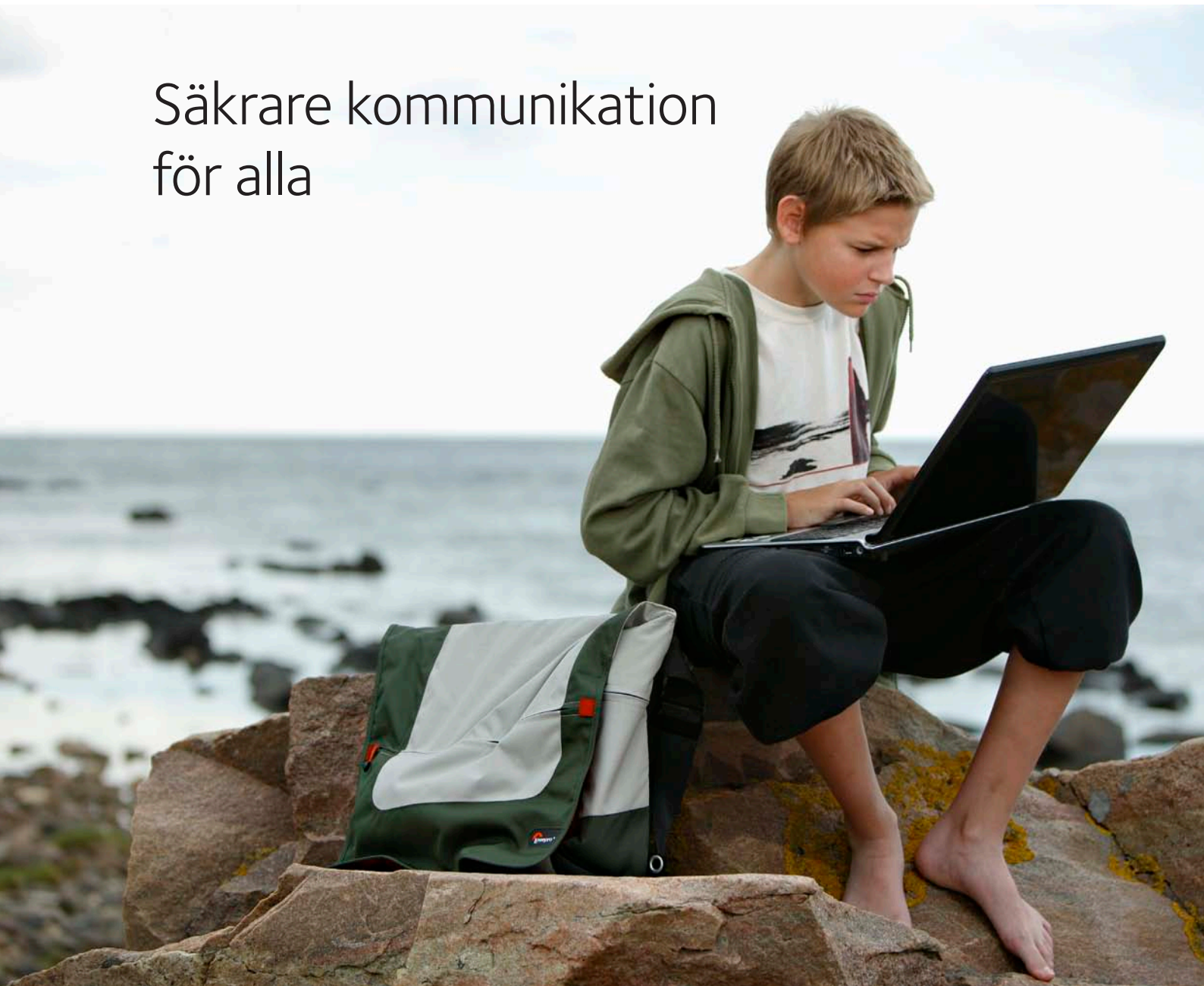




Säkrare kommunikation
för alla



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 så hög säkerhet och så få störningar som möjligt. Vi arbetar med förebyggande åtgärder, incident- och krishantering samt 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 är säkra – 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, reservkraft, 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, där 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.

Investerat ca 1,5 miljarder de senaste tio åren

De senaste tio åren har vi investerat ca 1,5 miljarder kronor 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 anstormningen. 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 mobila basstationerna har en 30 meter hög, motordriven mast och är självförsörjande på el och kyla. 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 också kan utgöra ett alternativ till det fasta elnätet. Därför genomför FMV, Telia Sonera och PTS ett försök samt långtidstest av olika bränsleceller på telestationer, som ersättning för annan typ av reservsystem.

Bränsleceller kan kanske ge en teknik med ännu bättre egenskaper än de

nuvarande reservsystemen – de räcker länge, bullrar lite och är miljövänliga. Två av de frågor som projektet ska besvara är: Är bränsleceller tillräckligt tillförlitliga? Vilken typ av bränsle (vätgas eller metanol) är mest lätthanterligt?

Nu ska det bli färre avbrott på grund av grävskador

Helt störningsfri är inte telefonin och Internet ännu, inte minst på grund av att det varje år grävs av tusentals tele-, Internet- och elledningar i Sverige. Kostnaderna är skyhöga – flera hundra miljoner kronor varje år.

För att minska risken för avbrott har ett stort antal myndigheter, företag och organisationer byggt upp Internettjänsten Ledningskollen.se. Arbetet samordnas och delfinansieras av PTS. Med en enda förfrågan kan den som planerar ett grävprojekt nå alla som har ledningar nedgrävda på platsen.

Tjänsten lanserades under hösten 2009 i Uppsala län. Nu förbereder PTS, tillsammans med Vägverket och Svenska Kraftnät, en utrullning i resten av landet under slutet av 2010.

Stora besparingar med liknande system i Danmark

Det är för tidigt att redovisa några nyckeldata ur det svenska projektet. I Danmark finns ett liknande system. Det visar på stora besparingar:

- De direkta kostnaderna för grävskador har minskat med ca 70 miljoner svenska kronor per år.
- Samhället har sparat ytterligare ca 70 miljoner svenska kronor per år vad gäller följdskostnader (skador mot tredje part m.m.).
- Antalet grävskador som beror på bristande kunskap om var olika ledningar är nedgrävda, har minskat med 75 procent.

Säker tillgång till tid livsviktigt för kommunikationsnäten

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 SP Sveriges Tekniska Forskningsinstitut hanterar. Nationella tidsservrar för Internet finns i skyddade utrymmen och kopplingspunkter för Internet på ett antal platser i landet.

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 existerande 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.

Den senaste tiden har vi satsat medel bland annat på att införa den nya tekniken för att minska sårbarheten med radiobaserade tidskällor, men också



för att bygga ytterligare ett klocklaboratorium med atomklockor av högsta kvalitet i ett skyddat berggrum.

Ny teknik 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 mycket, men är möjligt att manipulera. En skicklig 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.

Sedan en tid tillbaka 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 ett föregångsland

DNSSEC är det enda heltäckande skyddet för att upptäcka förfalskade DNS-svar. .SE (Stiftelsen för Internetinfrastruktur), som hanterar den svenska toppdomänen .se, lanserade DNSSEC som tjänst i januari 2007. 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 myndighet med den nya tekniken

Som första statliga myndighet i Sverige, och sannolikt också i världen, införde PTS DNSSEC i september 2008. Alla som söker information på vår webbplats eller vill använda våra e-tjänster, kan vara säkra på att de besöker vår riktiga webbplats och inte en falsk kopia. Vi verkar aktivt för att fler myndigheter och företag ska börja använda den nya tekniken.

Tele- och Internetbolagen ska bedriva säkerhetsarbete

Att kommunikationsnäten fungerar och är säkra är i första hand tele- och Internetbolagens ansvar. För att ge dem stöd i hur de kan åstadkomma det, har PTS tagit fram allmänna råd om god funktion och teknisk säkerhet – 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 53 större tele- och Internetbolag

I mitten av 2008 genomförde vi tillsyn utifrån det allmänna rådet om god funktion och teknisk säkerhet mot 53 större tele- och Internetbolag. Rapporten från 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. PTS



bedömning är att bestämmelserna om god funktion och teknisk säkerhet i stort efterlevs.

Ökat fokus på säkerhetsarbete

Fokus på säkerhetsarbete har ökat de senaste åren. En undersökning som vi genomförde i maj 2005 visade att bara drygt två tredjedelar av företagen använde sig av riskanalyser i sitt säkerhetsarbete. I mitten av 2008 hade den andelen stigit till 9 av 10 företag. Företagen kan dock bli generellt bättre i säkerhetsarbetet och särskilt gäller detta dokumentationen. Exempelvis anger bara 6 av 10 som genomför riskanalyser att de har dokumenterade rutiner för detta. Avsaknaden av dokumentation kan leda till en tveksamhet kring hur systematiskt säkerhetsarbetet verkligen är.

Stadsnäten bör arbeta förebyggande

Nyligen avslutade vi en tillsyn över ett antal stadsnät som används för att leverera telefoni och Internet runt om i landet. Tillsynen visade att stadsnäten bedriver säkerhetsarbete och att frågor relaterade till teknisk infrastruktur, till exempelvis elförsörjning och viktiga förbindelser, är relativt väl omhändertagna. Det förebyggande arbetet med riskanalyser, riskhantering och planering för avbrott och störningar 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.

Under 2009 hade PTS elva tillsynsärenden om driftstörningar och två ärenden med planlagd tillsyn.

När näten går ner måste de snabbt upp igen

PTS har tillsammans med tele- och Internetbolagen tagit fram ett särskilt krisinformationssystem. Något förenklat består systemet av två delar – en

teknisk del som gör att de konkurrerande företagen och PTS snabbt kan få en bild av läget i alla nät och en administrativ del som gör att vi snabbt kan ta gemensamma och väl underbyggda beslut. Syftet med systemet är att telefonin snabbt ska komma igång igen.

Det finns en konsumentversion av den tekniska delen, där alla kan se läget i näten på en Sverigekarta. Den finns till exempel på Telias och Tele2:s webbplatser.

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, hur de hanterade incidenten 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. Till exempel inledde vi snabbt tillsyn när Com hem drabbades av ett avbrott som berörde uppskattningsvis 800 000 av företagets bredbands-, telefoni- och tv-kunder.

Krisledningsövning ger bättre färdighet

Telö, en återkommande krisledningsövning för bland annat myndigheter, tele- och Internetbolag samt andra som arbetar med elektronisk kommunikation, tränar sektorn så att den är bättre förberedd när krisen kommer. Den senaste övningen, Telö 09, genomfördes den 6-7 maj 2009. Då var scenariot grundat på terrorhändelser som påverkade Sveriges elektroniska kommunikationer och andra delar av samhället. Övningen samordnas av PTS.

Ny högre utbildning för informationssäkerhetschefer

Försvarshögskolan har i samverkan med det amerikanska National Defense University överfört en kvalificerad utbildning för informationssäkerhetschefer till Sverige. Utbildningen är fokuserad på ledarskap snarare än teknik. En pilotutbildning för svenska deltagare föll väl ut och PTS deltar och medfinansierar en fortsättning och förädling av utbildningen för att göra den relevant för informationssäkerhetschefer hos tele- och Internetbolagen. Vi kommer att marknadsföra utbildningen inför nästa utbildningstillfälle som är våren 2011.

Information ska göra Internet säkrare

Inom Internetområdet arbetar PTS även med information och tjänster till konsumenterna och småföretag så att de ska kunna använda Internet på ett säkrare sätt. Vi har byggt upp 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 även 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 950 000 tester och för Testa lösenord är siffran över 650 000.

Oberoende råd och stöd om IT-säkerhet

PTS bidrar även med avancerade råd och stöd till näringsliv och offentlig sektor för att deras IT-säkerhet ska vara så god som möjligt. I slutändan gynnar det alla oss som använder deras tjänster. Den funktion på PTS som

sköter detta är Sitic, Sveriges IT-incidentcentrum. Under 2009 producerade Sitic exempelvis:

- 208 särskilda råd med information om sårbara program och hur sårbarheten kan åtgärdas
- 9 blixtneddelanden med kritisk information om brister som bör åtgärdas omedelbart
- 715 meddelanden om begäran av nedtagning av infekterade datorer som i många fall fjärrstyrs i illegala IT-attacker.

Din personliga integritet ska skyddas

Den elektroniska kommunikationen underlättar våra liv, men innebär också att vi lämnar ifrån oss information om oss själva. Den här informationen – ofta personliga uppgifter – är viktig och måste skyddas. Vi bedriver därför tillsyn även på integritetsområdet.

Ett exempel är mobila innehållstjänster – ringsignaler, bilder, nyheter och väderprognoser. Den här snabbt växande marknaden innebär nya affärsmöjligheter för tele- och Internetbolagen: att sälja personuppgifter, exempelvis uppgifter om var användaren befinner sig, vidare till leverantörer av innehållstjänster.

PTS och Datainspektionen har gemensamt granskat hur personuppgifter hanteras i mobila innehållstjänster. Ett resultat av arbetet är ett det nu är tydligare hur ansvaret för uppgifterna fördelas mellan de olika aktörerna. För konsumenten innebär det en ökad trygghet när uppgifterna hanteras på rätt sätt.



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