronisk kommunikation används. Detta samtidigt som tjänster som idag rekommenderas för myndigheter inte faller under denna lag (som RAKEL och SGSI). Netnod anser utredaren borde tagit höjd för de föreslagna förändringar i lagen som finns i *SOU 2021:25 Struktur för ökad motståndskraft*.

Fördjupning av Netnods synpunkter:

Det sätt på vilket kommunikation sker idag är att flera olika spelare är inblandade i varje flöde av information. Varje spelare tillhandahåller en del av den totala funktionalitet som krävs för kommunikation. Detta påpekade Statskontoret redan i rapporten 1997:18, *Svenska*

Netnod
Greta Garbos Väg 13
169 40 Solna

delen av Internet.[1] Dessa slutsatser har återkommit i ett flertal rapporter och utredningar där Netnod specifikt vill peka på den av Kungl. Ingenjörsvetenskapsakademien (IVA) publicerade slutrapporten i projektet *Digitalisering för ökad konkurrenskraft* där arkitekturen konstaterades ha övergått från att vara som stuprör till att vara som en lasagne.[2] De problem som därmed uppstår har även dessa dokumenterats relativt väl, till exempel av Totalförsvarets forskningsinstitut (FoI) i rapporten *Vilse i lasagnen? - En upptäcktsfärd i den svenska digitaliseringens mångbottnade problemstruktur*.[3]

Därför anser Netnod att utredningen utvärderar situationen på ett både alltför förenklat och för komplicerat sätt. Genom att använda lasagnemodellen som beskrivningsmodell blir det tydligt att en funktion uppnås genom att en tjänst, process eller verksamhet skapas genom i sin tur användning av andra tjänster, processer eller verksamheter.

Alla tjänster består av en kedja med fler än en underleverantör

En webbaserad tjänst som hanterar information har behov av produktion av tjänsten (webbsidan) i sig men denna kan i sin tur kräva såväl transport, lagring och beräkning vilka i sin tur var och en använder sig av programvara, operativsystem, datorer och slutligen fastigheter. Detta implementeras genom att det kan finnas flera olika tillhandahållare av de olika delarna som tillsammans skapar den webbaserade tjänsten. Varje sådan tillhandahållare (intern eller extern, privat eller offentlig) levererar en tjänst, process eller verksamhet som ska uppfylla de krav respektive köpare ställer. Bland dessa krav finns de säkerhetsrelaterade. I den kedja av leverantörer som skapas kommer därför kravställning på en leverantör leda till att krav i sin tur ställs på tjänster, processer eller verksamheter från andra (under-) leverantörer.

Netnod anser därför att utredaren gör en grov förenkling när det som undersöks är situationen att det finns en köpare (den offentliga aktören) som ska köpa en tjänst av en och endast en tillhandahållare. Sanningen är snarare att det alltid finns underleverantörer, interna eller externa. Det ska dessutom noteras att det även vid egen drift finns externa tillhandahållare som det finns beroenden till, till exempel tillhandahållare av programvara, operativsystem, datorer och fastigheter.

Ett enklare sätt att se på det är att en leverantör i sin tur kan använda sig av underleverantörer, och att leverantörer kan vara såväl interna som externa, privata och offentliga. Kravställningen är densamma, lösningarna kan variera (juridiskt och tekniskt). Ett sådant holistiskt och modernare synsätt ser Netnod till exempel i Säkerhetsskyddslag (2018:585).

Frågor som ställs i utredningen om man kan lita på olika lösningsalternativ bör därför istället vara en diskussion om vilka krav som ställs på vilka nivåer i värdekedjan, och på vilka sätt dessa krav kan implementeras och uppfyllas. Enbart med en sådan uppdelning av en tjänst kan en effektiv risk- och sårbarhetsanalys göras där olika typer av händelser identifieras, en

[1] https://www.snus.se/internetutredningen/
[2] https://www.iva.se/globalassets/projekt/201902-iva-digitalisering-slutrapport-l.pdf
[3] https://foi.se/rapportsammanfattning?reportNo=FOI-R--4814--SE

analys av sannolikhet och konsekvens för händelsen görs. Efter detta görs en utvärdering av de åtgärder som finns för att sänka sannolikhet eller konsekvens (eller båda) för att utgående från det göra en bedömning om det finns en risk att händelsen kan leda till en incident. Det vill säga om information kan anses hanteras på ett adekvat sätt eller inte.

En springande fråga är hur vi som samhälle förväntar oss att nya lösningar för säkrare informationshantering och digitalisering ska tas fram om vi i utredningsform fastslår att inga tekniska lösningar är tillräckligt säkra och att det som krävs är en absolut säkerhet såväl praktiskt som teoretiskt? Samtidigt så verkar skyddsvärde inte spela någon egentlig roll eftersom man föreslår att ingen sekretess ska gälla om överlämnandet bara avser teknisk bearbetning.

Man måste göra en risk- och sårbarhetsanalys

I praktiken bygger all säkerhet på en risk- och sårbarhetsanalys där olika skyddsmekanismer skapas för att höja förmågan gällande att möta olika typer av hot. Som exempel finns de av Militära underrättelse- och säkerhetstjänsten (Must) godkända krypteringsmetoder och rutiner för att kunna hantera enligt Säkerhetsskyddslagens skyddsvärd information upp till dess högsta skyddsnivå. It-driftutredningens resonemang gör att de ifrågasätter denna modell och indirekt MUST kompetens på området och att den hantering av risker gällande skyddsvärd information som hittills använts i samhället förkastas.

Som exempel på detta är när utredaren skriver att man skall kunna bryta sekretess i vissa fall för att kunna göra "outsourcing av IT" men samtidigt refererar till teknisk lagring eller teknisk bearbetning, vilket är ett vidare begrepp som innefattar exempelvis de (egna) WAN, som idag köps som tjänst. Till exempel sker detta genom lösningen SGSI som implementerats genom en lång kedja av kund/leverantörsförhållanden som anses vara acceptabla vid överföring av information mellan två geografiskt separerade delar av en organisation via en tjänst som tillhandahålls av en tredje part. Denna tjänst, SGSI faller dessutom inte under lag (2003:389) om elektronisk kommunikation, vilket enligt utredaren krävs för att det inte ska räknas som en utkontraktering. Utredaren drar dessutom slutsatsen att tjänster, processer eller verksamheter som faller under denna lag ej kan utföras av myndigheten själv vilket Netnod anser vara felaktigt. Snarare är det som så att alla de tjänster, processer eller verksamheter som uppfyller de rekvisit som finns i lagen faller under densamma

> *Nyttjande av sådana elektroniska kommunikationstjänster som regleras i lagen (2003:389) om elektronisk kommunikation innebär enligt vår definition inte heller utkontraktering, eftersom det inte är fråga om en tjänst, process eller verksamhet som annars skulle ha utförts av myndigheten själv.*

Detta skulle ge att frågan om utkontraktering sker eller inte beror på vilken kompetens organisationen har, vilket är högst förvirrande. Kravställning måste ställas på informationshantering oavsett om den är intern eller extern, av offentlig eller privat aktör. Dessa krav uppfylls genom en blandning av avtalsmässiga, juridiska och tekniska lösningar.

En slutsats som skulle kunna dras är att lag (2003:389) behöver utökas att täcka alla typer av kommunikation i samhället och inte bara de tjänster som tillhandahålls av tillståndspliktiga leverantörer, dvs leverantörer av allmänna kommunikationstjänster, vilket i praktiken *SOU 2021:25 Struktur för ökad motståndskraft* kan sägas göra genom att föreslå ett utökat ansvar för PTS. Detta om lagen (och dess förordning etc) kan anses påverka möjligheten att få adekvat skydd för information i ett förhållande mellan kund och leverantör.

När kan en uppgift anses vara röjd?

Utredaren skriver vidare:

> *Vi bedömer att en myndighet som utkontrakterar it-drift har lämnat ut de uppgifter som omfattas av utkontrakteringen till tjänsteleverantören. Detta gäller oavsett om omständigheterna när uppgifterna tillgängliggjordes tjänsteleverantören var sådana att man – t.ex. pga. kryptering eller annan teknisk säkerhetsåtgärd – inte måste ha räknat med att tjänsteleverantören eller någon annan utomstående skulle komma att ta del av uppgifterna.*

Detta innebär i förlängningen att de tidigare nämnda teknikerna VPN, SD-WAN, MPLS inte är möjliga tekniker att använda då teknisk bearbetning sker hos tredje part, och detta oavsett om krypto används eller inte.

Istället bör man anse en uppgift vara röjd först då någon kan ta del av den. Det är exakt därför kryptering används som skydd, och en bedömning ska göras vid varje tillfälle baserat på bedömt skyddsvärde vilken kryptering som är adekvat. Annars blir slutsatsen att all krypterad trafik utanför myndigheten är röjd, vilket inte kan vara utredarens åsikt då det strider mot annan reglering.

Dessutom kan information bli röjd även om informationen hanteras av organisationen själv. Det finns ett flertal fall då det vid dåligt handhavande av information av organisationer som själv hanterat information uppstått informationsläckage eller intrång. Likaså måste information kunna hanteras av en underleverantör utan att den är röjd, och detta om information anses ha tillräckligt juridiskt och tekniskt skydd, vilket till exempel är beskrivet i Säkerhetsskyddslagen och -förordningen. Exempel på skyddsmekanismer är som tidigare nämnts säkerhetsskyddsavtal och av MUST godkänt krypto.

Krypto måste alltid användas

Krypto är därför ett skydd som rekommenderas att användas inom en organisation för att inte en antagonist vid ett lyckat intrång kan komma åt informationen. Det gäller att för gott försvar kunna bryta den kedja av händelser som till exempel beskrivs av Lockheed Martin i deras av dem kallade *Cyber Kill Chain*.[4] Det är idag alldeles för många organisationer som

[4] https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

väljer att inte utkontraktera (till specialister) just för att de är oroliga över den avtalsmässiga situationen. Resultatet blir, om och om igen, att den egna interna driften har för låg förmåga vilket visar sig vid intrång eller andra typer av incidenter.

Det utredaren skriver implicerar att kryptografi saknar funktion, vilket Netnod inte håller med om. Om det skulle vara så har vi ett ganska stort problem i Sverige.

Skyddsvärde

På sidan 73 skriver utredaren vidare:

> *I vår enkät ställde vi också frågan om myndigheterna utgår från någon standard eller modell som stöd för ett systematiskt informationssäkerhetsarbete. 77 procent av myndigheterna har svarat att de utgår från en standard som stöd för ett systematiskt informationssäkerhetsarbete. Bland dessa utgår alla myndigheter utom en från ISO 27001. Det är en av de standarder som rekommenderas i de nya föreskrifterna från MSB. Knappt 20 procent av myndigheterna anger att de inte utgår från någon standard och sex myndigheter (4 procent) har svarat att de inte vet om de gör det.*

Det står också att:

> *Reglerna om informationssäkerhet skiljer sig delvis åt mellan statliga myndigheter å ena sidan och kommuner och regioner å den andra. För statliga myndigheter gäller förordningen om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap och de föreskrifter som MSB meddelat med stöd av förordningen.*

Vi kan inte ha en situation där information har olika skyddsvärde beroende på vilken typ av organisation som handlägger den. Om kommuner och regioner inte har resurser att upprätthålla korrekt säkerhet, i jämförelse med andra myndigheter, så bör de hindras att hantera denna information. Detta istället för att lagstiftningen anpassas. Som tidigare påpekats måste man för att kunna göra en adekvat genomlysning först ställa tydliga krav och därefter se hur detta kan implementeras och det både tekniskt och juridiskt.

Ny lagstiftning, NIS-2

Netnod har som tidigare nämnts åsikten att utredaren har utgått alldeles för mycket från dagens juridiska situation och dessutom OSL. Man har inte tittat tillräckligt på annan existerande eller kommande lagstiftning eller hur skydd och kund/leverantörsförhållanden implementeras i praktiken. Ett exempel på kommande lagstiftning är det föreslagna så kallade NIS2-direktivet som i Artikel 18 (2) skriver:

> *2. De åtgärder som avses i punkt 1 ska åtminstone inbegripa*
> *(a) strategier för riskanalys och informationssystemens säkerhet,*
> *(b) incidenthantering (förebyggande, upptäckt och åtgärder till följd av incidenter),*
> *(c) driftskontinuitet och krishantering,*

(d) *säkerhet i leveranskedjan, inbegripet säkerhetsaspekter som rör förbindelserna mellan varje entitet och dess leverantörer eller tjänsteleverantörer, såsom leverantörer av datalagrings- och databehandlingstjänster eller hanterade säkerhetstjänster,*

(e) *säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem, inbegripet hantering av och information om sårbarheter,*

(f) *strategier och förfaranden (testning och revision) för att bedöma effektiviteten i riskhanteringsåtgärderna för cybersäkerhet,*

(g) *användning av kryptografi och kryptering.*

Vi ser även här att hantering av skyddsvärd information måste börja med en identifiering av vilket skyddsvärde informationen har, och sedan utgående från detta skapa en kravställning på alla ingående processer och verktyg som behöver vara koordinerade för att ett skydd ska existera. Att se enbart på en av alla delar ger inte ett förtroligt svar.

Även information som hanteras inom en organisation måste skyddas

Vi ser också flera fall där information frigjorts (eller låsts fast av ransomware) för att man misslyckats med att skydda information på ett adekvat sätt. Kompetens har helt enkelt saknats, och denna brist på kompetens pekar utredaren på. En av de största sannolikheten för att man tappar information på ett eller annat sätt med olika stora konsekvenser är just genom eget handhavandefel. De senaste årens erfarenheter av molntjänster är att de är säkrare, inklusive att de har en mycket högre tillgänglighet än egen drift, och i de fall något driftsätts av en organisation själv ska detta ses tekniskt som en molntjänst med motsvarande kravställning.

Netnod anser detta är huvudanledningen till att public/hybrid cloud uppskattas och används i så stor omfattning, dvs att man får så god funktionalitet och skydd till ett acceptabelt pris när man är i en situation att man får ett kund/leverantörsförhållande där korrekta krav kan ställas. Och, återigen, detta oberoende av om underleverantören är inom den egna organisationen eller är en underleverantör.

Patrik Fältström
Teknik- och Säkerhetsskyddschef
Tel: +46-706059051
Email: paf@netnod.se