Sveriges beredskap mot nätangrepp

KBM:s utbildningsserie 2008:1

KRISBEREDSKAPS
MYNDIGHETEN

Titel: Sveriges beredskap mot nätangrepp
Utgiven av Krisberedskapsmyndigheten (KBM)
Upplaga: 400 ex
Text: Omvärldsanalysgruppen på Informationssäkerhetsenheten, KBM
Omslagsfoto: Keystone

ISBN: 978-91-85797-13-4
ISSN: 1652-3539
KBM:s dnr: 1104-2007
Produktion: Jupiter Reklam AB
Tryck: NRS Tryckeri, Huskvarna, 2008

Skriften kan laddas ner från Krisberedskapsmyndighetens webbplats
www.krisberedskapsmyndigheten.se

Sveriges beredskap mot nätangrepp

Innehållsförteckning

Förord

Under våren 2007 utsattes Estland för en Internetblockad som varade under flera veckor. Under denna tid fungerade nätet inte normalt. Det blev svårt att nå myndigheter och massmedia via Internet, nätbankerna fick under en kort period avbryta sin verksamhet och under flera längre perioder var det svårt att kommunicera med omvärlden via Internet.

Hur skulle Sverige klara av en liknande situation? Det är en av de frågor vi haft för ögonen när vi tagit fram denna rapport, som är uppdelad i två avsnitt. I den första delen kartläggs händelserna i Estland, inklusive de speciella förhållanden som ledde fram till att landet utsattes för omfattande nätattacker. I den andra delen ser vi på hur Sverige är rustat för liknande händelser, där landet utsätts för mer eller mindre organiserade attacker.

Genomgången av situationen i Sverige har utgått ifrån ett antagande av antagonistiska hot i tre nivåer. Den första nivån av begränsad blockering och mindre manipulering av innehållet på vissa hemsidor utgör normalt inget allvarligt hot mot samhället och kan för det mesta hanteras av de drabbade organisationerna och nätoperatörerna. De två andra nivåerna utgör däremot sådana hot som i allmänhet kräver avancerad kunskap att iscensätta samt har ett syfte att till exempel påverka kommunikationerna, förvränga myndighetsinformation eller sabotera kritisk infrastruktur som el- eller vattenförsörjning. Erfarenheten från Estland visar också att attacker kommer att drabba flera aktörer och sektorer samtidigt.

Genomgången visar att det idag finns oroväckande sårbarheter i det svenska samhället vad gäller allvarliga hot på nivå två och tre.

För det första har såväl Riksrevisionens genomgångar som KBMs egna undersökningar avslöjat påtagliga brister i myndigheternas hantering av sin egen informationssäkerhet.

Bland annat saknas viktiga rutiner, myndigheters hemsidor går att kapa – och problemen har inte uppmärksammats tillräckligt på ledningsnivå.

För det andra innebär den svenska förvaltningstraditionen med självständiga myndigheter att det sannolikt skulle bli betydligt svårare i Sverige än i Estland att upprätthålla en aktuell lägesbild i en situation där svenska nät attackeras på bred front. Det saknas framför allt möjlighet att snabbt detektera många samtidiga angrepp på svenska myndigheter om de inte är delar av ett större trafikflöde som syns på stamnätsnivå.

För det tredje finns det bara ett begränsat antal personer i Sverige med operativ erfarenhet av att hantera storskaliga, utdragna nätincidenter. Vid ett sådant angrepp kan det behövas fler kunniga personer än vad som finns tillgängligt idag.

För det fjärde kan hushållens ökade bredbandsförbindelser med hög kapacitet eskalera hotet från en koordinerad attack. Ett botnät av infekterade hemdatorer med höghastighetsuppkopplingar kan bli ett kraftigt vapen mot samhällets informationssystem. Även myndigheters datorer kan tas över och användas i sådana attacker. Detta visades i en undersökning över DNS-användningen i Sverige som publicerades nyligen.

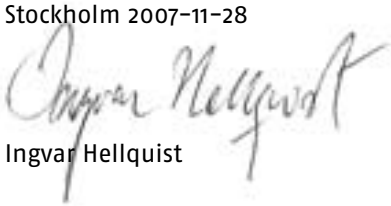
I övrigt har stamnätsinfrastrukturen i Sverige mycket hög kapacitet och risken för att den svenska grenen av Internet skulle blockeras helt är relativt liten.

Föreliggande handling utgör en delrapport i det pågående arbetet vid Krisberedskapsmyndigheten med att studera området cyberförsvar (cyber defence). Delrapporten utgör ett underlag till den årliga lägesbedömning om samhällets informationssäkerhet som myndigheten tar fram på uppdrag av regeringen. Den är därmed inte någon utredning i vanlig bemärkelse, utan snarare en kartläggning av området och ett försök till analys av vilka konsekvenser de estniska erfarenheterna av nätangrepp kan få för skyddet

av svenska samhällsfunktioner. Den syftar inte till att ge konkreta åtgärdsförslag, utan begränsar sig till att ringa in viktiga problemområden som borde bli föremål för en bredare diskussion. De förslag som detta utmynnar i planeras ingå i den handlingsplan för informationssäkerhets-området som Krisberedskapsmyndigheten kommer att överlämna till regeringen i mars 2008.

Delrapporten har tagits fram av Informationssäkerhetsenhetens grupp för omvärldsanalys. Arbetet har underlättats kraftigt av den generösa hjälp som erhållits från estniska myndigheter och från personer med speciell insikt i hur hantering av nätincidenter fungerar.

Stockholm 2007-11-28



Ingvar Hellquist

Del 1

Nätattackerna mot Estland

Sammanfattning

Från slutet av april till mitten av maj 2007 genomfördes omfattande angrepp mot den estniska grenen av Internet. Händelsen hade av allt att döma ett direkt samband med oroligheter i Estland i samband med förflyttningen av ett ryskt krigsminnesmärke.

Angreppen följde ett mönster där enkla åtkomstattacker efterhand följdes av underrättelseinhämtning och fokuserade, välkoordinerade attacker som involverade mycket stora botnät.

Flera nätbanker blockerades under attackerna, men de centrala näten och datorsystemen vid estniska myndigheter kunde skyddas. Det skedde inte heller några lyckade attacker mot elnät eller annan kritisk infrastruktur i landet. Angreppen bestod huvudsakligen av åtkomstattacker av olika slag samt hackade webbsidor (sk defacements).

Angreppen visar att attacker på informationsresurser kan användas för att skapa uppmärksamhet, störa verksamheten hos myndigheter och näringsliv och fungera som en påtryckningsmetod bland andra, exempelvis i kombination med ekonomiska sanktioner. De visar att angripare idag har möjlighet att genomföra nätattacker och samtidigt dölja sitt eget agerande.

Händelserna i Estland visar också att effekterna av liknande nätattacker kan begränsas genom dels förebyggande åtgärder, dels ett kraftfullt samlat agerande under själva krisen. De förebyggande åtgärderna omfattar främst beredskap för att kunna övervaka mönster och avvikelser i nättrafiken, beredskap för att snabbt införa skyddsåtgärder i de egna näten – samt ett effektivt internationellt samarbete inom incidenthantering. Under själva angreppet underlättades arbetet av att man snabbt sammankallade en stab med representanter från olika delar av samhället. Dessa erfarenheter borde ha konsekvenser även för svensk krisberedskap.

Bakgrund och händelse-utveckling

Estlands befolkning uppgår till cirka 1,4 miljoner personer. Av dessa är omkring 400 000 personer rysktalande, huvudsakligen av rysk-etniskt ursprung. Inom denna grupp av "ryssar" finns det olika grupper som i varierande grad integrerats i det estniska samhället. En stor del talar det estniska språket och accepterar Estland som stat medan andra inte gör det och är av uppfattningen att Ryssland är deras stat och att Estland åter ska komma under ryskt styre.

Stalins regim reste 1947 en bronsstaty som föreställer en soldat ur Röda armén. Denna staty är för delar av den ryska minoriteten i Estland en symbol för Sovjetunionens seger över Nazityskland. Statyn har länge stått i centrala Tallinn och hedras numera varje år den 9 maj, vilket är den ryska minnesdagen över segern i andra världskriget och det stora fosterländska kriget mot nazismen. För många i den estniska befolkningen är statyn dock ett minne av den sovjetiska ockupationen och en symbol för förtryck. Det är en av de få symboler från sovjettiden som finns kvar i Estland efter landets självständighet 1991. Tidigare hade statyn inte någon större polariserande effekt. Människor som ville hedra minnet av de soldater som deltog i kriget mot Tyskland kom och placerade blommor vid platsen – utan provokativa intentioner – och de personer som blev påminda om problemen från Sovjettiden kunde ignorera statyn.

Situationen förändrades dock den 9 maj 2006, då polisen ingrep när det uppstod bråk mellan olika grupper som bar sovjetiska respektive estniska flaggor. Denna händelse skapade inre konflikter och den estniska regeringen tog därför ett beslut om att flytta statyn och ett antal sovjetiska soldatgravar intill. Detta var emellertid inget som politikerna i det estniska parlamentet var eniga om utan det fördes en debatt i frågan. Det bestämdes att flytten skulle ske efter den 9 maj 2007.

Torsdagen den 26 april placerade estniska myndigheter ett stort, staketomgärdat tält på platsen för att påbörja utgrävningarna efter soldatgravar i marken runt monumentet. Det ledde omedelbart till en demonstration, som i förstone gick lugnt tillväga. Men när den plötsligt urartade under kvällen och omfattande kravaller utbröt togs under natten till den 27 april ett snabbt beslut om att flytta bronsstatyn omgående till hemlig ort. Förflyttningen skedde redan tidigt den påföljande morgonen.

Kravallerna ledde till omfattande förödelse i centrala Tallinn med krossade skyltfönster, plundrade butiker och bränder som följd. Det var mestadels berusade ungdomar som deltog. Ett stort antal personer greps, ett femtiotal skadades och en ung man av rysk-etniskt ursprung fick också sätta livet till. Myndigheterna tog efter den första kravallnatten ett beslut om att förbjuda all försäljning av alkohol och att förbudet skulle gälla till den 2 maj. Kravallerna fortsatte under nästa dag, fredagen den 27 april, och under den följande helgen. Sent på fredagskvällen startade de första nätattackerna.

På söndagen den 29 april meddelade Estlands försvarsminister Jaak Aaviksoo att bronsstatyn officiellt skulle återinvigas den 8 maj. Detta skedde också, och statyn och dess stenmur finns numera på en krigskyrkogård i Tallinn.

Nätattackerna var inte de enda händelser som inträffade i samband med oroligheterna på gatorna i Tallinn. Under perioden slutet av april till mitten av maj påverkades Estland också av en rad sanktioner från rysk sida. Det genomfördes oannonserade reparationer av järnvägsförbindelser mellan Estland och Ryssland, pappershanteringen vid gränsövergångar blev plötsligt onormalt omfattande, transittrafik ströps och stora ryska varubeställningar annullerades.

Nätattackerna

Den första vågen av nätattacker inleddes på kvällen den 27 april, mindre än ett dygn efter förflyttningen av bronsstatyn och vid en tidpunkt då det pågick våldsamma upplopp i centrala Tallinn.

Denna första angreppsvåg bestod nästan uteslutande av enklare åtkomstattacker och skräppost. Åtkomstattackerna riktades framför allt mot webbservrar med hög publik profil och syftade till att strypa tillgängligheten till dem.

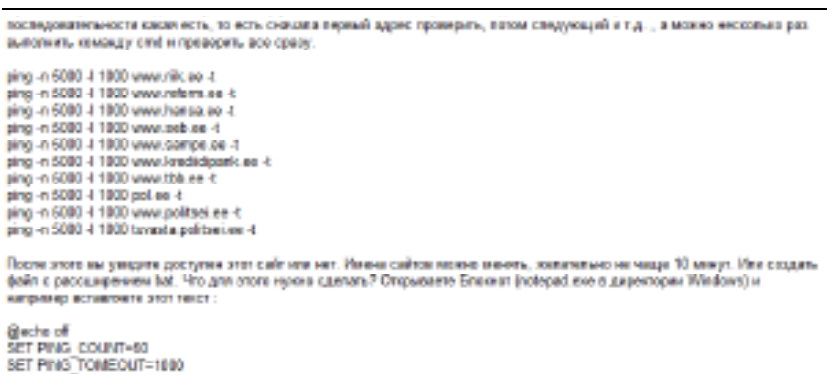
Till de drabbade hörde flera politiska partier, presidentens och parlamentets webbplatser, den estniska polisen, flera centrala myndigheter samt även några estniska legationer utomlands.

Bland annat fick den estniska regeringens publika briefingrum (www.valitsus.ee/brf) temporärt spärras för åtkomst från utlandet. Hackare lyckades också bryta sig in på det styrande Reformpartiets webbplats. Där placerade man en falsk officiell ursäkt för flytten av bronsstatyn, undertecknad premiärministern Andrus Ansip. Man försåg också premiärministerns bild med en Hitlermustasch.

Ett exempel på en ryskspråkig webbsida (zyklonteam.org) där det erbjöds attackverktyg specialanpassade för att rikta attacker mot estniska webbplatser.

I samband med att oroligheterna spridit sig runt Tallinn hade detaljerade attackinstruktioner också i snabb takt börjat spridas på en rad ryskspråkiga webbplatser och diskussionsforum för hackare, ofta tillsammans med uppmaningar att köra dessa kommandosekvenser för att skada Estland. Dels postades uttryckliga kommandon, dels tillhandahölls färdiga attackverktyg som var speciellt anpassade för att attackera webbplatser i Estland.

De instruktioner som dokumenterats (och som i åtskilliga fall fortfarande går att läsa på Internet) uppmanar typiskt till så kallad pingflodning mot namngivna estniska webbplatser. Det är en metod där man skickar stora mängder onormala testsignaler till en Internetansluten dator i syfte att dränka den i databitar. Även andra, liknande metoder förekom under denna första angreppsvåg. Ett exempel är SYN-flodning. Flera varianter av denna angreppstyp förekom.



последовательности какая есть, то есть сначала первый адрес проверить, потом следующий и т.д. , а можно несколько раз выполнить команду cmd и проверить все сразу.

ping -n 5000 -l 1800 www.rik.ee -t
ping -n 5000 -l 1800 www.reform.ee -t
ping -n 5000 -l 1800 www.hansa.ee -t
ping -n 5000 -l 1800 www.seb.ee -t
ping -n 5000 -l 1800 www.sampo.ee -t
ping -n 5000 -l 1800 www.hredaldpank.ee -t
ping -n 5000 -l 1800 www.tbb.ee -t
ping -n 5000 -l 1800 pol.ee -t
ping -n 5000 -l 1800 www.politsei.ee -t
ping -n 5000 -l 1800 tarvasta.politsei.ee -t

После этого вы увидите доступен этот сайт или нет. Имена сайтов можно менять, желательно не чаще 10 минут. Или создать файл с расширением bat. Что для этого нужно сделать? Открываете Блокнот (notepad.exe в директории Windows) и например вставляете этот текст :

@echo off
SET PING_COUNT=60
SET PING_TOMEOUT=1800

I samband med oroligheterna började attackinstruktioner och uppmaningar att attackera estniska webbservrar spridas på många ryska diskussionsforum för hackare. I ovanstående exempel uppmanas läsarna att pingfloda en rad namngivna estniska webbplatser.

Under fredagskvällen och natten till lördagen den 28 april var situationen tämligen kaotisk på den estniska sidan. Det gick ganska snabbt att sluta sig till att den kraftigt ökade trafiken mot de estniska grenarna av Internet hade ett samband med oroligheterna i landet och flytten av bronsstatyn. Men det rådde ändå vissa oklarheter kring motiven.

Att myndigheter och politiska webbplatser utsetts till attackmål var vad man kunnat förvänta. Några massmedia attackerades också, bland annat dagstidningen Postimees. Här fanns ett direkt motiv att finna i det att dessa media rapporterat direkt från upploppen i Tallinn – och i något fall till och med uppmanat befolkningen att skicka in sina digitalfoton/mobilfoton till polisen för att hjälpa till att identifiera upploppsmakarna.

Men samtidigt riktades även stora trafikflöden mot webbsidor hos småkommuner och skolor på den estniska landsbygden. Detta gav i förstone intrycket av att denna attackvåg inte var speciellt väl koordinerad, utan snarare resultatet av ett otal attacker från många enskilda aktörer som uppmanats till en gemensam aktion. Det fanns emellertid indikatorer på att större, koordinerade botnät redan nu börjat användas.

Under de följande dygnen infördes filtrering och andra skyddsåtgärder på estnisk sida. Vid en förnyad våg av åtkomstattacker efter helgen kunde effekten därför minskas markant.

Vid denna tid hade man emellertid börjat märka av flera förändringar. Dels kunde skilda typer av underrättelseinhämtning detekteras i de estniska näten, jämte försök till intrång och övertagande av utrustning i själva nätinfrastrukturen. Det skedde bland annat bandbreddstester för att mäta kapacitetstak i de estniska näten.

Dels märkte man nu av att större botnät börjat tas i bruk, och angreppen blev alltmer sofistikerade. Parlamentet tvingades stänga av sin e-post under 12 timmar, estniska

massmedia slutade svara på utländska anrop, och vid ett tillfälle den 1 maj tvingades flera internetoperatörer i Estland släppa samtliga kundkoppel under 20 sekunder för att starta om sin utrustning.

Redan något dygn efter den första attackvågen hade de estniska myndigheterna organiserat en stab för att skaffa en samlad lägesbild och koordinera arbetet. Den sammanträdde varje dag på försvarsministeriet i Tallinn, och samarbetet underlättades kraftigt av att det är gångavstånd mellan ministerierna. Det praktiska arbetet leddes av incidenthanteringsorganet CERT Eesti (CERT-EE) vid närbelägna Centrum för Informationsteknik (RIA).

En första information till utländska CERT-organisationer gick ut redan den 28 april, efter den första natten av nätattacker. Strax före lunch på måndagen (30 april) spreds därefter mer detaljerad information om målsystemen i Estland till CERT-EEs utländska samarbetspartner, vilket gjorde det möjligt att skapa signaturer och filtrera trafik nära angreppskällorna.

Trafikstatistik uppsamlad på en mätpunkt i Estland. Här ser man den plötsliga flod av ping-paket som sent på fredagskvällen den 27 april började skickas in mot estniska datorer. Angreppet varade under nästan ett dygn. Diagrammet visar därefter hur en förnyad stor attackvåg träffar nätet natten till måndag, men den stryps relativt snabbt och man har vid detta tillfälle också upphört att svara på ping-anropen för att inte i onödan belasta det egna nätet.

När nästa stora attackvåg inleddes några dygn senare, den 4 maj, hade man därför relativt god beredskap. Under närmare ett dygn riktades mycket stora trafikflöden mot estniska myndighetsservrar och myndighetsnät. Dessa attacker var betydligt mer organiserade än vad man sett tidigare, och kunde liknas vid ett hällregn av nättrafik över de estniska näten – eller ett uthålligt och koordinerat hamrande på näten med många olika verktyg och tillhyggen.

Att attackerna skedde på ett koordinerat sätt kunde man bland annat sluta sig till genom att de involverade stora botnät som i tät sekvens riktades mot noggrant utvalda mål med olika attackverktyg. Man kunde se stora, parallella angreppsflöden vars enskilda komponenter/verktyg och avskjutningsramper byttes ut med bara några sekunders lucka.

Dessutom var det tydligt att angriparna omgrupperat sina botnät. Efter den första attackvågen hade incidenthanteringsorganisationer över hela världen involverats och hjälpt till att släcka ner attackerande datorer inom sina respektive närliggande operatörsnät. Nu ökade antalet botnätsangrepp från jurisdiktioner utan incidenthanteringsorganisation (CERT) eller med påtagligt svag incidenthanteringsförmåga.

Attackerna skedde dock inte enbart från utlandet. Redan från den första angreppsvågen hade man märkt av ett stort antal attackerande dator inifrån Estland. Parallellt med incidenthanteringsarbetet arbetade den estniska polisen därför med att försöka spåra gärningsmännen. Enligt uppgift lyckades man identifiera flera personer. Efter drygt en vecka greps en ung man som bland annat publicerat instruktioner och attackmål på estniska diskussionsforum samt uppmanat andra att hjälpa till i attackerna. Mannens visades upp i estnisk television, något som omedelbart fick en avskräckande effekt på andra nätaktivister i Estland. Antalet inhemska attacker sjönk bokstavligen över en natt till en mycket låg nivå.

Under perioden 6 – 8 maj minskade den fientliga aktiviteten något. Därefter inleddes vad som antagligen var tänkt att bli den stora huvudattacken. Det skedde sent på kvällen den 8 maj estnisk tid, eller midnatt till den 9 maj Moskvatid, alltså precis då den ryska minnesdagen över segern i andra världskriget tog sin början.

Huvudattacken innebar en mycket intensiv kanonad av koordinerade nätangrepp mot estniska servrar. Tillvägagångssättet liknade det som man sett redan några dygn tidigare, men skillnaden var att de botnät som nu involverats var betydligt större. Totalt räknar man med att botnät med betydligt fler än en miljon slavdatorer deltog i huvudattacken. Antalet deltagande datorer är dock, som alltid i dessa sammanhang, en relativt grov uppskattning. Den baseras på trafikflöden och påverkas bland annat av vilka bandbredder de attackerande datorerna disponerar.

Genom att man under huvudattacken hade vidtagit speciella skyddsåtgärder kunde effekten av attackerna minskas till en nivå betydligt lägre än vad som uppmättes vid den första stora, koordinerade attackvågen den 4 maj.

Mellan den 10 och 15 maj angreps även två estniska banker, Hansapank och SEB Eesti Uhisbank. Det skedde genom omfattande åtkomstattacker som under en begränsad tidsperiod helt slog ut deras verksamhet på Internet och blockerade deras kontakt med utlandet under något längre tid. Den 15 maj skedde ytterligare fokuserade attacker mot estniska myndighetsnät.

I massmedia har det även rapporterats om attacker mot det estniska telesystemet, och att åtminstone en publik televäxel slagits ut. Under de inledande dygnen i april skedde det omfattande telefonangrepp – försök att blockera estniska myndigheter genom telefonsamtal. Några lyckade tekniska attacker har dock inte rapporterats. Däremot skedde det försök att angripa mobiltelenät i Estland samt system som den estniska räddningstjänsten använder, något som hade kunnat få stora konsekvenser.

Det har heller inte framkommit några uppgifter om attacker mot Scada-system eller andra system för styrning eller övervakning av kritisk infrastruktur i Estland, exempelvis elnätet.

Attackernas omfattning, trafikmätningar

Angreppens totala omfattning har inte kunnat klarläggas helt. Resultat från trafikmätningar är kraftigt beroende av var mätpunkterna finns, och de mätningar som gjorts i Estland är av naturliga skäl de mest rättvisande. Ett antal sådana mätgrafer har offentliggjorts, och vi har haft tillgång till ytterligare uppgifter. Materialet räcker emellertid inte för att ge någon fullständig bild av omfattningen. Det står emellertid klart att det största attackerna skapat trafikflöden på runt 1 Gbps (Gigabit per sekund) gentemot målnäten.

Personer med bakgrund inom internationell operatörsverksamhet har uppgivit att attacker på flera Gigabit per sekund inte är ovanliga idag. Samma källor uppger att attackerna mot Estland inte innehöll något tekniskt nytt, men att situationen förvärrades genom att nätförbindelserna i landet inte klarade riktigt stora, uthålliga trafikflöden.

Att det historiskt förekommit större attacker hade inte så stor betydelse ur estniskt perspektiv. För Estland var attackerna massiva och utgjorde en kraftig belastning på internationella förbindelser och interna nätresurser. Under de största attackvågorna tog man till trafikfiltrering och andra åtgärder. Men det var också nödvändigt att söka hjälp utifrån med att strypa flödena så nära källorna (de attackerande datorerna) som möjligt.

I mitten av maj publicerades företaget Arbor Networks en rad uppgifter om attackerna på en blogg. Arbor Networks driver ett trafikövervakningsverktyg med mätpunkter

utplacerade över hela Internet. På bloggen rapporterades att man detekterat totalt 128 unika DDoS-attacker mot estniska webbplatser. Av dem bestod 115 attacker av ping-flodning, 4 av SYN-flodning och 9 av andra attackslag. Mest drabbade var parlamentet och premiärministerns webbplatser (36 attacker), den estniska polisen (35 attacker) och estniska finansministeriet (35 attacker). Den dominerande andelen attacker företaget såg var mindre än en timme långa och genererade trafikflöden på maximalt 30 Mbps. En fjärdedel av attackerna var dock större, och de tio allra största attackerna beräknades till 90 Mbps och hade utsträckningar på upp till 10 timmar.

Officiella estniska reaktioner

Nätattackerna ledde till omfattande skriverier i massmedia och fackpress över hela världen. Från estnisk sida pekade man i förstone ut Ryssland som angripare, men tog snabbt tillbaka anklagelsen sedan det visat sig mycket svårt att peka ut någon enskild angripare. I den mån ursprunget kunde spåras pekade spåren mot datorer spridda över hela världen.

Angreppen ledde också till att man från estnisk sida gjorde ett utspel gentemot NATO där man ville föra upp frågan om nätangrepp (cyberattacker) på den säkerhetspolitiska agendan genom att hävda att sådana angrepp borde infogas i NATOs avtalstext om ömsesidigt militärt bistånd. Detta togs även upp under NATO-möten i juni och diskussionen fortgår inom organisationen.

I slutet av september efterlyste Estlands president Hendrik Ilves även en FN-konvention mot cyberkrigföring och cyberterrorism i ett tal inför FNs generalförsamling.

Rysk aktivism som påverkansfaktor

Flera nya politiska rörelser har under de senaste två åren förändrat den inrikespolitiska spelplanen i Ryssland. Den radikala, Putin-trogna nasji-rörelsen ("vi", "oss") är av speciellt intresse, eftersom dess medlemmar har kopplats till flera händelser som har anknytning till nätattackerna mot Estland.

Det var nasji-aktivister som utsatte Estlands ambassad i Moskva för en blockad i samband med kravallerna i Tallinn. Aktivisterna spände bland annat upp en stor banderoll föreställande bronsstatyn framför ambassadbyggnaden, rev ner den estniska flaggan och hamnade i handgemäng med den estniska ambassadörens livvakter. I samband med blockaden ofredades även den svenske ambassadören i samband med att han lämnade den estniska ambassadbyggnaden i bil och under en kort stund fastnade i folksamlingen.

En nasji-kommissarie uppges ha träffat en ledande rysk-etnisk oppositionspolitiker i Tallin den 20 april, precis en vecka innan kravallerna utbröt och nätattackerna inleddes.

En nasji-företrädare trädde den 2 maj fram i media och berättade att han själv deltagit i nätattackerna mot Estland, och att de skulle ha skett från en plats i utbrytarregionen Transdniester i Moldavien. Samtidigt dementerade han att den ryska administrationen skulle ha varit delaktig.

I direkt anslutning till bronsstatyn har estniska myndigheter vid upprepade tillfällen gripit (och sedermera utvisat) ryska ungdomar som i tyst protest posterat sig vid statyn i gamla ryska uniformer. Under en period om två månader skedde sådana gripanden vid åtminstone sju olika tillfällen.

Slutsatser – händelserna i Estland

Händelserna i Estland visar med tydlighet att koordinerade nätangrepp inte längre är någon avlägsen vision, utan kan användas redan idag som ett verksamt medel för politisk påverkan. En angripare eller grupp av angripare kan utan stora problem iscensätta attacker som stör den normala verksamheten för myndigheter och näringsliv i ett annat land – och dessutom dölja sin egen medverkan i angreppet.

Händelserna i Estland har också visat att det går att försvara sig mot nätangrepp. Det är emellertid viktigt att skaffa sig manöverförmåga genom att snabbt organisera sig och förbereda motåtgärder som kan begränsa effekterna.

En kritisk faktor i detta sammanhang visade sig vara förmågan att snabbt få fram en tillförlitlig lägesbildsfunktion genom att upprätta en nationell stab med medverkan från många samhällssektorer. Även om attackerna skedde via Internet berörde de verksamheter på många samhällsområden, från skolor i glesbygd till rikskspridda massmedia, banker och centrala myndigheter.

Tekniskt var det också väsentligt att ha tillgång till trafikmätningar på strategiskt valda platser i de egna näten, vilket man fick tillgång till dels från den sammanhållna nätmiljö Estlands myndigheter utnyttjar, dels från inhemska nätoperatörer.

En annan kritisk faktor var internationell samverkan. Incidenthanteringsorganet CERT-EE hade ett internationellt kontaktnät och kontaktade snabbt sina samarbetspartner i andra länder för att få assistans i arbetet med att strypa trafiken från datorer som användes i attackerna. Redan inom något dygn hade omvärlden larmats, och några dygn senare spreds mer detaljerade uppgifter som hjälpte operatörer över hela världen att filtrera onormalt stora trafikflöden riktade mot målsystem i Estland.

Del 2

Konsekvenser av nätangrepp mot Sverige

Inledning

Nätattackerna mot Estland har givit estniska myndigheter och privata aktörer praktisk erfarenhet av att hantera ett storskaligt nätangrepp. Medias flitiga rapportering kring händelserna bidrog även till en ökad medvetenhet hos omvärlden om att koordinerade nätangrepp inte längre tillhör framtiden. Vi har tagit de estniska erfarenheterna som utgångspunkt för att analysera svenska sårbarheter och de konsekvenser som skulle kunna uppstå om Sverige blev utsatt för ett liknande angrepp.

För att underlätta läsförståelsen och för att få ett tydligare samband mellan den estniska delrapporten och den svenska delen av rapporten har vi listat de utmärkande dragen i den estniska delrapporten:

Utmärkande drag för händelserna i Estland:

Bakgrund – Redan innan nätattackerna skedde i Estland hade det i samhället byggts upp någon form av aggressioner.

Syfte – Troligen fanns det ingen ekonomisk bakomliggande orsak till attackerna. De har istället förklarats som politiskt ideologiska, till viss del ett slags "cyberriots", alltså demonstrationer från gatan som flyttat ut på nätet

Förlopp – I ett inledande skede handlade det främst om enkla åtkomstattacker som sedan gick över till mer sofistikerade och välkoordinerade attacker som involverande stora botnät.

Mål – Myndigheter, politiska webbplatser och media blev angripna men även banker, små kommuner och landsortsskolor. I media talades det även om attacker mot det estniska telesystemet utan att några lyckade försök rapporterades. Försök gjordes även att angripa mobilnät och systemet som används av den estniska räddningstjänsten.

Försvårande faktor – Läget förvärrades förmodligen av att de estniska nätförbindelserna inte klarade av riktigt stora och uthålliga trafikflöden.

Nyckelfaktorer för en effektiv hantering:

Organisering av motåtgärder – En förmåga att snabbt kunna organisera sig har visat sig vara mycket betydelsefull i syfte att planera motåtgärder för att begränsa effekterna av en eventuell attack.

Etablerande av stab – För att så tidigt som möjligt kunna bilda sig en övergripande lägesbild är det nödvändigt att representanter från olika berörda delar av samhället snabbt kommer på plats i stabsliknande funktioner.

Tekniska data – För att kunna hantera ett större angrepp krävs tillgång till trafikmätningar från strategiskt valda platser i de egna näten. I Estland underlättades detta tack vare myndigheternas samlade nätmiljö samt nära samarbete med inhemska nätoperatörer.

Internationell samverkan – Goda kontakter med andra aktörer även utanför landets gränser har visat sig vara nödvändiga för möjligheten att kunna strypa trafiken nära datorer som används i attacker.

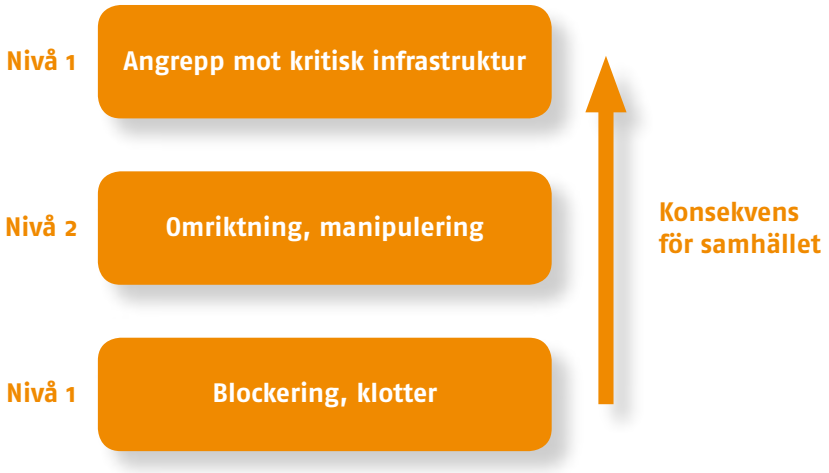
Möjliga hot och hotnivåer

Nätangrepp av det omfattande slag som drabbade Estland våren 2007 har hittills inte inträffat i Sverige. Frågan om huruvida någonting liknande skulle kunna ske här är inte helt enkel att besvara. Den övergripande säkerhetspolitiska situationen skiljer sig åt mellan länderna, de potentiella hotbilderna likaså. Händelserna ger oss likväl anledning att fundera över vilka konsekvenser ett eller flera liknande nätangrepp skulle få om de riktades mot samhällsfunktioner i Sverige.

I den här framställningen utgår vi helt från storskaliga antagonistiska hot, alltså angrepp som iscensätts av en eller flera aktörer med intention och förmåga att skada vitala samhällsfunktioner i landet. Vi bortser från kriminella angrepp av begränsad omfattning samt driftstabilitet, frågor som helt hanteras inom ramen för polisiärt arbete respektive myndighetsansvaret för internetsäkerhet.

Nätangrepp kan iscensättas på en rad olika sätt. Det kan ske åtkomstattacker som syftar till att begränsa tillgången till datorresurser, exempelvis e-postsystem och webbplatser. Det kan ske intrång som syftar till att störa driften, förändra information eller helt ta över ett informationssystem. Det finns även en kategori av nätangrepp som syftar till att störa eller slå ut samhällsviktig infrastruktur av helt annat slag än informationssystemen i sig, exempelvis telenät, elnät, vattenrening, processindustrier och liknande.

Angreppsformerna kan graderas efter vilka potentiella konsekvenser ett lyckat angrepp kan få på samhället och därefter placeras i några distinkta hotnivåer. Dessa nivåer är väsentliga att ha i åtanke i ett resonemang kring samhällets förmåga att hantera nätangrepp.



Nivå 1 – Blockering och klotter

Nivå 1

Här handlar det dels om attacker med syfte att blockera åtkomsten till informationsresurser, så kallade åtkomst-attacker (denial-of-service), dels begränsade intrång på främst webbplatser med syfte att demonstrera målobjektens bristande säkerhet (defacements). Det senare sker ofta i kombination med publicering av tydliga signaturer (tags) och nedsättande eller fientliga kommentarer.

Attacker på denna nivå är ofta relativt enkla att utföra, och när motivbilden involverar aktivism är målobjektet ofta av symboliskt viktig karaktär. Ibland utförs defacements i stort antal – inte minst i samband med konflikter mellan hackare eller hackargrupper. När information manipuleras på denna nivå är den relativt enkel att detektera.

Nivå 2 – Omriktning, manipulering

Nivå 2

Här handlar det dels om attacker där nätanrop, referenser eller signaturer manipuleras på ett sådant sätt att trafik kastas bort, leds fel eller information felaktigt bedöms som tillförlitlig, dels mer avancerade intrång där syftet är att överta målsystem och manipulera information i bedrägligt syfte.

Attacker på den här nivån har ett högre syfte än att demonstrera angriparens förmåga. Här sker manipulering av information, exempelvis genom att publicera falska myndighetsmeddelanden, falska nyheter, leda om trafik till en förfalskad webbplats eller internetbank, lura av användare inloggningsuppgifter, annonsera falska vägval (routes) i nät eller helt överta en eller flera myndighetsdatorer.

På den här nivån ställs det betydligt högre krav på angriparens förmåga än på nivå 1. Metoderna har ofta nära koppling till dem som används inom avancerad nätkriminalitet, exempelvis riktad spridning av skadlig kod (malware) via trojaner eller manipulerade webbsidor, utnyttjande av botnät eller avancerad exploatering av säkerhetshål genom sk exploits.

Attackmetoderna på denna nivå kan ge en angripare möjlighet att genomföra regelrätta psykologiska informationsoperationer (psyops, perception management) där falsk eller delvis förfalskad information hjälper angriparen att uppnå sina mål.

Nivå 3

Nivå 3 – Riktade angrepp mot kritisk samhällsinfrastruktur
Här handlar det om attacker mot informationssystem som styr anläggningar av vital betydelse för samhället, till exempel elnät, kärnkraft, vattenförsörjning, järnvägsnät, vägsignalering och liknande. Dessa system kallas ofta med ett samlingsnamn för SCADA-system (Supervisory Control and Data Aquisition).

Det rör sig här i allmänhet om mycket specialiserade informationssystem, grupperade kring industriella styrsystem, inte sällan helt specialtillverkade lösningar. Angrepp på denna nivå ställer normalt mycket stora krav på angriparens förmåga, men effekten av ett lyckat angrepp på ett informationssystem av denna typ kan få mycket svåra konsekvenser för samhället.

Från samhällets sida är det naturligtvis viktigt att göra en väl avvägd prioritering i arbetet med att hantera incidenter av ovan nämnda slag. Något förenklat kan sägas att attacker på nivå 1 visserligen är irriterande, skapar tillfälligt bortfall av nätresurser, prestigeförlust och kanske intäktsbortfall – men inte behöver innebära något allvarligare hot mot samhället än just temporär driftstörning. Det är först på nivå 2 och 3 som angrepp kan få allvarligare konsekvenser för samhället.

Attacker på nivå 3 kan få mycket stora konsekvenser och ibland ge närmast irreparabla skador vad gäller kritisk infrastruktur. I många länder har skyddsåtgärder på denna nivå kraftigt prioriterats. Bland de svenska myndigheterna är det framför allt Säkerhetspolisen och Krisberedskapsmyndigheten som studerar denna typ av hot.

Internet i Sverige

Uppbyggnad och spridning

Internet i Sverige baseras på ett antal stora och fysiskt åtskilda stamnät som hanteras av privata nätoperatörer. Flera av dem har egna internationella förgreningar och egna förbindelser med andra operatörer. Internetoperatörerna utbyter trafik dels direkt med varandra, dels i knutpunkter belägna i Sverige eller i utlandet.

I Sverige finns flera knutpunkter som förmedlar stora trafikmängder. Dessa drivs av företaget Netnod, som ägs av Stiftelsen för Internetinfrastruktur. Syftet med knutpunkterna är att underlätta trafikutbytet och skapa en stabil och robust infrastruktur i de centrala delarna av Internet i Sverige. Detta förstärks genom att knutpunkterna finns på skyddade driftplatser. Utbytet av Internettrafik sker på fem platser: i Stockholm, Göteborg, Malmö, Sundsvall och Luleå. Trafikutbytet i de olika städerna är oberoende av varandra.

Netnod arbetar i nära samarbete med Svenska Internetoperatörers Forum (SOF) som främst samlar de operatörer som har direktkoppling till de nationella Internetknutpunkterna. SOF jobbar även med frågor kring samtrafik samt andra funktioner och driftfrågor som är nödvändiga för att Internet i Sverige ska fungera bra[1]. Under år 2000 skapade Netnod ett driftbolag, Autonomica, som förutom driften av Internetknutpunkterna i Sverige även sköter en av de 13 rotnamnservrarna i Internets katalogsystem DNS (Domain Name System). Rotnamnservern ligger utspridd på 26 platser i världen men styrs från Stockholm[2].

[1] http://www.isoc.se/sajt/bilder/pdf/vem%20g%C3%B6r%20vad.pdf
[2] http://www.netnod.se/

Någon samlad nätinfrastruktur för myndighetsnät finns inte i Sverige. De svenska myndigheterna ansvarar själva för sina IT-system och förbindelser med omvärlden. Det sätt på vilket Estland samlat sina myndighetsnät i en homogen och väl skyddad nätmiljö saknar motsvarighet i Sverige.

I Sverige finns det idag cirka 2,5 miljoner bredbandsabonnemang, vilket motsvarar ungefär hälften av alla hushåll. Antalet abonnenter med Internetanslutning med kapacitet att hantera minst 2 Mbit/s nedströms (i riktning till abonnent) uppgick i december 2006 till drygt 1,5 miljoner, vilket motsvarar två tredjedelar av alla abonnemang med fast anslutning.

En ökning av antalet Internetaccesser med betydligt snabbare hastigheter än 2 Mbit/s har också skett. Andelen abonnemang med fast anslutning till Internet har koncentrerats till sex stora Internetleverantörer som har nära 90 procent av marknaden (2007). Det totala antalet företag som erbjuder bredbandsabonnemang är drygt 170[3].

Idag kan 75 procent av de grundläggande offentliga tjänsterna i Sverige utföras elektroniskt, det vill säga att den elektroniska ärendehanteringen finns tillgänglig via Internet. Sverige har satsat på att få hög kvalitet i tjänster från de stora myndigheterna, snarare än lokala och regionala tjänster[4].

Det finns idag en nationell toppdomän för Sverige, .se. Stiftelsen för Internetinfrastruktur (II-stiftelsen) har ansvaret och har till uppgift att utveckla och sköta driften av toppdomänen. Antalet aktiva domäner på .se är idag drygt 676 000[5].

[3] http://www.pts.se/Archive/Documents/SE/Bredband_i_Sverige_2007.pdf
[4] http://www.capgemini.com
[5] http://www.iis.se

De flesta operatörers nät övervakas från egna centraler, där det finns egen incidenthanteringsfunktion och en abuse-avdelning som är aktiv dygnet runt. Det finns även funktioner för intrångsdetektering som är igång dygnet runt, liksom logiska agenter i nätet, sk prober eller sensorer, som kan skickar larm om onormalt trafikflöde vid exempelvis åtkomstattacker. Man försöker vid sådana tillfällen spåra den störande källan och filtrera bort dess trafik. Vissa operatörer har kontakter med externa incidenthanteringsfunktioner, bland annat andra inhemska operatörers motsvarande grupper, för att tidigt få varningar om pågående angrepp och för att upptäckta säkerhetshål[6].

[6] http://www.pts.se/Archive/Documents/SE/Ar%20Internet%20i%20Sverige%20robust.pdf

Offentlig ansvarsfördelning

Ansvarsfördelning på departementsnivå

Arbetet med informationssäkerhet i Sverige styrs av ansvarsprincipen vilket innebär att myndigheter, företag och organisationer som har det normala verksamhetsansvaret även har ansvar för informationssäkerheten.[7] Principen gäller även på departementsnivå, vilket innebär att myndighetshandläggare på de olika departementen sköter informationssäkerhetsfrågor för respektive myndighet. Informationssäkerhet är dock ett bland många områden som ligger på handläggarnas bord.[8] Det finns därmed inget särskilt departement som ansvarar för informationssäkerhetsfrågor. Däremot har vissa departement fått samordningsansvar för specifika frågor. Ett exempel är elektroniska kommunikationer, vilket Näringsdepartementet har ansvar för. Vidare har ett antal expertmyndigheter (Försvarets Radioanstalt, Krisberedskapsmyndigheten, VERVA, Post- och telestyrelsen, Försvarets Materielverk, Polisen och Försvarsmakten) givits särskilt ansvar inom olika segment av informationssäkerhetsområdet.

Regeringen har dock hittills inte samordnat informationssäkerhetsfrågorna inom regeringskansliet för att alla departement ska ha samma information/uppfattning om hot, risker, sårbarheter och behovet av åtgärder inom området (se avsnittet sid 26 om Riksrevisionens granskning av regeringens styrning). I ett sådant arbete skulle högre krav kunna ställas på expertmyndigheterna på området om att producera relevant och användbar information som kan ligga till grund för beslutsfattande.

[7] Prop 1999/2000:30, Det nya försvaret
[8] "Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen", RIR 2007:10, s 47

Ansvarsfördelningen bland svenska myndigheter

Som tidigare nämnts är alla myndigheter skyldiga att sörja för att det existerar en tillräcklig informationssäkerhet inom deras egen verksamhet. Men vissa myndigheter arbetar mer direkt med informationssäkerhet än andra.

Polisen

Rikspolisstyrelsen (RPS) har via Rikskriminalpolisen (RKP) skapat en IT-brottsenhet som består av fyra grupper. De ingår i nätverk av IT-experter både internationellt vid Interpol och G8:s kontaktlista samt nationellt med kontaktpersoner inom ämnesområdet. Vid Säkerhetspolisen (Säpo) har säkerhetsskyddsenheten ett särskilt tillsynsansvar enligt säkerhetsskydds-lagstiftningen vad gäller viktiga samhällsfunktioners skydd mot IT-angrepp, och där analyseras kontinuerligt IT-relaterade incidenter, hot och sårbarheter.

När det gäller att skapa en helhetsbild kring incidenter har RKP tillsammans med Säpo bildat en samordningsfunktion för brottsrelaterade IT-incidenter (S-BIT). Det är en ingång för den som behöver komma i kontakt med polisen vid en misstänkt brottsrelaterad IT-incident. S-BIT fungerar även som en kontaktyta mot andra aktörer i samhället som har uppgifter inom informationssäkerhetsområdet.

Försvarsmakten

Försvarsmakten (FM) har ett tillsynsansvar enligt säkerhetsskyddsförordningen som omfattar Försvarshögskolan, Försvarets Materielverk, Totalförsvarets forskningsinstitut, Försvarets Radioanstalt, Fortifikationsverket och Pliktverket.

Övervakningen av FM:s egna nät utförs av Försvarsmaktens Computer Emergency Response Team (FM CERT). Övervakningen inriktas på att säkerställa sekretess, tillgänglighet, riktighet och spårbarhet i nätet. Försvarsmaktens telenät- och markteleförband (FMTM) har till uppgift att sköta

systemdrift och systemdriftsledning av FM:s gemensamma telekommunikationsinfrastruktur.

FM utövar i praktiken rollen som National Communications Security Authority (NCSA) samt National Distribution Authority (NDA) genom den militära underrättelse- och säkerhetstjänstens (MUST) säkerhetskontor. En del av de hot Försvarsmakten och dess tillsynsmyndigheter på informationssäkerhetsområdet ställs inför utgörs av främmande länders underrättelse- och signalspaningstjänster.

Försvarets materielverk och CSEC

Vid Försvarets Materielverk finns organisationen CSEC, Sverige Certifieringsorgan för IT-säkerhet, som arbetar med certifieringsstandarden Common Criteria (CC). Även om CSEC inte har något utpekad, operativ roll vid ett nätangrepp kan dess arbete få betydelse vid incidenthantering. Alla de certifieringsorgan som arbetar med Common Critera har nämligen omfattande dokumentation om produktegenskaper och sårbarheter i exempelvis programkod. I vissa fall skulle CSEC genom sitt kontaktnät kunna få tillgång till sådan information som kan underlätta felsökning och avhjälpning av kritiska fel.

Försvarets radioanstalt

Försvarets radioanstalt (FRA) ska stödja insatser med IT-inslag vid nationella kriser, medverka till identifiering av inblandande aktörer vid IT-relaterade hot mot samhällsviktiga system, genomföra IT-säkerhetsanalyser, ge tekniskt stöd till myndigheter och statligt ägda bolag, tillhandahålla signalskyddsverksamhet med kryptologisk behörighet samt upprätthålla en hög teknisk kompetens på informationssäkerhetsområdet.

FRA ska efter begäran assistera myndigheter och statligt ägda bolag som förvaltar information som anses känslig ur ett sårbarhetsperspektiv eller ur ett säkerhets- eller försvarspolitiskt perspektiv. Uppdraget begränsas dock till statligt ägda bolag som bedriver samhällsviktig verksamhet. FRA har i uppgift att säkerställa att sakkunskapen finns att

tillgå på det nationella planet. FRA bistår Säpo i tillsynen i enlighet med säkerhetsskyddslagstiftningen.

Post- och telestyrelsen samt Sitic

Inom informationssäkerhetsområdet har Post- och telestyrelsen (PTS) ett ansvar som bland annat följer av lagen om elektronisk kommunikation (2003:389). Det avser till exempel krav på god funktion och teknisk säkerhet samt integritetsskydd i elektronisk kommunikation som telefoni, mobiltelefoni och Internet. PTS strävar efter att åstadkomma robustare och driftsäkrare nät samt förhindra att näten slås ut under störningar. Myndigheten utreder och informerar även på området Internetsäkerhet.

Sveriges IT-incidentcentrum (Sitic) är en del av PTS. Sitics uppgift är att fungera som en nationell central för rapportering av IT-incidenter samt en resurs för stödjandet av samhällets skydd mot IT-incidenter. Sitic sprider information om nya problem som kan komma att störa IT-aktiviteter samtidigt som de ger råd om förebyggande åtgärder och sammanställer statistik.

Sitic samverkar med ett antal nationella och internationella organisationer för att kunna agera operativt vid en incident. Sitic är medlem i FIRST, som är ett internationellt forum för betrodda CSIRT:s som tillsammans hanterar IT-säkerhetsincidenter och uppmuntrar förebyggande åtgärder inom området genom att utveckla och utbyta teknisk information, verktyg, metoder, processer och "best practices".[9]

Sitic är också medlem i EGC som är en informell grupp bestående av europeiska systerorganisationer. Dess syfte är att utveckla effektiv samverkan inom informationssäkerhetsområdet genom att ta fram åtgärder för att hantera större IT-säkerhetsincidenter som kan få effekter över nationsgränserna, utbyta information och teknik relaterat till IT-säkerhetsincidenter, skadlig kod och sårbarheter samt identifiera kompetenser och expertis som kan avropas inom gruppen[10].

[9] www.sitic.se
[10] http://www.egc-group.org

Krisberedskapsmyndigheten

Krisberedskapsmyndigheten (KBM) har det sammanhållande myndighetsansvaret för frågor rörande samhällets informationssäkerhet, vilket även inbegriper mer omfattande nätincidenter som kan påverka stabiliteten hos det svenska samhället.

Varken KBM eller någon annan myndighet har något utpekat ansvar för nationell ledning av arbetet med informationssäkerhetsfrågor. Däremot leder KBM myndighetssamarbetet SAMFI (Samverkansgrupp För I nformationssäkerhet) där Post- och telestyrelsen/Sitic, Försvarsmakten, Verva, Rikspolisstyrelsen och Försvarets Materielverk ingår.

KBM arbetar också aktivt med samverkansprojekt mellan stat och näringsliv, bland annat på SCADA-området. Internationellt utgör KBM också Sveriges nationella kontaktpunkt för informationssäkerhetsfrågor.

2006 fick KBM tillsammans med Statens Räddningsverk ett uppdrag att förbereda och påbörja inrättandet av en lägesbildsfunktion i syfte att snabbt kunna upptäcka allvarliga händelser, varsko berörda aktörer och kunna ge en samlad nationell lägesbild och tvärsektoriell analys. I händelse av omfattande hot mot teknisk infrastruktur, som exempelvis ett omfattande nätangrepp skulle innebära, har KBM rollen att sammankalla strategiska aktörer till en stabsfunktion. Dessa aktörer är i första hand de myndigheter som ingår i samarbetsorganet SAMFI (se nedan). Skulle detta scenario utvecklas aktiveras KBM:s lägescentral för att följa läget och sammanställa en aktuell lägesbild. Det ingår också i KBM:s uppdrag att analysera konsekvenserna av den inträffade händelsen, både på kort och lång sikt, samt att ge förslag på tänkbara åtgärder. Vidare ska KBM informera departementet och andra berörda aktörer om den aktuella lägesbilden. När det rör hot mot teknisk infrastruktur är det naturligt att lägescentralen bemannas med stöd från såväl KBM som andra aktörer, exempelvis Sitic och FRA.

Samverkan

SAMFI

Samverkansgruppen för informationssäkerhet (SAMFI) är ett samarbetsorgan för myndigheter med informationssäkerhetsrelaterad verksamhet. Det bildades år 2003 mot bakgrund av regeringens då nya strategi för samhällets informationssäkerhet som föreslagits i propositionen Samhällets säkerhet och beredskap (2001/02: 158). SAMFI består av Krisberedskapsmyndigheten, Post- och telestyrelsen, Försvarets Radioanstalt, Försvarets Materielverk, Polisen/Säkerhetspolisen (via S-BIT), Försvarsmakten och Verva. Krisberedskapsmyndigheten är sammankallade myndighet.

Genom informationsutbyte och samverkan stödjer SAMFI de medverkande myndigheternas arbete. Till vardags agerar organet huvudsakligen inom områden såsom strategi och regelverk, tekniska frågor och standardiseringsfrågor, nationellt och internationellt agerande samt genom medvetandehöjande åtgärder. Vid händelser av större samhällsbetydelse har SAMFI potential att fungera som ett nationellt, strategiskt ledningsstöd till de enskilda myndigheterna.

Övriga samverkansforum

Det finns en mängd frivilliga formella och informella samverkansforum för informationssäkerhetsfrågor. Dessa forum har i många fall bildats med utgångspunkt från ett gemensamt intresse och är därför naturligt uppdelade sektorsvis. Ett exempel på detta är Nationella Telesamverkansgruppen (NTSG) som bildades i augusti 2005 och är ett frivilligt samarbetsforum för teleoperatörer eller andra organisationer med egen teknisk utrustning. Syftet är att stödja återställandet av den nationella infrastrukturen för elektroniska kommunikationer vid extraordinära händelser i samhället. Dessa operatörer/organisationer har genom sin roll möjlighet till stor påverkan på den kritiska nationella infrastrukturen för elektronisk kommunikation[11].

[11] www.telesamverkan.se

Det förekommer också samverkan mellan svenska underrättelsemyndigheter avseende hotbildsbedömningar och händelser i omvärlden. I denna krets ingår bland annat MUST, Försvarets Radioanstalt och Polisen.

Sårbarheter i svenska grenen av Internet

Nätinfrastrukturen

Stamnätsinfrastrukturen i Sverige kännetecknas av hög kapacitet, operatörsnät som i åtskilliga fall sträcker sig utanför rikets gränser och har många förbindelser med omvärlden. Risken för att den svenska grenen av Internet skulle blockeras helt genom åtkomstattacker får därför betecknas som relativt liten.

Den internationella sammanflätning som skett minskar dock samtidigt möjligheten att isolera "Sverige" från resten av Internet, vilket skulle kunna vara önskvärt vid omfattande globala störningar på nätet, eller i en säkerhetspolitisk situation där vi av någon anledning önskar begränsa trafikutbytet med omvärlden, eller åtminstone öka kontrollen över trafikflöden in och ut ur landet. För närvarande är det mycket svårt att avgöra exakt vilka stamnätsförbindelser som passerar gränserna. Detsamma gäller den totala trafikmängd som dessa förbindelser klarar av att förmedla.

Även de svenska accessnäten kännetecknas generellt av hög individuell kapacitet hos bredbandsförbindelserna till våra hushåll, vilket är en naturlig följd av den snabba teknikutvecklingen. Detta ger oss tillgång till en mängd nya tjänster, men det ökar också sårbarheten. När data, telefoni och radio/tv skickas över samma förbindelse kan en störning få allvarligare konsekvenser än när förbindelserna var separerade.

Den stora bandbredden hos hushållens Internetförbindelser innebär också nytt potentiellt hot mot viktiga samhällsfunktioner. Slagstyrkan hos ett botnät av infekterade hemdatorer kan bli mycket stor om alla system är anslutna till bredbandsförbindelser med hög kapacitet. Samlade i ett enda botnät skulle Sveriges 2,5 miljoner bredbandsanslutna hushåll i teorin kunna få en total kapacitet som är åtminstone 500 – 1000 gånger så stor som hos den största attackvåg som kunde observeras i Estland.[12]

[12] Vi räknar här med att varje bredbandsförbindelse klarar att förmedla minst 200 kbit per sekund "uppströms" (i riktning från hushållet, ut på Internet) samt att det inte finns några flaskhalsar i operatörernas stamnät som begränsar det totala trafikflödet. Det senare torde i praktiken begränsa effekten.

En faktor som förstärker detta hot är att privatägda datorer ofta skyddas betydligt sämre mot skadlig kod och regelrätta intrång än datorer hos företag och myndigheter. Oftast saknas den kompetens och de rutiner som krävs för att bibehålla en hög säkerhet, till exempel genom att uppgradera programvara ofta, täta till alla säkerhetshål och undvika förinstallerade lösenord.

Stamnätsinfrastrukturen kan utsättas för trafikstockningar (congestion) i samband med åtkomstattacker. Även e-postservrar placerade hos operatörer kan överbelastas, även om detta problem minskat radikalt på senare år. Nätutrustningar kan störas, i vissa fall även slås ut eller övertas genom riktade intrång. Bland personer som arbetar med internetsäkerhet är dessa effekter välkända, och inom standardiseringsorganet IETF arbetar man sedan länge aktivt med att komma till rätta med både existerande och potentiella problem. Två av de grundfunktioner som anses speciellt kritiska på Internet är katalogtjänsten DNS och gränsrouting (BGP-routing).

Det globala DNS-systemet har hittills utsatts för två omfattande attackförsök som kraftigt stört delar av systemet men inte lyckats slå ut det. Under 2002 drabbades ett antal av de 13 så kallade rotserversystemen av kraftiga störningar. Attackerna ledde till att man förstärkte DNS-systemet, och vid ett förnyat attackförsök i februari 2007 lyckades angriparna enbart allvarligt störa driften hos tre rotserversystem. De system som distribuerat sin drift till många servrar spridda världen över klarade sig generellt väl.

Idag får DNS-systemet sägas vara mycket robust. Detta gäller även DNS-infrastrukturen i Sverige, inklusive den svenska toppdomänen .se som förvaltas av Stiftelsen för Internetinfrastruktur. Sårbarheterna i den svenska delen av DNS-systemet ligger idag inte på operatörsnivå utan huvudsakligen hos de domännamnsägare som själva förvaltar sina domäner.

Några mer omfattande attacker mot den globala gränsroutingen har inte skett hittills, varken utomlands eller i Sverige. Vid sidan om kommersiella avtal om trafikutbyte

bygger systemet till stora delar på förtroenden i det internationella operatörssamarbetet. Inom IETF har man börjat inventera de attackmöjligheter som finns och säkra det meddelandeutbyte som görs, men mycket återstår att göra.

Vad som däremot utgör en tydlig sårbarhet är det begränsade antal personer i Sverige som besitter den operativa erfarenhet som krävs för att hantera omfattande och tidsmässigt utdragna nätincidenter. Dessa personer finns huvudsakligen hos nätoperatörerna och knutpunktsbolaget. Situationen är densamma på många håll i världen.

I den vardagliga driften fungerar den svenska Internetinfrastrukturen väl, och begränsade incidenter kan hanteras av nätoperatörerna själva och det fristående knutpunktsbolaget, utan ytterligare stöd från staten. Men vid mycket omfattande incidenter av samhällshotande karaktär är det möjligt att det kommer att krävas mer mankraft, och då främst personer med erfarenhet av de speciella uppgifter som kan bli aktuella, exempelvis analys av trafikdata. Att se till att denna kompetens upprätthålls och finns tillgänglig i en tillräckligt vid krets av personer skulle kunna utgöra ett bidrag från samhället till en i övrigt väl fungerande Internetinfrastruktur.

Myndighetsnät och offentliga webbplatser

Nästan alla svenska myndigheter är idag Internetanslutna. Åtskilliga av dem tillhandahåller medborgartjänster och tjänster gentemot företag och andra intressenter i samhället. Omfattningen av denna verksamhet kommer sannolikt att öka under de närmsta åren, inte minst mot bakgrund av initiativet med den så kallade 24-timmarsmyndigheten som syftar till att få myndigheter att dygnet runt tillhandahålla e-tjänster till medborgarna.

Myndigheters nät kan drabbas av angrepp på flera olika nivåer. Webbplatser kan drabbas av åtkomstattacker och

defacements, e-postservrar kan blockeras. Den information i DNS-systemet som pekar ut var myndigheternas tjänster finns kan under vissa förutsättningar manipuleras. Dessutom kan datorer inne i myndigheternas interna nät drabbas av riktade angrepp, exempelvis med skadlig kod som inte är tidigare känd och därmed inte går att detektera. Svenska företag har redan drabbats av sådana angrepp, och det är inte osannolikt att ett bredare, planerat angrepp på nivå 2 kommer att beledsagas av sådana, riktade attacker.

Sårbarheten hos ett myndighetsnät beror bland annat på hur det är anslutet till Internet och hur olika resurser (exempelvis webbplats eller e-postserver) annonseras på nätet. En inledande inventering av hur myndigheter använder sig av Internets katalogsystem DNS har nyligen utförts. Den kommer troligen att kompletteras framöver med en genomgång av hur viktigare myndigheter går att nå, genom en kartläggning av operatörer och viktigare nätanslutningar.

Under september 2007 genomförde KBM och Stiftelsen för Internetinfrastruktur (.SE) en gemensam kartläggning av hur DNS används av svenska myndigheter och andra samhällsviktiga organisationer. Undersökningen omfattade drygt 800 olika aktörer och resulterade i ett antal mycket intressanta iakttagelser som finns redovisade i en rapport. Kartläggningen visar på ett stort antal direkta fel och brister i hanteringen hos aktörerna vad det gäller DNS-system. Sannolikt visar resultatet på att det behövs mer kunskap om DNS-systemet hos aktörerna.[13]

En av de mest framträdande bristerna visade sig vara att drygt 10 procent av namnservrarna körs med gammal programvara, vilket gör det enkelt att bryta sig in i datorn och rikta om webbtrafik och e-post till falska adresser. 40 procent av namnservrarna tillät dessutom en funktion som kallas öppen rekursion, vilket innebär att de kan utnyttjas i åtkomstattacker. Många verksamheter hade dessutom alltför få, alltför koncentrerade eller felaktigt inställda namnservrar.

[13] "Nåbarhet på nätet, hälsoläget i .SE 2007" .SE, KBM

Värt att notera är också att få svenska myndigheter idag använder möjligheten att verifiera e-post genom funktioner som SPF (Sender Policy Framework) eller möjligheten att säkerställa informationen om sin internetdomän genom digitalt källskydd (signering). Det senare innebär att det i ett krisläge kan bli svårt att verifiera om den information en myndighet sprider på Internet verkligen kommer från den myndigheten eller från en falsk avsändare.

Signering av domäner i domänsystemet DNS åstadkommer man med tekniken DNSSEC (DNS Security Extensions). Det är emellertid mycket få svenska aktörer som hittills börjat använda tekniken. Post- och telestyrelsen och Stiftelsen för Internetinfrastruktur arbetar aktivt med att öka användningen, och detta kan betraktas som ett mycket viktigt arbete för att stärka integriteten bland svenska nätdomäner. Stiftelsen begärde dessutom nyligen att det internationella domänorganet ICANN ska signera den översta så kallade rotzonen i DNS-systemet.

En revision av hur myndigheter sköter sin interna informationssäkerhet genomfördes under 2005 och 2006 av Riksrevisionen, och sammanfattades i en rapport tidigare i år. Det saknas fortfarande en fullständig inventering av de svenska myndigheternas nättjänster, en prioritering som visar vilka tjänster som kan betraktas som särskilt samhällsviktiga samt en genomgång av hur dessa skyddas mot nätangrepp på nivå 1 och 2.

För de myndigheter på vilka det ställs särskilda krav enligt säkerhetsskydds-lagstiftningen är Säkerhetspolisen tillsynsmyndighet. Där görs regelbundna granskningar, och man har även ett väl fungerande operativt samarbete med den öppna polisen. Säkerhetspolisen arbetar dessutom aktivt med att kartlägga de system som kan vara sårbara för angrepp på nivå 3.

En påtaglig brist är dock att det hittills saknats enhetliga säkerhetskrav på myndigheternas nättjänster i form av föreskrifter, särskilt sådana krav som stärker myndigheternas förmåga att motstå yttre angrepp på olika nivå.

Från och med den 1 januari 2008 kommer dock en ny föreskrift från Verva angående informationssäkerhet att träda i kraft. VERVA har beslutat att standarderna Ledningssystem för informationssäkerhet (SS-ISO/IEC 27001) samt Riktlinjer för styrning av informationssäkerhet (SS-ISO/IEC 27002) ska gälla i hela statsförvaltningen.

Ansvarsprincipen på informationssäkerhetsområdet fråntar inte staten ansvaret för att garantera att de statliga myndigheternas IT-användning uppfyller kraven på säkerhet. Det är en förtroendefråga gentemot både allmänheten och företagen.[14] Med anledning av detta har Riksrevisionsverket granskat regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen. Ett övergripande problem som framkommer i och med granskningen är avsaknaden av styrning och kontroll över myndigheternas arbete med informationssäkerhet.

Det finns stora brister även i myndigheternas arbete med informations-säkerhet och det uppges till stor del bero på att ledningen inte tar på sig det tillräckliga ansvaret för informationssäkerhetsfrågorna. Ofta saknas information om myndighetens skyddsvärda informationstillgångar. Det saknas också kontinuitetsplaner och personalen uppges många gånger sakna utbildning på området. Det är därmed inte överraskande att ledningarna i Riksrevisionens granskning uppges ha en oklar bild av de risker respektive myndighet står inför.[15]

Ett annat problem är otydlighet och okunskap om hur säkerhetsincidenter skall hanteras. Vilka incidenter skall rapporteras? Hur skall de dokumenteras och hur skall brister åtgärdas?

De brister som finns på myndigheterna skulle vid ett större nätverksangrepp troligen leda till svårigheter med att hantera det krisläge som uppstår.

[14] "Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen", RiR 2007:10, sid. 13
[15] "Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen", RiR 2007:10

Annan samhällsviktig informationsinfrastruktur

Svenska massmedia

Massmedia är troligen den samhällssektor i Sverige som, vid sidan om nätoperatörerna, idag hunnit skaffa sig den mest omfattande erfarenheten av kraftiga trafikavvikelser i sina Internetförbindelser. Det handlar dels om hantering av den onormalt tunga trafikbelastning som kan uppstå vid viktigare nyhetshändelser, dels regelrätta nätangrepp när någon individ eller samhällsgrupp retat upp sig på vad som publicerats.

Ett massmediums existens hänger på att ständigt vara tillgängligt. Därför har stora resurser också investerats i framför allt riksmediernas nyhetswebbar. Det är högst sannolikt att dessa i ett krisläge kommer att visa sig vara minst lika robusta, om inte mer, än många av de webbplatser som drivs av myndigheter.

Trots detta går det inte att utesluta att svenska massmedia kommer att bli särskilt drabbade i samband med ett större nätangrepp mot Sverige. I Estland drabbades rikspressen redan i den inledande attackvågen. Inga centraliserade webbplatser går idag att skydda helt mot riktade åtkomstattacker om de trafikmängder som riktas mot webbplatsen är tillräckligt stor för att överbelasta tillgängliga nätförbindelser. Visserligen byggs kapaciteten kontinuerligt ut, men samtidigt blir medieinnehållet också alltmer resurskrävande – liksom antalet användare med bredbandiga internetförbindelser.

Digitala kontrollsystem (SCADA)

Åtkomstattackerna mot Estland drabbade, enligt alla tillgängliga uppgifter, inte några datorbaserade system för styrning eller övervakning av kritisk infrastruktur (digitala kontrollsystem). För att kunna göra en kvalificerad bedömning av hur de svenska kontrollsystemen skulle ha klarat

en liknande attack som den mot Estland krävs mer detaljerade studier. Syftet med denna rapport är dock främst att belysa konsekvenserna för Internetinfrastrukturen och därför diskuteras problematiken kring säkerhet i digitala kontrollsystem endast från en mer generell utgångspunkt.

De digitala kontrollsystemen har traditionellt sett byggt på industriella protokoll och tekniker samt både varit fysisk och logiskt isolerade från andra nätverk. Dagens kontrollsystem görs i allt högre utsträckning tillgängliga via publika nätverk, använder allt mer samma tekniker som vanliga IT-system (Ethernet, TCP/IP och standardlösningar för databaser och OS) och integreras i viss utsträckning med administrativa informationssystem. Sammanfattningsvis så leder detta till en radikalt förändrad hotbild. Säkerhet i digitala kontrollsystem är därför ett område som har fått stor uppmärksamhet under de senaste åren och dessa frågor studeras både av industri och av stat.

Det krävs en ökad samhällelig beredskap för att hantera säkerheten i digitala kontrollsystem, speciellt med avseende på kvalificerade antagonistiska IT-angrepp riktade mot samhällsviktiga verksamheter. De grundläggande säkerhetsproblemen kan till stor del hänföras till beroenden mellan IT-system och fysiska försörjningssystem. Frågeställningen omfattar alltså både vad som brukar benämnas CIIP (Critical Information Infrastructure Protection) och CIP (Critical Infrastructure Protection). I dagsläget finns mycket få svenska aktörer med djupare teknisk kompetens inom området. Speciellt små och medelstora operatörer av samhällsviktig infrastruktur saknar såväl resurser som kompetens för att upprätthålla ett kvalificerat säkerhetsarbete. Eftersom området innehåller aspekter som är vitala ur nationellt säkerhetshänseende så är det även mycket viktigt att säkerställa att det finns en statlig kompetens inom området.

Mot bakgrund av ovanstående så driver KBM sedan 2005 ett arbete kring säkerhet i digitala kontrollsystem och myndigheten avser att permanenta och utöka detta

arbete från och med 2008. KBM avser att leda och finansierat ett sammanhållet statligt initiativ kring säkerhet i digitala kontrollsystem. Vidare information finns dels i den handlingsplan för informationssäkerhet som myndigheten för närvarande tar fram, dels i den separata rapport (Roadmap) som beskriver hur det praktiska arbetet planeras att genomföras.

Svensk incidenthantering

Angreppsscenarier

Hur en incident kommer att hanteras hänger rimligen ihop med dess karaktär samt hur allvarlig den bedöms vara. Man kan förutsätta att hanteringen av angrepp på nivå 1 mot enstaka, samhällsviktiga webbplatser och myndighetsnät i normalfallet kommer att ske internt av den drabbade organisationen, vid behov genom att söka stöd hos den eller de nätoperatörer till vilka organisationen anslutit sig, hos polisen för att utreda brottet samt vid behov hos Sitic för att få kompletterande råd.

Åtkomstattacker kan kräva snabba åtgärder i ett eller flera operatörsnät. Här är det främst nätoperatörer som väntas bli involverade. Det finns även en möjlighet att söka stöd hos Sitic, men dess möjlighet att aktivt påverka trafikflöden är begränsade.

Samma förhållande gäller för angrepp på nivå 2 och nivå 3 mot samhällsviktiga informationssystem. När den egna organisationen inte kan hantera händelsen är det först och främst egna säkerhetskonsulter som kallas in, därefter nätoperatören. Här handlar det inte sällan om avancerade intrång med potentiellt mycket stora konsekvenser, och polisen involveras vanligen snabbt.

Några riktigt omfattande angrepp mot viktiga svenska samhällsfunktioner eller mot den svenska grenen av Internet har hittills inte skett. Det är mycket troligt att ett sådant angrepp under åtminstone en inledande fas skulle hanteras som flera skilda incidenter. Vid angrepp som parallellt drabbar flera svenska myndigheter eller andra samhällsviktiga organisationer saknas det nämligen möjlighet att upprätthålla en samlad lägesbild över tillståndet i de självständigt förvaltade myndighetsnäten och myndigheternas webbplatser. En sådan lägesbild handlar dels om att detektera verkliga eller potentiella intrång, dels om att studera trafikmönster. Nätoperatörerna förfogar var och en över sin del av denna överblick, men ingen av dem kan idag se helheten.

För närvarande saknas följaktligen möjlighet att detektera och följa omfattande och breda nätangrepp som parallellt drabbar många svenska samhällsfunktioner, möjligen med undantag för mycket stora åtkomstattacker. Dessa upptäcks nämligen snabbt på stamnätsnivå.

Nationell CERT-verksamhet i Sverige

Internationellt har det på senare år skapats åtskilliga organisationer för hantering av IT-incidenter, vanligen under beteckningen CERT (Computer Emergency Response Team). Från samhällets sida är det idag Sitic (Sveriges IT-incidentcentrum) som har ett utpekat uppdrag att hantera IT-relaterade incidenter i Sverige, inklusive störningar i den svenska grenen av Internet. Sitic är medlem i flera internationella samarbetsorgan. Verksamheten fick nyligen ökade anslag, vilket nu gör det möjligt att upprätthålla 24-timmarsdrift på samma sätt som incidentorganisationerna hos de större nätoperatörerna.

Sitics uppdrag består till stor del av rådgivning samt spridning och utbyte av information som berör IT-incidenter. Alla de större operatörerna i Sverige har idag egen incidentberedskap och sköter de flesta ärenden på egen hand, inklusive sådana incidenter som kräver internationell samverkan för att spåra trafik eller stoppa attackflöden nära källan. Sitics verksamhet är operativ i den meningen att organisationen hanterar incidentlarm förmedlade via det internationella samarbetet mellan CERT-organisationer. Nätoperatörer har dock vid återkommande tillfällen pekat på att de helst skulle se att Sitics verksamhet inte bedrevs vid tillsynsmyndigheten på telekommunikationsområdet.

Samarbetet sinsemellan mellan nätoperatörerna i Sverige tycks fungera väl under normala förhållanden. Hur incidentarbetet skulle organiseras vid ett storskaligt nätangrepp mot

svenska samhällsintressen är emellertid en öppen fråga idag. Särskilt oklar är Sitics roll i ett sådant läge.

Sitic har byggt ett system (Honeynet) med sensorer som fångar upp angreppsförsök. I ett pilotprojekt samlar man även in anonymiserade trafikdata från nätoperatörer. Däremot finns det för närvarande inte någon funktion som samlar trafikdata från myndigheternas Internetanslutningar och skapar en övergripande bild av trafikmönstren hos dem.

Det går lätt att konstatera att den svenska förvaltningstraditionen med självständiga myndigheter gjort det svårt att få en fungerande lägesbild av hur samhällsviktiga organisationer drabbas i en situation där Sverige utsätts för ett omfattande nätangrepp, eller står inför ett överhängande hot om sådant angrepp. Att upprätthålla en rättvisande lägesbild är en kritisk funktion vid kriser. Här skulle Sitic kunna ha en betydligt tydligare roll än idag.

Ytterligare en faktor komplicerar dock situationen. Vid omfattande åtkomstattacker som blockerar hela stamnätsförbindelser räcker det inte med att strypa egen trafik. Det drabbade nätet måste snabbt söka hjälp utifrån, och fientliga trafikflöden måste strypas så nära källan som möjligt, vilket ofta innebär i nät på helt andra platser i världen.

Med tanke på att många attackflöden idag är mycket kortvariga ställs det stora krav på en incidenthanteringsorganisation för att kunna arbeta operativt med incidenter. Det krävs mycket goda personliga kontakter med andra stamnätsoperatörer över hela världen för att tillräckligt snabbt kunna strypa sådana flöden. Detta är i själva verket en sfär som för närvarande står långt utanför statlig kontroll. Saken har framskymtat i några tidningsreportage på sistone, och är sedan länge allmänt känt bland dem som arbetar med stamnätsdrift. Detta är också den estniska erfarenheten.

Nationell krishantering i sammandrag

Sveriges nätoperatörer skulle troligen klara av attacker inom nivå 1 på egen hand utan statlig inblandning. Det är först på de andra två nivåerna som en mer organiserad, nationell krishantering kan bli aktuell. I jämförelse med Estland finns det då ett antal faktorer som skulle kunna vara till såväl fördel som nackdel för Sveriges vidkommande.

Om vi tittar på de utmärkande dragen från angreppen i Estland har vi redan konstaterat att de föregicks av en form av aggression innan attackerna tog vid. Vid allvarligare händelser som sprider oro på gatorna i form av demonstrationer kan vi alltså vänta oss att även hotbilden på nätet ökar. Vilka aktörer som blir målet för en presumtiv attack kommer troligen att bero på en rad olika omständigheter. Men av exemplet från Estland har vi lärt oss att det inte är sannolikt att endast en sektor eller aktör kommer att bli angripen. Attacker kommer snarare att drabba flera aktörer samtidigt. I Estland var de massiva attackerna ett problem på grund av att nätförbindelserna inte riktigt kunde klara stora, uthålliga trafikflöden. De svenska stamnäten har betydligt högre kapacitet. Detta innebär dock inte i sig något skydd mot angrepp som riktas mot enskilda webbplatser.

Om vi tittar vidare på de faktorer som visat sig vara viktiga för en effektiv hantering har vi redan konstaterat att det är väsentligt att snabbt organisera motåtgärder, etablera en stab, få tillgång till tekniska data samt inleda internationell samverkan.

Det som mest tydligt utgör sårbarheter i den svenska nätinfrastrukturen är brister i de svenska myndigheternas hantering av sin egen säkerhet, avsaknaden av samlad lägesbild över trafiken i de svenska myndighetsnäten samt den höga graden av personberoende. Det är relativt få personer i Sverige som har relevant erfarenhet av att

hantera trafikflöden på operatörsnivå. Av dessa är det dessutom bara en liten grupp som har det omfattande kontaktnät som kan behövas vid riktigt omfattande angrepp.

Det är mycket möjligt att Sitic skulle fungera som ett organ för operativ samordning i samband med ett större nätangrepp mot Sverige, tillsammans med en mer strategiskt inriktad myndighetsstab med representanter för polis, underrättelsemyndigheter med flera. Erfarenheterna från Estland visar att en sådan organisationsform fungerade väl. Vid sidan om den samlade myndighetsstab som träffades dagligen under ledning av försvarsministeriet samlades alla operatörer i landet hos CERT-EE för att diskutera problemen inbördes, skapa en gemensam operativ lägesbild och koordinera sitt arbete.

Samtidigt bör man ha i åtanke att CERT-EE redan från början var nära knutet till den samlade myndighetsmiljö som finns i Estland och som går under beteckningen X-Road. Denna nätmiljö, liksom de många myndighetsservrarna i landet, tillhörde måltavlorna för nätangreppen. CERT-EE hade tillgång till trafikdata – och fick tillgång till ytterligare trafikdata av operatörerna.

Någon motsvarande tillgång till egna trafikdata från myndighetssfären finns inte i Sverige. Den svenska myndighetsstrukturen innebär att det är betydligt svårare att snabbt få fram en motsvarande lägesbild av när och hur de offentliga informationsresurserna drabbas vid ett storskaligt nätangrepp.

KBM:s utbildningsserie

2007:4 Rätt i kris – Rätt juridiskt och etiskt vid mötet med medier i kriser och olyckor
2007:3 Krisberedskap och sekretess – informationsdelning mellan företag och offentlig sektor
2007:2 Utvärdering av övningar – En handbok för utvärdering av stabs- och beslutsövningar
2007:1 Öva krishantering – Handbok i att planera, genomföra och återkoppla övningar
2006:2 Risk- och sårbarhetsanalyser. Vägledning för kommuner och landsting
2006:1 International CEP Handbook. Civil Emergency Planning in the NATO/EAPC-Countries
2005:1 Medvind i säkerhetsarbetet
2004:1 Trossamfundens medverkan i krishantering
2003:8 Risk- och sårbarhetsanalyser – Introduktion för kommuner
2003:7 Sant eller falskt? Metoder i källkritik
2003:6 Nyheter vid kriser
2003:4 Crises Journalism – A guidance for government agencies
2003:3 Krisjournalistik – En introduktion för myndigheter
2003:1 Crisis Communication Handbook
2002:1 Åsk- och regnoväder över Orust – tusen och åter tusen frågor

ISBN 978-91-85797-13-4
ISSN 1652–3539

Krisberedskapsmyndigheten

Box 599
101 31 Stockholm

Tel 08 593 710 00
Fax 08 593 710 01

kbm@kbm-sema.se

www.krisberedskaps
myndigheten.se