Informations- och Cybersäkerhets-strategi för Sveriges riksbank

Oktober 2023

Inledning

Informationsteknologi används i samtliga delar av Riksbankens uppdrag. Innovationstakten är hög och ambitionerna likaså. Detta förutsätter att man kan hantera risker relaterade till informations- och cybersäkerhet.

Riksbanken verkar i ett finansiellt ekosystem där man är beroende av andra parter som i sin tur är beroende av Riksbanken. Med informations- och cybersäkerhetsstrategin strävar Riksbanken efter att beskriva riktning och mål för arbetet med informationssäkerhet och cybersäkerhet på medellång sikt. Syftet med den är att reducera risk och verka för att verksamhetens informationstekniska miljöer ska vara robusta. Detta gör Riksbanken med egna resurser men också genom olika samarbetspartner, när så är lämpligt.

Informations- och Cybersäkerhetsstrategin riktar sig till en bredare målgrupp där behov av insyn finns gällande Riksbankens övergripande arbete med informationssäkerhet och specifikt cybersäkerhet.

Introduktion

Riksbanken är Sveriges centralbank. Vi ser till att pengarna behåller sitt värde över tid och att betalningar kan ske säkert och effektivt. Vi ger också ut Sveriges sedlar och mynt.

Cybersäkerhetsmiljön

Riksbankens uppdrag är i hög grad beroende av att ha förmågan att hålla sin cybersäkerhet på en nivå som är relevant för sitt uppdrag ställt mot risker och hot. Finansbranschen i Sverige och runt om i världen använder innovativ teknik för att förbättra tjänster, automatisera arbete och sänka kostnader. Bland dessa kan nämnas molntjänster, artificiell intelligens (AI), machine learning (ML), quantum computing, internet of things (IOT) samt andra teknologier och verktyg som underlättar finansiella flöden mellan institutioner samt tillgodoser behovet av analyser.

Även om den moderna tekniken möjliggör en hög grad av integration och automation så finns det också risker och sårbarheter med den. Ett intrång som äventyrar data och verksamhet hos ett finansinstitut eller någon av dess underleverantörer har potential att spridas till anslutna partners och i slutändan störa både nationella och internationella finansiella system.

De två huvudsakliga hotaktörerna utgörs av kriminella element och statliga aktörer, men även ideologiskt motiverade krafter kan ligga bakom ett angrepp.

Cyberkriminalitet handlar i de flesta fall om att tjäna pengar och förövarens verksamhet styrs till stor del av var den största chansen till framgång finns. Med mycket höga dagliga transaktionsvolymer och angripare som i många fall motiveras av ekonomisk vinning är det inte förvånande att centralbanker utsätts för cyberattacker.

Viljan att påverka samhällsviktiga system för att på så sätt störa eller påverka förtroendet för dessa hos allmänheten är andra möjliga angreppsmotiv där det också förekommer angrepp utförda eller understödda av nationalstater. Den statliga aktören har mycket hög teknisk förmåga som tillsammans med långtgående resurser och hög uthållighet gör den till den dimensionerande hotaktören.

Hotlandskapet

Hot utvecklas över tid och är av delvis generell karaktär, men också direkt inriktat mot finansiella aktörer, däribland Riksbanken. Några hot som är högt upp på agendan är nedanstående.

Insider – I takt med att teknisk infrastruktur blir allt svårare att attackera finns alltid möjligheten att nyttja den personal som faktiskt har tillgång till information och värden. Det är med andra ord lättare att utnyttja personal som redan har tillgång till informationen än att forcera starka tekniska hinder.

Tredje parter – Dagens centralbanker nyttjar tjänster från leverantörer utanför sina egna kärnverksamheter. En leverantörskedja kan vara en möjlig väg in i Riksbanken. Men den kan också utsättas för spridningseffekter som inte var avsedda för Riksbanken (så kallat collateral damage)[1].

Utpressning – Att införa skadlig kod med efterföljande kryptering följt av krav på pengar för att dekryptera är ett modus operandi som har funnits sedan många år tillbaka. I vissa fall har också information förts ut från den drabbade verksamheten som sedan hotats med publicering av den stulna informationen. I båda fallen följt av krav på betalning för att låsa upp data respektive att ej publicera dataläckaget (så kallat ransom ware)[2].

Sabotage och spionerі – Både Riksbanken och den finansiella sektorn som helhet utgör en måltavla för den som antingen vill störa viktiga samhällsfunktioner eller tillskansa sig intellektuellt kapital av någon sort.

[1] https://sv.wikipedia.org/wiki/Sidoskada

[2] https://sv.wikipedia.org/wiki/Ransomware

Riksbanken och den finansiella sektorn

Sveriges riksbank är både en central funktion för den finansiella sektorn och utgör också en del i den svenska och internationella betalinfrastrukturen. En av Riksbankens uppgifter är att arbeta för att betalningssystemet i Sverige har hög motståndskraft. En hög nivå på cybersäkerhet är väsentligt inte bara i de transfererande systemen utan också i de logistikkedjor där fysiska värden hanteras. Liknande beroenden finns till och från underleverantörer av informationsbehandlande tjänster, myndigheter emellan samt mot privat finanssektor. Allt för att hela eller delar av svensk betalinfrastruktur skall kunna upprätthålla förväntad servicenivå.

En framgångsrik attack mot Riksbanken skulle inte drabba enbart själva centralbanken, utan effekterna skulle sannolikt också slå mot det finansiella systemet både inom och utanför Sveriges gränser. Detta gör att Riksbankens ansvar inte slutar med dess egen verksamhet utan Riksbanken behöver ta ett ansvar i linje med sin roll i det finansiella systemet, vilket också regleras i Riksbankslagen.

Med detta följer att det i allt högre grad finns ett behov av för sektorn gemensamma strategier mot cyberangrepp samt effektivt samarbete mellan offentliga och privata deltagare. Riksbanken samarbetar med andra myndigheter och finansiella institutioner (FMI) för att minska risker och främja det finansiella systemets motståndskraft som helhet. Även om det är viktigt att samarbeta och visa upp en enad front mot angriparen så behöver samtidigt Riksbankens egna förmågor att möta angrepp befinna sig på hög nivå.

Riksbanken behöver dessutom förhålla sig till en del lagstiftning på områden som säkerhetsskydd samt offentlighets- och sekretesslagstiftning som också påverkar hur arbetet med cybersäkerhet kan och bör utföras, exempelvis med hänsyn till tjänsters geografiska placering eller leverantörers huvudmannaskap.

Riksbankens cybersäkerhetsresa

Sedan ett antal år tillbaka har Riksbanken låtit outsourca sin IT-drift till en extern leverantör. Riksbanken använder därutöver fler leverantörer för att stödja olika delar av sin verksamhet. Oaktat formerna för utförandet av IT-leveransen har Riksbanken identifierat cybersäkerhet som ett fokusområde sedan ett antal år tillbaka i takt med att omvärlden har förändrats och med detta hotbilden samt angriparens möjligheter. Riksbanken har utvecklat både interna och externa förmågor i syfte att optimera skyddet för sin verksamhet. Riksbanken har samarbetat i många år med offentliga och privata aktörer i finansiell sektor, både nationellt och internationellt, för att minska cybersäkerhetsrisker för det finansiella systemet. Riksbanken är representerad och deltar i löpande arbeten i bland annat, CRCC (Cyber Resiliense Coordination Centre) samt WPSI (Working Party for Security Issues) som är BIS (Bank for International Settlements) forum för säkerhetsfrågor. Riksbanken följer dessutom CPMI-IOSCO vägledning för FMIs cyberskydd. I Sverige pågår uppbyggnaden av ett nationellt cybersäkerhetscenter (NCSC). NCSC är än så länge en ung organisation men Riksbanken bevakar på vilket sätt den framöver kommer att utvecklas. En pilot för den finansiella sektorn pågår inom ramen för NCSC i Stabilitetsrådets regi, där Riksbanken ingår.

Riksbankens strategi där finansiella centralbankstjänster förväntas ligga i framkant får inte hämmas av en informations- och cybersäkerhetsstrategi utan ska snarare möjliggöras av en sådan.

Under senaste åren har Riksbanken stärkt sina förmågor både internt men också genom externa partner. Riksbankens säkerhetsfunktion har under 2022 omorganiserats för att bättre kunna möta cyberhot.

Riksbankens prioriterade verksamhet och tillgångar

Riksbanken har identifierat och definierat sin mest kritiska verksamhet och tillhörande tillgångar i syfte att bedöma vilka modus operandi en eventuell angripare skulle välja. Ett av Riksbankens viktigare uppdrag är att operera avvecklingssystemet som är den transfereringsplattform där nästan alla svenska interbankbetalningar sker.

Bankens system för överföring av internationella betalningar är också föremål för att skyddas särskilt. Detta gör Riksbanken både med egna definierade kontroller men också inom ramen för de obligatoriska program som plattformens leverantörer ställer krav på.

Riksbanken mäter sin mognad avseende bland annat cyberhot genom ett ledningssystem för informationssäkerhet som baserar sig på ISO 27000. Mätningarna sker periodiskt och rapporteras till direktionen.

Riksbanken är både facilitator av och deltagare i TIBER-tester. TIBER[3] (Threat intelligence-based ethical red teaming) är ett ramverk som har tagits fram av Europeiska centralbanken (ECB). Det innebär att man på ett standardiserat sätt testar hur väl viktiga infrastrukturföretag och banker står upp mot cyberhot. Kortfattat innebär testet att en cyberattack simuleras mot ett företag eller myndighet under ordnade former. Även Riksbanken är underställt kravet på att genomgå dessa tester.

Informations- och Cybersäkerhetsstrategin är en del av Riksbankens strategi. Riksbankens roll inom det finansiella systemet innebär att perspektivet på cybersäkerhet är en angelägenhet för såväl Riksbankens egna tjänster som Riksbankens del i den finansiella stabiliteten i stort. Riksbanken har också antagit en IT- och digitaliseringsstrategi som informations- och cybersäkerhetsstrategin relaterar till. Baserat på antagandet att cyberintrång är oundvikliga betonar informations- och cybersäkerhetsstrategin behovet av att upptäcka samt att ha förmågor som kan möta och agera vid sådana händelser och slutligen återställa normal drift efter eventuella störningar.

Informations- och Cybersäkerhetsstrategin relaterar till Riksbankens Ledningssystem för Informationssäkerhet (LIS) genom att Riksbankens nivå av cybersäkerhet identifieras och mäts för att ställas i relation till den beslutade mognadsgraden[4]. Aktiviteter med koppling till cybersäkerhet planeras inom ramen för den årligen återkommande verksamhetsplaneringen (VP).

Riksbankens cybersäkerhetsvision:

Säkerställa cyberresiliens mot en föränderlig hotmiljö till gagn för det svenska finansiella systemet

Riksbankens cybersäkerhetsuppdrag:

Främja effektiviteten och stabiliteten i det svenska finansiella systemet genom robust cybersäkerhetsförmåga, kompetens, informationsutbyte och samarbete

Följande avsnitt beskriver de strategiska målen som kommer att bidra till att Riksbanken uppnår sin cybersäkerhetsvision och sitt cybersäkerhetsuppdrag.

[3] https://www.riksbank.se/sv/finansiell-stabilitet/riksbankens-ansvar-inom-finansiell-stabilitet/forebygga-finansiella-kriser/riksbankens-arbete-med-cyberrisker/tiber-se/

[4] LIS-rapport **2021** Dnr 2021-000957 samt LIS-rapport **2022** Dnr 2022-00933

Målsättningar

Mål 1 – Stärk cybersäkerhetsförmågor

Stärkta förmågor ger bättre förutsättningar för att möta cyberhot proaktivt såväl som reaktivt

- Säkerställ att Riksbanken ses som en attraktiv arbetsgivare inom cybersäkerhet.
- Säkerställ att respektive verksamhet i Riksbanken förstår sina exponeringar för cyberrisk.
- Säkerställ att de proaktiva och reaktiva förmågorna är tillräckligt stora för att kunna möta både aktuell hotbild och den risk Riksbanken har beslutat att acceptera.

Mål 2 – Öka samverkan

Ökad samverkan mellan stabilitetsmyndigheter, säkerhetsmyndigheter och privata aktörer på cybersäkerhetsarenan ger bättre situationsbild och cyberresiliens

- Säkerställ att Riksbanken deltar i ömsesidigt utbyte av underrättelser i syfte att cybersäkerhetsmässigt stärka deltagarna i svensk betalinfrastruktur.
- Säkerställ att Riksbanken regelbundet genomför övningar med aktörer som är relevanta för att upprätthålla en säker betalmarknad.

Mål 3 – Testa cybersäkerhetsförmågor

Inga proaktiva aktiviteter kan ge samma bekräftelse eller relevanta svar som realistiskt utförda tester kan

- Säkerställ att Riksbanken kan förbättra sin motståndskraft mot cyberhot genom att regelbundet testa sitt cyberskydd och följa upp åtgärders effektivitet.

Strategiska åtgärder

Även om Riksbanken har förbättrat sin övergripande cybersäkerhet och motståndskraft krävs ett kontinuerligt arbete för att bibehålla Riksbankens önskade nivå gentemot hotaktörerna. Storleken och omfattningen av säkerhetsfunktionerna inom Riksbanken har utökats för att nå bankens strategiska mål. Förutom de viktiga prioriteringarna relaterat till hur Riksbanken förvaltar IT-komponenter kommer också fokus att behöva läggas på att ytterligare stärka detekterings-, svars- och återställningsförmågorna.
Riksbankens Ledningssystem för Informationssäkerhet (LIS) bygger på den internationellt erkända standarden ISO/IEC 27001[5]. Riksbanken har också utvärderat NIST CSF[6] (cyber security framework) som ett komplement till ISO och kommer att följa valda delar av detta ramverk som består av 5 huvudområden – Identifiera (*Identify*), Skydda (*Protect*), Detektera (*Detect*), Agera (*Respond*) och Återställa (*Recover*). NIST är en amerikansk standard som har kommit att öka i popularitet, men stora delar av dessa ramverk snarlika.

Styrning och uppföljning

Riksbanken styr genom policyer och regler som berör såväl personal som teknologi och processer. Vissa av dessa omfattar cybersäkerhet. Riksbanken ska ha den styrning och information som behövs för att hantera och övervaka cybersäkerhetsrisk.

För att uppnå målen ovan behöver Riksbanken fortsätta att utveckla styrningen och riskhanteringen genom bland annat:
• en uppdaterad riskaptit och mätvärden för att stödja riskbaserat beslutsfattande, t.ex. nyckelrisk indikatorer (key performance indicators) och mognadsmål.
• förbättrade rapporteringsverktyg för att stödja effektiv styrning av riskarbetet.
• tydliga roller och ansvar över de tre försvarslinjerna.
• konsekventa riskbedömningar av tredje partsleverantörer under hela livscykeln.
• personalplanering för cyberresurser för att möta framtida behov av cybersäkerhetskompetens och talang.

[5] https://www.sis.se/
[6] https://www.nist.gov/cyberframework

Mål 1 – Stärk cybersäkerhetsförmågor

Förmågor inom NIST CSF är indelade i fem huvudområden: Identifiera *(Identify)*, Skydda *(Protect)*, Detektera *(Detect)*, Agera *(Respond)* och Återställa *(Recover)*. Nedan redovisas målsättningar per område för att Riksbanken ska nå sina ambitioner inom ramen för informations- och cybersäkerhetsstrategin. För att nå framgång i sitt cyberförsvar krävs att förmågorna inte bara når höga nivåer utan också saknar uppenbart svaga sektorer. Riksbanken räknar med att angriparen kartlägger och analyserar våra svagheter.

Målsättning

I 2022 års utgåva av ISO 27002 har kontrollerna närmat sig den indelning i förmågor som NIST använder sig av. Detta medför att Riksbanken med sitt ledningssystem för informationssäkerhet också kan planera för och redovisa sina cybersäkerhetsförmågor på ett tydligare sätt.

Område	Identifiera (Identify)	Skydda (Protect)	Detektera (Detect)	Agera (Respond)	Återställa (Recover)
Målsättning	Kravställning och styrning ger förutsättningar för att hantera och besluta i cybersäkerhetsfrågor --- Rätt kompetens finns och kan verka inom tydliga roller --- Bankens informationsstödjande tillgångar är kartlagda	Behörighetskontroller ger rätt information till rätt person vid rätt tillfälle --- Sårbarheter blir identifierade och hanterade --- Data är klassificerade och skyddade --- De anställda hålls medvetna om förfaranden och risker	Cyberattacker detekteras och hanteras --- Säkerhetskonfigurationer hålls uppdaterade och övervakade --- Underrättelser om cyberhot ger förvarning eller grund för bedömningar	Planer och processer för att mildra händelser är upprättade --- Incidenter hanteras i relevant tid --- Forensiska resurser utreder uppkomna händelser --- Incidenter är koordinerade mellan inblandade parter	Återställningsplaner tillser att beredskap finns att återgå till normal operation --- Processer finns och övas för att säkerställa att hela organisationen kan återgå i skarpt läge

Mål 2 – Öka samverkan

I det digitala sammanhanget står ingen aktör oberoende av sin omvärld. Det finansiella systemet är tätt sammanvävt med både kända men också mer perifera beroenden. Samma sak gäller beroendet till infrastruktur som telekommunikation och elkraftförsörjning. En framgångsfaktor när incidenter inträffar, men även i preventivt arbete, är hur effektivt samverkan och utbyte av information sker aktörer emellan. NCSC[7] (Nationellt Cybersäkerhetscenter) är under uppbyggnad och kommer att stödja finanssektorn (inledningsvis som pilot) med en strategisk samt en operativ gruppering där stabilitets[8] och säkerhetsmyndigheter[9] kommer att finnas representerade men också privata aktörer som är viktiga för finansiella systemets stabilitet. I samband med att NCSC etableras kommer MSBs forum FIDI-Finans att läggas ner. Riksbanken kommer att ingå som representant i NCSCs båda forum det vill säga det strategiska och det operativa.

Riksbanken har dessutom representation i andra forum som berör cybersäkerhetsrisker som till exempel ett medlemskap i ISF[10] (Information Security Forum). Riksbanken är också representerad i BIS (Bank for International Settlements) CRCC (Cyber Resilience Coordination Centre), ett forum för säkerhetschefer från stora delar av centralbanksvärlden (cirka 60 länder), BIS WIPSI (Working Party for Security Issues) och ESCB (European System of Central Banks) SRM WG (Security Risk Management Working Group).

Målsättning

Vid eller inför olika händelser av cyberhotande karaktär så ökar finansbranschens möjlighet att skydda sina tjänster mot dem eller mildra effekterna av dem om det finns en god informationssamverkan. Möjligheten att utbyta underrättelser om pågående attacker eller indikationer om sådana behöver nå ut till fler aktörer i den finansiella sektorn. Målsättningen är att underlätta sådan samverkan.

[7] https://www.ncsc.se/

[8] Finansinspektionen, Riksgälden och Riksbanken

[9] FMV, FRA, Försvarsmakten, MSB, Polisen, PTS och Säkerhetspolisen

[10] https://www.securityforum.org/

Mål 3 – Testa cybersäkerhetsförmågor

Alla aktörer i finansiell sektor bör arbeta proaktivt med sina system, processer och organisationer. Om man aldrig testar sina förmågor kommer man aldrig få kvittens på sin uppnådda nivå. I samband med att man bygger eller förändrar systemstöd görs idag många typer av tester till exempel funktionella tester för att bekräfta att förändringarna levererar förväntat resultat, eller så kallade penetrationstester (pentester) för att identifiera säkerhetssårbarheter och motverka intrång. Dessa tester sker ofta isolerat och mot de miljöer som har varit föremål för förändringen.

I ett större perspektiv kan man testa sin cyber-resiliens under mer eller mindre realistiska former (till exempel genom så kallad red-teamtestning). Syftet är att agera som en tänkt angripare skulle, och attackera på ett sätt som angriparen skulle bedöma som mest sannolikt att lyckas med.

De olika testerna utesluter inte varandra. Samtliga tester bör ske med helheten i cyberförsvaret i beaktande.

Målsättning

Penetrationstester

System och teknisk infrastruktur behöver förändras av olika skäl. Ibland för att erbjuda ny eller förändrad funktionalitet till Riksbankens verksamhet. Andra gånger för att höja kvalitet eller säkerhet. I samband med förändringar finns alltid en risk att man introducerar oönskade effekter eller felaktigheter. Penetrationstester bör därför genomföras regelbundet vid större förändringar eller riskbaserat när så bedöms lämpligt.

Red-team tester

Riksbanken har liksom alla organisationer där människor, processer och teknologi ingår olika sårbarheter som kan utnyttjas av illasinnat motiverade aktörer. Målet med regelbundna red-team tester är att testa teser och möjliga modus operandi som en angripare skulle kunna resonera sig fram till. Därigenom kommer testerna att spegla ett scenario som ligger nära det som en angripare skulle välja. Det ”röda” laget är en form av kontrollerad aktör som angriper på ett realistiskt sätt där det ”blå” försvarande laget inte vet om att testet sker. Purple-team tester (där det ”röda” och det ”blåa” laget arbetar tillsammans) brukar man använda för att moderera övningen i syfte att optimera tidsåtgången och utkomsten.

Tester av säkerhetsmedvetenhet

Dagens attacker riktar sig precis som tidigare mot teknisk infrastruktur. I allt högre utsträckning har människan också blivit måltavla i cyberattacker. Anställda, konsulter och leverantörer arbetar i Riksbankens system i olika utsträckning. Utbildning samt kunskapstester av personal är viktig för att minska risker och säkerställa att medvetenheten om cyberhot är hög. Därav behöver Riksbanken höja sina förmågor också med anledning av denna exponering.

SVERIGES RIKSBANK
Tel 08 - 787 00 00
registratorn@riksbank.se
www.riksbank.se

PRODUKTION SVERIGES RIKSBANK)
ISSN ISSN. (online)