Analys av cybersäkerhetsrisker för kritisk infrastruktur

Trots att dagens samhälle är fullständigt beroende av fungerande digital informations- och kommunikationsteknologi (IKT) så är riskhanteringen av densamma för kritiska samhällsfunktioner inte alltid högst på agendan. Historien har visat att det är ofta först efter ett större haveri som resurser mobiliseras för att sätta fokus på hur avbrott och andra incidenter skulle förutsetts and undvikits. Samtidigt finns det en tendens bland aktörer inom säkerhetsbranschen att måla drastiska bilder av alla möjliga *hot* och sårbarheter innan haverier äger rum.

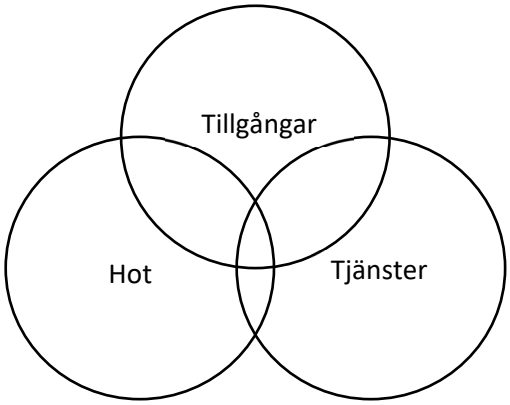
Tillgången till och styrning av kritiska funktioner i samhället (såsom elnät, vattenförsörjning, trafiksignalsystem) möjliggörs bland annat genom IKT-infrastrukturer. Dessa är heterogena stora system med många komponenter. De utgörs av gammal och ny teknologi blandad, allmän teknologi blandat med specialbyggd. En del komponenter har lång levnadstid och deras styrning av den fysiska miljön kräver specifika kunskaper från domänen. Dessa processnära IT-system benämns populärt operationell teknologi (OT), i kontrast till generell IT. IKT infrastrukturen (IT och OT sammantaget) är avsedd att leverera en tilltänkt *tjänst* inom givna kvalitetsramar. I kritisk infrastruktur innebär detta höga krav vad gäller korrekthet, determinism (teknisk förutsägbarhet) och tillgänglighet. Ett informationssäkerhetshot har därmed högst relevans om dess konsekvenser kan påverka leveransen av de tilltänkta tjänsterna. Utöver tillgänglighet är skydd av information och otillbörlig tillgång till data centralt inom den traditionella (IT-drivna) informationssäkerhetsområdet. Inför analyser av informationssäkerhetsrisk finns begreppet *tillgång* som ett sätt att tydliggöra att vissa element i systemet (fysiska komponenter, data, program, eller annat) är nödvändiga för att tillhandahålla tjänsterna.

Ovannämnda systemegenskaper gör det svårt att bedöma en övergripande säkerhetsnivå för dessa systemmiljöer. Det är inte säkert att man har en fullständig medvetenhet om alla konfigurationer i alla tillgångar i systemet delvis beroende på att det inte är möjligt att använda traditionella datainsamlingsverktyg överallt eftersom miljöerna är känsliga (eftersom de styr kritiska processer). Samtidigt är det självklart så att utan en helhetsbild av vad som ingår i sammansatta cyberfysiska system, och en hel del kunskaper om sårbarheter i varje komponent och varje operationell process så är det svårt att bedöma vari de största riskerna till leveranskontinuitet ligger.

Många ansatser för att bedöma risker och dokumentera det underliggande resonemanget har därmed tre ingredienser som belyses i Figur 1. Vilka tjänster som är fokus för analysen?

Vilka systemtillgångar eller säkerhetsrelaterade tillgångar är nödvändiga för att kunna säkerställa leveransen av tjänsten och bör därmed vara en del av analysen? Vilka hotbilder ska beaktas?

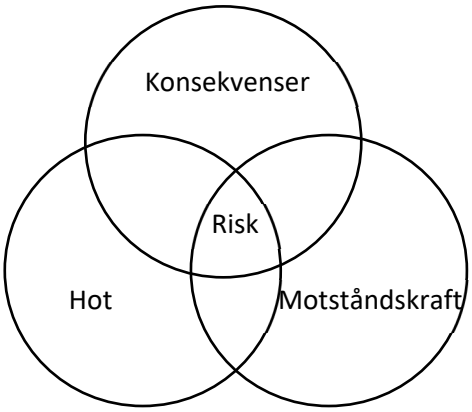
I denna rapport försöker vi sammanfatta ansatser och metoder för riskbedömning inom den kritiska infrastruktursektorn och de insikter som forskning inom forskningscentret RICS (Resilient Information and Control Systems) har gett de senaste åren.



Figur 1: Centrala element som bidrar till förståelse av risker inom verksamheter

Metoder och angreppssätt för analys av cybersäkerhetsrisker

Riskanalys av tekniska system är ett väletablerat område med många metoder, standarder och mycket forskning. I denna skrivning är avsikten inte att täcka all teoribildning inom riskanalys, utan endast att presentera de synsätt som drivit arbetet inom RICS. Generellt sett brukar riskanalys ta sin utgångspunkt i att *risk* definieras som ett värde som bestäms av *sannolikhet* gånger *konsekvens* för att något oönskat händer i det studerade systemet. Inom ramen för OT-miljöer för kritisk infrastruktur kan vi inledningsvis tänka på konsekvenser som har negativa effekter på den fysiska processen och övrig verksamhet som bedrivs av infrastrukturägaren. Den oönskvärda konsekvensen skulle för ett elnätsbolag exempelvis kunna handla om oplanerade och långvariga strömavbrott, skador på transformatorer, eller läckta kunduppgifter. Storleken på konsekvensernas upplevda skada kan variera mellan olika roller och aktörer relaterade till verksamheten. Sannolikheten å andra sidan att sådana negativa verksamhetseffekter skulle realiseras kan generellt sett orsakas av många anledningar, alltifrån stormar till materialutmattning och mänskliga misstag. Vad gäller riskanalys inom cybersäkerhetsområdet avgränsas orsaksfloran till att på ett eller annat sätt involvera hot som utövas genom IKT-infrastruktur (och att vara antagonistiskt, dvs att det finns ett mänskligt uppsåt att attackera. Med denna avgränsning kan man konstatera att sannolikheten för att konsekvenserna skall realiseras då beror dels IKT-infrastrukturen och dess komponenters inneboende motståndskraft mot attacker samt attackerarnas kompetens, drivkrafter och resurser. Vi illustrerar detta i Figur 2.



Figur 2: Komponenter som krävs för kvantifiering av risker

Trots att riskanalys alltså tydligt involverar analyser inom tre områden som förs samman för att tillhandahålla övergripande riskbedömningar så har i princip alla riskanalysmetoder sitt fokus eller sin utgångspunkt i någon av dem. Vi kan konstatera att dessa tre områden täcker tre väldigt separata kunskapsdomäner; någon viss process med tillhörande verksamhet (exempelvis elnät), IT och OT samt tillhörande säkerhet, samt hotaktörers egenskaper och förmågor. Vi kan vidare konstatera att dessa tre i sig är komplexa och att denna inbördes komplexitet tydligt påverkar den övergripande riskanalysen. För att exempelvis förstå konsekvenserna av en cyberattack som leder till att en viss brytare öppnas i ett elnät måste man förstå elnätets utformning och driftläge. Kanske utlöser brytarfrånslaget en kaskadeffekt som orsakar ett stort strömavbrott, eller kanske händer ingenting. Hur svårt det är för angriparen att ta sig så långt in IKT-infrastrukturen så att det är möjligt att skicka signalen om att öppna brytaren beror på hur en stor mängd styrsystem och andra datorer är sammankopplade och vilka typer av IT-skyddsmekanismer som finns implementerade. Hur troligt det är att olika attackerare faktiskt försöker att genomföra angreppet beror exempelvis på deras politiska och ekonomiska motiv samt på deras kunskap om såväl den angripna IKT-infrastrukturen som elnätet. Alla dessa ämnen måste riskanalytikern skaffa sig information och kunskap om. Om inte alla dessa delar analyseras med samma nogsamhet kommer riskanalysen i slutänden att vara obalanserad. Att göra en välbalanserad riskanalys är alltså mycket svårt, men är dock kanske inte nödvändigt i alla situationer. Om syftet med riskanalysen exempelvis främst är att ta fram en beredskapsplan för händelser av lyckade angrepp blir det naturligt att fokusera på verksamheten och dess konsekvenser, är målet att öka verksamhetens motståndskraft mot cyberangrepp blir fokuset de komponenter som skyddar IKT-infrastrukturen, och om frågan är hur stor IT-säkerhetsbudget organisationen bör ha kommer fokus oundvikligen hamna på hotbilden.

Metod och angreppssätt varierar också kraftigt inom riskanalysområdet. I sin enklaste form bedöms de tre områdena på enkla nominalskalor (exempelvis 1-5 eller hög-medel-låg) som sedan vägs samman till ett totalt riskvärde eller som illustreras i riskmatriser (med sannolikhet och konsekvens på axlarna). I andra änden av metodspannet finns de som använder statistiska beräkningar med fördelningar över tid, kostnader och andra storheter som också tar hänsyn till osäkerheten i bedömningarna. En allmän diskussion inom riskanalysområdet är hur kvantitativt och statistiskt det är möjligt och meningsfullt att genomföra riskanalyserna. Denna diskussion hänger i sin tur också samman med en annan diskussion om datadriven respektive “antagandedriven” analys. I princip skulle man vilja

basera sina analyser på statistiska data från observerade fenomen (hur lång tid tar det för olika attackerare att lyckas med olika typer av attacker och vad blir kostnaderna av strömavbrott på olika platser och tider, etc.). Denna typ av data är dock förstås en bristvara, i alla fall utanför organisationen, inte minst eftersom riskanalys naturligt omgärdas av mycket sekretess, vilket gör att man istället ofta är hänvisad till experters bästa gissningar som grund för sina bedömningar. Beroende på tillgänglig information och syfte är det vanligt att riskanalyser också antingen följer ett angreppssätt som primärt är uppifrån-och-ned eller nedifrån-och-upp.

Ytterligare en inneboende utmaning inom riskanalysen är att hantera den strukturella komplexiteten i det analyserade systemet, som nämnts ovan. Det är förstås så att det finns en stor mängd attackerare som utgör det totala hotet, det finns en stor mängd potentiella attackytor på IKT-infrastrukturen, det finns en stor mängd attackvägar från dessa attackytor som leder fram till en stor mängd värdefulla tjänster och information i verksamheten, som i sin tur alla potentiellt har en stor mängd olika typer av konsekvenser. Även för starkt avgränsade analysobjekt så har kombinationerna av alla dessa varianser en tendens att explodera och överskrida vad som är hanterbart för analytikern. Att skaffa sig en övergripande bedömning av en "total risk" är således svårt, både konceptuellt och praktiskt. Lösningen blir förstås att förenkla problemet på olika sätt. Metodmässigt kan man skönja angreppssätt som är checklistebaserade respektive beroendebaserade. Den föregående kategorin kan illustreras med många typer av standarder som exempelvis kan stipulera en uppsättning goda IT-säkerhetsskydd som kan prickas av för att uppnå lägre övergripande risk. Den senare kategorin baserar istället ofta på någon form av graf- eller trädstruktur i vilken orsak- och verkanssamband beskrivs. Exempel på detta är klassiska metoder baserade på felträd samt attackgrafer. Det är utvidgningar av detta senare paradigm som RICS arbetat med.

Forskning inom RICS

Forskarna på Kungliga Tekniska Högskolan (KTH) arbetar med metoder och formalismer för att automatiskt generera attackgrafer utifrån modeller av IKT-infrastruktur. Den underliggande tanken och filosofin med detta angreppssätt är att de ingenjörer som förvaltar och utvecklar IKT-infrastrukturer i verksamheter som opererar kritisk infrastruktur skall kunna få automatiskt stöd att genomföra riskanalyser om de kan tillhandahålla en beskrivning den existerande eller tilltänkta systemdesignen. Detta analysstöd tillhandahålls alltså då i form av vad som skulle kunna ses som virtuella penetrationstester av systemmiljön eftersom attackgraferna visar vilka möjliga sätt miljön kan angripas.

Inom ramen för RICS har tidigare forskningsresultat använts för förfinade analyser specifikt inom smarta elnät och ett scenario för införande av distribuerad och förnybar elproduktion. I samarbete med ett annat forskningsprojekt[1] utvecklades en omfattande referensarkitektur över hur IKT-infrastrukturen för scenariot sannolikt skulle kunna se ut. Denna referensarkitektur modellerades sedermera i en programvara[2], baserad på tidigare forskningsresultat, som just genererar attackgrafer. Referensmodellen beskriver IKT-infrastrukturer hos en elnätsoperatör med centralt styrsystem (SCADA),

[1] EU-projektet SEGRID, se: www.sergid.eu

[2] securiCAD, som utvecklas av företaget foreseeti, se www.foreseeti.se

transformatorstationsautomation och elmätare hos kunder, en elproducent med både handelssystem och driftsystem, en styrsystemsleverantör samt en stamnätsoperatör. Alla systemmiljöerna är förenklade men ändå realistiska i sin arkitekturella uppbyggnad. Totalt sett avbildas 24 olika datornätverk i en modell som innehåller 560 olika systemkomponenter. Studien jämför sedan fyra olika försvarsstrategier, tex användandet av DMZ-nätverk, olika grader av uppdaterad programvara och härdning av operativsystem. För varje scenario beräknas en uppskattad fördelning för hur lång tid det tar för en hypotetisk attackerare att nå olika systemkomponenter i infrastrukturen samt tillhörande attackvektor. På så sätt kan olika scenariona jämföras med varandra utifrån ett attackmotståndskraftsperspektiv. Analyserna finns redovisade i en artikel i tidskriften Energy Informatics[3].

Detta var ett exempel på tillämpad forskning. Projektet har även producerat resultat av teoretisk karaktär. För att automatiskt kunna generera attackgrafer från systemmodeller på det sätt som beskrivs ovan behövs att modellerna följer en fördefinierad struktur. Detta görs genom att modellerna beskrivs i speciellt utformade domänspecifika språk (DSL, Domain Specific Languages). Dessa språk definerar vilka typer av attacker och försvar som *potentiellt kan finnas* i en viss domän och dess olika systemkomponenter. Man kan i ett språk exempelvis stipulera att systemmodeller skall innehålla *nätverk*, *datorer*, *data* och *inloggningsuppgifter* och att om *datorer* är kopplade till samma *nätverk* kan dessa kommunicera med varandra, och är det vidare så att *inloggningsuppgifter* till *dator A* finns sparade på *dator B* så bildas en potentiell attackvektor (som en del av en större graf) från *dator B* till *dator A,* men också att är möjligt att försöka exekvera skadlig kod från den ena *datorn* på den andra bara på grund av att de är kopplade till samma *nätverk*. För att kunna programmera sådan attacklogik i ett domänspecifikt språk behövs ytterligare en nivå av formalism för hur detta skall göras, nämligen ett metaspråk. I RICS har vi bidragit till utvecklingen av Meta Attack Language (MAL). MAL beskriver alltså de grundläggande primitiver som används för att bygga domänspecifika språk (attacksteg, försvarsmekanismer, systemkomponenter) samt hur deras beroenden används för att generera probabilistiska attackgrafer. Utöver den formella beskrivningen av MAL finns även en språkkompilator och ett antal språkutvecklingsinitiativ samlade på GitHub[4]. MAL har inom ramen för andra projekt sedermera använts till att bygga domänspecifika språk för säkerhetsanalyser inom exempelvis transformatorstationsautomation, fordonsautomation och molnmiljöer.

Sett från perspektivet i Figur 1, har det arbete som forskare vid Linköpings universitet (LiU) drivit följt en tillgångsbaserad ansats. Man börjar genom att ställa frågan: om risker mot ett system som ska utformas (vid design/anskaffningsstadiet) ska kvantifieras, så krävs det metoder för att identifiera vilka tillgångar kommer att finnas som behöver skyddas? Metoden går ut på att redan vid anskaffningen identifiera de tillgångar som bör vara i fokus för säkerhetsanalysen. De flesta skyddsvärda tillgångar inom IKT system kan betraktas som data som skall lagras, eller data som skall skickas inom nätverk (personliga kunddata, mätvärden som ska skickas till styrenheten för att kunna bevara stabiliteten i den fysiska processen, kommandon som operatören eller styrenheten skickar till fjärrstationer). Men

[3] https://energyinformatics.springeropen.com/articles/10.1186/s42162-018-0010-x
[4] www.mal-lang.org

även kunskapen om en viss algorithm, lagrad kod för att realisera den eller nycklar för att komma åt den är att betrakta som tillgångar bland fler andra. Metoden går ut på att att genom denna fokus på tillgångar och de systemkomponenter som tillgången huseras i eller passeras igenom identifiera vilka attacker som är sannolika och vilka säkerhetsmekanismer kan erbjuda motstånd mot dessa sårbarheter. Detta resonemang förs i flera iterationer. Allteftersom nya säkerhetsmekanismer som i sin tur lägger komplexitet till systemet tillförs, identifieras nya tillgångar (t.ex. kryptonyklar, certifikat och andra tillgångar) som blir potentiellt lika viktiga att skydda som det ursprungliga systemets skyddsvärda objekt. Detta arbete har publicerats i flera artiklar och en doktorsavhandling under 2015[5]. Medan detta arbete har fokus i riskanalys då systemet är under skapande fasen och därmed är granulariteten på den nivån som guidar utvecklarna, har det senare arbetet vid LiU sitt fokus på den operationella fasen.

Det senaste arbetet vid LiU tar avstamp i det tredje perspektivet i Figur 1: tjänster. Medan det första ansatsen har en angripare/försvarares perspektiv, och den andra ansatsen en kravställare/utvecklares, i denna ansats har man fokus på systemägarens affärsfokus. Innan man modellerar systemet för att resonera kring riskerna ställer man frågan: Om systemet ska tillhandahålla sina tjänster vad är det som krävs för en säker operation av systemet? Vilka element bidrar till detta och hur kritisk är varje element? Vilka andra (element eller tjänster) krävs för en säker operation och vilka beroenden skapar dessa? I detta arbete som initierades inom RICS genom att etablera samarbete med universitetet i Cardiff och Airbus group (security and innovation) har vi fokuserat explicit på SCADA system. Genom att samla input från 36 domänexperter på olika nivåer i verksamheter (management, driftinjengör, säkerhetsansvarig osv) börjar vi från ett avnämareperspektiv. 17 av dessa avnämare kom från kontakter inom RICS projektet. De olika experterna angav svar till likartade frågor som efter vår bearbetning ledde tiltl har vi lyckats skapa ett generisk beroendemodell för SCADA system (modellen skapades från 1521 angivna av experter av vilka 640 element var unika). Modellen kan ses som ett mål-orienterat träd som på den högsta nivån har sex högnivå element som bidrar till SCADA systemets mål. Dessa element täcker vid skilda delar av beroenden som påverkar riskanalysen (Management, Employees, Data, System life cycle, System architecture, External dependencies). Arbetet är realiserat som en anpassningsbar modell (en blueprint) med hjälp av Open Groups ”dependency modelling standard” inom verktyget iDepend[6]. Modellen har tillämpats på ett antal exempel och kan utvärderas vidare inom verksamheter som visar intresse.

Sammanfattning

Riskanalys och dokumentation av vilka antaganden som ligger bakom en en viss riskbedömning är fortfarande ett område under utveckling. Arbetet under RICS-projektet och vår exponering av resultaten till olika avnämare har visat att modellering hjälper att skapa de dialoger som krävs för att bestämma den ”rätta” granulariteten och det fokus som passar just i det sammanhang som arbetet bedrivs. Olika aktörer, alltifrån systemutvecklare till driftpersonal och beslutsfattare kan ha olika ingångar och olika behov av prediktioner, vilket gör att ha en flora av ansatser för riskanalyser inte nödvändigvis är en nackdel, kanske till och med en fördel för att ta fram olika synvinklar.

---

[5] Alla publikationer visas på www.rics.se och fulltexten kan fås ifall inte ”open access” publicering.

[6] https://idependeu.herokuapp.com