



TU-STIFTELSEN
NETNOD
STUPI
FMV
SUNET
FROBBIT

Sverige under IT attack



Dagens beroenden

- **I takt med att fler och fler använder Internet för fler och fler tjänster ökar också beroendet och förväntningarna på att Internet skall "finnas och fungera"**
- **Attacker mot sårbarheter i samhället kommer att koordineras eller samverka med attacker på IT infrastruktur**
 - Idag är det mycket svårt att få ett samlat grepp om samband och beroenden
- **Hur stor skada kan samhället lida, och hur snabbt?**
- **Vi skall försöka visa på ett antal scenarion som snabbt utvecklar sig och där det krävs nya modeller för försvar och beredskap**
 - Hela förloppet är kanske inte sannolikt men varje enskild incident är möjlig

00.00

**Fredagen den 23 februari 2007
Veckan innan Stockholms sportlov**

00.00

- **I nästa dags morgon tidning publiceras material som kommer att uppfattats som stötande av vissa av världens befolkningsgrupper**
- **Materialet läggs under natten ut på tidningens web-plats**

01.00

01.00

- **Materialet uppmärksammas av de första opponentererna**
- **På chat-sidor och debattforum i andra tidszoner postas länkar, och diskussionerna går snabbt heta**
- **Tidningen börjar ta emot e-post som kräver att materialet skall tas bort och att en ursäkt publiceras**

02.00

02.00

- **Tidningens externa mailsystem slutar fungera på grund av lasten från inkommande e-post**
- **Bland e-posten finns också hot om attacker mot tidningens website**
- **Den inkommande e-posten innehåller en modifierad trojan som inte tidigare upptäckts**
- **En intet ont anande nattredaktör klickar på en länk i ett inkommande e-post-meddelande**
 - Inom loppet av några minuter har trojanen spritt sig till stora delar av tidningens redaktion
- **Extremister inom de grupper som känner sig kränkta kontaktar likasinnade i Sverige och anser att något måste göras**

03.00

03.00

- **Tidningens interna e-post system börjar bli långsamt**
- **Flera användare av tidningens interna system upplever problem med deras datorer. Data saknas även på centrala servrar**
 - Genom ett tidigare oupptäckt säkerhetshål i den databasserver som tidningen använder har stora mängder data raderats slumpvis
- **Tidningens personal upptäcker att deras hemsida är utsatt för en "defacement attack"**
 - Systemansvariga kontaktas

04.00

04.00

- **Anställda på tidningen har problem att komma åt deras web-site och även andra siter på Internet**
- **I diskussionsforum på Internet erbjuds 15 kontokortsnummer i utbyte mot login på tidningens routrar**
- **IT-ansvariga märker att antalet besökare är onormalt hög, men ser inget anmärkningsvärt**

05.00



NSII

05.00

- **Tidningens web-plats är nu helt onåbar**
 - IT ansvariga söker efter trafikmönster som matchar en DDoS attack, ICMP paket, TCP SYN, mönster i sourceadresser eller förfälskade sourceadresser
 - IT ansvariga hittar inget utom onormalt mycket frågor från hela världen
- **IT ansvariga kontaktar sina Internetoperatörer**
 - De verifierar stora volymer av data mot tidningens webbplats
 - Abuse-avdelningarna hos Internetoperatörerna kan inte hitta något mönster i attackerna heller
 - Filtrering är omöjligt
- **I diskussionsforum framförs åsikter om att Sverige som nation bär ansvar**
- **De som surfar in på regeringens websida möts av en hackad version**

06.00



NSII

06.00

- **Tidningens primära Internetoperatör detekterar att en av deras länkar till en upstream-operatör är överbelastad**
 - Detta tar ut BGP sessionen varvid trafiken flyttar till tidningens sekundära operatör
- **Den sekundära operatören upplever också problem**
- **De Svenska operatörerna ber sina upstream-operatörer om hjälp med filtrering**
 - Då trafikmönster saknas blockerar de större operatörerna all trafik mot tidningens webbplats
- **Regeringens websida börjar bli i det närmaste onåbar**

07.00

07.00

- **Sprängladdningar exploderar vid XXX**
 - Stora delar av Mälardalen blir strömlöst
 - Telestationer, operatörernas driftscentraler och datahallar går över till backupdrift
 - Lika så banker och andra kritiska system

08.00

08.00

- **GPS mottagare slås ut med störsändningar**
 - Navigationssystem slås ut
 - Blåsljusmyndigheternas kommunikationssystem Tetra slutar fungera
 - Vissa delar av mobilnätet kan också sluta fungera
- **Internetoperatörerna jobbar febrilt med att stoppa DDoS attacker mot central infrastruktur**
 - Trafiken är omöjlig att urskilja och fler och fler Svenska Internettjänster blockeras hos de stora operatörerna för att säkra trafik till de delar som fortfarande fungerar

08.00

- **Kidnappade routrar runt om i världen annonserar det IP prefix som tillhör regeringen.se och trafiken riktas om till en helt annan plats**
 - Den IP adress som pekas på för MX för regeringen.se annonseras från en annan plats och e-post från omvärlden leds om.

Frågeställningar

Frågeställningar

- **Vilken myndighet har det övergripande ansvaret vid en storskalig attack?**
 - Vem *SER* attacken?
- **Hur kan jag som användare lita på att den information som myndigheter lämnar ut på nätet faktiskt kommer från den myndigheten?**
 - Hur visste jag att www.val.se faktiskt var valresultatet?
 - Hur vet regeringen.se att deras e-post inte hamnar någon annanstans?
 - Ingen av siterna har certifikat och är signerade
 - Internet är idag en live-kanal för omvärlden
- **Information och pålitlighet är ännu viktigare i händelse av kris**

Vad kan/bör man göra?

- **Först och främst måste någon ha ansvar, kunskap och beredskap**
 - Sverige bör ha som målsättning att klara sig isolerat (på flera nivåer) från omvärlden så länge som möjligt
 - Inget som ligger i intresset hos kommersiella aktörer
- **Informationssystem för kriser?**
 - "Kris-server park", www.kris.se (iofs redan upptaget)?
 - Aktiveras vid nationella eller regionala kriser, Länsstyrelsen?
 - Distribuerat, anycast baserat/web-cache
 - Nättopologiskt distribuerad
 - Säkra back-up vägar för aktuell information?
 - Bör myndigheter ha rätt att 'kidnappa' populära tjänster vid kris?
 - Skall vara dimensionerat för att hantera *alla*
 - 3.5M hushåll => 3.5M pps

Vad kan/bör man göra?

- **Viktigt att all myndighets information kommer från signerade källor**
 - Nyheten att Forsmark har haft ett reaktorhaveri under NO vind måste gå att dementera som effekt av en kapad expressen.se/aftonbladet.se hemsida genom att titta hos 'rätt' myndighet

Hur ser myndigheternas anslutningar ut idag?

- Inte helt vetenskapligt
- Undersökt DNS
- Undersökt lite statistik kring routing till myndigheternas webplatser
- Baserat på listan på http://www.sverige.se/upload/Adresskort/xls/adresskort_myndigheter.xls

Myndighets DNS

- **Hur man inte gör.....**
 - arn.se:20061021-20.39.05:ERROR:9::Too few NS records (1) for zone arn.se
 - mail.arn.se. 3600 IN A 195.7.83.164
- **Totalt antal myndigheter : 368**
- **Total med web-plats : 306**
- **Siter som inte har .SE domäner**
 - www.alkoholkommitten.nu
 - www.eudebatt.nu
 - www.mia.eu
 - www.ppm.nu
 - www.kasam.org
 - www.utn.nu

Myndighets DNS

- **Delade URL:er**
 - 2 www.esf.se
 - 2 www.psyccdef.se
 - 2 www.sadev.se
 - 3 www.kammarkollegiet.se
 - 3 www.sfhm.se
 - 4 www.regeringen.se
 - 6 www.dom.se

Myndighets DNS

- **Mest Frekventa web-hosting**

2	159.72.128.133	2	62.13.78.173	skolverket.se
2	192.165.5.25	2	83.140.144.60	"magnum.pistol.se"(sadev.se)
2	193.10.58.5	3	194.71.131.90	ingen reverse
2	193.181.235.130	3	195.67.43.211	ingen reverse
2	194.16.220.134	3	213.131.146.2	ingen reverse
3	2 194.18.73.1	3	217.114.80.109	jarfalla.se+ ??
4	2 194.71.213.33	4	130.242.29.103	www.maritima.se
5	2 195.7.65.133	4	130.242.56.18	www.smvk.se
6	2 212.214.95.72	4	195.67.43.222	ingen reverse
7	2 213.131.146.65	4	81.216.70.132	ingen reverse
		5	217.114.80.115	krisnatet.se, rsos.se
		6	159.190.0.57	Domstolar
		7	159.190.0.61	Domstolar
		23	147.186.254.17	Polisen

Myndighets DNS

- **DNS Check tester: 15618**
- **DNS Check WARNING: 1740 (11.1%)**
- **DNS Check ERROR: 772 (4.9%)**

Länsstyrelser...

- “Länsstyrelsernas verksamhet omfattar bland annat naturvård och miljöskydd, social omvårdnad, kommunikationer, livsmedelskontroll, djurskydd och allmänna veterinära frågor, lantbruk, rennäring (i Norrbottens, Västerbottens och Jämtlands län), fiske, jämställdhet mellan kvinnor och män, kulturmiljö, regional utveckling, hållbar samhällsplanering och boende, ***civilt försvar, krishantering i fredstid och räddningstjänst.***”

Länsstyrelser...

- **21st totalt...**

1 193.44.115.10

1 212.85.69.168

1 62.80.203.114

1 62.80.203.130

1 62.80.203.146

1 62.80.203.154

1 80.88.101.39

1 82.99.22.197

1 83.166.8.242

12 62.80.203.178

Länsstyrelser...

k.lst.se:20061025-07.21.10:INFO:79::Start check
k.lst.se:20061025-07.21.10:INFO:81::Found NS sunic.sunet.se for parent lst.se
k.lst.se:20061025-07.21.10:INFO:81::Found NS ns1.lst.se for parent lst.se
k.lst.se:20061025-07.21.10:INFO:81::Found NS ns2.lst.se for parent lst.se
k.lst.se:20061025-07.21.10:ERROR:6:ns2.lst.se:NS not found (NOERROR)
k.lst.se:20061025-07.21.10:ERROR:6:ns1.lst.se:NS not found (NOERROR)
k.lst.se:20061025-07.21.10:ERROR:6:sunic.sunet.se:NS not found (NOERROR)
k.lst.se:20061025-07.21.10:ERROR:9::Too few NS records (0) for zone k.lst.se
k.lst.se:20061025-07.21.10:ERROR:12::No nameservers authoritative
k.lst.se:20061025-07.21.10:INFO:106::Ready with this zone

- **Totalt antal tester: 243**
- **Antal fel: 100 (41%)**

Myndighets routing

- Antal rutter : 115
- Totalt antal Paths från route-views: 6808
- Unika Paths: 1659
- Totalt antal source AS: 42

Myndighets routing

•Mest populära rutter :

2 130.235.0.0/16,
2 130.238.0.0/18,
2 137.61.0.0/16,
2 192.121.176.0/23,
2 192.36.25.0/24,
2 193.44.0.0/15,
2 194.16.0.0/15,
2 194.71.83.0/24,
2 195.66.32.0/19,
2 212.112.160.0/19,
2 213.180.64.0/19,
2 217.16.192.0/20,
2 217.70.32.0/23,
2 62.80.192.0/20,
2 80.252.160.0/20,
2 81.216.10.0/23,
2 83.241.128.0/17,

3 194.18.0.0/16,
3 194.198.0.0/16,
3 195.198.0.0/16,
3 212.214.0.0/16,
3 212.247.0.0/16,
3 213.131.128.0/19,
4 130.243.0.0/16,
4 159.190.0.0/16,
4 193.11.0.0/16,
4 194.47.0.0/16,
4 195.7.64.0/19,Pi.se
4 62.20.0.0/16,Telia
6 130.237.0.0/16,SUNET
6 192.71.85.0/24,Steria
6 195.67.0.0/16, INFOCARE Service Ab
10 217.114.80.0/20, Elektropost Stockholm Ab
11 193.12.0.0/14, SWIPNET
12 62.119.0.0/16,Utfors
16 193.10.0.0/16,SUNET
17 130.242.0.0/15, SUNET/NorduNET

Myndighets routing

- **Mest populära source AS per path :**
 - 116 1653 SUNET
 - 180 12352 WinEasy
 - 180 21195 DGCSYSTEMS
 - 180 2874 Equant Nordics
 - 264 8195 IONIP
 - 270 16115 UNSPECIFIED (Advantage-e) (OMX)
 - 390 3246 TDCSONG
 - 450 30811 ElektroPost
 - 873 3301 Telia
 - 900 1257 Swipnet
 - 1168 8434 Telenor

Slutsatser

Slutsatser

- **Staten hanterar gemensamma resurser och koordinerar samhällsfunktioner**
- **Nu och mer i framtiden, kommer vi att ha Internetbaserad kommunikation och integrering av samhällsfunktioner**
- **Vad bör man göra?**
 - Informationshantering och informationsgivning skall fungera för alla i händelse av kris
 - Fysisk redundans för samhällsfunktioner
 - Fysisk redundans för användaren
 - Logisk redundans via routing, autenticering, DNS, etc.

Slutsatser

- **Vad bör man göra [forts].**
 - Krissamordning
 - Dokumentera preventiva åtgärder
 - Hur kan Sverige klara sig fristående
 - Hur kan Sverige vidmakthålla resurser internt
 - Extra DNS, redundans, kapacitet
 - Beroenden på autenticeringsnycklar?
 - Hur kan vi göra felsökning av Sverige? Kidnappade rutter, DNS, etc.
 - Hur kan en myndighet upptäcka det?
 - Prober, datainsamling analys?
 - Datakorrelation är mycket viktigare än datalagring

Slutsatser

- **Myndigheter måste ha kontaktstrukturer och kunskap för att få ändringar genomförda (i händelse av kris)**
- **NSII har studerat förslag på åtgärdsprogram för myndigheter**
 - Ansökt om pengar från Vinnova.....
 - Förhoppningsvis sått ett frö hos vissa myndigheter..
- **NSII hoppas på dialog och debatt**
 - Och framförallt på resultat :-)