INTERNET STIFTELSEN

I2021/00342

Internetstiftelsens remissvar på It-driftsutredningens delbetänkande Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering (SOU 2021:1)

Om Internetstiftelsen

Internetstiftelsen är en oberoende, affärsdriven och allmännyttig organisation. Vi verkar för ett internet som bidrar positivt till människan och samhället.

Vi är en stiftelse och vår urkund slår fast att vi ska säkerställa en stark och säker infrastruktur för internet som tillgodoser dagens och framtidens behov i Sverige samt främja forskning, utbildning och undervisning med inriktning på internet. Vi ansvarar för internets svenska toppdomän .se och sköter även drift och administration av toppdomänen .nu. Intäkterna från affärsverksamheten finansierar en rad satsningar i syfte att möjliggöra att människor kan nyttja internet på bästa sätt och att ge kunskap om internetanvändningen i Sverige samt digitaliseringens påverkan på samhället. Vi tillhandahåller evenemang och utbildningsinsatser som gör det enklare att förstå och använda internets tjänster och som bidrar till ökad kompetens och fler möten som främjar internetinnovation. Vi stöttar även olika fristående uppdrags- och forskningsprojekt som på olika sätt gynnar internets utveckling och ger förutsättningar för internetentreprenörer och utvecklare att ta steget från idéstadie till färdig produkt eller tjänst. Med våra identitetsfederationer förenklar vi inloggning och höjer säkerheten i identitets- och kontohantering för både användare och leverantörer av olika tjänster inom skola, hälso- och sjukvård.

Internetstiftelsen har blivit tillfrågade att lämna remissvar på delbetänkande från utredningen om Säker och kostnadseffektiv IT-drift (SOU 2021:1). Internetstiftelsens CISO har deltagit i den referensgrupp som regeringen utsett för att biträda utredningen.

Internetstiftelsens remissvar är främst avgränsat till de delar av utredningens bedömningar som rör frågan om *kryptering* samt *krav på skyddsåtgärder*.

Övergripande synpunkter

I ett digitaliserat samhälle är de informationstillgångar som hanteras ofta verksamhetskritiska. Med hjälp av säkra kryptografiska funktioner går det emellertid att skydda sådana informationstillgångar. Se Internetstiftelsens kommentarer på avsnitt 10 nedan.

Även om det i leverantörsavtalet finns med klausuler om att hantering av information ska ske säkert har myndigheterna fortfarande ansvar för att följa upp hur säkert *säkert* är, det vill säga att kunna göra uppföljningar av att kraven är uppfyllda.

Internetstiftelsen anser att utredningen lagt ner oproportionerligt mycket kraft på att diskutera OSL och röjandebegreppet, medan den viktiga frågan om hantering av information under annan lagstiftning inte har behandlats mer än övergripande.

10 En sekretessbrytande bestämmelse

Avsnitt 10.1.4 avtalsreglerad tystnadsplikt, kryptering och pseudonymisering

I avsnitt 10.1.4 framhåller utredningen att det inte finns några *”nu kända säkerhetsåtgärder som gör det helt, både i teori och praktik, omöjligt för tjänsteleverantören att ta del av uppgifterna”.*

Det påståendet är **enligt Internetstiftelsen** direkt felaktigt. Det finns idag sådana tekniker, som exempelvis one-time-padkrypton eller kvantkrypton. Nackdelen med dessa tekniker är att de är opraktiska och komplexa, men de existerar i allra högsta grad.

Verksamhetskritiska informationstillgångar utgör oftast inte bara ett stort värde för den egna verksamheten, den kan också vara värdefull för andra. Ett tydligt tecken på att så är fallet är enligt Internetstiftelsen den kraftiga ökningen av statsunderstödda attacker det senaste året.

Verksamhetskritiska informationstillgångar kan handla om staters relationer till varandra, uppgifter om enskilda medborgare, företagshemligheter, risk- och sårbarhetsanalyser om en specifik verksamhet, uppgifter som rör enskildas hälsotillstånd, personuppgifter med mera.

Möjligheterna att skydda information från att någon utan tillåtelse ska kunna få tillgång till viktig information ökar och på marknaden finns ett stort utbud av produkter och tjänster inom detta område.

Krav på att använda signalskyddssystem framgår i Säkerhetsskyddsförordning (2018:658), 3 kap. Informationssäkerhet

5 § Innan säkerhetsskyddsklassificerade uppgifter behandlas i ett informationssystem utanför verksamhetsutövarens kontroll ska denne försäkra sig om att säkerhetsskyddet för uppgifterna i systemet är tillräckligt.
Om säkerhetsskyddsklassificerade uppgifter ska kommuniceras till ett informationssystem utanför verksamhetsutövarens kontroll ska uppgifterna skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten.

Nationellt godkända kryptosystem ger säkra kryptografiska funktioner. I dag finns det flera olika varianter av nationellt godkända kryptosystem som skyddar en verksamhets informationstillgångar.

Genom att svenska myndigheter ställer krav och granskar säkerheten i produkterna eller tjänsterna kan det hållas för sannolikt att de utför de funktioner de är avsedda för

att göra och att det inte finns några dolda fel eller funktioner i produkterna. I kombination med en säker hantering och en tydlig dokumentation bidrar sådana system till att höja säkerheten i en verksamhets informations- och kommunikationssystem.

Avsnitt 10.1.15 om CLOUD Act och liknande regleringar

I avsnitt 10.1.15 anger utredningen att CLOUD Act och liknande regleringar inte har någon betydelse för frågan om uppgifterna anses ha röjts. **Internetstiftelsen anser** att utredningen inte i tillräcklig omfattning har resonerat kring det faktum att om svenska myndigheter lämnar ut information till en leverantör som lyder under en annan rättsordning än den svenska så har myndigheten förlorat den juridiska kontrollen över informationen. En svensk myndighet som har sekretessbelagd information ska enligt OSL ha full kontroll över när sådan information lämnas vidare till någon annan.

Närmare om en sekretessbrytande bestämmelse

Internetstiftelsen noterar att utredningen har kommit till annan bedömning än tidigare utredning som behandlat frågan om utformning av sekretessbrytande bestämmelse. I SOU 2018:25 (Juridik som stöd för förvaltningens digitalisering) punkt 10.6.5 resoneras kring skyddet för sekretessintressen genom en intresseavvägning, där hänsyn ska tas till integritetsintressen rörande enskilda och skydd för det allmänna. Utredningen lämnar som förslag att en uppgift inte ska lämnas ut om övervägande skäl talar för att det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut, eller om det av andra skäl är olämpligt.

En sekretessbrytande bestämmelse enligt utredningens förslag som tar sikte på utkontraktering av it-drift om myndighetens behov att lämna ut uppgifter vilket då skulle väga tyngre än de intressen som sekretessen avser att skydda, riskerar **enligt Internetstiftelsen** att undergräva samhällets totala skyddsnivå. Detta eftersom utredningens slutsats är att sekretess inte hindrar en myndighet från att lämna ut uppgifter till en tjänsteleverantör som har i uppdrag att endast tekniskt bearbeta eller tekniskt lagra uppgifterna för myndighetens räkning. Det måste fortfarande **enligt Internetstiftelsen** ställas krav på skyddsåtgärder som är relevanta i sammanhanget.

Till detta kommer även förslaget till ett omarbetat NIS-direktiv, NIS2. I Artikel 18 av direktivet ställs krav på riskhanteringsåtgärder för cybersäkerhet, och där medlemsstaterna ska säkerställa att väsentliga och viktiga entiteter vidtar lämpliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder för att tillhandahålla sina tjänster. Med beaktande av den senaste tekniska utvecklingen ska dessa åtgärder säkerställa en säkerhetsnivå i nätverks- och informationssystem som är lämplig i förhållande till den föreliggande risken.

De åtgärder som avses i det omarbetade NIS-direktivet 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.

Faktum är att kraven på myndigheternas arbete med informationssäkerhet kommer att skärpas allt eftersom EU-direktiven antas och omsätts i svensk lag.

Sammanfattning

Enligt direktiven är syftet med utredningen att skapa bättre förutsättningar för den offentliga förvaltningen att få tillgång till säker och kostnadseffektiv it-drift genom antingen samordnad statlig it-drift eller tydligare rättsliga förutsättningar för att kunna anlita privata leverantörer av it-drift.

Internetstiftelsen anser att utredningen har felaktiga utgångspunkter när det gäller vilket skydd som kan åstadkommas med hjälp av krypteringsåtgärder. Korrekt använd krypteringsteknik innebär att uppgifter inte kan sägas ha gjorts tillgängliga för tjänsteleverantören.

Internetstiftelsen anser att utredningen i oproportionerligt hög grad lagt kraft på OSL och den osäkerhet som funnits kring röjandebegreppet, inte att lösa utmaningar med till exempel tredjelands rättsordning utifrån gällande EU-lagstiftning och därmed inte heller tillräckligt belyst frågan om hur kontrollen över informationen ska hanteras om den hamnar hos en leverantör under annan rättsordning än den svenska.

Internetstiftelsen anser slutligen att förslaget om sekretessbrytande bestämmelse undergräver skyddsnivån hos svenska myndigheter om detta inte kombineras med konkreta och relevanta krav på skyddsåtgärder.

Revideringen av NIS 2 och införandet av Cyber Security Act kommer att ställa ännu starkare krav på verksamheter inom EU att leva upp till höga krav på informationssäkerhet.

Stockholm den

Carl Piva,

Vd, Internetstiftelsen