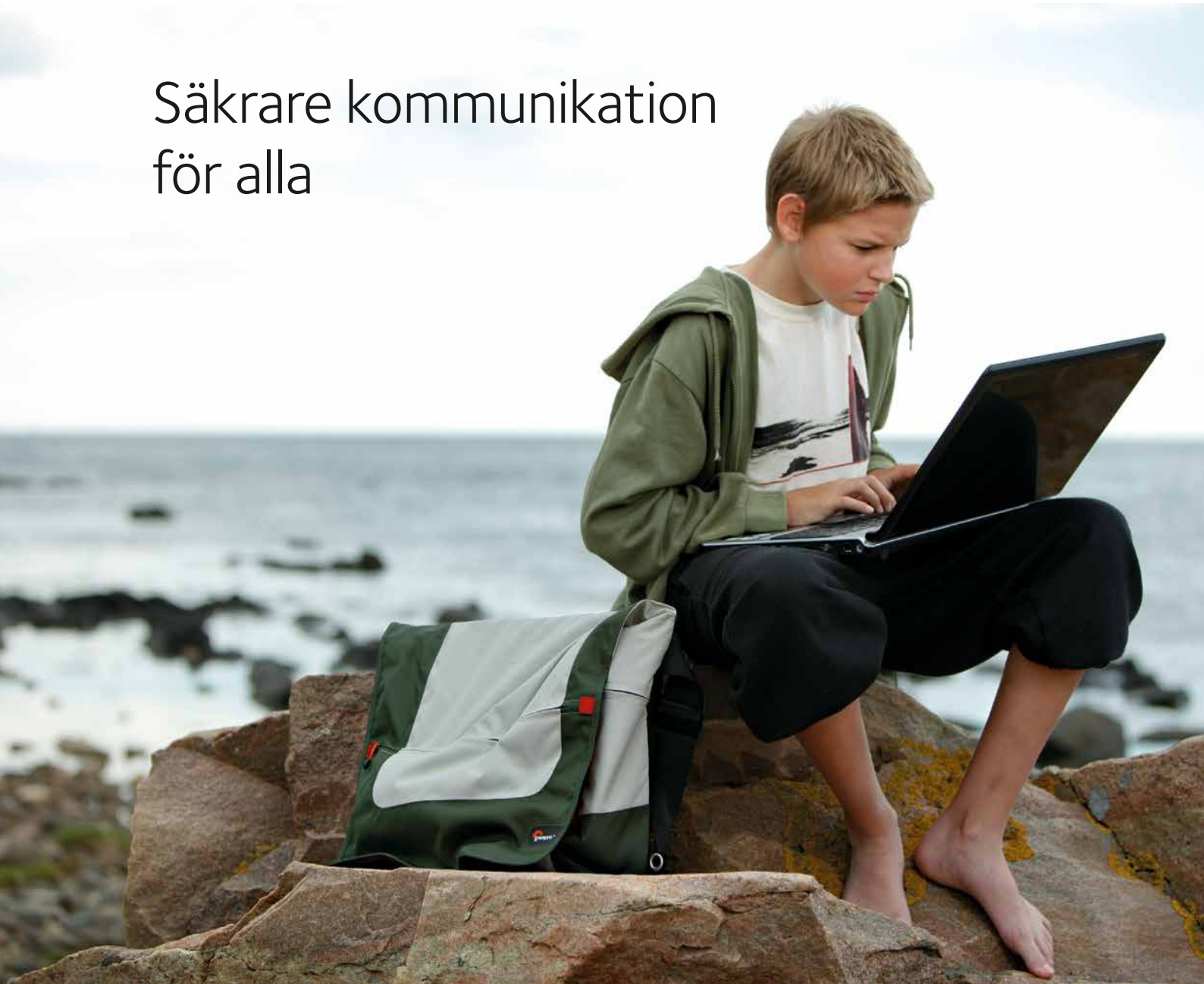
Säkrare kommunikation för alla



Säkrare kommunikation för alla

Vi använder allt mer elektronisk kommunikation. Med hjälp av telefoner och datorer håller vi kontakten med våra vänner, tar del av vad som händer i omvärlden och sköter våra bankaffärer. Telefoner och datorer behövs till våra sjukhus, flygplatser och vår industri, för att nämna några exempel. Här presenterar vi hur PTS arbetar för att alla ska kunna ringa och använda internet med hög säkerhet och så få störningar som möjligt. Vi arbetar med förebyggande åtgärder, krishantering och granskning i efterhand.

Hängslen och livrem på våra kommunikationsnät

Grundregeln är att det är tele- och internetbolagen som ska se till att kommunikationsnäten fungerar och har en grundläggande nivå av säkerhet – det står i lagen. Men ibland kräver samhället ännu högre säkerhet än vad som är affärsmässigt motiverat för företagen, efter att de har uppfyllt lagkraven. Då kan PTS agera för att höja säkerheten.

PTS finansierar till exempel mobila basstationer, reservelkraft, dubbla förbindelser, så att trafiken i många fall kan ta en alternativ väg om det blir problem med en ledning, och bergrum, för att skydda kritisk infrastruktur. Vi har exempelvis finansierat dubbla förbindelser mellan alla kommunhuvudorter i Sverige. Man kan säga att vi sätter hängslen och livrem på våra kommunikationsnät.

Privat–offentlig samverkan för konkret samhällsnytta

Arbetet med att säkra kommunikationsnäten är i många fall exempel på framgångsrik privat-offentlig samverkan. Vi och tele- och internetbolagen samarbetar och samfinansierar projekt för att åstadkomma konkret samhällsnytta. En styrka är att PTS har ekonomiska medel som vi kan använda för att starta projekten. Vi får ofta förfrågningar från andra länder som är intresserade av hur vi jobbar tillsammans med företag och organisationer mot ett gemensamt mål.

Investeringar de senaste tio åren

De senaste tio åren har vi gjort stora investeringar för att höja säkerheten i näten. Pengarna kommer från de statliga anslagen (skatter) och från de större nätägarnas beredskapsavgift. Det är en avgift som ska finansiera åtgärder som stärker de elektroniska kommunikationerna mot allvarliga hot och påfrestningar i fredstid, exempelvis sabotage, olyckor och naturkatastrofer.

Mobila basstationer ger flexibla mobilnät

Om många människor försöker använda mobilen samtidigt finns det en risk att näten inte klarar belastningen. Det kan hända vid en kris, men också vid mer vardagsnära händelser, som en festival. Mobilnäten kan också gå sönder.

PTS har finansierat ett antal mobila basstationer. De är placerade hos telebolagen för att kunna sättas in av dem om nätens kapacitet går ner. De ligger färdigpackade i containrar för snabb och enkel transport.

Bränsleceller kan driva telestationer när elen går

Telestationer kräver ständig tillgång till el. Därför behövs reservalternativ om elnätet går ner. Hittills har dessa utgjorts av batterier och elverk.

Nu utvärderas om bränsleceller kan utgöra ett alternativ till det fasta elnätet. Därför genomför FMV, TeliaSonera och PTS ett försök samt långtidstest av olika bränsleceller på telestationer, som ersättning för annan typ av

reservelsystem. Bränsleceller kan kanske ge en teknik med ännu bättre egenskaper än de nuvarande reservelsystemen – de räcker länge, bullrar mindre och är miljövänliga.

Ställ rätt krav när du köper robust elektronisk kommunikation

PTS har tagit fram en vägledning som förbereder dig inför inför köpet av olika typer av elektronisk kommunikaiton. Vägledningen beskriver vad du bör känna till och tänka på när du köper t.ex. internetanslutning eller telefoni. Det gäller att kunna ställa rätt krav vid köpet, men också i den dagliga verksamheten, så att kommunikationen blir säker och robust – krav som utgår från genomförd risk- och sårbarhetsanalys.

Den viktigaste robusthetsåtgärden är att se till att ha väl beprövade reservsystem för elkraftsförsörjning på plats i händelse av strömavbrott. Det är också viktigt att ha redundans, alltså alternativa sätt att få tillgång till de resurser som krävs för verksamheten. Verksamhetens krav gentemot leverantören måste sedan slås fast i avtal. Det är vanligt att tillgängligheten och kvaliteten på tjänsterna definieras i ett servicenivåavtal eller SLA (Service Level Agreement) som en del i det avtal som upprättas vid upphandlingen av elektronisk kommunikation. Vägledningen finns att ladda ner från PTS webbplats.

Färre avbrott på grund av grävskador

Grävskador orsakar årligen avbrott och skador i kritisk infrastruktur för miljontals kronor. För att minska risken för avbrott har ett stort antal myndigheter, företag och organisationer tagit fram webbtjänsten Ledningskollen.se. Arbetet samordnas och finansieras av PTS, Svenska Kraftnät och Trafikverket. Med en enda förfrågan kan den som planerar ett grävprojekt nå alla som har ledningar nedgrävda på platsen.

Tjänsten lanserades nationellt i december 2010, och är väl utnyttjad, med en stadig ökning av användare. Nästan 40 000 företag och privatpersoner har under det första året använt webbtjänsten för att komma i kontakt med ledningsägare när det ska genomföras någon form av grävarbete.

I Danmark finns ett liknande system där man visar på stora besparingar. Bl.a. har de direkta kostnaderna för grävskador minskat med ca 70 miljoner svenska kronor per år, och antalet grävskador som beror på bristande kunskap om var olika ledningar är nedgrävda har minskat med 75 procent.

Nödvändigt med säker tillgång till tid

Många viktiga samhällsfunktioner är beroende av korrekt tid, ofta utan att vi tänker på det. Till exempel behöver delar av våra kommunikationsnät ständig tillgång till rätt tid, annars fungerar de inte. Ett annat exempel där rätt tid är viktig är ekonomiska transaktioner mellan banker, finansinstitut eller handelsplatser, där aktörerna, i det här fallet datorsystem, måste vara ”överens” om tiden för att transaktionerna ska kunna utföras.

Atomklockor ger Sverige korrekt tid

I Sverige får vi korrekt tid genom ett antal atomklockor som PTS har delfinansierat och som Sveriges Tekniska Forskningsinstitut (SP) hanterar.

PTS har tillsammans med SP under 2000-talet investerat ca 50 miljoner kronor i forskning och utveckling, inköp och teknisk infrastruktur för nationell tidhållning. Uppbyggnaden har givetvis skett med utgångspunkten att tiden ska vara korrekt, men dessutom, och här är Sverige världsledande, att den ska spridas till användarna på ett säkert och lättillgängligt sätt.

Ny säkrare metod för tidsjämförelser

SP har, med finansiellt stöd av PTS, bland annat utvecklat en metod för tidsjämförelser med hjälp av existerade datatrafik i optiska fibernät. Tekniken är utvecklad för att minska beroendet av radiobaserade metoder, som exempelvis det amerikanska satellitsystemet GPS. Att använda GPS för tidsjämförelser är visserligen billigt, men signalerna kan störas ut och förvrängas, vilket kan få stora konsekvenser för samhället.

PTS har bland annat satsat medel på att införa den nya tekniken för att minska sårbarheten med radiobaserade tidskällor, men också för att bygga ytterligare ett klocklaboratorium med atomklockor av hög kvalitet i ett skyddat bergrum.

Teknik som garanterar äkta webbplatser

Alla webbplatser har en adress som består av ett antal siffror eller siffror blandat med alfabetiska tecken – en ip-adress. Den behövs när datorerna kommunicerar med varandra. Domännamnsystemet DNS, som är en del av internet, kopplar ip-adressen till en textadress. Tack vare DNS kan därför en person som surfar skriva in www.pts.se i sin webbläsare, i stället för en ip-adress, för att komma till vår webbplats.

DNS underlättar för användaren, men är också möjligt att manipulera. En illasinnad person kan sätta upp en falsk webbplats och manipulera DNS så att den som surfar kommer till den falska sidan, trots att hon eller han har skrivit rätt textadress. Där kan den illasinnade personen exempelvis sprida falsk information eller använda sidan för att försöka komma över känsliga uppgifter.

Nu finns en teknik för att skydda webbplatser mot detta. Tekniken heter DNSSEC (DNS Security Extensions). Den bygger på kryptografi och digitala signaturer och gör att det går att upptäcka om adresshänvisningen till en viss webbplats har förfalskats.

Sverige är ett föregångsland

.SE (Stiftelsen för Internetinfrastruktur), som hanterar den svenska toppdomänen .se, har lanserat DNSSEC som tjänst. Sedan dess har alla domäninnehavare under .se-domänen möjlighet att dra nytta av den förbättrade säkerheten. Sverige är därmed ett föregångsland vad gäller att införa den nya tekniken för ökad säkerhet.

PTS första myndigheten med den nya tekniken

Som första statliga myndighet i Sverige, och sannolikt också i världen, har PTS infört DNSSEC. Vi verkar aktivt för att fler myndigheter och företag ska börja använda den nya tekniken.

IPv6 – nödvändigt för internets utveckling

De adresser som datorer behöver för att kommunicera med varandra, ip-adresser, håller på att ta slut och många tror att läget blir kritiskt under de närmaste åren. En ny ip-standard, kallad ip version 6 eller IPv6, finns tillgänglig och erbjuder praktiskt taget obegränsat med adresser. Att införa IPv6 är inte alldeles enkelt och tar sin tid om dåliga lösningar och misstag ska kunna undvikas. Adressbristen kan hämma utvecklingen i Sverige och andra länder, vilket är ytterligare ett skäl till att i god tid införa IPv6. För att alla på internet ska kunna kommunicera oavsett ip-version, måste IPv6 införas vid sidan av det befintliga IPv4, det innebär att de två standarderna kommer att samexistera under många år framöver.

PTS har tagit fram en vägledning om hur IPv6 kan införas i praktiken. Vägledningen är tänkt att vara ett stöd för it-personal vid praktiskt införande av IPv6. Vägledningen finns att hämta på www.pts.se/ipv6.

Tele- och internetbolagens säkerhetsarbete

Att kommunikationsnäten fungerar och är säkra är tele- och internetbolagens ansvar. För att ge dem stöd i hur de kan åstadkomma det, har PTS tagit fram allmänna råd om driftsäkerhet – en tolkning av hur vissa bestämmelser i lagen om elektronisk kommunikation kan efterlevas.

I råden står det att tele- och internetbolagen bör bedriva ett kontinuerligt och systematiskt säkerhetsarbete för att uppnå säkrare elektroniska kommunikationer. I korthet innebär råden att tele- och internetbolagen bör

- genomföra riskanalyser, så att de vet vilka risker de är utsatta för
- hantera de risker som identifieras i riskanalysen
- ha planer för vilka åtgärder som ska vidtas vid störningar eller avbrott
- ha rutiner för att följa upp händelser och ta hänsyn till detta vid planering och utbyggnad av infrastrukturen.

Tillsyn mot många större tele- och internetbolag

För några år sedan genomförde vi tillsyn utifrån bestämmelserna om driftsäkerhet mot 53 större tele- och internetbolag. PTS bedömning är att bestämmelserna om driftsäkerhet i stort efterlevs.

Tillsynen visade att 84 procent av företagen angav att de bedriver ett säkerhetsarbete. Säkerhetsarbete innebär i detta fall att förebygga avbrott och störningar genom att genomföra riskanalyser och riskhantering, planera för hantering av avbrott och störningar samt följa upp dessa när de inträffar.

Stadsnäten bör arbeta förebyggande

En tillsyn över ett antal stadsnät som används för att leverera telefoni och internet runt om i landet visade att också stadsnäten bedriver ett säkerhetsarbete. Frågor relaterade till teknisk infrastruktur, till exempel elförsörjning och viktiga förbindelser, är relativt väl omhändertagna. Det förebyggande arbetet med riskanalyser, riskhantering och planering för avbrott och stör-

ningar är däremot inte lika väl utvecklat. PTS anser också att stadsnäten bör lägga större fokus på de mjuka faktorerna i säkerhetsarbetet. Exempel på sådana faktorer är nyckelpersonsberoende, kompetensförsörjning och dokumentation av processer.

PTS har gett Svenska Stadsnätsföreningen (SSNf) uppdraget att ta fram ett utbildningspaket för driftsäkerhet som i första hand ger information om hur man kan förvalta säkerhetsarbetet för statsnätet långsiktigt och systematiskt. Syftet med utbildningspaketet är bl.a. att höja stadsnätens förmåga att hantera incidenter och extraordinära händelser i fredstid. Utbildningen för driftsäkerhet finns att tillgå och målet är att utbilda ca 100 stadsnät.

Gemensam lägesuppfattning vid driftstörningar

Om en svår påfrestning på våra elektroniska kommunikationsnät skulle uppstå, behöver teleoperatörerna kunna ge en bild av driftstörningsläget till allmänheten och organisationer. PTS har tillsammans med teleoperatörerna tagit fram ett koncept, Gemensam Lägesuppfattning (GLU), där teleoperatörerna på ett standardiserat sätt kan presentera driftstörningsinformation till allmänheten och till de organisationer som agerar i händelse av en nationell kris.

Genom en speciell funktion i systemet informeras också SOS Alarm om störningar som påverkar 112. SOS Alarm visar sedan denna information på sin samverkanswebb som i sin tur används av bl.a. räddningstjänsten och länsstyrelser.

Standardiserad driftinformation

Även operatörerna behöver sinsemellan ha ett utbyte av information vid driftstörningar. Driftinformation för operatörer (DIO) är ett koncept där driftinformation om akuta fel och planerade avbrott utbyts mellan aktörer inom området elektroniska kommunikationer. PTS driver och delfinansierar projektet som syftar till att skapa en mer ekonomisk, säkrare och effektivare

överföring av information om driftstörningar orsakade av akuta fel eller planerade avbrott.

Det ska inte få hända igen

När det blir ett avbrott kan vi inleda tillsyn i efterhand. Det innebär att vi kontaktar det berörda bolaget för att få detaljerad information om vad som hände, vilka konsekvenserna blev, hur de hanterade avbrottet och vad företaget gör för att det inte ska hända igen. Vi kan kräva att de ska vidta vissa åtgärder och, om de inte gör det, utkräva vite. PTS genomför årligen 5-10 tillsynsinsatser vid mer omfattande störningar och avbrott.

Krisledningsövning ger bättre färdighet

PTS har inom ramen för sitt robusthetsarbete en strategi för utbildningar och övningar. Den bygger på en helhetssyn där alla delar från individ- och företagsnivå, till övergripande sektorsnivå ingår. Syftet med strategin är att öka sektorns förmåga att hantera kriser och extraordinära händelser, så att konsekvenserna för samhället minimeras.

På sektorsnivå är ambitionen att vartannat år genomföra en större krisledningsövning, Telö, där fokus ligger på samverkan inom sektorn elektronisk kommunikation. Den senaste övningen, Telö 11, genomfördes i november 2011. Målet med Telö 11 var bland annat att öva ett antal förberedda rutiner kring hur sektorn samverkar. Det handlade till exempel om att skapa en gemensam lägesbild samt att sprida samstämmig information.

Utbildning för informationssäkerhetschefer

Försvarshögskolan har i samverkan med det amerikanska National Defense University överfört en kvalificerad utbildning för informationssäkerhets-

chefer till Sverige. Utbildningen är fokuserad på ledarskap snarare än teknik. PTS medverkar i styrgruppen för att vidareutveckla utbildningen och finansierar även deltagare från samhällsviktiga teleoperatörer.

Information ska göra internet säkrare

Inom internetområdet arbetar PTS även med information och tjänster till konsumenter och småföretag så att de ska kunna använda internet på ett säkrare sätt. Vi har en särskild webbplats, www.pts.se/internetsakerhet, där alla råd och tjänster finns samlade. Där kan konsumenterna och småföretagarna till exempel se filmer om hur de bör ställa in sitt trådlösa nätverk och hur de använder bluetooth på ett säkert sätt.

På webbplatsen finns våra tjänster Testa datorn, som skannar datorn efter säkerhetshål, och Testa lösenord, som lär ut knepen så att alla ska kunna skapa starka lösenord. Testa datorn har utfört över 1 050 000 tester och för Testa lösenord är siffran över 810 000.

Din personliga integritet ska skyddas

Den elektroniska kommunikationen underlättar våra liv, men innebär också att vi lämnar elektroniska spår, information om när, var och med vem vi kommunicerar. Den här informationen kan ofta vara känslig och måste skyddas. Vi bedriver därför tillsyn även på integritetsområdet.

Ett exempel är att mobiloperatörer behandlar uppgifter om sina abonnenter och kan föra sådana uppgifter vidare, t.ex. för att underlätta betalning av mobila innehållstjänster – ringsignaler, bilder, nyheter och väderprognoser. Detta innebär nya affärsmöjligheter för tele- och internetbolagen: att sälja personuppgifter, exempelvis uppgifter om var användaren befinner sig.

PTS och Datainspektionen har gemensamt granskat hur personuppgifter hanteras i mobila innehållstjänster. Ett resultat av arbetet är att det nu är tydligare hur ansvaret för uppgifterna fördelas mellan de olika aktörerna.

Foto: Christer Engström, Stefan Holm, Ulf Isacson FOLIO
Tryck: Kaigan AB, mars 2013. 500 ex.

Post- och telestyrelsen Box 5398 102 49 Stockholm
Växel: 08-678 55 00 pts@pts.se www.pts.se