Hotbildsbedömning för Sveriges banker

Publicerad maj 2023

Svenska Bankföreningen
Swedish Bankers' Association

Hotbildsbedömning för Sveriges banker

Publicerad maj 2023

Bankernas säkerhetsorganisationer beskriver och bedömer årligen den branschgemensamma hotbilden med utgångspunkt från bankernas verksamhet. Ett hot består av en förmåga, en vilja och ett tillfälle.

Bankerna följer hotbilden hela tiden och bedriver ett strukturerat arbete för att hantera risker och arbetar med ständiga förbättringar av säkerheten. Bankernas specialister på fysisk säkerhet, identifiering, cybersäkerhet, informationssäkerhet, bedrägerier, kortsäkerhet, penningtvätt, outsourcing, sanktioner och säkerhetsskydd bidrar till rapporten.

Covid-19-pandemin har sedan början av 2020 påverkat bankerna på flera sätt. Trycket från kunder på telefonbank, internetbank och kontor har under denna period varit särskilt högt men är idag normalt. Områden som påverkats av pandemin är kontinuitetsfrågor, informationssäkerhet, cybersäkerhet, bedrägerier, personalsäkerhet och behörigheter. Även fysiska aspekter av ett förändrat arbetssätt påverkar hotbilden.

Sedan flera år har det säkerhetspolitiska läget försämrats. I februari 2022 förvärrades läget ytterligare genom Rysslands invasion av Ukraina, vilket har ritat om hotbilden. Områden som påverkas av invasionen är identifiering, informationssäkerhet, cybersäkerhet, penningtvätt, sanktioner, kontanter, civilt försvar och beredskapsfrågor.

Hotbilden beskrivs uppdelat i nio olika områden enligt nedan med sidhänvisningar. Varje område avslutas med en sammanfattande bedömning.

Bankrån, värdetransportrån och angrepp mot uttagsautomater

Under 2021 och 2022 inträffade inga bankrån, vilket inte tidigare har noterats under 40 års mätningar. Förklaringen till minskningen av bankrån är att kontanthanteringskedjan från depå via värdetransportbolag till uttagsautomat har stärkts, att banker har minskat den manuella kontanthanteringen över disk och att kunder använder alltmer elektroniska betalningar.

2022 inträffade endast ett försök till värdetransportrån. De tio senaste åren har inneburit en markant minskning av antal värdetransportrån jämfört med decenniet innan. Förklaringen till minskningen av värdetransportrån är effektivare skyddssystem, sedelinfärgning, färre transporter och bättre samverkan och förebyggande åtgärder mellan värdetransportbolagen och Polisen.

2022 inträffade tre angrepp mot Bankomat AB:s uttagsautomater under en vecka i april. Ett angrepp mot en uttagsautomat är en sprängd uttagsautomat eller en uppsågad uttagsautomat men det är inte skimming av kort.

Även om hotbilden mot bank- och värdetransportrån består så har det skifte som inleddes för femton år sedan, från bank- och värdetransportrån mot bedrägerier, nu fullbordats.

Bedömningen är att antalet bank- och värdetransportrån och angrepp mot uttagsautomater kommer att fortsätta att ligga på en låg nivå 2023.

Under 2021 och 2022 inträffade inga bankrån, vilket inte tidigare har noterats under 40 års mätningar.

Allt fler medarbetare vill inte representera banken i rättsliga sammanhang. Det finns en rädsla för att bli hotad och förföljd.

Kränkning, personhot och våld mot bankpersonal

Flera medarbetare och chefer i bankerna vittnar om ett högre tonläge och tuffare bemötande från kunder de senaste åren. Allt fler banker kräver därför att kunder avtalar tid för besök på bankkontoret. Kränkningar från kunder via sociala medier förekommer, exempelvis från kunder som avvisas från kontoret eller där kundrelationen avvecklats. Det kan handla om att banken centralt har stängt av ett konto och att kunden söker en förklaring från det lokala bankkontoret och då möter bankpersonal som de upplever motarbetar dem.

Som en konsekvens av ett tuffare klimat på kontor och kundcenter har hotbilden för att avveckla kundrelationer förändrats. På grund av att fler kunder uttrycker olaga hot mot bankens personal avvecklar bankerna fler kunder i dag. När banken avvecklar kundrelationer behövs en intern process som bedömer och förutser en eventuell hotbild mot både bankens kontor och medarbetare. Banken kan också behöva ha utbildningar i konflikthantering och diskussionsmaterial för alla medarbetare som arbetar på kontor och telefonbank.

Bankerna försöker utveckla metoder för att kunna förstå och rikta insatserna bättre – är det ett olaga hot, en höjd röst eller en obehaglig situation? De situationer som uppkommer i fysiska möten tenderar att följa med till webb- och telefonmöten. Steget från ett normalt tonläge till att bli otrevlig upplevs vara kort samtidigt som gränsen för vad medarbetarna kan acceptera är olika för olika individer.

Medvetenheten om hotbilden är större på bankkontor än på huvudkontor, eftersom personal på bankkontoren möter kunder fysiskt. Beroende på hur hotbilden utvecklas kan utökade fysiska skyddsåtgärder behöva införas.

Allt fler myndighetsförfrågningar

Bankerna får allt fler förfrågningar från myndigheter, om exempelvis transaktioner rörande brottsutredningar. Antal myndighetsförfrågningar fortsätter att ligga på en hög nivå och det finns indikationer på en ökad oro hos vissa medarbetare som arbetar med kundkännedom, penningtvättsanmälningar och bedrägerier. Exponering av enskilda medarbetare, i stället för banken, kan medföra en ökad hotbild mot individen. För att bemöta hotbilden arbetar bankerna med att skydda medarbetares identiteter. E-post skickas i större utsträckning från funktionsbrevlådor, exempelvis sakerhetsavdelningen@banken.se eller kundkontakt@banken.se. Vidare begränsas bedrägeriutredares externa kundkommunikation.

Allt fler medarbetare vill inte representera banken i rättsliga sammanhang. Det finns en rädsla för att bli hotad och förföljd. Medarbetare kan tycka att det är jobbigt att polisanmäla hot eller brott de varit utsatta för i sitt arbete, eftersom det kan generera nya hot. Banken kan inte göra en sådan anmälan, utan det måste ske av den medarbetare som drabbats av hotet, om polisen ska gå vidare med anmälan. En anmälan blir en offentlig handling med medarbetaren som målsägande. Banken kan säkerställa att det finns stöd vid en eventuell rättegång, men många medarbetare upplever ändå stor otrygghet i dessa situationer.

Den utveckling som har skett de senaste åren där svenska myndigheter kräver alltmer avancerade och långtgående utredningsåtgärder från banker har förändrat hotbilden för bankens medarbetare. För ett antal år sedan var framför allt medarbetarna i kontorsrörelsen utsatta, idag är även klagomålsansvariga, penningtvätts- och bedrägeriutredare samt de som arbetar med krav utsatta. Myndigheternas krav på banken har därmed bidragit till att hotbilden mot bankernas medarbetare har ökat. Att säkerställa en trygg arbetsmiljö för bankpersonal är inte bara ett ansvar för banken utan en del av ett större åtagande för samhällets olika aktörer att motverka penningtvätt och bedrägerier.

BEHOV AV ÅTGÄRDER

Med anledning av utvecklingen ser Bankföreningen behov av följande åtgärd och initiativ från politik och myndigheter.

- Myndigheternas krav på banken har bidragit till att hotbilden mot bankernas medarbetare har ökat. Det borde därför vara möjligt för banken att göra en polisanmälan om en medarbetare av någon anledning inte vill göra det.

Bedömningen är att hotbilden mot bankernas personal påverkas av både myndighetskrav och samhällets utveckling.

Bankerna behöver kunna balansera behovet av kontroll både vid nyanställning och under pågående anställning i banken.

Hotbilden från insiders och möjliggörare

Incitamenten att plantera en insider eller möjliggörare på en bank bedöms vara starka eftersom det ger större möjlighet till både bedrägerier och penningtvättsupplägg för kriminella, och större möjlighet till påverkan för en antagonist. En insider eller möjliggörare kan vara en person med behörigheter i banken som möjliggör för en extern antagonist (kriminell gruppering, främmande makt, etc.) att genomföra transaktioner och aktiviteter.

Dessa personer söker kontakt med bankens personal för att utnyttja dem på olika sätt. Sociala medier som LinkedIn och andra öppna informationskällor används för att kartlägga medarbetare i banken och för att söka efter möjliggörare. Kriminella och andra fientliga aktörer annonserar exempelvis efter personer som är beredda att injicera skadlig kod i bankens system. Social manipulering smälter på så sätt ihop med den fysiska hotbilden genom otillbörliga kontakter som senare kan leda till fysiska hot mot anställda.

Att bygga säkerhet tar tid

Frågan som aktualiseras är hur banken kan skydda medarbetare från otillbörliga kontakter från exempelvis en statsaktör eller organiserad brottslighet. Inom säkerhetsskyddslagstiftningen är det reglerat hur det ska hanteras, men hotet finns i bredden av verksamheten, från bedrägerier till hur man rundar sanktioner. Kulturbyggande runt säkerhet är mer utmanande idag på grund av bland annat högre personalomsättning. Säkerhetsmässigt är en hög personalomsättning sällan fördelaktigt, eftersom säkerhet ofta tar tid att bygga upp. Det kan finnas aktörer som vill exploatera att medarbetare idag inte har samma lojalitetsband till sin arbetsgivare som de hade för tjugo år sedan då personalomsättningen var lägre.

Vissa tillvägagångssätt kan inte genomföras utan en möjliggörare på insidan som kan bankens produkter, tjänster och rutiner. Incitamenten kan bestå i att få information som underlättar genomförandet av brottsupplägget, eller att möjliggöraren felaktigt beviljar en kredit eller ignorerar ett transaktionslarm. Det kan handla om information om rutiner och processer, regelsättning vid kreditgivning och transaktionsmonitorering. Vid sidan av bankens egen kreditberedningsprocess skapar låneförmedlare, med fler parter i lånekedjan, olika typer av incitament till bedrägerier och penningtvättsupplägg vid återbetalning.

Bankerna behöver kunna balansera behovet av kontroll både vid nyanställning och under pågående anställning i banken. Risken för att insiders används är något som bankerna kan behöva bli mer vaksamma på. Detsamma gäller sabotagerisken som blivit mer påtaglig.

Bedömningen är att insiders och möjliggörare är ett hot som finns internt i bankerna och som kommer att bestå under 2023. Givet kriget i Ukraina, och dess geopolitiska konsekvenser, har vissa statsaktörer ett förhöjt intresse av insiders och möjliggörare.

Den säkerhetspolitiska utvecklingen

Ett antal händelser de senaste trettio åren påverkar utvecklingen av Sveriges säkerhet: Sovjetunionen imploderar 1991, terrorhotet ökar från 2001 och digitalisering, cyberhot och hybridkrigföring tilltar från 2011.

Sedan Rysslands olagliga annektering av ukrainska Krim 2014 har Sveriges säkerhetspolitiska läge successivt försämrats. Säkerhetspolitik karakteriseras av att betydande värden står på spel. Svensk säkerhetspolitik har vilat på en regelverksbaserad ordning som har sitt ursprung i folkrätten, regler och avtal.

De säkerhetsförslag som Ryssland presenterade i december 2021 skulle omkullkasta den europeiska säkerhetsordningen, omöjliggöra ett svenskt Nato-medlemskap och också innebära en storskalig relativ omfördelning av makt och inflytande i det internationella systemet.

I och med Rysslands invasion av Ukraina i februari 2022 har den europeiska säkerhetsordningen upphört som ett gemensamt system. I avsaknad av Natos säkerhetsgarantier befinner sig Sverige i ett besvärligt säkerhetspolitiskt läge vilket också påverkar hotbilden mot bankerna.

Gråzonen

Hotbilden från främmande makt karaktäriseras idag till stor del av så kallad gråzonsproblematik och krigföring kan i den delen beskrivas som kontaktlös, det vill säga via fjärrstridsmedel och global spaning. Gråzon är ett konceptuellt begrepp där vare sig ”krig” eller ”fred” råder. Gråzonsaktiviteter är ett samlingsnamn för antagonistiska påverkansaktiviteter exempelvis att manipulera information, projicera makt på olika sätt, avsiktligt kränka ett lands luftrum, cyberattacker och så vidare. Syftet med gråzonsaktiviteter mot Sverige är att försöka påverka svenskt beslutsfattande och minska vår handlingsfrihet. Det kan handla om att skada tilliten, undergräva våra värderingar, splittra oss och försvaga vår motståndskraft eller att störa samhällsviktiga funktioner som bankverksamhet.

Svenska banker utgör idag en stor del av de baltiska ländernas finansiella infrastruktur vilket också

> Bankerna behöver också kunna besvara frågan vad som händer med banksektorn vid höjd beredskap och ytterst krig.

påverkar hotbilden. Risken för antagonistiska gråzonsaktiviteter med syfte att påverka banker och finansiell infrastruktur bedöms därför ha ökat. Bankerna är vana vid att skydda verksamheten mot olika hot och att planera och öva för att kunna hantera och återta verksamheten vid störningar och incidenter. Rysslands invasion av Ukraina visar ändå hur snabbt det kan gå och att utvecklingen utanför Sverige kräver ett långsiktigt beredskapsarbete i Sverige. Bankerna behöver också kunna besvara frågan vad som händer med banksektorn vid höjd beredskap och ytterst krig.

Sektorns beredskapsarbete

I Sverige byggs nu ett nationellt cybersäkerhetscenter upp. Centret ska stärka Sveriges förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och främja ett utökat informationsutbyte mellan privata och offentliga aktörer, exempelvis avseende detektion, sårbarheter, hot och risker. Den finansiella sektorn är pilotbransch.

Syftet är att stärka cybersäkerheten inom finanssektorn och tillsammans öka Sveriges motståndskraft mot cyberhot. Bankerna har ett behov av att ta del av underrättelser och information som har bäring på den säkerhetspolitiska hotbilden mot Sverige och den svenska finansiella sektorn.

Tröskeln för användning av ickemilitära påverkansmedel sjunker vilket ökar fokuset på beredskaps- och totalförsvarsfrågor i Sverige. Förslagen i utredningen ”Struktur för ökad motståndskraft” (SOU 2021:25) innebär att en målbild nu har börjat skönjas och genom den nya Beredskapsförordningen (2022:524) inrättas beredskapssektorn ”Finansiella tjänster” med Finansinspektionen som sektorsansvarig myndighet.

BEHOV AV ÅTGÄRDER

Med anledning av utvecklingen ser Bankföreningen behov av följande åtgärd och initiativ från politik och myndigheter.

- Myndigheterna inom beredskapssektorn ”Finansiella tjänster” behöver accelerera arbetet genom att sätta upp mål för beredskapsarbetet, identifiera de samhällsviktiga funktionerna och styra mot dem.

Bedömningen är att Sveriges säkerhetspolitiska läge och utveckling påverkar hotbilden mot bankerna.

Informations- och cybersäkerhetshot

Hotbilden inom informations- och cybersäkerhetsområdet har under 2022 fortsatt att drivas av framför allt hotet från statsstödda aktörer, där Rysslands anfallskrig mot Ukraina har en stor tyngd, men även hotet från grovt organiserad brottslighet.

Specifikt mot Ukraina har den ryska krigsmakten och hotaktörer anslutna till Ryssland genomfört destruktiva cyberattacker riktade mot energi-, vatten- och annan kritisk infrastruktur som en del av hybridkrigföringen. Destruktiv skadlig kod, ”wiper malware”, har använts för att förstöra kritiska system genom att permanent kryptera eller radera data och filer i de system som attackeras. Även överbelastningsattacker, som påverkar tjänsters tillgänglighet, har varit ett tydligt inslag i hybridkrigföringen. Ryssland har också attackerat Ukrainas digitala infrastruktur rent fysiskt genom attacker med kryssningsrobotar mot viktiga datacenter i landet.

Rysslands invasion har inneburit en utveckling där en mängd verktyg och metoder för cyberangrepp utvecklas och används. Detta har synliggjort det digitaliserade samhällets exponering mot cyberangrepp. För de svenska bankerna har utvecklingen inneburit ett allt större fokus på att inhämta information om cyberhot och att ständigt ha en uppdaterad bild av cyberhotslandskapet.

Erfarenheter från Ukraina

Bankerna och den finansiella infrastrukturen i Ukraina har fungerat relativt väl under kriget. Viktiga framgångsfaktorer har varit gemensamma förberedelser, beredskapsplaner och övningar bland sektorns aktörer. Dagarna innan krigsutbrottet ändrade Ukraina sin lagstiftning för att göra det möjligt att lagra data från myndigheter och privata företag utanför landets gränser. I samband med krigsutbrottet påbörjades en storskalig överföring av information såsom folkbokföring, mark- och fastighetsägande, skatteregister, utbildningsregister till molntjänster för att på så sätt skydda informationen från attacker med kryssningsrobotar och liknande stridsmedel.

Sedan krigsutbrottet har det inte i någon större utsträckning rapporterats om att ryska hotaktörer genomfört destruktiva cyberattacker mot västerländska banker och finansiella företag. Bedömningen är att Rysslands cyberattacksförmågor är och har varit fokuserade på operationer i Ukraina. Trots det finns anledning till fortsatt hög vaksamhet mot tänkbara cyberhot mot svenska banker.

Destruktiv skadlig kod

Till skillnad från utpressningsprogram, ”ransomware”, som krypterar sina offers data tills en lösensumma är betald, syftar destruktiv skadlig kod till att förstöra system och data. Användningen av destruktiv skadlig kod är därför vanligtvis inte ekonomiskt motiverad utan används främst av hotaktörer som har för avsikt att orsaka skada och svårigheter för samhällskritisk infrastruktur.

Bankerna exponeras främst mot dessa typer av attacker genom sitt digitala tjänsteutbud och den känsliga information som banker hanterar. Det finns också en indirekt exponering mot bankerna genom det faktum att attacker riskerar att sprida sig till andra aktörer och geografier än den tänkta träffytan. Detta inträffade exempelvis 2017 när den skadliga koden ”NotPetya”, som ursprungligen var utformad för att slå mot kritisk infrastruktur i Ukraina, inklusive den ukrainska centralbanken, fick en global spridning och drabbade ett stort antal organisationer.

Sedan invasionen i februari 2022 har Ryssland attackerat Ukraina med en stor mängd av olika typer av destruktiv skadlig kod. Trots detta har effekterna av attackerna varit mindre än förväntat, mycket tack vare den uppbyggnad av cyberförsvaret som Ukraina genomfört sedan kriget och ockupationen av Krim 2014.

Överbelastningsattacker

Hotbilden angående överbelastningsattacker är fortsatt relevant. I anslutning till invasionen i Ukraina har överbelastningsattacker drabbat både ukrainska myndigheter och banker, framför allt strax innan och i början av kriget.

Aktivistgrupper med anknytning till Ryssland har genomfört ett större antal överbelastningsattacker mot framför allt verksamheter och företag i Natoländer och dess allierade. De har också specifikt attackerat banker i Europa. Bedömningen är att i de flesta fall har bankernas skydd fungerat väl och attackerna har inte fått någon större påverkan på de digitala kanalerna.

Överbelastningsattacker har det senaste året även syftat till att skapa uppmärksamhet och sprida desinformation. Attackerna kan också användas för att testa en banks säkerhet som en del av planering för senare attacker, eller som en avledande manöver medan man samtidigt attackerar banken på annat sätt, till exempel genom skadlig kod.

I början av 2023 drabbades Sverige av ytterligare överbelastningsattacker i anslutning till koranbränningen i Stockholm i januari. Attackerna har genomförts brett och drabbat ett större antal myndigheter, offentliga organisationer och näringslivet, däribland bankerna. Inledningsvis tog aktivistgruppen Anonymous Sudan på sig attackerna, men analyser har visat att det kan finnas kopplingar till statsstödda aktörer och att attackerna skulle kunna vara en del av ett större narrativ med inslag av desinformation riktat mot Sverige. Det visar på svårigheten att knyta cyberattacker till en specifik aktör. Även för dessa händelser är bedömningen att attackerna inte har fått någon större påverkan på bankernas digitala kanaler.

Beroenden till kritisk infrastruktur

Sabotaget mot gasledningarna Nord Stream 1 och 2 i september 2022 visar på riskerna mot kritisk infrastruktur på grund av det rådande säkerhetsläget i närområdet. Ytterligare tänkbara scenarios är sabotage mot fiberinfrastruktur i Östersjöområdet, liknande det sabotage som inträffade i Frankrike i

Skadlig kod eller länkar till skadlig kod via e-post till medarbetare i bankerna är ett vanligt förekommande hot.

oktober 2022. För de svenska bankerna innebär det att de måste lägga ett ökat fokus på att se över sina beroenden till kritisk infrastruktur och planera för att eventuellt ytterligare öka sina resurser och sin kapacitet, exempelvis elektronisk kommunikation och elförsörjning.

Övriga relevanta cyberhot

De tekniska riskerna relaterade till distansarbete är fortfarande aktuella, men i det postpandemiläge vi nu befinner oss i har de åtgärder, skydd och extra kontroller som bankerna etablerade blivit en del av vardagen. Användning av företagshanterade datorer och tillgänglighet till VPN med multifaktorsautentisering minskar sårbarheten för cyberangrepp och informationsläckage. Bedömningen är att bankerna har klarat den tekniska omställningen väl.

De fysiska riskerna och anpassningarna på grund av covid-19-pandemin har också medfört nya arbetssätt och nya risker eftersom medarbetarna inte är omgärdade av det sammanhang som kollegor på ett fysiskt kontor skapar. I jämförelse med den ordinarie arbetsplatsen erbjuder inte hemmakontoret den tillhörighet och fysiska skydd som ett kontor fyllt med kollegor skapar, vilket kan påverka både företagskultur och lojalitet. Distansarbete innebär också att medarbetare behöver förstå bankens interna riktlinjer för hur man ska arbeta hemma på ett säkert sätt samt hur till exempel känslig information ska hanteras.

Användande av IT-leverantörer och molntjänster är fortsatt aktuellt för svenska banker. Samtidigt som det kan finnas stora fördelar är det också förknippat med risker och hot. Skadlig kod kan spridas genom etablerade leverantörsled och aktiviteter som ingår i utveckling, produktion och distribution av både mjukvara och hårdvara. Bankerna har normalt ett antal IT-leverantörer som löpande och automatiskt levererar uppdateringar gällande såväl funktion som säkerhet för sin respektive lösning. Det kan dock vara svårt att upptäcka om det exempelvis finns en bakdörr som en del av en uppdatering. Bankerna behöver därför aktivt övervaka sina IT-leverantörer.

Skadlig kod eller länkar till skadlig kod via e-post till medarbetare i bankerna är ett vanligt förekommande hot. Det har förekommit kampanjer där en större mängd anställda hos banken fått phising-mejl som skickats ut opportunistiskt. Även ”spear phishing”, det vill säga nätfiske som riktar sig mot utvalda personer hos bankerna förekommer. Bedömningen är att skadlig kod via phishing kommer fortsätta vara en hög risk för bankerna. Övningar och utbildning för att personalen ska kunna upptäcka phishing-mejl samt tekniska lösningar för att blockera phishing-mejl är fortsatt viktiga motåtgärder.

Under perioden 2022–2023 har förekomsten av banktrojaner minskat, och bedömningen är att svenska banker och bankkunder inte har drabbats i någon större omfattning. Banktrojaner som infekterar mobiltelefoner och mobilbankslösningar syftar ofta till att stjäla kundernas inloggningsuppgifter. Banktrojaner utvecklade för Android-telefoner har varit vanligare än för iOS-telefoner. Bankkunderna har ofta fått sina mobiltelefoner infekterade genom att ladda ner appar som innehållit skadlig kod.

BEHOV AV ÅTGÄRDER

Med ett försämrat säkerhetspolitiskt läge och ökade cyberhot ser Bankföreningen behov av ett antal samordnade åtgärder och initiativ från politik, myndigheter, näringsliv och andra delar av samhället:

- Den politiska styrningen av cybersäkerhetsområdet på nationell nivå behöver förbättras. Ett cybersäkerhetsråd bör inrättas inom statsrådsberedningen med uppgift att följa upp den nationella cybersäkerhetsstrategin och se till att den leder till konkret handling. Det är viktigt att rådet blir en effektiv arena för samverkan mellan olika myndigheter och samtidigt driva en rad nyckelfrågor för att öka cybersäkerheten.
- Utbytet och användningen av information mellan myndigheter och näringslivet behöver förbättras. Bankerna har behov av mer och snabbare underrättelser om potentiella cyberhot och sårbarheter. Samtidigt är bankerna beredda att bidra med sina förmågor på området. Bankföreningen ser därför mycket positivt på den samarbetspilot som Nationellt cybersäkerhetscenter nu bedriver tillsammans med den finansiella sektorn.
- En nationellt sammanhållen övnings- och teststrategi för cyberdomänen bör inrättas. Den kan bidra till strukturerade och mätbara resultat, vilket ger värdefulla underlag och rekommendationer till beslutsfattare, och ska kunna bidra till Sveriges informations- och cybersäkerhetsstrategi.

Bedömningen är att hotbildens sofistikeringsgrad ökar och påverkas av Rysslands invasion av Ukraina. Den IT-brottsrelaterade hotbilden blir mer komplex och samverkande. Inom cyberområdet kan hotbilden också påverkas av en antagonist med uthållig förmåga och vilja som ser ett tillfälle kopplat till den säkerhetspolitiska utvecklingen.

Bedrägerier och finansiell brottslighet

Minskat antal bank- och värdetransportrån, digitalisering, och samhällets ökade krav på e-handeln att använda bankens säkerhetslösningar har förändrat den finansiella brottsligheten.

År 2022 anmäldes 193 391 bedrägeribrott i Sverige, enligt Polisen, vilket är en ökning med 481 brott i jämförelse med 2021 (+0,25 procent). De fyra senaste åren har dock antalet polisanmälda bedrägeribrott minskat med cirka 25 procent. Förklaringen till minskningen är framför allt genomförandet av PSD2 (det andra betaltjänstdirektivet). Kravet på stark kundautentisering i PSD2:s tekniska standard som trädde i kraft den 1 januari 2021 har resulterat i en markant minskning av antal kortbedrägerier, mestadels så kallad Card Not Present, när det fysiska kortet inte är närvarande vid transaktionen.

Antal bedrägerier minskar men brottsvinsterna ökar

Även om antal polisanmälda bedrägerier har minskat med 25 procent de senaste fyra åren så har bedrägerivinsterna ökat med 30 procent på två år, enligt Polisen (rapporten De dödliga bedrägerierna, sid. 11, Dnr: A554.314/2022). Minskningen av antal polisanmälda bedrägerier de senaste fyra åren består till stor del av en minskning av antal kortbedrägerier. Ökningen av bedrägerivinster kan förklaras av att bedrägerier med inslag av social manipulering, exempelvis vishingbedrägerier, har ökat markant.

År 2019 var antal polisanmälda vishingbedrägerier 5 285, vilket hade stigit till 21 582 (+408 procent) 2022. Under samma tidsperiod har antalet större utredningar mot de brottskluster som misstänks stå för en stor del av dessa vishingbedrägerier minskat från tio utredningar 2019 till en (1) utredning 2022, enligt Polisen.

Organiserad brottslighet med stort våldskapital påverkar idag bankerna genom att agera som en ”fullsortiments-brottsorganisation” med påverkan på områdena fysisk säkerhet, bedrägeri och penningtvätt där de olika delarna går in i varandra.

Enligt Polisen kan närmare hälften av bedrägeribrotten kopplas till organiserad brottslighet och gängkriminalitet. Medlen används för investeringar i både kriminella miljöer och i den lagliga ekonomin.

Digitalisering går fort

En av huvudutmaningarna är att tjänsteutveckling och digitalisering går väldigt fort vilket innebär att även hotbilden förändras snabbt. Snabbheten kräver i sin tur ett realtidsskydd avseende informationsdelning, och det uppstår ett behov av att dela tekniska uppgifter som cookies, IP-adresser, information om sårbarheter och riktade attacker. Bankerna tar ned falska hemsidor på löpande band, vilket kräver ytterligare kompetens och resurshantering.

> Historiskt sett har bankerna haft förmåga att kunna parera bedrägeribrott, men digitaliseringen i samhället och PSD2 har förändrat förutsättningarna.

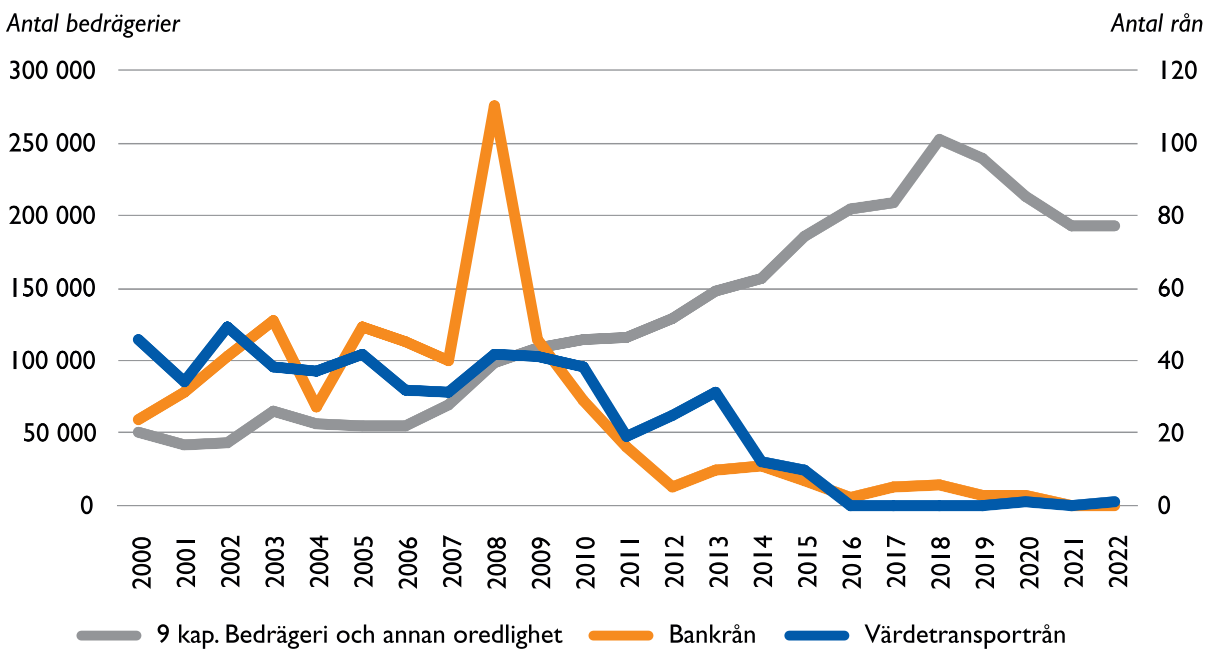
Banken behöver också förstå vilka hot och sårbarheter för både bedrägeri och penningtvätt som nya produkter medför, samt ta fram motverkande åtgärder. Nya tjänster och produkter utvecklas inte alltid av banken själv utan kan ske i samarbeten med andra aktörer eller av tredje parter. En ständig avvägning måste ske mellan smidighet och kundvänlighet å ena sidan, och tröghet och ökad säkerhet å andra sidan. Utvecklingen är starkt affärsdriven och bankens kunder förväntar sig att banken erbjuder nya produkter och tjänster i takt med den tekniska utvecklingen. Utvecklingen påverkas också av politiska incitament, exempelvis PSD2, som ger banken sämre möjligheter att hinna vidta relevanta motåtgärder.

Med PSD2 och tjänsteleveranser som bygger på tredjeparters access till konton och data, hos banker kallat ”open banking”, har flera aktörer tillkommit i betalningskedjan vilket medför nya risker och förutsättningar. För konsumenter kan det vara svårt att förstå vad man ger sitt samtycke till och vilken aktör som får tillgång till kunduppgifter. Det saknas idag tydlig kravställning mot tredje parter. Alla har inte den kontroll mot slutkund som myndigheterna ställer krav på banken att ha. Det kan handla om riskbedömning av kunder, åtgärder för kundkännedom och bedrägerimonitorering samt en process som säkerställer att momenten hänger ihop med varandra, utöver kraven på bankerna att vara tillgängliga dygnet runt.

Lagstiftningen påverkar området

Just nu utvärderas från EU-håll om man ska gå från ”open banking” till ”open finance”, vilket kan öppna upp bankernas infrastruktur för ännu fler aktörer inom olika finansiella tjänster utöver betalningar och kontoinformation. ”Open finance” låter fler finansiella aktörer få tillgång till och möjligheten att dela en stor mängd finansiell data. Det handlar alltså inte bara om betalningar, utan även om bolån, lån, sparande, pensioner och försäkringar som kan öppnas för tredje part. Det innebär att fler kundupp-

Antal bedrägerier samt bank- och värdetransportrån 2000–2022



Källa: Bankföreningen och BRÅ.

gifter ska få användas inom en rad finansiella tjänster inom EU med kundernas samtycke. Det politiska målet är att förbättra och skräddarsy finansiella produkter och tjänster för kunder samt skapa ökad konkurrens inom finanssektorn.

Risker som lyfts är bland annat cybersäkerhetsrisker, bedrägerier och finansiell brottslighet.

Viktiga frågor är därför kundernas kunskap och medvetenhet av hur produkter och tjänster fungerar, men också hur data lagras, används och distribueras. Lika viktigt är att det behöver finnas liknande kravställning mot samtliga aktörer inom "open finance".

Historiskt sett har bankerna haft förmåga att kunna parera bedrägeribrott, men digitaliseringen i samhället och PSD2 har förändrat förutsättningarna. Kortbetalningarnas affärsmodell, infrastruktur och riskfördelning har tidigare fungerat som ett slags skydd för konsumenter. Men när kraven ökar på att e-handeln ska använda bankens säkerhetslösningar i större utsträckning, ökar samtidigt kraven på kunderna, både att kunna använda de digitala verktygen och att klara av att stå emot olika former av bedrägeriförsök. Hotbilden har därmed förändrats och då behöver de förebyggande åtgärderna hänga med.

Social manipulering ökar

Som en konsekvens av de ökade autentiseringskraven för e-handeln, har brottsligheten drivits mot tillvägagångssätt med större inslag av social manipulering som exempelvis telefonbedrägerier. Brottsligheten har på så sätt blivit mer riktad och mer personlig. Konsumenter och företag har blivit mer utsatta för bedrägeribrottslighet som får större konsekvenser för dem, vilket även påverkar bankerna. Bedragarna riktar in sig mot de äldre, de mest sårbara i samhället.

Många av aktörerna bakom bedrägerierna har koppling till grov organiserad brottslighet. Det är idag lönsamt för organiserad brottslighet att investera i den här typen av bedrägliga brottskoncept eftersom andelen uppklarade bedrägerier är låg.

Bankföreningen anser att det är ett stort systemhotande samhällsproblem som drabbar såväl enskilda människor som banker, företag och myndigheter.

Trenden att bedragare försöker förmå kunder att genomföra autentiserade transaktioner, genom telefon, e-post eller sms, har de senaste åren förstärkts. Utvecklingen går mot att en kund luras och manipuleras att lämna ifrån sig information, alternativt att på bedragarens uppmaning genomföra en transaktion själv, en så kallad behörig transaktion enligt PSD2.

För kortbedrägerier är utvecklingen liknande, det vill säga allt fler bedrägerier sker där transaktionerna rent tekniskt godkänts av betalaren. Ett exempel där kunder utsätts för social manipulering är vid anslutning av digitala plånböcker. Tillvägagångssättet är att kunder luras att dela information om koder för autentisering och signering till bedragare som i stället ansluter ett kort till en digital enhet under bedragarens kontroll. Bedragaren utger sig ofta att vara från bank, myndighet, polis eller fraktföretag via e-post och sms, och hänvisar kunderna till ett gränssnitt där uppgifterna ska fyllas i av kunden.

Trenden med bedrägerier där transaktionerna godkänts av betalaren medför därmed ett mer komplext problem för banken att både övervaka och förstå när det finns en bedragare bakom en kunds transaktioner på internet- och mobilbank. Bankerna lägger ned mycket tid och resurser på att prata med sina utsatta kunder.

Bedrägeriuppläggen varierar. Aktuella omvärldshändelser används ofta som bete. Den gemensamma nämnaren för bedrägeriuppläggen är försöket och viljan att påverka och förmå bankkunden att göra något: klicka på en länk, genomföra en betalning eller ringa ett nummer.

När bankerna inte hanterar kundinterface (det tekniska gränssnittet) genom app eller hemsida får bankerna mindre data till sin bedrägeriövervakning. Transaktioner till uppsamlingskonton är svårare att övervaka jämfört med betalningar och överföringar. Om banken inte kan se mottagarkonton försvåras bankens penningtvätts- och bedrägeriövervakning.

En dom från Högsta domstolen i juni 2022 (Mål T4623-21) rörande obehöriga transaktioner, riskerar att få konsekvenser som spiller över på penningtvättsområdet, främst i form av så kallad "friendly fraud"; det vill säga när den bedragna kunden och bedragaren är i maskopi med varandra.

Bedragarna använder sig redan av ett automatiserat och robotiserat arbetssätt, och bankerna kommer att behöva följa utvecklingen av bedragarnas användande av AI (artificiell intelligens).

Bättre datadelning ger bättre riskbedömningar

Att kunder idag utför många bankärenden själva medför att det blir allt viktigare för banken att kunna upptäcka ett avvikande beteende. Bankerna arbetar systematiskt med preventiva metoder, som limiter och begräsningar i produkter, samt aktiv monitorering utifrån kundernas beteende för att hantera de risker som finns. Om lagstiftningen skulle tillåta mer datadelning mellan aktörer i samhället skulle det bidra till en bättre monitorering genom bättre riskbedömningar i både det preventiva arbetet och i bankernas monitorering.

Utvecklingen inom realtidsbetalningar innebär delvis samma och delvis nya risker. Realtidsbetalningar kräver förmåga att både anpassa limiter och att blockera transaktioner, men också precisa preventionsverktyg eftersom monitorering endast kan eliminera en liten del.

Att kunder idag utför många bankärenden själva medför också att det blir allt viktigare för kunden att kunna hantera de digitala verktygen. Banken måste utbilda och informera om hur produkter och tjänster fungerar.

Hembesöken fortsätter

Antal hembesök av bedragare som påstår sig vara banktjänstemän eller är utklädda till poliser och hemtjänstpersonal fortsätter vara ett problem. Bedragarens förevändning är ofta att denne vill ”hjälpa till” med något påstått problem, medan syftet med hembesöket är att stjäla värdesaker eller komma åt kundens bankkort, säkerhetsdosa eller e-legitimation. Risken för att antalet hembesök och personrisker ökar när banken täpper till möjligheten till andra tillvägagångssätt är en realitet som behöver beaktas i arbetet för att motverka bedrägerier. Brott mot människor med svaga tekniska kunskaper ökade under covid-pandemin. Det har inte nödvändigtvis med ålder att göra. Utan sociala sammankomster där man kan prata om dessa frågor blir okunskapen större.

Alla banker informerar sina kunder om hur bankens tjänster fungerar, men enbart information kommer inte att vända brottsutvecklingen med social manipulering. Det finns ingen enskild förändring som kan lösa utmaningarna med social manipulering, utan det handlar snarare om ett antal förebyggande och samverkande åtgärder.

De största bedrägerihoten

Svenska konsumenter och företag är idag utsatta för bedrägeriförsök på många olika sätt. Allt ifrån phishing av inloggningsuppgifter (till exempel e-legitimation och säkerhetsdosa) till spridning av skadlig kod via e-post, sms och hemsidor. Konsumenter och företag utsätts också för romansbedrägerier, investeringsbedrägerier, vishingbedrägerier, smishingbedrägerier, kreditbedrägerier, BEC-bedrägerier (Business E-mail Compromise, till exempel VD-bedrägerier) samt ID-kapningar, annons- och sociala medier-bedrägerier.

Både konsumenter och företag utsätts i allt högre utsträckning för bedrägerier vars syfte är att snabbt komma åt och tömma kundens bankkonton. För att kunna genomföra den typen av bedrägerier manipuleras kunden på olika sätt att använda sin e-legitimation eller säkerhetsdosa.

De största bedrägerihoten 2022 har varit vishingbedrägerier, smishingbedrägerier, investeringsbedrägerier, romansbedrägerier och kreditbedrägerier. Tillvägagångssätten förklaras nedan.

- **Tillvägagångssätt i vishingbedrägeri** (telefonbedrägeri) är en konsument som blir uppringd av en bedragare och under telefonsamtalet blir lurad att antingen lämna ifrån sig koder från sin säkerhetsdosa eller att identifiera sig eller signera uppdrag med sin e-legitimation. Kunderna luras att själva utföra transaktionerna, exempelvis under förevändning att pengar behöver skickas till ett ”säkert konto”.

- **Tillvägagångssätt i smishingbedrägeri** (falska sms) är att bedragaren till en konsument skickar ett sms som informerar om ”misstänkt aktivitet på kort eller konto”, eller ett sms från ”mamma som har bytt telefon och behöver hjälp” med en uppmaning att göra något: att uppdatera en programvara eller kundinformation, att klicka på en länk eller att ringa ett nummer.

- **Tillvägagångssätt i romansbedrägeri** är en konsument som blir kontaktad och uppvaktad av bedragare. För bedragaren handlar det om att nå människor i situationer där de är som mest sårbara, och kärlek är i det sammanhanget en stark mänsklig drivkraft.

- **Tillvägagångssätt i investeringsbedrägeri** är att en konsument blir kontaktad och erbjuden en påhittad investeringsmöjlighet av bedragaren.

- **Tillvägagångssätt i kreditbedrägeri** är att en bedragare ansöker om ett lån med falska underlag, eller att kunden inte har någon intention att betala tillbaka lånet. Identiteten kan vara utvandrad, överlåten till någon annan eller fabricerad.

De största bedrägerihoten 2022 har varit:

- vishing
- smishing
- romans
- investering
- kredit

Bedragarna verkar vara väl insatta i hur både bankernas produkter och teknik fungerar men också hur branschens processer för clearing fungerar.

Bedragare skyr inga medel för att lyckas med sina upplägg. Telefonbedrägerier förekommer i många former. En trend som har förstärkts de senaste åren är att bedragare blir allt duktigare på att kartlägga sina tilltänkta offer i olika målgrupper. Genom information från hemsidor kan bedragarna se en persons personnummer, adress, inkomst och annat. Med hjälp av informationen bygger bedragaren upp en trovärdig historia i syfte att manipulera det tilltänkta offret. Bedragare döljer sig ofta bakom ”spoofade” telefonnummer, det vill säga maskerade nummer där bedragaren väljer själv vilket telefonnummer som ska uppvisas i displayen samt bankens jinglar (förinspelade meddelanden) för att försöka framstå som att det verkligen är banken som kontaktar sina kunder.

Kreditbedrägerier

Att knyta samman förståelsen för de olika uppläggen av kreditbedrägerier – från perspektivet kundens ansökan av krediten till perspektivet kundens betalning av krediten – är utmanande.

Angående perspektivet kundens ansökan av krediten fortsätter antalet falska arbetsgivarintyg, lönespecifikationer, manipulerade kontoutdrag och åtgärder som syftar till att påverka utfallet av kreditansökan att ligga på en hög nivå.

För bankerna kräver kreditprocessen mycket resurser och analysarbete och mycket preventions- och monitoreringsarbete för att förhindra kreditbedrägerier. Analyser av så kallade ”straight rollers” (personer som tar upp lån utan avsikt att betala) har resulterat i att onboarding-processen har setts över hos vissa banker och att varningssignaler på så sätt kunnat identifierats tidigt i processen.

Eftersom kreditbedrägerier delvis bygger på falska inkomstuppgifter har ett antal banker börjat använda externa tjänster för att kontrollera kunders inkomstuppgifter och konton. Med dagens förutsättningar och kunskap behöver banken ha internutbildningar om risken för kreditbedrägerier eftersom tidig upptäckt är väsentlig för att stoppa efterföljande penningtvätt.

När det handlar om kundens betalning av krediten finns risk för att banken tar emot medel från penningtvättsupplägg om medlens ursprung är tvivelaktigt, och då hamnar banken i en svår situation för hur kundförhållandet ska hanteras. Dessutom riskerar ärendena att snabbt bli komplexa.

Målvakter möjliggör bedrägerier

Målvakter är i detta sammanhang möjliggörare för finansiell brottslighet och antalet målvakter i Sverige fortsätter att vara ett problem. Bankernas arbete försvåras av att när kriminella upptäcks i en bank byter de snabbt bank och fortsätter sina brottsliga aktiviteter i en annan bank. Bankerna arbetar strukturerat med att analysera och motverka målvakternas möjligheter till upprepad brottslighet och avslutar målvaktskonton som upptäcks, där pengar tycks komma från insättningar från någon som är utsatt för romansbedrägeri eller lönekapning.

I ett typiskt investeringsbedrägeri blir en kund manipulerad till att göra en investering i tron att den kommer att ge hög avkastning. Kunden luras först på små belopp som ofta relativt snabbt eskalerar till större belopp eftersom

”investeringen” gått så bra. När kunden har slut på egna medel uppmanas denne att låna pengar för att investera ytterligare. Ofta inser kunder inte att de är lurade och fortsätter med sina aktiviteter i sin iver att få tillbaka förlorade medel. Kunden riskerar att hamna i en desperat situation där den gör allt för att få sina pengar tillbaka. Till slut riskerar kunden att låta sig utnyttjas som målvakt för att ”rädda investeringen” genom att ta emot och skicka vidare pengar som kommer från andra drabbade kunder vilket i förlängningen kan innebära penningtvätt. Kryptovalutor används ofta för att flytta pengar i vishing- och investeringsbedrägerier.

Utfärdande av Mobilt BankID

Från hösten 2022 kan bankerna förstärka utfärdandeprocessen av Mobilt BankID genom en onlinekontroll mot Polisens utfärdade id-handlingar (pass och nationellt id-kort). Syftet med den extrakontrollen är att motverka bedrägerier.

Tillvägagångssätten förändras hela tiden. Under de första månaderna 2023 verkar det som att antal kortbedrägerier återigen ökar, vilket beror på att bedragare hittar sätt att komma runt stark kundautentisering genom kortinlösare utanför EU. Andra återkommande problem är abonnemangsfällor, ej erhållna varor och att det finns många påhittade hemsidor.

Bedömningen är att riskerna för bedrägerier och finansiella brott är fortsatt hög och ökande, och att hotbilden blir alltmer komplex och samverkande genom kombinerande tillvägagångssätt i samma brottsupplägg.

BEHOV AV ÅTGÄRDER

Med anledning av utvecklingen av specifikt telefonbedrägerier, och att det ligger i allas intresse att bryta utvecklingen, ser Bankföreningen behov av ett antal åtgärder och initiativ från politik och myndigheter.

- Lagstiftaren bör begränsa publicering av personuppgifter på internet med stöd av utgivningsbevis. Det är exempelvis enkelt att kartlägga ensamstående äldre med god ekonomi.

- Teleoperatörer verksamma i Sverige bör åläggas att försvåra / omöjliggöra maskering av telefonnummer genom en anti-spoofing-infrastruktur för telefon och sms, liknande det som redan finns för telefon i Finland och de förslag som planeras för sms.

- Kontrollmöjligheterna mot utfärdarna av ID-handlingar är begränsade. Förslagen i ID-kortsutredningen (SOU 2019:14), att minska antalet utfärdare av fysiska ID-kort och att förbättra bankers möjlighet att kontrollera id-handlingar, bör genomföras. Syftet är att stärka säkerheten i Sverige, och för bankernas del att minska antal obehöriga transaktioner. Att ställa större krav på svenska bankkunder att hantera fler säkerhetslösningar är förmodligen inte rätt väg att gå, de befintliga är tillräckligt säkra. Utmaningen ligger snarare i hur de ska användas.

- Bankerna bör också få utbyta information med varandra på ett enklare sätt. Det är enkelt för kriminella att dela information men svårt för samhällets goda krafter att dela information. Ett flöde av information mellan bankerna och Polisen krävs för en förebyggande effekt, till exempel en målvaktsförteckning där uppgifter från bland annat Polisens penningtvättsregister bör ingå.

- Polismyndigheten bör utveckla möjligheterna för brottutsatta att polisanmäla brott digitalt. De begränsade möjligheterna att polisanmäla brott riskerar att skapa ett mörkertal angående brottslighetens omfattning när många brottsutsatta är hänvisade till att ringa 114 14 där väntetiderna kan vara långa.

Kryptotillgångar, inklusive kryptovalutor, är en relativt ny bransch som är mycket sårbar för penningtvätt.

Penningtvätt

Av all penningtvätt som sker bedöms 85 procent av de svarta pengarna tvättas genom det finansiella systemet. Resterade tvättas genom virtuella valutor, spelmarknaden och ”hawala-banking” (ett system för penningöverföring utanför banksektorn) samt genom spelbolag och handel med varor och tjänster. De svarta pengarna har sitt ursprung i alla typer av kriminell verksamhet som resulterar i ekonomisk vinning.

2022 gjordes 45 113 misstankerapporter till Finanspolisen, en ökning med 20 procent jämfört med 2021 då motsvarande antal var 37 528. 2020 gjordes 24 505 misstankerapporter. Bankerna svarade, tillsammans med övriga rapportörer inom den finansiella sektorn, för 90 procent av det totala antalet rapporter 2022. 9 procent av antal misstankerapporter kom från spelsektorn. De senaste åren har 74 procent av antal misstankerapporter till Finanspolisen gjorts av banker.

De största penningtvättshoten

Rysslands invasion av Ukraina i februari 2022 har givit upphov till stora flyktingströmmar. Flyktingar är generellt sårbara för att utnyttjas för penningtvätt. Det kan också vara svårt för dem att få tillgång till det svenska finansiella systemet i de fall de saknar id-handlingar, vilket kan skapa konflikter. Kriget medför också en möjlighet för kriminella att utnyttja det stora hjälpbehovet.

Kryptotillgångar, inklusive kryptovalutor, är en relativt ny bransch som är mycket sårbar för penningtvätt. Marknaden är global och mycket volatil. Flera av världens största aktörer är registrerade i länder med bristande antipenningtvättsregimer eller med sekretessregler som förhindrar transparens. Kryptovalutor används ofta som betalningsmedel av kriminella vid illegal handel på till exempel Darknet (det icke-indexerade internet) samt vid ransomware-attacker. På flera handelsplatser för kryptovalutor är det möjligt att betala med bankkort. Ett penningtvättsupplägg som ökar i omfattning är försäljning av presentkort mot betalning i kryptovaluta.

Särskilda högriskgrupper är förmedlare av tjänster avseende kryptotillgångar, betalningsförmedlare och valutaväxlare. Dessa aktörer omfattas inte av samma omfattande regelverk som banker, och vissa aktörer är helt oreglerade. De har i många fall dåliga processer och kontroller för att förhindra penningtvätt, samtidigt som de använder bankernas infrastruktur och därigenom överför sina egna risker till banken. Vid transaktioner som rör kryptotillgångar går medlen i stor utsträckning till förmedlare av tjänster vars mottagarkonton finns i forna östblocket.

Även betalningsförmedlare och valutaväxlare är sårbara för penningtvätt. Det finns exempel på sådana verksamheter som drivs av kriminella. Eftersom dessa använder sig av bankernas betalinfrastruktur påverkar dessa sårbarheter banken.

Den kraftigt ökade förekomsten av bedrägerier ger också upphov till ökade penningtvättsaktiviteter. Bedrägerier är ett typiskt förbrott till penningtvätt. Det noteras att en hel del ”money mules” (bland annat målvakter) hanterar brottsvinster från bedrägerier och den efterföljande penningtvätten. Dessa ”money mules” är personer som, medvetet eller omedvetet, låter sina bankkonton utnyttjas för att överföra medel mellan olika banker. De är ofta yngre personer som individuellt hanterar mindre belopp.

Ett annat vanligt tillvägagångssätt för att undvika upptäckt i bankernas övervakningssystem är så kallad ”smurfing”, där flera små transaktioner sker i stället för färre och större transaktioner för att undvika att flaggas av bankernas övervakningssystem.

Kontanter ger dålig spårbarhet

Kontanter är fortfarande ett mycket attraktivt betalningsmedel i den illegala ekonomin eftersom spårbarheten är mycket dålig. Kontantintensiva kunder är därför förknippade med hög risk. Trots att kontantanvändningen generellt minskar i hela EU så ökar behovet av sedlar, vilket visar att kontanter fortfarande är viktiga verktyg som värdebevarare. Bankerna har generellt bra kontroll över de direkta insättningar / uttag som sker till banken, men så fort placeringsfasen ligger utanför banken, till exempel genom kontantköp hos handlare, grossister, spelbolag, och restauranger, har banken svårare att vidta åtgärder. Bankerna har lagt ut mycket av kontanthanteringen till tredje parter, exempelvis till Loomis, vilket gör banken sårbar i de fall den tredje parten inte efterlever AML-rutiner och vidtar relevanta kontroller. När kontanter förs utomlands för att växlas in i länder med stor kontantanvändning och dåliga kontroller, och sedan förs tillbaka till Sverige, är det mycket svårt för banken att kunna göra nödvändiga kontroller.

Marknaden för varor i lyxsegmentet såsom bilar, smycken och märkeskläder har vuxit kraftigt och attraherar kriminella, både som verktyg för att tvätta pengar, och som slutinvestering av kriminella tillgångar. Många lyxvaror är lätta att flytta och att sälja igen, vilket innebär att de kan användas för att överföra värden utan spårbarhet. De medför också goda möjligheter att tvätta kontanta medel i de fall handlarna tar emot kontanter.

Ett vanligt upplägg är att köpa en lyxvara kontant och lite senare lämna tillbaka den. Handlaren har då inte så mycket kontanter tillgängligt utan pengarna återbetalas genom insättning på kortkonto (i strid med kortregelverken). På så vis kommer svarta kontanter enkelt in i det finansiella systemet.

I de fall köpet av lyxvaror är den slutliga placeringen av svarta pengar exponeras bankerna genom handlarens insättning av dagskassor. Det är vanligt att kriminella köper högvärdesvaror i syfte att sälja varan vidare på andrahandsmarknaden. I de fallen kan pengar sättas in direkt i den kriminellas bankkonto och den kriminella kan motivera betalningen med dokumentation om att en vara sålts. I detta sammanhang ska också nämnas den omfattande handeln med stulna och förfalskade varor.

Fastighetsmarknaden medför stora möjligheter till kriminell verksamhet och till att tvätta pengar. Fastigheter och bostadsrätter är attraktiva eftersom de kan nyttjas på så många sätt (använda själv, hyra ut, sälja vidare, bygga nytt, renovera). Bostadsrättsföreningar är särskilt sårbara och kan lätt tas över av kriminella. Det finns många upplägg där värden kan överföras mellan olika individer genom under- eller övervärdering av objektet vid köp eller försäljning. Bostadslån kan användas för att finansiera dessa upplägg, ibland med hjälp av möjliggörare. Det finns risk för att fastighetsmäklare underlåter att göra penningtvättsrelaterade kontroller eftersom det kan riskera affären och därmed deras provision. Företag i byggbranschen förekommer ofta i bankernas utredningar om misstänkt penningtvätt.

Brister i lagstiftningen

Den nationella antipenningtvättsregimen innehåller brister, vilket medför att staten i många fall agerar som möjliggörare för kriminellas verksamhet och penningtvätt. Lagstiftningen ligger alltid efter den utveckling som sker i samhället. Många regler är utformade efter förhållanden som inte längre är relevanta medan existerande företeelser inte omfattas av befintliga regelverk.

Inte heller myndigheter är tillräckligt anpassade till dagens samhälle, vilket visar sig till exempel i dåliga eller obefintliga kontroller, något som möjliggör välfärdsbrottslighet.

Finanspolisen har inte tillräckliga resurser för att hantera alla misstankerapporter som lämnas av de aktörer som omfattas av penningtvättsregelverket och ge återkoppling. Det utbredda användandet av samordningsnummer samt den dåliga kontrollen av dem utnyttjas av brottslingar i penningtvättsupplägg.

Ett vanligt upplägg är att köpa en lyxvara kontant och lite senare lämna tillbaka den.

Kriminellas utnyttjande av välfärdssamhället utgör en särskild utmaning eftersom det rör sig om stora summor som kommer från avsändare med högt förtroende, det vill säga myndigheter. Det är svårt för en bank att kontrollera om det rör sig om korrekt utförda tjänster eller kriminella handlingar, samt att ifrågasätta summornas rimlighet och mottagarens legitimitet. Kontrollerna borde göras av den utbetalande myndigheten. Så fort nya bidrag eller stöd ges ut drar det till sig kriminella – något som tydligt visat sig beträffande ekonomiska stöd under covidpandemin, utbetalning av elstöd samt olika ekonomiska stöd relaterade till miljöbefrämjande åtgärder.

Spelsektorn medför en hög risk för penningtvätt; den är kontantintensiv med goda möjligheter att kunna genomföra snabba överföringar såväl inom som utanför Sveriges gränser. Spelföretag kan vara både online-baserade och traditionella kasinon på fysiska adresser. De flesta online-baserade företag är ofta belägna i lågskatteländer. Även om marknaden är reglerad och omfattas av penningtvättsregelverket finns åtskilliga olicensierade företag.

BEHOV AV ÅTGÄRDER

Med anledning av utvecklingen inom penningtvättsområdet ser Bankföreningen behov av ett antal åtgärder och initiativ från politik och myndigheter.

- Risker för penningtvätt och finansiering av terrorism behöver omfattas av samma reglering och tillsyn, oavsett var de uppstår. Om banker ska kunna tillhandahålla konton till högriskverksamheter behöver regleringen och kontrollen av dessa ökas betydligt.
- Den organiserade brottsligheten utnyttjar det faktum att bankerna inte kan dela information. När de kriminella upptäcks i en bank byter de snabbt bank och fortsätter sina brottsliga aktiviteter i en annan bank. För att åtgärderna mot penningtvätt och finansiering av terrorism ska kunna bli effektiva behöver bankerna därför få bättre möjligheter att dela information om misstänkta kunder, transaktioner och aktiviteter med varandra.
- De nya reglerna om samverkan och informationsutbyte mellan banker och brottsutredande myndigheter är ett bra steg framåt, men de behöver utvecklas ytterligare. Genom permanenta samverkansformer kan den erfarenhet och det förtroende mellan aktörerna som är nödvändig byggas upp för att uppnå resultat.
- Staten behöver ta ansvar för att kontrollera och verifiera de uppgifter som finns i statliga register för att minska risken för att dessa utnyttjas av den organiserade brottsligheten. Detta gäller till exempel Bolagsverkets register över företrädare och verklig huvudman till juridiska personer.

Bedömningen är att den sammanlagda risken för banker att utnyttjas för penningtvätt får anses vara hög.

De senaste två åren har antalet fall av misstänkt finansiering av terrorism via kryptovalutor ökat.

Finansiering av terrorism

Finanspolisens statistik över misstankerapportering skiljer inte mellan rapporter avseende penningtvätt och rapporter avseende finansiering av terrorism. Det finns därför ingen information om hur många rapporter om misstänkt finansiering av terrorism som gjordes under 2022 och om antalet rapporter ökar eller minskar.

En specifik brist är att bankerna saknar tillräcklig information om hur finansiering av terrorism sker för närvarande, samt vilka personer (både juridiska och fysiska) som är inblandande. Dålig information om vad bankerna ska reagera på och leta efter medför svårigheter att skapa bra scenarioregler som är baserade på relevanta parametrar för att kunna upptäcka misstänkt terrorfinansiering.

De senaste två åren har antalet fall av misstänkt finansiering av terrorism via kryptovalutor ökat. Bristande regelefterlevnad inom kryptobranschen och möjligheterna att lätt kringgå sanktioner gör det attraktivt. Användningen av kryptovalutor innebär att penningtvättare slipper problematiken med att transportera stora mängder sedlar långa sträckor. De behöver inte heller använda sig av banksystemet i någon större utsträckning och undkommer då bankernas kontroller. Det noteras att både våldsbejakande islamistiska organisationer och högerextrema organisationer använder sig av kryptovalutor i ökad omfattning.

Crowdfunding är en investeringsform där en stor grupp individer med små summor finansierar en verksamhet eller ett projekt. Utvecklingen av crowdfunding-plattformar möjliggör för privatpersoner att starta insamlingar på nätet, vilket även erbjuder goda möjligheter att finansiera terrorism.

För banken är det mycket svårt att skilja legitima insamlingar från den som sker med brottsliga intentioner. Våldsbejakande islamistiska organisationer är fortsatt förknippade med högre risk för finansiering av terrorism. Dessa kan finansiera sig genom bidrag och gåvor från medlemmar och sympatisörer i Sverige, men också med pengar från välfärdssystemet. De finansieras också genom medel från icke-statliga organisationer (NGO:s) och personer i utlandet. Medlen kan användas för rekrytering och radikalisering. Insamlings- och hjälporganisationer har verksamheter som typiskt sett är sårbara för finansiering av terrorism. Risken varierar dock beroende på organisationens typ av verksamhet, i vilka geografiska områden den är aktiv i samt vilken kontroll organisationen omfattas av.

Bedömningen är att den sammanlagda risken för att banker utnyttjas för finansiering av terrorism bedöms vara medelhög.

Restriktiva åtgärder – sanktioner

Restriktiva åtgärder – eller sanktioner – är en del av EU:s gemensamma utrikes- och säkerhetspolitik. EU använder dem som en del i en integrerad, övergripande politik som omfattar politisk dialog, kompletterande insatser och andra tillgängliga instrument. Syftet med sanktionerna är att de som sanktionerna riktas mot ska förändra sin politik eller sitt beteende, så att den gemensamma utrikes- och säkerhetspolitikens mål främjas. Sanktionerna kan riktas mot:

- regeringar i länder utanför EU på grund av deras politik.
- enheter (företag) som tillhandahåller medel för den politik som sanktionerna är riktade mot.
- grupper eller organisationer, till exempel terroristgrupper.
- enskilda personer som stöder den politik som sanktionerna är riktade mot, är inblandade i terroristverksamhet etc.

Sanktioner som utfärdas av tredje länder, som USA, Kanada, Storbritannien, och Australien är också relevanta för svenska banker. Sådana sanktioner är visserligen inte bindande i EU, men bankerna behöver förhålla sig till dem för att kunna tillgodose utländska korrespondentförbindelsers krav.
Det finns också en risk för svenska banker att drabbas av amerikanska ”secondary sanctions” om banken har relationer med någon som omfattas av amerikanska sanktioner.

EU har för närvarande utfärdat sanktioner mot Ryssland, Belarus, Nordkorea och Iran.

Sanktioner mot Ryssland och Belarus har ökat kraftigt i antal under 2022 och fler kommer att komma under 2023. Rysslandssanktionerna har funnits sedan 2004 och kommer antagligen att finnas kvar en länge tid. De medför tolknings- och tillämpningsproblem för både bankerna och bankernas kunder.

Efterlevnaden av sanktioner kräver att bankerna har en god kundkännedom. Bland annat är korrekta uppgifter om verkliga huvudmän nödvändiga.

Det finns metoder för att kringgå sanktionerna, som att skaffa sig medborgarskap någonstans i EU, sätta upp europeiska bolag och att använda sig av bulvaner. Det noteras att skalbolag är vanliga verktyg för de personer som försöker undvika sanktionerna.

Bedömningen är att den sammanlagda regelefterlevnadsrisken som sanktioner medför för bankerna bedöms vara medelhög.

Efterlevnaden av sanktioner kräver att bankerna har en god kundkännedom.

Formgivning och grafisk produktion: www.luxlucid.com   Stockholm, maj 2023

Svenska Bankföreningen
Swedish Bankers' Association

Telefon: 08-453 44 00
E-post: info@swedishbankers.se
www.swedishbankers.se