SÄRTRYCK UR *STRATEGISK UTBLICK 8*

Cyberförsvar – färdighet kräver övning

Tommy Gustafsson och David Lindahl

Sedan millennieskiftet har cyberincidenter och förmodade cyberoperationer haft en omfattande påverkan på många länder och organisationer. Sverige har en hög grad av digitalisering av samhällsviktiga system och de personer som dagligen hanterar dessa system har en central roll inom vårt totalförsvar. Därför är det viktigt att regelbundet öva dessa personer i att hantera cyberincidenter. I dagens läge sker för få övningar och det är dessutom svårt att genomföra dem realistiskt och pedagogiskt. För att säkerställa den nationella totalförsvarsförmågan behövs relevanta övningsmiljöer, ökad övningsvolym och forskning kring övningsmetodik.

Cyberoperationer

Cyberrymden är en arena där det under de senaste decennierna har skett en betydande utveckling av både förmåga och doktrin. Det är en arena där militära och civila aktörers intressen möts och hotet från cyberangrepp ställer nya krav på Sveriges totalförsvar. En konventionell konflikt begränsas av geografi. För att en fiende ska kunna slå mot Sverige måste de först passera rikets gräns och det skydd som Försvarsmaktens förband utgör. En cyberoperation, det vill säga aktiviteter i cyberrymden utförda av en stat för att nå militära eller politiska mål, gör det möjligt för en angripare att slå mot alla de datorer som är nåbara för kommunikation utan att det konventionella försvaret kan göra något.

Det innebär att enskilda systemadministratörer i civila organisationer riskerar att hamna i konfliktens frontlinje. De behöver därför ha den kompetens som krävs, både för att se till att systemen har en bra säkerhetsnivå och för att kunna hantera angrepp.

Cyberoperationer används idag regelbundet för underrättelseinhämtning, industrispionage och sabotage. Internationella konflikter har förekommit som helt eller delvis har utspelat sig i cyberrymden. Det finns exempel på cyberoperationer där nationer har anfallit civila mål både direkt och indirekt med hjälp av proxyorganisationer såsom hackergrupper. Under kriget mellan Ryssland och Georgien 2008 störtdes en dryg tredjedel av Georgiens internet allvarligt, myndigheters kommunikation stoppades och riksbanken tvingades stänga ner alla datortjänster i elva dygn.

En annan betydande verksamhet är olika typer av påverkansoperationer. De flesta påverkansoperationer verkar vara fokuserade på att manipulera opinionen i en viss fråga, men det finns exempel som indikerar att cyberoperationer också har använts för att påverka suveräna nationers strategiska beslut. Ett sådant är cyberangreppen 2009 mot Kirgizistan i samband med att landet förhandlade om att husera en NATO-bas på sitt territorium.

Det är svårt att begränsa verkan av cybervapen, som exempelvis skadlig kod, och cyberangrepp. År 2010 tog sig cybervapnet Stuxnet långt utanför sina avsedda mål i Iran och sju år senare slog angreppet NotPetya inte bara mot tio procent av Ukrainas datorer, utan spred sig utanför landet och blev världens hittills mest kostsamma cyberangrepp. Sammantaget visar utvecklingen inom cyberarenan att det finns ett hot mot Sveriges samhällsviktiga system även om Sverige i sig inte är målet för ett visst angrepp.

Cyberförsvarets förmågebehov

Många ramverk och vägledningar inom cybersäkerhet lyfter fram behovet av kunskap om

FOI Memo 6747
Projekt Nr I181103
Godkänd av Mike Winnerstig

Augusti 2019

hot och skyddsåtgärder. Denna kunskap behövs bland annat för att göra rätt saker med de resurser som finns till hands, exempelvis att prioritera tekniska och administrativa skyddsåtgärder. Proaktiva åtgärder är viktiga och det är ofta enskilda systemadministratörers kunskap och agerande som avgör om en incident inträffar och om dess konsekvenser i så fall blir allvarliga eller inte. Ett bra sätt att bygga upp denna kunskap är att öva. Övning ger en erfarenhetsbaserad inlärning utan att behöva hantera skarpa incidenter. Genom att öva blir systemadministratörer skickligare och systemen säkrare.

Cyberövningar används internationellt för att öka försvarsförmågan, till exempel *Locked Shields* och *Crossed Swords* som arrangeras i Estland samt *Cyber Czech* i Tjeckien. Att öva är också i linje med Sveriges nationella strategi för cybersäkerhet från 2017, som bland annat konstaterar att ”[r]egelbundna nationella och internationella övningar är en förutsättning för att utveckla och utvärdera strukturer för hantering av allvarliga IT-incidenter…”.

Förutom kunskapsnivån hos enskilda system-administratörer har det visat sig att samverkan också är en viktig framgångsfaktor för att snabbt och effektivt kunna hantera avancerade storskaliga cyberincidenter. När Estland år 2007 utsattes för angrepp drog de stor fördel av en sedan flera år etablerad nationell samverkan mellan systemadministratörer från olika organisationer inom samhällsviktig verksamhet. Övningar är ett sätt att etablera denna typ av samverkan.

En nationell förmågeuppbyggnad

För att åstadkomma en nationell förmågeuppbyggnad inom cyberområdet finns det tre betydande övningsrelaterade utmaningar som behöver adresseras: för det första krävs tillgång till relevanta övningsmiljöer och scenarier, för det andra en ökad övningsvolym, och för det tredje behövs forskning som säkerställer att rätt kompetens lärs ut på rätt sätt.

För att skapa relevanta övningsmiljöer och scenarier behövs dels betydande kunskap om IT och om hur aktuella cyberangrepp går till, dels ett pedagogiskt handlag för att utveckla övningar som förmedlar de komplexa detaljerna hos cyberincidenter. Idealt skulle övningar bedrivas direkt i övningsdeltagarnas normala IT-miljöer men det är sällan möjligt eftersom det skulle medföra betydande driftstörningar i just den IT-miljö man vill skydda.

Ett alternativ är då att skapa en replik av den egna IT-miljön men de flesta organisationer har inte tillräckliga resurser för att prioritera att sätta upp parallella IT-miljöer. Även om man kopierar de tekniska systemen är det mycket svårt att simulera användarnas aktiviteter vilket därmed begränsar scenarionas relevans. Ett ”tyst” nät där bara angriparna och de övade är aktiva skiljer sig mycket från verkligheten.

> “Många organisationer som bedriver samhällsviktig verksamhet är inte medvetna om sin roll för Sveriges totalförsvars-förmåga och därmed är de inte heller medvetna om hur viktig deras cybersäkerhets-förmåga är.”

Ytterligare problem är att det ofta krävs flera iterationer av en övning innan de pedagogiska momenten fungerar optimalt och förändringstakten inom området medför också att övningsmiljöer snabbt skulle blir föråldrade. De flesta organisationer är för små för att ha egen personal som kontinuerligt vidareutvecklar övningsmiljöer och scenarier.

Det finns vissa kommersiella initiativ inom området, men dessa har hittills saknat relevanta övningsmiljöer för totalförsvaret. Resurser för att utveckla själva övningen måste därför fortfarande avsättas av den organisation som vill öva, vilket aktualiserar de svårigheter som beskrivs ovan. I de fall där de kommersiella initiativen är utländska, medför detta ett säkerhetsproblem ur ett totalförsvarsperspektiv. Sammantaget medför svårigheterna med att utveckla och underhålla övningsmiljöer och scenarier, samt avsaknaden av relevanta kommersiella alternativ, att det behövs en nationell totalförsvarssatsning inom detta område.

Liknande satsningar sker redan i flera länder, med framträdande exempel i Estland och Norge. Dessa satsningar syftar till att stärka den nationella cyberförsvarsförmågan i respektive land

och inkluderar ofta aktörer från försvarsmakt, civila myndigheter, aktörer inom samhällsviktig verksamhet och högre lärosäten. Denna blandning av aktörer säkerställer att de övningar som utvecklas bygger på relevant teknik, och relevanta scenarier och att de får en tillräcklig spridning för att få en positiv och långvarig effekt på den nationella cyberförsvarsförmågan. En central komponent i dessa satsningar är upprättandet av en nationell cyberanläggning (på engelska *cyber range*) där övningar kan utvecklas och genomföras.

I samarbete med Myndigheten för samhällsskydd och beredskap och Försvarsmakten driver FOI anläggningen *Cyber Range And Training Environment* (CRATE) som används såväl inom forskningsprojekt som inom övnings- och kursverksamhet. Det är idag en avancerad cyberanläggning och inkluderar en omfattande IT-infrastruktur samt en mängd specialutvecklade verktyg för att ta fram och genomföra övningar. CRATE skulle kunna utgöra en bra grund för en svensk nationell cyberanläggning.

Utmaningen att öka övningsvolymen kräver både en större medvetenhet och en bättre tillgång till relevanta cybersäkerhetsövningar. Många organisationer som bedriver samhällsviktig verksamhet är inte medvetna om sin roll för Sveriges totalförsvarsförmåga och därmed är de inte heller medvetna om hur viktig deras cybersäkerhetsförmåga är. De dimensionerar i första hand sitt säkerhetsarbete för att hantera driftstörningar och skulle därför troligen inte prioritera cybersäkerhetsövningar även om dessa fanns tillgängliga. Att enbart förbättra övningsmöjligheterna utan att höja medvetenheten skulle därför inte leda till ökad övningsvolym.

För att adressera utmaningen med att säkerställa att rätt kompetens lärs ut på rätt sätt krävs forskning inom pedagogik relaterat till cybersäkerhet. Trots att Sverige i likhet med flera andra länder har genomfört övnings- och utbildningsinsatser under mer än ett decennium har det endast skett begränsad forskning inom detta område. Att arrangera övningar med fokus på totalförsvarets behov förefaller som en fungerande metod, inte minst med tanke på de effekter detta får för framtida samverkan, men ytterligare forskning som styrker detta är nödvändig.

Andra viktiga forskningsfrågor inom området är teknik- och metodutveckling i cyberanläggningar, metoder för att öka övningsvolymen samt hur övningar kan användas för att ta fram nya data. Internationella exempel visar också att en nationell cyberanläggning kan användas för att bidra till kompetensförsörjningen på längre sikt genom att låta högre lärosäten nyttja den i forskning och utbildning.

Genom att adressera utmaningarna med att tillhandahålla övningsmiljöer, skapa en ökad övningsvolym och en kunskapsuppbyggnad kring dessa genom forskning kan Sveriges cyberförsvarsförmåga, och därmed vår totalförsvarsförmåga, utvecklas för att möta framtidens behov.

För vidare läsning

Mikael Wedlin och Erik Westring, Internet som militär arena, Strategisk utblick 7, 2017, FOI-R--4454--SE.

Ann-Sofie Stenérus Dover och Camilla Trané, NCS3-studie: Påverkan på organisationers säkerhetsarbete av kursverksamhet inom området säkerhet i industriella informations- och styrsystem, 2016, FOI Memo 5920.

FOI
Totalförsvarets forskningsinstitut
SE-164 90 Stockholm

Telefon: +46 8 5550 3000
www.foi.se