Cyberattacker mot kritisk infrastruktur under pandemin – lärdomar för krisberedskapen och totalförsvaret

David Lindahl, Birgitta Liljedahl och Annica Waleij

Cyberangrepp mot samhällsviktig verksamhet och kritisk infrastruktur har skett över hela världen de senaste åren och vid flera tillfällen lett till allvarliga störningar. Hälso- och sjukvårdssektorn har inte varit förskonad; sjukhus har stängts ner och information om patienter har kommit i orätta händer. Sedan coronavirusutbrottet har det rapporterats om omfattande aktivitet när det gäller cyberhot relaterade till pandemin. Här finns lärdomar att dra för krisberedskapen och totalförsvaret.

Kritisk infrastruktur och cyberangrepp

Hälso- och sjukvårdskedjan är ett av de sju prioriterade områden som Myndigheten för samhällsskydd och beredskap (MSB) har identifierat som centrala för att stärka såväl den fredstida krisberedskapen som arbetet med civilt försvar. De övriga områdena är energiförsörjning, livsmedelsförsörjning (inklusive dricksvatten), transporter, finansiella tjänster, information och kommunikation samt skydd och säkerhet.

Både inom och mellan dessa områden finns det kritiska beroenden. Gemensamt för samtliga är ett starkt beroende av informationsteknologi (IT) och den så kallade cyberdomänen, vilket skapar sårbarheter som kan nyttjas vid cyberangrepp.

Hälso- och sjukvårdssektorn utsätts för cyberangrepp även i den normala vardagen. Attacker med så kallade gisslanprogram, där data krypteras mot krav på lösensumma för att öppnas igen, är inte ovanliga. Ett exempel är Wannacry, ett gisslanprogram som drabbade bland annat Storbritanniens sjukvård 2017, vilket gjorde att flera sjukhus blev tvungna att stänga ner verksamhet och inte kunde ta emot patienter till sina akutmottagningar.

Vår oro – någons vapen

I en kris, oavsett om den är naturligt eller antagonistiskt orsakad, kommer många människor att börja leta efter information. I vårt moderna, digitaliserade samhälle, innebär det att aktiviteter på sociala medier, med sökmotorer och i appar av olika slag ökar. Om man inte redan i förväg vet var man kan hitta tillförlitlig information om ett ämne kan det vara svårt att hitta den på Internet. En sökning på nyckelord kan leda till sidor med felaktig information. Och även om sidan ser trovärdig ut kan det vara en falsk sida skapad för att vilseleda genom att utnyttja någon annans goda namn.

Angriparna vet att människor är oroliga i kristider, och kommer att söka efter information som har att göra med krisen. Osäkra och oroliga människor kan också lättare förmås att ta risker för att bli lugnade. Möjligheterna för angripare är alltså stora under kriser eftersom både antalet möjliga offer ökar och oddsen att lyckas lura dem är bättre än normalt. I en kris pågår de vanliga angreppen fortfarande men nya kampanjer anpassade till krissituationen tillkommer.

Det är svårt att föreställa sig mängden aktivitet som har skett för att utnyttja människors sökningar. Dustyfresh, en IT-expert, har publicerat en sammanställning över nya webdomäner som har registrerats sedan den 14 mars och vars nyckelord eller namn innehåller ”corona” eller ”covid”. På bara några dagar i mars månad hittade han omkring 3 600 nya webbplatser och det totala antalet är i början av juni över 47 000 stycken.

Ökade attacker under pandemin

Det har rapporterats om en mycket stor aktivitet över hela världen när det gäller cyberhot relaterade till coronaviruspandemin. Framför allt har det skett en ökning av bedrägerier riktade mot privatpersoner. En av de vanligaste metoderna är att angripare skapar webbplatser och appar av olika slag, som utger sig för att informera om coronaviruset, men som installerar skadlig kod på offrets utrustning. Ett exempel är appen ”Covid-19 tracker”, som utger sig för att kunna tala om hur utbredningen av viruset ser ut i ens geografiska närhet och skicka varningar och information

FOI Memo: 7329
Projektnummer: I189160
Godkänd av: Karin Mossberg Sonnek

November 2020

om hur man undviker viruset. I andra fall har angriparnaanvänt enklare lösningar som massutskick av e-post som uppmanar läsaren att öppna Microsoft Office-bilagor med skadlig kod. Just bedrägerier har antagligen ökat så mycket för att de kan levereras genom de vanliga metoderna för appar och e-post. Genom att locka till sig offren med falska appar kommer angriparna runt problemet med att hacka brandväggar och andra försvarsmekanismer i offrens IT-utrustning. Användaren godkänner själv installationen och stänger av skydden så att den skadliga koden kan angripa. Det som sedan händer är till exempel att appen blockerar möjligheten att använda telefonen eller datorn och hotar med att angriparen har tillgång till data från enheten som hen tänker sprida om en lösensumma inte betalas.

Det här är en situation som har drabbat flera sjukhus och vårdinrättningar i stor skala där skadlig kod har kommit in i nätverken och spridit sig från dator till dator. Exempel på detta är, förutom ovan nämnda Wannacry-angrepp, att vi under pågående coronakris har sett att bland annat brittiska Hammersmith Medicine Research blev angripet och bestulet på information. Omkring 2 300 patienters personliga information publicerades på Internet som hämnd för att sjukhuset inte betalade.

Hur ser hoten ut?

Generella drag hos angreppen är att de härmar legitima informationskällor, och ofta specifikt hälso- och sjukvårdsinformation. Världshälsoorganisationens, WHO:s, namn och logga har använts flitigt, men även olika länders smittskydds- och folkhälsomyndigheters namn. Detta är problematiskt på två sätt. För det första riskerar det att locka människor att ladda ner skadlig kod och bli drabbade av informationsstöld eller gisslanprogram. För det andra, och än viktigare, riskerar detta att skapa misstro mot de organisationer som bekämpar pandemin då deras varumärken och loggor kan associeras med bedrägerier.

De allra flesta hoten riktar sig mot vanliga privatpersoner och är relativt simpla, som massutskick av e-post med en länk som laddar ner skadlig kod. Om man inte klickar på länkarna är det oftast ingen fara. Ett fåtal angrepp har däremot varit mer avancerade. Ett exempel är försök att sprida kod som programmerar om routrar från ett par olika företag. Om man försöker nå vissa webbplatser når man i stället en fejkad webbplats som ser ut som den riktiga, men som infekterar besökardatorn med skadlig kod.

Vad är cyberaktörernas drivkraft?

De allra flesta angrepp som har rapporterats är utförda för ekonomisk vinning. Angriparen vill låsa datorer och telefoner och få lösensummor eller installera spionprogram som stjäl banklösenord. Flera angrepp kopplade till hackergrupper associerade med stater har också rapporterats. Exempelvis publicerade en statlig aktör, enligt EU:s antidesinformationsenhet, falsk information på sociala medier om att en transport med återvändande ukrainare, som hade besökt Wuhan i Kina, var smittade med coronaviruset. Detta ledde till upplopp, och aktörer med koppling till den aktuella staten försökte även utföra bedrägerier via e-post för att få in skadlig kod i myndigheters datornätverk.

Liknande aktioner, mot bland annat militära förband, biotech-industri och myndigheter, har rapporterats från exempelvis Indien, Vietnam, USA och Sydkorea. Även i Sverige agerar statliga aktörer under krisen. Utifrån öppna källor, verkar det som att staters agerande under pandemin följer normala rutiner. Huvudsakligen rör det sig om underrättelseaktiviteter, cyberspionage och förberedelser för framtida angrepp. Fokus ligger på militära och civila beslutsfattare, kritisk infrastruktur och industri.

Syftet för statliga aktörer är oftare underrättelseinhämtning av olika slag än sabotage eller lösensummor, men även påverkansoperationer utförs för att destabilisera stater och påverka opinionen i en för aktörerna önskad riktning. Under krisen tar de också tillfället i akt att stresstesta de sårbarheter som krisen öppnar upp för, till exempel att många människor arbetar hemma med bristfälliga säkerhetslösningar. För både de kriminella och de statliga aktörerna gör coronaviruset att de normala verktygen får ytterligare en dimension. På samma sätt som med kriminalitet verkar statliga angrepp, skräddarsydda för att utnyttja krisen, ske parallellt med rutinaktiviteterna.

Utmaningar för hälso- och sjukvårdssektorn

Hälso- och sjukvårdssektorn kan vara ett tacksamt mål för stater som vill störa verksamhet eller för kriminella som vill skaffa snabba pengar. I ett normalt läge kanske attackerna hade observerats och undvikits. Men i ett krisläge är hälso- och sjukvårdssektorn inte sällan bemannad av stressad och trött personal och då ökar sannolikheten för misstag. Kommunikationsbehovet ökar då människor som söker sig till sjukvården för att få hjälp och information inte kan stängas ute. Det kommer också stora mängder av information från olika håll som man måste förhålla sig till, och det gör det lätt att sprida felaktig information. Sjukvården i ett krisläge kan komma att behöva flytta såväl patienter som personal. Då är det lätt att någon i personalen begår ett misstag för att man inte har samma rutiner för informationshantering överallt eller för att man kastas in i en ny roll utan tillräcklig utbildning.

Behovet av cyberhygien

Det är viktigt att förberedelser för att hantera cyberhot har genomförts i god tid innan en kris. Rutiner för att till exempel skaffa sig information eller för att få teknisk hjälp måste ha etablerats innan krisen för att kunna användas rätt under en kris.

Den allmänna cyberhygienen är det viktigaste för hälso- och sjukvårdpersonal i gemen, det vill säga att följa redan fastlagda rutiner för att på så sätt minimera antalet angrepp. Det gör att IT-säkerhetspersonal kan ta hand om de angrepp som trots detta tar sig förbi säkerhetsåtgärderna. Det är även viktigt att inte blanda privat IT-utrustning med sjukvårdens. För att detta ska fungera måste alla vara medvetna om att deras agerande kan leda till cyberangrepp. Därför bör alla personalkategorier inom vård och omsorg få utbildning och tydliga förhållningsregler om vad man får och inte får göra.

Det är alltså vitalt att komma ihåg att alla i en organisation som kan ta emot digital kommunikation måste utbildas, då det räcker med att en enda person gör ett misstag för att organisationen ska drabbas.

I en kris gäller det för alla att vara mer vaksam än vanligt när man letar efter information. Källkritik är avgörande. Man ska inte lita på allt man ser och hör, utan verifiera information så långt det är möjligt. Viktigt är också att genomföra regelbunden backup på data för att minimera skador från gisslanprogram.

Lärdomar för svensk krisberedskap och totalförsvaret

Vi kan anta att cyberangriparna snabbt kommer att anpassa sig till nästa kris unika förutsättningar. De förpackar om sina verktyg med nya, för den aktuella krisen relevanta, sökord och letar efter nya vägar att ta sig in igen. I dagsläget är det helt enkelt en situation vi får leva med.

Hoten mot samhället är komplexa och ofta sammanlänkade. Dels finns de direkta hoten, som cyberattacker mot hälso- och sjukvårdskedjan, dels de indirekta hoten där angrepp mot en helt annan sektor får kaskadeffekter även på hälso- och sjukvårdskedjan. Vi behöver öka förståelsen för beroenden inom och störningar mot övrig kritisk infrastruktur som bland annat el- och vattenförsörjning, och den transportsektor som är en förutsättning för att hälso- och sjukvården skall kunna fungera. Ingen kedja är starkare än sin svagaste länk. Det gäller även IT-kedjan.

Hälso- och sjukvården är en viktig nationell strategisk resurs som ska tillhandahålla vård för såväl civilsamhället som det militära försvarets behov. Vid en kris, höjd beredskap, eller ytterst i krig ställs sjukvårdens kapacitet på sin spets, och kapacitetstaket inom vården kan snabbt nås. Av central betydelse är att arbeta sektorsöverskridande för att samhället ska bli robust nog att hantera såväl en naturlig pandemi som andra oönskade händelser, exempelvis en antagonistisk CBRN-händelse, det vill säga en händelse som involverar giftiga kemiska, radiologiska eller smittsamma ämnen, när stora delar av den nationella verksamheten är ansträngd och begränsad av exempelvis ett samtida långvarigt elavbrott. Då krävs att cyberhygienen redan är etablerad och hanteras rutinmässigt. Det gäller såväl inom kritiska sektorer som arbetar under stress, som hos befolkningen.

Detta är ett utdrag ur FOI:s rapport Perspektiv på pandemin - Inledande analys och diskussion av beredskapsfrågor i ljuset av coronakrisen 2020 FOI-R--4992--SE.

För vidare läsning

David Lindahl, Birgitta Liljedahl och Annica Waleij, 2020, Cyberattacks in the healthcare sector during the first three months of the Covid-19 pandemic, FOI Memo 7062.

Annica Waleij, Birgitta Liljedahl, Susanne Börjegren och David Lindahl, 2019, Vidare kontext för en CBRN-relaterad hotbild. FOI, Stockholm, Sweden, FOI-R--4781--SE.

Annica Waleij, Louise Simonsson och Birgitta Liljedahl, 2019, Konsekvenser av energibortfall på samhällets funktionalitet och civilbefolkningens hälsa, FOI-R--4755--SE.

FOI
Totalförsvarets forskningsinstitut
SE-164 90 Stockholm

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