Post & Telestyrelsen
Att: Mia Gombor
Rättsavdelningen
Box 5398
102 49 STOCKHOLM

Remiss ang. PTS förslag till allmänna råd om god funktion och teknisk säkerhet samt uthållighet och tillgänglighet vid extraordinära händelser i fredstid

.SE (Stiftelsen för Internetinfrastruktur) har beretts tillfälle enligt 27 § 3 verksförordningen (1995:1322) att yttra sig över rubricerade förslag och konsekvensutredning.

Allmänna synpunkter

.SE kan i allt väsentligt instämma i PTS konsekvensutredning. Beroendet av elektroniska kommunikationer och kommunikationstjänsternas tillgänglighet ökar hela tiden, beroendet av energiförsörjningen till dessa likaså. Som samhälle betraktat har vi blivit sårbarare än kanske någonsin förut. Ett gott och varnande exempel på detta är den senare tidens stormar som dragit fram över Sverige. Som en följd av dem har det också blivit uppenbart hur sårbara särskilt överförings- och distributionssystemen för elektricitet samt kommunikations- och transportsystemen är.

Dessutom möter vi nya hot som vi ännu inte med säkerhet kan känna till och som förorsakas av vår yttre eller interna säkerhetsmiljö, hot mot de samhällsviktiga kommunikations- och informationssystemen. Då är det viktigt att tillhandahållarna av elektroniska kommunikationer delar uppfattning om en gemensam hotbild så att man går i takt när det gäller att öka säkerheten.

Vid bedömningen av riskerna måste vi komma ihåg, att vi är allt mer beroende av händelser hos andra, inom och utanför Sverige. Många kan dra sig till minnes millennieskiftet, då vissa befarade att datorsystemen skulle kollapsa med ett universellt kaos som följd, vilket till all lycka dock aldrig inträffade.

Det som PTS anför i avsnitt 3.2 om marknadsbestämd säkerhet för elektroniska funktioner förutsätter att användarna har en beställarkompetens som .SE betvivlar att de i verkligheten kan leva upp till. Där har PTS som tillsynsansvarig myndighet ett stort ansvar att formulera kraven på användarnas vägnar, där användare definieras som enskilda konsumenter. Eftersom kraven på tillhandahållarna inte är tydligt och starkt formulerade upplever dessa förmodligen inte heller något tryck på att öka säkerheten i sina tjänster och nät. Säkerhet är inte (ännu) ett försäljningsargument.

Stiftelsen för Internetinfrastruktur (.SE)

Postadress
Box 7399
103 91 STOCKHOLM

Besöksadress
Ringvägen 100A, 9 tr
STOCKHOLM

Telefon
08-452 35 00
Telefax
08-452 35 02

Internet
info@iis.se
www.se

Org. Nr
802405-0190

.SE föreslår vidare att en del av de medel som PTS förfogar över för robusthetshöjande åtgärder läggs på att studera riskerna med det ökade kommunikationsberoendet i kritiska infrastrukturers styr- och reglersystem, som är en annan kategori användare av elektroniska kommunikationer. Automatiska mätare som levererar mätvärden direkt från slutkund till elbolaget och tillåter mer optimering av produktion och distribution, koncentrerade driftcentraler som servar fler geografiskt spridda driftställen, koncentration av processindustrins insamling av kontrollinformation är exempel på system som tidigare fungerat utan anslutning till kommunikationsnät och med krav på 100 % tillgänglighet. Sådana system (s.k. SCADA-system)[1], knyts numera allt oftare ihop med hjälp av elektroniska kommunikationstjänster, till synes utan beaktande av hur det påverkar tillgängligheten eller hotbilden.

Här finns det anledning att från svensk sida följa utvecklingen i USA och insatser för att genom förslag till ett gemensamt språk öka beställarkompetensen vid upphandling så att säkerhet integreras i SCADA-systemen.[2] Det kan också finnas skäl att studera och eventuellt anpassa för den svenska marknaden en motsvarighet till kraven i USA:s NERC CIP[3] vilken är designad för att säkerställa hög tillgänglighet och tillförlitlighet i elförsörjning, men som sannolikt också går att tillämpa på andra kritiska infrastrukturer.

När det gäller sårbarheter i infrastrukturen kan det enligt .SE finnas skäl att formulera nyckeltal för dessa. Exempelvis hur många abonnenter får maximalt vara beroende av samma accessledning utan att den behöver kompletteras med redundans? Hur många timmars otillgänglighet är acceptabelt innan extraordinära insatser krävs för att återställa funktionaliteten?

.SE föreslår också att PTS utreder konsekvenserna av att införa motsvarande krav på tillhandahållare av elektroniska kommunikationer som de som sedan den 1 januari 2006 gäller om leveranssäkra elnät, med bl.a. en schablonersättning till drabbade kunder.

Förslag till allmänna råd

.SE anser att PTS allmänna råd enligt förslaget bör kompletteras så att de innehåller en klar och tydlig deklaration om målsättningen att varje tillhandahållare ska införa ett ledningssystem för informationssäkerhet som lever upp till kraven i standarden för Ledningssystem för Informationssäkerhet (”LIS”) ISO/IEC 27001[4]. Råden kan då även innehålla en nyansering med innebörden att kraven i standarden bör appliceras i den mån de kan anses vara relevanta och rimliga med avseende på organisationen och dess verksamhet. Tillhandahållarna av elektroniska kommunikationer bör dock kunna motivera för PTS vid en tillsyn om de valt att _inte_ följa delar av de allmänna råden.

[1] Supervisory Control And Data Acquisition
[2] http://www.msisac.org/scada/
[3] North American Reliability Council Critical Infrastructure Protection Standard
[4] Ledningssystem för informationssäkerhet – Krav, International Organization for Standardization. ISO/IEC, 27001:2005, 2006-02-06. URL: http://www.iso.org/

De allmänna råden bör även innehålla rekommendationer om upprättandet av mål för arbetet, mätningar mot uppställda mål och om korrigerande och förebyggande åtgärder i syfte att uppnå ständig förbättring.

När det gäller konkurrensmässiga effekter av krav på ökad säkerhet anser .SE att säkerhet måste få kosta, men att säkerhetsåtgärderna måste bygga på en balanserad riskanalys och beräkning av kvarstående risk. Säkerhet måste ses som en viktig investering, på samma sätt som snabb hårdvara och effektiva applikationer. Ingen är betjänt av att vi har aktörer med bristande säkerhet, vare sig dessa är stora eller små. Målet kan enligt .SE:s uppfattning inte vara konkurrens till varje pris, i vart fall inte till priset av bristande säkerhet, tillgänglighet och robusthet.

Danny Aerts
VD

/gm Anne-Marie Eklund Löwinder
kvalitets- och säkerhetschef