Nätsäkerhet/Enheten för säkerhetsskydd och intern informationssäkerhet
Gudrun Thelander
08-678 57 85
gudrun.thelander@pts.se

Minnesanteckningar Integritetsforum 9 november 2017, kl. 9.30 – 12

1 Inledning

Alla hälsades välkomna och en kort presentationsrunda av deltagarna följde.

2 Internationella frågor

- EU:s översyn av ePrivacy-direktivet

- Förhållandet till GDPR

Det pågår en större översyn/ett moderniseringsarbete inom EU av flera regelverk för att anpassa den inre marknaden till en digital miljö och få en klar och tydlig reglering. Bl.a. förhandlas just nu den föreslagna kodexen för elektronisk kommunikation och den s.k. ePrivacyförordningen.

Förslaget till ePrivacy förordning presenterades av kommissionen i januari 2017. Parlamentet har genomfört en första läsning av förslaget och tagit fram kommentarer på förslaget, som går längre än kommissionens förslag i syfte att ytterligare stärka integritetsskyddet. Rådet håller fortfarande på att diskutera kommissionens förslag. Målet för ordförandelandet Estland är att de ska kunna presentera en framstegsrapport vid årsskiftet och att nästa ordförandeland, Bulgarien ska kunna ta fram ett färdigt kommenterat förslag i mitten av 2018.

GDPR, en förordning direkt tillämplig i svensk rätt, träder i kraft 25 maj 2018 och kommer att ersätta PuL. GDPR, som innehåller en hel del förändringar gentemot PuL, kommer gälla som lag. Även om GDPR är direkt tillämplig förutsätter det att varje medlemsland tar fram en del egna bestämmelser. Datainspektionen är den myndighet som kommer utöva tillsyn och övervaka bestämmelserna i GDPR och den nya dataskyddslagen.

ePrivacydirektivet (som är genomfört i 6 kap. LEK) gäller tills vidare och förhållandet dem emellan regleras av Art 95 i GDPR. I bifogad presentation finns detaljer kring de justeringar som föreslås i LEK till följd av att PuL upphävs.

Om ni upptäcker några tillämpningssvårigheter eller om något blir oklart genom att GDPR träder i kraft kontakta oss gärna.

3 PTS tillsynsarbete

- Avslutad tillsyn.

För ca 1 år sedan startade PTS tillsyn över hur teleoperatörer och återförsäljare av abonnemang hanterar uppgifter om abonnenter och deras kommunikation i butiksmiljö. Tillsynen skedde både i operatörernas egna och i återförsäljares butiker. Bakgrunden till tillsynen var de uppgifter PTS sett i media om incidenter samt de incidenter som rapporterats in till PTS. Tillsynen startade med två operatörer och ökades sedan på till att totalt omfatta fyra operatörer. 14 besök genomfördes, bl.a. i butiker. Fokus för tillsynen var säljstödsystemen och hur dessa användes i butikerna.

Det kan vara svårt för operatörer att ha kontroll över en återförsäljares organisation och att förmedla de krav man har på sig själv till en återförsäljare.

Slutsatserna av tillsynen som avslutades efter sommaren är att säkerhetsarbetet t.ex. policys, behörighetshantering, loggar och uppföljningsrutiner är på plats eller kommer att vara det hos alla inom kort.

Vi har också sett att man infört legitimationskontroll av kunder i butiker.

En av de viktigaste åtgärderna är att arbeta bort slarvig hantering av uppgifter i butik.

En uppmaning är att ni själva åker ut och kollar om det slarvas i butikerna.

- Kommande tillsyn. (SS7)

Den kommande tillsynen kommer att bli mer teknisk och inrikta sig på säkerhet i nätens signalering.

- Pågående tillsyn. (Förmågetillsyn)

Information om PTS tillsyn om operatörers förmåga att identifiera och internt rapportera incidenter som påbörjades i somras.

PTS får in en hel del rapporter från operatörer men tror att det inträffar fler incidenter än vad vi får in rapporter om. Mot den bakgrunden granskas

operatörernas förmåga att identifiera integritetsincidenter. Här avses primärt förmågan hos tjänstetillhandahållarens medarbetare och uppdragstagare att identifiera och förstå när en händelse utgör en integritetsincident, och inte tjänstetillhandahållarens tekniska åtgärder, såsom loggning eller övervakning, för att upptäcka en incident.

4 Anpassning till hemlig övervakning och avlyssning

6 kap 19 § i LEK handlar om anpassning av verksamheten så att hemlig avlyssning av elektronisk kommunikation kan verkställas efter att beslut fattats i domstol. Dessa bestämmelser har funnits sedan mitten av 90-talet. PTS har tittat på den bestämmelsen i samband med vissa tillsyner

Fråga har uppstått om hur bestämmelserna ska tolkas när det gäller utlämnande av uppgifter efter kontorstid. Tar det allt för lång tid så blir det mer eller mindre verkningslöst med utlämnandet då en tidsfaktor kan vara väldigt avgörande i t.ex. brottsutredningar. Man bör alltså ha en organisation så man kan verkställa sådana beslut efter kontorstid, alltså personal tillgänglig dygnet runt. Det finns möjlighet för PTS att meddela undantag framför allt för små operatörer men vi har inte fått någon sådan ansökan under åren.

Om/när nya tjänster, som omfattas av bestämmelsen i 6 kap 19§ i LEK, införs hos en operatör ska systemen anpassas så att kraven uppfylls innan lansering sker.

5 Allmänna råd om kakor

Ett förslag har varit ute på remiss och analys av svaren pågår. Tanken är att ett beslut ska komma i slutet av november. Har ni några frågor kontakta Anna Montelius på PTS som är ansvarig för arbetet.

Förslaget finns att läsa här
http://www.pts.se/sv/Dokument/Remisser/2017/PTS-forslag-till-Allmanna-rad-om-kakor-och-jamforbara-tekniker/

6 PTS föreskriftsarbete

En förstudie där PTS ser över PTSFS 2014:1 som nu är några år gammal pågår. Om det finns brister kommer vi att lämna förslag på ändringar av föreskriften. Vi måste även förhålla oss till ePrivacy.

7 PTS planerade arbete under 2018

Just nu planerar PTS vad vi ska jobba med så allt är mycket preliminärt. Vi är också nyfikna på om ni har någon uppfattning vad vi ska arbeta med. Här nedan följer några exempel.

- Arbete pågår och kommer fortsätta under 2018 med en förstudie där PTS föreskrifter och allmänna råd (PTSFS 2014:1) om skyddsåtgärder för behandlade uppgifter utvärderas och ses över.

- Arbete kopplat till översynen av regelverken inom EU kommer att ra mycket tid nästa år. PTS kommer vara inblandat i den nationella implementeringen. Det är spännande förändringar där alla säkerhetsregler samlas i den nya koden istället för olika regelverk och det kommer att skapa både utmaningar och möjligheter. Föreskrifter är också kopplade till detta.

- En plan för vår tillsyn kommer att tas fram och målet är att den ska vara klar innan årsskiftet. Inriktningen är att fokusera mer på nätdelen och kärnan i operatörsverksamheten samt risken för att uppgifter kan läcka från själva överföringen av information.

- Vad gäller datalagring har det kommit ett utredningsförslag kring brottsbekämpande ändamål som är ute på remiss nu. Det kommer under nästa år troligen att leda till förändrad lagstiftning. Om förslaget från utredningen står sig pekar man på PTS i vissa avseenden (adressöversättning som leder till tappad spårbarhet). PTS måste ta fram regler och precisera vad som gäller kring lagring så vi kommer behöva starta funderingar kring en sådan föreskrift innan allt är klart. Det kommer förstås bli debatt och så men vi behöver börja vårt arbete för att skapa tydlighet i det som inte är tydligt i överliggande reglering. Vi kommer behöva samverka med er för att regleringen ska fånga behovet.

- NS4 (Enheten för säker och konfidentiell kommunikation) tittar tillsammans med systerenheten NS3 (Enheten för driftsäkerhet och betrodda tjänster) på att göra en gemensam tillsynsinsats inriktad både på driftsäkerhet och konfidentialitet hos små och medelstora operatörer. Aktiviteten är ännu inte planerad i detalj.

- PTS ser att det finns behov av att komplettera/följa upp vissa tillsyner vi haft. T.ex. hur säkerställs att man är den uppger sig att vara i kontakt med kundtjänst. Det blir spännande att höra hur ni från operatörshåll funderat kring det här.

- Årlig tillsyn som följer den vanliga mallen där vi går igenom incidentrapporter som vi fått in kommer ske även 2018.

8 Övriga frågor?

Fråga: Vilken blir tillsynsmyndighet när GDPR kommer in? Har man bestämt att DI kommer vara i alla led?

- GDPR är klart men vad gäller ePrivacy pågår arbete fortfarande på EU-nivå så här har man inte alls kommit i mål vad gäller frågan om tillsynsmyndighet. Den förändring som sker är att man i vissa delar knyter väldigt mycket till GDPR vilket ger tätare koppling men samtidigt refererar man till koden på telekomsidan. Än så länge är det en öppen fråga - det kan bli en kombination av flera tillsynsmyndigheter.

Fråga: Kommer man ha något myndighetssamarbete då det kan vara så att uppgifter måste rapporteras till flera olika ställen, vilket blir jobbigt då vi har stor belastning. Vi får ett överlapp vad gäller rapporteringen varför det skulle vara önskvärt att bara behöva anmäla till en myndighet. Det kan bli olika beslut på en och samma incident.

- Det kommer alltid finnas ett visst överlapp. Säkerhetsincidenter ska rapporteras till PTS. Vi är på väg in i en värld där vi har många parallella rapporteringsskyldigheter. PTS kan inte lova att vi löst frågan till den 25 maj 2018 men vi tänker så klart på den. Det ska inte göras svårare än det måste vara för er.

9 Avslutning

Nästa Integritetsforum kommer preliminärt att hållas den 27 april 2018.