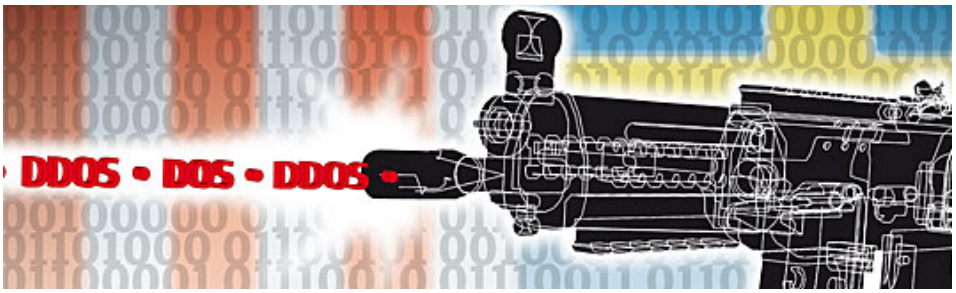
SvD NÄRINGSLIV

Sverige deltar i USA:s övning mot cyberkrig

IT-ATTACKER. Sverige ska öva nätförsvar i en USA-ledd storövning efter sommaren. I manövern ”Cyber Storm 3” slipas USA:s nya strategi mot en massiv attack från hackare och fientligt inställda stater.



7 augusti 2010 kl 07:00

När den estniska delen av internet försommaren 2007 utsattes för en serie attacker gav det säkerhetspolitiska effekter långt bortom landets gränser. Angreppen, som följde på våldsamma gatuprotester i Tallinn understödda av Ryssland, ledde till att Estland delvis tvingades kapa sin uppkoppling mot omvärlden.

Sedan dess har land efter land skärpt sin kapacitet att utkämpa konflikter där webbens fiberoptiska kablar och datorer är slagfält. Hotet är reellt, menar Jan Donnér, chef för avdelningen för informationssäkerhet på FRA.

–Vi ser hur flera stater och organisationer bygger upp sin kapacitet att kunna slå mot andra länder. Man vill verka utan att synas, säger Jan Donnér.

Traditionellt har nätattacker varit individer som hackat sig in eller kriminella som gör intrång för att stjäla ekonomisk information. Men uppbackade av en stat kan hackarna numera lika gärna vara cyberkrigare och syftet underrättelseverksamhet eller sabotage mot kritisk infrastruktur.

I september deltar Sverige för första gången i övningen ”Cyber Storm”. Myndigheter som Myndigheten för samhällsskydd och beredskap, MSB, och FRA blir då en liten del av USA:s hittills största övning i försvar mot nätattacker. Parallellt ska Sverige ha en egen övning.

Meningen med Cyber Storm 3 är att USA:s säkerhetsdepartement DHS ska öva tillsammans med över 200 myndigheter och företag. I kärnan finns CIA, Pentagon och krismyndigheter. Informationen utåt är knapphändig.

–Målet är att stärka cybersäkerhetsberedskapen och insatsförmågan genom att testa policyer och öva processer och procedurer som krävs för att identifiera och svara på en cyberattack mot nationens kritiska infrastruktur, säger DHS-talesmannen Chris Ortman.

FLERA SÄKERHETSMYNDIG SAMÖVAR

FRA
Svensk civil myndighet med två uppgifter: signalspaning samt stödja statens informationssäkerhetsarbete. Ligger på Lovön i Mälaren.

Visa mer fakta

En tjänsteman på DHS förklarar mot anonymitet att storövningen mer konkret ska pröva beta-versionen av USA:s nationella beredskapsplan mot cyberangrepp som DHS nu arbetar fram, samt att i realtid testa beslutsfattande, samordning och informationsutbyte mellan deltagarna.

De svenska deltagarna säger att de inte vet så mycket om scenariot. Richard Oehme, chef på MSB:s enhet för samhällets informationssäkerhet, menar dock att vikten av samverkan med andra länder är av avgörande betydelse vid större och allvarligare it-incidenter och att samarbetet därför är viktigt:

–Det handlar om att bygga en gemensam lägesbild. Inget land klarar sig självt, säger han.

Planeringen för ”Cyber Storm 3” sker med upprustning på internet som bakgrund. USA klassar numera webben som egen arena vid sidan om land, hav och luftrum och rymden. Sedan i maj har domänen ett eget kommando i Pentagon, U.S. Cyber Command. Chef är general Keith Alexander, som även leder landets mest slutna underrättelsetjänst, signalspaningsmyndigheten NSA.

”Detta är vår tids Manhattan-projekt”, sade kongressledamoten Michael Arcuri, när han i februari presenterade den nya lagen om cybersäkerhet, med hänvisning till kodnamnet för forskningsprojektet som tog fram den första atombomben. ”Men denna gång är hotet större. Nästan varje gymnasieelev till hackare har möjlighet sabba vår fria tillgång till internet. Tänk då vad en fientlig stat kan göra”.

CCDCOE, Natos Cyberförsvarscenter, arbetar efter tesen att cyberattacker kommer att vara standard som komplement till konventionell krigföring i konflikter framöver.

DHS berättar inte vilka länder som ska delta men inbjudna är medlemmar i det internationella samarbetet International Watch & Warning Network. Förutom nära USA-allierade som även tillhör Nato som Storbritannien, Tyskland och Norge ingår även Japan, Finland, Australien, Nya Zeeland, Schweiz och Sverige i gruppen.

Saknas gör två av de tre stater som mest satsar på internetkrig: Kina och Ryssland. Det tredje landet, USA, genomförde cyberoperationer vid invasionen av Irak.

Planerna för Sveriges medverkan har skissats sedan dåvarande försvarsministern Mikael Odenberg och USA:s säkerhetsminister våren 2007 skrev under ett samarbetsavtal om tekniskt och kunskapsmässigt utbyte inom civil säkerhet.

USA och landets nära allierade har två gånger tidigare kört storövningen Cyberstorm, i februari 2006 och mars 2008.

Första gången var scenariot en attack mot själva internet. Tunnelbanan i Washington klappade ihop, datorerna i New Yorks hamn slocknade och bloggare och nyhetsmedier publicerade känslig information, enligt övningens scenario. Under ”Cyber Storm 2” använde motståndaren bland annat datavirus för att angripa Pentagon och slog till mot en rad länders regeringar.

I scenariot för Cyber Storm 3 ska fokus ligga på att få myndigheter och företag att samordna sitt försvar – ett område där Sverige traditionellt är långt framme. En annan orsak till att Sverige får vara med är i sammanhanget närmast gammaldags: det geografiskt strategiska läget – samma sak som gjorde att FRA under kalla kriget kun- de signalspana in bakom järnridån.

Men numera är tillgången den internettrafik som strömmar genom kablar, säger säkerhetskonsulten och tidigare översten Ingvar Hellquist, som tidigare var chef

på Krisberedskapsmyndighetens enhet för informationssäkerhet och som rest till Washington för att planera medverkan i Cyber Storm:

–När internet föddes hamnade en av nätets noder i Sverige. Det är en av få som ligger antingen utanför USA eller i traditionellt allierade stater. Med både sådana tillgångar och den kompetens vi har är det naturligtvis lättare att få vara med och öva.

SvD.se beklagar att det, på grund av tekniska problem, för tillfället inte går att kommentera den här artikeln.

JOSEF EL MAHDI
08-13 55 28 josef.el.mahdi@svd.se