Trafikutskottets och försvarsutskottets offentliga utfrågning om IT-säkerhet

ISSN 1653-0942
ISBN 978-91-85943-33-3
Riksdagstryckeriet, Stockholm, 2008

Förord

IT-säkerhet är en viktig del i den fortsatta IT-utvecklingen där beroendet av IT-system i såväl offentlig som privat sektor alltmer ökar. Enligt vissa studier är mer än 99 procent av det svenska samhällets kritiska infrastruktur beroende av Internet som den stora bäraren av information. Användningen av IT, som är väl integrerat i vårt samhälle, gör att frågor om tillit och säkerhet i våra IT-system måste beaktas inom alla samhällsområden och sektorer för att människor ska kunna känna förtroende för tekniken, för myndigheter och för e-förvaltningen. Det breda informationssäkerhetsarbetet i samhället och statens roll i detta är en fråga som kräver fortsatt och kontinuerlig analys, inte minst givet den snabba utveckling som kännetecknar IT-området.

Riksdagens försvarsutskott och trafikutskott har därför tagit initiativ till en offentlig utfrågning för att inhämta information om de aktuella utmaningarna på IT-säkerhetsområdet samt om vad som görs och behöver göras för att trygga säkerheten i den fortsatta utvecklingen av IT-samhället. Utfrågningen ägde rum den 3 april 2008.

Inbjudna medverkande var:
Dan Larsson, Försvarets radioanstalt (FRA)
Anne-Marie Eklund-Löwinder, Stiftelsen för Internetinfrastruktur (.SE)
Kurt Erik Lindqvist, Netnod Internet Exchange AB
Ingvar Hellquist, Krisberedskapsmyndigheten (KBM)
Anders Johanson, Post- och telestyrelsen (PTS)
Stefan B. Grinneby, Sitic – Sveriges it-incidentcentrum, PTS
Roland Ekström, Kampanjen Surfa Lugnt
Östen Frånberg, Kungliga Ingenjörsvetenskapsakademien (IVA)

Utskotten bedömer att vad som framfördes under utfrågningen är av allmänt intresse och därför bör göras tillgängligt för en vidare krets. Därför publiceras här en utskrift från utfrågningen.

Stockholm i maj 2008

Ibrahim Baylan	Rolf Gunnarsson
Ordförande trafikutskottet	Vice ordförande försvarsutskottet

Innehållsförteckning

Program

Tid:	Torsdagen den 3 april 2008, kl. 9.00–12.00
Plats:	Andrakammarsalen
9.00	**Inledning** *Ibrahim Baylan*, ordförande trafikutskottet
9.05	**De samhällskritiska systemens sårbarhet** *Dan Larsson*, Försvarets radioanstalt (FRA)
9.15	**Hälsoläget på Internet i dag** *Anne-Marie Eklund-Löwinder*, Stiftelsen för Internetinfrastruktur (.SE)
9.25	**Nätangrepp – trender och åtgärder** *Kurt Erik Lindqvist*, Netnod Internet Exchange AB
9.35	**Handlingsplan om informationssäkerhet** *Ingvar Hellquist*, Krisberedskapsmyndigheten (KBM)
9.50	**Säker och robust elektronisk kommunikation** *Anders Johanson*, Post- och telestyrelsen (PTS) *Stefan B. Grinneby*, Sitic, PTS
10.05	**Paus**
10.20	**Kampanjen Surfa Lugnt – erfarenheter och utmaningar** *Roland Ekström*, Kampanjen Surfa Lugnt
10.30	**Internetframsyn* och IT-säkerhet** *Östen Frånberg*, Kungliga Ingenjörsvetenskapsakademien (IVA) *Internetframsyn – ett IVA-projekt om Internets framtidsfrågor
10.40	**Frågestund**
11.55	**Avslutning** *Rolf Gunnarsson*, vice ordförande försvarsutskottet

Stenografisk utskrift från trafikutskottets och försvarsutskottets offentliga utfrågning den 3 april 2008 om IT-säkerhet

Ordförande under utfrågningen var Ibrahim Baylan (s). Bilder som visades under utfrågningen finns som bilagor.

Inledning

Ordföranden: Hjärtligt välkomna till denna hearing om IT-säkerhet. Jag ber om ursäkt för att vi är någon minut försenade. Det vore lätt att skylla på trafiken om det inte vore för att jag är ordförande i just trafikutskottet. Men det är som det är.

IT-säkerhet är ett område som diskuterats och debatterats under lång tid, egentligen ända sedan Internet fick ett ordentligt genomslag i vårt samhälle. Ibland blir man naturligtvis fundersam över hur långt vi kommit. Jag kan konstatera att Internet är en fantastisk tillgång för oss. Den underlättar och till och med förbättrar våra liv på många sätt. Vi har hittat allt fler användningsområden för Internet. Det gäller både oss som privatpersoner och det offentliga, vårt gemensamma samhälle.

Det innebär att vi också blir alltmer sårbara. I och med att vi använder Internet till så mycket blir vi, när det inte fungerar eller när någon medvetet går in för att sabotera, mycket mer sårbara i våra vardagsliv och i samhället i stort. Därför är det viktigt för oss riksdagsledamöter, från både trafikutskottet och försvarsutskottet, att lära oss mer om hur det ser ut i dag och även hur framtiden kommer att se ut.

Vilka hot och möjligheter finns det? Vilka åtgärder behöver vidtas för att vi ska ha ett bättre och mer hållbart informationssystem? Det är mot den bakgrunden vi anordnat dagens hearing. Det ska bli mycket intressant att lyssna på de experter som är här och därefter, under hearingens senare del, få möjligheter att ställa lite frågor till dem.

Vi börjar med den punkt som handlar om de samhällskritiska systemens sårbarhet.

De samhällskritiska systemens sårbarhet

Dan Larsson, Försvarets radioanstalt: Det är trevligt att vara här och se så många kolleger och riksdagsledamöter. Jag jobbar alltså på FRA, där jag är nationell incidenthanteringssamordnare. Det innebär att om något går riktigt snett bland myndigheter och statligt ägda bolag ser vi till att samla de resurser som krävs samt hjälper till att åtgärda och kanske även mildra problembilden.

Jag finns också med i den svenska delen av ISO, informationssäkerhetsstandarden, där Sverige är mycket framgångsrikt. Vi har för övrigt ett möte i

eftermiddag om informationssäkerhet. Som av en händelse finns det en liten blänkare om att det kommit ut en bok med titeln *Terror Online* som behandlar just det område som jag tänkte ta upp i dag. Jag ska alltså försöka fokusera på det uppdrag FRA har och lite grann visa på de problembilder som vi ser finns.

Vi talar om kritiska infrastrukturer, något som för den oinvigde kan vara svårt att veta vad det är. Det är ganska många enheter vi kan tala om i det sammanhanget. Jag har valt den del som kallas Scadasystem, det vill säga processorer som är mycket känsliga och där det finns ett krav att de ska snurra på för att verksamheten inte ska gå ned. Det är vad vi på FRA ser som den största hotbilden framöver; det är alltså målbilden för de illvilliga battingar som nu ger sig på dem.

Vad är det då vi talar om? Jo, vi talar om det som försiggår här i dag, nämligen om regeringens och riksdagens verksamheter. Om de slutar fungera blir det plötsligt illa för Aktiebolaget Sverige. Vi talar om bensin- och oljeleveranser. Vi talar om livsmedeltransporter och vattenrening. Vi talar om bank och finans, och där vill jag ge ett exempel. Även om det inte var nationellt kritiskt hade vi för ett antal år sedan en bank vars bankomater gick ned några dagar före jul, vilket svenska folket inte gillade. Det medförde mycket *bad-will* för den banken. Vi talar också om transportsystemet, och här finns ett antal ledamöter som representerar transportsektorn. Vi talar om energisektorn. Vi talar om informationssystem rent allmänt, samt om telekom. Vi talar även om räddningstjänst, polis och så vidare.

Nu finns det många som säger, inte minst är vi medvetna om det bland kolleger, att vi ibland har en tendens att överdriva vissa saker. Jag vill dock påstå att så inte är fallet. I stället vill jag säga så här: Vi har nu under ett antal år tittat på detta med terrorhot, framför allt cyberterror. Det finns många som tittar på den traditionella terrorverksamheten och har en god överblick över vad den sysslar med. Cyberterror är ett nytt fenomen, och det är inte många som satt sig in i vad det skulle innebära om den så att säga blommade ut för fullt.

Vi har därför tittat lite grann på tendenser och trender, på vad det är som används. Vi gick häromdagen ut och sade lite kaxigt att inom tre år kommer tangentbordet på en dator att vara minst lika farligt som ett massförstörelsevapen. Det står vi för. Vi hittar otroliga saker på nätet. Det finns otroliga mötesplatser där man chattar och talar om vad man har för avsikter. Det är bara att gå in och titta på jihadisternas hemsidor. De budskap som finns på dessa hemsidor är mycket breda. Man kan tolka dem hur man vill. Vi tolkar dem naturligtvis på vårt sätt. De lämnar mycket öppet för egna tolkningar.

Därmed kommer vi till frågan om det är fakta eller *fiction*. Den ena delen är alltså faktadelen och den andra *fiction*-delen. Det finns i dag två läger, och de har naturligtvis olika syn på detta. Vi tillhör definitivt det läger som anser att man ska ta hoten på allvar; jag återkommer till det lite senare. Belackarna, *fiction*-delen, tycker att de eventuella bevis som kommit fram i frågan är ofullständiga. De tycker inte att man ska skrämma upp folk. Det är riktigt, det ska man inte göra. Det som presenteras ska vara underbyggt med fakta. Det

finns ingen sammanställd statistik på vad man eventuellt skulle kunna göra. Detta är ett nytt fenomen, och ingen har sammanställt någonting. Framför allt har det inte hänt någonting. Vi möter ganska ofta uttalandet att det är lite tråkigt att ingenting har hänt. När vi diskuterar med managementfolk, och med beslutsfattare över huvud taget, lutar de sig ofta just mot argumentet att allt gått bra hittills.

Om vi då tittar på faktadelen, och nu har jag baserat den på att FRA kanske är den enda myndighet, förutom Säpo, som är ute och ser det verkliga livet. Hur ser det ut bland våra myndigheter? Vad är riskbilden? På hur stort allvar ska man ta det här? Det vi ser är vilken information verksamheterna har i sina maskiner, burkar och allt vad det kan tänkas vara; ibland tycker vi att det är lite tråkigt att vi inte kan dela med oss av allt vi ser. Vi kan också snabbt se vilken skada det skulle göra för Aktiebolaget Sverige om det kom ut.

Det handlar naturligtvis om utbildningsnivån. Att det ser ut som det gör grundar sig självklart på stor okunskap bland de beslutsfattare vi träffar. Där får vi vara lite självkritiska. Vi är kanske dåliga på att sprida budskapet, dåliga på att tala om vad som är hotbilden.

När vi tittat på webben har vi kunnat se att sättet att rekrytera förändrats starkt under de senaste åren. Man går alltså ut på olika chattforum och låtsas vara någon helt annan än man i själva verket är. På det sättet får man information från dem som vi kallar småhackare, de som finns runt cyberterroristerna och inget hellre vill än att dela med sig av sina *findings* och sina kunskaper. Där hämtar cyberterrorcellerna sin information.

En sista punkt jag vill nämna gäller självkritiken. Vi inser att vi borde vara mycket tydligare mot beslutsfattarna och tala om för dem vilka riskbilder som verkligen existerar där ute.

Ordföranden: Vi återkommer naturligtvis med frågor under den frågestund vi har efter pausen.

Hälsoläget på Internet i dag

Ordföranden: Vi går vidare i programmet och tar pulsen på Internet. Det råder fortfarande feber där, antar jag, eller vad säger du, Anne-Marie Eklund-Löwinder, kvalitets- och säkerhetschef på Stiftelsen för Internetinfrastruktur, .SE?

Anne-Marie Eklund-Löwinder, Stiftelsen för Internetinfrastruktur: Absolut! Inte heller jag tänker måla fan på väggen eller försöka skrämma någon. Hälsoläget på Internet skulle dock kunna vara mycket bättre, visst är det så, och då talar jag om normalläget, som det är när solen skiner, det är vindstilla och allt går som det ska. Om vi tittar på patienten ser vi att den behöver lite friskvård både i form av vitaminer och vaccin och kanske också ett och annat operativt ingrepp. Jag skulle vilja påstå att det finns många verksamheter som

hänger i en ganska skör tråd, och så fort det börjar blåsa kommer den att gå av.

Jag fick frågan om Internet är sårbart. Javisst, det finns väl egentligen ingenting som inte är sårbart. Just nu är det på modet med någonting som kallas för *botnet*. Man läser om det, man hör talas om det, och det sägs att 20–25 procent av alla datorer som är anslutna till Internet förmodas vara kapade och ingå i någon typ av sådana nätverk. Det är alltså stora mängder datorer som är infekterade, styrs av någon och kan samordnas i en attack mot något, oklart vad. Det finns inte någon självklar aktör bakom de olika attackerna, utan varje angrepp är resultatet av någon sorts mänskligt agerande mot någonting som man vill uppnå, antingen det är ekonomisk vinning eller att man bara vill jäklas med någon eller skada en nation.

Jag har fått i uppdrag att tala om hela Internet. Det är naturligtvis svårt att göra det från ett litet land i norra Europa. Det är emellertid viktigt att förstå att samma teknik finns på hela Internet. Det som är ett problem för oss är alltså ett problem överallt. Om man zoomar in på det som jag känner till bäst i vår verksamhet, domännamnssystemet som kan liknas vid patientens centrala nervsystem, finns det en hel del hot. Vi har alltså gjort en hotanalys där vi tittat på vilka hoten är. Den säger ingenting om hur stor risken för att drabbas av sådana hot är, men de finns där och de behöver hanteras på olika sätt. Varje gång någon ansluter någonting till Internet blir man en del av helheten, en del av det stora nätet. Då har man också ansvar för att göra det på ett korrekt och säkert sätt så att andra inte utsätts för risker. Samtidigt är ingen ensam ansvarig, utan här måste man samarbeta i olika former.

Jag ska rätta trafikutskottets ordförande en smula och säga att jag började plugga på universitetet 1981, och 1984 höll jag min första föreläsning i ADB-säkerhet. Det var före Internets tid skulle man kunna säga, i alla fall före det Internet som vi känner. Vi har alltså jobbat med detta en hel del.

Vi gjorde med stöd av Krisberedskapsmyndigheten en undersökning av domännamnssystemet i Sverige 2007. Vi tittade på sådant som hur verksamheten hanterar sin DNS, alltså sitt domännamnssystem, hur man hanterar sin elektroniska post, hur man ansluter sin webb till Internet. Undersökningen bygger på information som är öppen och tillgänglig. Vi behövde alltså inte ha tillgång till något speciellt för att göra en sådan undersökning, utan den bygger på sådant som finns i nätet. Vi tittade bara på domäner som tillhör verksamheter som vi med visst fog kan bedöma vara kritiska i någon mening – bank och finans, statliga myndigheter, landstingen och så vidare. Vi tittade på totalt 828 domäner. I dag har vi 715 000 se-domäner, och många av dem kanske inte är så kritiska, även om de förstås blir det sett ur attacksynpunkt.

Hur såg det då ut? Av de 828 testade domänerna hade en fjärdedel så allvarliga brister att det påverkar tillgängligheten och nåbarheten för de tjänster och resurser som man ansluter till nätet. Mer än hälften av dem hade brister av en karaktär som kanske inte omedelbart påverkar tillgängligheten men ändå är av sådan art att de på sikt behöver åtgärdas. Med ”på sikt” menar jag då inte i ett tioårsperspektiv utan kanske inom 12–18 månader. Detta är repre-

sentativt för Internet som helhet. Det är inte exceptionellt för just .se eller Sverige. Så ser det ut. Problemen innebär att det finns för få maskiner som svarar på frågor om var resurserna finns. Programvaran är för gammal och innehåller därför sårbarheter och otydligheter. Datakvaliteten är dålig, och det finns brister i sättet att ansluta sina system till Internet.

Diagrammet som visas på skärmen är i vissa avseenden naturligtvis ganska alarmerande. De röda staplarna skulle inte alls behöva vara så långa, och utan att behöva anstränga oss nämnvärt skulle vi kunna minska felprocenten till kanske 15, och det utan att göra något som behöver kosta speciellt mycket eller kräva särskilt mycket av oss. Det är helt enkelt fråga om lite ordning och reda, att städa upp lite på hemmaplan, följa den bästa *common practice*, den erfarenhet som finns, och göra som man ska – gör om, gör rätt, som det brukar heta. Tar vi i kanske vi till och med kan minska felprocenten till 10; under det torde det inte vara meningsfullt att gå, för någonstans kommer det alltid att finnas problem. Någonting svarar inte, men då har man någonting annat som tar vid i stället.

Jag ska gå in lite närmare på några av de specifika saker vi tittade på. Jag förstår om det här är gallimatias för de allra flesta av er, men ett mycket vanligt problem som länge varit känt är det som heter öppnade kursiva namnservrar. Det gör det möjligt för utomstående att utföra tillgänglighetsattacker utan att anstränga sig speciellt mycket. Vem som helst kan göra en sådan attack. Det är emellertid enkelt att åtgärda, och dessutom är åtgärderna billiga. Det är alltså en lågt hängande frukt, men vi plockar den inte.

Vi tittade på viktiga parametrar för e-post, bland annat hur man skyddar e-posten när man transporterar den mellan användare i nätet. I 60 procent av fallen sker det inte alls, och för de återstående 40 procenten går det inte att avgöra hur skyddet är infört, om det är på ett bra sätt. Något som slog oss med häpnad är det faktum att många, framför allt myndigheter, skickar sin elektroniska post utanför landet för att tvätta den från virus och spam – och de gör det oskyddat! Och även om det görs skyddat vet man ingenting om hur det ser ut hos leverantören. Man vet inte om de skickar tillbaka den skyddat. Det är naturligtvis mycket allvarligt ur avlyssningsperspektiv.

Samma sak gäller webbtrafiken. Ungefär 75 procent saknar skydd för webbtrafik, och där skydd finns är det i många fall undermåligt. Det innebär till exempel att på många av de webbplatser som kräver att användaren lämnar ifrån sig någon typ av känslig information är den inte tillräckligt skyddad. Skyddet borde således vara långt vanligare, framför allt sett i ljuset av e-förvaltning, e-handel och sådant som vi verkligen vill använda nätet till, det som är den roliga delen, skulle jag vilja säga.

Vi planerar för en uppföljning av undersökningen, och förmodligen har vi en ny rapport till hösten.

En annan fråga gäller dominerande programvaror. I det här fallet handlar det om Microsoft, som ju är dominerande på webbsidan. Det finns områden med andra dominerande programvaror. Det i sig behöver dock inte vara ett

problem, men det blir ett problem den dagen just det programmet innehåller ett allvarligt fel. Då får man en stor träffyta för attack.

Behöver vi förbereda oss för attacker? Ja, självklart. Som jag sade inledningsvis behöver patienten en rejäl dos friskvård. Allmänna kommunikationsnät är och förblir en viktig del av samhällets informationshantering och också i vår hantering av allvarliga händelser, svåra påfrestningar och beredskapssituationer. Det som inte är infört den dagen solen skiner och det inte blåser kommer inte att fungera den dagen det börjar storma. Vi måste redan från början veta vad vi ska göra. Vi måste bygga upp ett fungerande försvar mot alltmer sofistikerade attacker. Som Dan berättade är det just nu på modet att försöka komma åt Scadasystem.

I ljuset av 25 års arbete finns det några saker som jag vill poängtera. Vi behöver ha koordinering men kanske inte så mycket ansvarsfördelning. I dag får man intrycket, och det intrycket har jag haft i många år, att myndigheterna konkurrerar med varandra. Så får det *inte* vara. Myndigheterna ska samverka och samarbeta. Det behöver vidtas praktiska åtgärder. Vi behöver inte fler utredningar där man häller ned alla myndigheter i en burk, skakar om och häller ut dem igen och ser om det blir bättre. Vi behöver fler konkreta åtgärder. Det robusthetsarbete som bedrivs av till exempel PTS är ett mycket bra exempel på konkretion där man faktiskt kommer framåt.

IT-säkerhet är inte Svarte Petter. Det är viktigt att komma ihåg och något som vi alla behöver fundera över om vi ska fortsätta att använda informationssystem i den omfattning som vi vill. Det tror jag är bra för Sverige från både tillväxtsynpunkt och ur andra aspekter. Det innehåller många delar. Skyddsnätet består inte av endast en maska utan av en väldig massa maskor som ska hänga ihop och filtrera på en lagom nivå så att vi lägger ned lagom med insatser. Den kommersiella och tekniska utveckling som vi ser skapar oerhört många möjligheter, och jag vill inte att vi enbart ska se det som ett problem. Det är inte en obotlig patient. Det är en patient som går att fixa.

Vi tar i vår rapport också upp några råd och rekommendationer om hur man får just den delen av infrastrukturen, alltså de saker vi tittade på, att bli mer robust. Någon behöver naturligtvis peka med hela handen och kanske inte helt och fullt låta alla göra som de vill och se om det blir bra i slutändan. Det är viktigt att vi ansluter kritiska resurser till fler namnserveroperatörer så att de alltid fungerar, alltså även om det blåser. Vi kan behöva ha en central namnserverdrift som svarar på frågor om dessa resurser ifall verksamhetens egna system skulle vara onåbara. Det kan vara nödvändigt att bygga upp och upphandla en virustvätt och skräppostrensning inom landet för att slippa skicka så mycket information över landets gränser.

Jag tycker att vi även ska utfärda riktlinjer för vad som är acceptabelt i hanteringen av elektronisk post. Dessutom finns det behov av att inrätta någon sorts central funktion. Om den sedan är upphandlad eller inte låter jag vara osagt, men det är inte okej att alla myndigheter själva ska lära sig det ganska komplicerade arbete det innebär att ha ett bra transportskydd i form av certifikat och andra kryptografiska metoder. Det är nämligen det vi talar om.

Alla säkerhetsfunktioner behöver någon form av krypteringsteknik. Endast så kan vi skydda information. Det gäller det som transporteras i nätet, nätets egna styrfunktioner och all den information som transporteras och lagras i databaser och informationssystem.

Ordföranden: Ska man tro på Computer Sweden är det Sveriges främsta IT-säkerhetsexpert vi just lyssnat till. Då har man rätt att dra över några minuter. Kanske är det så inom IT-sektorn att det som gällde förra året inte gäller längre, eller? Ja.

Nätangrepp – trender och åtgärder

Ordföranden: Då går vi vidare i programmet, till den punkt som handlar om nätangrepp, trender och åtgärder.

Kurt Erik Lindqvist, Netnod Internet Exchange: Tack! Om de två föregående talarna inte skulle måla fan på vägen kanske det är mitt jobb.

Jag jobbar alltså på ett företag som heter Netnod. Vi handhar driften av gemensamma kritiska Internetresurser i Sverige, bland annat. Vi arbetar nära en del svenska och utländska myndigheter och driver en hel del tjänster som krävs för att Internet ska fungera så som vi tror att det ska fungera.

Vi har sysslat lite med att säkra den här infrastrukturen och att titta på hotbilder. Om man ser på hot kan man dela in dem på många sätt, och jag tänker dela in dem på några sätt.

Det första är hot mot nationen Sverige. Då tänker jag mig former av hot som riktar sig mot Sverige rent allmänt, mot myndigheter eller mot vad som kan uppfattas som svenskt. Sådana hot som sker i dag sker nästan varje vecka. De sker ganska ofta. De kan närmast betraktas som delar i större skeenden. Detta är verktyg som används för att förstärka existerande hotbilder.

Ett känt exempel som ofta används är attackerna på Estland i maj förra året. Jag hade förmånen att vara på plats och jobba med de estländska myndigheterna. Det här var självklart bara ett komplement till de kravaller som faktiskt skedde på gatorna, även om attackerna säkert tjänade flera syften. De var en del i ett större skeende; de var inte isolerade till att bara ske på Internet. De var inte heller speciellt uppseendeväckande som attacker på Internet. Det sker varje vecka större och mer omfattande attacker, men de kanske inte riktar sig mot nationalstater eller mot sådant som är estländskt. Däremot var det inte första gången som det här skedde.

Jag jobbade tidigare hos en stor teleoperatör som hade Nato som kund. Där hade man under kampanjen i Kosovo faktiskt ganska omfattande attacker som riktade sig mot Nato, som ett komplement, återigen, till de demonstrationer som skedde mot Natos handlingar runt omkring i världen.

Här är det viktigt att komma ihåg att Internet speglar samhället i övrigt vad gäller kriminalitet och terrorism och så vidare. Det här är bara en förlängning

av andra skeenden. Om vi förstår existerande hotbilder och om vi förstår vad de här hotbilderna syftar till kan vi säkert också ana oss till vad man kan tänkas försöka uppnå med de här cyberattackerna. Det är kanske viktigt att man i den här hotbildsbedömningen också tar med IT-aspekter.

Det finns också hot mellan nationalstater. Det finns säkert andra myndigheter här som är betydligt bättre på att prata om det än vad jag är. Men det finns något som kanske är viktigt att komma ihåg ur någon sorts nationellt perspektiv och någon sorts hotbildsperspektiv. För att man ska skydda sig mot det här och skydda sig mot alla IT-attacker gäller det att allmänna system, såsom vi hörde här innan, är så robusta som möjligt och så skyddade som möjligt. Om de system som vi använder varje dag – det gäller myndigheter, länsstyrelser och så vidare – är tillförlitliga, är robust byggda och fungerar väl i ett normalfall är sannolikheten för att de ska fungera väl också i en krissituation betydligt bättre. Det är ofta väldigt svårt att börja laga läckande båtar när de redan är sjösatta.

Här är det viktigt, återigen, att understryka att man försöker säkra kända problem, som mycket av det som Anne-Marie pratade om faktiskt är. Det är också så att angripare tenderar att välja mjuka mål, lätta mål och inte mål som på förhand är kända som ganska hårda eller robusta.

Det är också viktigt att säga, när nationalstater är inblandade, att det finns exempel på att nationer har angripit andra nationer. Det har antingen varit som ett rent offensivt vapen eller så har syftet varit underrättelseinhämtning – jag delar in i två kategorier. Men då pratar man om motståndare som har väldigt stora resurser bakom sig.

En annan form av hot är hot mot oss alla som medborgare. Medborgarnas beteende för att hitta information och för att kommunicera med myndigheter ändras. I dag är Internet en väldigt stor del av det här. Vi har sett exempel på det. Regeringens webbplats gick ned för att allmänheten ville läsa budgeten. Det är kanske inte den mest uppseendeväckande händelsen, men det räckte tydligen för att sätta en ganska kritisk informationskanal ur spel. Nu vill jag inte på något sätt nedvärdera budgeten, men så var det i alla fall. Det har funnits andra tillfällen då man har kunnat se att medborgarna har vänt sig till Internet som medium för att hitta information, antingen på nyhetsplatser eller på regeringssidor. Jag tänker på tsunamikatastrofen och så vidare.

Det finns en annan sak som är väldigt oklar för mig som medborgare. Det finns inget klart och tydligt kommunicerat gränssnitt när det gäller hur jag ska hitta information och under vilka omständigheter jag ska hitta information. Jag gick i skolan någon gång i början av 80-talet. Då fick man lära sig att man skulle stänga dörrar och gå in och lyssna på radio. Någon liknande informationskanal kanske skulle vara intressant i dag. Tyvärr är det så med Internet att även om jag sätter mig framför datorn och tittar på min webbläsare kommer informationen inte till mig automatiskt. Det måste finnas en klar och tydlig informationskanal när det gäller hur jag får information från myndigheterna.

För mig som är inblandad i en ganska central drift av Internet i Sverige är det ganska oklart om det finns en kanal i dag som skulle kunna hantera den informationsspridningen. Man bör anta att det här är något som ska kunna hantera ungefär 3 ½ miljoner hushåll som samtidigt vill hämta information.

Man kan titta på andra händelser, som stora nyhetshändelser. Beteendemönstret verkar vara att man helt enkelt klickar på *reload*. Man vill hämta informationen på nytt hela tiden, vilket gör att det är en konstant bombardering av förfrågningar vad gäller information, vilket är ett ganska stort skalproblem.

Vad gäller hot rent allmänt och kanske också hot mot myndigheter är i praktiken all form av hot på Internet någon form av attacker. Väldigt många av dem sker i dag för ekonomisk vinning. Om man ska kalla det för maffiaorganisationer eller terrororganisationer är kanske mindre intressant. Det är organiserad brottslighet där man hyr, köper, driver olika former av attackverktyg som består av hundratusen till miljontals kapade datorer. Det är datorer som är infekterade med olika former av program som kan användas för att fjärrstyra de här datorerna så att de skickar oönskad e-post eller utför överbelastningsattacker, liknande dem vi såg i Estland. Och det är andra liknande attackformer.

Ur den här aspekten är myndigheten egentligen bara ytterligare ett mål. Tyvärr är det en högre risk, för myndigheter är ganska benägna att följa upp attacker och att polisanmäla – det gäller kanske i mindre utsträckning på andra områden. Utdelningen är kanske lite mindre, det vill säga att det är svårt att utöva utpressning mot en myndighet. Däremot finns det andra former av attacker som man kan tänka sig mot myndigheter. Det kan handla om informationsläckage eller om stulen information som kan säljas eller användas i utpressningssyfte mot myndigheter. Det kan alltså handla om att man då inte ska läcka hemlig information, till exempel.

Kostnaden för att skapa en sådan här attack i dag är ganska låg jämfört med de pengar som man normalt får ut av det här, och väldigt lite av detta polisanmäls.

Sedan gäller det allmänna hot mot samhället. Ofta sker de här attackerna mot aktörer som har väldigt mycket att förlora på störningar, till exempel online-banker, aktiehandelsplatser, online-spel och handelsplatser. Dessa har på något sätt realtidsinteraktion med sina kunder och tjänar pengar på transaktioner. Om transaktionerna hindras från att utföras är det självklart att det är en stor skada för den som driver den här tjänsten. Då kanske man är mer benägen att betala det här snarare än att vänta på en polisutredning.

Man använder också väldigt mycket så kallade *spam-runs*. Man skickar spam. Vi skulle aldrig få spam om det inte var så att folk faktiskt handlade till följd av den här Viagrareklamen. Detta anses i dag vara en miljardindustri. Man tjänar ganska mycket pengar på det här, på *phishing* och genom det som sker mer och mer, nämligen att man lämnar marknadsdrivande information och investerar i lämpliga aktier.

Allt det här är i grund och botten kriminalitet som bör bekämpas av polis och åklagare. Men återigen: Utan resurser och utan polisanmälningar är det svårt att komma vidare med det här.

Den stora risken med allt det här är på något sätt, i förlängningen, att allmänhetens tilltro till systemet skadas om detta inte åtgärdas. Om det här inte följs upp och om det inte kommer fällande domar som kan publiceras och som syns i pressen finns det nog väldigt stor risk för att allmänhetens tilltro till systemet tar skada. Ett exempel är de kända Nordeamejlen vad gäller *phishing*. Även om Nordea till slut faktiskt gjorde någonting åt det här, eller försökte göra någonting åt det, är det ganska uppenbart att allmänhetens tilltro till ett sådant system självklart måste skadas om det är en och samma bank som konstant dyker upp i de här mejlen. Nu vill jag kanske inte hacka på just Nordea, men jag nämner det som exempel.

Vad gör man då i Sverige? Sverige ligger faktiskt ganska långt framme eller har legat ganska långt framme vad gäller distribuerad säkerhet och fysiskt skydd. De resurser som vi driver ligger i dag skyddade i bergrum som är byggda och drivs av PTS. Det här är någonting som omvärlden tittar på i dag. Vi har haft flera besök där man från omvärlden har tittat på vad vi har gjort i Sverige tillsammans med PTS.

Jag tror att det är viktigt att vi behåller det här ledarskapet vad gäller de här initiativen, framför allt vad gäller distribuerad kunskap. I dag bedriver vi vår verksamhet på fem platser i Sverige, oberoende av varandra.

Det är viktigt att säga att det i Sverige är ett väldigt bra samarbete mellan alla operatörer vad gäller de här frågorna. Det är även ett bra samarbete med internationella aktörer. Det här samarbetet används då vid olika former av attacker.

Vad tror jag att vi måste göra? Om man nu ska använda termen staten – det är någon sorts gråluddigt moln – så tror jag att staten måste ta ett ansvar gentemot sina medborgare och leverera de tjänster som man levererar rent allmänt även till sina medborgare på Internet.

Man måste tala om hur ansvaret för informationsgivning ser ut. Vart ska jag som medborgare vända mig för att få information? Staten måste på något sätt göra det här genom en centralaktör som har en teknisk lösning, en teknisk plattform som gärna är ganska adekvat i fråga om det som jag pekade på tidigare. Det här är något som flera länder tittar på i dag. Här har vi en chans att vara ledande och kanske visa hur det här egentligen skulle göras. Man måste då också jobba med brottsbekämpning, som vi sade innan.

Jag vill också att man ska säkerställa att det finns kompetens i Sverige. Det kan man bland annat göra genom att staten ställer högre krav i sina upphandlingar och är en kunnig kund. Man bör ha en central kravprofil när det gäller hur myndigheter ska göra det här, så att man, som Anne-Marie pekade på, inte är sämst i klassen, som man är i dag. Det är svårt att ställa krav på resten av samhället vad gäller robusthet när man är sämst i klassen. Man kanske ska ägna sig lite åt att äta sin egen hundmat.

Samtidigt som alla myndigheter har väktare i receptionen som ser bra ut vore det kanske bra om man hade en närvaro på Internet som var robust och tillgänglig. Man kanske kunde vara lite mer framåt vad gäller ny teknik, rent allmänt.

Jag tror också att det är precis som Anne-Marie sade. Vi har väldigt mycket kunskap i Sverige på det här området. Vi ligger väldigt långt framme. Vi har legat väldigt långt framme. Men omvärlden börjar i dag fokusera mer och mer på det här, kanske mer än vad vi gör. Vi hade ett försprång 1997, när det här arbetet började. Inget av det här är speciellt svårt. Det handlar inte om att man inte vet hur man gör. Men pappersutredningar skyddar väldigt dåligt mot attacker på Internet. Här är det då viktigt att man ägnar sig, precis som Anne-Marie sade, mer åt konkreta åtgärder än åt fler utredningar och skapande av nya myndigheter.

Den svenska staten har en väldigt liten operativ roll i det här. Man driver ingen egen operatör längre. Man har ingen direkt insyn i de verkliga trafikflödena. Däremot kan man underlätta en hel del arbete, och man kan se till att det finns långsiktiga robusthetsåtgärder som kanske är sådant som andra aktörer inte gärna ägnar sig åt. Där tror jag att myndigheterna har en väldigt viktig roll att spela. Men återigen: Det ska göras genom att man snarare samarbetar med varandra än konkurrerar med varandra.

Ordföranden: Tack för det! Den oro man känner som ansvarig politiker handlar inte alltid, inte bara i alla fall, om det man hör och läser om utan också om mycket av det som händer som man aldrig får höra talas om. Det är svårt att göra en bedömning, eftersom de aktörer som blir utsatta kanske inte är så intresserade av att sprida detta. Det gör det hela ganska mycket svårare.

Handlingsplan om informationssäkerhet

Ordföranden: Vi går vidare på dagordningen och går då till Krisberedskapsmyndigheten och Ingvar Hellquist, som är chef för informationssäkerhetsenheten. Han ska prata om den handlingsplan som presenterades i går. Varsågod!

Ingvar Hellquist, Krisberedskapsmyndigheten: Tack så mycket! Tack för att jag fick komma och prata!

Uppgiften att hålla samman det nationella informationssäkerhetsarbetet är en tuff uppgift.

Informationssäkerheten i Sverige är inte tillräckligt bra, men nu lämnar Krisberedskapsmyndigheten en handlingsplan som kan ändra på det förhållandet.

Handlingsplanen är ett resultat av ett regeringsuppdrag som gavs i början av 2007. Efter ett års arbete och en omfattande samverkan med myndigheter,

näringsliv och landsting lämnas förslag till 47 åtgärder som ska kunna ge ett säkrare och effektivare Sverige.

Myndigheterna som ingår i Samverkansgruppen för informationssäkerhet, kallad Samfi, har lämnat samråd till den här handlingsplanen.

Innan jag går in på handlingsplanen vill jag kort beskriva de hot och risker och sårbarheter som vi med de här förslagen försöker hantera.

Vi redovisar årligen en lägesbedömning för regeringen. Det gjorde vi i år den 1 mars. Den innehåller några dramatiska beskrivningar av vad som hände under 2007. Det mest omtalade, som vi redan har hört nämnas, är de IT-attacker som riktade sig mot Estland i april och maj 2007. Det unika var att de var riktade mot ett land. De som styrde attackerna kom också undan och blev inte identifierade.

Attackkapacitet utnyttjades från datorer över hela världen, också från Sverige. Det var nära att angriparna lyckades nå in i kritiska samhällsfunktioner, men nu blev det begränsade störningar. Det beror bland annat på att man i Estland har en fungerande basnivå för informationssäkerhet i samhället och att man fick ett omfattande stöd från omvärlden för att blockera de här attackerna.

Vi har studerat de här attackerna närmare och lämnat en rapport över dem. Den presenterades i november. Där försökte vi att konstatera hur de svenska förutsättningarna för att klara en motsvarande attack ser ut. Där pekar vi på att det finns allvarliga brister i myndigheternas förmåga att hantera sin egen informationssäkerhet, att förvaltningstraditioner med självständiga myndigheter gör det svårt att få en gemensam lägesbild, att det bara finns ett fåtal experter i Sverige som har operativ erfarenhet och förmåga att hantera så här omfattande attacker och att hushållens bredbandskapacitet, svagt skyddade myndigheter och företag kan vara värdar för mycket stora attacker.

Vi hörde Anne-Marie beskriva lite grann hur tillståndet såg ut i den studie som vi gjorde tillsammans.

I den här lägesbedömningen, som vi lämnade, slog vi också fast att vårt beroende av IT stadigt ökar. Det sker särskilt i tidskritiska verksamheter. Vi har särskilt noterat sjukvården och finanssektorn. Sedan konstaterade vi att IT-kriminaliteten ständigt ökar.

Så över till handlingsplanen, som vi lämnade till regeringen i går. I den lämnar vi förslag för att förbättra samhällets informationssäkerhet, från normaltillstånd till kris. Det är alltså inte bara en krisplan. I handlingsplanen föreslår vi också en förvaltningsprocess där de här åtgärderna årligen följs upp och uppdateras.

Den startar inte från början, utan den tar sin utgångspunkt i flera centrala utredningar. En av de mest centrala är informationssäkerhetsutredningen *Säker information* från 2005, den som Anders Svärd ledde.

Regeringen har beskrivit och berört frågan i en proposition från den 18 mars i år, *Stärkt krisberedskap – för säkerhets skull*, och i kommittédirektivet *En ny myndighet med ansvar för frågor om samhällets krisberedskap och*

säkerhet. Direktivet rörde den nya myndigheten, Myndigheten för samhällsskydd och beredskap, som ska inrättas den 1 januari 2009.

I handlingsplanen har vi identifierat fyra områden som är prioriterade.

Det behövs en grundläggande säkerhetsnivå för samhällets informationssäkerhet. En sådan basnivå behövs för att säkerställa skyddet av samhällsviktiga informationstillgångar och tillgången till sådan information.

Samhället måste kunna hantera omfattande IT-relaterade störningar och kriser. För det behöver det inrättas en operativ nationell samordningsfunktion.

Det behövs en bred satsning på kompetenshöjande åtgärder på alla nivåer i samhället, från grundskola till spetsforskning. Det handlar om de experter som jag talade om tidigare. Bland annat föreslår vi att ett nationellt kunskapscentrum för informationssäkerhet ska inrättas.

Det behövs ett förbättrat sektorsövergripande arbete inom området. Det kan man uppnå genom heltäckande föreskrifter på området. De bör kunna utformas för att gälla alla myndigheter under regeringen. Samtidigt behöver det sektorsvisa ansvaret förtydligas. Det behöver också ges ändamålsenliga rekommendationer till samhället.

Vad finns det då för syfte med att ha en god informationssäkerhet? Jo, vi har pekat på att det handlar om att främja samhällets effektivitet och kvalitet i informationshanteringen, att främja näringslivets lönsamhet och tillväxt, att stödja samhällets brottsbekämpning och beredskap mot allvarliga störningar och kriser, att främja medborgarnas fri- och rättigheter och personliga integritet och att främja medborgarnas förtroende för informationshantering och IT-system.

Att man har en god vardagssäkerhet är oftast liktydigt med att man har en bra förberedelse för att kunna hantera det som sedan övergår till att bli en krissituation. De verktyg och metoder och attacker som man blir utsatt för är som regel desamma. Det är bara styrkan i dem som varierar.

Våra åtgärdsförslag lämnas inom områdena

- informationssäkerhet i verksamheter
- kompetensförsörjning
- informationsdelning, samverkan och respons
- kommunikationssäkerhet
- säkerhet i produkter och system.

Vissa av de här åtgärderna föreslår vi att regeringen beslutar om. Men i många fall kan man besluta om åtgärderna inom ramen för befintligt myndighetsansvar och den normala budgetprocessen.

Vi föreslår att regeringen ska besluta att ge MSB, som den nya myndigheten förkortas, rätt att utfärda föreskrifter och allmänna råd för att myndigheter ska kunna uppnå grundläggande och särskilda tilläggskrav på informationssäkerhet.

Vi föreslår en operativ nationell samordning. Där föreslår vi att regeringen ska ge uppdrag som handlar om att underlag ska lämnas om hur man kan skapa en sådan administrativ och teknisk infrastruktur för informationsdelning och respons för hela samhället. Förslaget bör då omfatta en gemensam

kunskapsdelning, en gemensam lägesbild och en operativ förmåga vid omfattande IT-incidenter.

Vi föreslår att regeringen beslutar om att inrätta ett nationellt kunskapscentrum för informationssäkerhet. Syftet ska vara att öka och samordna kvalificerad kunskapsutveckling och samtidigt utgöra ett expertcentrum inom området. Det kan organiseras i form av en stiftelse med en styrgrupp, med intressenter från såväl stat som näringsliv och akademi. Vi föreslår också att det kan delfinansieras genom statliga anslag.

Vi föreslår att regeringen ska kräva ett formellt ansvarstagande från myndigheterna för hantering av informationssäkerhetsrisker och ställa krav på att myndigheterna i årsredovisningarna talar om på vilket sätt gällande krav inom informationssäkerhet uppfylls.

Vi föreslår en översyn av lagstiftningen på informationssäkerhetsområdet. Regeringen bör tillsätta en utredning för att göra en heltäckande analys av författningar som berör informationssäkerhetsområdet.

Det är en rasande snabb utveckling. Det är en lagstiftning som inte riktigt hinner hänga med. Det är väldigt många olika områden som påverkas, och det får effekter som man inte riktigt kan förutse. Detta ställer då krav på att man trots att det går saktare ändå gör en rejäl utredning om detta.

Vi föreslår en obligatorisk incidentrapporteringsplikt för myndigheter när det gäller allvarliga incidenter. Den ska vara omedelbar, för att man ska ha en möjlighet att få en gemensam lägesbild och genomföra de här responserna. Det finns vissa typer av incidenter som är undantagna på grund av annan lagstiftning. Det handlar om förundersökningssekretess och annat.

Vi föreslår att man ska utveckla förmågan att förebygga och bekämpa IT-relaterad brottslighet. Det gör vi genom att vi föreslår att regeringen ska tilldela Rikspolisstyrelsen särskilda medel för att utveckla förmågan att bekämpa IT-brottslighet.

Vi föreslår att regeringen ska etablera ett forum för samverkan inom ramen för Epcip – European Programme for Critical Infrastructure Protection – och den nära koppling som finns till informationssäkerhet, CIIP. Vi föreslår att det uppdraget ges till den nya myndigheten och PTS som en förberedelse inför ordförandeåret.

Som har nämnts här flera gånger tidigare föreslår vi en statlig samordnad satsning på säkerheten i digitala kontrollsystem, en Scadasatsning. Det är egentligen självklart att det beror på den viktiga funktion som de har för samhällskritisk verksamhet.

Utöver de här nio förslagen finns det ytterligare 38 förslag. Det är svårt att gå in på allihop här. Jag vill lyfta fram några med betoning på näringslivet, eftersom det kanske har den största betydelsen för samhället i de här frågorna.

Målsättningen med de förslagen är att staten ska ha en kontinuerlig samverkan med existerande nätverk för informationssäkerhet, att det ska finnas en god privat–offentlig samverkan i de sektorer och tvärsektoriella områden där samhällets kritiska infrastruktur befinns i privat ägo och att man ska ha ett fördjupat samarbete med finanssektorn i informationssäkerhetsfrågor och att

man ska kunna tillämpa branschgemensamma säkerhetskrav som är framtagna i samverkan med staten.

Jag anser att det är en stor skillnad i förutsättningarna den här gången för att förslagen ska kunna realiseras. Det är en nyvunnen medvetenhet hos alla samhällsaktörer, och det finns samförstånd mellan de myndigheter som har varit med och tagit fram den här handlingsplanen. Nu förväntar vi oss att regeringen fattar de nödvändiga besluten.

Ordföranden: Tack så mycket! En rasande snabb utveckling – ja, det kan man verkligen säga. Det känns nästan alltid som att vi är två steg efter. Vi kanske kommer ifatt någon gång, men än är vi inte där.

Säker och robust elektronisk kommunikation

Ordföranden: Vi går vidare på dagordningen. Det är två företrädare för Post- och telestyrelsen, Anders Johanson och Stefan B. Grinneby, som ska prata om säker och robust elektronisk kommunikation. Varsågoda!

Anders Johanson, Post- och telestyrelsen: Tack! PTS, kommunikationsmyndigheten alltså, jobbar för att alla i Sverige ska ha tillgång till effektiva, prisvärda och säkra elektroniska kommunikationer. Jag är då ansvarig, inom PTS, för den här delen som handlar om säkra elektroniska kommunikationer.

Det finns ungefär 450 företag som levererar elektroniska kommunikationstjänster.

Vår målbild är ungefär att alla ska ha tillgång till säker elektronisk kommunikation. Med det menar vi då telefoni, Internet, bredband och annan kommunikation baserad på Internetprotokollet. Det är säkert många här i salen i dag som har bredband hemma med till exempel tjänster som tv, telefoni och Internetåtkomst. Det är blandat i denna bredbandsöverföring.

Det är en påtagligt snabb utveckling och en hård konkurrens bland de företag som finns på marknaden, dessa 450 plus tusentals tjänsteföretag. Det är en mycket hård konkurrens. Lönsamheten är många gånger dålig – det ser vi på börsen, till exempel. Och säkerheten kommer i många fall på undantag.

Sverige ska ha en robust infrastruktur. Det är någonting som riksdagen har slagit fast sedan många år tillbaka. Redan på Televerkets tid satsades det mycket på det, och det satsas fortfarande en del på det.

Integritetsskyddet ska, till exempel, vara högt, så att det inte läcker uppgifter ur den elektroniska kommunikationen på ett otillbörligt sätt, och vi ska ha ett skydd mot IT-incidenter i näten.

En grundläggande lagstiftning för oss när det gäller detta är lagen om elektronisk kommunikation. Riksdagen skärpte för övrigt den rejält, vad gäller säkerhet, för två år sedan i efterdyningarna av stormen Gudrun, som framför allt drabbade södra Sverige hårt.

Jag ska gå igenom de tre områden som vi arbetar med inom myndigheten.

Det första området handlar om att åstadkomma robusta elektroniska kommunikationer. Här är då ett antal exempel på åtgärder som görs. De här åtgärderna – det är för närvarande ungefär 90 samverkansprojekt – sker i privat–offentlig samverkan. Vår myndighet, andra myndigheter och framför allt de operatörer som agerar på marknaden är involverade.

När det gäller finansieringen är det så att operatörerna delvis själva finansierar för att de har nytta i sina affärer av att systemen fungerar, men det är också samhället som finansierar, genom skatter och genom att operatörerna måste betala avgifter till staten, som PTS administrerar och tar in. De robusthetsåtgärder som PTS finansierar finansieras alltså både av skatter och genom avgifter från operatörerna.

Sedan finns det ett antal punkter som visar exempel på sådant som har gjorts och som pågår nu. Det gäller till exempel de sista punkterna här. Alla viktiga knutpunkter i elektronisk kommunikation finns i skyddade utrymmen, i skyddade bergrum, så att vi har ett högt fysiskt skydd för dem. Det gäller till exempel Netnode som nyligen presenterades här och alla stora operatörer.

Under de senaste åren har det lagts ned ett omfattande arbete på att genomföra gemensamma krisövningar i branschen och också på att utforma gemensamma informationssystem för att få lägesbilder av krisläget och kunna agera tillsammans.

Det är en väldigt positiv och spännande utveckling att de stenhårt konkurrerande företagen i en kris i form av att det är avbrott eller stopp i kommunikationerna sätter sig tillsammans, arbetar gemensamt och lägger konkurrensen åt sidan för att åtgärda så att det hela kommer i gång igen. Sedan kan man börja konkurrera igen om kunderna.

Bland annat har vi ett europeiskt finansiellt stöd för att utforma de gemensamma lägesuppfattningssystemen från det europeiska program, Europeiska finansieringsprogrammet, som Ingvar Hellquist nyss nämnde.

Det andra området är tillförlitlighet och exempel på vad som görs där. Regeringen beslöt för drygt ett år sedan om en strategi för säkrare Internet. Där jobbar vi nu enligt en handlingsplan ihop med många aktörer för att förverkliga den.

PTS har också mandatet att ge ut föreskrifter, allmänna råd och rekommendationer och utövar tillsyn över operatörernas säkerhetsarbete. Det tillsynsarbetet har kunnat stärkas avsevärt efter riksdagens komplettering av lagen för ett par år sedan.

Det är väldigt viktigt med internationell samverkan och information till Internetanvändare eftersom de är en del av hela säkerhetsproblemet. Det är svårt för oss alla som privatpersoner att veta hur man ska hantera det tekniska skyddet. Därför görs det en hel del arbete på det. Det kommer vi att höra mer om efter pausen till exempel när det gäller kampanjen Surfa Lugnt.

Det tredje området är skydd mot IT-incidenter i form av enheten Sitic som finns i PTS. Den fångar upp sårbarheter och incidenter som sker på nätet och informerar om det. Vi ska strax få några minuters presentation om hur det går till.

Slutligen vill jag från min sida ta upp några orosmoln. Vi har tidigare under morgonen hört att samhället i dag är helt beroende av att elektronisk kommunikation fungerar. Komplexiteten ökar kraftigt i elektronisk kommunikation. Det är väldigt påtagligt.

Alltmer komplexa system växer samman, telefoni, medier, bredband och alltihop. Sårbarheterna ökar, och det uppstår nya sårbarheter. Robusthetsåtgärderna minskar totalt sett relativt utvecklingen. Det är många gånger den hårda konkurrensen som gör att man sjösätter och lanserar nya lösningar utan att det är säkrat och kvalitetssäkrat.

Robusthetsåtgärderna och de finansiella musklerna från statens sida i detta minskar. Risken är att vi får fler kriser och incidenter som inträffar som ställer till oreda i samhället.

Stefan B. Grinneby, Sitic: Jag har några få bilder om vad vi redan gör. Ni har hört lite grann om hoten. Sitic, som Anders berättade om, publicerar information om sårbarheter som kan hota tekniska system. Vi har i och med år 2008 fått en lite utökad budget för att göra mer aktiva insatser åt de myndigheter som behöver det bäst.

Kort kan man säga att när man ansluter något till Internet i dag, som andra talare också har sagt, är man direkt en del av Internet. Man är också direkt angripen. Man råkar ut för saker och ting med detsamma.

En oskyddad maskin som sätts upp på Internet i dag är förmodligen övertagen inom ungefär 30 minuter. Om man vet om det eller inte avgörs av hur pass noga man observerar vad som händer i ens system. Någonstans vid någon kritisk punkt får man en kris. Man har så lite kontroll över systemet att ett problem uppkommer i verksamheten man bedriver.

Det kan vara svårt att avgöra när det sker. I mitt perspektiv har du problem när den första angriparen har lyckats ta över en liten bit av din maskin. Men det kan dröja ganska länge innan du på något vis märker det. Vi försöker i dag hjälpa myndigheterna att etablera en högre kunskapsnivå om det.

Det har visat sig att en metod att hantera det är väldigt bra. Man måste följa någon typ av modell för att veta om man är på väg åt rätt håll eller inte. Sitic agerar efter principen att de som jobbar med detta dagligen är de som vet bäst. Man känner sina egna system.

Man kan ta ett exempel. Du står och lagar mat hemma i köket, och plötsligt uppstår det något problem med såsen. Såsen skär sig och så vidare. Att det plötsligt ska komma in någon annan kock och rädda din sås är ganska osannolikt. Det är väldigt svårt att laga mat i någon annans kök. Du kan ha hjälp av att det står någon och tittar över axeln och ger dig goda råd under tiden. Det är på det sättet vi försöker agera i dag.

Detta är vår Siticmodell just nu. Vi har en sexstegsmodell där vi erbjuder myndigheter hjälp med att hantera de problem som uppstår. Vi kan också hjälpa dem med att avgöra om de har ett problem. Det är någonting vi redan gör i dag.

Sexstegsprocessen har en ganska kortfattad enordsrad med namn. Jag har skrivit till lite mer om hur man kan se på det hela. Det första är att bestämma: Har man ett problem eller inte? Är man hackad, som det populärt heter? Oftast vet man inte det.

Det gäller sedan att få stopp på det ymniga blodflödet ur patienten, som Anne-Marie Eklund-Löwinder talade om. Man måste på något vis få hejd på problemsituationen med detsamma.

Man måste ställa sig en fråga. De flesta människor hoppar sedan direkt till steg fem. Jag kan sammanfatta det för er. Ni sitter hemma och jobbar vid er dator. Den verkar gå lite långsamt. Då startar ni om den. Jag vet inte om det är någon som har gjort det. Det kan i varje fall hända.

Ni har kört steg ett, två och fem i ett handgrepp. Det är färdigt där. Men ni vet inte vad det var som hände. Vi är intresserade av att ta reda på vad som egentligen hände. Där har vi hjälp av våra syster- och brodermyndigheter. Det finns gott om duktiga tekniker på andra myndigheter.

Det kan vara intressant att veta vem som gjorde detta för att stoppa den personen från att agera likadant igen. Där är det återigen inte Sitic själv som agerar utan andra myndigheter tillhörande Justitia som hjälper oss.

Det är inget konstigt med återhämtandet. Men sedan gäller det att se till att det inte händer igen. Det kan vi bara göra genom att i det här fallet utbilda myndigheterna. Vi tror inte att alla i dagsläget har kapacitet eller förmåga att göra det på egen hand. Vi hjälper till att köra den här processen hos myndigheterna så att de blir skickligare. På det sättet blir de bättre medborgare på Internet.

Ordföranden: Tack så mycket. Vi har gått igenom en dryg timme i rasande fart. Nu är det dags för en kaffepaus.

Kampanjen Surfa Lugnt – erfarenheter och utmaningar

Ordföranden: Nu går vi in på kampanjen Surfa Lugnt. Det ska handla om erfarenheter och utmaningar. Roland Ekström, som är projektledare, ska förmedla erfarenheter och utmaningar.

Roland Ekström, Kampanjen Surfa Lugnt: Tack för inbjudan att komma hit – det är trevligt! Surfa Lugnt-kampanjen, som den heter, har nu rullat i tre år. Vi startade i april 2005. De budskap vi har jobbat med i kampanjen har varit desamma hela tiden: Framför allt - använd nätet! Inse att det finns faror, och saker man kan göra för att skydda sig! Utgångspunkten för oss är hela tiden att ha balans i budskapet. Det är lätt att skrämma människor genom att tala om alla faror som finns. Samtidigt är det viktigt att vi bevarar nätets möjligheter för allas bästa och för allas möjligheter. Det är alltså balansen i budskapet som är vår stora utmaning.

Vi formulerar ofta det personliga ansvaret. Man har ett ansvar när man är på nätet, för man är en del av ett gemensamt trafiksystem. Det måste man tänka på när man agerar på nätet. Ett viktigt budskap är också sunt förnuft. Hur ser då sunt förnuft ut på nätet? Det är samma typ av sunt förnuft som finns i det vardagliga övriga livet. Detta är våra utgångspunkter.

De intressenter jag visar här på bilden är de som står bakom kampanjen. Det är en blandning av myndigheter, organisationer och företag. De är inte i första hand sponsorer eller finansiärer, utan de är medspelare i ett gemensamt arbete. Det är en viktig hållning i vårt arbete att för att detta ska kunna fungera över tiden måste vi inse att vi gör saker och ting tillsammans. Min roll som projektledare är inte att driva kampanj utan att samordna intressenternas insatser så att det blir vettiga svar på den rätt stora efterfrågan på kunskap och information som faktiskt finns.

Vem vänder vi oss till? Vi pratar om allmänheten – de som inte har några speciella kunskaper om hur nätet och datorer fungerar. Det är hemsurfare, småföretagare, föräldrar och unga. Vi har speciellt jobbat med de äldre – seniorerna. Vi har haft en stor ökning av användningen av nätet bland dem. Bland de äldre finns också en stor oro för vad som finns på nätet och vad som kan hända när man är där.

En annan grupp som hyser stor oro är föräldrar. Det går alltmer upp för föräldrar att de inte vet vad barnen gör på nätet. Vi försöker i sammanhanget att prata mycket om vuxenansvaret. Man har ett vuxenansvar för att ta reda på hur nätet fungerar, vad barnen faktiskt gör där och vilka problem de kan möta som de kanske inte är vuxna nog att kunna hantera.

Det är dessa vi vänder oss till – en bred grupp.

Vår verksamhet består av de saker jag visar på denna bild. Det har skapats mer av en idérörelse av människor ute i landet som tycker att det här med Internet och hur vi använder nätet är en viktig fråga. Vi har nu ett informatörsnätverk på drygt 2 000 människor runt omkring i landet. Till deras förfogande finns en webbplats med verktyg som successivt byggs ut med filmer, material och annat som man kan använda när man pratar om detta i skolan, på sin arbetsplats, bland äldre seniorer, på bibliotek, hos konsumentvägledare och annat.

Vi har hela tiden jobbat med en mycket handfast folder som vi inte skickar ut, utan försöker dela ut i olika sammanhang, till exempel på möten. Vi har under de här tre åren överlämnat ett ganska stort antal till ganska många människor.

En av de viktiga saker vi har i verksamheten är vår expertpanel. De är intressenternas bästa människor när det gäller kunskap om hur nätet fungerar och hur man skyddar sig på nätet. Vi svarar kontinuerligt på tusentals frågor från allmänheten. Vi har en rätt stor frågedatabas. Om det är något vi har nu efter tre år så är det bra koll på vad folk faktiskt inte vet. Det är en rätt stor spridning på det, och det är en ganska intressant kunskapsbas som vi kan titta på och se vad det är som folk egentligen undrar över. Ibland misstar man sig på var kunskapsnivån ligger i olika målgrupper.

Vi kör också regionala möten; det här är ingen Stockholmsföreteelse. Vi är årligen ute på rundturer i landet på flera olika ställen och har möten där vi samlar informatörer och intresserade människor. Det finns ganska många människor som är intresserade av de här frågeställningarna. De tycker att de vill engagera sig i att sprida kunskap vidare.

Vi kör också en årsdag. Nästa årsdag är den 16 april. Vi försöker att med hjälp av SVT få den inspelad och tv-sänd så att vi kan återanvända de intressanta diskussioner som förs under dagen på många sätt – via webben, ute på möten och annat.

Vad har vi då för erfarenheter? Om man pratar om att driva kampanj kan man säga att det här nog är en av de enklare man kan göra. Det finns ett oerhört positivt mottagande av de budskap som finns och när det gäller vikten av frågeställningarna. När vi började med Surfa Lugnt hade vi rätt mycket tekniska utgångspunkter. Det finns ett antal tekniska saker man kan göra för att skydda sig. Men vi har alltmer insett att man inte kan prata teknik med allmänheten. Man måste prata om teknik *och* användning. Det är först då tekniken får ett värde för folk. Vi har alltså rört oss erfarenhetsmässigt från teknik till teknik och användning.

Vi har en mångfald kontakter. Jag vill påstå att alla grupper och nästan alla åldrar vänder sig till oss eller till våra informatörer i olika sammanhang och vill veta mer. Det tycker jag är intressant. Jag kan inte säga att vi har tänkt ut hur det går till, men jag skulle tycka att det vore oerhört intressant om vi framöver kunde fundera på varför Surfa Lugnt har fått en sådan mångfaldsingång hos så väldigt många. Trots att vi har intressenter bakom oss som gärna lyfter fram att de finns med i olika sammanhang uppfattas vi som en objektiv kraft i informationsgivningen.

I dag kan man nog säga att vi har funnit ett uthålligt arbetssätt. Vi har inte jättestora resurser; det är mycket intressenternas egna insatser det handlar om. Men vi är uthålliga, och i dag är kampanjen egentligen mindre av kampanj och mer av process.

Vilka är våra utmaningar? Vi började för tre år sedan med att prata om varför man ska skydda sig på nätet. Det känns som en lite passerad fråga i dag. Nu handlar frågan mer om vad det är som är problemet och hur man gör. Surfa Lugnt kanske går från att vara en informationskampanj till att egentligen mer bli en utbildningssatsning.

Vi har ett antal utmaningar som vi bör fundera på nu. En är att vi inte har organisation och resurser för att driva utbildning. En annan är att utbildning för så här breda målgrupper är komplicerat. Vi rör oss med Internet över generationer. Hur man funderar som ungdom på nätets säkerhet är en helt annan utgångspunkt är hur man gör det som senior. Det gör att vi inte kan göra *ett* utbildningspaket, utan vi får göra många paket som tar hänsyn till att folk har tagit till sig nätet under de senaste decennierna på olika sätt. Nu kommer generationer som aldrig har upplevt något annat än nätet. Men vi har också stora grupper för vilka nätet är någonting ganska nytt fortfarande.

Vi har säkert också en del att göra bland våra intressenter när det gäller att skapa bättre användarvänlighet. Om man tittar på de frågeställningar och annat som vi möter till och från kan man säga att de produkter och andra tjänster som vi använder för att öka säkerheten inte är alldeles användarvänliga. Där har vi säkert en del att göra också när vi ska paketera utbildning och annat framöver.

Men för mig är den viktigaste utmaningen framöver att det inte längre räcker med att tala om att det finns problem. Vi måste också hjälpa folk mycket konkret med hur man fixar problemen.

Ordföranden: Tack så mycket! Det här är kanske den absolut svagaste länken i vårt informationssystem i ett säkerhetsperspektiv. Det handlar om nyfikenheten som gör att människor klickar på allt möjligt och omöjligt och att mana till eftertanke när man är ute och surfar.

Internetframsyn och IT-säkerhet

Ordföranden: Nu går vi vidare till dagens sista föreläsning. Den handlar om Internetframsyn – ett projekt inom IVA och IT-säkerhet som Östen Frånberg, som är projektledare, ska berätta om.

Östen Frånberg, Kungliga Ingenjörsvetenskapsakademien: Tack så mycket för att vi fick komma hit och prata om Internetframsyn! Jag heter Östen Frånberg och är projektledare på IVA, men också ordförande för Internet Society i Sverige.

Min presentation kommer att vara i två avsnitt. Jag ska måla med ganska breda perspektiv när det gäller vad projektet Internetframsyn har åstadkommit och sedan komma in på lite mer detaljer om IT-säkerhet.

IVA är en ingenjörsvetenskapsakademi – en av de äldsta i världen. De har som motto att vara till nytta för samhället och att främja tekniska och ekonomiska vetenskaper, näringsliv och utveckling.

Som ordförande Baylan sade inledningsvis handlar det om framtiden. Internetframsyn har alltså tittat in i denna framtid, närmare bestämt till år 2015. De mål som man har satt upp för projektet är att med utgångspunkt i dagens situation och stöd från forskning och utveckling som pågår ta fram åtgärder så att Sverige kan vara en framgångsrik Internetnation år 2015.

Projektet ska också prioritera ett antal förslag och peka på vilka personer eller organisationer som ska göra någonting med förslagen så att det går att realisera målbilden 2015. De som är tänkta att bli primära målgrupper är personer och organisationer inom näringslivet och inom offentlig sektor. Vi har också för avsikt att mäta i den sekundära målgruppen, det vill säga hos allmänheten, för att se om den här effekten har uppstått.

Ett så stort projekt som Internetframsyn, som har omfattat ett 50-tal personer, har alltså pågått under ett helt år. Vi har delat in projektet i tre olika pane-

ler. Det är en användarpanel som har tagit fram de krav som användarna kan tänkas ha år 2015 och ställt dem mot infrastrukturpanelen, som har haft till uppgift att försöka ta fram scenarier när det gäller om detta går att realisera. Det handlar om de kapaciteter och annat som kan krävas för framtidens videokonferenser. Kommer vi att ha sådana nät och den kvalitet på näten som vi behöver?

En panel – säkerhets- och juridikpanelen – är den som har arbetat med det ämne som jag ska komma tillbaka till lite mer i detalj. Det finns en tung rapport som kommer att levereras den 10 april. Jag kommer tillbaka lite närmare till det.

Jag visar här några av de områden som man behöver adressera för att bestämma hur Sverige kan bli en framstående Internetnation. Det första är en avancerad användning, men man måste också tänka på nyttoaspekten av användningen. I Sverige har vi hög användning inom företag, myndigheter och privatpersoner. Om vi gör en internationell mätning ligger vi bland de bästa länderna i det avseendet.

Om vi tittar på utnyttjandegrad i applikationer ser vi att Sverige är ett land med många applikationer. Vi har hört om den offentliga sektorn och myndighetsförvaltningen tidigare i dag. Alltmer av detta läggs på Internet.

Nästa block är tillgången till bredband och tjänster. Sverige är ett land med mycket kopparnät, som ni säkert läser om i tidningarna. Det finns ju problem med detta. Men vi har också en väl utbyggd industri och kunskap när det gäller radio och Internet över bredband. Vi har också fiber. De ökade kraven ställer krav på högre hastigheter, och där använder vi mycket av fiberteknologi.

Det finns en viktig sak när det gäller tjänster. En sådan här industri växer upp ur tekniken, så att säga. På det viset kan tjänsterna ofta bli lite isolerade på olika operatörer. Vi pratar om att försöka skapa en gemensam tjänstemarknad så att det ska vara möjligt att komma åt en tjänst. Man kan till exempel tänka sig att man ska kunna komma åt 3:s musiktjänst från Tele 2 eller från TDC. Så ser en framtid ut.

Sverige har många duktiga personer som är ledande i internationella verksamheter. Många av dem sitter här i salongen i dag, har jag sett. Men vi behöver stärka vårt avtryck internationellt, framför allt när det gäller tjänster. Vi har också en forsknings- och utvecklingsverksamhet i Sverige som man kan säga är lite spridd på många händer. Här tror vi att man ska stärka och samverka bättre och kanske specialisera sig på vissa områden inom vissa forskningsbegrepp för att kunna bli internationellt konkurrenskraftig.

Jag visar här resultatet av projektet Internetframsyn. Det är tio stycken fokuserade områden. Det första är ökad tillit till Internet. Jag kommer att prata lite mer om det i samband med de kommande bilderna. Nummer två är en gemensam öppen tjänstemarknad – en infrastruktur för framtidens Internettjänster. Vi måste också lära oss att utnyttja de möjligheter som skapas både inom företag och inom offentlig sektor. Offentlig sektor har mycket kunnande som andra länder inte har. Det skapar en möjlighet.

Vi måste också se till att vi får ett företagsvänligt klimat. Många små företag strävar och stretar med små möjligheter för att försöka konkurrera på den internationella marknaden. Här kan många svenska institutioner hjälpa till.

Vi har pratat om den digitala klyftan. Vi tycker att det känns destruktivt, och vill i stället prata om den digitala trappan där alla människor kan ta ett steg. Inget steg är för litet eller för obetydligt för den individ som tar det här steget. Vi vill gärna se att trappan leder till himlen. Den har alltså inget sista steg, utan man kan röra sig uppåt hela tiden.

Vi anser att vi måste få ett flexibelt arbetsliv – ett arbetsliv där man inte är bunden till ort eller till terminal utan flexibel. Begreppet arbeta hemifrån får alltså en större dimension. Man frånkopplar sig från den fysikaliteten.

Vi anser också att det finns mycket att göra här när det gäller skolan. Vi vill gärna se IT-baserad pedagogik på lärarnivå. Det gäller alltså lärarhögskolan och utbildningen av lärarna. Vi vill också se något som vi kallar för dataslöjd, precis som i syslöjd och metallslöjd. Där skulle man få lära sig sådant som: Hur är det att koppla ihop sina datorer? Vad är det för brandväggar? Hur fungerar det ena och det andra? Vi tror att det skulle vara ett viktigt grundämne för grundskolan.

När det gäller forskning, utveckling och innovationer har Sverige mycket resurser. Tyvärr är de lite spridda, så vi tror att en sammanfattning och en samling skulle vara viktig. När det gäller internationell profilering så är ju Internet internationellt. Vi måste lära oss och vi måste förstå att vi arbetar på en internationell marknad. Där måste vi synas och finnas.

Nu kommer jag till det andra avsnittet, som handlar om säkerhet och innovativitet. Internets framsyn har tagit fram en rapport per varje sådan här panel. Jag har här en kopia – en förhandsutgåva – från juridik- och säkerhetspanelen. Den som är ledare och ordförande för panelen finns här i salen. Det är Henrik Nilsson, som sitter här någonstans. Han kommer från advokatfirman Bird & Bird, och han har gjort det här arbetet.

Jag skulle vilja prata om den säkerhet som projektet har kommit fram till. Det är tre punkter som är viktiga. Den första är tillitsbegreppet. Användare, leverantörer, företag och myndigheter måste ta ett gemensamt ansvar för informationssäkerheten. Det ska naturligt vara så att den personliga integriteten ska ha ett adekvat skydd även i den elektroniska miljön. Den snabba utvecklingen av Internet ställer naturligtvis krav på att lagstiftningen hänger med. Vi hörde från KBM att man var fundersam över hur lagstiftningen fungerar visavi tiden och snabbheten på Internet. Vi gör samma analys. Vi anser att man bör göra en översyn av den straffrättsliga och civilrättsliga lagen.

Jag ska nu komma till en mycket konkret sak. När det gäller att bekämpa IT-brottsligheten tycker vi att man bör pröva idén att se det på liknande sätt som miljöbrott och ekonomiska brott. Man bör försöka inrätta en liknande funktion.

Punkt två är att man behöver ha en välspridd acceptans när det gäller e-identiteter. Vi tycker att Finansdepartementet och Näringsdepartementet bör ge ansvariga myndigheter i uppdrag att driva den färdplan för e-legitimitet

som redan är på gång hos Verva. Jag såg Vervas representant för tekniken som bänkgranne med mig här. Slutligen tycker vi att e-legitimiteten ska vara plattforms- och terminaloberoende. Den ska finnas både på laptop och på mobiltelefoner, naturligtvis.

Den tredje punkten är en generell kvalitetsguide för Internetförbindelser. Ni vet alla att man får upp till 8 megabit, upp till 16 megabit och så vidare. Här tycker vi att branschen bör ta ansvar för att specificera Internetförbindelserna och att Konsument- och telerådgivningsbyrån tillsammans med marknadens parter, PTS och konsumenter och andra aktörer ska arbeta för en sådan specifikation.

Tillit och tillgänglighet går hand i hand; visst är det så. Tillit till Internet är en förutsättning för att användarna ska känna sig tillfredsställda. Tjänstetillhandahållare och användare har ett gemensamt ansvar för att säkra funktionaliteten. Här tycker vi att SLA – Service Level Agreement – som är vanligt mellan företag och Internetleverantörer också ska användas för privatpersoner och kanske också på andra ställen. Då får man en tydligare roll mellan leverantör och konsument.

Vi har hört mycket om kriget på Internet. Vi upplever att det kommer att fortsätta. Vi har ju hört många som har pratat om det ämnet i dag. Attackerna kommer att vara organiserade av grupper som kommer att använda detta för utpressning, terrorattacker och annat. Vi gör samma analys som den vi hörde om här tidigare under förmiddagen. Vi ser också att spam, virus och *spyware* kommer att fortsätta. Men de motmedel som vi har, som jag vet att Surfa Lugnt så förtjänstfullt går ut och berättar om, kommer också att finnas. Krigföringen kommer att fortsätta oberoende av terminal. Den kommer att flytta in även i mobilvärlden så småningom.

Min fjärde punkt är mycket konkret. Den som har arbetat med det här, Christina Jonsson, finns också i lokalen. Det handlar om informationssäkerhet. Informationssäkerheten bidrar till skydd mot förvanskning av information som hotar den personliga integriteten. KBM pratade mycket om det här området. Det finns faktiskt ett resultat. Det är gjort av Susex – The Swedish University Information Security Group. Den finns inom Sunet, det statliga universitetsnätet. De har tagit fram en handbok i IT-säkerhet. Länken finns längst ned här. Jag skulle vilja säga till alla myndigheter: Titta på den och dra lärdom av den! Det är ett färdigt resultat och material. Det är uppdaterat, och författaren finns här i lokalen. Det är bara att använda det.

Till sist vill jag berätta lite mer om Internetframsyn. Det finns en broschyr som ligger i ett antal exemplar vid utgången av salen här. Vi har en slutkonferens den 10 april – nästa torsdag – mellan klockan 13 och 16. Det går fortfarande att anmäla sig. Vi har över 150 anmälningar, och det finns fortfarande utrymme kvar i Wallenbergssalen, där vi kommer att hålla till. Det går bra att anmäla sig på IVAs hemsida. Den rapport som jag höll upp kommer tillsammans med ett antal andra att finns tillgängliga då.

De som har varit med och hjälpt oss i arbetet är elva stycken medfinansiärer och medarbetare. Ni ser dem på bilden jag visar här. Jag vill tacka dem officiellt för allt det arbete som de har gjort med oss och för oss under året.

Ordföranden: Tack ska du ha! Där fick du med lite reklam på slutet; det var driftigt gjort.

Frågestund

Ordföranden: Vi övergår nu till en frågestund där ledamöterna har möjlighet att ställa frågor. Jag ber om korta koncisa frågor och, om möjligt, även korta koncisa svar.

Désirée Liljevall (s): Herr ordförande! Tack, alla föreläsare, för intressanta föredragningar! Inom två år ska alla svenskar som vill kunna få en e-legitimation, e-ID. Det har Verva med flera lagt fram förslag om. Vi hörde precis Östen Frånberg från IVA nämna det också. Målet är att e-legitimationen ska kunna användas med olika typer av teknik oberoende av utgivare inom statens ramverk.

E-ID används redan i dag av flera svenska myndigheter vid kommunikation med till exempel kommunerna. Myndigheterna har dock hittills inte lyckats enas om en enda lösning. Vissa myndigheter kräver att den kommunala tjänstemannen identifierar sig med e-ID vid översändning av viktiga handlingar. Andra hänvisar till en hemsida med en särskild inloggning. Ytterligare några tycker att det går lika bra att skicka handlingarna med budbil eller att tjänstemannen själv traskar i väg med sin portfölj till myndigheten.

Det känns inte bra att de statliga myndigheterna använder sig av olika lösningar för identifikation, framför allt inte säkerhetsmässigt. Min fråga är främst riktad till representanterna för PTS och IVA, men även .SE. Hur kan myndigheterna kraftsamla och komma fram till en gemensam lösning för att nå de mål om elektronisk identifikation som Verva har satt upp?

Anders Johanson, Post- och telestyrelsen: Det här är inte PTS verksamhetsområde annat än att vi förstås liksom alla myndigheter har anledning att ha identifikationssystem av våra intressenter. Det är Verva som jobbar med de här frågorna.

Ingvar Hellqvist, Krisberedskapsmyndigheten: I handlingsplanen är ett förslag att man ska skynda på och ett annat att KBM tillsammans med FoU ska göra en studie och en granskning av vad som är tekniskt genomförbart. Det är alltså omnämnt där.

Östen Frånberg, Kungliga Ingenjörsvetenskapsakademien: Inom IVA har Verva varit den organisation som har arbetat med frågan. Wiggo Öberg som sitter här bakom mig har alltså arbetat med detta, och jag skulle vilja lämna över ordet till honom.

Wiggo Öberg, Verva: Jag jobbar alltså med e-legitimationsfrågorna på Verva. E-legitimation har en ganska lång historia i Sverige. Vi har haft nuvarande situation i ungefär sju år. Syftet var från allra första början att skapa ett enhetligt sätt för myndigheterna att identifiera medborgare mot offentliga tjänster. Man kan tycka många saker om detta – att det har gått för långsamt och så vidare. Det finns många skäl till det, och tiden räcker inte till för att gå in på detta i dag.

Men vi kommer nu i mitten på juni att lägga fram ett antal alternativa förslag till hur det här kan fortsätta i en riktning som vi alla kan tycka är acceptabel. Vi vill också skapa en likriktning för området och en friare användning som kan liknas vid att man använder en fysisk legitimation, som vi gör i vardagslivet. Det ska kunna fungera på motsvarande sätt för en elektronisk dito. Det är vår ambition, och det är vad vi jobbar för. Vi ser goda möjligheter att lyckas med det, men vi behöver naturligtvis ert stöd som politiker i de här frågorna för att driva på utvecklingen i rätt riktning.

Ordföranden: Du kan känna det massiva stödet här just nu, och det kommer säkert mer sedan.

Eliza Roszkowska Öberg (m): Jag har en fråga i samband med en proposition från Försvarsdepartementet där man föreslår att en ny myndighet ska bildas för att driva samhällets krisberedskap.

Hur kommer IT-säkerhetsarbetet att fördelas i framtiden? Hur kommer vardagssäkerheten att hanteras, och av vem? Med vardagssäkerhet menar jag den IT-säkerhet som inte rör allvarliga krissituationer eller omfattande IT-attacker.

Jag skulle vilja höra kommentarer från Ingvar Hellqvist från KBM, Stefan B. Grinneby från Sitic och Patrik Fältström från Näringsdepartementets IT-råd.

Ingvar Hellquist, Krisberedskapsmyndigheten: Propositionen säger att den nya myndigheten har ett informationssäkerhetsansvar att hålla samman arbetet. Det finns också direktiv utgivna för tillkomsten av den nya myndigheten som också adresserar frågan. Där kan man se att vi har ett samordningsansvar för informationssäkerhetsfrågor i kris i den nya myndigheten.

Som jag sade i mitt föredrag tidigare är normalbilden den som kan eskalera till en krissituation. Det återstår lite arbete för att se hur rollen ska se ut i vardagstillvaron och när den övergår i en kris, vilket är ett svårdefinierat

tillstånd. Just när det gäller den problematiken mellan vardagsverksamheten och krisverksamheten återstår nog lite arbete att göra.

Stefan B. Grinneby, Sitic: Sedan Sitics verksamhet startade har vi sett att det finns en ganska stor villighet hos myndigheter och andra organisationer att ta till sig informationssäkerhetstänkande och informationssäkerhetsarbete. Vi har stött på väldigt positiva reaktioner med den ökade utåtriktade verksamhet som vi har bedrivit under den senaste tiden.

Jag tror att det vi kommer att göra framgent är att öka samarbetet med myndigheterna och lära dem att bli duktigare på att hantera sin egen säkerhet. De måste göra det själva, för det finns ingen annan som har tillräcklig god insyn i hur verksamheten fungerar för att kunna göra det utifrån. Men, som Ingvar säger, det är naturligtvis bra om någon på ett övergripande plan håller samman det som behöver uppnås, men exakt hur det ska göras måste var och en bestämma själv. Det är då den bästa effekten finns att hämta.

Vi kommer att fortsätta att jobba med att utbilda myndigheterna och erbjuda dem den praktiska hjälp de behöver och hjälpa dem att göra det de inte kan göra själva, det vill säga ha internationella kontakter med liknande organisation som Sitic till exempel. Det är någonting som är väldigt bra att vi gör.

Patrik Fältström, Cisco: Jag sitter som ledamot i IT-rådet, men jag representerar inte Näringsdepartementet på något sätt. Jag är anställd på Cisco.

Den första reaktionen är att jag helt och hållet håller med Eliza. Det är en sak som jag blev förvirrad av här under morgonen, och det är att folk blandar ihop den vardagliga säkerheten med den säkerhet och robusthet som behövs när det verkligen händer någonting. Det var tillräckligt oklart i föredragen här i morse för att göra mig lite orolig för att de som håller på med säkerhet inte riktigt själva kan skilja på de här olika sakerna. Jag undrar också hur det ligger till här egentligen.

Som en extern part som inte jobbar på någon av myndigheterna spelar det ingen roll för mig eller för privat sektor vilken myndighet som har ansvar för de olika funktionerna utan bara att det är välbestämt vem det är som har hand om det och att det delade ansvar som vi har i Sverige med ansvarsprincipen hålls kvar.

När man ser de här presentationerna verkar det som om det är lite oklart mellan myndigheterna vem som gör vad, till exempel mellan KBM och PTS om man hårddrar det lite grann. Det är inte bra. Det skapar lite oro hos alla oss här som delar på ansvaret att se till att Internet fungerar både i offentlig och i privat sektor.

När det gäller själva krishanteringen, när det väl händer någonting, är det otroligt viktigt att veta vad som är viktigt. Den absolut första bilden vi såg här var från FRA som sade att riksdag och regering var ett av de viktigaste områdena. Jag undrar hur mycket av Sverige som slutar att fungera om folk inte kommer i kontakt med riksdag och regering en dag eller två. Jag tror att det

kommer att funka rätt bra ändå. Vi utanför bryr oss inte om vem som gör saker, men vi vill inte ha något krig mellan de olika myndigheterna.

Jag har ytterligare ett exempel från Estland. I Estland hade man bestämt sig för vilka tjänster som var samhällsviktiga, och då menar jag verkligen viktiga. De hade plockat ut två saker. Det första var att medborgarna fortfarande kommer åt pengar av landets valuta, det vill säga att bankomaterna fungerar. Det förhindrar att folk börjar handla med stenar eller trycka egna pengar, och det är rätt viktigt för att behålla ett land som ett land.

Den andra saken som var viktig där är att medborgarna kan kommunicera med varandra, inte medborgare till myndigheter, inte myndigheter till medborgare.

Den typen av prioritering skulle jag vilja se att vi tillsammans gör i Sverige. Bara genom att bestämma sig för två sådana viktiga saker blir det implikationer på att det måste finnas elförsörjning och alla möjliga andra saker. Men i dag vet vi inte vad som är viktigt, och det måste vi enas om.

Sven Bergström (c): Herr ordförande! Jag har frågor som snuddar vid dem som redan har ställts. Flera föredragshållare betonade att samhället är helt beroende av nätet och av att e-kommunikationen fungerar, och så har vi hört exempel på att det finns lägen då det inte fungerar. Estland var ett, och bombning av hemsidor och annat har vi också hört talas om, bland annat i Regeringskansliet.

Tidigare fanns det också uppgifter om oro för att nätet skulle sprängas på grund av mängden information. Även om vi har fiberoptiska kablar är nätet inte dimensionerat för den oerhört snabbt växande informationsmängden. Hur ser till exempel Anne-Marie Eklund-Löwinder på detta? Finns det några sådana risker över huvud taget? Det är den ena frågan.

Den andra är om vi ändå inte håller på att gå baklänges när det gäller säkerheten. Förut fanns det en rad av varandra oberoende informationssystem i ett hushåll. Vi hade telefon som inte var beroende av elektricitet. Vi hade radio och tv och så vidare. Nu håller vi på att slussa in all information via dator. Vi tittar på tv och lyssnar på radio via dator. Är vi inte mer sårbara? Hur kommer det att funka i ett läge när vi inte har en transistorradio som går på batterier, utan vi är helt beroende av att datorn funkar, om elen havererar eller nätet går ned? Är vi inte i ett lite sämre läge för hushåll och bostäder om vi gör oss så här ensidigt beroende av ett enda system?

Anne-Marie Eklund-Löwinder, Stiftelsen för Internetinfrastruktur: Låt mig börja bakifrån. Visst blir vi sårbarare om man har en typ av kommunikationskanal som bärare för ett stort antal tjänster som samtidigt är beroende av en löpande elförsörjning. Precis som med allting annat finns det möjligheter att åtgärda det, men då måste man också fundera på hur det ska gå till att få ut elkraft i bostadsområden. En väldigt enkel sak som vi spekulerade i på den tiden jag jobbade på IT-kommissionen var att låta någon dela ut mobiltelefon

till alla i huset när elen har gått för att man åtminstone ska kunna upprätthålla kommunikationen mellan varandra.

Vilken var den första frågan? Jag tappade tråden.

Sven Bergström (c): Finns det någon risk för att nätet sprängs av den snabbt växande informationen?

Anne-Marie Eklund-Löwinder, Stiftelsen för Internetinfrastruktur: Tack och lov är inte de här nollorna och ettorna så fysiskt påtagliga. Det som händer är att det går trögare. Det går långsamt. Det kan naturligtvis också innebära att den viktiga trafiken blir lidande av en massa skräp när den verkligen behövs. Därför är det också viktigt att vi prioriterar vad det är som är viktigt, så att man vet vad man ska strypa och vad man ska hjälpa till med när det behövs.

Kurt Erik Lindqvist, Netnod Internet Exchange: Låt mig bara tillägga något till det här med trafikökning. Vi ser i dag en hel del av den trafik som går mellan operatörerna som vi hanterar. Det finns ett visst beroende i det här. Den trafik man skickar genererar också intäkter som återinvesteras för att se till att kapaciteten ökar. Det är inte så att trafiken bara ökar och mängden peng in inte ökar. Den ramlar inte ned från himlen, utan den kommer faktiskt av användandet. Det säkerställer på något sätt att det här systemet klarar av att skala för och hantera den trafikökning vi ser, och den har varit enorm de senaste åren.

Anne-Marie pratade om att prioritera det. Det är ofta en fråga för ändsystemen. Operatörernas nät skalar för det här, men frågan är om myndigheternas nät klarar av att hantera stora trafikökningar vid extraordinära händelser eller huruvida man kan få fram trafiken till slutsystemet, till medborgarna. Det är där det finns risk för flaskhalsar och problem med prioritering.

Ordföranden: Man skulle kanske kunna lägga till en sak när det gäller det som Sven Bergström frågade om när det gäller att alltmer sker via datorn. Vi har också ett trafiksystem som ska bli alltmer IT-intelligent. Vad innebär detta?

Anders Johanson, Post- och telestyrelsen: Sven Bergströms fråga om beroenden är väldigt viktig. Men jag kan påminna om att även förr i världen när Televerket hade sin telefoni krävde det också elektricitet, men man lade omfattande resurser på att det skulle fungera i alla lägen. I dag när komplexiteten och beroendet är ännu större är elförsörjningen fundamental för väldigt mycket i samhället och för all elektronisk kommunikation. Det finns olika sätt att angripa det här. Företagen som säljer kommunikationstjänster har ett grundläggande kommersiellt intresse av att det ska fungera mot sina kunder, men samtidigt kan de inte gardera sig mot vilka stora katastrofer som helst.

Där finns till exempel de här robusthetsmedlen från staten som PTS hanterar och kan stärka upp. Men det finns mycket större behov än vad det finns medel för att stärka det här.

Men det finns ett par andra sätt också att gå, och ett är att kunderna ställer större krav gentemot sin leverantör och till exempel frågar vad som händer vid ett elavbrott. Hur klarar sig det här kommunikationssystemet då? Där finns det mycket mer att göra. Det är en upplysning till företag och andra som till exempel vill ha ip-telefoni så att de förstår att sådana frågor ska ställas.

En annan motverkande sak är att det finns många alternativa kommunikationskanaler i dag. Det kan många gånger vara så att om den ena kommunikationsformen, till exempel en mobiltelefonioperatör, är utslagen kan det finnas andra som är i gång. Det är någonting som vi var och en kan gardera oss lite mot. Jag har själv till exempel inte bara ett SIM-kort. Jag har också ett extra SIM-kort i min telefon för att klara mig om min vanliga leverantör inte fungerar. Det är en enkel liten vardagsåtgärd.

Ordföranden: Sedan kan man naturligtvis fråga sig om det är en sådan katastrof att vi inte alltid är tillgängliga och inte alltid kan se på tv och inte alltid kan prata med någon annan just nu. Det känns ju så ibland, men det kanske inte är det egentligen.

Annelie Enochson (kd): När jag för en tid sedan läste de förträffliga böckerna av Stieg Larsson om Lisbeth Salander trodde jag att detta var bara *fiction*. Sedan började jag inse att det här är nog verklighet. Jag tycker att detta är ett väldigt svårt område. När vår IT-chef för ett tag sedan kom till oss i de olika partierna och berättade om säkerheten här blev vi något rädda när vi såg hur lätt det var att komma in i våra system. Vi hörde detta om oskyddad dator, 30 minuter och allt.

När jag lyssnar här tycker jag att det borde vara så att nyckelordet är långsiktighet och framtidsseende. Vi har hört de olika myndigheterna prata om handlingsplaner och så vidare. Jag funderar på vad vi som beslutsfattare konkret kan göra. Vad är det som måste göras? Vad är ert budskap om första prioritet till oss som beslutsfattare? Jag vill rikta frågan till tre personer. Till Kurt Erik Lindqvist på Netnord, Östen Frånberg på IVA och Patrik Fältström som är här som ledamot i IT-rådet.

Kurt Erik Lindqvist, Netnod Internet Exchange: Mycket av det som har sagts, om man tittar på KBM:s tidsplan som jag läste igenom snabbt i går, är ju inte helt nya idéer. Det är ingenting som är föreslaget för första gången. Det vore trevligt om man kunde se de här förslagen genomförda någon gång snarare än föreslagna på nytt. Mycket av det som Anne-Marie talade om är också väldigt lågt hängande frukt som man tycker bara borde vara att göra. Jag tror att riksdagen bör ställa högre krav på myndigheterna att genomföra detta och ställa krav på regeringen att inte bara återkomma och säga att man har en plan

och en fin, vacker rapport till. Man borde faktiskt komma tillbaka och presentera utförda åtgärder.

Sedan tror jag att det är viktigt att man understryker det som har sagts flera gånger förut, nämligen att det måste finnas en långsiktighet i det här arbetet. Det måste finnas en säkerhet där vi i det privata näringslivet eller externa aktörer känner att det finns en långsiktighet som kommer att fortgå. Det måste vara samma myndigheter och samma personer hos myndigheterna som har en finansiering över en lång tid. De här projekten får inte stå och falla med nästa val eller med nästa trendvind på något sätt. Det måste finnas långsiktighet. Det är frågor som det tar väldigt lång tid att bygga upp kunskap och kännedom om.

Östen Frånberg, Kungliga Ingenjörsvetenskapsakademien: Jag har ett antal förslag till konkreta åtgärder. Projektet Internetframsyn kommer att övergå i en realiseringsfas, byta namn och heta Ambient Sweden från och med april i år, om några veckor alltså. Då skulle vi gärna vilja få kontakter med er som är riksdagsledamöter för att diskutera de förslag som vi har och hur de kan anpassas så att de passar beslutsmekanismen och de organ som ni sedan vill berätta vad som ska göras för. Det här realiseringsprojektet kommer som sagt att ha sin planeringsfas under april och maj, och vi skulle gärna vilja få den här kontakten. Det är det långsiktiga arbetet.

Det mer kortsiktiga, väldigt konkreta arbetet gäller informationssäkerhet. Det finns en statlig myndighet som har gjort ett bra arbete på det här området. Det är universitetsnätet Sunet på KTH som har gjort det arbetet. Det arbetet kan man ta och lämna vidare och låta andra myndigheter implementera. Man kan läsa den här handboken, kopiera det och införa det. Det är ett väldigt bra arbete. Det är uppdaterat och en mycket stor handbok.

Det är det långsiktiga förslaget och det väldigt konkreta, kortsiktiga förslaget.

Patrik Fältström, Cisco: Jag vill nämna tre saker väldigt kort. För det första: Bestäm vilka tjänster och vilka funktioner i landet som verkligen är viktiga! Det tycker jag är en väldigt bra diskussion. Se till att det bestäms.

För det andra: Ställ krav på myndigheter, precis som Kurt Erik Lindqvist sade, att de faktiskt gör någonting. De måste också förklara hur det matchar det som ni har bestämt är viktiga tjänster och funktioner i samhället.

För det tredje: Se till att myndigheterna direkt, de myndigheter som har ansvar för att de här funktionerna fungerar, får pengar i stället för att det ska bli potentiellt tjafs med att myndigheterna ska ge varandra pengar.

John Daniels, Försvarsmakten: Jag heter John Daniels och är chef för militära säkerhetstjänsten i Försvarsmakten. Jag skulle vilja ta upp två saker. Den ena är hur vårt sätt att använda begreppet IT-incidenter bär lite grann hur vi tänker. 95 procent av de IT-incidenter vi har pratat om här i dag är egentligen

rena brott som alla återfinns i brottsbalkens olika kapitel. Men vi har pratat väldigt lite om brottsbekämpningsförmågan här i dag. Jag tror inte att det är någon här i salen som kommer från någon brottsbekämpande myndighet, från Justitiedepartementet eller liknande.

De flesta av de här brotten är gränsöverskridande, och i många fall är det grovt organiserade kriminella som ligger bakom. De bör också mötas av bättre förmåga hos polisen och rättsvårdande myndigheter att hantera de här brotten. Om ni kommer hem i kväll eller på fredag och har haft inbrott i bostaden ringer ni självklart till polisen, men jag tror inte att ni ringer om ni har haft intrång i er dator och blivit av med pengar eller liknande, och ringer ni kommer ni sannolikt inte att få speciellt mycket hjälp när det gäller intrånget i datorn. Har ni däremot haft inbrott i bostaden lär ni få hjälp av polisen.

Det andra som jag också vill ta upp är mer explicit min hemmaarena. Underrättelseverksamheten jobbar naturligtvis också på det här området. Man brukar säga att underrättelsetjänst är *The trade of all tricks*, och det här är ett av de trick som man nu lägger till sin arsenal. Alla de stora underrättelsetjänsterna jobbar med IT-intrång. Det är helt självklart. Jag vill trycka på att det är ett hot som är väldigt konkret, och de är väldigt duktiga i många fall. Det drabbar myndigheter, regering, riksdag och liknande.

Peter Pedersen (v): Om man är född på 50-talet och uppväxt med skrivmaskin och blyertspenna känner man sig som en immigrant i den digitala världen. När vi diskuterar olika saker: säkerhetsfrågor, brott på Internet, pornografi och så vidare, är det precis som om Internet skulle vara en egen värld. Fildelning är ett annat exempel. Jag tycker att det var befriande att representanten från Must säger att vi ska betrakta det som all annan verksamhet och bekämpa det. Vi skulle till exempel aldrig acceptera att någon lånade vår bil då och då eller att man flyttade in i vårt hus, kapar vårt hus, och bor där ett antal veckor under sommaren.

Det har vidtagits åtgärder. I dag är det i princip omöjligt att stjäla en bil om man inte stjäl nyckeln. Det går inte att bryta upp dörren och ta en ny bil i besittning. Men när det gäller datasäkerhet känns det som om tonvikten väldigt mycket ligger på att jag som användare ska se till att det fungerar. Om jag skaffar antispionprogram, brandväggar och virusprogram ska jag ändå tänka mig för hur jag agerar på nätet, får man höra. Vad innebär det konkret? Hur mycket ansvar ligger egentligen på användaren? Kan man förvänta sig att Internetoperatörerna ska ha ett högre säkerhetskrav och kunna säga att man, när man levererar en tjänst, ska ha mycket större säkerhet och att om du använder just deras tjänst minimerar man risken för dataintrång, att någon kapar din dator och så vidare?

Hur ser ni på relationen mellan användare och den som tilldelar en tjänst, till exempel teleoperatören och bredbandsbolagen, när det gäller ansvaret? Hur ser ansvarsfördelningen ut? Är det *fifty–fifty* eller ligger huvudansvaret på användarna? Man kan nästan få intrycket att det är det senare, vilket jag tycker är mycket märkligt i så fall.

Vi skulle heller aldrig acceptera att 90 procent av all trafik gick ut på att någon åker omkring med en bil med lite reklam på taket för att djäklas med de andra trafikanterna och göra reklam för olika varor. Så ser det i princip ut på nätet. Om jag har förstått er rätt är en majoritet av informationen på nätet spam. Det kan vara felaktigt, men väldigt mycket är åtminstone spam. Varför accepterar vi det på nätet men inte i den vanliga trafiken?

Anne-Marie Eklund-Löwinder, Stiftelsen för Internetinfrastruktur: Detta är ett spännande område. Jag delar din uppfattning till 100 procent när det gäller detta att varför är det alltid användaren som sitter med Svarte Petter just nu. Sedan blev det lite fel på slutet. Jag tror personligen att det är mycket svårt att ställa det kravet på Internetoperatörerna. De är bara taxichaufförerna i det här sammanhanget. Det är på biltillverkaren, alltså programvarutillverkarna, de som har innehållstjänster, de som vill förmedla någonting till användarna på nätet och de som har en utrustning som används för det, som kraven behöver ställas. Det är de som måste se till att det fungerar från början så att användarna kan andas ut lite och inte behöver känna sig osäkra på om bilen har tre eller fyra hjul, om det finns någon ratt eller om bromsarna funkar som de ska.

Ingvar Hellquist, Krisberedskapsmyndigheten: Jag tycker att du har helt rätt. Komplexiteten i det här och gällande lagstiftning gör att det är svårt att veta vad det får för konsekvenser. Om vi tar en dator hos en enskild användare som utgör grunden för en attack, finns det då ett oaktsamhetsbrott hos den som låter sitt verktyg åstadkomma stor skada för någon annan? Nej, det finns det inte. Egentligen är den enskilda användaren helt oskyldig. I ett längre perspektiv kanske det är just därifrån de största förlusterna och attackerna kommer att komma. Kan man alltså fortsätta att ha en sådan här oskyldighetsaspekt från dem som är verktyget i attackerna? Och hur ska i sådana fall en lagstiftning kunna hantera en sådan fråga? Den är inte lättlöst.

Just nu tycker jag att föremålet som utför attacken har en väldigt liten skuld i det här ärendet – de borde kanske ha mera – tack vare sin okunskap. Då måste man komma till rätta med okunskapen, och den kommer man kanske inte till rätta med bara genom lagstiftning. Det är en samhällsangelägenhet att ha en kompetensutveckling i hela kedjan, som jag sade förut.

Kurt Erik Lindqvist, Netnod Internet Exchange: Det är farligt att fortsätta på analogier, men det är inte så att du förväntar dig att Vägverket på något sätt ska bekämpa brottslingar som ska stjäla din bil. Orsaken till att du har ett så bra låssystem på din bil är att du har märkt att bilen blev stulen. Det är ganska uppenbart. Biltillverkarna har utvecklat väldigt effektiva låssystem därför att de som köpte bilar ställde krav på det och började köpa bilar som hade bättre lås.

Jag håller helt med både dig och Anne-Marie att användare i dag förväntas ta ett väldigt stort, kanske lite väl stort, ansvar. Men det är nästan ingen av de

här användarna som ställer krav på sin biltillverkare att göra låsen bättre i dag. De är nästan obefintliga, och till viss del är det så att den stackars användaren inte vet om att han har sin bil stulen. Han sitter glatt där och tror att bilen står på parkeringsplatsen eller att datorn fortsätter att fungera eftersom han inte har märkt det. Den kanske går lite långsamt, så att det är dags att köpa en ny. Jag förstod inte riktigt om det var det som Ingvar menade, att man skulle lagstifta till brottslighet. Det finns väldigt många andra dumheter man kunde lagstifta mot också, men det är väldigt svårt att lagstifta mot okunskap och dumhet.

Nyckeln till det här är att ställa mer krav på att de som levererar systemen till en användare levererar säkra system, och de kraven måste komma från slutanvändaren, inte från någon annan.

Anders Johanson, Post- och telestyrelsen: Många undersökningar visar precis det som Peter Pedersen säger, att det är svårt för användare och småföretagare att använda Internet på ett bra sätt och utveckla sin verksamhet. Man litar inte riktigt på det, och man vet inte riktigt hur man gör. Varför är det så? Det är en väldigt snabb utveckling i branschen. Det är en i många stycken omogen bransch.

Men jag tycker ändå att man ser positiva tecken, till exempel tillhandahåller den största Internetleverantören, Telia Sonera, men också andra, flera tjänster, och i de tjänsterna ingår det skyddsfunktioner som antivirusprogram och brandvägg, så att man inte lika mycket som förr själv måste tänka på att köpa detta och installera. Det är ett steg i rätt riktning. Jag tror att det framöver kommer att bli mer så att man kommer att sälja inte bara enkel användning utan också en säker användning. Men det återstår att se, för det är samtidigt en snabb teknikutveckling.

Men hur mycket till exempel leverantörssidan än tillhandahåller det här är det precis som med bilarna. Även om det finns säkerhetsbälten, och till och med lagstiftning om att det ska finnas, ankommer det på den som sitter i bilen att använda säkerhetsbältet. Det är vi alla vana vid i dag och vet hur man gör, men i den här världen är det inte riktigt lika enkelt för användaren. Jag tror att kunskapsbehovet kommer att finnas, också om tio år, även om skyddsmekanismerna är mycket bättre.

Per Hellqvist, Symantec: Jag heter Per Hellqvist och arbetar på Symantec. Vi är leverantörer av IT-säkerhetstjänster och sådant. Du frågar vad man kan göra när det gäller ansvar. Det finns två ställen man kan rikta sökarljuset mot, dels orsaken, dels verkan. Man brukar säga att datasäkerhet och IT-säkerhet börjar hos klienterna. Det är faktiskt på slutanvändardatorerna, alltså våra hemdatorer, som mycket av problemen börjar. Man använder i dag hemdatorer som man har kapat genom att lura användaren att klicka på olika saker eller automatiskt installera olika typer av elak kod på deras maskiner. Sedan använder man de maskinerna till exempel i överbelastningsattackerna som vi

såg mot Estland eller för att skicka spam. Du har rätt där. Det är ungefär 80–90 procent av all e-post som skickas som är spam, alltså elektronisk reklam.

Antingen kan vi rikta in oss på att titta på hur vi ska hjälpa slutanvändarna att känna igen varningstecknen och hur de ska surfa lugnare genom till exempel Surfa Lugnt-kampanjen. Det arbetet börjar redan i skolan. Hur uppför man sig på nätet? Vilka varningstecken ska jag se upp med? Vad jag förstår finns det i dag inte en schemalagd timme centralt sett som går ut på det här. Man lär sig hantera datorn men inte de otäcka sidorna på Internet. Det kan handla om cyberbrottslingar eller olika typer av upphovsrättsbrott.

Det enda då är att rikta in strålkastarna på dem som orsakar problemen, alltså själva brottslingarna.

Som vi har pratat om lite grann tidigare är det oerhört starka ekonomiska intressen som ligger bakom. Vi pratar egentligen om maffialiknande organisationer. I dag tjänar man så mycket pengar på Internetbrottsligheten att man i princip startar bolag. Man har heltidsanställd personal som sitter och skriver virus, maskar och trojaner och som sedan utför själva attacken. Man kan i dag specialbeställa trojaner för att attackera vissa myndigheter, bolag, banker eller vad man nu vill. Då ingår support och uppdateringar.

Vi måste se till att de rättsvårdande myndigheterna har de resurser som finns och framför allt verka för att främja ett internationellt samarbete. För när svenska poliser ringer sina ryska kolleger och säger att vi har en kille på Nevski Prospekt 43 som ligger bakom kraftfulla attacker mot svenska banker – är ni snälla och plockar honom åt oss – svarar den ryska kollegan tillbaka: Är du inte klok? Vi har folk som skjuter på varandra på gatan med maskingevär, och du vill att vi ska plocka upp någon dataputte. Är du vänlig och återkommer?

Man följer spåren mellan länderna. Sådant samarbete måste underlättas. I dag kan man sitta och se Ryssland kapa datorer i Sydafrika och sedan attackera en bokhandlare i Miami eller var som helst. Vilka lagar är det som gäller? Och hur ska vi hjälpa polisen att följa spåren tillbaka?

Albin Zuccato, Telia Sonera: Jag vill bara ge några kommentarer till att operatörerna ska ta allt ansvar eller ett större ansvar. Jag tror att operatörerna i dag redan tar sitt ansvar. Man erbjuder säkerhetstjänster. Det är kunden som måste välja att köpa de tjänsterna. Det kan man inte göra gratis. Vi måste satsa på utbildningen.

När vi jämför med bilen har staten kommit in och gjort föreskrifter om hur bilens säkerhet ska se ut. Det finns grundskyddsföreskrifter för att man ska kunna lansera en bil. Det kommer att behövas likadant för datorerna. Varför kan man sälja en dator i Sverige som är helt öppen? Det skulle man kunna fundera lite över, inte bara snacka om basskyddet för myndigheter utan att det ska finnas ett basskydd inbyggt i de datorer som säljs.

Erland Jonsson, Chalmers: Jag tycker att Peter Pedersen sätter fingret på en väldigt viktig fråga. Man kan fråga sig varför det är på det här sättet. Min uppfattning är att IT-infrastrukturen inte har designats med någon säkerhet i sikte. Den är osäker. Ingen har gjort den så. Den har blivit det på något sätt. Problemet är att den fortsätter att vara det. Det är fortfarande ingen som leder den här utvecklingen.

Om man skulle leda utvecklingen och göra en bra design av något skulle man naturligtvis se till att så lite ansvar som möjligt ligger på användaren och så mycket som möjligt ligger inbyggt i systemet. Man kan konstatera att det redan nu finns massor av grejer som är kända sedan 20–30 år tillbaka när det gäller hur man ska designa de system som inte finns där. Det är inte kommersiellt attraktivt. Det är massa olika anledningar till att de inte finns där. Det är en fundamental fråga som man skulle kunna fundera på hur man ska adressera och hur man ska kunna göra det.

Henrik Rasmusson, City åklagarkammare i Stockholm: Till skillnad från vad John Daniels trodde finns det faktiskt en representant från rättsväsendet här. Jag har sysslat lite med IT-brottslighet de senaste åren och i vart fall kommit i kontakt med en del av de problem som vi drabbas av. Det verkar finnas en allmän uppfattning om att det är någon sorts laglöst land på Internet och att det är okej. Det är en del av funktionen att man ska kunna vara lite hemlig, kunna göra småbrottslighet utan att man drabbas.

Jag tror inte att riksdagen helt kan frånta sig ansvaret för det. Man har faktiskt satt in en integritetsspärr i lagen om elektronisk kommunikation som tillåter i princip alla bötesbrott fritt på Internet. Det ska man vara medveten om. Det är något som man också har i sin hand att reglera om man vill ändra på det.

Om inte polis eller åklagare som är ansvarig för ett anmält brott bedömer att brottet ger annat än böter får vi inte leta efter gärningsmannen. Det är alltså fritt fram att begå olaga hot, vissa typer av angrepp, spamattacker och liknande, förtal, förolämpning, den typen av brottslighet. Det är fritt fram att göra det på Internet i dag, för vi får inte fråga operatörerna vem som har gjort attacken. Vi kan hitta en ip-adress, men vi kan inte hitta abonnenten.

Min tolkning är att man har bedömt att kommunikationsnät ska ha ett särskilt skydd. Man har inte samma skydd när man begår brott i verkliga livet. Stjäl man en bil har man rätt att söka spår i verkligheten, men om man begår brott på Internet har man begränsat möjligheten för oss att söka spår. Det kan man fundera på.

Jag ska också säga någonting om internationaliseringen på det här området. Det är ett jätteproblem för polis och åklagare att brotten på Internet inte begås på en plats. Vi är fortfarande tyvärr organiserade så att det är regionala brottsbekämpningar i huvudsak i landet. Man bekämpar brottsligheten inom sin region. Det må vara en mindre stad eller ett större län, men det är fortfarande inom regionen. Under sådana här IT-utredningar hoppar man fram mellan regionerna när man följer spåren, om man nu kan följa spåren. Då

bollas man också mellan olika polismyndigheter, mellan olika åklagarmyndigheter, mellan olika domstolar, ibland mellan nationer.

Där måste man, tycker jag, ta ett motsvarande grepp som man nyligen har inlett på materialrättens område med nationella funktioner, i vart fall nationella, på längre sikt kanske internationella. Samma polis, samma åklagare ska kunna arbeta med samma brott, oavsett var det slutligen har begåtts, var gärningsmannen slutligen finns. Det var några synpunkter.

Ordföranden: Det är naturligtvis alltid en avvägning. Nu pratar vi om bekymren, men de här verktygen ger också enorma möjligheter. Det är den avvägning som vi ofta står inför.

Ska vi slutligen som svar på denna fråga låta världens största mjukvarutillverkare få ordet.

Magnus Lindkvist, Microsoft AB: Jag jobbar som säkerhetsrådgivare på Microsoft, har gjort det i fem år ungefär. Det är en väldigt utmanande uppgift och framför allt väldigt rolig. Jag tror att temat för det här är att det går väldigt fort med Internet och utvecklingen av datorer. Man brukar prata om hundår. Sju hundår är ett människoår. Ett dataår är kanske 150 år helt plötsligt. Vi sitter alltså i en utveckling där vi har ett plan som flyger något fantastiskt fort som vi samtidigt byter alla motorer på och försöker lista ut vad vi ska göra med det.

Jag vet inte hur många här inne som är föräldrar och som kan känna att barnen är ganska duktiga på datorer men att man själv inte har riktigt koll på vad som händer. Det är en del av den situation vi sitter i. Jag brukar säga att jag kan gå i en affär i dag, jag kan plocka upp en korg, jag kan handla min mat, jag kan gå ut och betala. Varför fungerar det så bra? Jo, för att någon har visat mig det här tidigare. Det finns en fungerande process. Men i dag vet vi inte riktigt hur processen är. Vad ska vi göra med datorerna? Vad håller era barn på med egentligen? Och vad gör de i morgon? Det är något helt nytt med vad de gör i dag. Vi utvecklar nya programvaror som gör nya fantastiska saker med datorerna, och det här går extremt fort.

Anne-Marie pratade lite tidigare om att det finns krav för att ansluta till Internet och vad man ska göra. Det är möjligt, men jag skulle hävda att det är lite som att gå mot röd gubbe. Det må vara olagligt, men det finns ingen påföljd direkt. Jag är ganska anonym. Jag kan göra väldigt mycket saker, och det är väldigt liten risk att jag råkar illa ut. Som Pelle sade är det det här som brottsligheten älskar. Det här är verkligen en bra grogrund, för lagens arm har väldigt svårt att nå fram. Om jag hoppar via olika länder till exempel måste det samarbetas, och då blir det ännu mer komplicerat.

Vi har pratat om olika banker som har råkat illa ut och säkerhetssystemen där. De exempel som vi har är där vi har använt engångskoder och användarna har blivit duperade att lämna ifrån sig dem. Det har inte varit något problem i de tekniska systemen, utan jag har helt enkelt lämnat ifrån mig koderna

frivilligt för jag trodde att det var banken som frågade efter dem. Är det mitt ansvar som kund att jag inte ska lämna ifrån mig de här koderna? Är det leverantören som har gjort ett konstigt IT-system? Eller är det banken som har gjort ett konstigt system där det är för lätt att lämna ifrån sig koderna? Frågan blir komplex där också.

I dag sitter många användare med förlegade system anslutna till Internet som inte stöds av leverantören längre. Det finns egentligen ingen påföljd för mig om jag inte håller min dator i fräscht skick. Jag kan bli kapad och datorn går lite segt, men herregud, det är ju Windows, det går ju alltid lite segt. Vad ska jag göra åt det? Det finns de som verkligen vill göra något åt det, och så finns det de som startar om datorn.

Ordföranden: Jag kan också säga att det går ned i åldrarna. Min lille son som då var 17 månader lyckades vända uppochned på min skärmbild. Det var ett någorlunda lustigt samtal som jag hade med supporten på riksdagen, kan man säga. Så kan det gå.

Christer Winbäck (fp): Kurt Erik Lindqvist nämnde att terrorism alltid finns men att det här bara är ett annat verktyg. Jag tycker att ”bara” andas lite aningslöshet. Vi vet ju alla att det är betydligt enklare, billigare och större spridning, och det finns många andra saker som gör att just cyberbrott är så pass framgångsrika, om man nu ska kalla det så för vad det är i dag. Det är det som är ett av de stora problemen här i dag. Var ligger då ansvarsgränserna?

Om vi ska fortsätta med trafikjämförelser har vi i dag bilar som går på våra vägar. För att bilarna ska gå på vägarna finns det ackrediteringsinstitut som ska godkänna dem. Vi har Svensk Bilprovning, oaktat hur det är organiserat, som ska se till att bilarna håller sig i trim. Det handlar om ett ansvar hos användaren men också hos leverantörerna. Vi ska komma ihåg att de krav som finns vad gäller säkerhet i bilar inte kommer från användarna i regel. Det är prestanda och lullull som användarna som köper bilarna vill ha. Kraven på säkerhet, säkerhetsbälte och Sips och Mips och allt vad det heter kommer faktiskt från myndigheter, försäkringsbolag och andra som har en insikt i vad det här innebär. Det innebär då också att vi måste se till att ställa krav, inte bara på datortillverkare, mjukvarutillverkare och dem som använder det utan även på dem som levererar tjänster av olika slag.

Vi fick höra av Anne-Marie Eklund-Löwinder att vad gäller namnservrar är det stora brister i detta. 23 procent har så allvarliga fel att de i princip borde stängas av, om jag förstod det rätt, och 64 procent hade allvarliga brister. Jag tycker att det här ett stort problem. Frågan är om man ska ha någon form av ackreditering för att över huvud taget få minimisäkerhetsnivåer för att kunna få erbjuda tjänster så att vi åtminstone där kan spärra en del av de här besvärliga sakerna.

Det andra som jag ville fråga om som är väldigt viktigt, och där får jag väl hålla med Peter Pedersen, är hur mycket man ska ställa krav på våra användare. Att lära dem från barnsben och att pö om pö få större kunskap är naturligtvis jättebra. Men vi har också bekymmer. Jag ska återge vad Viiveke Fåk sade häromåret i samband med lösenord och annat – apropå att svära i kyrkan: Vi har väldigt många nycklar, och vi förstår inte alltid hur allvarligt det är att släppa in obehöriga. Vad gäller fysiska nycklar har vi ett fåtal, men vi har ett otal lösenord, pinkoder och annat. Nycklarna byter vi sällan ut, men många lösenord måste bytas flera gånger om året.

Det är klart att man ska ställa krav på användare, men vi blir äldre. Jag vet inte hur många kort och koder jag har. Till slut håller man inte ordning på det. Det innebär att man slarvar. Man skriver upp, och ni vet allt det där. Det är också ett bekymmer. Jag vet att branschen arbetar med att se till att man får någon form av *sign-on* och så vidare. Men hur ska man göra för att få det här bra? Hur går det arbetet? Jag tycker också att det är en viktig fråga. Jag hade de två frågorna.

Anne-Marie Eklund-Löwinder, Stiftelsen för Internetinfrastruktur: Vi ska vara medvetna om att det här är en kommersiell marknad och att kravställningen är viktig. Där har staten en roll, inte som lagstiftare och tillsynsansvarig utan framför allt som stor kund och användare. Om jag går in på Onoff och säger åt dem att jag tycker att de ska ge mig en bättre dator så kastar de ut mig antagligen. Men om jag har ett behov av hundratusentals datorer varje år och ställer krav på dem på ett relevant sätt har jag mycket större konsumentkraft som kommer oss andra till godo i förlängningen.

Jag tycker, precis som du, att användar-ID och lösenord är en gammal teknik. Vi ska försöka komma bort från den. Det finns flera olika alternativ. Jag tror inte att vi ska sikta in oss på ett enda. Det är samma sak där. Låt marknaden ta fram bra lösningar! Kravställ och anpassa efter de behov som finns! Så kommer vi att få jättebra lösningar på den marknaden också.

Per Hellqvist, Symantec: Det var flera bottnar i din fråga. Jag spårade in lite grann på cyberterrorism och sådant. Visst finns det spår på cyberterrorism, och visst finns det intressenter som är sugna på att göra både det ena och det andra. Visst går det. Dock är min personliga uppfattning att terroristers mål är att få maximal uppmärksamhet. Det får man faktiskt fortfarande genom att spränga bussar och tåg. Det är blod och saker som gör sig bra i tv. Slocknade webbplatser och sådana saker gör sig inte lika bra i tv.

Däremot måste vi förstå vilka system som är viktiga. Jag föreslår att ni lyssnar på Patriks råd sedan tidigare. Det handlar om att ni ska bestämma er för vad som verkligen är viktigt att skydda och sedan fokusera uppfattningen om hur de ska skyddas och lägga medel och metoder för att skydda dem.

Kurt-Erik Lindqvist, Netnod Internet Exchange: Jag vill inte på något sätt försöka spela ned hotet från cyberterrorismen, men det blir som Per säger och som jag också sade. Det här är attacker som är väldigt billiga att producera, men det är också väldigt liten utväxling. Det kanske är dyrare att producera brinnande byggnader, men utväxlingen är väldigt mycket högre i tv-tid.

Mats Berglind (s): Det är flera som har varit inne på hur viktigt det är att myndigheterna samverkar i de här frågorna. Om vi skulle råka ut för en sådan attack som den i Estland i dag, vilken myndighet är det då som har huvudansvaret för att samverkan kommer i gång och att rätt åtgärder vidtas?

Ingvar Hellquist, Krisberedskapsmyndigheten: Jag var lite grann inne på det när jag hade min redovisning om den rapport vi skrev om incidenterna i Estland. Jag pekade på att om samma sak, inte på samma sätt utan kanske med en större kapacitet, hade inriktat sig mot Sverige hade vi inte haft de möjligheterna att ha en gemensam lägesbild. Vi hade därmed också haft svårt att utnyttja vår responskapacitet som nu Sitic representerar. Man måste ju veta var man ska sätta in åtgärderna. Har man inte en sådan lägesbild blir det svårt. Det internationella samarbete som kan komma att behövas på en nivå över det teleoperatörerna gör, där andra saker är inblandade hade inte heller etablerats. Vi hade inte klarat den lika bra.

Däremot är kapaciteten i Sverige och det svenska Internet avsevärt mycket större än i Estland. Så man ska inte dra den slutsatsen att den estländska attacken hade påverkat oss, för det hade vi kanske inte ens märkt. Och teleoperatörer och andra är skickliga på det här. Men vi saknar en övergripande lägesbild och en möjlighet att samordna som det ser ut just nu, och det finns inget utpekat sådant ansvar. Förvaltningsmodellen där var och en gör så gott den kan inom sitt område är alltså inte rätt medicin för den här typen av attacker.

Kurt Erik Lindqvist, Netnod Internet Exchange: De svenska teleoperatörerna har ju ett väldigt väl fungerande samarbete med internationella aktörer för att bekämpa den här typen av attacker. Skulle en liknande men som Ingvar säger en i sådana fall väldigt mycket större attack ske i Sverige, mot myndigheter framför allt kanske, är det myndigheternas operatörer som i första rummet skulle tvingas att arbeta med attacken. Det är sådant man gör varje dag. Det var även många svenska operatörer som var med och hjälpte Estland. Eftersom mycket av trafiken till Estland passerar Sverige var de med och bekämpade attacken. Det här är inget som är unikt eller på något sätt svårt att hantera. Det här ingår i daglig drift i dag.

Däremot är det kanske ur någon sorts myndighetsövergripande aspekt oklart vem som har ansvar för det här. Det finns ingen myndighet som vill gripa in och bekämpa det. Det måste teleoperatörerna göra, och det gör de i dag.

Staffan Danielsson (c): Det är en mycket intressant diskussion. Jag vill anknyta till den fråga som Peter Pedersen ställde, som är central i sammanhanget här, och till inlägg från Post- och telestyrelsen. Man sade att samhället är helt beroende av att e-kommunikationen fungerar. Minskad robusthet skapar mer kriser, och robuståtgärderna minskar ty konkurrensen ökar. Det är beroende på att utvecklingen går så fort, som Microsoft sade här.

Men det är det vi måste hantera. Användaren har ett ansvar. Det är självklart om vi tar bilexemplet. Men branschen har ett starkt ansvar för hur datorerna ska vara utrustade och se ut så att de säljer. Vilken praxis, vilka standarder jobbar man fram i detta snabba tempo?

Sedan är frågan vad staten ska kunna hinna med att göra i form av hur det ska se ut – de här kraven ställer vi på datorer som säljs så att de inte står nakna och kan utnyttjas för attacker. Det är egentligen min fråga. Det bästa är att konkurrensen fungerar, att branschen tar sitt ansvar och att den hänger med. Hänger branschen med? Vad behöver staten möjligen tillföra? Hur ser ni på ansvaret där?

Anders Johanson, Post- och telestyrelsen: Operatörerna har ju ett kommersiellt intresse av att det fungerar för kunderna. Ju större tryck från kunderna, till exempel i avtal från stora kunder att det ska fungera, desto större intresse också från operatör att leverera enligt det. Men vi ser tydligt att det är en tuff och hård konkurrens och att många operatörer inte sköter det här bra. Från PTS kan vi om vi i vår tillsyn kommer fram till att man inte uppfyller lagens grundläggande krav utdöma ett vite eller ytterst avstänga dem från verksamhet. Det sista är rätt så hypotetiskt.

Men det är väldigt olika incitament. Läget är väldigt olika. Just nu håller vi på med en tillsyn över 55 operatörer som ska vara klar senare under våren. Då ska vi se dagsläget.

Utöver detta har vi, som har nämnts här, riktigt samhällskritiska och samhällsviktiga verksamheter där man inte rimligen kan begära att operatörerna ska kunna gardera mot till exempel rejäl terrorism eller svåra oväder, stormar eller värre. Då har det funnits ända sedan televerkstiden och finns fortfarande i dag robusthetspengar från stat och via avgifter från operatörerna. De minskar nu, vilket oroar oss. Vi ser att investeringar i robusthet minskar totalt sett, relativt utveckling och sådant.

Magnus Lindkvist, Microsoft: Den dator som vi pratade om innan är ett fantastiskt verktyg. Man kan göra så otroligt många olika saker med den. Vi skulle kunna låsa ned den maskinen så att man inte kunde råka illa ut, men det finns ingen som skulle köpa den datorn, kan jag säga. Alla vill kunna göra vad de vill med sin dator, och tålamodet när det gäller att klicka på något är väl nere på en halv sekund eller en sekund. När blir ni själva frustrerade när ni inte får svar?

Det klickas vilt, måste jag säga. Jag lutade mig tillbaka till Pelle och frågade: Hur många användare råkar illa ut på grund av att man bara råkar slå på sin dator och ansluta den till Internet i dag? Tar du en modern dator har den väldigt robusta och gedigna säkerhetsfunktioner inbyggda. Vi tog en siffra som vi inte kan backa upp med några fakta men en känsla. Det är att 80 procent av de användare som råkar illa ut gör det på grund av att de själva har valt att ta emot en fil eller klicka på något på en webbsida som verkar intressant eller är något de vill ha. Det går inte att hindra en användare att vara nyfiken, och det vill vi definitivt inte göra.

Gitte Bergknut, Eon Sverige: Vi har snuddat vid det ett par gånger här under dagen men det har inte riktigt kommit fram, det ömsesidiga beroendet som finns och den stora sårbarheten i samhället. Vi har hamnat, tycker jag, på en ganska detaljerad nivå om vem som bär ansvar när det gäller enskilda datorer. Visst, det kan man hålla på och prata om ganska länge. Men vi kanske har missat en av de större problemställningarna som vi har åtminstone i min bransch, energibranschen. Det är att våra system är sårbara. Våra leverantörer erkänner att de system som de levererar till oss är sårbara. Vi är beroende av Internet för att vi ska kunna leverera el till den här salen. Där har vi ett väldigt stort samhällsproblem.

Det vi egentligen efterlyser från er som sitter som beslutsfattare och kravställare är: Vad är det för minimikrav som olika samhällsviktiga funktioner ska leva upp till? Det gäller leveranssäkerheten som många politiker pratar om men också informationssäkerhet. Jag har jättestora problem när jag ska prata med min ledning. De förstår inte varför jag vill att vi ska lägga flera miljoner på att säkra upp vår miljö när inte grannenergibolaget gör det. Det behövs mer helhetsgrepp och att olika myndigheter inom olika sektorer tar med informations- och IT-säkerhetskrav när de ställer sin kravbild. Det är inte en fråga för en enskild separat myndighet. Det är en verksamhetsfråga.

Irene Oskarsson (kd): Det är oerhört mycket intressant som redan har berörts. Jag känner att det sista inlägget också tangerar det som från början var min fråga. Men det finns en punkt som flera av er har tangerat och sagt är viktig. Då kan man få en följdfråga utifrån att hastigheten går med 150 år om året. Det gäller utbildningsfrågan, kompetensfrågan. Vi har berört att vi som gick ut naturvetenskaplig linje för 20 år sedan drygt, som jag själv gjorde, utan att ha sett en dator i dag lever i en datavärld. Det är den allmänna kunskapen hos oss vardagsanvändare. Men hur ser kunskapsnivån ut? Vad är det som behövs på utbildningsområdet för att klara av att möta hoten? Har vi tillräckligt på utbildningsområdet i de här frågorna? Eller behöver vi göra mer där? Jag vet inte om Anne-Marie är den som är mest lämpad att svara.

Ordföranden: Jag skulle kunna svara på den frågan. Svaret är nej förstås.

Anne-Marie Eklund-Löwinder, Stiftelsen för Internetinfrastruktur: Precis vad jag tänkte säga. Det är ett mycket kort svar: Nej.

Ordföranden: Det här är en väldigt stor fråga. Jag kan som före detta skolminister säga att jag mötte den väldigt ofta. Jag ser att det finns vissa skolor som har kommit längre och andra kortare. Jag tror att det finns väldigt mycket mer att göra här. Jag tror att vi får nöja oss med det som svar.

Jag får tacka er.

Avslutning

Rolf Gunnarsson (m): Först av allt vill jag tacka alla medverkande i dagens öppna utfrågning om IT-säkerhet.

Hur kan man då sammanfatta en sådan här förmiddag? Det har varit en bra och lärorik utfrågning. Den har gjort mig trygg – till viss del – men, för att citera en domare i *Let's dance*, ju mer man gräver i detta ämne, ju mer man lär sig om dessa frågor och ju mer man försöker förstå frågorna, desto mer rädd blir man, rädd för hur lite vi egentligen vet och hur sårbara vi är på detta område. Man skulle efter dagens utfrågning lätt kunna klappa sig för bröstet och låtsas att vi nu klarat av problemen med IT-säkerhet och att vi inte behöver lägga mer krut på det. Så kan man självklart inte resonera, vilket jag tror att alla politiker och riksdagskolleger som är här håller med mig om.

Jag har fått klart för mig, och jag tror som sagt inte att jag är ensam om det, att detta är något stort och svårt och sådant som vi ständigt måste ha med oss i vårt arbete. Man blev inte precis tryggare av att någon liknade det hela vid ett skenande flygplan. Det gjorde mig inte tryggare.

Dagens utfrågning har gett oss många svar. Dagens utfrågning har varit värdefull. Det är en viktig pusselbit i det fortsatta arbetet i riksdagen och något som vi måste ha med oss i många olika sammanhang. Jag tror att samtliga utskott är berörda av dessa frågor.

Vi vet att det hänger många kvalificerade IT-hot över oss. I försvarsutskottet hade vi en genomgång förra veckan, och där upplevde vi samma sak. När genomgången var klar så inte var man gladare och kände sig säkrare när man gick därifrån. I stället var man betydligt mer oroad över vad som finns att göra.

När vi får ett USB-minne av någon som vi besökt petar vi stolt in den i vår dator och kör i gång. Men vi vet inte vad vi fått på köpet, om jag uttrycker mig så.

Många är berörda av IT. Många har också tillgång till våra datorer. Jag skulle kunna räkna upp en rad kategorier människor som har tillgång till och kunde gå in i min dator, men jag tänker inte göra det. Det finns, som sagt, stor anledning för oss politiker – vilket togs upp i slutet av hearingen – att fortsätta att arbeta med dessa frågor, vara observanta och lyhörda samt ta till oss det som måste göras på detta område. Jag tror till och med att vi kan nå stor enig-

het i IT-frågorna. Jag tror inte att den politiska skiljelinjen är särskilt bred vad gäller dem.

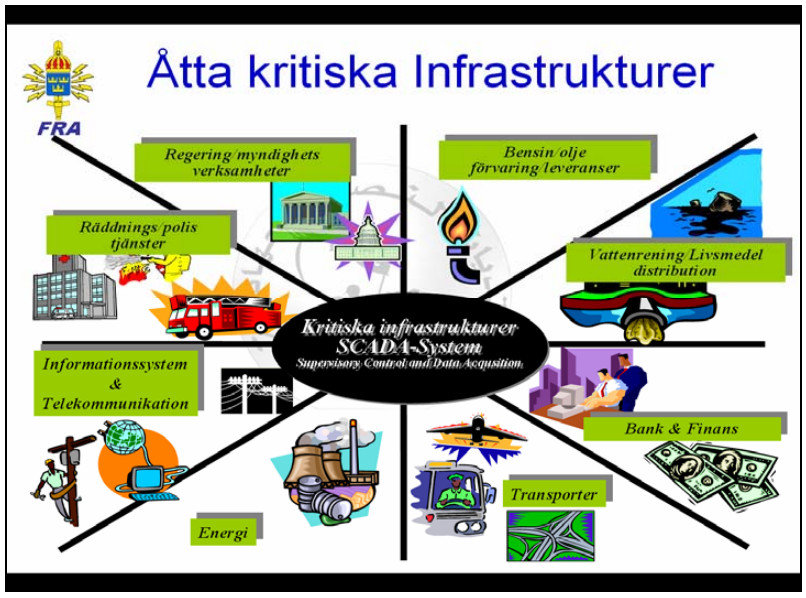
Med dessa ord vill jag än en gång tacka allesammans och förklara denna utfrågning avslutad.

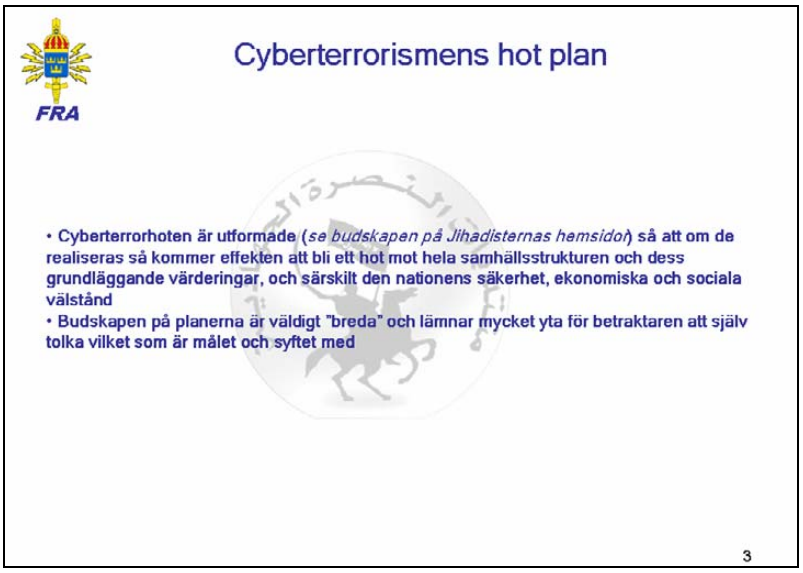
(Applåder)

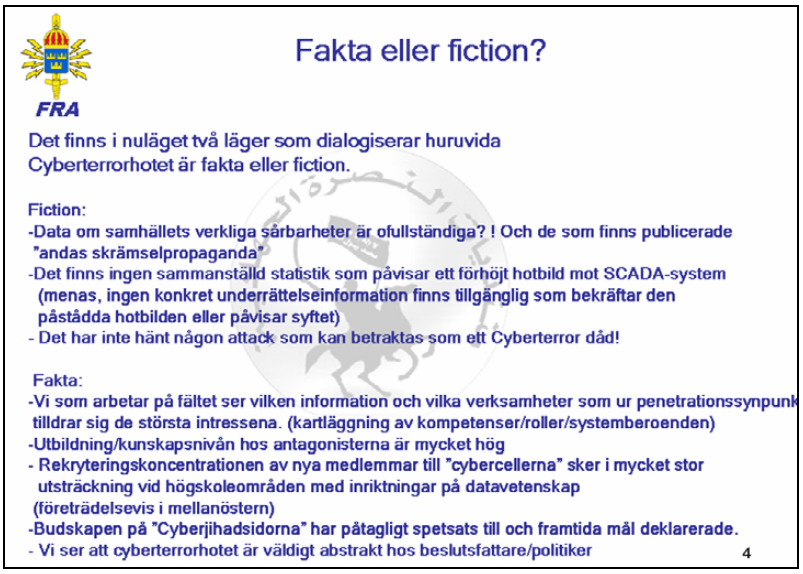
BILAGA

Bilder från utfrågningen

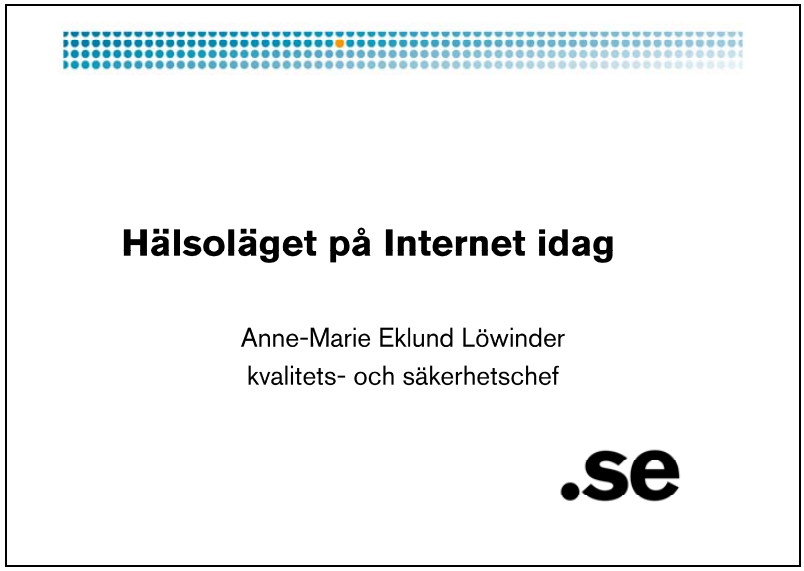
Bilder som visades av Dan Larsson, Försvarets radioanstalt, under hans presentation vid den offentliga utfrågningen om IT-säkerhet.

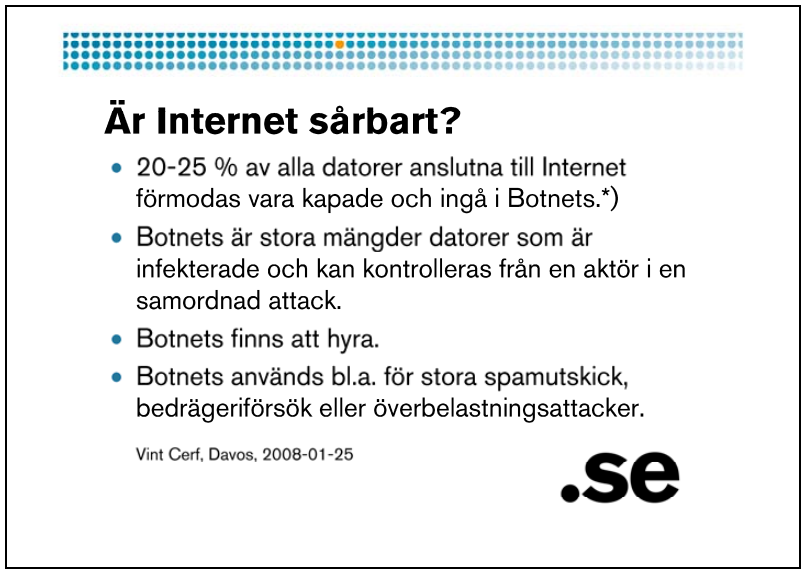



FRA
Cyberterrorismens hot plan
• Cyberterrorhoten är utformade (*se budskapen på Jihadisternas hemsidor*) så att om de realiseras så kommer effekten att bli ett hot mot hela samhällsstrukturen och dess grundläggande värderingar, och särskilt den nationens säkerhet, ekonomiska och sociala välstånd
• Budskapen på planerna är väldigt "breda" och lämnar mycket yta för betraktaren att själv tolka vilket som är målet och syftet med
3

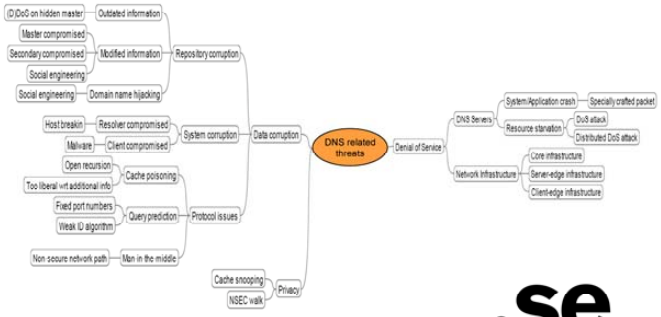

FRA
Fakta eller fiction?
Det finns i nuläget två läger som dialogiserar huruvida Cyberterrorhotet är fakta eller fiction.
Fiction:
-Data om samhällets verkliga sårbarheter är ofullständiga? ! Och de som finns publicerade "andas skrämselpropaganda"
-Det finns ingen sammanställd statistik som påvisar ett förhöjt hotbild mot SCADA-system (menas, ingen konkret underrättelseinformation finns tillgänglig som bekräftar den påstådda hotbilden eller påvisar syftet)
- Det har inte hänt någon attack som kan betraktas som ett Cyberterror dåd!
Fakta:
-Vi som arbetar på fältet ser vilken information och vilka verksamheter som ur penetrationssynpunk tilldrar sig de största intressena. (kartläggning av kompetenser/roller/systemberoenden)
-Utbildning/kunskapsnivån hos antagonisterna är mycket hög
- Rekryteringskoncentrationen av nya medlemmar till "cybercellerna" sker i mycket stor utsträckning vid högskoleområden med inriktningar på datavetenskap (företrädelsevis i mellanöstern)
-Budskapen på "Cyberjihadsidorna" har påtagligt spetsats till och framtida mål deklarerade.
- Vi ser att cyberterrorhotet är väldigt abstrakt hos beslutsfattare/politiker
4

Bilder som visades av Anne-Marie Eklund-Löwinder, Stiftelsen för Internet-infrastruktur, under hennes presentation vid den offentliga utfrågningen om IT-säkerhet.





Hot mot domännamnssystemet



.se

Undersökning av .SE 2007

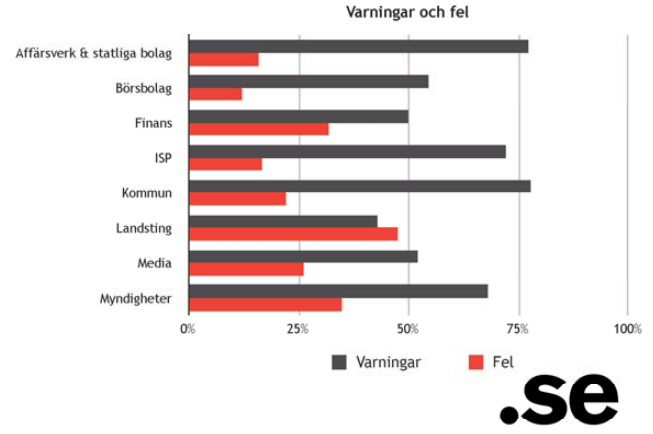
- Hur hanterar verksamheter sin DNS?
- Hur hanterar verksamheter sin e-post?
- Hur ansluter verksamheter sin webb till Internet?
- Undersökningen omfattade affärsdrivande verk och statliga bolag (49), ett antal av de största börsnoterade bolagen i Sverige (66), banker och finansbolag (22), Internetoperatörer (18), kommuner (290), landsting (21), mediaföretag (23), statliga myndigheter inkl länsstyrelser, exkl. myndigheter under Riksdagen (339).
- Totalt 828 domäner och 1043 namnservrar.

.se

Resultat – tester av DNS

- Av 828 testade domäner hade
  - 23 % allvarliga fel.
  - 64 % brister av en karaktär som genererar varning.
- Definition av fel och varningar
  - Fel = bör åtgärdas för att verksamheten ska förvissa sig om god tillgänglighet och nåbarhet till DNS och andra resurser.
  - Varningar = är fel som kan påverka driften, men åtgärder bedöms inte vara lika akuta, även om de skulle höja kvaliteten.

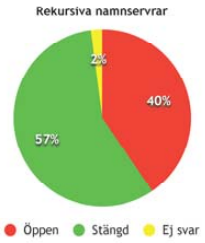
.se



.se

Öppna rekursiva namnservrar

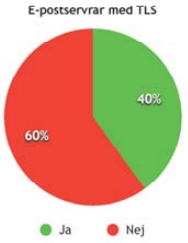
- Har få legitima användningsområden.
- Gör det möjligt för utomstående att utföra tillgänglighetsattacker mot andra via den öppna namnservern.
- Grundproblemet är att operatörer inte filtrerar på avsändaradress. Kan missbrukas och bör elimineras.



.se

Viktiga parametrar för e-post

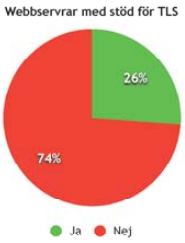
- Saknar stöd för transportskydd av e-post: 60 % saknar skydd, oklart om det är aktiverat hos resterande 40 %.
- Placering: 16 % e-postservrar i utlandet.
- Skydd mot falskt angivande av domännamn i avsändaradressen: 16 %.



.se

Viktiga parametrar för webb

- Saknar stöd för transportskydd av webb: 74 %, hos de 26 % som har skydd är det i många fall undermåligt infört.
- Microsoft IIS dominerande programvara (59 %).

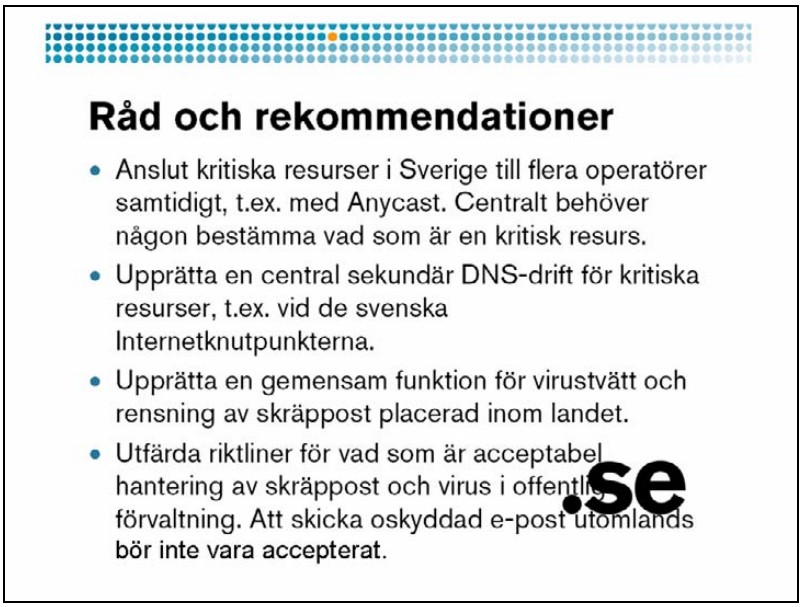


.se

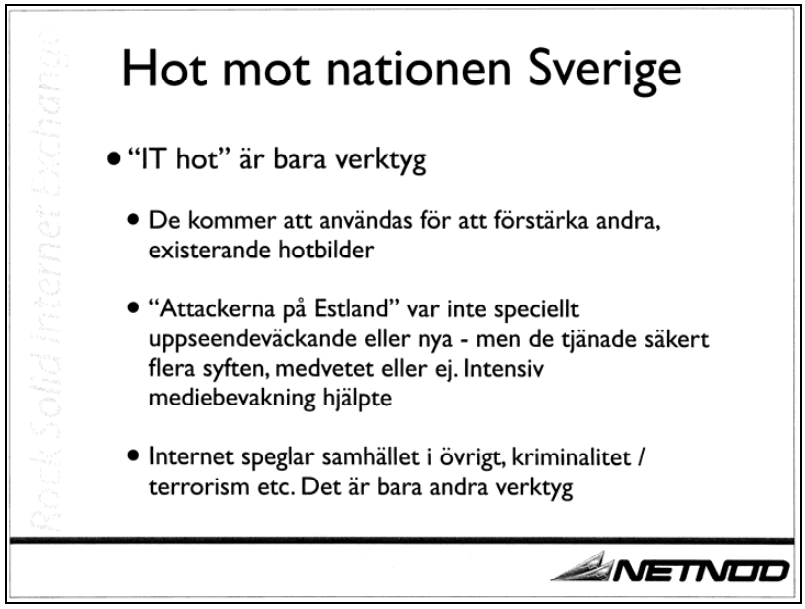
Behöver vi förbereda oss för attacker?

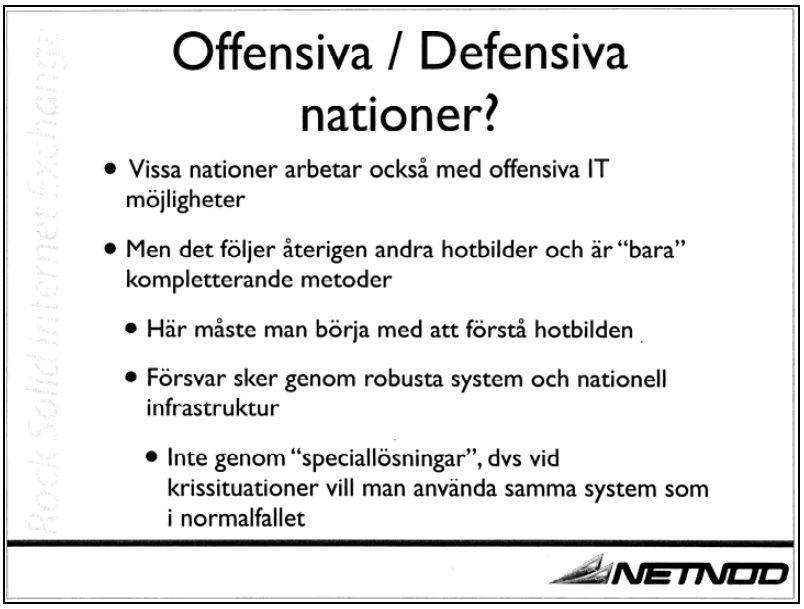
- Allmänna kommunikationsnät är och förblir en viktig del i samhällets hantering av allvarliga händelser, svåra påfrestningar och beredskapssituationer.
- Nationella och internationella händelser under de senaste åren visar tydligt på vikten av robusta kommunikationer.
- Det är viktigt att utveckla samarbetet mellan myndigheter och i dialog med operatörer och leverantörer, nationellt såväl som internationellt.
- Arbetet med säkerhets- och robusthetshöjande åtgärder innehåller många delar: Skyddsnätet har fler maskor än en.
- Den tekniska och kommersiella utvecklingen skapar många möjligheter men också en del problem.

.se


Råd och rekommendationer
• Anslut kritiska resurser i Sverige till flera operatörer samtidigt, t.ex. med Anycast. Centralt behöver någon bestämma vad som är en kritisk resurs.
• Upprätta en central sekundär DNS-drift för kritiska resurser, t.ex. vid de svenska Internetknutpunkterna.
• Upprätta en gemensam funktion för virustvätt och rensning av skräppost placerad inom landet.
• Utfärda riktliner för vad som är acceptabel
hantering av skräppost och virus i offentlig
förvaltning. Att skicka oskyddad e-post utomlands
bör inte vara accepterat.
.se

Bilder som visades av Kurt Erik Lindqvist, Netnod Internet Exchange AB, under hans presentation vid den offentliga utfrågningen om IT-säkerhet.

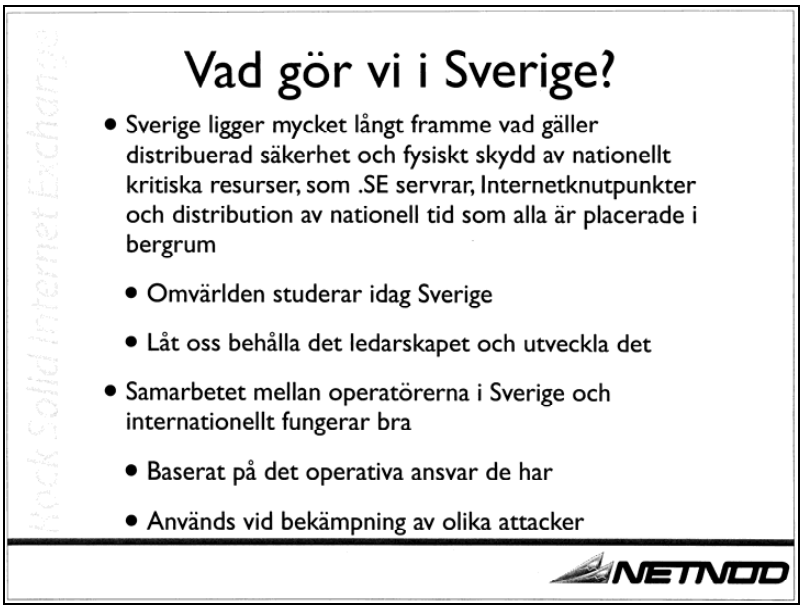


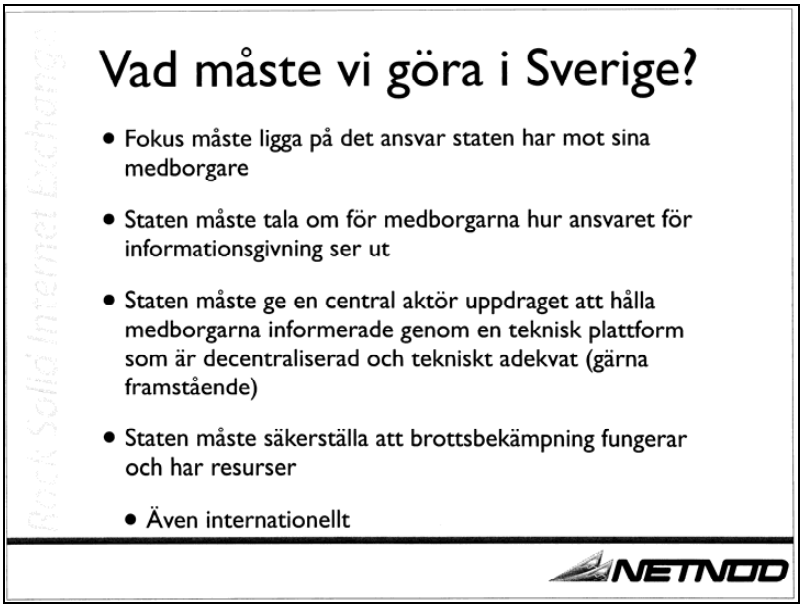

Rock Solid Internet Exchange
Offensiva / Defensiva nationer?
• Vissa nationer arbetar också med offensiva IT möjligheter
• Men det följer återigen andra hotbilder och är "bara" kompletterande metoder
• Här måste man börja med att förstå hotbilden
• Försvar sker genom robusta system och nationell infrastruktur
• Inte genom "speciallösningar", dvs vid krissituationer vill man använda samma system som i normalfallet
NETNOD

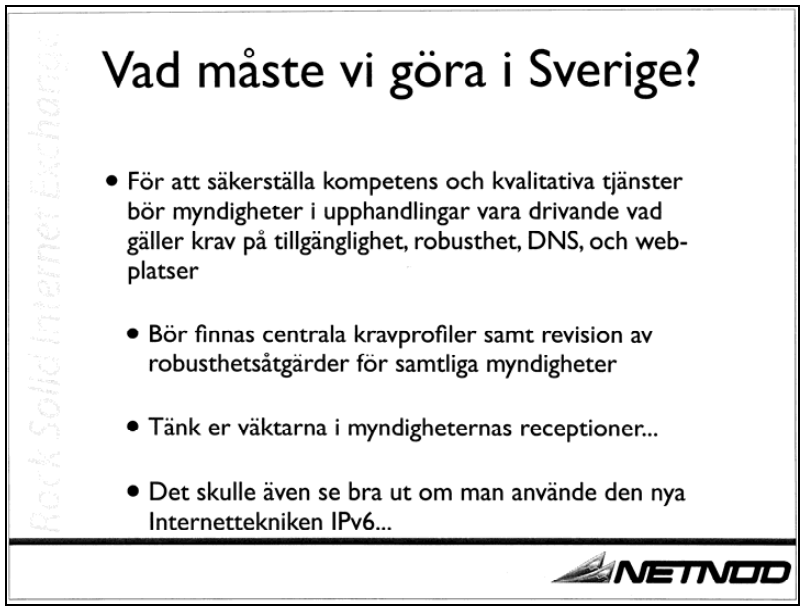

Rock Solid Internet Exchange
"Hot" mot medborgaren
• Medborgarens beteende för att hitta information ändras, och idag är Internet en del av detta
• Se Budget, Tsunamikatastrofen etc
• Däremot är det högst oklart för mig som medborgare *VAR* jag skall hitta information *NÄR*
• Dessutom är det för mig som inblandad i driften av Internet klart att det inte finns infrastruktur för det i Sverige
• Ett system skall klara ungefär 3,5M hushåll - samtidig
NETNOD

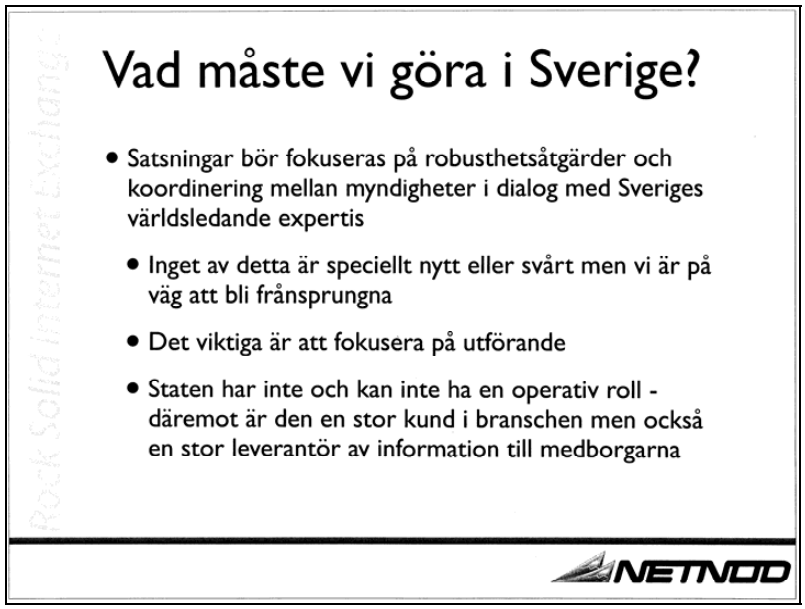

Hot mot myndigheter
• I praktiken drivs alla hot på Internet idag för ekonomisk vinning
• Maffia / Terrorister hyr eller köper attacker
• De flesta attackmöjligheter ägs/styrs av organiserad brottslighet
• Består av 100k-1M infekterade datorer. Används för att fjärrstyras till att skicka spam eller utföra överbelastningsattacker
• Myndigheter är bara ytterligare ett mål - fast med högre risk och mindre utdelning, men även informations läckage kan vara värdefullt för en angripare
Rock Solid Internet Exchange
NETNOD


Hot mot IT samhället i allmänhet
• Attacker sker som utpressning mot aktörer som har mycket att förlora på störningar
• On-line banker, spel, handel etc
• Eller som sk "spam-runs"
• Massutskick. Gör pengar på att sälja annonserade varor, genom phising eller genom t.ex. aktiemarknadsdrivande påståenden
• Detta är kriminalitet och skall bekämpas av polis och åklagare som annan brottslighet
Rock Solid Internet Exchange
NETNOD


Vad gör vi i Sverige?
• Sverige ligger mycket långt framme vad gäller distribuerad säkerhet och fysiskt skydd av nationellt kritiska resurser, som .SE servrar, Internetknutpunkter och distribution av nationell tid som alla är placerade i bergrum
• Omvärlden studerar idag Sverige
• Låt oss behålla det ledarskapet och utveckla det
• Samarbetet mellan operatörerna i Sverige och internationellt fungerar bra
• Baserat på det operativa ansvar de har
• Används vid bekämpning av olika attacker
NETNOD


Vad måste vi göra i Sverige?
• Fokus måste ligga på det ansvar staten har mot sina medborgare
• Staten måste tala om för medborgarna hur ansvaret för informationsgivning ser ut
• Staten måste ge en central aktör uppdraget att hålla medborgarna informerade genom en teknisk plattform som är decentraliserad och tekniskt adekvat (gärna framstående)
• Staten måste säkerställa att brottsbekämpning fungerar och har resurser
• Även internationellt
NETNOD


Vad måste vi göra i Sverige?
• För att säkerställa kompetens och kvalitativa tjänster bör myndigheter i upphandlingar vara drivande vad gäller krav på tillgänglighet, robusthet, DNS, och web-platser
• Bör finnas centrala kravprofiler samt revision av robusthetsåtgärder för samtliga myndigheter
• Tänk er väktarna i myndigheternas receptioner...
• Det skulle även se bra ut om man använde den nya Internettekniken IPv6...
NETNOD


Vad måste vi göra i Sverige?
• Satsningar bör fokuseras på robusthetsåtgärder och koordinering mellan myndigheter i dialog med Sveriges världsledande expertis
• Inget av detta är speciellt nytt eller svårt men vi är på väg att bli frånsprungna
• Det viktiga är att fokusera på utförande
• Staten har inte och kan inte ha en operativ roll - däremot är den en stor kund i branschen men också en stor leverantör av information till medborgarna
NETNOD

Bilder som visades av Anders Johanson, Post- och telestyrelsen, under hans presentation vid den offentliga utfrågningen om IT-säkerhet.

1. Robusta e-kommunikationer
PTS åtgärdar

I privatoffentlig samverkan
Avgifter från operatörer och skattefinansiering

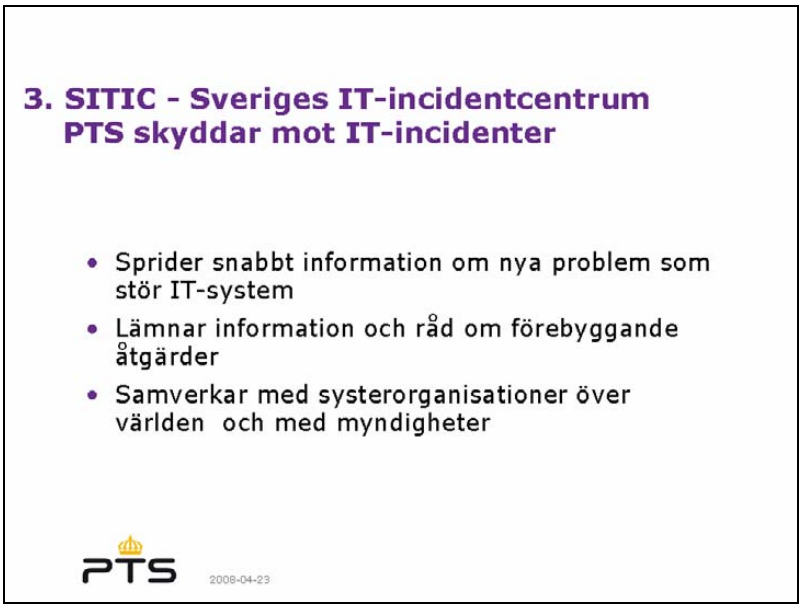
- Alternativa förbindelser för fibernät
- Mobila basstationer
- Reservelektricitet
- Skyddade bergrum för viktiga knutpunkter
- Gemensamma övningar
- Gemensamma lägesuppfattningssystem

PTS 2008-04-23

2. Tillförlitlighet
PTS genomför

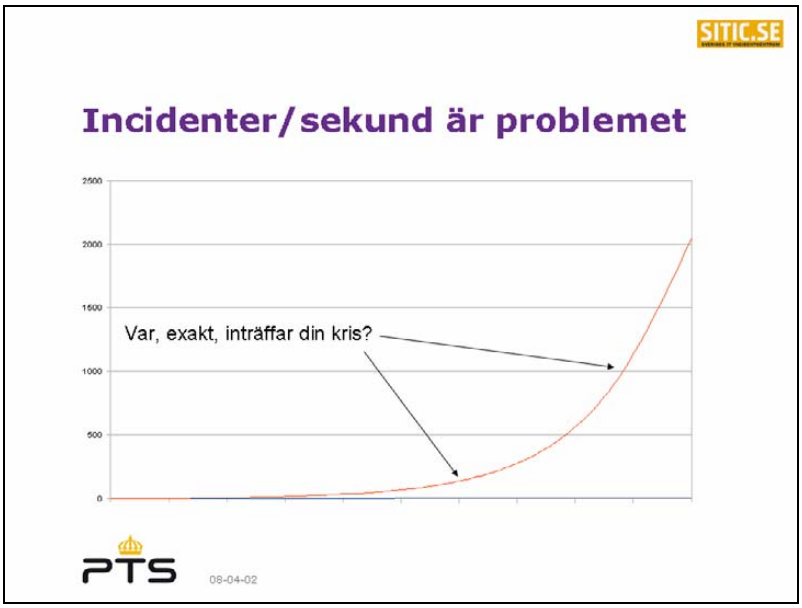
- Regeringens strategi för säkrare Internet
- PTS handlingsplan för säkrare Internet
- PTS - föreskrifter, allmänna råd, rekommendationer
- Tillsyn av operatörernas säkerhetsarbete
- Tillsyn av operatörenas integritetsskydd (t.ex. trafikdatalagring)
- Internationell samverkan
- Information om Internetsäkerhet
- Kampanjen Surfa Lugnt med många organisationer

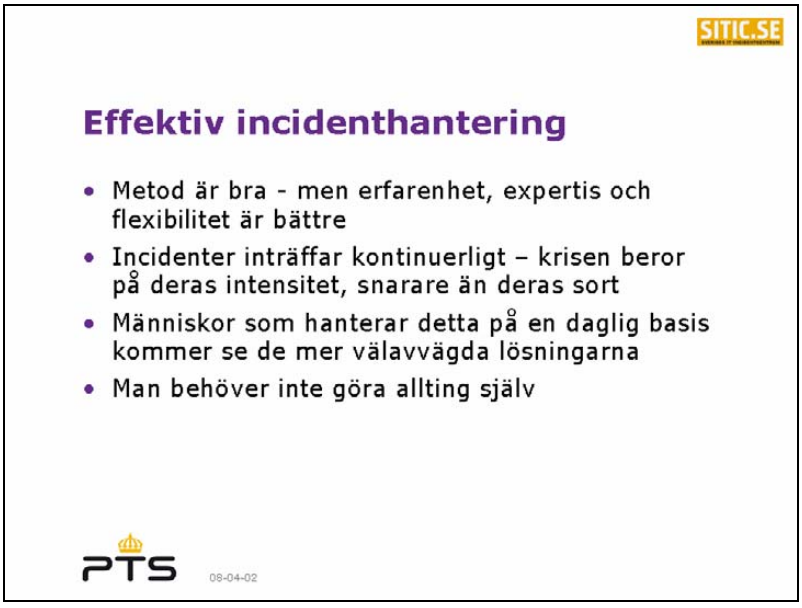
PTS 2008-04-23

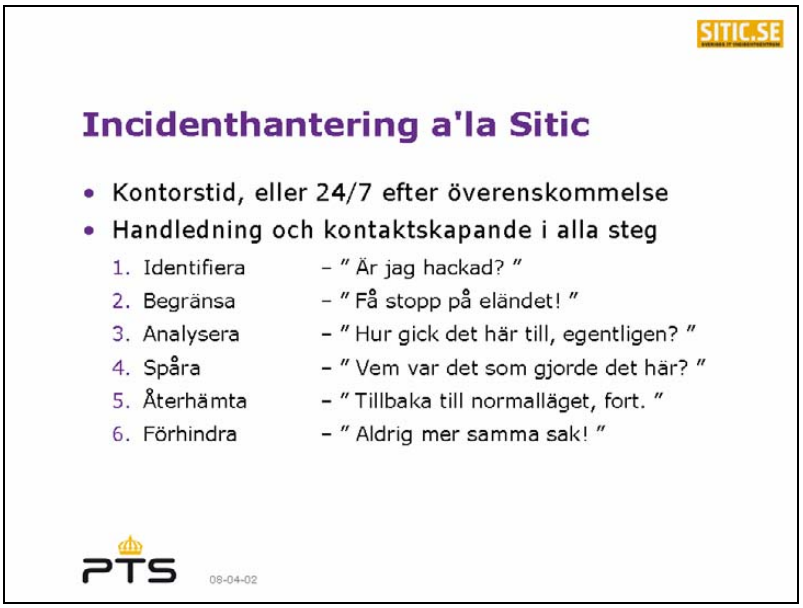

3. SITIC - Sveriges IT-incidentcentrum
PTS skyddar mot IT-incidenter
• Sprider snabbt information om nya problem som stör IT-system
• Lämnar information och råd om förebyggande åtgärder
• Samverkar med systerorganisationer över världen och med myndigheter
PTS
2008-04-23


Trender
PTS oro
• Samhället helt beroende av att e-komm. fungerar
• Komplexitet och sårbarheter ökar
• Robusthetsåtgärderna minskar
• Minskad robusthet skapar mer kriser
PTS
2008-04-23

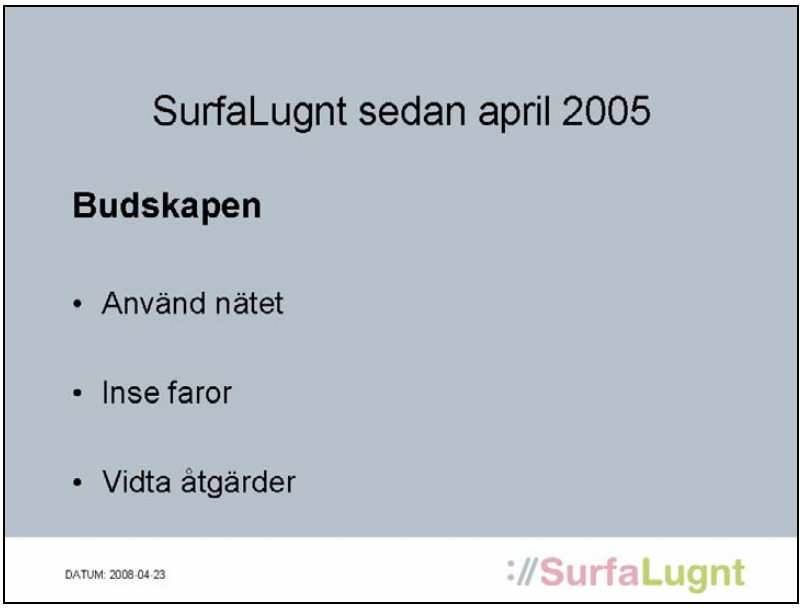
Bilder som visades av Stefan B. Grinneby, Sitic, under hans presentation vid den offentliga utfrågningen om IT-säkerhet.

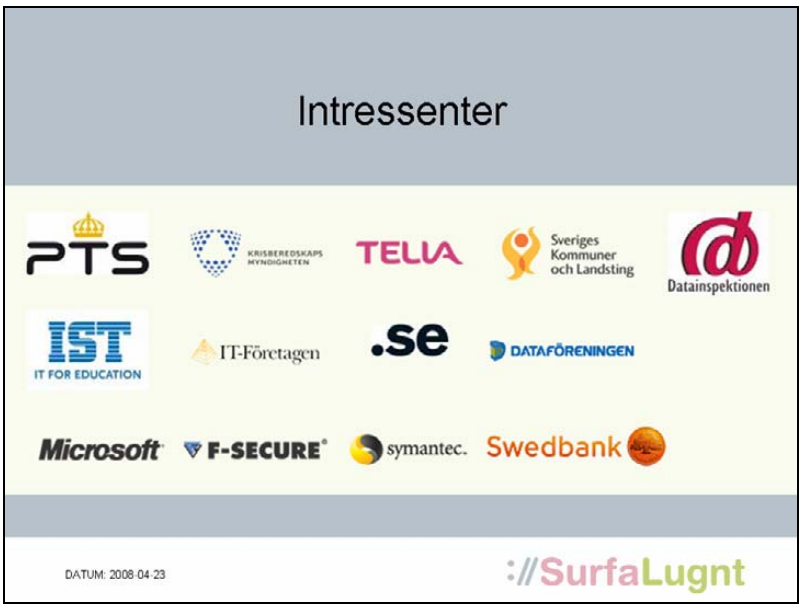


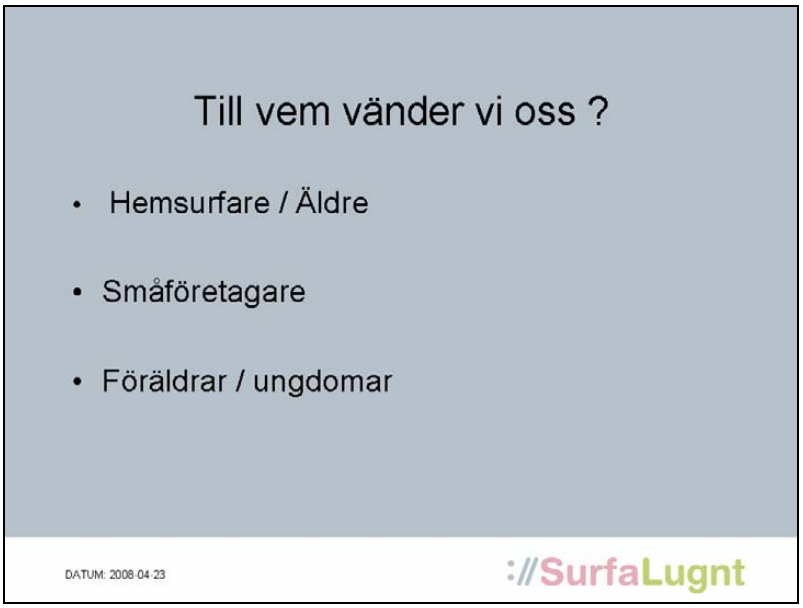



SITIC.SE
Incidenthantering a'la Sitic
• Kontorstid, eller 24/7 efter överenskommelse
• Handledning och kontaktskapande i alla steg
1. Identifiera – ” Är jag hackad? ”
2. Begränsa – ” Få stopp på eländet! ”
3. Analysera – ” Hur gick det här till, egentligen? ”
4. Spåra – ” Vem var det som gjorde det här? ”
5. Återhämta – ” Tillbaka till normalläget, fort. ”
6. Förhindra – ” Aldrig mer samma sak! ”
PTS
08-04-02

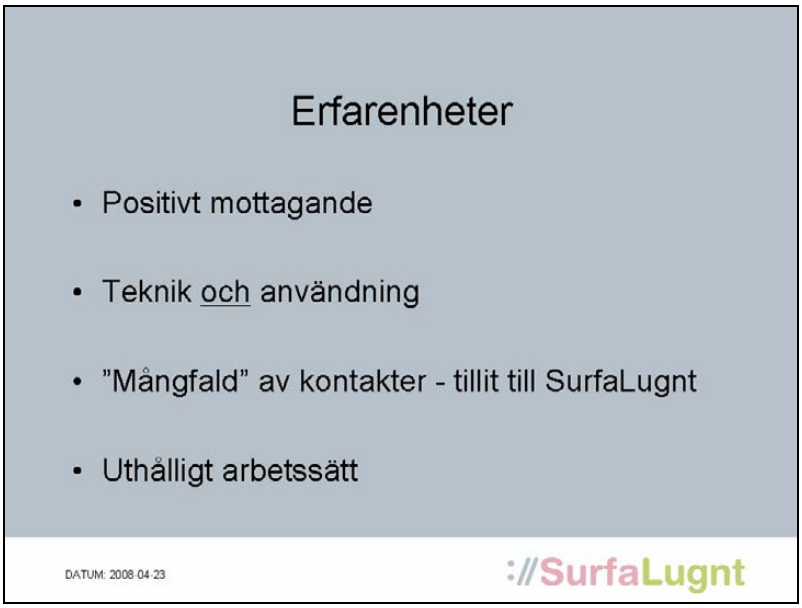
Bilder som visades av Roland Ekström, Kampanjen Surfa Lugnt, under hans presentation vid den offentliga utfrågningen om IT-säkerhet.

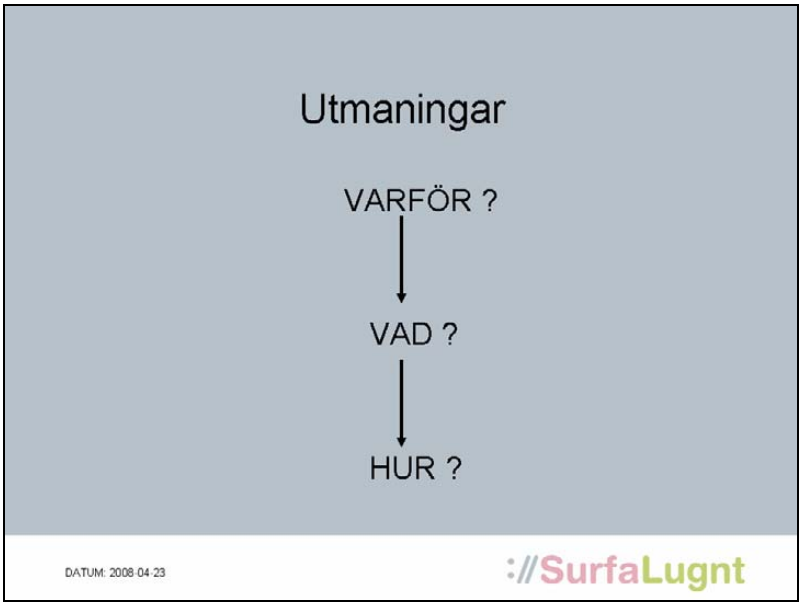





Till vem vänder vi oss ?
• Hemsurfare / Äldre
• Småföretagare
• Föräldrar / ungdomar
DATUM: 2008-04-23
://SurfaLugnt


Verksamheten
• Informatörsnätverk
• Verktyg på webben
• Handfast folder (1 miljon utdelade)
• Expertpanelen – Frågor och svar
• Regionala möten
• Årsdag
DATUM: 2008-04-23
://SurfaLugnt


Erfarenheter
• Positivt mottagande
• Teknik och användning
• ”Mångfald” av kontakter - tillit till SurfaLugnt
• Uthålligt arbetssätt
DATUM: 2008-04-23
://SurfaLugnt


Utmaningar
VARFÖR ?
VAD ?
HUR ?
DATUM: 2008-04-23
://SurfaLugnt

Bilder som visades av Östen Frånberg, Kungliga Ingenjörsvetenskapsakademien, under hans presentation vid den offentliga utfrågningen om IT-säkerhet.

Kungl. Ingenjörsvetenskapsakademien

Internetframsyn mål och målgrupp

IVA

Mål

Målet med projektet är att med utgångspunkt i dagens situation och med stöd av tillgänglig forskning identifiera de viktigaste åtgärder som behövs vidtas för att Sverige ska vara en framstående internetnation år 2015. Projektet ska även föreslå lämpliga ansvariga för utförandet av de förslag som läggs fram.

Primär målgrupp

Beslutsfattare inom näringsliv och offentlig sektor

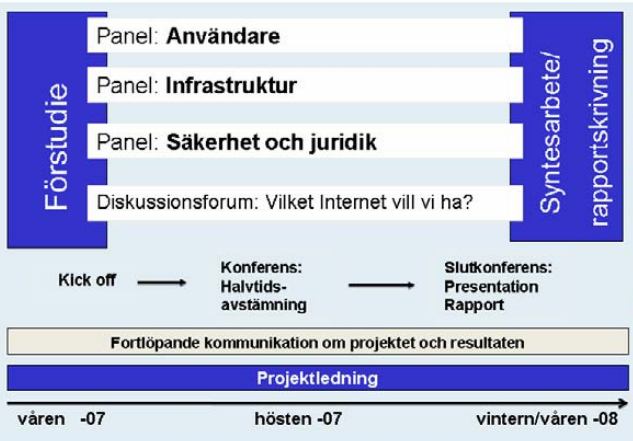
Sekundär målgrupp

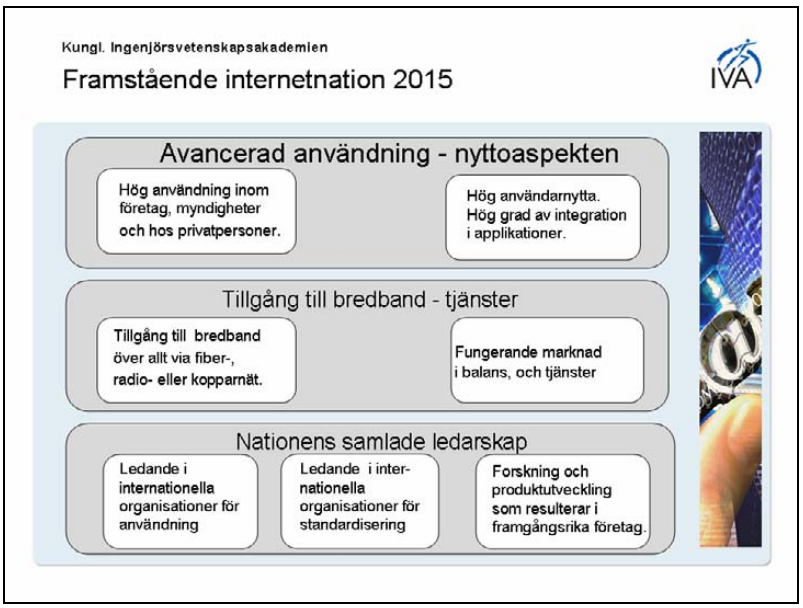
Allmänheten

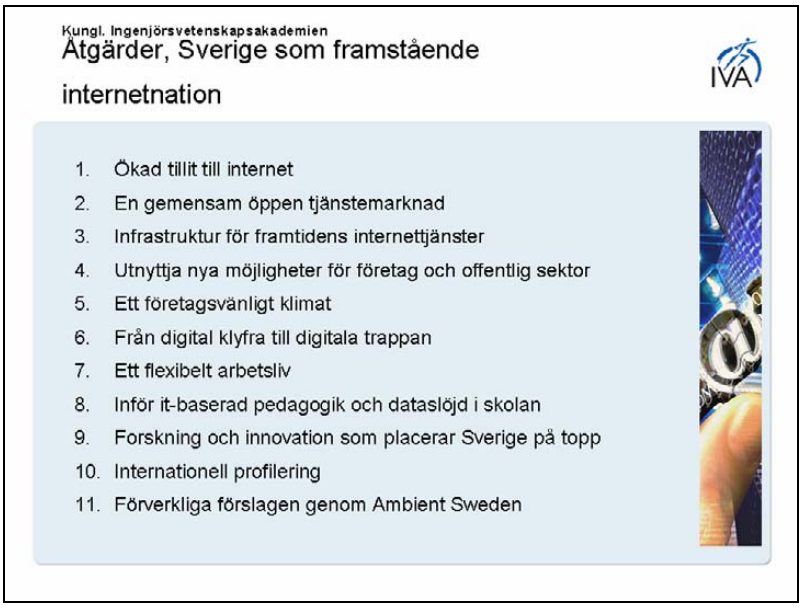
Kungl. Ingenjörsvetenskapsakademien

Aktiviteter

IVA




Kungl. Ingenjörsvetenskapsakademien
Framstående internetnation 2015
IVA
Avancerad användning - nyttoaspekten
Hög användning inom företag, myndigheter och hos privatpersoner.
Hög användarnytta. Hög grad av integration i applikationer.
Tillgång till bredband - tjänster
Tillgång till bredband över allt via fiber-, radio- eller kopparnät.
Fungerande marknad i balans, och tjänster
Nationens samlade ledarskap
Ledande i internationella organisationer för användning
Ledande i internationella organisationer för standardisering
Forskning och produktutveckling som resulterar i framgångsrika företag.


Kungl. Ingenjörsvetenskapsakademien
Åtgärder, Sverige som framstående internetnation
IVA
1. Ökad tillit till internet
2. En gemensam öppen tjänstemarknad
3. Infrastruktur för framtidens internettjänster
4. Utnyttja nya möjligheter för företag och offentlig sektor
5. Ett företagsvänligt klimat
6. Från digital klyfra till digitala trappan
7. Ett flexibelt arbetsliv
8. Inför it-baserad pedagogik och dataslöjd i skolan
9. Forskning och innovation som placerar Sverige på topp
10. Internationell profilering
11. Förverkliga förslagen genom Ambient Sweden

Kungl. Ingenjörsvetenskapsakademien

Säkerhet

Tillit

En basnivå för informationssäkerhet, Användare, leverantörer, företag och myndigheter skall ha ett större medvetande om ansvar för informationssäkerhet.

- *Den personliga integriteten – skall även ha adekvat skydd i elektronisk miljö.*
- *Den snabba framväxten av Internet ställer krav på lagstiftning och nu kan en översyn av den samlade civil- och straffrättsliga lagstiftningen vara påkallad.*
- *Bekämpa IT-brottsligheten på liknande sätt miljöbrott och ekonomisk brottslighet.*

2. En välspridd och allmänt accepterad e-identitet för alla sammanhang, dvs flera sätt för en användare att identifiera sig på internet, även mobilt.

- *Finans- och Näringsdepartementet bör ge ansvariga myndigheter i uppdrag att driva färdplanen för e-legitimationer vidare som spänner över samhällets behov.*
- *E-identiteterna bör vara plattforms- och terminaloberoende.*

3. Generell kvalitetsguide för internetförbindelser, i form av vägledande "färgmärkning".

- *Branschen bör ta ansvar för att specificera olika slags internetförbindelser.*
- *Konsumenternas tele- & rådgivningsbyrå (KITB) bör formulera kraven i samråd med PTS, branschens aktörer, konsumenter och forskning*

Kungl. Ingenjörsvetenskapsakademien

Tillit och tillgänglighet går hand i hand

1.Tillit och infrastruktur är A-O,
Tillit till internet förutsätter även att tillgängligheten till internet är tillfredsställande. Tjänstetillhandahållare och användare har ansvar för säkra funktionalitet och tillgänglighet . Inför SLA (Service Level Agreement) mellan leverantörer och användare/företag/myndigheter

2. "Kriget" fortsätter även 2015 – spridning till mobila terminaler är ett faktum
Attackerna av organiserade grupperingar som har utpressning eller terrorattacker som syfte. Även spam, virus, och spyware, kommer att fortsätta liksom även dess motreaktioner. Denna "krigföring" kommer fortsätter oberoende av vilken terminal som används.

3. Konkurrens är en drivkraft för god beredskap
Ansvar för robustheten i nätinfrastrukturen ligger hos internetoperatörerna
Vidta åtgärder för att skydda infrastrukturen och för förstörande incidenter.
Konkurrensen är en god drivkraft för att skapa beredskap att åtgärda störningar och fel.

4. Tillgängliga rutiner för ökad informationssäkerhet
Informationssäkerhet bidrar till skydd mot förvanskning av information och hot mot den personliga integriteten. Införandet har framgångsrikt genomförts av SUSEC (Swedish University information SECurity group). En IT-säkerhetshandboken finns som är uppdaterad och tillgängligt för alla, http://itsakhandbok.irt.kth.se/susec/.


Kungl. Ingenjörsvetenskapsakademien
Slutkonferens, Internetframsyn 10 april kl.13.00
IVA
Tid: Torsdagen den 10 april 2008 kl 13:00–16:00
Plats: IVAs Konferenscenter, Grev Turegatan 16, Stockholm
Anmälan: Via www.iva.se/internetframsyn senast den 4 april
Presentationer och Rapporter kommer att finnas på IVAs hemsida


Kungl. Ingenjörsvetenskapsakademien
Medfinansiärer
IVA
BIRD & BIRD
TDC
telenor
TeliaSonera
3
Internet Society
The Swedish Chapter
VINNOVA
PTS
Post & Telestyrelsen
hi
Svenska Stadsnätsföreningen
ERICSSON

RAPPORTER FRÅN RIKSDAGEN 2004/05–2005/06

2004/05:RFR1	TRAFIKUTSKOTTET Transportforskning i en föränderlig värld
2004/05:RFR2	NÄRINGSUTSKOTTET Statens insatser för att stödja forskning och utveckling i små företag Rapport till riksdagens näringsutskott
2004/05:RFR3	KONSTITUTIONSUTSKOTTET Nationella minoriteter och minoritetsspråk
2004/05:RFR4	SKATTEUTSKOTTET Skatteutskottets offentliga seminarium om skattekonkurrensen den 15 mars 2005
2005/06:RFR1	JUSTITIEUTSKOTTET Brottsskadeersättning och skadestånd på grund av brott. Undersökning av skillnader mellan beslutad brottsskadeersättning och av domstol sakprövat skadestånd
2005/06:RFR2	JUSTITIEUTSKOTTET Särskild företrädare för barn Uppföljning om tillämpningen av lagen (1999:997) om särskild företrädare för barn
2005/06:RFR3	MILJÖ- OCH JORDBRUKSUTSKOTTET Förutsättningarna för småskalig livsmedelsproduktion – en uppföljning
2005/06:RFR4	KONSTITUTIONSUTSKOTTET Regeringsmakt och kontrollmakt. Offentligt seminarium tisdagen den 15 november 2005 anordnat av konstitutionsutskottet
2005/06:RFR5	KULTURUTSKOTTET Statsbidrag till teater och dans En uppföljning av pris- och löneomräkningens konsekvenser
2005/06:RFR6	UTRIKESUTSKOTTET Utrikesutskottets uppföljning av det multilaterala utvecklingssamarbetet
2005/06:RFR7	TRAFIKUTSKOTTET Sjöfartsskydd En uppföljning av genomförandet av systemet för skydd mot grova våldsbrott gentemot sjöfarten
2005/06:RFR8	UTRIKESUTSKOTTET Vår relation till den muslimska världen i EU:s grannskapsområde
2005/06:RFR9	NÄRINGSUTSKOTTET Näringsutskottets offentliga utfrågning om elmarknaden den 18 maj 2006

RAPPORTER FRÅN RIKSDAGEN 2006/07–2007/08

2006/07:RFR1	FINANSUTSKOTTET En utvärdering av den svenska penningpolitiken 1995–2005
2006/07:RFR2	UTRIKESUTSKOTTET OCH MILJÖ- OCH JORDBRUKSUTSKOTTET Offentlig utfrågning den 12 december 2006 om en gasledning i Östersjön – fakta om projektet – internationell rätt – tillvägagångssätt vid tillståndsprövning
2006/07:RFR3	TRAFIKUTSKOTTET Trafikutskottets uppföljning av flyttning av fordon
2006/07:RFR4	TRAFIKUTSKOTTET Trafikutskottets offentliga utfrågning om trafiklösningar för Stockholmsregionen
2006/07:RFR5	MILJÖ- OCH JORDBRUKSUTSKOTTET Offentlig utfrågning om förutsättningarna för att bedriva småskalig livsmedelsproduktion
2006/07:RFR6	KULTURUTSKOTTET Offentlig utfrågning på temat Var går gränsen för den konstnärliga friheten?
2006/07:RFR7	UTRIKESUTSKOTTET Sveriges deltagande i EU:s biståndspolitik
2006/07:RFR8	SKATTEUTSKOTTET Uppföljning av kvittningsregeln för nystartade företag
2006/07:RFR9	SOCIALUTSKOTTET Socialutskottets offentliga utfrågning på temat hiv/aids torsdagen den 15 februari 2007 (Omtryck, tidigare utgiven som 2006/07:URF4)
2007/08:RFR1	SKATTEUTSKOTTET Inventering av skatteforskare 2007
2007/08:RFR2	TRAFIKUTSKOTTET Offentlig-privat samverkan kring infrastruktur – en forskningsöversikt
2007/08:RFR3	MILJÖ- OCH JORDBRUKSUTSKOTTET Uppföljning av de fiskepolitiska insatsernas resultat och konsekvenser för företag inom fiskeområdet
2007/08:RFR4	SOCIALUTSKOTTET Socialutskottets offentliga utfrågning på temat våld mot äldre, den 19 september 2007
2007/08:RFR5	TRAFIKUTSKOTTET Uppföljning av hur stormen Gudrun hanterats inom transport- och kommunikationsområdet
2007/08:RFR6	FÖRSVARSUTSKOTTET Utvärdering av 2004 års försvarspolitiska beslut
2007/08:RFR7	SKATTEUTSKOTTET Öppet seminarium om attityder till skatter

RAPPORTER FRÅN RIKSDAGEN 2007/08–

2007/08:RFR8 FÖRSVARSUTSKOTTET
Forskning och utveckling inom försvarsutskottets ansvarsområde

2007/08:RFR9 JUSTITIEUTSKOTTET
Uppföljning av Kriminalvårdens behandlingsprogram för män som dömts för våld i nära relationer

2007/08:RFR10 TRAFIKUTSKOTTET
Trafikutskottets offentliga utfrågningar hösten 2007 om trafikens infrastruktur

2007/08:RFR11 KONSTITUTIONSUTSKOTTET
Offentlig utfrågning den 22 november 2007 om tillstånd för digital marksänd tv

2007/08:RFR12 MILJÖ- OCH JORDBRUKSUTSKOTTET
Offentlig utfrågning om förutsättningarna för att låta transportsektorn omfattas av ett system med handel av utsläppsrätter

2007/08:RFR13 SKATTEUTSKOTTET
Skatteutskottets uppföljning av skogsbeskattningen

2007/08:RFR14 TRAFIKUTSKOTTET
Förnybara drivmedels roll för att minska transportsektorns klimatpåverkan

2007/08:RFR15 SOCIALFÖRSÄKRINGSUTSKOTTET
Äldreförsörjningsstödet i dagspressen 2002–2007

2007/08:RFR16 TRAFIKUTSKOTTET
Anpassningen av trafikens infrastruktur när klimatet förändras

2007/08:RFR17 RIKSDAGENS UTSKOTT
Riksdagens framtidsdag 2008 – konferensrapport

2007/08:RFR18 SOCIALUTSKOTTET
Socialutskottets offentliga utfrågning på temat Tillgänglighet inom hälso- och sjukvården

2007/08:RFR19 FINANSUTSKOTTET
Finansutskottets offentliga utfrågning Statlig arbetsgivarpolitik och jämställdhet

2007/08:RFR20 NÄRINGSUTSKOTTET OCH KULTURUTSKOTTET
Näringsutskottets och kulturutskottets offentliga utfrågning om upphovsrätt på Internet