INTERNET STIFTELSEN

Dnr: 20-7032

Internetstiftelsens remissvar på förslag till nya föreskrifter och allmänna råd om säkerhetsåtgärder för leverantörer av samhällsviktiga tjänster enligt NIS-lagen

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.

Övergripande synpunkter

Internetstiftelsen har beslutat att lämna remissvar på förslag till nya föreskrifter och allmänna råd om säkerhetsåtgärder för leverantörer av samhällsviktiga tjänster inom sektorn digital infrastruktur enligt lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen). Föreskrifterna syftar till att förtydliga bestämmelserna om säkerhetsåtgärder 12-14 §§ NIS-lagen samt Myndighetens för samhällsskydd och beredskap (MSB:s) föreskrifter och allmänna råd om informationssäkerhet för leverantörer av samhällsviktiga tjänster (MSBFS 2018:8), som gäller sedan 2018. Vi har även lämnat synpunkter på den konsekvensutredning som bifogats de föreslagna föreskrifterna.

Internetstiftelsen är av uppfattningen att det är bra att kraven i den så kallade NIS-lagen förtydligas i föreskrifter från tillsynsansvariga myndigheter. En otydlig och vag kravställning ger sannolikt inte förväntad effekt. En ökad tydlighet från myndighetens sida är ett viktigt steg för att föreskrifter både ska kunna efterlevas och bidra till en högre skyddsnivå.

Detaljerade synpunkter - Riskanalys och riskbedömning

Internetstiftelsen anser att 4 § i huvudsak anger de olika delar som en riskanalys åtminstone ska innefatta på ett bra sätt, vilket kan förväntas ge mindre osäkerhet vid den praktiska tillämpningen.

Hot som bör analyseras 4 §

Den föreslagna föreskriften anger att analys av organisatoriska hot åtminstone bör omfatta ”*bristfälliga processer för att uppnå en hög säkerhet i nätverk och informationssystem (särskilt bristfälliga rutiner vid förändringshantering)*.”

Internetstiftelsen ställer sig frågande till hur den med kursivering markerade delen av stycket ovan förhåller sig till stycket som följer längre ner, som lyder:

”Riskanalyser bör innehålla planerade förändringar som kan få negativa konsekvenser på säkerheten i nätverk och informationssystem…”

Internetstiftelsen föreslår att texten i stycket ovan tas bort eller förenklas så att det blir tydligt vad som adresseras här, som inte har adresserats i det tidigare stycket.

Kvalificerade bedömningar 4 §

Enligt Internetstiftelsens uppfattning är det för otydligt att skriva “kan” i en föreskrift som preciserar krav som ställs. Begreppet *kan* i en föreskrift innebär en oklarhet i om det är en frivillig åtgärd eller inte. Stiftelsen är av uppfattningen att detta stycke kan tas bort eftersom PTS tidigare i dokumentet bland annat skrivit att man *ska* utgå från vedertagen standard på området.

Internetstiftelsen vill dessutom göra PTS uppmärksam på att den föreslagna beskrivningen varken stämmer med sannolikhetsnivåerna eller konsekvensgraderna som finns i MSB:s metodstöd för riskanalys.

Deltagare i riskanalysarbetet, 5 §

Den föreslagna föreskriften 5 §, punkt 3 lyder: “Leverantörens dokumentation av riskanalysarbetet ska innehålla en hänvisning till riskanalysen.”

Såvitt Internetstiftelsen kan bedöma blir detta i de allra flesta fall en hänvisning till sig själv? Internetstiftelsen är av uppfattningen att riskanalysen är dokumentationen av riskanalysarbetet. Det är den handling som dokumenterar de resonemang som leder fram till vad som är skyddsvärt. Riskanalysen relaterar det skyddsvärda till de hot som verksamheten kan utsättas för och de sårbarheter som verksamheten kan vara behäftad med. I förlängningen syftar riskanalysen till att ta fram ett beslutsunderlag för skyddsåtgärder samt att skapa spårbarhet för detta underlag.

Leverantörens dokumentation, 5 §

Internetstiftelsen tolkar denna paragraf som att man ställer krav på att (1) metoden för riskanalysen ska vara dokumenterad samt att (2) dokumentation från riskanalyser ska

bevaras i 5 år. Enligt Internetstiftelsens uppfattning saknas utöver detta krav på dokumentation av riskägares utverkande av acceptans av (eventuell) kvarstående risk.

Åtgärder och åtgärdsplan

I 6 § föreslås följande lydelse *"samtliga åtgärder ska vidtas på en nivå som är proportionerlig i förhållande till den föreliggande risken".*

Internetstiftelsen saknar ett tydligt uttalande om mot vad den proportionaliteten ska ställas. Även om vi förstår att det avser kostnader för införande behöver det enligt Internetstiftelsens uppfattning förtydligas.

Längre ner i samma stycke anges: *"I den bedömningen ska leverantören beakta samtliga tekniska lösningar som vid var tid finns tillgängliga på marknaden."*

Internetstiftelsen betonar att allt inte nödvändigtvis löses med teknik. Det kan i vissa fall lika gärna lösas med administrativa och/eller organisatoriska åtgärder. Enligt Internetstiftelsens uppfattning är det dessutom ett orimligt krav att leverantören ska ha kännedom och kunskap om samtliga tekniska lösningar på marknaden. Det är ett krav som inte heller är möjligt att följa upp. Vi föreslår en alternativ formulering:

Leverantören [..] ska vidta de risklindrande åtgärder som anses lämpliga och tillräckliga med beaktande av tillgänglig teknik, kostnaden för genomförandet av åtgärderna och definierade kriterier för riskacceptans.

Internetstiftelsen anser att punkt 1-8 i 7 § på ett korrekt sätt anger de åtgärder som ska dokumenteras i åtgärdsplanen. Internetstiftelsen anser vidare att den föreslagna tidsperioden på fem år eller till dess att åtgärdsplanen uppdateras är lämplig.

Fysiska och logiska skydd 8 §

Enligt Internetstiftelsens uppfattning överlappar åtgärderna i 8 § de åtgärder som ska vidtas med stöd av 6-7 §§. Vår bedömning är att 8 § kan tas bort, alternativt att det tydligare förklaras vad skillnaden är mellan föreskrifterna. Internetstiftelsen anser att riskbedömningen ska omfatta fysiska och logiska risker vilket leder till åtgärder som ska vidtas för att lindra risker som identifierats genom riskbedömningen.

Allmänna råd – Fysiska och logiska skydd 8 §

Internetstiftelsen anser att kraven är överlappande även här. Detta har redan räknats upp bland de hot som ska analyseras (och därför också ska hanteras genom åtgärder då det befinns nödvändigt). Stycket kan enligt Internetstiftelsens mening tas bort.

Fysisk och logisk behörighets- och åtkomsthantering 11 §

Internetstiftelsen föreslår att pluralformen för person istället bör användas, alltså ”personer”.

Internetstiftelsen anser att begreppet ”system” bör bytas ut, eftersom man inte ger ett helt system åtkomst i egentlig mening, utan kanske snarare en automatiserad process.

Enligt Internetstiftelsen är kärnan i kravet att åtkomsten är kontrollerad och begränsad. Vi föreslår därför en alternativ formulering, ungefär enligt följande exempel:

Leverantören […] ska vidta åtgärder för att styra och begränsa åtkomst till nätverk och informationssystem till behöriga systemidentiteter.

Allmänna råd - Åtkomsthantering, 11 §

Internetstiftelsen föreslår att ordet “system” byts ut mot ordet “processer”.

Synpunkter på konsekvensutredningen (Dnr 20-7032)

Internetstiftelsen vill även lämna några kommentarer till de förtydliganden och förklaringar som presenteras i PTS konsekvensutredning för de föreslagna föreskrifterna.

Avsnitt 2.1 Domännamnssystemet – väsentligt för fungerande digitalt samhälle

I 2.1 saknar Internetstiftelsen en källreferens till påståendet att antalet attacker mot DNS förutspås fördubblas från 2018 till 2023. Att överbelastningsattackerna förväntas öka kommer att kräva vidareutvecklade säkerhetsåtgärder.

Avsnitt 2.4.3 Säkerhetsåtgärder som leverantören vidtar utifrån sin riskanalys är det lämpligaste regeringsalternativet

Felstavning i rubriken, ska vara regleringsalternativet, inte regeringsalternativet.

Avsnitt 3 Aktörer som berörs av regleringen

I MSBFS 2018:7, 9 kap. Identifiering av leverantörer av samhällsviktiga tjänster inom digital infrastruktur anges:

> *1 § Med samhällsviktiga tjänster rörande digital infrastruktur där incidenter skulle medföra en betydande störning vid tillhandahållandet av tjänsten avses*
>
> *1. administration och förvaltning av domännamn på internet som utförs av registreringsenheter för toppdomäner med fler än 250 000 aktiva domäner, eller*
>
> *2. DNS-tjänster i form av*
>
> *a) en auktoritativ namnservertjänst som har fler än 25 000 aktiva domännamn anslutna, eller*
>
> *b) en rekursiv namnservertjänst som används av fler än 100 000 användare.*

Internetstiftelsen har inget problem med att tolka punkt 1 ovan, om registreringsenheter för toppdomäner. Däremot anser Internetstiftelsen att PTS behöver förtydliga MSB:s

vägledning för anmälan och identifiering av leverantörer av samhällsviktiga tjänster enligt NIS-regleringen när det gäller vad som avses med leverantörer av DNS-tjänster. Detta skulle underlätta för leverantörer av DNS-tjänster att avgöra om de har anmälningsskyldighet. Under samtal som Internetstiftelsen fört med många aktörer i branschen har det framkommit ett antal frågor som vi tror PTS kan och bör besvara. Dessa svar skulle vara en mycket användbar vägledning för branschen där många aktörer är småföretagare som inte har egen juridisk kompetens, och små möjligheter att skaffa sådan hjälp externt. En lättillgänglig vägledning skulle hjälpa många att kunna göra rätt för sig. Följande är några av de frågor som Internetstiftelsen identifierat

Auktoritativa DNS tjänster

- Ska bara .se-domäner räknas? Bara europeiska ccTLD-domäner? Alla domäner oavsett TLD?
- Om kunden finns i ett annat land, ska den räknas?
- Om alla DNS servrar står i ett annat land, vad gäller då?
- Ska huvuddomäner och/eller subdomäner som av kunden till DNS-tjänsten definierats som zoner, räknas som zoner/domäner, det vill säga om sll.se, karolinska.sll.se och sos.sll.se av kunden i tjänsten har definierats som tre separata zoner, ska dessa då räknas som tre domäner?

Resolvertjänster

- Hur ska kundantalet beräknas?
- Räknas kunder i andra länder? Inom eller utanför EU?
- Är antal kunder lika med antal unika IP-adresser som ansluter?
- Hur ska en öppen resolver-tjänst (som inte säljer tjänsten) räkna antal användare?

Incidentrapportering

- När är ett fel så allvarligt att det måste rapporteras?
- Om bara en av servrar går offline?
- Om mer än hälften går offline?
- Bara om alla servrar är onåbar?

Avsnitt 3.2 Antalet företag som berörs och storleken på företagen

Av texten ”Därtill finns också två svenska stiftelser, vilka har cirka 30 respektive 70 anställda, men vars årsomsättning är okänd” drar Internetstiftelsen slutsatsen att en av de två svenska stiftelser som omnämns är vår. Det är långt ifrån okänt vilken årsomsättning Internetstiftelsen har. På https://internetstiftelsen.se/om-oss/mer-om-oss/arsredovisningar/ kan man hitta alla årsredovisningar från 2009 och framåt.

Avsnitt 4.3 Riskanalys, riskbedömning och dokumentation 4-5 §§

I punkt 5 nämner PTS accepterad risk, men inte att riskacceptans ska dokumenteras som Internetstiftelsen också kommenterar i svaret på förslaget till föreskrifter.

Över huvud taget är både föreskrifter och konsekvensutredning fokuserade på nätverk och informationssystem, medan man inte alls nämner de informationstillgångar som hanteras i dessa nätverk och informationssystem, något som Internetstiftlesen anser är av stor betydelse för ett definiera skyddsvärde och därmed komma fram till proportionerliga skyddsåtgärder.

Avsnitt 4.3 Riskanalys, riskbedömning och dokumentation 4 - 5 §§

I stycket Kostnader 4 § på sidan 22 hänvisar PTS till etablerade standarder för riskanalyser och skriver:

“Att leverantören kan välja riskanalysmetod innebär att leverantören kan behålla en sedan tidigare fungerande metod eller välja den metod som bäst passar verksamheten. Den valda riskanalysmetoden ska dock utgå från en etablerad standard, exempelvis SS-EN ISO/EIC 27001:2017 alternativt 27002:2017”.

Riskanalysmetod berörs inte i varken 27001 eller 27002. De etablerade standarder som finns är ISO 31000 respektive ISO 27005, och dessa har lite olika scope. ISO 31010 anger olika metoder (allmänt) medan ISO 27005-standarden ger riktlinjer för hantering av informationssäkerhetsrisker och stödjer de allmänna koncept som anges i ISO/IEC 27001. Den är utformad för att hjälpa till med implementering av informationssäkerhet baserat på en riskhanteringsstrategi. ISO 31000 tillhandahåller principer, ramverk och en process för hantering av risker. Den beaktar alla typer av risker till skillnad från de tidigare nämnda 27005 som alltså är specifik för informationssäkerhetsrisker.

Det är inte fel att ha referenser till både ISO 31000 och 27005, men det är enligt Internetstiftelsen inte korrekt att i detta sammanhang referera till ISO 27001 och 27002.

Kostnader 4-5 §§

Kostnadsberäkningarna som PTS gör i sin konsekvensanalys förefaller mycket summariska. Internetstiftelsen har lång erfarenhet av att göra regelbundna riskanalyser där förberedelse, genomförande och sammanställning av rapport tar ungefär 30 timmar, återföring och individuella bedömningar, 4 timmar (givet 30 minuter * 8 deltagare), slutrapport 4 timmar, handlingsplan 2-3 timmar. Det vill säga cirka 40 timmar/analys. Även om riskanalyser kan grupperas räcker det i allmänhet inte med att bara göra en. De 40 timmarna ska alltså multipliceras med antalet riskanalyser. Till det kommer val och eventuell upphandling av lösning samt implementation vilket varierar beroende på vilka åtgärder som behöver genomföras.

Från Internetstiftelsens erfarenhet är även 30 timmar per år för omvärldsbevakning lågt räknat.

Avsnitt 4.5 Åtgärdsplan

I stycke 4.5.4, Hantering av planerade tekniska och organisatoriska förändringar, 12 § hänvisar PTS till etablerade standarder, Internetstiftelsen saknar kommentar i konsekvensutredningen till vilken standard som avses.

Sammanfattning

Internetstiftelsen är positiv till att kraven i den så kallade NIS-lagen förtydligas i föreskrifter och allmänna råd från tillsynsansvariga myndigheter. Detta till trots lämnar vi ett antal detaljerade synpunkter för att ytterligare förtydliga kraven, så som Internetstiftelsen bedömer det. Det är enligt Internetstiftelsen också viktigt att det sker en harmonisering mellan MSB:s föreskrifter och metodstöd och de föreskrifter och allmänna råd som PTS utfärdar för att ytterligare underlätta tolkningen av NIS-lagen.

Stockholm den 24 augusti 2020

Danny Aerts,

Vd, Internetstiftelsen