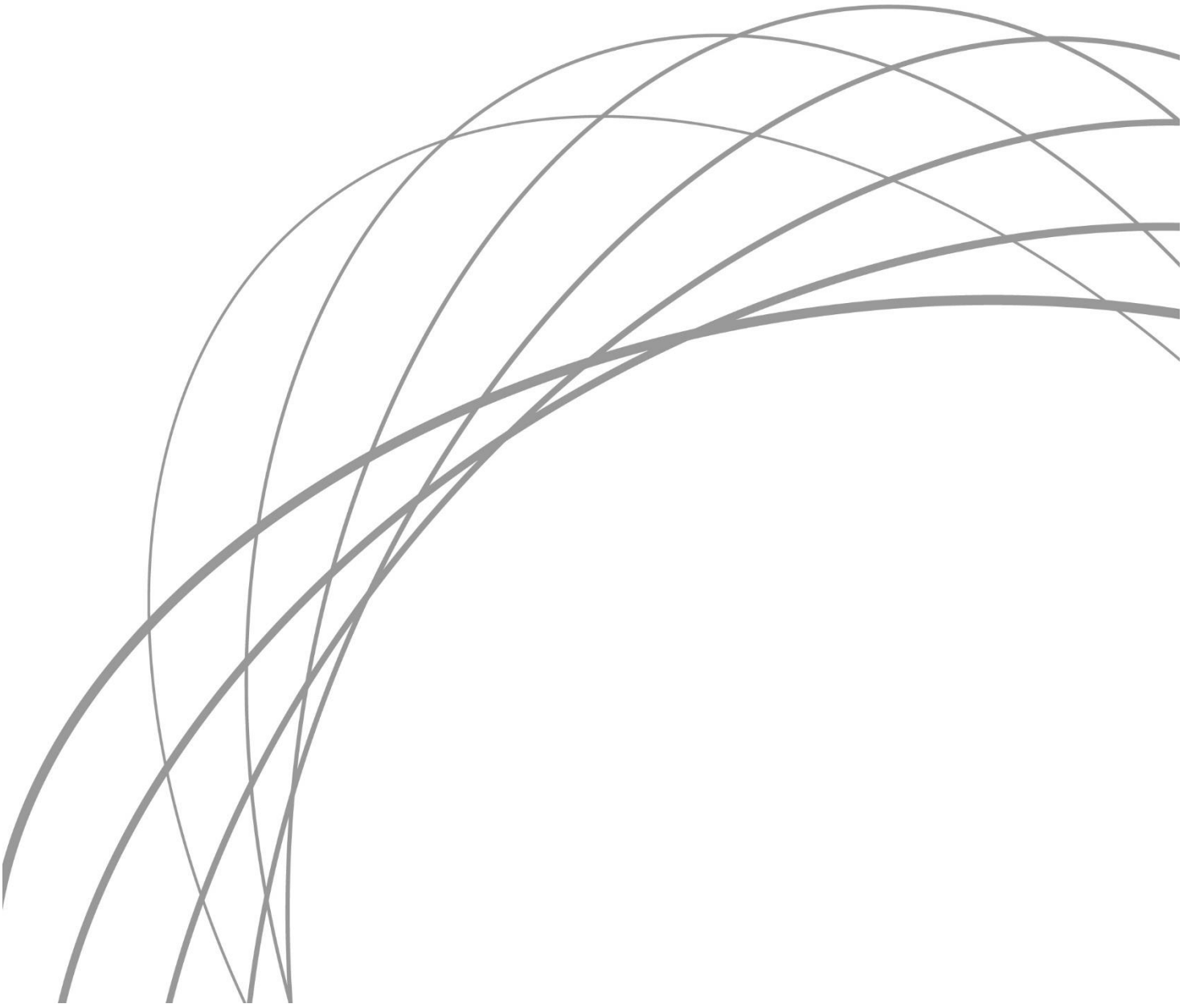
2020-06-18

För dig som leverantör av digitala tjänster enligt NIS-lagen

Vi vill på detta sätt ge aktuell information om reglerna i NIS för att underlätta för er att följa kraven på säkerhetsåtgärder och incidentrapportering.

Nr 2/2020



Innehåll

Post- och telestyrelsen

Postadress:
Box 5398
102 49 Stockholm

Besöksadress:
Valhallavägen 117 A
www.pts.se

Telefon: 08-678 55 00
Telefax: 08-678 55 05
pts@pts.se

PTS arbete med anledning av coronaviruset

Den rådande situationen med anledning av coronaviruset (covid-19) har påverkat hela samhället. PTS har sedan i mitten av februari 2020 en krisstab igång som bevakar och hanterar händelser knutna till smittspridningen av coronaviruset. Krisstaben sammanställer lägesbild för PTS egen verksamhet och myndighetens ansvarsområden (postsektorn och sektorn för elektronisk kommunikation) samt svarar upp mot andra aktörers informationsbehov (till exempel Myndigheten för samhällsskydd och beredskap, MSB).

PTS har därför ställt frågor om pandemins påverkan till aktörer som omfattas av NIS-lagen, både leverantörer av samhällsviktiga tjänster (DNS-leverantörer, TLD-leverantörer) och leverantörer av digitala tjänster (molntjänstleverantörer, internetbaserade marknadsplatser, internetbaserade sökmotorer). Frågorna till leverantörer av digitala tjänster löd:

- Hur ser er verksamhets förmåga ut vad gäller upprätthållande av era digitala tjänster på kort och lång sikt?

- Har några särskilda utmaningar uppkommit med anledning av den rådande situationen?

Svaren som vi fått har gett oss en värdefull inblick i hur branschen hanterar det aktuella läget. Vi vill därför passa på att än en gång tacka er som har återkopplat till oss.

Svaren visar att leverantörer av digitala tjänster i Sverige i regel har god förmåga att upprätthålla sina tjänster och att inga större utmaningar uppkommit med anledning av den rådande situationen. Detta tycker vi naturligtvis är positivt!

Läs mer om PTS arbete kopplat till coronaviruset.

En mer digital arbetsmiljö ställer högre krav på ett säkert digitalt arbetssätt

När många arbetar hemifrån är pressen större än vanligt på hur vi upprätthåller god nätverks- och informationssäkerhet. Leverantörer av digitala tjänster är enligt NIS-lagen skyldiga att vidta lämpliga åtgärder för att säkerställa en nivå på säkerheten i nätverken och informationssystemen som är lämplig i förhållande till risken.

Enligt Kommissionens genomförandeförordning (EU) 2018:151, Art 2.1 a) ska detta säkerhetsarbete innefatta systematiskt förvaltning av nät- och informationssystem. Detta innebär bland annat att ni ska ha ändamålsenliga policyer för hantering av informationssäkerheten, inklusive riskanalyser och mänskliga resurser.

Enligt Art 2.1 d) ska ni även säkerställa att åtkomstkontroll för nät- och informationssäkerhet hanteras, tillåts och begränsas baserat på verksamhetskrav och säkerhetskrav. Det innebär bland annat att ni behöver rutiner för fysisk och logisk åtkomst, inklusive administrativ säkerhet för nät och informationssystem.

Risker med det nya digitala arbetssättet

Har ni funderat över huruvida ert nya arbetssätt innebär nya risker? Även om driftskapaciteten är god och inga särskilda utmaningar uppkommit kan det vara bra att reflektera över om ni behöver påminna er personal om säkert distansarbete eller uppdatera någon annan intern information.

Här kan du ta del av goda råd särskilt inriktade på säkerhet och infrastruktur vid arbete hemifrån från CERT.se vid MSB.

Enisa, EU:s nätverks- och informationssäkerhetsbyrå, påminner oss också om att inte bara ”Stay Safe” utan att även ”Stay Cyber Safe”:

Här kan du ta del av två kortare videofilmer som Enisa har tagit fram på detta tema.

https://www.enisa.europa.eu/topics/wfh-covid19/working-from-home-covid19

https://www.enisa.europa.eu/media/multimedia/videos/covid19_Stronger_together

Översyn av NIS-direktivet

Under fjärde kvartalet i år kommer en översyn av direktivet om säkerhet i nätverks- och informationssystem (NIS-direktivet) att ske. Detta framgår av EU-kommissionens arbetsprogram för 2020. I nuläget finns väldigt lite officiell information om detta arbete, men PTS kommer gå ut med mer information längre fram.

Ta del av EU-kommissionens information om översynen och kommissionens arbetsprogram.

Information och nyheter från EU-samverkan

Som en av tillsynsmyndigheterna för NIS-lagen i Sverige samverkar PTS med andra myndigheter i EU, bland annat genom Enisa. Genom denna samverkan diskuterar vi bland annat juridiska gränsdragningar, praktiska frågor samt utbyter information om upptäckta sårbarheter och incidenter.

Här är några nyheter och publikationer som uppmärksammats under våren 2020.

- **SaltStack sårbarhet**: Företaget SaltStack:s open-source-ramverk ”Salt” är ett populärt verktyg för att administrera servrar i molnmiljöer. Två allvarliga säkerhetsbrister upptäcktes under mars 2020. Användare har uppmanats att uppdatera sin mjukvara till den senaste versionen. Läs mer:
  https://labs.f-secure.com/advisories/saltstack-authorization-bypass
  https://thehackernews.com/2020/05/saltstack-rce-vulnerability.html

- **BGP Hijack**: Det ryska telekombolaget Rostelekom genomförde en BGP Hijack som bland annat påverkade Google, Amazon, Facebook, Akamai, Cloudflare, GoDaddy och Digital Ocean. Läs mer:
  https://www.zdnet.com/article/russian-telco-hijacks-internet-traffic-for-google-aws-cloudflare-and-others/

- **Cloud Computing Compliance Criteria Catalogue (C5)**: C5 är en katalog publicerad av den tyska myndigheten för IT-säkerhet (BSI), vilka sätter kriterier för grundläggande säkerhet i molntjänster. Katalogen används av molntjänstleverantörer, kunder och granskare. Samtliga tre roller delar på ansvaret för att upprätthålla en lämplig nivå av informationssäkerhet. Läs mer:
  https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Criteria_Catalogue/C5_NewRelease/C5_NewRelease_node.html

Att hålla sig uppdaterad om identifierade sårbarheter och incidenter hos andra bolag är ett bra sätt för leverantörer av digitala tjänster att omvärdera, utveckla och förbättra det egna informationssäkerhetsarbetet.

Återkommande NIS-information

Detta nyhetsbrev skickas tre-fyra gånger om året. Finns det ämnen eller frågor som du tycker att vi ska ta upp, hör av dig till oss via e-post. Detsamma gäller om du har kolleger som vill ta del av information om NIS.

Vårt nästa nyhetsbrev kommer under hösten 2020. Till dess önskar vi en skön sommar!

Om du har några frågor gällande NIS-regleringen är du välkommen att kontakta oss via e-post: nis@pts.se

Mer om NIS på PTS webbplats