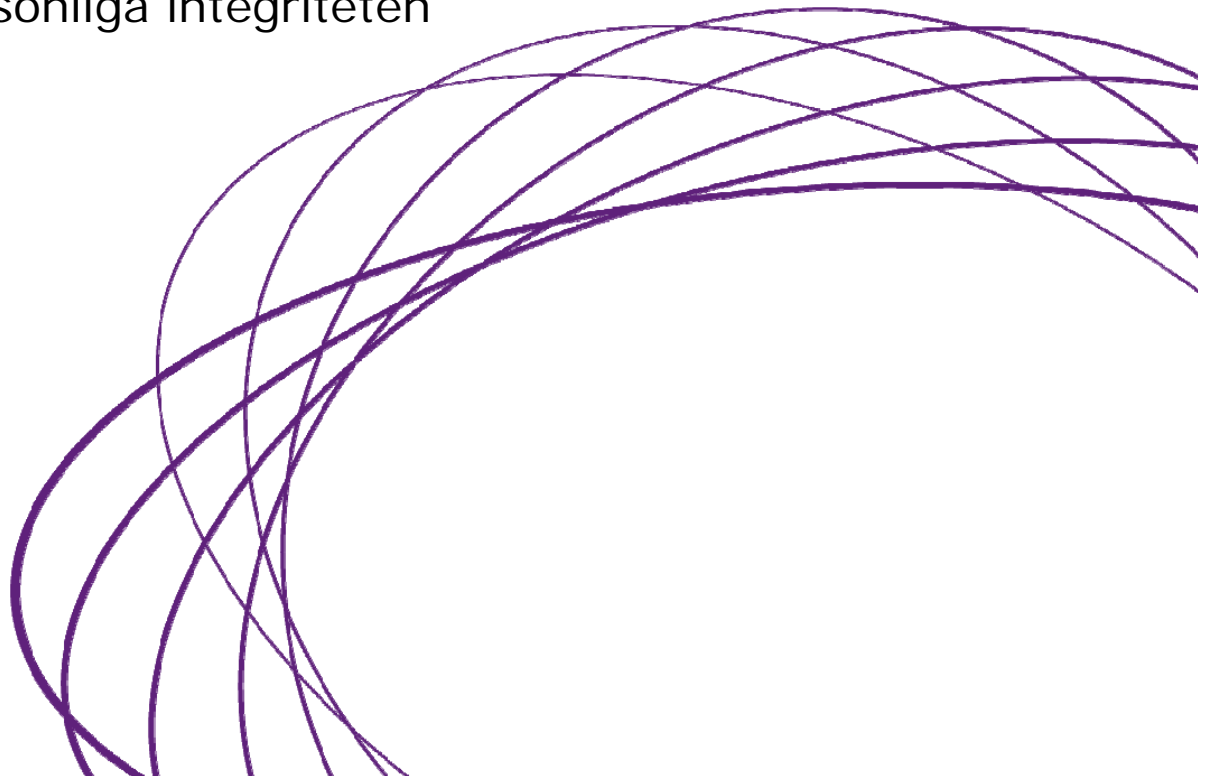


Integritetsforum

Internetleverantörers arbete för användarnas säkerhet i förhållande till den personliga integriteten

8 juni 2009



Agenda

- Inledning
- Bakgrund: PTS tidigare arbete inom området, regler för analys och behandling av trafik
- Hantering av illasinnad trafik i näten och de drabbade användarna; behovsbild för en branschpraxis
- Diskussion
- Kommande integritetsforum
- Avslutning

Bakgrund

- PTS tidigare arbete inom området
- Regler för analys och behandling av trafik

Tidigare skrivelser

- I december 2004 sände PTS en skrivelse till fem operatörer. Skrivelsen publicerad på PTS webbplats.
- Författningsförslag som skulle ge Internetleverantörer en legal möjlighet att vidta akuta åtgärder som filtrering av meddelanden som äventyrar tjänsten eller nätets funktion.

PTS skickar skrivelse till operatörer om e-postfiltrering

2004-12-13

Post- och telestyrelsen (PTS) har erhållit ett flertal konsumentklagomål avseende påstådd filtrering av e-postmeddelanden. Filtrering skall ha skett på så vis att e-postmeddelanden med vissa typer av bifogade filer raderats under pågående transport. Såvitt PTS känner till är detta ett förfarande som tillämpas av ett flertal operatörer.



POST & TELESTYRELSEN

DATUM
15 februari 2005

RAPPORTNUMMER
PTS-ER-2005:7
ISSN 1650-9862

Strategi för att säkra Internets infrastruktur

Regler

- Tillhandahållare av allmänt tillgänglig ekom.tjänst resp allmänna kom.nät ska:
 - vidta lämpliga åtgärder för att säkerställa att behandlade uppgifter skyddas (6:3 LEK)
 - se till att verksamheten uppfyller rimliga krav på god funktion och teknisk säkerhet (5:6a LEK)

6:17 LEK

- Central bestämmelse om förbud mot avlyssning
- Ingen annan än berörda användare får ta del av eller behandla uppgifter i ett elektroniskt meddelande som överförs i ett elektroniskt kommunikationsnät eller med allmänt tillgänglig elektronisk kommunikationstjänst
- (undantag: trafikuppgifter, utlämnande, cachning, radiobefordrade meddelanden)
- Straffsanktionerat enl. 7:15, 2 st LEK
- Behandling endast om *samtycke* inhämtats

Samtycke

- Uttolkas på samma sätt som i PUL
 - *Individuellt* (t.ex. i avtal med abonnenten)
 - *Frivilligt* (ska kunna återkallas, kan dock utgöra villkor för tillhandahållande av tjänst)
 - *Särskilt* (specifikt angivna ändamål etc.)
 - *Otvetydigt* (tydligt för abonnenten att *samtycke* lämnas)
 - *Informerat* (information till abonnenten ska lämnas i direkt samband med att samtycke inhämtas, dvs. grundläggande information redan i avtalet)

PTS skrivelse (2004)

- Automatisk analys/filtrering ej undantaget från 6:17 – torde därför kräva samtycke
- Kan inhämtas via abonnemangsvillkor
 - dock ej tillräckligt med vaga förbehåll om begränsad avstängning eller tillgång till vissa tjänster
- Villkor kan förtydligas med information via Internet
 - avseende vilka behandlingar som kan komma att vidtas
 - under vilka förutsättningar detta kan ske
- Slutsats: Kombination av villkor och förtydliganden via Internet krävs för samtycke

Bakgrund till PTS författningsförslag (2005)

- Operatören kan endast vidta åtgärder som omfattas av undantagen till 6:17 LEK eller som omfattas av abonnenternas samtycke
- Dessa undantag omfattar inte analys av kommunikation och / eller borttagande av skadlig kod m.m.
- Samtycke kräver att användaren är införstådd med behovet av åtgärder – kan vara svårt att inhämta vid behov av omedelbara åtgärder

PTS författningsförslag

- En ny bestämmelse i 6:17 som medger undantag från förbudet att behandla uppgifter för:
"sådan behandling som är nödvändig för att upptäcka och förhindra spridandet av elektroniska medelanden som äventyrar den elektroniska kommunikationstjänsten eller kommunikationsnätets funktion"
- Förslaget har inte föranlett någon lagändring ännu

Hantering av illasinnad trafik och de drabbade användarna

- Slutsatser från PTS utredning om botnät i Sverige
- Behovsbild för en branschpraxis

PTS botnätrappport

- PTS söker i rapporten svar på frågorna
 - Går det att mäta utbredningen i Sverige?
 - Vad kan olika aktörer göra åt problemet med botnät?
 - Vilka åtgärder vidtas / vidtas inte idag?
 - Vad finns det för orsaker till att inte agera?
 - Vad anser PTS borde göras?
- Rapporten finns att hämta här:
<http://www.pts.se/sv/Dokument/Rapporter/Internet/2009/Botnat---Kapade-datorer-i-Sverige---PTS-ER-200911/>

Slutsatser i rapporten (1/2)

- Underlag saknas för att fastställa utbredningen i Sverige – i princip sker ingen övervakning eller mätning
- Det går att motarbeta botnät på flera sätt, t.ex.:
 - Tillhandahållande av säkerhetsprogramvara
 - Analys av trafik / kartläggning i nätet
 - Kontakt med drabbade användare för att informera och stötta. Ev. följt av tillfälliga begränsningar av Internettjänsten.

Slutsatser i rapporten (2/2)

- Alla Internetleverantörer ser inte sin roll på samma sätt.
 - Trafikanalys och andra tekniska åtgärder vidtas inte alls eller i mycket liten omfattning.
 - Olika förhållningssätt mot drabbade kunder.
- Olika hinder upplevs mot att agera
 - Internetleverantören drabbas inte själv av problemet.
 - Risk att säkerhetsåtgärder vänds till något negativt av konkurrenter.
 - Åtgärder strider mot regler om avlyssning i LEK.
 - Risk för ändamålsglidning.

Behovsbild för branschpraxis (1/3)

- Gemensamma principer och metoder för att upptäcka och kartlägga spridning av säkerhetshot
 - Trafikanalys, spårning av illasinnad nättrafik.
 - Systematisk hantering av anmälningar, abuse-ärenden.
 - Deltagande i nätverk för utbyte av information.
- Kan ge ökade möjligheter att
 - Upptäcka säkerhetshot på ett tidigt stadium.
 - Samarbeta kring metoder för att bemöta hoten.
 - Samla statistik till en nationell bild av säkerhetsläget.

Behovsbild för branschpraxis (2/3)

- Gemensam policy för hantering av drabbade användare - åtgärder som får och bör vidtas samt under vilka förutsättningar, t.ex:
 - Skriftlig eller personlig kontakt med användaren.
 - Råd och stöd för att rensa infekterad dator.
 - Tillfälliga begränsningar av Internetåtkomst (t.ex. walled garden) för att skydda övriga användare.
- Kan leda till
 - Ökad medvetenhet och ansvarstagande för användare
 - Transparens och konkurrensneutralitet

Behovsbild för branschpraxis (3/3)

- Gemensam modell för att etablera rätten att vidta säkerhetsåtgärder.
 - Baserad på PTS rekommendation.
 - Var, hur och när abonnentens eller användarens samtycke inhämtas.
 - Var och hur aktuell information publiceras om vilka åtgärder Internetleverantören vidtar och hur användaren påverkas.
- Leder till
 - Tydlighet mot abonnenten
 - Ökad trygghet för Internetleverantören att vidta åtgärder

Diskussion

- Vad anser ni vara de viktigaste säkerhetshoten för branschen att bekämpa?
- Hur bekämpas dessa hot på bästa sätt?
- Hur kan branschen bäst samarbeta?
- Medger nuvarande regelverk ett effektivt säkerhetsarbete? Är PTS rekommendation för hantering av samtycke osv. funktionell?
- Hur ser ni på PTS förslag till nästa steg: Bildandet av en arbetsgrupp för utveckling av en branschpraxis?

Diskussion

- Vad anser ni vara de viktigaste säkerhetshoten för branschen att bekämpa?
- Hur bekämpas dessa hot på bästa sätt?
- Hur kan branschen bäst samarbeta?
- Medger nuvarande regelverk ett effektivt säkerhetsarbete? Är PTS rekommendation för hantering av samtycke osv. funktionell?
- Hur ser ni på PTS förslag till nästa steg: Bildandet av en arbetsgrupp för utveckling av en branschpraxis?

Kommande integritetsforum

- Mötesform
- Regelbundenhet
- Innehåll

Nästa Integritetsforum 26/8 em.

- Trafikdatalagring på agendan – hur PTS ska lägga upp arbetet
- Lagen träda i kraft 1/1 2010? vilket i så fall blir vägledande för ambitionen för föreskrifterna
- Två föreskrifter, en om säkerheten kring de lagrade uppgifterna, en om ersättningen vid utlämnande.
- Ev. arbetsgruppsmöten med aktörerna (operatörer, LEA, DI, IT&Telekomftgn) under september
- Preliminärt föreskriftremiss och samråd om de två föreskrifterna under oktober