2020

Cybersäkerhet i Sverige

– Hot, metoder, brister och beroenden

FRA

FÖRSVARSMAKTEN

MSB Myndigheten för samhällsskydd och beredskap

Polisen

Säkerhetspolisen

Grafisk form: Sinfo Yra
Illustrationer: Matilda Petersson
Foto: iStockphoto

Innehåll

Sammanfattning

- Statliga aktörer har mycket hög uthållighet och förmåga att genomföra cyberoperationer, vilket gör dem till det dimensionerande hotet inom cybersäkerhet för verksamheter med höga skyddsvärden.
- Statliga aktörer drivs av sina intressen inom utrikes- och säkerhetspolitik, militärt försvar samt av egna ekonomiska incitament.
- Kriminella aktörer drivs primärt av ekonomiska incitament och är ett generellt hot som kan riktas mot samtliga verksamheter.
- Mängden sårbarheter ger hotaktörer möjlighet att nyttja ett stort antal angreppsmetoder.
- Säkerhetsbrister uppstår om inte verksamheterna arbetar systematiskt med cybersäkerhet.
- Utkontraktering ställer höga krav på kravställning samt förståelse för de egna behoven av cybersäkerhet och förmåga att bedöma de lösningar som erbjuds.
- Molntjänster kan möjliggöra en högre säkerhet för vissa verksamheter men samtidigt introducera svårhanterade risker som kan vara svåra att överskåda.
- Komplexa beroenden i det digitaliserade samhället innebär att konsekvenserna av cyberangrepp blir svåröverblickbara.
- Allt fler verksamheter digitaliserar delar av eller hela sin verksamhet vilket innebär ökade krav på tillgänglighet av elektricitet och fungerande uppkoppling till internet.
- Brist på relevant kompetens inom cybersäkerhet är ett samhällsproblem.

Inledning

Sverige befinner sig i en tid där den tekniska utvecklingen sker i mycket högt tempo. Det innebär fördelar och nya möjligheter för hela samhället, som förändras i takt med en tilltagande digitalisering. Vi blir mer effektiva, globala och tekniskt avancerade. Digitaliseringen har samtidigt blivit ett krav där effektivitet, globalisering och avancerad teknik även utvecklats till påbud som alla verksamheter behöver förhålla sig till. Verksamheternas konkurrensförmåga och cybersäkerhet är direkt kopplade till hur väl man hanterar en kontinuerlig anpassning till digitalisering och teknisk utveckling.

Den digitala transformationen innebär att det har skapats ett beroende av kontinuerligt fungerande informations- och kommunikationsteknik. I vår strävan efter att använda alla de möjligheter som den teknologiska utvecklingen erbjuder finns det dock en baksida. Där tekniken implementeras på ett ogenomtänkt eller otillräckligt sätt uppstår brister som kan utnyttjas av hotaktörer.

Parallellt med arbetet att ta Sverige framåt i utvecklingen måste således ett anpassat och balanserat säkerhetsarbete bedrivas. Om detta inte sker och verksamheter utvecklar system som är exponerade och tillgängliga för cyberangrepp, skapar vi ett svagare och mindre robust samhälle. Då finns en risk för att de fördelar vi räknar med på kort sikt inte blir lika goda, eller i värsta fall omvandlas till negativa faktorer, i ett längre och samhällsövergripande perspektiv.

Bakgrund

I 2019 års två regeringsförklaringar aviserades att regeringen avser att upprätta ett nationellt center för att öka informations- och cybersäkerheten. Försvarets radioanstalt (FRA), Försvarsmakten, Myndigheten för samhällsskydd och beredskap (MSB) samt Säkerhetspolisen bedriver inom ramen för sina uppdrag verksamheter som är centrala för att skydda Sverige mot cyberhot.

Det nationella cybersäkerhetscentret ska stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot mot Sverige och minska cybersårbarheterna. Vidare ska centret ge ett utvecklat och samordnat stöd om hur olika verksamheter i privat och offentlig sektor kan skydda sig mot cyberattacker. En central del i skyddet kan vara gemensamma analyser och lägesbilder om hot, sårbarheter och risker. Centret ska också kunna stödja Regeringskansliet i frågor kring cybersäkerhet. Verksamheten ska bidra till att förbättra skyddet mot antagonistiska hot och minska de digitala sårbarheterna.

Rapporten

Regeringen har uppdragit åt FRA, Försvarsmakten, MSB och Säkerhetspolisen att tillsammans vidta förberedande åtgärder och lämna förslag för att ett nationellt cybersäkerhetscenter ska kunna inrättas under 2020. Parallellt med detta sker en fördjupad myndighetssamverkan som syftar till att främja denna uppgift. Som en del i detta har myndigheterna tillsammans med Polismyndigheten gemensamt tagit fram denna rapport. Syftet är att tillsammans – utifrån de lägesuppfattningar som respektive myndighet har – sammanställa en lägesbild som på ett enkelt och tillgängligt sätt beskriver cybersäkerhet ur ett nationellt perspektiv.

Rapporten grundas på kunskap och bedömningar från myndigheter med uppgifter som är centrala för att skydda Sverige mot cyberhot. Den är inte hemlig, men innehållet är till del baserat på sekretessbelagd information. Rapporten är avsedd att användas som ett underlag vid exempelvis verksamhetsplanering, utvecklingsarbete, beslut om investeringar, upphandlingar, säkerhetsåtgärder, analyser eller andra riskbedömningar.

Innehållet är tänkt att kunna användas av samtliga offentliga som privata verksamheter. Den riktar sig främst till personer som arbetar kontinuerligt med cybersäkerhet, men kan även vara av intresse för andra beslutsfattare och ledningsgrupper.

Som en konsekvens av att rapporten är ett resultat av flera myndigheters gemensamma insatser är textens utformning avsiktligt generaliserad. Vi har undvikit terminologi och uttryck som är bundna till en viss myndighets verksamhet eller ett specifikt verksamhetsområde. Syftet är att rapportens innehåll ska upplevas som relevant och vara möjligt att tillämpa för så många verksamheter som möjligt.

Hotaktörer

De cyberhot som riktas mot Sverige är mångfacetterade och kan kopplas till flera olika typer av hotaktörer. I huvudsak utgörs dessa av statliga aktörer och kriminella grupper. I viss omfattning förekommer även ideologiskt motiverade aktörer, såsom hacktivister eller grupperingar med terrorkopplingar. Statliga aktörer genomför cyberangrepp mot Sverige i syfte att exempelvis inhämta information som kan gynna det egna landets utrikes- och säkerhetspolitiska intressen eller i syfte att stärka det egna landets ekonomi och företag genom företagsspionerі. Cyberkriminalitet syftar i de allra flesta fall till att tjäna pengar och de ideologiskt motiverade aktörerna agerar i enlighet med sina egna formulerade agendor.

Metoder och verktyg för cyberangrepp utvecklas ständigt och hotaktörernas spelplan förändras i takt med teknikutvecklingen. Hotaktörerna använder sig ofta av enklast möjliga metod för att uppnå önskat resultat och i många fall krävs inte att man använder sig av avancerade metoder.

SVÅRIGHETER MED ATT IDENTIFIERA EN HOTAKTÖR PÅ CYBEROMRÅDET

Förutsättningarna för anonymitet och förnekbarhet är goda på cyberområdet och identifiering av en hotaktör är ofta behäftad med viss osäkerhet. Identifiering, eller *attribuering*, kräver ofta att flera olika informationsunderlag läggs samman och bedöms. Beroende av underlagen blir bedömningen mer eller mindre säker.

Ytterligare en försvårande faktor är att det händer att olika hotaktörer komprometterar varandras infrastruktur, stjäl verktyg och implantat från varandra eller till och med tar över varandras mål. Det kan leda till förvirring och möjliggör så kallade ”false flag”-operationer, där identifieringen av vem som är ansvarig för ett cyberangrepp riskerar att felaktigt baseras på de verktyg eller den infrastruktur som har använts vid angreppet.

Förutom de rent tekniska åtgärder som står till buds kan en hotaktör även använda sig av ombud, proxys. Det kan vara kriminella nätverk eller andra grupperingar som förses med uppdrag och i vissa fall även de andra hjälpmedel som behövs.

Att skydda sig mot cyberangrepp från kvalificerade hotaktörer är en nationell angelägenhet. Bland de svenska mål som utsätts för cyberangrepp finns verksamheter som är väsentliga för vårt samhälles grundläggande funktioner, på kort eller lång sikt. Datorer i Sverige angrips också i syfte att användas som verktyg i cyberangrepp mot mål i andra länder.

Statliga aktörer

De statliga aktörerna utgörs i de flesta fall av nationella underrättelse- och säkerhetstjänster eller grupperingar som har kopplingar till dessa.

Dessa aktörer använder cyberangrepp för att uppfylla olika nationella intressen. Det kan handla om att ge det egna landet utrikes- och säkerhetspolitiska fördelar, gynna det egna landets forskning och utveckling och skapa konkurrensfördelar för inhemska företag, eller skaffa fram underlag för att utföra påverkansoperationer. Det kan även handla om förberedande angrepp som genomförs i syfte att skapa förutsättningar att vid ett senare tillfälle kunna genomföra operationer vars syfte exempelvis kan vara att orsaka skada för den verksamhet som utsätts.

Ett stort antal stater bedöms i dagsläget ha förmåga att genomföra cyberangrepp. Förmågan kan antingen vara egenutvecklad, bygga på öppet tillgängliga verktyg eller vara kommersiellt upphandlad. Vissa statliga aktörer är mycket kvalificerade och genomför cyberangrepp på ett sätt som är storskaligt, systematiskt, uthålligt och globalt för att tillgodose det egna landets intressen. Cyberangrepp erbjuder goda möjligheter till anonymitet, förnekbarhet och vilseledning för den bakomliggande aktören jämfört med mer traditionella metoder. Detta öppnar upp för nya möjligheter att agera utan att hamna i öppna konflikter med andra länder.

Cyberangrepp från statliga aktörer mot svenska mål sker hela tiden, en del med framgångsrikt resultat. Aktörerna utvecklar sin metodik och sina verktyg och de blir allt mer sofistikerade. Samtidigt fortsätter de att använda sig av äldre kända metoder så länge dessa fortsatt ger resultat.

Statliga aktörer benämns ofta Advanced Persistent Threat (APT), i dessa sammanhang. De är resursstarka i form av pengar, personal och expertis och i kombination med att de har en stor långsiktighet och uthållighet utgör de ett stort hot mot Sverige i de fall Sveriges intressen står i motsatt förhållande till deras egna.

Utrikes- och säkerhetspolitiska intressen

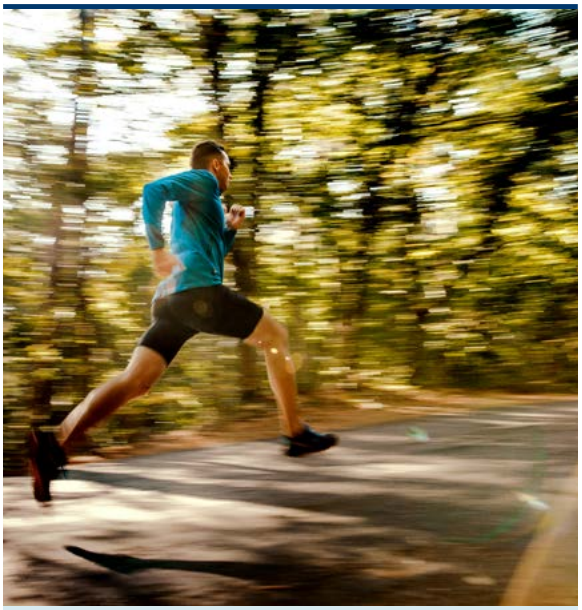
För att tillgodose sitt eget lands utrikes- och säkerhetspolitiska intressen använder statliga aktörer cyberangrepp mot en stor variation av mål i olika syften som ger olika effekter.

Så går en cyberoperation till

1. En cyberoperation har ett syfte som ska uppnås vilket inriktar hotaktören som ska verkställa angreppet.
2. För att förstå hur syftet kan uppnås kartlägger hotaktören de mål som ska utsättas för cyberangrepp. Det kan handla om att förstå vilka personer eller vilken teknisk miljö som ska angripas.
3. När hotaktören vet hur syftet kan uppnås söker hotaktören efter sårbarheter att utnyttja.
4. De sårbarheter som hittas utnyttjar hotaktören i utformningen av cyberangreppet.
5. Efter att ett lyckat cyberangrepp har genomförts kan hotaktören ha större eller mindre kontroll över målets it-miljö.
6. När hotaktören har möjlighet att agera inne i it-miljön kan olika aktiviteter genomföras för att uppnå önskvärd effekt, det vill säga syftet med operationen.

Cyberangrepp från statliga aktörer i syfte att inhämta underrättelser pågår ständigt mot svenska mål. De angriper bland annat verksamheter som hanterar känslig eller skyddsvärd information som rör Sveriges säkerhet, men även öppen information kan vara av intresse. Syftet är att ge den egna staten större handlingsfrihet och inflytande i utrikes- och säkerhetspolitiska frågor genom att skaffa sig ett informationsöverläge gentemot andra länder.

Det förekommer att cyberangrepp genomförs för att påverka skeenden i Sverige eller utomlands. Allt ifrån stulen information som används för att misskreditera makthavare och splittra landet, till angrepp som syftar till att slå ut infrastruktur, skada tilliten till institutioner, eller på annat sätt framtvinga eller förhindra att en stat agerar.



EXEMPEL FRÅN VERKLIGHETEN

2018 publicerade en hotaktör personlig information om svenska idrottsutövare på en hemsida som aktören själv kontrollerade. Denna information användes för att misskreditera Sveriges antidopningsarbete i internationella sammanhang och genom detta gynna sina egna intressen.

Hotaktören fick åtkomst till informationen genom ett cyberangrepp som gav aktören otillåten åtkomst till data.

Statliga aktörer genomför angrepp för att få åtkomst till individers personliga information. Angreppen sker exempelvis i syfte att få fram känsliga uppgifter som kan användas i utpressningssyfte mot personer i maktposition eller personer som har tillgång till information som aktören vill åt. Det sker även i syfte att bedriva flyktingspionage för att kontrollera oppositionella eller tysta opinioner utomlands. För att komma åt information om individer kan verksamheter som hanterar stora mängder av denna typ av uppgifter angripas. Angrepp sker även direkt mot individers personliga it-utrustning.

Militär förmåga

De statliga aktörerna bedriver underrättelseinhämtning mot bland annat svensk försvarsindustri och svenska myndigheter i syfte att kartlägga Sveriges förmåga och sårbarheter med koppling till Sveriges försvarsförmåga. I detta söker man information från öppna källor, men även genom cyberangrepp. Många länder utvecklar dessutom en förmåga att genomföra avancerade cyberoperationer, bland annat offensiva cyberangrepp.

I konflikter mellan stater är cyberoperationer ett av de medel som kan användas för att minska ett lands försvarsvilja. De kan stödja påverkansoperationer där information som stjäls genom cyberangrepp sedan kan manipuleras och publiceras för att påverka opinionen. Stater kan även genomföra angrepp som stör eller avbryter samhällsviktiga eller försvarsrelaterade funktioner i syfte att minska ett lands förmåga att stå emot ett kommande militärt angrepp eller försvaga ett lands motståndskraft mot påtryckningar. Genom att välja vilka mål hotaktören inriktar sig mot och hur stor effekt som ska uppnås, finns möjlighet för en statlig aktör att operera i ett tillstånd av fred där krigets lagar inte är tillämpliga. Problematiken kring attribuering och förnekbarhet stärker denna möjlighet. I det fall ett cyberangrepp orsakar skada på samma sätt som ett konventionellt väpnat angrepp kan det under vissa förutsättningar vara att betrakta som ett väpnat angrepp.

Som förberedelse för att använda cyberangrepp i konflikter studerar statliga aktörer sårbarheter som kan utnyttjas. De utvecklar därefter de verktyg som behövs för att genomföra cyberoperationer. De utnyttjar sedan sårbarheterna för att ta sig in i system och infektera dessa för att kunna slå ut systemet i det fall en konflikt uppstår. Attackerna förbereds således med fördel i fredstid och kan sedan koordineras med konventionella stridsmedel om det gynnar operationen.

Takten i den tekniska utvecklingen är hög och det upptäcks kontinuerligt nya sårbarheter som sedan åtgärdas. Det pågår således en ständig kapplöpning mellan medel och motmedel. Därför krävs det ett konstant utvecklingsarbete för att upprätthålla en förmåga till avancerade cyberoperationer.

KAN CYBERANGREPP STARTA KRIG?

Ett cyberangrepp kan under vissa förutsättningar vara att betrakta som ett väpnat angrepp och därmed ge en angripen stat rätt att vidta åtgärder i självförsvar enligt artikel 51 i Förenta nationernas stadga. Detta skulle kunna utlösa förpliktelser enligt EU-fördragets artikel 42.7 som innebär att övriga medlemsstater i EU är skyldiga att ge den utsatta medlemsstaten stöd och bistånd med alla till buds stående medel.

Ekonomiska intressen

Vissa stater bedriver omfattande program som syftar till att stjäla företagshemligheter från andra länder, för att sedan ge dem till företag i det egna landet i syfte att öka sin egen konkurrenskraft. Brister i det egna landets innovationsförmåga uppvägs med andra ord genom industrispionage som möjliggörs genom cyberangrepp.

Cyberangrepp i syfte att genomföra industrispionage mot svenska mål är numera en del av vardagen. Dessa angrepp innebär att svenska företag som utvecklar ny teknik kan komma att konkurreras ut av sina egna lösningar som stulits av statliga aktörer.

Kunskap och innovationer är stöldbegärliga för de stater som vill ta genvägar i sin egen teknikutveckling. Många svenska företag och lärosäten har stora mängder forskningsresultat, utvecklingsprojekt och patentsökningar och dessa representerar enorma värden. För Sverige som är ett utrikeshandelsberoende land är det viktigt att vara en säker marknadsplats. Cyberhotet från statliga aktörer som drivs av ekonomiska intressen är över tid mycket allvarligt för Sveriges fortsatta välstånd och förtroende i omvärlden.

EXEMPEL FRÅN VERKLIGHETEN

2018 genomförde en hotaktör en cyberoperation mot ett stort antal universitet och högskolor i flera länder. Även svenska universitet och högskolor fanns bland de drabbade.

Syftet med denna cyberoperation var sannolikt att, med hjälp av spearphishing, stjäla information för att gynna det egna landets forskning och utveckling.

Det finns även exempel i omvärlden där statliga aktörer har använt cyberangrepp för att skaffa sig monetära tillgångar, exempelvis genom att angripa banker för att stjäla pengar, kryptovaluta eller genom att angripa verksamheter och infektera dem med utpressningstrojaner (ransomware) för ekonomisk utpressning. I tider av sanktioner kan stater sättas under stor ekonomisk press och då kan cyberangrepp för att stjäla pengar vara en lösning för landets överlevnad.

Ideologiskt motiverade aktörer

Med ideologiskt motiverade hotaktörer avses organisationer, enskilda individer eller grupper vars handlingar är drivna av ideologiska skäl och ambitioner. Tillgång på verktyg och kunskap inom cyberområdet varierar stort och följaktligen är förmågan varierande såväl bland enskilda individer som bland grupper.

Det finns ett flertal ideologiskt motiverade aktörer som betraktar angrepp mot svenska mål som legitima. Den generella förmågan att utföra cyberattacker står däremot för närvarande sannolikt inte i paritet med ambition, vilja och avsikt att genomföra sådana. Försök till cyberangrepp med enklare tekniska medel och metoder kommer emellertid troligen att fortsätta, såsom kapade hemsidor eller distribuerade överbelastningsattacker (DDoS).

HACKTIVISM

Hacktivism kan beskrivas som en slags digital och civil olydnad som realiseras genom att utnyttja teknik för att förmedla någon typ av politiskt budskap som kan avse exempelvis censur eller mänskliga rättigheter. Det kan handla om att uppmana andra att utföra cyberangrepp för ett visst angivet syfte.

Kriminella aktörer

Cyberkriminalitet är en internationell och gränsöverskridande verksamhet som genomförs där det finns möjligheter att tjäna pengar. Kriminella söker genom minsta möjliga risk erhålla största möjliga avkastning. Där det finns pengar att tjäna kommer således även de kriminella att befinna sig. Vilket mål aktören väljer är oftast inte intressant, utan det viktigaste är vilken vinst man kan räkna med. Ransomware, bedrägerier, stölder och liknande kriminella aktiviteter drabbar inte enbart företag utan även myndigheter och deras leverantörer. Det innebär att detta kan drabba även verksamheter med höga skyddsvärden.

En tillbakablick på inträffade händelser visar att hotaktörer har en tendens att använda de verktyg som fungerar för stunden. Istället för att använda nya och avancerade metoder väljer de att förfina existerande metoder och det blir allt svårare för användare att upptäcka förfalskningar och bedrägerier.

DDoS-angreppen fortsätter där det vanligaste motivet är utpressning men också många gånger med intentionen att endast orsaka målet skada.

Spridningen av utpressningstrojaner har skiftat från att riktas brett och urskillningslöst, till att istället riktas mot specifika företag. Förhoppning-

DARKWEB

Darkweb är ett sammanhållet begrepp för att beskriva ett antal slutna nätverk som utnyttjar internet som bärare. Åtkomst till Darkweb kräver ofta särskilda mjukvaror, konfigurationer eller åtkomsträttigheter. Exempelvis är TOR ett sådant nätverk på vilket Darkweb-innehåll kan existera.

Darkweb används av de kriminella för sin brottsliga verksamhet genom att sälja produkter och tjänster. Det har uppstått en mikro-infrastruktur av forum som inriktas särskilt mot vissa typer av produkter och tjänster. Krypterade kommunikations- och betalningslösningar bidrar till att säljare och köpare kan ha ett skyddat utbyte med varandra.

en är att gå från flera små, till färre och istället större betalningar. Denna strategiska skiftning har varit framgångsrik vilket bekräftas av den rapportering som finns i öppna källor, exempelvis diverse säkerhetsföretags årliga rapportering.

Kriminella hotaktörer fokuserar även på att inhämta kreditkortsuppgifter som antingen används av dem själva, eller så säljs uppgifterna vidare på Darkweb. Tidigare har ett tillvägagångssätt varit att använda phishing av olika slag för att lura till sig sådana uppgifter direkt från enskilda individer. Ett skifte är att aktörer flyttat fokus från angrepp direkt mot individer till att istället angripa mindre e-handelsplatser där de får större effekt av sina cyberangrepp.

Personuppgifter är känslig information och samtidigt en eftertraktad tillgång som kan säljas på Darkweb eftersom de kan användas för att underlätta brottslig verksamhet som exempelvis bedrägerier. Personuppgifter kan även säljas till andra kriminella individer och grupper som har möjlighet att utnyttja uppgifterna i andra brottsliga sammanhang.

Företag som i någon utsträckning hanterar kryptovalutor, antingen genom att tillhandahålla tjänster som växlar kryptovaluta mot ”vanliga” valutor, eller där kryptovalutor accepteras som betalningsmedel, kan också bli mål för cyberangrepp enligt samma princip.

Metoder för initial åtkomst

Ett viktigt steg i ett cyberangrepp är den initiala kontroll angriparen behöver skaffa sig i systemet man vill få åtkomst till. Målsättningen med detta steg är vanligen att angriparen vill få möjlighet att exekvera skadlig kod i systemet för att på så sätt exempelvis erhålla möjligheter att påverka systemet i sig eller kunna nå priviligierad information i detsamma.

Även om hotaktörernas metoder utvecklas löpande så ser vi att gamla beprövade tekniker fortfarande i stor utsträckning fungerar och att de fortsätter att använda sig av dessa. I detta avsnitt beskrivs vanliga eller effektiva metoder som används för att få initial kontroll vilka ofta benämns attack- eller angreppsvektorer. Dessa metoder används ofta vid cyberangrepp men ska inte betraktas som en uttömmande lista, utan en delmängd av de metoder som ofta används av flera typer av aktörer.

För att dessa metoder ska kunna användas förutsätts att det finns en eller flera sårbarheter som kan utnyttjas av angriparen.

VANLIGT FÖREKOMMANDE SÅRBARHETER SOM EN ANGRIPARE UTNYTTJAR

- Brister i autentiseringsmekanismer
- Brister i behörighetshantering
- Arkitekturella svagheter (segmentering och filtrering i nätverk), virtualisering, otillräcklig separering av nät som gör att information tillgängliggörs på ett sätt som inte är avsett
- Brister i underhålls-, livscykel- och uppdateringsrutiner
- Äldre it-system som inte underhålls i tillräcklig utsträckning är i bruk
- Otillräcklig härdning mot skadlig kod, vitlistning av applikationer saknas, övertro på antivirusprodukter
- Brister i utveckling och underhåll av interna applikationer
- Ej administrerad och hanterad utrustning ansluts till nätverket
- Loggning och detektion är bristfällig
- Ingen organisation eller kunskap för incidentupptäckt och hantering
- Aktiva konton för medarbetare som inte längre arbetar kvar

EN MARKNAD FÖR HANDEL MED SÅRBARHETER

Det pågår ständig forskning i jakt på nya och okända sårbarheter, så kallade zero-day-sårbarheter. Okända sårbarheter som upptäcks av hotaktörer kan utnyttjas utan omvärldens vetskap och utan skydd mot dessa sårbarheter.

Till följd av detta har det uppstått en marknad för zero-days där både kriminella och statliga aktörer utgör köpare och säljare. På denna marknad säljer individer och företag sårbarheter till mäklare, som sedan säljer vidare till andra tillverkare, kriminella eller statliga aktörer.

Lösenordsattacker

Angripare har tillskansat sig lösenord sedan datorsystem kunde kopplas upp med modem på det sena 1980- talet. Dessa metoder fortsätter än idag att användas med stor framgång. Särskilt vanligt är det med lösenordsattacker mot publikt tillgängliga e-postservrar, databaser och tjänster för exempelvis fjärrstyrning (Remote Desktop Protocol, RDP) och Virtual private network (VPN-anslutningar).

Kvalitén på lösenord är ofta väldigt låg i många verksamheter, vilket innebär att en stor del av lösenorden går att forcera med beräkningskraften på en vanlig laptop. Ett stort problem är också när samma lösenord används till flera olika konton, vilket är alltför vanligt. Allt detta innebär stora risker för säkerheten.

En vanlig metod är att forcera fram lösenord från lösenordshashar (ett resultat av en matematisk envägsfunktion av ett lösenord för att skydda det) från läckta databaser som tillgängliggjorts på internet. I de fall lösenord är av bättre kvalitet ska man ha i åtanke att statliga aktörer har betydligt större resurser än kriminella och kan använda superdatorer för att forcera fram lösenord som är av stort intresse för den statliga aktören.

När en hotaktör väl har fått initial åtkomst till ett nätverk är en bristfällig lösenordshantering i många verksamheter ett tacksamt mål att ge sig på för eskalering av behörigheter och på så sätt ta kontroll över hela it-miljön.

Angrepp via e-post

Att använda e-post för att genomföra angrepp kallas nätfiske (phishing) eller, i de fall angreppet är riktat mot en eller ett fåtal individer, riktat nätfiske (spearphishing). Syftet med denna metod är att få en användare att agera på ett sätt som hjälper angriparen. Detta sker genom att angriparen skickar e-postmeddelanden som ska verka legitima och på så sätt får användaren att klicka på en länk i meddelandet, öppna ett bifogat dokument eller tillåta innehåll i e-postmeddelandet, exempelvis en bild, att hämtas från internet. Gör användaren något av detta hjälper det angriparen på något sätt att uppnå sitt syfte.

Angreppet kan handla om att lura mottagaren att lämna ifrån sig ett lösenord, kreditkortsuppgifter, delta i penningtvätt eller installera skadlig kod. I det fall hotaktören är ute efter att samla in vissa uppgifter behöver inte alltid användaren aktivt ange sina uppgifter för att hotaktören ska få tag på det den är ute efter, utan det kan ske i bakgrunden utan att användaren är medveten om att så sker.

Phishing och spearphishing är framgångsrikt eftersom det i stor utsträckning utnyttjar mänskliga egenskaper, exempelvis nyfikenhet. Det är även framgångsrikt då det utnyttjar bristfällig implementation av tekniska skyddsåtgärder, som exempelvis avsaknad av kontroll enligt Sender Policy Framework (SPF) i de fall avsändaren av e-postmeddelandet är förfalskat.

Phishing

Phishing är den metod som riktas mot en bredare målgrupp och har som mål att träffa så många offer som möjligt. Detta leder till att när angripare använder phishing är det mycket sällan dessa inkluderar några personliga detaljer.

Något som har uppmärksammats under 2019 i utformandet av phishing är användandet av moln-

baserade tjänster, vilket utnyttjar det befintliga förtroendet mellan användare och tjänsteleverantör. En ökning har noterats av phishing-angrepp där angriparen använder sig av Sharepoint och Office-365 för att få tillgång till användarens inloggningsuppgifter samt för att leverera skadlig kod. Allt detta sker då via en för användaren ”godkänd” krypterad anslutning (HTTPS) till t.ex. Google eller Microsoft. Det är i huvudsak kriminella som använder sig av phishing och det är en vanlig metod som används dagligen. Verksamheter med en medvetenhet om hotet, implementerade e-postskydd samt att mottagare gjorts uppmärksamma på att inte klicka på länkar eller öppna dokument som de inte förväntar sig att få, har visat sig vara bättre rustade att möta denna metod än de som inte har det.

EXEMPEL FRÅN VERKLIGHETEN

I december 2019 upptäcktes en phishingkampanj som skapade en falsk hemsida som utgav sig för att vara en registreringssida för Regeringskansliets upphandlingsfunktion.

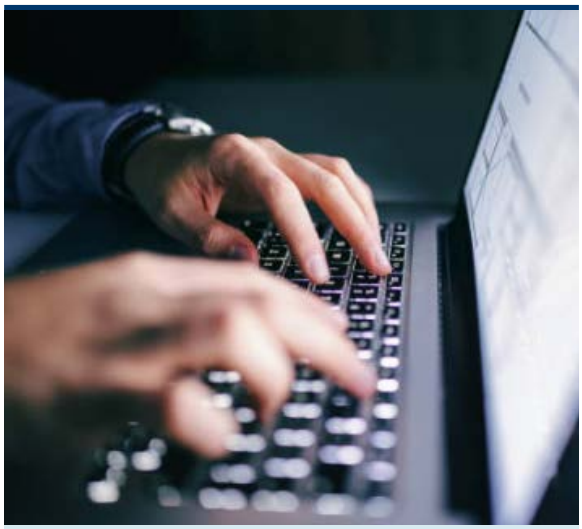
Besökare lockades via e-post att registrera sig och i samband med detta ange uppgifter om sin verksamhet. Denna kampanj riktades även mot ett flertal andra länder där samma tillvägagångssätt användes.

Spearphishing

Ett spearphishingangrepp inkluderar personliga detaljer som exempelvis ett namn eller referenser till något som är av intresse för mottagaren och skickas vanligtvis till ett begränsat antal mottagare. Detta kräver att hotaktören har kartlagt organisationen eller personen för att kunna utforma ett riktat angrepp.

Spearphishing förekommer ofta i cyberangrepp som genomförs av statliga aktörer. Dessutom använder även kriminella spearphishing i allt större utsträckning. Kriminella har skiftat från att försöka träffa många till att istället träffa få, men istället utvalda offer, i spridandet av exempelvis ransomware. Detta skifte i valet av mål har gjort det nödvändigt för kriminella att anpassa sin aktivitet att bli mer riktade mot enskilda mål och då gått över till spearphishing.

Spearphishingangrepp som liknar en tjänst mottagaren faktiskt använder har mycket större framgång än phishingangrepp, men det kräver mer resurser från hotaktören då de behöver veta mer om användaren, vilka tjänster som används och vad användaren förväntas få för e-post.



EXEMPEL FRÅN VERKLIGHETEN

Under hösten 2019 blev statliga verksamheter utsatta för phishing där angreppen lyckades i ett par fall. I ett fall fick en användare ett e-postmeddelande med en länk till sharepoint.com från en avsändare i dennes kontaktlista, som såg legitimt ut och var betrodd av antispam-filter. När användaren klickade på sharepoint-länken visades en förfalskad inloggningssida till Office-365. Att sidan använde sharepoint.com ökade trovärdigheten avsevärt. Användaren angav sina uppgifter för att logga in, varpå användaren då ovetandes skickade uppgifterna vidare till en av angriparen kontrollerad databas.

Angriparen kunde sedan logga in med användarens inloggningsuppgifter och därefter skicka ut samma phishing-mejl till nya mottagare, bland annat till kontakter i den angripnes kontakbok

Webbattacker

Webbapplikationer är många gånger komplicerade konstruktioner sammansatta av lager på lager av abstraktioner och komplexa kodberoenden. Framförallt sammanflätas presentationslagret – den kod

som beskriver hur något ska visas i webbläsaren – med sådan kod som är logisk, det vill säga den kod som avgör vad som ska visas. Detta kan innebära att en angripare ges möjlighet att genom någon form av användarinput, skjuta in logisk kod genom presentationslagret som sedan används av webb-applikationen.

Ett exempel på detta är SQL-injection (Structured Query Language, SQL, ett standardiserat programspråk för relationsdatabaser) vilket innebär att angriparen injicerar kod genom exempelvis ett inmatningsfält. Koden följer sedan med hela vägen till en bakomliggande databas där den exekveras. Exempelvis kan detta leda till att information i bakomliggande databaser kan läsas eller förändras eller att inloggning kan ske utan giltigt lösenord.

Detta är en metod som används av både statliga aktörer och kriminella.

Angrepp mot publikt exponerade tjänster

En server exponerar vanligtvis ett flertal tjänster mot de nätverk till vilka den är ansluten och för varje tjänst används ett givet protokoll. Alla protokoll och tjänster består av diverse programvarukomponenter. Vissa komponenter kan bestå av öppen källkod och används av många. Andra komponenter kan vara proprietära och utvecklade av organisationen själv eller inköpta från företag. Det förekommer att tjänster som inte är avsedda att användas externt ändå är publikt exponerade. Dessa är sårbara om de inte är korrekt konfigurerade för detta eller har ett sämre underhåll och därmed inte säkerhetsuppdaterats i tillräcklig omfattning.

En sårbarhet i någon av alla dessa komponenter kan ge en angripare möjlighet att genomföra ett angrepp mot servern. För en tid sedan identifierades en sådan sårbarhet i komponenterna för SMB (Server Message Block) som är ett vanligt protokoll för kommunikation i Windows-baserade nätverk. Sårbarheten gjorde att en angripare kunde exekvera godtycklig kod på servern utan att först behöva autentisera sig.

Metoder för att genomföra serverattacker kan generellt sägas vara relativt enkla att använda givet att verktygen är publikt tillgängliga. Strax efter att en sårbarhet blivit publikt känd blir ofta verktyg som utnyttjar sårbarheten allmänt tillgängliga på internet. Detta gör att metoderna kan användas av kriminella, statliga aktörer och ideologiskt motiverade aktörer.

Däremot förutsätts oftast avsevärt mer kunskap för att själv kunna utveckla dessa verktyg och utveckla kod som utnyttjar sådana här sårbarheter. Statliga aktörer har denna kompetens, men även en del enskilda individer.

EXEMPEL FRÅN VERKLIGHETEN

2017 utsattes ett stort antal organisationer för ekonomisk utpressning som möjliggjordes av en sårbarhet i Windows SMB-protokoll som utnyttjades för att installera skadlig kod i form av utpressningstrojaner, så kallad ransomware. Bland de utsatta fanns även organisationer i Sverige.

Denna utpressningskampanj kallas i öppna källor för WannaCry. Konsekvenser av denna typ av cyberangrepp kan bli stora för organisationerna som drabbas.

Vattenhålsangrepp

Till skillnad mot phishing där angriparen skickar något till offret innebär vattenhålsangrepp att angripare placerar skadlig kod på en hemsida och sedan väntar på att användare ska besöka hemsidan. Detta kan göras som ett riktat försök där skadlig kod placeras på en hemsida som är av stort intresse för en given användare eller grupp av användare. Metoden kan exempelvis kombineras med webbattacker för att placera den skadliga koden på aktuell hemsida, eller genom exempelvis annonsnätverk.

Vattenhålsattacker används av både statliga aktörer och kriminella.

EXEMPEL FRÅN VERKLIGHETEN

En hotaktör angrep en legitim utländsk webbsida och modifierade koden på sidan för att stjäla inloggningsuppgifter från webbsidans besökare. Hösten 2019 besökte en person på en svensk myndighet webbsidan från sin arbetsplats men i det här fallet stoppades angreppet hos myndigheten och ingen information delades vidare.

Besökare från Sverige var sannolikt inte det främsta målet men hade angreppet lyckats hade hotaktören kommit över personens lösenord och potentiellt kunnat använda informationen för att utföra vidare angrepp för att ta sig in i myndighetens nätverk.

Angrepp mot mjukvaruleverantörer

Denna metod kallas supply chain-angrepp och innebär att en angripare först identifierar en mjukvara som används av målet. Därefter angrips mjukvaruleverantören där angriparen exempelvis lägger till skadlig kod i programvaran som används. Detta innebär att när programvaran uppdateras laddas även den skadliga koden ner direkt in i organisationen. Denna metod innebär att angriparen inte har kontroll över spridningen av den skadliga koden från mjukvaruleverantören.

Det händer även att öppen källkod utsätts för modifiering och därefter tillgängliggörs på en publik webbplats. När användare därefter laddar ned den modifierade koden följer de skadliga delarna med.

Detta är en avancerad metod som används primärt av statliga aktörer.

EXEMPEL FRÅN VERKLIGHETEN

2017 skedde ett av de mest skadliga cyberangreppen någonsin och som i öppna källor kallas NotPetya. Detta angrepp utfördes genom att först göra ett supply chain-angrepp mot ett mjukvaruföretag i Ukraina. Koden för en viss mjukvara modifierades och skadlig kod infördes som sedan spreds till flera organisationer som var de slutliga målen för angreppet. Genom detta kunde aktören etablera ett första steg in i dessa organisationer.

Genom att modifiera kod i mjukvara som de slutliga målen normalt använder kan aktören ta sig igenom det yttre skydd som annars finns. I det här fallet fick den skadliga koden en omfattande spridning, även till verksamheter som sannolikt inte tillhörde de avsedda målen.

Angrepp mot mobila enheter

Mobiltelefoner, surfplattor och andra bärbara enheter är plattformar som genom cyberangrepp kan omvandlas till verktyg för inhämtning. En infekterad mobiltelefon kan användas för att inhämta mycket information om individen (e-post, kreditkort, planerade resor, bilder, meddelanden, kontaktlistor, gps-positionering m.m.) samt använda för att på distans avlyssna telefonens omgivning. Denna risk finns även hos de allt fler nya typer av små enheter som kopplas upp mot internet i sakernas internet (internet of things, IoT). Ett vanligt tillvägagångssätt att få in skadlig kod på mobiltelefoner är genom applikationer som oftast installeras från en tredje part.

Utöver att inhämta personlig information eller att användas för avlyssning kan mobiltelefoner sprida infektioner vidare till nätverk som mobiltelefonen kopplas in på. Beroende på omständigheterna kan

det vara bra att tänka på hur och när man använder mobiltelefoner. Mobiltelefoner är it-system som kräver löpande tekniskt underhåll och övervakning precis som andra it-system.

EXEMPEL FRÅN VERKLIGHETEN

Forskare på företaget Checkmarx upptäckte under 2019 allvarliga säkerhetsbrister hos Googles och Samsungs kameraapplikationer. Dessa sårbarheter innebar att det gick att gå runt en mobilapplikations åtkomsträttigheter och få full kontroll över mobiltelefonens kamera. Detta innebar att det gick att på distans ta foton, spela in video, lyssna på samtal, lokalisera mobiltelefonens position med mera.

Innan sårbarheterna publicerades hann Google och Samsung åtgärda sårbarheterna och ge ut säkerhetsuppdateringar.

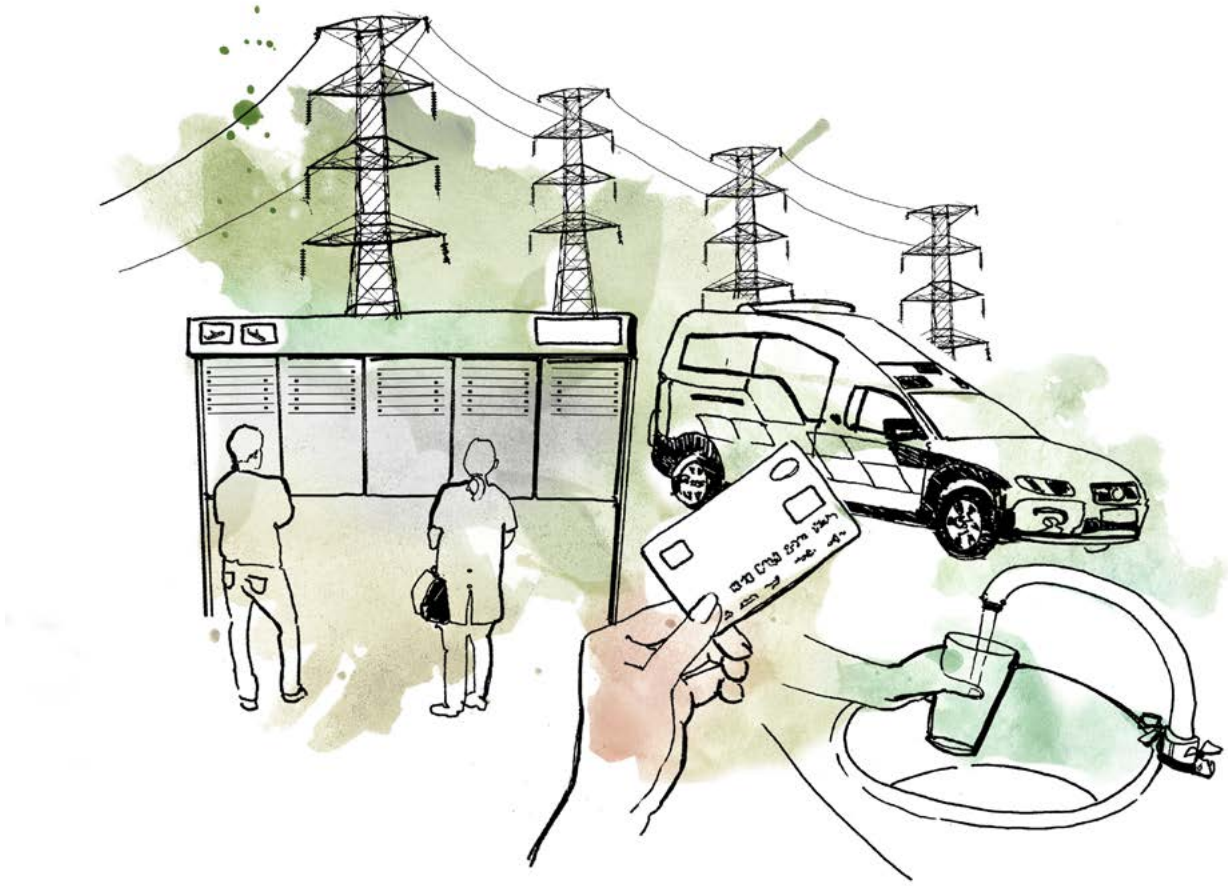
Cyberangrepp på mobiltelefonerer används riktat inte minst av statliga aktörer för att inhämta personlig information om målen.

Fysisk åtkomst

Istället för att använda avancerade yttre angreppsvektorer kan en människa, med fysisk åtkomst till nätverk som kanske är svårtillgängliga via internet, användas för att föra in skadlig kod.

En metod är att använda sig av USB-stickor som innehåller skadlig kod och som sprids på sätt som gör det möjligt att de hamnar i rätt händer och kopplas in i de nätverk som är målet för angreppet. Det kan göras på ett sätt som innebär att personer ovetande för in den skadliga koden.

En annan metod är att rekrytera en människa på insidan av en organisations yttre skydd för att på så sätt underlätta injicering av skadlig kod eller på annat sätt exempelvis tillgängliggöra kritisk information. En insider kan vara en person som antingen blir rekryterad av en aktör eller en missnöjd anställd som själv blir aktören som gör skada. En insider kan även skapas genom att man utnyttjar dennes personliga situation på olika sätt för att få insidern att agera som hotaktören vill.



Brister och beroenden

Det högteknologiska svenska samhället anammade tidigt de möjligheter som informationstekniken erbjuder. Arbetet med cybersäkerhet har dock inte gått i samma takt som digitaliseringen, vilket över tid har inneburit en ökande risk. Med implementeringen av ny teknik har vi skapat ett beroende av kontinuerligt fungerande informationsteknik och kommunikation. Beroendet sträcker sig från kritiska system som är av betydelse för samhällets funktionalitet, till system och applikationer som används i den enskildes vardag.

I detta avsnitt ges exempel på mer strukturella brister och beroenden som är aktuella ur ett svenskt perspektiv.

Avsaknad av ett strukturerat säkerhetsarbete

Cybersäkerhet är en viktig del i nästan allt säkerhetsarbete eftersom digital information och digitala tjänster används i någon form i de flesta verksamheter. Det har dock visat sig att arbetet med cybersäkerhet i Sverige går trögt, med brister i cybersäkerheten som följd. Genomförda tillsyner och granskningar visar att arbetet med cybersäkerhet inte är ändamålsenligt sett till de hot och risker som finns.

Ett bristande säkerhetsarbete är ett risktagande. Röjande av integritetskänsliga uppgifter kan skada individer. Skador på system och funktioner eller manipulering av uppgifter kan skada hela verksamheter.

Effekten av en organisations säkerhetsarbete avgörs i hög grad av ledningens inställning. Alla behöver ta ansvar, men det är avgörande att ledningen tar ansvar för, stödjer och följer upp säkerhetsarbetet. Det är viktigt att detta tydliggörs på alla nivåer inom organisationen.

Bristen på ett systematiskt cybersäkerhetsarbete

är vanligt förekommande. Ett systematiskt förhållningssätt förutsätter att ett grundarbete genomförs som identifierar verksamhetens skyddsvärden, vilka hot och risker som riktas mot dem, och identifierar vilka säkerhetsåtgärder som behöver vidtas. För att upprätthålla en god cybersäkerhet krävs dock kontinuitet – om en verksamhet förändras innebär det att deras säkerhetsintressen också förändras. Dessutom varierar säkerhetshotet över tiden. Planering och genomförande av säkerhetsarbete är inte en engångsföreteelse vars resultat gäller för all framtid, utan en dynamisk process som kräver fortlöpande uppföljning och utvärdering.

De framsteg som sker inom informationsteknik gör att samhället behöver förhålla sig till nya teknologier i samband med sin verksamhetsutövning. Dessa tekniksprång ställer krav på att verksamheterna förstår och kan bedöma förändringar i sin teknikanvändning. När ny teknik introduceras sker det gradvis och det kan på så vis vara svårt att fastställa en tidpunkt när man behöver revidera en säkerhetsanalys. Det är ofta svårt att tydligt definiera ett särskilt tillfälle när en verksamhet har anammat en ny teknik i sådan omfattning att den påverkar tidigare bedömningar.

Regelverken ställer krav på säkerhet och skapar enhetlighet i tillämpningen. Lagar kan dock inte skrivas anpassat för varje verksamhet, vilket innebär att de uttrycks generellt för att kunna tillämpas av alla som omfattas av dem. För att nå full effekt behöver lagarna brytas ned och omsättas i åtgärder som är anpassade för den specifika verksamheten i fråga. För att förstå regelverken, tillämpa kravställningen på sin verksamhet och bedöma hur implementeringen behöver ske samt hur den ska underhållas och anpassas över tid, krävs kompetens.

EXEMPEL PÅ ÅTERKOMMANDE BRISTER SOM INNEBÄR ETT RISKTAGANDE

- Man har inte fullt ut identifierat sina skyddsvärden.
- Kunskap om dimensionerande hotbeskrivning* saknas.
- Lågt engagemang i säkerhetsfrågor.
- Otydligt ansvar och ägarskap för säkerhetsfrågor.
- Bristfällig hot- och riskanalys.
- Information är inte korrekt inventerad och klassificerad.
- Processer, regler och policys saknas eller har brister.
- Beslutade säkerhetsåtgärder genomförs inte.
- Bristfällig livscykelhantering av system.
- Brister i avtal med leverantörer och deras underleverantörer om sekretess, kontrollmöjligheter och andra hanteringsregler.

** Dimensionerande hotbeskrivning utgör en beskrivning av antagna antagonistiska förmågor hos hotaktörer som särskilt säkerhetskänsliga verksamheter kan behöva skyddas mot, även om det inte föreligger något identifierat hot mot den säkerhetskänsliga verksamheten.*

Bristande kravställning vid upphandling och utkontraktering

En väl beskriven kravställning är en förutsättning för en bra upphandling. Att kravställa cybersäkerhet kräver kompetens, både när det gäller anskaffning av varor, tjänster och vid utkontraktering.

Det finns tillfällen där anskaffning av varor och tjänster som hanterar information med ett högt skyddsvärde har genomförts utan tillräcklig identifiering och värdering av systemets skyddsvärden. Det har skapat risker för den information eller verksamhet som systemet hanterar. Detta är inte ovanligt, vilket innebär att krav på säkerhet istället arbetas in i efterhand, i takt med att det uppenbaras. Om verksamheten omfattas av upphandlingsregler kan hela utkontrakteringen behöva göras om. Även i de fall en helt ny upphandling inte behöver ske är säkerhet kostsamt och ibland svårt att arbeta in i efterhand.

Med en adekvat kravställning kan utkontraktering av it-infrastruktur vara en säkerhetshöjande åtgärd jämfört med att behålla hela ansvaret själv. Många svenska verksamhetsutövare, såväl offentliga som privata, utkontrakterar av denna anledning olika

delar av hanteringen av sin it-infrastruktur till tjänsteleverantörer.

Vid ett beslut om utkontraktering behöver beställaren förstå hur tjänsterna som ska levereras är konstruerade och vad en sådan lösning innebär ur säkerhetssynpunkt. För att avgöra om en utkontraktering ger ett tillräckligt skydd krävs att den som beställer har en förmåga att bedöma helheten i den lösning som erbjuds. Då krävs en förståelse för hur olika tekniska säkerhetsfunktioner fungerar och hur de tillsammans skapar en sammanhållen säkerhetslösning, men dessa bedömningar sker ofta på ett otillräckligt sätt.

EXEMPEL FRÅN VERKLIGHETEN

En verksamhetsutövare bedömde att delar av myndighetens it-infrastruktur skulle utkontrakteras genom upphandling. Inför upphandlingen identifierades dock inte alla skyddsvärden som var kopplade till systemen. Därmed bedömde man inte att det fanns behov av en säkerhetsskyddad upphandling.

Utkontraktering gjordes till en tjänsteleverantör, vars underleverantörer inte säkerhetsprövade personalen innan start och utan att man avtalat om regler för den information som hanterades, vilket innebar att skyddsvärda uppgifter var att betrakta som röjda.

Det är vanligt att flera tjänsteleverantörer delar på hanteringen av utkontrakterad it-infrastruktur, exempelvis som underleverantörer. Då kan det vara svårare för kunden att ställa krav på en kontinuerlig säkerhetsnivå som följs av samtliga leverantörer. Referenser till regelverk kan vara till stöd både för kunder och leverantörer, exempelvis när information och tjänster befinner sig på flera olika ställen.

Större tjänsteleverantörer som erbjuder sina tjänster gentemot svenska verksamhetsutövare bedriver i regel sin verksamhet i flera länder och omfattas på så vis av en annan jurisdiktion än den svenska. Det medför att utländsk lagstiftning kan bli tillämplig för de tjänster man levererar i Sverige, och den ger i vissa fall leverantören – och dess underleverantörer – rätt att ta del av information som hanteras inom ramen för den tjänst som levereras.

Utkontraktering av it-infrastruktur innebär även att det skapas ett beroende av tjänsteleverantören. När it-tjänster utkontrakteras sker det inte sällan till globala tjänsteleverantörer, vilket innebär att det beroende som uppstår är internationellt. Detta uttrycks ibland som en risk för förlust av digital suveränitet, ett begrepp som använts i EU-sammanhang och innebär att en stat förlorar delar av sin kontroll över sitt oberoende, självständighet och handlingsfrihet på det digitala området.

En annan effekt av utkontraktering av it-tjänster är att tjänsteleverantörer samlar flera kunder med verksamheter som innehåller skyddsvärden. Det innebär att den samlade mängden av kundernas information och tjänster hos en tjänsteleverantör gör att leverantören behöver beakta om dess verksamhet – till följd av kundernas skyddsvärden – når en nivå där den i sig är att betrakta som säkerhetskänslig. För att detta överhuvudtaget ska vara möjligt för tjänsteleverantören måste dock kunden kommunicera detta, då leverantören inte som regel själv kan identifiera detta genom sin leverans av det avtalade uppdraget.

I Sverige är verksamhetsutövare i hög utsträckning beroende av informationsteknologi. Kraven på hur en verksamhet ska hantera sin cybersäkerhet ställs genom reglering, men de finns även i form av marknadsmässiga krav på effektivitet, kvalitet och säkerhet för att kunna upprätthålla verksamhetens konkurrenskraft. Det är svårt för vissa verksamhetsutövare att helt på egen hand uppfylla de krav som ställs på säkerhet. En lösning för dessa verksamheter kan vara att utkontraktera sina behov till en tjänsteleverantör som har bättre möjligheter att möta säkerhetskraven. Genom att utkontraktera dessa delar av verksamheten kan verksamhetsutövarna lägga ett större fokus på sin kärnverksamhet samtidigt som cybersäkerheten blir bättre.

En vanlig form av utkontraktering sker via delade molntjänster, det vill säga att en verksamhet istället för att på egen hand investera i egen hård- och

mjukvara hyr de resurser som behövs, vilket kan vara allt från enskilda applikationer till hela eller delar av efterfrågad it-infrastruktur.

Det innebär dock säkerhetsutmaningar eftersom verksamhetsutövaren i praktiken lämnar över kontroll över system och information till en tjänsteleverantör. Användandet av molntjänster innebär dessutom att insynen försämras för verksamhetsutövaren jämfört med om man hade hanterat behovet inom den egna verksamheten.
En annan utmaning med delade molntjänster är att informationen i de allra flesta fall är indirekt exponerade mot såväl andra kunder som övriga på internet. Med andra ord kan en sårbarhet (såväl teknisk som administrativ) eller en felaktig konfiguration innebära att informationen direkt blir exponerad och sannolikt snabbt spridd till obehöriga. Det innebär att verksamhetsutövare måste hantera problematiken kring överförda hotbilder. Hotbilden mot en molntjänst blir den sammanlagda hotbilden mot alla kunder som använder molntjänsten.

Molnlösningar innebär också att en hotaktör inte längre enbart är hänvisad till att angripa ägaren till den information eller tjänst man vill påverka. Förutom molntjänstleverantören har alla övriga kunder en logisk access till den gemensamma it-infrastrukturen hos en leverantör. Det innebär att man är beroende av ett gott it-säkerhetsarbete hos såväl de andra kunderna som sin leverantör. Sådana hot är både svåra att bedöma och att hantera. Svårigheter att logga och spåra datatrafik i komplexa molnmiljöer kan dessutom göra det svårt att utreda incidenter ur såväl ett juridiskt som ett tekniskt perspektiv.

En annan samhällsutmaning är att molntjänsterna koncentreras till ett fåtal leverantörer. Det innebär att en hotaktör kan inhämta från eller slå ut flera samhällskritiska system samtidigt om man får tillgång till miljön. Den sammanlagda konsekvensen för samhället av ett angrepp blir i dessa fall högre än konsekvensen för ett angrepp mot ett enskilt system. Samtidigt kan en stor leverantör ha större resurser att fördela till sitt säkerhetsarbete, vilket kan göra dem svårare att angripa.

EXEMPEL FRÅN VERKLIGHETEN

Operation Cloud Hopper var ett omfattande cyberangrepp som avslöjades år 2017. Angreppet var inriktat mot tjänsteleverantörer som sköter drift och it-infrastruktur åt en rad samhällssektorer. Genom att kartlägga anställda hos tjänsteleverantörerna och skicka riktad e-post till dessa lurades de att avslöja inloggningsuppgifter eller att på annat sätt möjliggöra installation av skadlig kod hos tjänsteleverantören.

Efter intrången i nätverken lyckades hotaktören ta sig vidare till nätverk som tillhörde it-tjänsteleverantörernas kunder som var de egentliga slutmålen för cyberangreppet. Hotaktören lyckades på detta sätt stjäla information från ett stort antal företag och myndigheter i många länder inklusive Sverige. Hotaktörens syfte med cyberangreppet var sannolikt att gynna det egna landets ekonomiska utveckling och utrikespolitiska intressen genom att t.ex. skapa konkurrensfördelar för inhemska företag.

Det uppkopplade samhället

Digitaliseringen ökar möjligheterna för hotaktörer att genomföra cyberangrepp. När ny teknik introduceras uppstår ofta sårbarheter som i bästa fall åtgärdas i efterhand. Med fler uppkopplade enheter, exempelvis utrustning inom industrin för övervakning inom produktion, samt de flesta beståndsdelar i den ”smarta staden”, ökar risken för cyberangrepp. Alltmer utrustning kopplas upp, inte minst IoT-produkter som ofta har låg säkerhet med otillräckligt skydd. Dessutom har de ofta en kort livslängd, varför möjlighet till säkerhetsuppdateringar prioriteras bort efter en inledande period. Detta innebär att många IoT-produkter inte har möjlighet att ges ett ändamålsenligt skydd då de passerat sin förväntade livslängd, oavsett om de fortfarande används.

Sårbarheter i det uppkopplade samhället är sällan eller aldrig lokala företeelser. Introduktionen av nya tjänster och teknik sker i en takt som innebär att sårbarheterna ökar och att konsekvenserna av cyberangrepp blir svåröverblickbara.

EXEMPEL FRÅN VERKLIGHETEN

Ett exempel är internetexponerade frysar på en livsmedelsbutik. Dessa frysar var exponerade och åtkomliga på grund av dålig, eller obefintlig lösenordshantering. Detta möjliggjorde avstängning, eller reglering av temperatur, på distans.

Med en enkel sökning kunde flera liknande frysar identifieras och de som hade samma bristfälliga cybersäkerhetsarbete var även de exponerade för samma problematik.

EXEMPEL FRÅN VERKLIGHETEN

Mirai är ett botnät som angriper och infekterar IoT-produkter, till exempel hemmaroutrar och IP-kameror. Angreppet sker genom att utnyttja kända fabriksinställda inloggningsuppgifter där drabbade enheter infekteras med den skadliga koden. Den första varianten av Mirai upptäcktes 2016 och användes i mycket kraftiga överbelastningsattacker med bred påverkan, bland annat mot ett antal mål i Sverige.

Källkoden till Mirai är publikt tillgänglig och olika varianter av Mirai har fortsättningsvis använts i överbelastningsattacker och hot om överbelastningsattacker.

Det uppkopplade samhällets beroende av elektricitet och elektronisk kommunikation

Det uppkopplade samhället har ett stort beroende av fungerande eltillförsel och elektroniska kommunikationer. Allt fler verksamheter digitaliserar delar eller hela sin verksamhet vilket innebär ökade krav på tillgänglighet av el och fungerande uppkoppling. En konsekvens av digitalisering och effektivisering är att även förmågan att leverera el och upprätthålla kommunikationer är digitaliserad, och är därmed sårbar för samma svagheter och utsatt för liknande risker som övrig digitaliserad verksamhet. Förmågan att både producera och distribuera el styrs av ICS, som ibland har kontaktytor mot internet. I de fall dessa system är exponerade mot internet finns möjligheter för hotaktörer att utnyttja svagheter för att ta sig in i systemen.

En påverkan på elsystemet och leveransen av el skulle få stora konsekvenser för samhället. Förutom de omedelbara konsekvenserna med omfattande strömavbrott gällande människors liv och hälsa, så skulle väldigt många system som är beroende av fungerande informationsteknologi upphöra att fungera. Det som tidigare upplevdes som en smärre olägenhet skulle idag leda till betydande problem på flera nivåer i samhället. Denna utveckling förstärks i och med det ständigt ökade utbudet

av IoT. Om exempelvis ett dörrlås är uppkopplat och styrs via en applikation i mobiltelefonen kan det bli svårt att komma in vid långvariga strömavbrott, då mycket av det som tidigare var analogt nu kopplas upp och kopplas samman. Det skapar stora vinster, men som en följd av detta ökar beroendet av el, och i viss mån ökar de sårbarheter som kommer ur det stora elberoendet.

EXEMPEL FRÅN VERKLIGHETEN

I december 2015 drabbades Ukraina av omfattande strömavbrott. Det visade sig att störningarna orsakades av ett cyberangrepp som innebar att understationer kopplades bort, vilket i sin tur ledde till att kunder förlorade sin strömtillförsel. De tekniska lösningarna som användes i det ukrainska elsystemet har likheter med svenska förhållanden.

Tillvägagångssätten för intrången var inte nya eller unika och med undantag för enstaka delar av angreppet fanns det ingen programvara som användes vid angreppet som var specialgjord för elsektorn.

Uppkopplad samhällsviktig verksamhet

Det har visat sig genom inträffade incidenter och kartläggningar att stora delar av den samhällsviktiga infrastrukturen, till exempel vattenreningsverk och elproducenter, har industriella informations- och styrsystem (ICS/SCADA – industrial control systems/supervision control accusation data) som är uppkopplade mot internet och är därmed tillgängliga på distans. Dessa system behöver oftast inte vara internetanslutna, men av effektivitetsskäl kopplas de likväl till internet, vilket öppnar för möjligheten till åtkomst från distans. Många av dessa system är ålderstigna och har därför ofta sårbarheter som en hotaktör kan utnyttja. Antalet sårbarheter som är specifika för industriella informations- och styrsystem har ökat kraftigt under de senaste tio–tjugo åren. Det är ofta svårt att på ett ändamålsenligt sätt säkerhetsuppdatera ICS/SCADA då de inte är byggda för att regelbundet uppdateras. Detta förstärks av att verksamheten och säkerhetskrav ofta inte har utrymme eller resurser att tillåta att dessa system får förändras, vara avstängda eller att åtgärder som medför fördröjningar i datatrafiken införs.

Det är av stor vikt att dessa system och de processer de upprätthåller ges ett adekvat skydd över hela livslängden – som kan vara upp till 20 år – och att samtliga verksamheter som använder sig av ICS/SCADA är medvetna om de hot som finns, samt de sårbarheter som en hotaktör kan utnyttja.

Säkerställa relevant kompetens inom cybersäkerhet

För närvarande råder en stor brist på kompetens inom cybersäkerhetsområdet. I Sverige finns ett högt tekniskt kunnande men inte i tillräcklig mängd för att möta behovet. Det innebär att arbetsgivare behöver öka sina insatser för att rekrytera, utveckla och behålla personal med denna kompetens. Att utveckla egna utbildningsprogram eller köpa utbildningar, samt att kontinuerligt vidmakthålla kompetensen för att följa teknikutvecklingen är kostsamt men nödvändigt.

Dessutom finns ett behov av att höja grundkompetensen och medvetenheten om cybersäkerhet hos samtliga medarbetare. Även ledningsgrupper behöver kompetens för att prioritera och driva arbetet med hänsyn till cybersäkerhet. Bristen på

kompetens inom cybersäkerhet är dock inte ett svenskt fenomen - det är en global utmaning som de flesta länder måste hantera.

UNDERSKOTTET BEDÖMS VARA 70 000 OM TVÅ ÅR

Enligt IT & Telekomföretagens rapport *"IT-kompetensbristen – en rapport om den svenska digitala sektorns behov av spetskompetens"* är bristen på kompetens så stor att den fortsatta utvecklingen och tillväxtkraften inom sektorn hotas.

I rapporten bedöms underskottet ligga på ungefär 70 000 personer i Sverige år 2022.

Om det inte finns tillräckligt mycket personal med rätt kompetens inom cybersäkerhet innebär det att verksamheterna tar ett visst mått av risk. Så mycket som en femtedel av de allvarliga it-incidenter som rapporterats under 2019 till MSB av statliga myndigheter bedöms ha sin grund i handhavandefel. Konsekvenserna behöver dock inte vara uppenbara eller inträffa omedelbart, utan kan uppstå över tid.

BRISTER SOM KAN HA SIN ORSAK I KOMPETENSBRIST PÅ OMRÅDET ÄR:

- En betydande andel myndigheter arbetar inte systematiskt med att identifiera sina skyddsvärden eller att säkerhetsskyddsklassificera sina uppgifter.
- Säkerhetsincidenter med misstänkt eller konstaterad informationsförlust av hemliga uppgifter till följd av bristfälligt implementerad och underhållen it-säkerhetsarkitektur.
- It-system som hanterar skyddsvärd information är uppkopplat mot ett öppet nätverk.
- Bristfälliga kravställningar på cybersäkerhet vid upphandlingar.

Den här produkten är en gemensam bild av cybersäkerhet i Sverige 2020. Rapporten är framtagen av Försvarets radioanstalt, Försvarsmakten, Myndigheten för samhällsskydd och beredskap, Polismyndigheten och Säkerhetspolisen inom ramen för en fördjupad samverkan.

FRA FÖRSVARSMAKTEN MSB Myndigheten för samhällsskydd och beredskap Polisen Säkerhetspolisen