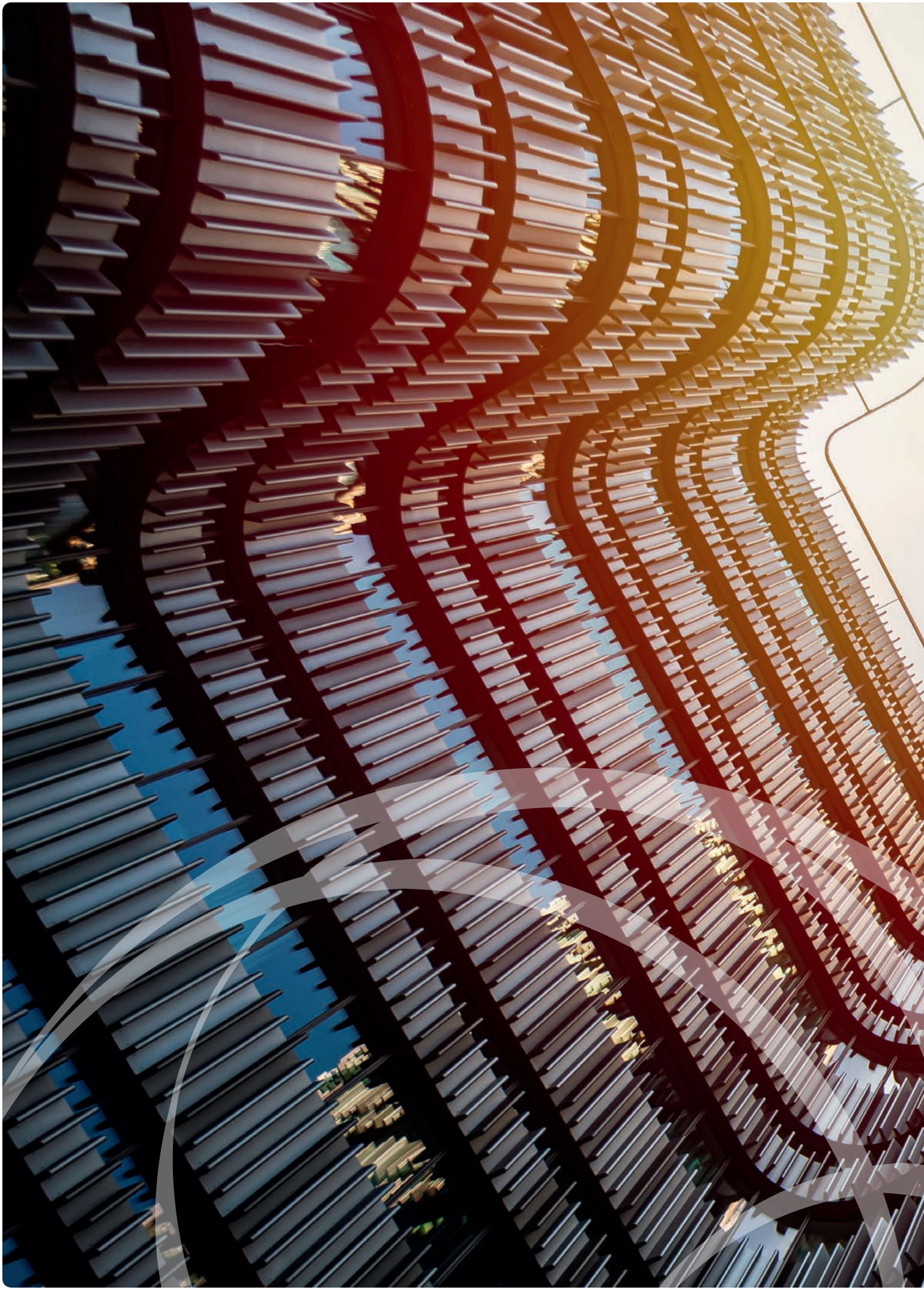
Hotbildsbedömning för Sveriges banker

Publicerad maj 2026

Svenska Bankföreningen
Finance Sweden



Hotbildsbedömning för Sveriges banker

Publicerad maj 2026

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.

Bankernas specialister på fysisk säkerhet, identifiering, cybersäkerhet, informationssäkerhet, bedrägerier, kortsäkerhet, penningtvätt, sanktioner, kontanter och säkerhetsskydd bidrar till rapporten.

Hotbildsbedömningen är uppdelad i ett antal avsnitt. Varje avsnitt avslutas med en sammanfattande bedömning samt en bedömning av hotnivå och en trendindikator. Hotnivån anger läget medan trendindikatorn anger riktningen och modellen förklaras i slutet på rapporten. Avsnittet om hotbilden mot säkerhetskänslig verksamhet bygger på öppna källor och säkerhetsmyndigheternas lägesbilder.

Åtgärder som bankerna inte kan vidta själva, men som bedöms ha en hotbildsreducerande effekt, listas som behov av åtgärder från politik och myndigheter.

Sammanfattning

Förhöjd

Inom området **kränkningar, hot och våld mot bankpersonal** rapporterar bankerna om ett fortsatt högt tonläge och tufft bemötande från kunder. Exponering av enskilda medarbetare kan öka hotbilden mot individen snarare än mot banken. En betydande andel av hoten är kopplade till bankernas arbete mot penningtvätt, exempelvis i samband med spärrade konton eller begränsning av tjänster. En trygg arbetsmiljö för bankpersonal är inte bara bankernas ansvar utan en del av ett samhällsåtagande.

Förhöjd

En **insider/möjliggörare** kan utnyttja sin insyn i banken för att genomföra olagliga transaktioner eller manipulera finansiella flöden på uppdrag av kriminella eller en främmande stat. Aktörer kan på så sätt även påverka beslut, informationsflöden och affärsstrategier i banken. Främmande stater kan använda insidernätverk för att samla underrättelser, destabilisera ekonomin eller påverka politiska beslut.

Förhöjd

Det försämrade säkerhetspolitiska läget innebär en fortsatt förhöjd hotbild mot den finansiella sektorn inom området **kontinuitet och civil beredskap**. Misstänkta sabotage mot kritisk infrastruktur, sårbarheter i digitala beroenden samt beroendet av utländska it-leverantörer ställer ökade krav på bankernas kontinuitets- och beredskapsarbete. Samtidigt kräver planeringen för höjd beredskap utveckling av bankernas krigsorganisation, personalförsörjning och samverkan, där otydliga mandat och regelverk i dagsläget utgör begränsande faktorer.

Förhöjd

Informations- och cybersäkerhetsområdet präglas av en breddad och mer komplex hotbild, där cyberutpressning i ökande grad bygger på informations- och identitetsstöld och utnyttjande av leverantörsberoenden. Samtidigt har överbelastningsangrepp fått minskad faktisk effekt till följd av stärkt motståndskraft hos bankerna, även om hotet kvarstår. Sammantaget innebär ökade tredjepartsrisker och framväxten av AI-baserade angreppsmetoder att kraven ökar på bankernas förmåga att upptäcka, hantera och motstå både direkta och indirekta cyberangrepp, där konsekvenserna i ett allvarligt scenario kan bli systempåverkande.

Hög

Social manipulering har gjort **bedrägeribrottsligheten** mer riktad och mer personlig. Bankernas åtgärdsprogram för att minska telefonbedrägerier har resulterat i cirka 60 procent lägre brottsvinster 2025 jämfört med 2023 och en tydlig nedgång av det genomsnittliga beloppet per telefonbedrägeribrott.

Hög

Penningtvättshoten är fortsatt omfattande till följd av att den kriminella ekonomin omsätter stora belopp årligen. Kriminella har en vilja att tvätta pengar genom i första hand den reguljära ekonomin. En brottsvinst som inte kan användas saknar i princip värde. Riskområdena är flera, men framträdande är till exempel kontanthantering, kryptovalutor och handel med lyxvaror och fordon.

Hög

Företag nyttjas frekvent och storskaligt i brottsliga syften, där målvakter används för att dölja de verkliga verksamhetsutövarna. Företag kan användas för olikartad brottslighet parallellt och brottsutbytet blir ofta stort. Inte sällan är det fråga om välfärdsbrottslighet och skattebrott som generar brottsutbyte. Det är vanligt att kriminella nätverk driver ett stort antal företag och genomför brottsliga transaktioner dem emellan.

Förhöjd

Finansiering av terrorism inbegriper många olika tillvägagångssätt såsom nyttjande av crowd funding, hawala och kryptovalutor. Finansiering av terrorism sker i allmänhet under falska förespeglingar och kan därför vara svår att upptäcka. En riskfaktor är att bankerna ofta saknar tillgång till aktuell information om var sådan finansiering misstänks samt vilka personer eller organisationer som kan vara inblandade.

Förhöjd

I och med tilltagande geopolitiska spänningar har **internationella sanktioner** blivit ett allt viktigare utrikes- och säkerhetspolitiskt påtryckningsmedel. Sanktionernas omfattning har ökat i snabb takt och därmed blivit allt svårare att såväl överblicka som tillämpa för verksamhetsutövarna. Här krävs utökad information, samverkan och dialog mellan aktörerna på sanktionsområdet. Särskilda utmaningar är det alltmer avancerade kringgåendet av sanktioner samt ökad diversitet mellan de olika sanktioner som bankerna måste ta hänsyn till.

Låg

Under 2025 inträffade inga **bank- och värdetransportrån** och inte heller några angrepp mot Bankomat AB:s uttagsautomater. Hotbilden mot bank- och värdetransportrån och angrepp mot uttagsautomater består men antalet rån och angrepp förväntas att ligga på en låg nivå 2026.

Låg

Det finns politiska incitament att öka kontantanvändningen i Sverige. För bankerna är **utmaningarna med kontanter** att det skapar risker för de som arbetar med kontanter och att spårbarheten för kontanter är låg eller obefintlig. Eftersom kontanter används i så liten omfattning i normalläget är det heller inte en realistisk lösning att kontanter kan ha en stor betydelse vid kris eller krigshändelse.

Förhöjd

Vad gäller **hotbilden mot säkerhetskänslig** verksamhet är bedömningen att det inom cyberdomänen finns både avsikt och god förmåga till avancerade och långvariga angrepp. Förmågan inom personal- och fysisk säkerhet bedöms vara mer begränsad med nyttjande av insiders respektive enklare fysiska angrepp genom lokala aktörer med begränsad uthållighet.

1 Kränkningar, hot och våld mot bankpersonal

Flera medarbetare och chefer inom banksektorn vittnar om ett fortsatt högt tonläge och tufft bemötande från kunder. Bankerna får signaler om att medarbetare känner sig otrygga. Bankerna bedömer att hotnivån ligger kvar på ungefär samma nivå som föregående år.

För banker med omfattande kontorsverksamhet är cirka hälften av incidenterna kopplade till fysiska kontor, medan resterande del riktas mot telefonbank och digitala kanaler.

Förändrade arbetssätt och nya risker

Större fokus på bokade kundmöten är idag ett etablerat arbetssätt inom bankerna. Beslutet är ofta affärsdrivet och syftar till att höja kvaliteten i kundmötet, men hänger även samman med kortare öppettider. Utvecklingen har bidragit till en minskad hotbild på kontoren, även om hot inte helt har eliminerats.

Det förekommer fortfarande att obehöriga personer tränger sig in i banklokaler i samband med in- och utsläpp av kunder. Även vid förbokade möten kan hotfulla situationer uppstå, vilket visar att hotbilden inte försvinner enbart genom förändrade rutiner.

Övergången till digitala kundmöten har dessutom medfört nya typer av risksituationer. I telefon- och webbmöten upplever medarbetare att kunder lättare uttrycker sig kränkande. Kränkningar via sociala medier förekommer också.

Hot kopplade till kundavveckling och regelefterlevnad

Bankerna avvecklar idag fler kundrelationer än tidigare, främst till följd av ökad upptäckt av oegentligheter och hotfullt beteende. Ett högre antal kundavvecklingar påverkar hotbilden, även om de mest allvarliga scenarier som tidigare befarades inte har realiserats i någon större omfattning.

Studier från bankerna visar att en betydande andel av hoten är kopplade till bankernas arbete mot penningtvätt, exempelvis i samband med spärrade konton eller begränsning av tjänster. När en kundrelation avslutas eller en person nekas att bli kund krävs därför interna processer för att bedöma och hantera en potentiell hotbild mot både personal och verksamhet.

Verktyg och stöd för medarbetare

Medarbetare kan hamna i svåra situationer, inte minst i mötet med ekonomiskt pressade kunder. För att hantera detta har bankerna utbildningar i konflikthantering för personal inom kontor och telefonbank samt tillgång till olika stödfunktioner.

Andra åtgärder för att hantera olämpligt kundbeteende är att banken kontaktar kunden per telefon eller skickar varningsbrev där det tydliggörs att kränkningar och hot mot personal inte accepteras.

Upplevd och faktisk hotbild

Hot kan vara antingen faktiska eller upplevda. En central utmaning är att bedöma allvaret i en situation, eftersom händelser som inte uppfyller lagens kriterier för hot ändå kan upplevas som starkt hotfulla och därmed bidra till en otrygg arbetsmiljö.

Bankerna har generellt god förmåga att identifiera hot, men graden av allvar och risken för eskalering är ofta svår att bedöma. Bankerna arbetar därför med att utveckla metoder för att bättre förstå och hantera hotbilden, exempelvis genom att skilja mellan reella hot och kränkande men tomma uttalanden.

Konflikter i den kriminella miljön bidrar till en ökad känsla av otrygghet i samhället, vilket i sin tur förstärker den upplevda hotbilden även inom delar av banken som inte utgör ett direkt kundmöte. Även om hot sällan realiseras och våld är sällsynt påverkas arbetsmiljön negativt.

Skillnader mellan olika delar av banken

Hotbilden varierar beroende på arbetsuppgifter och geografisk kontext. Medarbetare på mindre orter, som oftare möter kunder utanför arbetet, kan ha en annan sorts utsatthet än anställda i större städer eller medarbetare i telefonbank som inte möter kunder fysiskt.

Som nämnts tidigare är den personal som har kundkontakt generellt mest exponerade men det finns även exempel på att centrala beslutsfattare inom penningtvätts- och bedrägeriutredningar påverkas, särskilt när avvecklade kunder riktar sin frustration uppåt i beslutshierarkin. För avvecklade kunder är kundombudsmannen den funktion i banken som de hänvisas till. Detta har lett till en ökad belastning på kundklagomålsfunktioner och fler polisanmälningar kopplade till hotfulla incidenter.

Frustration kopplad till bankernas åtgärder

Myndighetsförfrågningar om exempelvis transaktioner rörande brottsutredningar och efterföljande banköverskridande åtgärder, såsom blockering av BankID och Swish, skapar ofta stark frustration hos kunder. Ett spärrat BankID uppfattas som ett stort ingrepp i vardagen eftersom många privata och offentliga e-tjänster har valt BankID som autentiseringsmetod. Åtgärden kan utlösa hot mot bankens personal eftersom det är bankerna som utfärdar tjänsterna. Att ställa kundkännedomsfrågor, ge avslag på en transaktion eller neka en produkt är återkommande källor till konflikter med kunder.

Bankernas åtgärder för att skydda medarbetare

För att minska exponeringen av enskilda medarbetare vidtar bankerna olika skyddsåtgärder. Medarbetare behöver inte alltid uppge både för och efternamn vid kundkontakt. Andra exempel är att använda centrala funktionsbrevlådor i större utsträckning och att personal i vissa roller har begränsad extern kundkontakt. Frågan om alias diskuteras, och det är viktigt att möjligheten att använda alias finns, men det bedöms sällan vara motiverat utifrån den faktiska hotbilden.

I rättsliga sammanhang kan rädslan för hot göra att medarbetare tvekar att representera banken. Polisanmälningar innebär ofta att den anställde blir målsägande och därmed offentligt exponerad. Bankerna försöker därför väga behovet av rättsliga åtgärder mot risken för ytterligare utsatthet, och erbjuder stöd vid eventuella rättegångar.

Att säkerställa en trygg arbetsmiljö för bankpersonal är inte bara ett ansvar för banken, utan en del av ett större samhällsåtagande för att motverka bedrägerier och penningtvätt.

Hot riktas främst mot de delar av banken som har kundkontakt.

En trygg arbetsmiljö för bankpersonal är inte bara bankernas ansvar utan en del av ett samhällsåtagande.

Särskilt allvarliga situationer – hot om självmord

Bankerna har noterat en kraftig ökning av hot om självmord från kunder under det senaste året. Dessa situationer är mycket svåra att hantera och upplevs som starkt belastande för den enskilde banktjänstemannen. Det finns särskilda processer och stödmaterial för hur medarbetare ska agera, exempelvis genom att uppmana kunden att ta kontakt med stödlinjer eller närstående. Vid uppfattad akut fara kan banken bryta banksekretessen och kontakta polis.

Behov av åtgärder från politik och myndigheter

- Bankerna efterfrågar förändringar som minskar exponeringen av enskilda medarbetare vid polisanmälningar och myndighetskontakter. Det bör vara möjligt för banken att göra en polisanmälan och stå som målsägande. Möjligheten att ha en centraliserad funktion, som kan företräda banken i rättsliga sammanhang exempelvis i bedrägeriärenden eller för att i domstol förklara hur exempelvis en betaltjänst fungerar, kan minska risken för personligt riktade hot och öka tryggheten för medarbetarna. Anmälaren skulle på så sätt bli neutraliserad, eftersom det är organisationens ställningstagande och inte den enskilde medarbetarens. Banken kan då också välja vilka personer som ska företräda banken och medarbetaren behöver inte känna sig utpekad utöver det hot denne tidigare har blivit utsatt för.

Förhöjd

Bedömningen är att hotbilden mot bankpersonal påverkas av bankernas åtgärder enligt penningtvättslagen och andra regulatoriska krav. Det är framför allt kundmötande funktioner som bär konsekvenserna av myndigheternas krav och samhällets utveckling.

2 Hotbilden från insiders och möjliggörare

Förekomsten av så kallade möjliggörare av brott gör sig kontinuerligt påmind och kräver vaksamhet och adekvata åtgärder. En möjliggörare av brott är i detta sammanhang en anställd på banken som genom sin yrkesroll gör något otillbörligt. Det kan vara för egen vinning, åt ett kriminellt nätverk eller åt en statlig aktör. Organiserad brottslighet och kriminella nätverk är den dimensionerande hotbilden vilket betyder att bankerna behöver anpassa resursfördelning och arbetsmetoder för att möta det.

Riskbeteenden och sårbarheter

Incitamenten för en extern fientlig aktör (antagonist) att plantera eller rekrytera en insider på en bank bedöms i allmänhet vara starka eftersom det ger större möjlighet till olika former av bedrägerier, penningtvättsupplägg, beslutspåverkan och tillgång till intern information. En insider kan antingen vara en aktiv möjliggörare, aktivt dela information eller ha en mer rådgivande eller coachande roll. Den anställde på banken kan även vara omedveten om att den används som insider.

Insidern själv är ofta en person med olika riskbeteenden och sårbarheter såsom drogmissbruk, spelmissbruk och/eller privatekonomiska problem. Men han eller hon kan även på annat sätt befinna sig i en utsatt situation genom släktskap eller vänskapsrelationer. Den typen av relation kan medföra att befattningsutövandet, som grundar sig i lämplighet, kan antas påverkas negativt. Även kopplingar till högrisländer eller kriminalitet kan förekomma. Ett annat incitament för illojalt beteende från en anställd är underliggande besvikelse på arbetsgivaren på grund av bristande uppskattning, utebliven befordran eller dålig löneutveckling.

Vissa tillvägagångssätt kräver en möjliggörare på insidan

Vissa tillvägagångssätt kan inte genomföras utan en möjliggörare på insidan. En anställd med kunskap om bankens produkter, tjänster, rutiner och processer, regelsättning vid kreditgivning och regler för transaktionsmonitorering är intressant för externa aktörer. Vid sidan av bankens egen kreditberedningsprocess skapar låneförmedlare, med fler parter i lånekedjan, olika typer av incitament till bedrägerier och penningtvättsupplägg för en insider.

Påtryckningar kan ta olika former

Det förekommer att externa fientliga aktörer söker kontakt med bankens personal för att bearbeta och 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. Antal kontakter med erbjudande om att genomföra betalda intervjuer, via exempelvis Linkedin, bedöms ha ökat de senaste åren.

Kriminella och andra fientliga aktörer annonserar också efter personer som är beredda att vara behjälpliga från insidan. Social manipulering smälter på så sätt ihop med den fysiska hotbilden genom att otillbörliga kontakter senare kan leda till fysiska hot mot anställda. Det kan handla om påtryckningar, hjälp med skulder, möjlighet att få ersättning för att lämna information eller att insidern upplever sig behövd. Det kan också handla om anställdas kontakter på krogen och olika former av missbruk som kan leda till utpressningssituationer. Det händer också att en

Hotaktörer och möjliggörare kan påverka beslut, informationsflöden och affärsstrategier i banken.

person med anknytning till en extern fientlig aktör söker anställning i bank i syfte att möjliggöra brott.

Bankerna efterfrågar tydligare regler

En fråga som aktualiseras är hur banken kan skydda medarbetare mot otillbörliga kontakter från exempelvis en statsaktör eller från organiserad brottslighet. Inom säkerhetsskyddslagstiftningen, som ofta träffar en avgränsad del av bankens verksamhet, finns instrument och större möjligheter att arbeta preventivt och att följa upp, men hotet finns i hela bredden av verksamheten, från bedrägerier till hur man rundar sanktioner. Bakgrundskontroller, som främst används vid anställningstillfället, ger inte samma möjligheter som en säkerhetsprövning gör.

Det är viktigt att bankerna har tillräckliga kontrollmöjligheter i samband med såväl anställningsförfarandet som under anställningstiden. Idag behöver bankerna till stor del förlita sig på den information som den arbetssökande själv lämnar. Sverige har också ett stort fokus på diskriminerings-, arbetsmiljö- och dataskyddslagstiftning som kan fungera motstridigt.

Bankerna efterfrågar tydligare lagar, regler och praxis om möjligheterna att göra löpande kontroller. Hur ska avvikelser som hittas under anställningens gång hanteras och hur ska man ställa sig till ärenden där det finns oegentligheter? Bankerna bör också ges möjlighet att dela information med varandra för att hindra att en insider efter upptäckt inte kan få anställning i en ny bank och där fortsätta sitt möjliggörande.

Den ökade rörligheten på arbetsmarknaden aktualiserar också frågan om det borde finnas någon form av meddelanderätt mellan banker för att hantera utmaningen med insiders.

Behov av information från brottsbekämpande myndigheter

Svårigheten med insiders är att det kan vara vem som helst. Bankerna hindras att upptäcka insiders och att vidta adekvata åtgärder eftersom de i många fall inte får tillräcklig information i rätt tid om brottsbekämpande myndigheter misstänker att en insider förekommer i en bank. Eftersom insiders ofta använder privata kommunikationsvägar för att olovligen sprida information och kommunicera med kriminella, är det brottsbekämpande myndigheter som har bäst förutsättningar att upptäcka aktiviteterna. Det är av vikt att myndigheter kan dela information till bankerna så att de kan vidta åtgärder.

Säkerhetspolisen har pekat ut att underrättelsehot kommer från i synnerhet Ryssland, Kina och Iran. Bankernas åtgärder för att hantera denna typ av hotbild sträcker sig från tekniska kontrollmöjligheter till att åtgärder vidtas för att medarbetare ska känna sig trygga med att kunna rapportera avvikande beteenden, med vetskapen att de inte upplevs som angivare.

Hotaktörer som nationalstater (Ryssland, Kina, Iran etc) och kriminella grupper har olika syften. Även om Polisen bedömer att hotet mot bankerna främst kommer från kriminella grupper och inte nationalstater, medför de identifierade kopplingarna mellan statsaktörer och kriminella nätverk i Sverige en väsentlig påverkan på insider-problematiken.

Bankernas egna kontrollmöjligheter

Bankernas interna kontrollmöjligheter är omfattande och består av in- och utpasseringsloggar, uppföljning av slagningar på kunder, behörigheter, dokumentationskrav med mera. Mest framgångsrikt är att korsbefrukta olika kontrollmiljöer. Anomalier i enskilda system och processer behöver inte betyda något, men när flera datapunkter slås samman kan bilden bli annorlunda.

För att kunna minska verksamhetens eller individers sårbarheter för risken att bli utnyttjad av kriminella aktörer, behöver flera avdelningar vara involverade i internutredningsprocessen. Det gäller även fall som rör misskötsamhet och regelöverträdelser.

Bedömningen är att insiders och möjliggörare är ett hot som finns internt i bankerna och som kommer att bestå under 2026.

3 Det säkerhetspolitiska läget, kontinuitet och civil beredskap

Sverige befinner sig i ett fortsatt besvärligt säkerhetspolitiskt läge. Rysslands anfallskrig mot Ukraina påverkar hotbilden mot den finansiella sektorn i Sverige.

Sabotage mot kritisk infrastruktur

Hotet mot kritisk infrastruktur som bankerna är beroende av består. Under 2025–2026 har hoten ytterligare förstärkts genom en rad incidenter som innefattar misstänkt sabotage mot telekommunikationsmaster, fiberoptiska kablar och annan digital infrastruktur. Utöver fysisk skadegörelse har det även rapporterats om GPS-störningar, särskilt i Östersjöområdet. Bedömningen är därför att hotet är fortsatt relevant för svenska banker. Hotbilden känns igen från rapporten i september 2025 från Försvarsmakten och dåvarande Myndigheten för samhällsskydd och beredskap, ”Utgångspunkter för totalförsvaret 2025 – 2030, Typsituation 1 – Hybrida hot”.

Svenska banker utgör idag en stor del av de baltiska ländernas finansiella infrastruktur, vilket också påverkar hotbilden. För några av bankerna är de tre baltiska länderna och Finland viktiga hemmamarknader. Hotbilden mot Baltikum och Finland känns igen i tidigare nämnd rapport ”Typsituation 6 – Förstärkning av alliansens norra flank” som innebär att svenska förband förstärker Natos norra flank i Finland i syfte att försvara alliansens territorium. Det samma gäller ”Typsituation 7 – Förstärkning av alliansen i Baltikumområdet” som anger en väpnad konflikt i området där svenska förband förstärker Nato i och omkring de baltiska länderna.

De svenska bankerna behöver ha fortsatt fokus på att se över sina beroenden till kritisk infrastruktur. De måste planera för att kunna öka sina resurser och sin kapacitet, exempelvis elektronisk kommunikation och elförsörjning. Det gäller oavsett om misstänkta sabotage är fientliga handlingar eller inte. Hot och sårbarheter i kritisk finansiell infrastruktur kan också vara svåra att överblicka för den enskilda banken då finansiell sektor på global nivå är starkt integrerad och sammankopplad på operativ- och teknisk nivå.

Beroendet av utländska it-leverantörer

Beroendet av utländska leverantörer av it-tjänster är omfattande i den finansiella sektorn. Nu lyfts dock frågor om digital suveränitet högre på agendan både nationellt och på EU-nivå. Svenska banker använder i hög grad amerikanska it-leverantörer och amerikansk betalningsinfrastruktur, vilket länge har bidragit till en stabil och förutsägbar grund. Bankerna behöver dock beakta hur en förändrad amerikansk utrikespolitik skulle kunna påverka tillgången till

De svenska bankerna behöver ha fortsatt fokus på att se över sina beroenden av kritisk infrastruktur.

dessa tjänster, direkt eller indirekt. Även om några omedelbara hot inte kan konstateras är det rimligt att inkludera den dimensionen i bankernas strategiska riskarbete, särskilt mot bakgrund av att amerikanska politiska prioriteringar i nuläget tenderar att skifta relativt snabbt. Bankerna behöver kontinuerligt följa och utvärdera riskerna med att förlita sig på utländska leverantörer för verksamhetskritiska tjänster.

Bankernas beredskaps- och kontinuitetsarbete

Beredskapsarbetet kopplat till civilt försvar har nu adderats till bankernas arbete med kontinuitet, krishantering och säkerhet. Då ett väpnat angrepp mot Sverige används som utgångspunkt för kontinuitetsplaneringen ställs kraven på verksamheten avsevärt högre än vid kriser i fredstid. Då behöver verksamheten kunna hantera frågor som flytt av data och kritiska funktioner, omfattande reservlösningar samt skydd av viktiga fysiska anläggningar som kontor och datahallar. Även etablering och bemanning av en krigsorganisation blir nödvändig i ett sådant scenario.

Bankföreningen har under de senaste åren efterlyst tydligare koordinering och planering mellan sektorns myndigheter, samt tydliga planeringsförutsättningar och vägledning om hur beredskapsarbetet ska prioriteras. Under 2025 har Finansinspektionen publicerat en planeringsinriktning, som är avsedd att komplettera och konkretisera de planeringsförutsättningar som gäller för hela det civila försvaret, till de specifika förhållandena i den finansiella sektorn. En ny struktur för privat-offentlig samverkan kring beredskapsfrågor inom den finansiella sektorn har också utvecklats. Den nya samverkan, med namnet FTPOS (Finansiella Tjänster Privat-Offentlig Samverkan, före detta FSPOS) ska möjliggöra en mer ändamålsenlig och skyndsam utveckling av den finansiella sektorns beredskapsförmåga.

Krigsorganisation, kompetens och personalresurser

Uppbyggnad och expandering av bankernas kompetens och personalresurser på området sker över tid. Samtidigt kan det vara utmanande för bankerna att planera för rätt kompetens och bemanning vid höjd beredskap eller ytterst krig. Det finns dels en begränsad tillgång till personal med både finansiell expertis och kunskap om totalförsvar, dels kan många kritiska funktioner i bankerna vara starkt specialiserade, vilket skulle kunna skapa sårbarheter vid frånvaro eller mobilisering. Bankerna behöver säkerställa att bemanningen klarar belastningstoppar, störningar i infrastruktur och geografisk spridning eller parallella kris- eller krigsscenarier. Det är dock redan i fredstid en utmaning för bankerna att få tillgång till viss nyckelkompetens inom säkerhet, it och beredskap, till följd av hög konkurrens om kvalificerad personal och begränsad tillgång på specialistkompetens.

Det råder betydande osäkerhet kring vilken befogenhet en beredskapsmyndighet har att identifiera en specifik verksamhet och därmed möjliggöra bankernas disponibilitetskontroller av personal hos Plikt- och prövningsverket. Finansinspektionen, som är sektorsansvarig myndighet för beredskapssektorn Finansiella tjänster, har i ett rättsutlåtande meddelat att de anser att ett sådant identifierande är ett myndighetsbeslut som de saknar rättsligt mandat för. Det medför att banker som har behov av att säkra personal till krigsorganisationen för finansiella samhällsviktiga tjänster utanför betalningsområdet, i nuläget inte har möjlighet att göra det, vilket försenar företagens etablering av en krigsorganisation. Som kontrast fungerar nuvarande rutiner för disponibilitetskontroll och ianspråktagande av personal bra för de finansiella företag som omfattas av Riksbankens föreskrifter om betalningar under fredstida krissituationer och vid höjd beredskap.

Fragmenterade beredskapsramverk och krav i Norden

Banker som verkar i flera nordiska länder och Baltikum möter utmaningar när varje land utvecklar egna ramverk och krav för civilt försvar. Skillnader i lagstiftning, förväntningar, styrning och planering gör att banker måste anpassa sina planer parallellt i flera jurisdiktioner, vilket ökar komplexiteten och kostnaderna. Det kan leda till målkonflikter när en lösning som uppfyller kraven i ett land inte är tillräcklig eller ens möjlig i ett annat. Det försvårar utvecklingen av en sammanhållen och effektiv beredskapsstruktur för hela koncernen.

Beredskapsarbetet kopplat till civilt försvar har nu adderats till bankernas arbete med kontinuitet, krishantering och säkerhet.

Behov av åtgärder från politik och myndigheter

- Det är viktigt att planering och koordinering mellan Finansinspektionen, Riksbanken och Riksgälden kommer på plats under 2026.
- Inför snarast förslagen i utredningen ”En ny funktion för krishantering vid allvarliga driftstörningar i den finansiella sektorns digitala infrastruktur” där Riksbanken ges uppdrag att etablera funktionen. Bankföreningen ser mycket positivt på att regeringen under våren 2026 lämnat en proposition om krishanteringsfunktionen till riksdagen. Då Riksbanken, Finansinspektionen och Riksgälden ska samverka i funktionen är det viktigt att funktionens styrning blir tydlig och inte överlappar med arbetet inom beredskapssektorn Finansiella tjänster.
- Inför förslagen från IVA:s projekt Resilient Digital Infrastruktur (Bankföreningen har deltagit och sponsrat projektet) från 2025 som identifierat konkreta åtgärder för att stärka Sveriges digitala motståndskraft. Några relevanta exempel från projektet som även skulle stärka bankernas motståndskraft:
  - Post- och telestyrelsen får mandat att samordna och samla in övervakningsdata från fiberägare och andra relevanta aktörer. Data från fiberövervakning ska integreras i nationella lägesbilder, vilket möjliggör snabbare och mer precis respons vid incidenter, och kan bidra till att förebygga incidenter.
  - Utbyggnad av elnätet ska fortsätta för att minimera risk för elavbrott.
  - Försvarsmakten tillsammans med teleoperatörerna tar fram en lösning för internationell roaming vid förlust av digital kontakt med andra länder.

  För att lyckas med denna typ av sektorsöverskridande förslag är det viktigt att sektorsansvariga myndigheter gemensamt koordinerar förmågehöjande insatser av svensk infrastruktur. Finansiella företag är beroende av andra sektorer såsom elektronisk kommunikation och elförsörjning för att få det finansiella systemet att fungera även i kris och ytterst krig. Det behövs en strukturerad dialog med närliggande sektorer om ömsesidiga beroenden och hur samhällsviktig finansiell verksamhet ska prioriteras vid resursbrist. Gemensamma prioriteringsprinciper och en delad lägesbild är avgörande för att undvika målkonflikter och säkerställa att kritiska finansiella funktioner kan upprätthållas.
- Inför åtgärder som möjliggör bankernas disponibilitetskontroller av relevant personal som arbetar med samhällsviktiga finansiella tjänster.
- Öka samordningen av nordiska och baltiska regelverk och krav för civilt försvar för privata verksamhetsutövare. Genom att enas om gemensamma nordiska principer, grundkrav och planeringsantaganden kan bättre förutsättningar skapas för effektiv beredskapsplanering för företag med verksamhet i hela eller delar av området, utan att ge avkall på nationellt ansvar eller säkerhetspolitiska behov. Nationella särkrav bör vara tydligt motiverade, proportionerliga och koordinerade. En sådan inriktning skulle stärka motståndskraften, minska de administrativa bördorna för privata verksamhetsutövare och bidra till ett mer robust och sammanhållet civilt försvar i Norden och Baltikum.
- Regeringen bör ta ett samlat nationellt grepp om Sveriges beroende av utländska it-tjänster, då frågan rör grundläggande kontinuitet i samhällsviktig verksamhet. Beroendena sträcker sig långt bortom banksektorn och berör hela samhällets funktionalitet, vilket motiverar tydliga signaler från myndighetshåll om frågans strategiska betydelse. Ett sådant grepp bör ta sin utgångspunkt i kontinuitets- och motståndskraftsperspektivet snarare än i enskilda leverantörer eller länder.

Bedömningen är att Sveriges säkerhetspolitiska läge och den försämrade hotbilden påverkar bankerna. Eftersom den framtida utvecklingen är svårbedömd både på kort och lång sikt behöver bankerna kontinuerligt övervaka och utvärdera hur läget påverkar hotbilden i den egna verksamheten. Oavsett utkomst av Rysslands krig i Ukraina kommer hybridhoten inte att försvinna och bankerna måste fortsätta fokusera på förmågeuppbyggnad och motståndskraft. Bankföreningen gör bedömningen att det nu finns bättre förutsättningar för ett effektivt beredskapsarbete i sektorn i och med de förbättringar som har genomförts.

4 Informationssäkerhets- och cybersäkerhetshot

Ett skifte i cyberutpressningshotet – informationsstöld, falska hot och leverantörsrisker

Under perioden har olika typer av cyber-utpressnings-angrepp fortsatt drabba ett stort antal verksamheter. Tidigare har ransomware-angrepp varit det vanligaste sättet där den som angrips får data i sina it-system krypterade. Utvecklingen visar att data inte bara krypteras vid angrepp utan data stjäls också, och aktörerna hotar med att lägga ut informationen publikt på internet om inte en lösensumma betalas. Det förekommer även utpressning med mer eller mindre trovärdig falsk information. Hotaktörer ger sken av att ha stulit data och hotar sina offer. Konsekvensen blir att resurser likväl måste läggas på att utreda händelserna.

Informationsstöld är för flera av de mest aktiva hotaktörerna förstahandsvalet. Att stjäla information går snabbare och kan göras mer dolt. Fler offer kan också attackeras på kort tid med större chans att lyckas. Att inte kryptera data ger ingen omedelbar operativ störning eller samhällspåverkan och händelsen ges då troligen inte lika stort polisiärt fokus. Det sker också en utveckling där små- och medelstora företag i större utsträckning drabbas jämfört med stora företag. Små- och medelstora företag förefaller ha en större benägenhet att betala lösensummor.

Hundratals företag faller offer för cyberangrepp varje månad. Jämfört med många andra sektorer har finansiella företag i västvärlden ofta en relativt hög nivå av cybersäkerhet. Då majoriteten kriminella hotaktörer är opportunistiska, det vill säga söker sig dit där hindren är lägst, blir dessa aktörer inte förstahandsvalet. De uppenbara sårbarheterna finns hos andra företag i andra sektorer. Samtidigt ingår de företag som drabbas i det digitala ekosystem som är viktigt även för finansiella företag.

Under 2025 ökade antalet totala offer globalt, något som kunnat observeras på webbplatser som publicerar information om cyberutpressnings-angrepp. En del av dessa offer är leverantörer till banker, och en del av dem har blivit betrodda att hantera bankernas data. På så sätt skapas en hävstångseffekt eftersom kunderna till leverantörer också drabbas. Leverantörers sårbarhet utgör därför en central risk för finansiella företag, då dessa ofta hanterar känslig information, såsom kunddata och transaktionsuppgifter, på uppdrag av bankerna. En cyberattack mot en leverantör kan därmed indirekt hota både bankernas säkerhet och kundernas integritet. Det finns dock inget som tyder på att leverantörerna har attackerats på grund av att de har banker som kunder.

Under senare år har en ny kategori cyberkriminella hotaktörer blivit alltmer synlig i Europa, bestående av västbaserade kriminella nätverk som inte ingår i det traditionella ryskspråkiga cyberkriminella ekosystemet. Denna typ av hot har tidigare främst observerats i USA, där flera uppmärksammade intrång med betydande affärspåverkan riktats mot stora företag, bland annat inom spel och kasinosektorn. Under det senaste året har motsvarande hot även riktats mot företag i Europa. Flera incidenter i Storbritannien visar tydligt på fenomenet med västbaserade kriminella aktörer som genomfört intrång med stor operativ och ekonomisk påverkan.

Parallellt har storskalig exploatering av sårbarheter i molnbaserade affärsplattformar, såsom Salesforce miljöer, observerats. Sårbarheterna har möjliggjort angrepp mot ett stort antal organisationer under kort tid. För svenska banker innebär utvecklingen att hotbilden breddas ytterligare. Hotet från västbaserade cyberkriminella aktörer bör beaktas som ett tilltagande riskområde.

Bankerna bör löpande bevaka och utvärdera cyberutpressnings-hotet och se över sina skyddsåtgärder. Om en attack skulle ske måste banken ha utvecklat åtgärder för att kunna upptäcka och hantera den, samt återställa verksamheten. Ett omfattande angrepp med cyberutpressning mot finansiell sektor skulle kunna få mycket stor påverkan. Studier och analyser från Internationella valutafonden (IMF), Europeiska systemrisknämnden (ESRB) och Riksbanken visar att en cyberattack mot finansiell sektor där samman-

kopplingen och koncentrationen av de aktörer som drabbas är tillräckligt omfattande, skulle kunna hota den finansiella stabiliteten.

Hot i digitala leveranskedjor

Bankerna är i hög grad beroende av it leverantörer, molntjänster och allmänt tillgänglig mjukvara i sin verksamhet. Hoten mot dessa digitala leveranskedjor har blivit fler över tid, dels till följd av ett större nyttjande av externa leverantörer, dels genom en ökande mängd cyberangrepp riktade mot leverantörerna. För finansiella företag är det i dag en realitet att leverantörer och samarbetspartners drabbas av dataintrång och cyberangrepp. Användningen av exempelvis Software as a Service bidrar till att bankernas attackyta expanderar utanför den egna direkta kontrollen.

Några exempel:

- Under 2025 har flera amerikanska banker, inklusive systemviktiga institut, drabbats av förlust av data eller exponering av kunddata till följd av intrång och brister hos tredjepartsleverantörer. Händelserna har i flera fall haft sitt ursprung hos specialiserade leverantörer som hanterar stora mängder kundinformation för många banker samtidigt, vilket tydliggör den strukturella riskexponering som följer av tredjepartsberoenden.
- I november 2025 drabbades den amerikanska finans- och fastighetstekniklevarantören SitusAMC av ett dataintrång. Företaget hanterar stora mängder känslig information åt banker, bland annat dokumentation kopplad till lån och inteckningar. Enligt rapportering uppmärksammades flera stora amerikanska banker om att kundrelaterad data kunde ha stulits från leverantörens system.
- Under 2025 utsattes Marquis Software Solutions, en leverantör av CRM-, marknads- och regelefterlevnadssystem för banker, för ett dataintrång. Angreppet ledde till att kunddata från minst 74 amerikanska banker och kreditinstitut exponerades och inkluderade uppgifter såsom namn, personnummer, kontouppgifter och annan känslig information. Enligt incidentrapporteringen berördes över 400 000 bankkunder, trots att bankernas egna IT-miljöer inte påverkades.

Zero-day-sårbarheter är sårbarheter som upptäcks av hotaktörer som sedan omedelbart använder dem för att angripa system innan de hunnit åtgärdas. Denna typ av sårbarheter fortsätter att vara ett påtagligt hot mot bankerna och visar inga tecken på att minska. Sårbarheterna utgör en betydande utmaning för bankerna eftersom de möjliggör angrepp där försvarsmekanismer saknas. Det är inte bara sårbarheter som utnyttjas, utan även fel i teknisk konfiguration och social manipulering av bankernas anställda.

Även händelser och incidenter där det inte finns en hotaktör i bakgrunden behöver beaktas i bankernas cybersäkerhetsarbete. Under 2025 drabbades stora it-leverantörer som Cloudflare, Amazon Web Services, Google Could och Microsoft Azure av incidenter vilket medförde längre störningar och avbrott i tjänsteleveranser. Incidenterna påverkade många branscher och tjänster globalt, vilket visar på de koncentrationsrisker som byggs upp när flera kunder nyttjar samma it-lösning.

Hotbilden innebär att tredjepartsrisker inte längre kan behandlas som en sekundär risk eller som huvudsakligen en avtalsfråga. Regelverk som DORA ställer krav på att banker systematiskt ska identifiera, klassificera och följa upp risker kopplade till sina IKT leverantörer. Utvecklingen driver en mer kontinuerlig och riskbaserad styrning av leverantörsrelationer, med krav på robusta avtal, incidentrapportering, tester av motståndskraft samt fungerande exit och substitutionsplaner. Sammantaget innebär det att angrepp mot leverantörer i högre grad måste vägas in i bankernas egen operativa risk- och hotbild, snarare än betraktas som externa avvikelser.

Destruktiva cyberangrepp mot samhällsviktig infrastruktur

Ryssland har under anfallskriget mot Ukraina vid upprepade tillfällen använt sig av destruktiv skadlig kod, så kallad wiper malware, i syfte att förstöra system och data i samhällsviktig infrastruktur. Ukraina har hittills varit framgångsrikt i att försvara sig mot dessa angrepp. Angrepp med wiper malware riskerar att sprida sig till andra aktörer och geografier än den tänkta träffytan. Denna typ av okontrollerad spridning har inte observerats mot svenska banker under det senaste året.

Bankerna behöver löpande bevaka och utvärdera cyberutpressningshotet och se över sina skyddsåtgärder.

Samtidigt visar det angrepp som riktades mot det polska energisystemet i slutet av december 2025 att hotet mot samhällsviktig infrastruktur i Europa är reellt, och att destruktiv skadlig kod fortsatt används som ett verktyg i statliga cyberoperationer. Angreppet, som bedöms ha haft ett destruktivt syfte, riktades mot energiproduktion och distributionsnära system och använde wiper malware i ett försök att slå ut eldistributionen. Även om angreppet inte ledde till faktiska avbrott, visar det att hotaktörer har både vilja och förmåga att genomföra denna typ av operationer även utanför Ukraina.

För finanssektorn innebär denna typ av angrepp en indirekt men betydande risk, då bankernas verksamhet är starkt beroende av fungerande elförsörjning och tillförlitliga kommunikationsnät. Ett lyckat angrepp med wiper malware mot energi- eller kommunikationsinfrastruktur skulle kunna leda till omfattande störningar i betalningssystem och tillgänglighet till digitala tjänster. I förlängningen skulle det påverka förtroendet för det finansiella systemet, även utan att bankerna själva är direkt angripna.

Mot denna bakgrund bör hotet från wiper malware inte förringas. Risken för direkta angrepp mot banker eller indirekt spridning via andra sektorer bedöms fortsatt som låg, men konsekvenserna av ett lyckat angrepp skulle vara omfattande. Vid ett snabbt försämrat säkerhetsläge i Europa kan hotet aktualiseras, och det finns därför goda skäl för bankerna att fortsatt bevaka utvecklingen och inkludera scenarier med destruktiv skadlig kod i sina risk- och beredskapsbedömningar. Ytterst skulle ett omfattande wiper malware-angrepp mot finansiell sektor i Sverige kunna få systemhotande påverkan.

Identiteter under angrepp

En infostealer är en typ av skadlig programvara som är utformad för att stjäla känslig information från it-system. Infostealers är inte längre ett hot i sig själv, utan ett av verktygen hotaktörer använder för att komma åt identiteter och inloggningsuppgifter. Infostealers används ofta av hotaktörer för att utföra ytterligare brottsliga aktiviteter som bedrägerier och utpressning.

I dagens it-miljöer, där molntjänster ofta ingår, förändras system och teknik ofta. Det som däremot består över tid är användarnas konton och inloggningsuppgifter. Därför hamnar nu identiteter i centrum för de hotaktörer som vill angripa exempelvis banker. Det är helt enkelt ofta lättare att logga in med stulna uppgifter än att ta sig in genom att angripa systemen direkt.

Skadlig kod eller länkar till skadlig kod via e-post till medarbetare i bankerna är ett vanligt förekommande hot. Även spear phishing förekommer, det vill säga nätfiske som riktar sig mot utvalda personer hos bankerna. Spear phishing har bland annat riktats mot medarbetare i bankerna som kan tänkas ha högre it-behörigheter. LinkedIn har använts för att kartlägga bankernas it-medarbetare, som sedan har fått falska jobberbjudanden med länkar till skadlig kod.

Syftet med denna typ av spear phishing är troligen att hotaktörerna ser detta som ett snabbt sätt att få fotfäste i bankernas infrastruktur. Samtidigt är det fortfarande vanligt förekommande med phishing, nätfiske, som inte riktar sig mot utvalda personer utan som är av mer opportunistisk, slumpmässig karaktär. Phishing mot it-leverantörers personal, som ett sätt att potentiellt sätt attackera bankerna, förekommer också.

En viktig grund för att hantera hotbilden är bankernas etablerade säkerhetshygien, systematiska arbetssätt och välutvecklade samverkan.

Vishing mot bankernas personal förekommer också, det vill säga hotaktörer som använder telefonsamtal eller röstmeddelanden för att lura bankpersonal att lämna ut känslig information, såsom inloggningsuppgifter. Syftet med vishingangrepp mot bankens personal kan inledningsvis vara svåra analysera.

Bedömningen är att angrepp som riktar sig mot användares konton och inloggningar har ökat och fortsätter att öka. Det handlar inte längre bara om stulna lösenord, utan i allt större utsträckning om att angripare kapar pågående inloggningar och sessioner. Det gäller både molnbaserade system och system som driftas internt. Att skydda användarnas identiteter har därför blivit en av de viktigaste säkerhetsfrågorna för bankerna. Övningar och utbildning för att personalen ska kunna upptäcka phishing-mejl och vishing-samtal samt bankens tekniska lösningar för att blockera phishing-mejl är fortsatt viktiga motåtgärder.

Överbelastningsangrepp – ett avtagande men inte avskrivet hot

Överbelastningsangrepp, som påverkar finansiella internettjänsters tillgänglighet, har varit ett av de vanligaste inslagen för att skada förtroendet för finansiella tjänster och finansiella företag. Under 2025 har den faktiska påverkan från överbelastningsangrepp minskat, vilket bland annat är ett resultat av att finansiella företag stärkt sina förmågor, skydd och anpassningsbarhet. Bankerna har även noterat minskade nivåer av angrepp efter sommaren 2025.

En annan bidragande faktor bedöms vara det tidigare mycket aktiva Gorilla-botnätet, som använts för storskaliga överbelastningsangrepp mot bland annat banker. Botnätet förefaller ha blivit nedtaget eller kraftigt begränsat efter att dess centrala infrastruktur och tillhörande kommunikationskanaler identifierats och stängts ned.

Överbelastningsangrepp är dock ett hot som kvarstår för bankerna att bevaka eftersom hotaktörer fortsatt har förmågan att anpassa och genomföra angrepp. Det primära syftet med angreppen är att underminera förtroendet för finansiell samhällsviktig verksamhet.

Riskexponeringen för överbelastningsangrepp växer också i takt med den tilltagande digitaliseringen. Angreppen kan även drabba leverantörer och då riskera att påverka finansiella aktörer. Bankerna behöver ställa krav på sina leverantörer att de säkrar sina system mot angrepp.

Generativ AI som ny dimension i bankernas hotbild

I takt med den snabba framväxten och tillgängligheten av AI baserade tjänster ökar risken för informationsläckage för bankerna, särskilt i de fall anställda använder externa AI tjänster på ett sätt som inte är förenligt med interna regelverk. Om känslig information, kunddata, interna analyser, affärslogik eller operativa uppgifter matas in i publika eller otillräckligt kontrollerade AI tjänster finns en risk att data lämnar bankens kontroll. I praktiken blir den då tillgänglig för tredjepart, antingen genom lagring, vidareträning av modeller eller genom bristande tekniska och organisatoriska skyddsåtgärder hos tjänsteleverantören. Dataöverföring till externa AI plattformar utgör en ny och i många fall underskattad informationssäkerhetsrisk inom finanssektorn.

Samtidigt har marknaden för AI tjänster fragmenterats kraftigt. En stor mångfald av generativa AI verktyg, assistenter och specialiserade applikationer har etablerats på kort tid. Ofta har det skett utan att tjänsterna genomgått samma mognads , säkerhets och regelefterlevnadsprocesser som traditionella it tjänster.

Utöver risken för informationsläckage tillför generativ AI även nya risker kopplade till hur användare tolkar och använder AI genererad output. AI tjänster kan producera svar som uppfattas som trovärdiga men som är ofullständiga, missvisande eller direkt felaktiga, så kallade hallucinationer. Om AI output används utan tillräcklig mänsklig granskning och kontextförståelse kan det leda till att bedömningar, analyser och rekommendationer blir felaktiga. Det kan påverka kreditbedömningar, riskanalyser, regelefterlevnad och strategiskt beslutsfattande.

Utvecklingen av generativ AI har sänkt trösklarna för att utveckla och anpassa skadlig kod, vilket innebär att fler hotaktörer än tidigare kan genomföra tekniskt avancerade cyberangrepp mot banker. AI används för att snabbt ta fram och anpassa skadlig kod till specifika mål. Detta leder till att tiden från angrepp till skada blir kortare. Särskilt allvarligt är framväxten av AI-stödd dynamisk skadlig kod som kan ändra sitt beteende under pågående angrepp, vilket försvårar upptäckt och incidenthantering.

Sammantaget innebär det att cyberhoten mot bankerna blir mer snabbrörliga, svårupptäckta och skalbara, med potentiellt större konsekvenser även vid enskilda säkerhetsbrister. För bankerna ökar därmed behovet av att tidigt kunna upptäcka intrång och ett ökat fokus på motståndskraft snarare än enbart förebyggande skydd.

Generativ AI sänker även trösklarna för att producera och sprida desinformation i stor skala, eftersom det möjliggör snabb framställning av trovärdigt formulerade texter och bilder. Narrativen kan anpassas till specifika målgrupper och händelser. Desinformationskampanjer kan användas för att påverka opinionen, skapa osäkerhet eller förstärka oro kring påstådda incidenter i finansiell sektor. Det kan i sin tur bidra till att skada och underminera förtroendet för banker och finansiella tjänster, med potentiella följdeffekter för den finansiella stabiliteten.

Bankerna har dock goda förutsättningar att hantera även dessa nya risker genom att bygga vidare på sitt etablerade systematiska säkerhetsarbete. Det arbetet behöver omfatta inte bara utveckling och införande av AI lösningar, utan även förmågan att förebygga, upptäcka och hantera cyberangrepp där AI används som ett verktyg av hotaktörer. Genom att tidigt integrera informationssäkerhet, regelefterlevnad och riskhantering skapas förutsättningar för att använda AI på ett kontrollerat och värdeskapande sätt samtidigt som den operativa motståndskraften stärks.

Utvecklingen av kvantdatorer – ett långsiktigt kryptografiskt skifte

Utvecklingen av kvantdatorer innebär på sikt ett hot mot dagens kryptering som används för att skydda kommunikation, identiteter och data i bankernas system. Orsaken är att tillräckligt kraftfulla kvantdatorer kan lösa vissa matematiska problem mycket snabbare än klassiska datorer, vilket undergräver säkerheten.

Även om praktiskt användbara kvantdatorer inte bedöms finnas inom en nära framtid, finns en risk att information som krypteras i dag kan lagras och dekrypteras av hotaktörer i framtiden, vilket gör frågan relevant ur ett långsiktigt konfidentialitets- och kontinuitetsperspektiv. För bankerna skulle övergången till kvantumsäkra kryptografiska lösningar kunna innebära omfattande omställningskostnader, då kryptografi är djupt integrerad i system, applikationer, kommunikation med kunder samt beroenden till leverantörer och gemensam infrastruktur.

Arbetet kräver därför god framförhållning, inventering av hur och var bankerna använder kryptografiska system och samordning med leverantörer. Samtidigt ger bankernas etablerade systematik inom säkerhet och förändringshantering goda förutsättningar att successivt och kontrollerat hantera detta teknologiska skifte.

Behov av åtgärder från politik och myndigheter

- Riksbanken bör få i uppdrag att definiera tydliga roller och ansvar för funktionen för krishantering. Riksbanken bör också definiera hur funktionen tillsammans med Nationellt cybersäkerhetscenter, CERT-SE och Försvarets Radioanstalt, FRA, ska krishantera och stötta vid cyberangrepp mot samhällsviktig finansiell verksamhet.
- Inför det nya brottet datastörning i brottsbalken. Överbelastningsangrepp omfattas idag av brottet dataintrång, trots att något intrång i ett visst datasystem inte skett. Vad det i själva verket är fråga om är en tillfällig störning av tillgången till datasystemet, men inte dess innehåll.

Bedömningen är att hotbilden inom informations- och cybersäkerhetsområdet är förhöjd och att den påverkas av kriminella grupper och statsstödda hotaktörer. Cyberutpressning vidareutvecklas från kryptering av data mot datastölder som är både enklare och snabbare att genomföra. Riskerna i digitala leveranskedjor förändras som en följd av ökat nyttjande av leverantörer och ett större antal cyberangrepp mot leverantörerna. Inom cyberområdet kan hotbilden också påverkas av en hotaktör med uthållig förmåga och vilja, som ser ett tillfälle kopplat till den säkerhetspolitiska utvecklingen. Under perioden märks dock en minskning av antalet överbelastningsangrepp. En viktig grund för att hantera hotbilden är bankernas etablerade säkerhetshygien, systematiska arbetssätt och välutvecklade samverkan både inom sektorn och med relevanta myndigheter. Denna struktur och mognad utgör en stabil bas för ett effektivt och långsiktigt säkerhetsarbete även i en föränderlig hotmiljö.

5 Bedrägerier och finansiell brottslighet

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

2025 anmäldes 229 161 bedrägeribrott i Sverige, enligt Polisen. Det är en ökning med 1 727 brott, eller 1 procent, jämfört med 2024.

Fler bedrägeriförsök men mindre brottsvinster

Brottsvinster för bedrägerier uppskattas enligt Polisen vara cirka 4,2 miljarder kronor år 2020, 4,6 miljarder kronor år 2021, 5,8 miljarder kronor år 2022, 7,5 miljarder kronor år 2023, 6,3 miljarder kronor år 2024 och 5,7 miljarder kronor år 2025.

Ökningen av brottsvinster för bedrägerier fram till trendbrottet 2024, kan till stor del förklaras av att bedrägerier med inslag av social manipulering har ökat markant. Som exempel var antalet polisanmälda vishingbedrägerier, det vill säga telefonbedrägerier, 5 285 år 2019, medan det år 2025 var uppe på 32 844.

Även om antalet polisanmälda telefonbedrägerier i stort sett legat på samma nivå de senaste två åren har brottsvinsterna från dem minskat med cirka 60 procent 2025 i jämförelse med 2023. Snittförlusten (brottsvinsten) för ett telefonbedrägeri var 2025 den lägsta sedan 2017 (då mätningar av modus började).

Enligt Polisen är förklaringen till minskningen i huvudsak bankernas åtgärdsprogram mot bedrägerier som lanserades i maj 2024. Bedrägeribrottsligheten har dock utvecklats till att bli väldigt flexibel och anpassningsbar. En konsekvens av det är att tillvägagångssätten utvecklas och breddas samtidigt som gruppen brottsoffer breddas, exempelvis mot yngre.

Nya produkter och tredjepartsleverantörer

En av utmaningarna i arbetet med att motverka bedrägerier är att tjänsteutveckling och digitalisering går väldigt fort, vilket innebär att hotbilden förändras snabbt. Snabbheten kräver i sin tur ett realtidsskydd avseende informationsdelning. Det uppstår även ett behov av att dela tekniska uppgifter. Bankerna tar ned falska hemsidor på löpande band, vilket kräver kompetens och resurser. Banken behöver 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 kunderna förväntar sig att banken erbjuder nya produkter och tjänster i takt med den tekniska utvecklingen. Alla aktörer i betalningskedjan 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 vilket skapar risker.

Andra aktörer får tillgång till bankernas information

Sedan 2023 finns ett lagförslag från EU att gå från open banking till open finance genom regelverk för Financial Data Access (FiDA), som blir direkt tillämplig i Sverige. Det politiska målet är att förbättra och skräddarsy finansiella produkter och tjänster för kunder, samt skapa ökad konkurrens inom finanssektorn. Förslaget kan öppna bankernas infrastruktur för fler aktörer inom olika finansiella tjänster utöver betalningar och kontoinformation.

Open finance låter fler finansiella aktörer få tillgång till och möjlighet att dela en stor mängd finansiell data. Det innebär att fler av bankens kunduppgifter ska få användas av tredje part, alltså inte bara för betalningar utan även för bolån, lån, sparande, pensioner och försäkringar.

Risker som lyfts rör bland annat cybersäkerhet, bedrägerier och finansiell brottslighet. Viktiga frågor är därför kundernas kunskap och medvetenhet om hur produkter och tjänster fungerar, men också hur data lagras, används och distribueras. Lika viktigt är att det ställs samma krav på samtliga aktörer i ekosystemet.

Nya regler för betaltjänster

Ett annat lagförslag som kommer att träda i kraft under 2026 är EU-kommissionens förslag om ändringar i regelverket för betaltjänster. Det kommer att utmynna i en betaltjänstförordning, Payment Service Regulation (PSR), som blir direkt tillämplig i Sverige. Lagförslaget innehåller såväl förslag för att motverka bedrägerier, som förslag om ökat konsumentskydd där banken föreslås få ett ökat ansvar för återbetalning till kunderna i vissa bedrägerisituationer.

Den nya betaltjänstförordningen innehåller ett omfattande paket av åtgärder för att motverka bedrägerier. Åtgärderna inkluderar bland annat förbättrad informationsdelning mellan olika aktörer, möjligheten för banker att stoppa transaktioner som misstänks vara bedrägliga, införandet av utgiftstak samt en så kallad ångerperiod för kunder i de fall där utgiftstaket har höjts. Det är mycket positivt att betaltjänstförordningen tydligt visar politiska ambitioner att bekämpa bedrägerier. Samtidigt är det avgörande att de nya reglerna både stärker konsumentskyddet och ger bankerna rätt verktyg för att effektivt kunna motverka bedrägerier.

Nya regler för realtidsbetalningar

Ytterligare förslag från EU är att betalningar ska gå snabbare. Under 2024 trädde nya regler i kraft för betalningar i euro. De innebär krav på betaltjänstleverantörer att erbjuda sina kunder realtidsbetalningar i samma kanaler där de erbjuds vanliga kontoöverföringar i euro. Med kanaler avses framför allt internetbank, mobilbank och telefonbank. Realtidsbetalningar har ett antal utmaningar vad gäller bedrägerier och ekonomisk brottslighet.

Utmaningarna kommer att växa om omedelbara betalningar blir ett tillgängligt alternativ vid fler typer av betalningar. För att balansera utmaningarna och begränsa risken för en ökning av antalet bedrägerier behöver bankerna justera befintliga system och hitta nya arbetsmetoder för att upptäcka och stoppa bedrägerier, samtidigt som kundernas medvetandegrad om riskerna med realtidsbetalningar måste höjas.

Ökad rapporteringsskyldighet för clearingbolag

I början av 2025 presenterade regeringen en proposition om åtgärder mot missbruk av betalningssystemet, där rapporteringsskyldighet för clearingbolagen utgör en central del. Bankföreningen har därför, tillsammans med banker och clearingbolag, tagit fram ett koncept som möjliggör monitorering av transaktioner på clearingnivå. Clearingbolag har en överblick av betalsystemet som ingen enskild bank kan ha. Detta är ett viktigt steg för att stärka förmågan att mer effektivt kunna motverka bedrägerier och penningtvätt samt minska sårbarheten i betalningssystemet.

Hotbilden förändras

Historiskt sett har bankerna haft förmåga att parera bedrägeribrott, men digitaliseringen i samhället 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 social manipulering.

Som en konsekvens av förändringarna har brottsligheten drivits mot tillvägagångssätt med större inslag av social manipulering, som exempelvis telefonbedrägerier. Antingen luras kunden att lämna ifrån sig information eller så vilseleds hon eller han till att på bedragarens uppmaning genomföra en transaktion själv. Hotbilden har därmed förändrats och då behöver de förebyggande åtgärderna anpassas.

Social manipulering fortsätter

Alla banker informerar sina kunder om hur bankens tjänster och produkter 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, utöver bankernas egna åtgärder, snarare om ett antal förebyggande och samverkande åtgärder av flera aktörer i samhället.

Den gemensamma nämnaren för bedrägeriupplägen är viljan att påverka och förmå bankkunden att göra något: klicka på en länk, genomföra en betalning eller ringa ett nummer. Brottsligheten har blivit mer riktad och mer personlig och tillvägagångssätten

anpassas alltmer efter förutsättningarna. I grunden är det samma modus som utvecklas för att bli mer träffsäkra, exempelvis infogar bedragare oftare det riktiga namnet på förälderns barn i modus ”sms-barn” (bedragaren utger sig då för att vara förälderns barn i ett sms). Det är idag lönsamt för organiserad brottslighet att investera i den här typen av bedrägliga brottskoncept eftersom andelen uppklarade bedrägerier är låg trots att spårbarheten är hög.

Bedrägerierna drabbar alla målgrupper. Aktuella omvärldshändelser används ofta som bete, exempelvis covid19-vaccin, utbetalningar av elstöd, skatteåterbäring mm. En annan trend är ökningen av antalet kunder som blir utsatta för bedrägerier flera gånger. Det vanligast förekommande återvinningsbedrägeriet är att brottsoffer vilseleds att de kan få tillbaka pengar från ett tidigare investeringsbedrägeri.

En växande utmaning är att utsatta kunder förmås att skicka pengarna via andra kunder och/eller institutioner i ett eller flera led innan de når den avsedda slutmottagaren. Det leder till svårigheter gällande ansvarsfördelning, utredning och rapportering.

Hybridmodus dominerar

Hybridformen mellan vishing och smishing dominerar idag, det vill säga ett sms från en fejkad aktör som innehåller ett telefonnummer till en falsk kundservice. Kunden ringer då själv upp bedragaren och luras i det samtalet eller så ”kopplas” kunden vidare till ”sin bank”.

Trenden med bedrägerier där kunden själv godkänt transaktionerna på internet- eller mobilbank medför ett mer komplext problem för banken att både övervaka och förstå. Bankerna behöver få ut riktig information till kunderna om vad banken och andra aktörer gör och inte gör. Andra aktörer kan exempelvis inte koppla till bankens säkerhetsavdelning och att allt det som bedragaren vill ”hjälpa till med” kan bankerna göra själva om det behövs, bankerna har ju redan all information om kunden.

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.

Företagare utsätts

När det blir allt svårare för bedragare att få ut stora summor från konsumenters bankkonton kraftsamlar mer sofistikerade bedragare mot företag. Företagare och användare med tillgång till flera engagemang, som revisorer, har blivit mer utsatta de senaste åren. Brottsbytet kan då bli flera hundra tusen kronor eller mer. Bedrägerierna kan i värsta fall rycka undan mattan för företagens verksamhet och medföra konkurs, eftersom företagare inte har samma grundskydd mot ekonomisk förlust till följd av brott som konsumenter.

Dualitet skapar tröghet och trygghet

Dualitet, det vill säga att två personer måste godkänna en transaktion, skapar en inbyggd tröghet men också en trygghet. Dualitet finns som tillval för kunden men är inte tvingande och även om alla företagskunder erbjuds dualitet är det inte alla som tar del av möjligheten. Även om företag erbjuds dualitet för signering eller dualitetsgräns på ett visst belopp, är det inte alla företag, föreningar och stiftelser som tillser att deras interna rutiner efterlevs. Det är även viktigt att den andra personen som ska godkänna en transaktion verkligen gör en kontroll och inte bara slentrianmässigt signerar.

Säkerhetsmedvetandet hos kunderna behöver stärkas. För att få höjda beloppsnivåer kan banken utbilda och skapa medvetenhet så att kunderna förstår. Exempelvis kan bankens kundkännedomsgenomgång behöva visa att kunderna har dualitetsprocessen på plats och att de jobbar efter den, för att banken ska kunna godkänna andra beloppsnivåer. Utnyttjas inte möjligheten till dualitet kan sänkta limiter övervägas. Det är av stor vikt att företagskunder informeras om möjligheterna till dualitet i bankernas system för att undvika bedrägeriförluster.

Bedrägeribrottsligheten har utvecklats till att bli väldigt flexibel och anpassningsbar.

Fjärrstyrningsprogram ger bedragaren kontroll

Kunder luras också att installera fjärrstyrningsprogramvara på sin telefon eller dator, vilket ger bedragaren full kontroll över skärm och tangentbord. Kunder är sällan insatta i hur det tekniska fungerar och hur produkter fungerar. Bedragaren kan då lägga upp transaktioner i kundens bank som kunden sedan luras att signera.

Om bankerna skulle kunna upptäcka när fjärrstyrningsprogramvara används på en dator, en tjänst eller en session skulle banken exempelvis kunna neka betalningar eller välja att stänga ned tjänsten eller sessionen. Utmaningen med fjärrstyrningsprogramvara är att det är en legitim programvara. För att motverka fjärrstyrning försöker bankerna upptäcka och analysera beteendemönster för hur kunder använder datorer och appar.

Banktrojaner

Banktrojaner fortsätter att drabba kunder till banker och finansiella företag runt om i Europa. Banktrojaner som infekterar mobiltelefoner och mobilbankslösningar syftar ofta till att stjäla kunders inloggningsuppgifter. Bankkunderna har fått sina mobiltelefoner infekterade genom att ladda ner appar som innehållit skadlig kod. Banktrojaner utvecklade för Android-telefoner är fortfarande betydligt vanligare än för iOS-telefoner. Under 2025 skedde en stor ökning av Android-trojaner men hotet är inte vanligt förekommande i Sverige.

Artificiell intelligens

Bedragarna använder sig redan av ett automatiserat och robotiserat arbetssätt, och bankerna behöver följa utvecklingen av bedragarnas användande av AI. Bankerna har också möjlighet att använda den typen av teknologi i sitt brottsförebyggande arbete. Automatiserade konversationer förekommer i vissa bedrägeriupplägg via sociala medier och chat-appar. Bankerna förväntar sig ökad kvalitet på språk och design samt ökad skalbarhet i kommande upplägg av telefonbedrägerier (phishing, smishing och vishing). Bankerna ser fortfarande inte så många AI-videor men det finns indikationer på att AI används på olika sätt. Verktygen kan exempelvis ta reda på mer om offrens syskon och föräldrars egennamn på ett mer automatiserat sätt.

Risken är att modus mot företagare, exempelvis BEC-bedrägerier (till exempel vd-bedrägerier som innebär att någon inom ett företag luras att genomföra transaktioner till bedragare) kommer att förstärkas med AI-inslag, genom röstkloning och inspelade meddelanden. Det kan bli allt svårare för bankerna att bedöma om en kund, som är drabbad av bedrägeri, kommunicerat med en riktig person eller inte. Den tekniska utvecklingen kommer att medföra ännu större utmaningar både för bankerna och för kunderna att kunna skilja på vad som är bedrägligt och vad som är genuint.

Monitorering av kunderna kräver data

Att kunder idag utför många bankärenden själva medför att det blir allt viktigare för banken att kunna tolka kundernas beteende och upptäcka avvikelser. Bankerna arbetar systematiskt med preventiva metoder, som limiter och begränsningar i produkter. Monitorering av kundernas transaktioner är därför ett viktigt verktyg för banken. Ju fler datapunkter bankerna har tillgång till, desto mer träffsäkra blir deras bedömningar.

Om lagstiftningen skulle tillåta mer datadelning, av exempelvis målvakter och IP-adresser, skulle det bidra till bättre riskbedömningar och monitorering. När banker inte längre kontrollerar det tekniska gränssnittet i exempelvis appar eller betalplattformar får de mindre data att analysera, vilket gör det svårare att övervaka transaktioner och spåra flöden.

Bankens bedrägeri- och penningtvättsövervakning försvåras också om transaktioner går till uppsamlingskonton, i stället för direkt till de verkliga mottagarna. Framväxten av realtidsbetalningar ökar ytterligare behovet av precisa riskmodeller och dynamiska begränsningar för att snabbt kunna agera.

För- och nackdelar med ökad datadelning

Den ökade datadelningen inom finanssektorn är både en förutsättning för bättre riskhantering och en källa till nya sårbarheter. Regelverk som Financial Data Access (FiDA) syftar till att skapa ett mer sammanlänkat finansiellt ekosystem där banker och andra aktörer får tillgång till mer information än tidigare. För att realisera nyttan behöver dock datadelning sträcka sig bortom den finansiella sektorn. Delning av viss typ av information med exempelvis teleoperatörer och andra samhällsaktörer kan ha en tydlig preventiv effekt, särskilt i kampen mot bedrägerier.

En bredare datadelning kan dessutom förbättra kreditprövningar och möjliggöra mer precisa riskmodeller och stärka konkurrensen genom att fler aktörer får tillgång till relevant information. Samtidigt innebär ett öppnare dataflöde att attackytan för cyberkriminella ökar. När fler parter hanterar känslig information, ökar också risken för att en enskild sårbar aktör blir en ingångspunkt för angrepp som får konsekvenser i hela det finansiella ekosystemet. Även små och svårupptäckta manipulationer av data kan påverka kreditvärderingar och riskanalyser och därigenom leda till felaktiga beslut med stora ekonomiska konsekvenser.

Därtill uppstår målkonflikter mellan olika regelverk och samhällsintressen. GDPR ställer krav på dataminimering, korta lagringstider och begränsad möjlighet till aggregering, vilket ofta står i direkt motsats till behovet av långsiktiga analyser, spårbarhet eller möjligheten att utreda grova brott. Samtidigt ökar förväntningarna på bankerna att göra mer för att förhindra bedrägerier, penningtvätt och annan ekonomisk brottslighet – något som förutsätter att relevant data lagras, kopplas samman och delas när det behövs.

Utmaningarna förstärks av att olika myndigheter – exempelvis Integritetsskyddsmyndigheten, Finansinspektionen, Skatteverket och Polismyndigheten – ibland gör olika tolkningar av vad som är tillåtet och lämpligt. I samverkan med brottsbekämpande myndigheter förväntas bankerna snabbt kunna ta fram samlad och strukturerad information, samtidigt som integritets- och tillsynsperspektiv begränsar möjligheten att ha sådan informationen aggregerad och indexerad i förväg.

Sammantaget behövs tydligare och mer ändamålsenliga förutsättningar för att banker ska kunna utbyta information om bedrägerier, bedragare och riskmönster. Utan en moderniserad struktur för datadelning riskerar gapet att växa mellan vad samhället förväntar sig av bankerna – och vad bankerna faktiskt har möjlighet att leverera.

Bedragare kartlägger sina offer

En trend som har förstärkts de senaste åren är att bedragare blir allt skickligare på att kartlägga sina tilltänkta offer i olika målgrupper. I öppna söktjänster på internet 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 maskerade telefonnummer där bedragaren själv väljer vilket telefonnummer som ska uppvisas i displayen. Det kan till exempel se ut som om det är banken som ringer.

Bedragare kommer också åt uppgifter genom dataintrång. De får då tillgång till mer informationsrik och sanningsenlig information och kan utifrån den rikta sina attacker bättre. Utöver att använda öppna källor för att utsätta en viss grupp för telefonbedrägerier finns exempel på personer som utför arbete åt teleoperatörers kundstock och som sedan använder de uppgifterna i bedrägligt syfte eller säljer dem vidare. Andra exempel är när ”vårdcentralen” ringer kunden när kunden har varit där som patient tidigare samma dag. Bankernas bedömning är att AI-verktyg redan idag kan göra en kartläggning inför mängdbrotten.

Elektronisk id-kapning i fysisk miljö

I takt med att den digitala säkerheten har stärkts har bedrägerier med fysiska inslag ökat. Under 2025 ökade antal BankID-stölder som sker fysiskt på samma plats som offret. Bedragare är kreativa och använder flera metoder för att vilseleda. Modus är att bedragare, som sällan arbetar ensamma, lyckas låna offrets telefon. Man lånar telefonen av taxichaufförer, man approcherar yngre personer i krogmiljö och man svarar på försäljningsannonser på diverse marknadsplatser, även dörrknackning förekommer.

När bedragaren väl har telefonen i sin hand har denne på något sätt även fått reda på offrets säkerhetskod till BankID. Säkerhetskoden behövs för att aktivera BankID på bedragarens mobil. Det tillvägagångssätt som bedragare har använt är det så kallade ”app-till-app-flödet”, där en enhet med ett aktivt BankID används för att skapa ett nytt BankID på en annan enhet. För att utgivningen ska lyckas måste båda enheter vara parkopplade med hjälp av Bluetooth och de måste vara bredvid varandra. Det krävs även att platstjänster aktiveras på båda enheterna.

Det är alltså flera steg och parametrar som ska vara uppfyllda för att man ska lyckas skapa ett BankID på det här sättet. I vissa fall är det troligt att det rör sig om ”friendly fraud” men inte i samtliga fall. Drabbade kunder har inte alltid förstått att ett bedrägeri har ägt rum och kan därför inte redogöra för händelseförloppet. Bedragarna kan sedan vänta med att använda BankID en längre tid för att runda monitoreringen vilket gör bedrägeriförloppet mer utdraget. Det är viktigt att bankerna säkerställer att historien som den utsatte återger överensstämmer med de parametrar som den utgivande banken kan se kopplat till BankID-transaktionen och utgivningen.

Brottsvinsten för ett telefonbedrägeri var 2025 den lägsta sedan 2017.

I slutet av 2024 och under 2025 ökade antal hembesök markant.

Antal hembesök ökar markant

I slutet på 2024 och under 2025 ökar antal hembesök markant. Hembesök av bedragare som påstår sig vara från olika företag och myndigheter är ett växande problem. Det kan även vara fysiskt uppsökande som falsk färdtjänst.

Bedragarens förevändning är ofta att ”hjälpa till” med något påstått problem, medan syftet med hembesöket är att stjäla värdesaker eller komma åt kundens bankkort och e-legitimation. Risken för att antalet hembesök ökar, och därmed att personriskerna ökar när banken täpper till möjligheten till andra tillvägagångssätt, är en realitet som behöver beaktas i arbetet med att motverka bedrägerier. Transparensen i det svenska samhället där personuppgifter är öppna förenklar målsökningen för bedragare.

Kreditbedrägerier

Kreditbedrägerier är sedan lång tid en vanlig företeelse. Att förstå de olika upplägen av kreditbedrägerier – i alla delar av kreditens förlopp, från ansökan till återbetalning – är utmanande. Antal falska underlag fortsätter att ligga på en hög nivå. Kreditbedrägerier kan utföras på flera olika sätt för varje del och flera delar av kedjan kan vara involverade. Att få en överblick över omfånget av bedrägeriet kan vara krävande. Om bankerna får felaktiga uppgifter från myndigheter som bankerna i sin tur baserar sina kreditbeslut på påverkas det förebyggande arbetet.

Ett exempel: Bedragaren ansöker om ett lån på falska grunder. Utgångspunkten kan vara falska underlag, felaktiga uppgifter eller att kunden inte har någon intention att betala tillbaka lånet. Identiteten kan vara från en utvandrad person, överlåten till någon annan eller fabricerad.

Ett vanligt upplägg är att någon under en kort tidsperiod tar så många och stora krediter som möjligt från olika kreditgivare, utan avsikt att återbetala, ofta med avsikt att hålla sig undan eller lämna landet. Fram till den tidpunkt då uppgifter börjar synas i kreditupplysningarna drar bedragaren nytta av att de olika kreditgivarna inte kan utbyta information. Syftet är att maximera brottvinsten på så kort tid som möjligt.

Ett annat förekommande upplägg är att någon tar varaktiga krediter, exempelvis bostadslån på falska grunder. Den som saknar kreditvärdighet skapar en falsk bild av sin ekonomiska ställning. Så länge personen följer de avtalade lånevillkoren, till exempel sköter räntebetalningen, är möjligheten till upptäckt av bedrägeriet ofta låg. Intresset för kreditbedrägerier ökar när ränteläget är lågt.

Betalning, avbetalning och lösen av krediter är ytterligare ett riskområde, eftersom det kan vara upplägg för penningtvätt. All betalning av krediter bör kontrolleras mot uppgifterna avseende kundkännedom. Om medlens ursprung är tvivelaktigt, hamnar banken i en svår situation för hur kundförhållandet ska hanteras. Dessutom riskerar ärendena att snabbt bli komplexa.

Eftersom kreditgivare alltid behöver göra någon form av kontroll av personens eller företagets existens, kreditvärdighet och betalningsförmåga gäller det alltså för bedragaren att manipulera systemet så att kreditvärdigheten förefaller bättre än den i själva verket är.

När det gäller företagskrediter handlar det ofta om att ta många parallella olikartade krediter under den tid ett företag kan användas som brottsverktyg. Det kan vara företagslån, snabba företagskrediter, stora kreditinköp av dyra varor såsom maskiner, redskap eller fordon. Det är i allmänhet en målvakt som står som företrädare för det bolag som tar krediten.

Resurskrävande att hindra kreditbedrägerier

Att motverka kreditbedrägerier kräver mycket resurser och ett omfattande analysarbete. Dessutom krävs hantering av kunder, utbildning av personal,

förändrade processer och monitorering. Exempel på kreditbedrägerier inom konsumtionskrediter är personer som tar flera krediter på kort tid utan avsikt att betala. Analyser av detta modus har resulterat i förändrade onboarding-processer för att tidigt kunna upptäcka varningssignaler. Mäklare agerar allt oftare möjliggörare för bedrägerier, framför allt i bostadsaffärer på privatsidan men även inom företagssidan.

Om information om återkallade uppehållstillstånd kunde uppdateras och löpande delas med bankerna, skulle det kunna stoppa fler kreditansökningar till personer som försvinner ur landet.

Skatteverkets förändrade sekretessregler 2024 kring inkomst av tjänst och inkomst av näringsverksamhet har gjort det svårare att få reda på var inkomsten kommer ifrån. Tidigare var det specificerat men idag går det inte att särskilja om det är inkomst av tjänst eller inkomst från enskild firma.

Eftersom kreditbedrägerier baseras på en eller flera falska uppgifter har några banker börjat använda externa tjänster för att kontrollera kunders inkomstuppgifter. Men även hos svenska myndigheter registreras falska uppgifter om inkomst, vilket försvårar möjligheten för bankerna att förlita sig på uppgifterna rörande identiteter och familjeförhållanden. Eftersom det är enkelt att ändra inrapporterade uppgifter till myndigheter blir kontrollmekanismerna delvis satta ur spel.

Investeringsbedrägerier

Investeringsbedrägerier är ett växande problem. Mörkertalet avseende antal utsatta och brottsvinster är förmodligen stort. Bedragare utnyttjar människors önskan om hög avkastning mot låg risk på sina investerade pengar. Ofta pågår kontakterna under lång tid och det är vanligt att konsumenter luras flera gånger. Så kallade deepfake-artiklar och bluffannonser med kändisar i sociala medier är ofta startpunkt.

Ofta befinner sig bedragarna (huvudmännen) utomlands, och initial kontakt sker idag främst via annonser i sociala medier, e-post eller genom rekommendation från vänner och ytligt bekanta. Falska annonser förekommer i stor utsträckning på digitala plattformar där kända personers namn och bilder används för att skapa förtroende.

Bedragarna utnyttjar kundernas bristande kunskap om komplexa investeringsformer som exempelvis kryptovalutor. För att öka trovärdigheten skapar bedragarna falska webbsidor där offren kan logga in och se ”sina investerade pengar växa”. Uppgifterna som visas på skärmen är helt fiktiva. De brottsutsattas pengar har aldrig investerats i några tillgångar utan hamnat direkt i bedragarnas fickor.

Bedragarna har ofta haft kontakt med offret under lång tid. Det kan ta tid innan beteendemönster och transaktioner börjar avvika markant från kundens normala beteende, så att banken börjar ställa frågor. Det är dessutom inte ovanligt att bedragaren förser kunden med ett manus med svar på kommande frågor från banken. Det gör det utmanande för bankerna att upptäcka och stoppa ett pågående bedrägeri. Banken får ju svar på sina kontrollfrågor, och ibland även underlag.

I vissa fall uppmanas offren att ta lån för att finansiera ytterligare investeringar. I andra fall initieras låneansökningar i deras identiteter utan att de är fullt medvetna om vad som sker. Fjärrstyrningsprogram är vanligt förekommande vid investeringsbedrägerier. Genom att signera uppdrag, ibland utan att förstå vad de godkänner, riskerar offren att förlora mycket pengar.

Kunderna överför pengar i syfte att göra en investering som utlovas ge väsentligt bättre avkastning än både bankernas sparkonton och den realistiska avkastningen på placeringar. När investeringen ser ut att ha ökat och offret försöker ta ut sina pengar försvårar bedragarna detta genom att påstå att avgifter och skatter behöver betalas. Detta gör att värdet på investeringen plötsligt sjunker drastiskt, vilket ofta gör att offret börjar inse att de har blivit lurade.

I många fall kontaktas offren senare av ytterligare bedragare som utger sig för att komma från myndigheter eller advokatbyråer och som erbjuder hjälp att få tillbaka pengarna. Självklart medför hjälpen en kostnad, vilket leder till att offren utnyttjas en gång till. Eftersom kontakten med bedragaren ofta pågår länge tenderar offret inledningsvis att lita mer på bedragaren än på den egna banken. Ett negativt tonläge i samhällsdebatten om finansiella företag påverkar relationen mellan bank och kund.

Bankerna lägger ned stora resurser på att prata med sina utsatta kunder men det är väldigt svårt att få kunden på andra tankar. Många gånger förnekar de själva hur stora belopp de har skickat i väg och hur lång tid det har pågått. För banken finns också en utmaning att förstå om kunden är utsatt för ett investeringsbedrägeri eller om kunden har gjort en dålig investering.

Pump and dump

Pump-and-dump-upplägg är en form av investeringsbedrägeri som bygger på att det finns en aktie som har ett värde men att det sker en omfattande marknadsmanipulation. Under hösten 2025 framkom att upplägget blivit mer organiserat och mer AI-orienterat samt att det skedde utanför Sverige i små amerikanska bolag noterade på Nasdaq.

Modus är att bedragare köper en stor andel av en ofta okänd aktie med låg likviditet (en aktie vars kurs är lätt att påverka). Därefter sprider bedragarna vilseledande och falsk information för att skapa intresse för aktien och driva upp kursen. Informationen sprids via sociala medier, e-postutskick, chattgrupper, investeringsforum och falska annonser. Kunderna upplever att det finns en aktiv investeringsgemenskap runt aktien. I praktiken rör det sig ofta om en eller två bedragare i kombination med flera AI-baserade chat-botar som förstärker intrycket av legitimitet.

När aktiekursen stigit tillräckligt högt säljer bedragarna sina innehav, vilket leder till ett kraftigt kursfall. De småsparare som köpt in sig på toppen, eller under resan uppåt, står då kvar med aktier som snabbt förlorat sitt värde och som ofta är svåra att sälja.

Romansbedrägerier

Romansbedrägeri bygger på långvarig social manipulering där bedragaren inleder en relation med offret på distans i syfte att lura av denne pengar. Kontakt börjar ofta på dejting-plattformar och sociala medier och övergår till chat-tjänster. För bedragaren handlar det om att nå människor i situationer där de är sårbara, och kärlek är en stark drivkraft.

Det tar ofta lång tid för bankerna att hitta de utsatta kunderna, av flera skäl. För det första startar kontakten i kanaler utanför bankens kontroll. Bankerna kan stänga ned phishing-sidor men bankerna kan inte stänga ned Meta. För det andra varierar belopp och transaktionstyp vilket försvårar arbetet med att hitta avvikelser. För det tredje inser kunderna inte alltid att de är lurade. De upplever att de har en pågående relation som känns bra. För det fjärde vill kunderna sällan berätta om ”relationen”, det är inbyggt i den här typen av brottslighet. De kan ha uppmanats att hålla ”relationen” för sig själv och att ljuga för banken. För det femte, ju längre bedrägeriet har pågått desto svårare är det för banken att nå fram till kunden när denne har investerat mycket känslor och pengar i ”kärleksrelationen”, och kanske känner skam över att ha blivit lurad.

Bankernas arbete för att motverka romansbedrägerier är uppdelat i förebyggande åtgärder, hantering av pågående bedrägeri samt åtgärder efter upptäckt.

- **Före ett romansbedrägeri** är fokus på att minska risken för att kunder blir utsatta. Information behöver vara aktuell och levande för att öka medvetenheten om hur romansbedrägerier går till och vilka varningssignalerna är. Parallellt utvecklas bankernas system och processer för att identifiera avvikande beteenden, exempelvis ovanliga betalningsmönster.
- **Under ett pågående romansbedrägeri** är bankernas mål att så tidigt som möjligt upptäcka och bryta händelseförloppet. När misstanke uppstår kontaktas kunden för att informeras om riskerna och för att skapa förståelse för att kunden kan vara manipulerad. Det finns ett inbyggt undvikande beteende hos den här typen av kunder vilket försvårar för banken att komma i kontakt med kunden. Diskussionerna är svåra eftersom kunden motsätter sig bankens kontakt och ofta har starkare förtroende för bedragaren.
- **Efter ett romansbedrägeri** försöker bankerna begränsa konsekvenserna och minska risken för återutsatthet. Återfall för den här typen av bedrägeri är dock väldigt hög.

Ökad social manipulering som startpunkt för en mängd bedrägeriupplägg aktualiserar frågan om det borde finnas någon meddelanderätt mellan banker avseende utsatta kunder även om det skulle vara väldigt integritetsingripande.

Målvakter möjliggör bedrägerier

Målvakter och målvaktskonton är en förutsättning för bedragarnas verksamhet. Antalet penningmålvakter verksamma i Sverige är stort. Kriminella som upptäcks i en bank byter snabbt till en annan bank och fortsätter sina brottsliga aktiviteter där. Bankerna arbetar strukturerat med att analysera och motverka målvakternas möjligheter till upprepad brottslighet.

Totalt har 95 000 personer registrerats som misstänkta för bedrägeribrott under perioden 2022–2025, enligt Polisen. Ett fungerande flöde av information mellan bankerna och Polisen är därför avgörande för att

höja effektiviteten i brottsbekämpningen. Utan sådan informationsdelning kommer det att vara svårt för bankerna att motverka målvakters manöverutrymme och förhindra bedrägerier och penningtvätt.

Bankföreningens åtgärdsprogram – ökat kundskydd mot bedrägerier

Telefonbedrägerier ökade markant under 2023 och Bankföreningens styrelse beslutade därför i december samma år att ta fram en rekommendation till bankerna avseende åtgärder för ökat kundskydd mot bedrägerier.

Rekommendationen fokuserade på telefonbedrägerier och presenterades i maj 2024 för regeringen och hade tagits fram i samarbete med Polisen. Rekommendationen förväntades även ha effekt även på andra bedrägerimodus.

Åtgärderna, som skulle vara införda senast under 2025, omfattar bland annat:

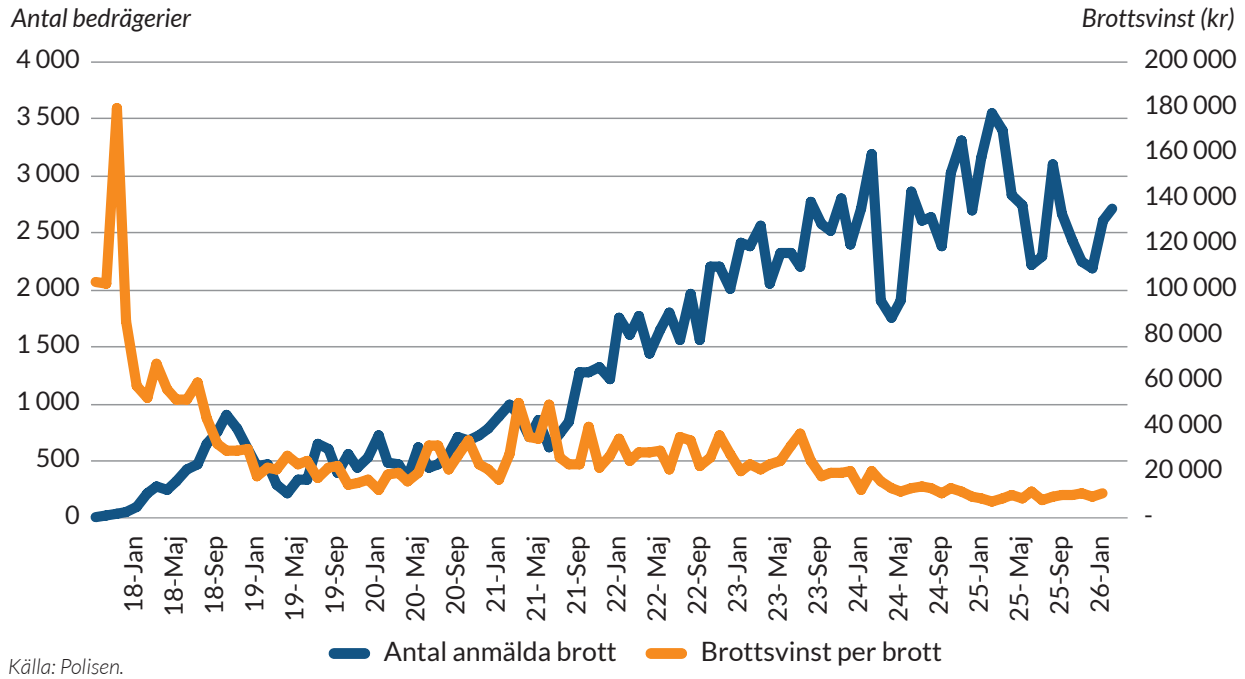
- Limiter (beloppsbegränsningar).
- Tidsfördröjning på betalningar och produkter.
- Möjlighet till dualitet (två måste godkänna transaktionen).
- Översyn av produkter som tillhandahålls.
- Ökad kontroll vid nya produkter.
- Blockera missbruk av bankers telefonnummer och sms (s k spoofing).
- Förbättrad transaktionsmonitorering.

> En ständig avvägning måste ske mellan smidighet och kundvänlighet å ena sidan, och tröghet och ökad säkerhet å andra sidan.

- Utvärdera id-metoder.
- Bankgemensamma initiativ för utfärdande av BankID.
- Bankgemensamma initiativ för blockering av BankID och Swish.
- Information och utbildning.

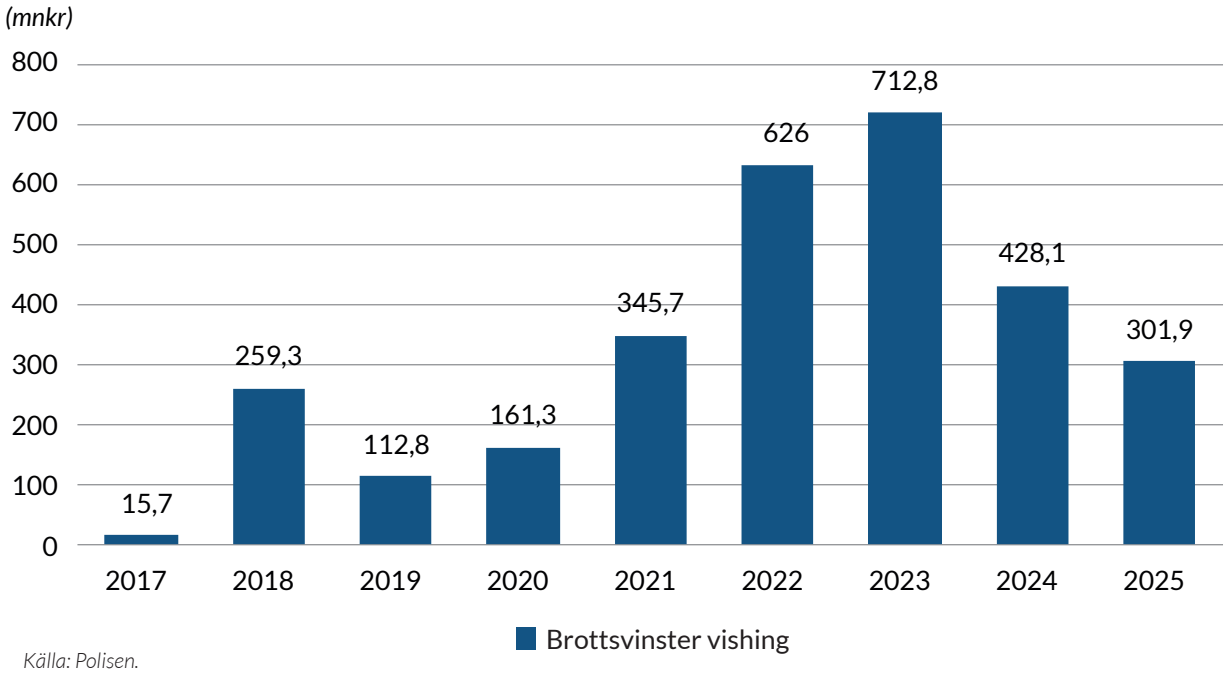
Åtgärderna implementerades under 2024 och 2025 med hänsyn till enskilda bankers kunder, produktutbud och infrastruktur. Bankerna har valt olika sätt att uppfylla rekommendationen på. Exempelvis kan en strikt begränsning för en viss produkt minska behovet av andra åtgärder. En mindre strikt produktbegränsning kan kombineras med tidigare

Antal anmälda vishingbedrägerier och brottsvinst i kr per vishingbedrägeri (2017–2025).



Källa: Polisen.

Brottsvinster i mnkr för vishingbedrägerier (2017–2025).



Källa: Polisen.

kundbeteende (belopp, frekvens, endast historiska betalningsmottagare etc.) vilket kan ge ett bra skydd. AI-baserade transaktionsövervakningsverktyg kan också ge ytterligare skydd.

Åtgärdernas effekt på bedrägeriutvecklingen har löpande följts upp tillsammans med Polisen. Syftet med det är att förstå hur brottsligheten och brottsvinsterna påverkas och förändras, särskilt i relation till modusförflyttningar.

Statistik från Polisen visar att brottsvinsterna från telefonbedrägerier minskade med cirka 60 procent 2025 i jämförelse med 2023. Snittförlusten (brottsvinsten) för ett telefonbedrägeri var 2025 det lägsta sedan 2017 (då mätningar av modus började).

Den förstärkta utfärdandeprocessen för Mobilt BankID har resulterat i att antalet obehöriga transaktioner vid utfärdande av Mobilt BankID, i princip har upphört. Beloppsgränser har haft god effekt med att minska brottsvinster.

Enligt Polisen är förklaringen till minskningen av brottsvinster i huvudsak bankernas åtgärdsprogram mot bedrägerier som lanserades i maj 2024. Utöver den minskning av förluster som har uppnåtts genom bankernas åtgärder har Polisen haft aktiviteter som påverkat lagföring både i Sverige och utomlands, och teleoperatörerna har också vidtagit åtgärder. Beloppen är dock fortsatt betydande och arbetet med att ytterligare begränsa förlusterna behöver fortsätta, speciellt avseende att förebygga stora förlustbelopp.

Bankföreningens åtgärdsprogram – ökat kundskydd mot investerings- och romansbedrägerier

Parallellt med de minskande brottsvinsterna för telefonbedrägerier ökade investerings- och romansbedrägerier under 2024. Bankföreningens styrelse beslutade därför i maj 2025 om en ytterligare rekommendation till bankerna avseende åtgärder fokuserade på investerings- och romansbedrägerier.

Åtgärderna, som ska vara införda senast under 2026, omfattar bland annat:

- Sprida kunskap för att uppmärksamma riskerna för att bli utsatt för bedrägeri, till exempel investerings- eller romansbedrägeri.
- Förhindra och begränsa att skärmdelningsverktyg används vid olika former av bedrägerier.
- Informera och hantera kunder som kan misstänkas vara eller ha blivit utsatta för bedrägeri. Kunderna blir ofta manipulerade och behöver bli informerade om vad som pågår för att förhindra att de utför transaktioner som är del i ett investerings- eller romansbedrägeri.

Åtgärderna kompletterar programmet från 2024 med förbättrade processer för att informera och hantera kunder som kan misstänkas vara eller ha blivit utsatta för investerings- eller romansbedrägerier. Åtgärdernas effekt på bedrägeriutvecklingen kommer att följas upp tillsammans med Polisen.

Behov av åtgärder från politik och myndigheter

- Lagstiftaren bör begränsa publicering av personuppgifter på internet. Det är i dagsläget allt för enkelt att söka fram exempelvis ensamstående äldre med god ekonomi. Förändringen behöver samtidigt tillgodose bankers legitima behov av att kunna utföra olika typer av kontroller.
- Teleoperatörer verksamma i Sverige bör åläggas att försvåra/omöjliggöra maskering av telefonnummer och sms. Teleoperatörer bör även skanna efter kända bedrägerimönster och blockera uppenbart bedrägliga sms samt ingå i samverkan med banker och andra relevanta aktörer för att motverka bedrägliga sms och stoppa trafik till webbplatser med skadlig kod.
- Skatteverket och Transportstyrelsen bör förse banker med bättre kontrollmöjligheter av deras id-handlingar i både fysisk miljö och på distans, liknande de möjligheter som Polismyndigheten tillhandhåller.
- Polismyndigheten bör utveckla ett informationsutbyte med bankerna runt Sverige-id (statlig e-legitimation, planerad till december 2026). Utbytet bör fokusera på användandet. Syftet med det är att motverka obehörig användning av Sverige-id exempelvis vid fjärrstyrning och utnyttjade identiteter samt att följa bedrägerimodus.
- Bankerna bör få utbyta information med varandra på ett enklare sätt. Ett flöde av information mellan bankerna och Polisen behövs också, exempelvis uppgifter om målvakter. För bankerna är syftet med en effektiv informationsdelning att stärka kundkännedom och riskbedömning av kunderna, samt transaktionsmonitorering.
- Polismyndigheten bör utveckla möjligheterna för brottutsatta att polisanmäla de vanligaste bedrägeriformerna på nätet. Det kan ta lång tid att komma fram via 114 14, vilket riskerar att skapa ett mörkertal angående brottslighetens omfattning.
- Den viktigaste åtgärden för att motverka investeringsbedrägerier är att sociala medieplattformar tar ett större ansvar för det som publiceras på deras plattformar. Plattformar som exempelvis Facebook, WhatsApp och Instagram är stora möjliggörare för falska annonser som publiceras där och som lurar kunderna. Plattformarna bör därför minska antalet bedrägliga annonser genom följande åtgärder:
  - Krav på verifiering av annonsörer och profiler.
  - System för övervakning av misstänkt beteende (liknande de som banker har infört).
  - Verifiering av kunders identitet och bedömning av riskprofil.
  - Procedurer och processer för rapportering av falska annonser.
  - Blockering av potentiellt falska profiler/annonsörer på ett centraliserat sätt.
  - Ekonomiskt ansvar när bedrägerier sker via plattformarnas kanaler.
  - Närmare samarbete mellan sociala medier, betaltjänstleverantörer och brottsbekämpande myndigheter.

Bedömningen är att bankernas gemensamma brottsförebyggande ansträngningar har haft stor framgång. Riskerna för bedrägerier och finansiella brott är dock fortsatt hög samtidigt som hotbilden blir alltmer komplex och samverkande genom kombinerande tillvägagångssätt i samma brottsupplägg.

Bankerna arbetar förebyggande för att få bort penningtvätt.

6 Penningtvätt

Regleringen av penningtvättsområdet är dels straffrättslig, dels administrativ. För bankernas del är det administrativa regelverket av störst betydelse för verksamheten.

Den **straffrättsliga regleringen** av penningtvätt innebär i praktiken kriminalisering av en rad olika så kallade penningtvättsåtgärder som syftar till att dölja att medel kommer från brott. Det kan röra sig om transaktioner av brottsutbyte mellan olika bankkonton eller omsättning genom inköp, men även andra åtgärder som till exempel att använda falska handlingar som representerar ett värde. Penningtvätt kan föregås av relativt enkla brott med enstaka aktörer inblandade eller av komplicerade brottsupplägg som ofta involverar en hel kedja av aktörer som agerar i samförstånd. Det brott som föregår penningtvätt och som leder till ekonomiskt utbyte brukar kallas förbrott. Den som gjort sig skyldig till penningtvätt i lagens mening döms för penningtvättsbrott alternativt näringspenningtvätt.

Det **administrativa penningtvättsregelverket** härrör från internationella principer som fastlagts av det mellanstatliga FN-organet FATF, Financial Action Task Force. Principerna har sedan omsatts till EU-lagstiftning. Sedan 2024 utgörs huvuddelen den svenska regleringen av EU-förordningen om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism, penningtvättsförordningen, AMLR. Förordningen är direkt tillämplig som svensk lag och ska tillämpas från och med den 10 juli 2027. AMLR kompletteras av EU-gemensamma tolkningsregler, så kallade tekniska standarder, RTS. En grundprincip för det administrativa penningtvättsregelverket är den så kallade riskbaserade ansatsen.

De verksamhetsutövare eller aktörer som omfattas penningtvättsregelverket ska leva upp till en rad krav som rör bland annat riskbedömningar av den egna verksamheten, kundkännedom, övervakning och rapportering till finanspolisen.

För bankernas del yttrar sig penningtvätt i normalfallet som transaktioner av brottsutbyte mellan olika bankkonton. Goda rutiner för kundkännedom och en ändamålsenlig övervakning av kundbeteende är därför de viktigaste verktygen för att banken ska upptäcka och förebygga penningtvätt. Övervakningen sker löpande för att upptäcka avvikande aktiviteter och transaktioner.

Förutom att genomföra åtgärder för att leva upp till penningtvättsregelverket, som till exempel övervakning, arbetar bankerna strategiskt med brottsförebyggande åtgärder och samverkan sinsemellan i syfte att helt få bort penningtvätt från banksystemet.

Penningtvättsrapporteringen

Enligt penningtvättsregelverket är verksamhetsutövare inom en rad olika branscher skyldiga att rapportera misstankar om penningtvätt till Sveriges finansiella underrättelseenhet, finanspolisen (Fipo).

Enligt Fipo:s statistik lämnades under 2025 totalt 66 341 rapporter om misstänkta transaktioner (STR) och 9 757 rapporter om misstänkta aktiviteter (SAR), vilket var en ökning med 26 procent respektive 15 procent, jämfört med 2024. Den finansiella sektorn stod för över 90 procent av rapporterna.

De största penningtvättshoten

Samhället vill inte ha pengar som härrör från brott. En brottsvinst som inte kan användas saknar i princip värde. Penningtvätt uppstår då kriminella försöker dölja härkomsten av sina brottsligt intjänade pengar.

Kriminella uppvisar ofta stor uppfinningsrikedom när det gäller att hitta nya sätt att tvätta pengar, försvåra för upptäckt eller säkrande av tillgångar som ska förverkas. Det kan handla om att investera brottsutbytet där omsättningsmöjligheterna är stora och kontrollerna inte är tillräckliga. Det finns även områden där kontroll av penningtvätt och tillsyn av föreskrivna åtgärder för att motverka penningtvätt ännu inte utövas på ett tillfredsställande sätt, till exempel avseende kryptovalutor.

Det internationella betalningssystemet utnyttjas också för att föra ett brottsutbyte utom kontroll för ett visst lands myndigheter. Överföringar kan ske till eller från länder som inte samarbetar med svenska myndigheter, eller där samarbetet inte fungerar effektivt. Under senare år har regeringen och myndigheterna trappat upp sina ansträngningar för att utöka det internationella rättsliga samarbetet i brottmål, vilket kan innefatta spårning och säkrande av bortförda tillgångar.

De främsta hoten mot bankernas arbete mot penningtvätt och finansiering av terrorism utgörs av den organiserade brottsligheten som genom kombinerad användning av målvakter, bulvaner och företag utnyttjar bankernas tjänster och produkter i brottsliga syften utan att exponera sig personligen. En annan aspekt av anonymiteten är den begränsade information som kan erhållas om motparter i betalningar som följer av den snabba utvecklingen av alternativa betallösningar. Eftersom penningtvätt kan genomföras på så många olika sätt är det en utmaning att överblicka utvecklingen och snabbt vidta effektiva motåtgärder.

Svårupptäckta penningtvättsupplägg

Eftersom en bank enbart kan se den del av en transaktionskedja som genomförts i den egna banken, är avancerade kedjor av penningtvätt med transaktioner i flera banker, ofta svåra att upptäcka. Bankerna har i dagsläget endast begränsade möjligheter att utbyta information med andra banker, men med AMLR följer förbättrade möjligheter som ska utnyttjas så långt som möjligt.

För att motverka den ökade bedrägeribrottsligheten, som ofta utgör förbrott till penningtvätt, har svenska banker genomfört tekniska förbättringar men även inskränkningar av tjänster i förhållande till kunderna. Det har medfört att de sammantagna brottsvinstena från telefonbedrägerier har minskat, men samtidigt har tillvägagångssätten för penningtvätt ändrats.

Antalet möjliga sätt att genomföra transaktioner har ökat under de senaste åren, en utveckling som förväntas fortsätta under 2026. Nya betaltjänstföretag som saknar bankernas rutiner och mognad inom penningtvättspreventionen tillkommer. Effekten av detta är i vissa fall minskad förståelse för pengarnas ursprung samt reducerade möjligheter för bankerna att övervaka och begränsa en kunds tjänster utifrån transaktionstyp. Detta medför att bankerna ställs inför utmaningar för att på ett effektivt sätt kunna övervaka och vidta åtgärder för transaktionstyper som bedömts utgöra en hög risk.

Samverkan inom penningtvättsområdet

Något som ökat i betydelse under senare år är informationsdelningen mellan dels brottsbekämpande myndigheter, dels verksamhetsutövare. Med informationsdelning avses här sådana avsteg från till exempel banksekretess eller röjandeförbud som regleringen möjliggör. Det är alltså inte fråga om ett fritt utbyte av information, utan det får ske undantagsvis i specifika situationer.

Penningtvättsförordningen AMLR innehåller ett flertal större förändringar. En av de mest framträdande rör möjligheterna till informationsdelning mellan privata aktörer, som kommer att kunna ske inom ramen för ett så kallat partnerskap (private-to-private, P2P). Detta är en nyhet i svensk rätt. Idag krävs medverkan av en myndighet.

Finansiellt underrättelsecentrum

I december 2024 gav regeringen i uppdrag till Polisen, Ekobrottsmyndigheten och Skatteverket att i samråd med näringslivet (banker med flera) inrätta ett finansiellt underrättelsecentrum (Finuc). Finuc innebär en utökad varaktig samverkan mellan myndigheterna och näringslivet inom bland annat penningtvättsområdet. Det övergripande syftet är att parterna gemensamt ska verka för att strypa den kriminella ekonomin genom effektiv informationsdelning och brottsförebyggande åtgärder.

Finuc är verksamt sedan den 1 april 2025, men uppbyggnaden av centrets verksamhet kommer att ske successivt fram till början av 2027. Förväntningen på längre sikt är att Finuc ska kunna agera snabbt och effektivt i såväl brottsförebyggande syfte som i förhållande till pågående avancerade penningtvättsupplägg. Bankerna välkomnar etableringen av Finuc.

Välfärdsbrottslighet och skattebrott

Så fort nya statliga eller kommunala bidrag eller stöd inrättas drar det till sig intresse från kriminella. Något som tydligt visat sig vid utbetalningar av ekonomiska stöd relaterade till covidpandemin, el- och miljöbefrämjande åtgärder.

Kriminella analyserar skattelagstiftningen och skatteförfarandet i EU och Sverige, för att hitta luckor och brister och skräddarsy brottsupplägg. Sådana brottsupplägg nyttjas av bland andra internationella kriminella organisationer som sätter upp en brottslig bolagsstruktur i Sverige.

Kriminellas utnyttjande av välfärdssamhället och skattesystemet utgör en särskild utmaning för bankerna eftersom utbetalningarna kommer från avsändare med högt förtroende, det vill säga myndigheter. Det är svårt för en bank att kontrollera om det finns bakomliggande brottslighet där myndigheter har lurats till utbetalning på felaktiga grunder. Mottagarna är dessutom i allmänhet vanliga personer eller företag där det saknas anledning att misstänka att de inte skulle ha rätt att ta emot pengarna. Här behövs breda proaktiva åtgärder från samhällets sida.

Kontrollerna måste i första hand göras av den beslutande eller utbetalande myndigheten. Från och med 2024 har en ny myndighet, Utbetalningsmyndigheten, inrättats med uppgiften att kontrollera utbetalningar från välfärdssystemet. Genom att arbeta med dataanalys och granskning hittar och hindrar Utbetalningsmyndigheten felaktiga utbetalningar, inklusive sådana med misstänkt brottslig bakgrund. I sin tur minskar detta bankernas risk för överföringar av brottsutbyte och därmed penningtvätt. När Utbetalningsmyndigheten har etablerat sina arbetssätt fullt ut samt fått legala verktyg att undersöka samtliga relevanta utbetalningsområden, kan man förvänta sig att myndigheten stoppar felaktiga utbetalningar i större utsträckning.

Fastighetsmarknaden och bostadsrättsföreningar

Fastighetsmarknaden är attraktiv för penningtvätt eftersom fast egendom kan nyttjas på många olika sätt och kräver en stor investering. Ett stort brottsutbyte kan då tvättas med endast ett inköp. Fastigheten kan sedan nyttjas till egen användning, uthyrning eller vidareförsäljning. Ytterligare pengar kan tvättas genom investeringar i form av exempelvis renovering och utbyggnad, vilket dessutom kan bidra till att generera mervärde. Företag i byggbranschen förekommer relativt ofta i bankernas utredningar om misstänkt penningtvätt.

Generellt sett finns ett intresse av att fastighetsaffärer genomförs snabbt, vilket i många fall hamnar i konflikt med kontrollintresset. Fastighetsmäklare kanske underlåter eller gör alltför summariska penningtvättsrelaterade kontroller. Inom en alltmer pressad och konkurrensutsatt fastighetsbransch är det viktigt att inte frångå kravet på ändamålsenliga kontroller, vilket inkluderar till exempel utländska köpare.

Bostadsrättsföreningar är sårbara för penningtvätt. Det förekommer penningtvättsupplägg där värden kan överföras mellan olika individer genom under- eller övervärdering av objektet vid köp eller försäljning. Bostadskrediter givna under felaktiga premisser kan användas för att finansiera dessa upplägg. Värt att notera är att regeringen under 2026 har föreslagit ett register hos Lantmäteriet där alla bostadsrätter ska registreras, vilket bankerna välkomnar.

Samverkan mellan banker blir viktigare.

Kryptotillgångar samt betalningar och valutaväxling

Kryptotillgångar, inklusive kryptovalutor, är en relativt ny bransch som är mycket sårbar för penningtvätt. Marknaden är global och volatil. Kryptovalutor används som betalningsmedel, men kanske framför allt som investeringsobjekt med avsikt att växlas till traditionell valuta. Flera av världens största kryptoaktörer är registrerade i länder med bristande antipenningtvättsregimer eller med sekretessregler som förhindrar transparens.

Kryptovalutor används ofta som betalningsmedel vid illegal handel på till exempel Darknet samt vid ransomware-attacker. I de fallen inköp av kryptovalutor kan betalas med bankkort uppstår en koppling mellan det traditionella finansiella systemet och kryptomarknaden.

Betalning i kryptovaluta förekommer i såväl detaljhandeln som mellan enskilda personer, vilket också ökar risken för penningtvätt. I och med ett större fokus på kryptovalutornas risker ökar dock medvetenheten hos näringslivet, vilket medfört att många aktörer idag inte befattar sig med sådana valutor.

Särskilda högriskgrupper är de som tillhandahåller tjänster avseende kryptovalutor, som betalningsförmedlare och valutaväxlare. De omfattas idag inte av samma omfattande regelverk som gäller för banker, och vissa aktörer är ännu helt oreglerade. De har i många fall bristfälliga 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.

En risk som ökat är att länder och andra aktörer utnyttjar kryptovalutor för att kringgå de omfattande rysslandssanktionerna från bland andra EU. Kryptovalutor har nämligen visat sig vara användbara för att ersätta globalt gångbara valutor som till exempel amerikanska dollar. Handel med kryptovalutor kan också vara ett alternativ för de aktörer som genom sanktioner utestängs från internationella betalningssystem.

Internationellt samarbete om korresponderande och konkurrensneutrala regleringar, definitioner och standarder, kan i framtiden bli helt avgörande för kontroll av kryptomarknaden och därmed minskade penningtvättsrisker framöver.

Samtidigt som omsättningen av kryptotillgångar är sårbar för penningtvätt ger den större möjligheter till analys än kontanter. Mycket data om transaktioner av kryptotillgångar är nämligen offentlig på internet. Att analysera denna data (så kallad block chain-analys) är både en möjlighet och en växande utmaning för intressenter på marknaden och brottsbekämpande myndigheter.

I december 2024 trädde EU:s förordning om marknader för kryptotillgångar (MiCA-förordningen, nedan; MiCA) i kraft. MiCA syftar bland annat till att underlätta rättssäkerheten för företag och locka fler investeringar till EU-länder. EU är nu den största jurisdiktionen i världen som infört ett omfattande regelverk för kryptomarknaden. Vilken effekt MiCA i praktiken kommer att få och hur effektivt tillsynen kommer att utövas återstår att se.

Även betalningsförmedling och valutaväxling som bedrivs yrkesmässigt eller i större skala är sårbar för penningtvätt. Eftersom sådan verksamhet använder sig av bankernas betalinfrastruktur påverkas bankernas riskexponering. Under senare år har reglering tillkommit i syfte att öka kraven på valutaväxlare och betalningsförmedlare, vilket bör bidra till en minskad risk för penningtvätt.

Lyxvaror och fordon

Marknaden för varor och tjänster i lyxsegmentet såsom smycken, klockor, guld, märkeskläder, resor och hotell har vuxit över tid. Den attraherar kriminella, både som verktyg för att tvätta pengar och som investering av kriminella tillgångar. Ofta sker betalningen med kontanter från brott eller med andra medel som har bakgrund. Många av lyxvarorna är lätta att flytta mellan olika länder och sälja vidare med bibehållet eller ökat värde. På så sätt kan lyxvaror användas för att överföra värden utan spårbarhet.

Ett förekommande tillvägagångssätt är att köpa en lyxvara kontant hos en handlare och sedan lämna tillbaka den. Handlaren har då inte så mycket kontanter tillgängliga, utan pengarna återbetalas genom insättning på kortkonto (i strid med kortregelverken). På så vis kommer kontanter med brottslig bakgrund in i det finansiella systemet.

I fråga om handel med fordon, främst personbilar, förekommer olika upplägg av penningtvätt. I vissa fall härrör köpeskillingen från ett brottsutbyte som tvättats i olika led, med hjälp av till exempel falska låneavtal och bankkonton i utlandet. Vidare kan det vara fråga om brottsupplägg där fordon som köpts med brottsutbyte importeras eller exporteras, samt upplägg i syfte att undvika skatter eller avgifter.

Spel och dobbel

Spelsektorn uppvisar en hög risk för penningtvätt. Spelföretagens konton kan användas i penningtvättsyften genom att pengarna förvaras och sammanblandas med andra medel. I sin tur innebär detta, när uttag eller överföringar från spelkontona görs, att pengarnas ursprung kan framstå som legitimt. Spelsektorn hanterar även kontanter i relativt stor omfattning, vilket är förenat med särskilt stora penningtvättsrisker.

Spelfusk genererar brottsutbyte som utbetalas till involverade personer. Sådan brottslighet har inslag av korruption och torde vara särskilt svårupptäckt för såväl myndigheter som andra aktörer.

Sedan traditionella kasinon under 2025 avvecklats i Sverige verkar spelföretag numera enbart på internet. Online-baserade företag är ofta belägna i lågskatteländer. Även om marknaden är reglerad och omfattas av penningtvättsregelverket förekommer åtskilliga olicensierade företag på den svenska och europeiska marknaden. Att spelföretagens intresseorganisationer verkar för goda rutiner och kunskapsspridning bland sina medlemmar bör bidra till att riskerna inom området minskar på sikt.

Behov av åtgärder 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 sådana verksamheter ökas betydligt. Regeringen har i januari 2026 gett Finansinspektionen i uppdrag att ta fram en vägledning till bankerna om hur målkonflikten mellan penningtvättsregelverket och rätten till bankkonto ska hanteras, vilket kan förväntas skapa tydlighet.
- För att åtgärderna mot penningtvätt och finansiering av terrorism ska kunna bli effektiva behöver bankerna få bättre möjligheter att dela information om misstänkta kunder, transaktioner och aktiviteter med varandra. Den organiserade brottsligheten utnyttjar det faktum att bankerna idag inte kan dela information sinsemellan. När kriminella upptäcks i en bank byter de omedelbart till en annan bank och fortsätter sina brottsliga aktiviteter där.
- De nya reglerna om samverkan och informationsutbyte mellan banker och brottsutredande myndigheter är ett steg i rätt riktning, men de behöver utvecklas ytterligare. Genom permanenta samverkansformer kan den erfarenhet och det förtroende mellan aktörerna som är nödvändig byggas upp och nå resultat. Inrättandet av Finuc är ett välkommet initiativ för ett effektivare informationsutbyte mellan berörda parter. Finuc behöver dock ges legala förutsättningar att kunna verka på ett ändamålsenligt och effektivt sätt, med en vid deltagarkrets och mot olika typer av ekonomisk brottslighet.

Hög

Bedömningen är att så länge den brottslighet som genererar ett ekonomiskt brottsutbyte fortsätter att ligga på en hög nivå i samhället, är risknivån för penningtvätt genom det reguljära finansiella systemet fortsatt hög. Bankerna försöker kontinuerligt begränsa sina risker, i huvudsak genom goda rutiner för att uppnå kundkännedom och en ändamålsenlig transaktionsövervakning. Kontrollen gällande skatte- och välfärdssystemet behöver öka ytterligare i syfte att begränsa förutsättningarna för brottsligheten som föregår penningtvätt.

7 Nyttjande av företag i brottsliga syften

Det har alltmer uppmärksammats att kriminella aktörer i stor omfattning nyttjar företag för att begå brott. Även om fenomenet har varit utbrett under lång tid, har en ökning skett under senare år. Delvis kan detta antas vara en följd av ökade insatser hos myndigheter och banker i förhållande till privatpersoner samt ett alltmer omfattande regelverk som rör penningtvättsprevention.

I allmänhet är det fråga om ett brottsligt nyttjande av små eller medelstora aktiebolag. Brottsliga inslag kan dock förekomma även i stora välrenommerade företag, där en del av verksamheten kan syfta till exempelvis skatteundandragande och därmed konkurrensfördelar. Att till exempel enskilda näringsverksamheter, handelsbolag, kommanditbolag eller stiftelser nyttjas i brottsliga syften är mindre vanligt, men förekommer. Brottspreventiva insatser som genomförs i förhållande till bolag driver en förflyttning av brottsligheten till andra associationsformer såsom ideella föreningar.

Anledningarna till att företag är särskilt attraktiva som brottsverktyg är många. Kriminella kan gömma sig bakom ett företags fasad av legitimitet. Det kan även handla om att kriminella genom ett företag öppnar för andra typer av lukrativ brottslighet, t.ex. genom att nyttja den säkerhet och stabilitet som ett bolag kan representera för samhället eller enskilda. Med hjälp av ett företag kan kriminella aktörer tillskansa sig stora belopp på relativ kort tid. De enskilt mest lukrativa ekonomiska brottsupplägen drabbar ofta den offentliga sektorn.

Låg upptäcktsrisk

Risken för att dömas till ansvar för brott har länge varit relativt låg, vilket beror på en mängd olika orsaker. Bland de viktigaste orsakerna återfinns sannolikt bristande möjligheter och skyldigheter till kontroll och informationsdelning mellan myndigheter och andra aktörer som är involverade vid ett företags bildande och löpande drift. Vidare kan en förundersökning om ekobrott i många fall syfta till att utreda en viss typ av anmäld brottslighet, medan resurser saknas till en bredare ansats innefattande samtliga typer av brottslighet som kan misstänkas inom brottsupplägget.

Brottstyper

Ett företag kan användas för att begå olika typer av brottslighet. Vanligt förekommande är exempelvis nyttjande av svart arbetskraft (skattebrott), momsbedrägerier (skattebrott), bedrägerier såsom exempelvis kreditbedrägerier och fakturabedrägerier samt olika typer av välfärdsbrottslighet. Vidare kan brottsupplägg som i sig syftar till penningtvätt via företag eller företagsstrukturer förekomma.

Mörkertalet kan misstänkas vara fortsatt stort. Man kan utgå från att många fall av penningtvätt samt eller skatte- och välfärdsbrottslighet med hjälp av företag, inte anmäls eller ens upptäcks.

Tillvägagångssätt

Många företag startas i syfte att användas för brott, där svagheter i olika system utnyttjas parallellt. Företaget används intensivt under den tid det tar innan varningssignaler hos myndigheter och banker genererar frågor och åtgärder. Företaget anses då förbrukat och

avvecklas eller överges. En sista åtgärd kan vara att utnyttja en konkurs för ytterligare brottslig vinning. När företaget överges är det tömt på tillgångar och bara skulder finns kvar.

De som bedriver den brottsliga verksamheten i ett företag tar sällan hänsyn till andra intressen än sina egna. Tidigare anställda eller affärspartners drabbas ofta av långvariga ekonomiska problem. Borgenärer har dåliga utsikter att få tillbaka pengar på sina fordringar.

Ofta blir det målvakten, det vill säga den person som figurerat som formell företrädare för företaget, som hålls straffrättsligt ansvarig för brottsligheten. Målvakten kan i vissa fall vara en ung person eller en person med svag anknytning till det svenska samhället.

Olika typer av brottslighet bedrivs ofta inom ett och samma företag, parallellt eller i följd. Det är även vanligt att samma kriminella nätverk driver många olika företag parallellt och genomför brottsliga dispositioner dem emellan. Det kan till exempel gälla storskaliga och systematiska upplägg för att begå skattebrott eller välfärdsbrott.

Avancerade brottsupplägg

I takt med att brottsbekämpande myndigheter blir alltmer effektiva och att regleringar skärps, behöver de kriminella utveckla sina brottsupplägg. Följden blir alltmer avancerade brottsupplägg. Till exempel förekommer avancerade företagsstrukturer med företrädare, bankkonton, redovisning eller kunder på olika platser, ofta i olika länder, samt skickligt förfalskade handlingar som underlag för transaktioner. Legitim och brottslig verksamhet kan dessutom kombineras inom samma företag eller företagsstrukturer. Sådana väl förberedda brottsupplägg är svårare att upptäcka för brottsbekämpande myndigheter och banker, vilket innebär att de kan bedrivas under en längre tid.

Vidare förekommer försök att förankra brottsupplägg genom kontakter med till exempel Skatteverket eller revisionsbyråer, i syfte att få dem att framstå mer legitima inför externa parter såsom banker och affärspartners. De personer som utför brotten i Sverige begriper inte alltid hur upplägget totalt sett fungerar och hur ett brottsutbyte de facto genereras, vilket innebär att de ofta har svårt att besvara detaljerade frågor från banker. Avancerade brottsupplägg kan säljas eller administreras av internationella kriminella nätverk.

Understödjare och möjliggörare

För att ett företag ska kunna drivas i brottsligt syfte är det nödvändigt att en rad olika initiala åtgärder vidtas. Till exempel behöver ett nytt företag startas upp eller ett befintligt företag förvärvas.

Externa aktörer kan behöva involveras som möjliggörare eller i vart fall understödjare av brottsligheten.

Till exempel kan det vara fråga om att förvärva ett så kallat historikföretag (företag med en dokumenterad historik av till synes legitim verksamhet) av en företagsförmedlare och därvid genomföra nödvändiga registreringar hos Bolagsverket.

För att skapa en varaktig legitim fasad är det ofta en del i brottupplägg att den löpande bokföringen ska skötas. En redovisningskonsult anlitas då för bokföring och skattedeklarationer till Skatteverket.

Brister hos en aktör skapar risker hos andra aktörer.

Som underlag för bokföring och som bevisning för betalningar kan osanna fakturor, kontoutdrag, transporthandlingar eller andra förfalskade skriftliga handlingar behöva införskaffas. Det är vanligt att externa möjliggörare tillhandahåller sådana handlingar mot betalning.

Andra aktörer, såsom legitima affärspartners, kreditgivare och kontoförande banker, behöver kunna lita på att bland annat registreringar hos Bolagsverket, uppgifter från Skatteverket och upprättad bokföring motsvarar verkliga förhållanden. Motparter behöver kunna veta vem man gör affärer med eller ger krediter till och under vilka premisser. Likaså behöver myndigheter veta exempelvis vem som driver en verksamhet, vilka som är anställda och i vilken omfattning arbete bedrivs.

Risker i förhållande till bankverksamhet och företagskonton

Ett företag utan tillgång till företagskonto är inte användbart, vare sig i legitima eller brottsliga syften. En del av brottsplanen innebär således ofta att få tillgång till konto i en svensk bank i många fall även valutakonto. Konto i en svensk bank innebär såväl låga transaktionskostnader, som förespeglar legitimitet i verksamheten.

Bankärenden genomförs ofta av målvakter, eller andra befullmäktigade personer som inte väcker misstankar.

Ur bankens synvinkel framstår förfarandet i allmänhet som normalt och väcker därför inga misstankar under en pågående bankförbindelse. Att till exempel genomföra förändringar i styrelse och verksamhet är normala åtgärder även för legitima verksamhetsutövare, och ger ofta inget misstänkt utslag i bankens kundkännedomsanalys (KYC).

Först då den brottsliga verksamheten avviker från det normala och till exempel ger utslag inom bankens transaktionsövervakning påbörjar banken en utredning och eventuell process för att avsluta kundrelationen. Vid det laget är det inte ovanligt att företaget redan tjänat sitt brottsliga syfte och anses som förbrukat.

När det gäller brottslighet med längre varaktighet, där ett företag eller en bolagsstruktur kontinuerligt används i såväl legitima som brottsliga syften är brottsligheten än svårare för banken och andra aktörer att upptäcka. Inom ramen för sådana verksamheter, som i vissa fall kan bedrivas av stora välrenommerade bolag, kan de brottsliga transaktionerna över företagskonton eller internationella betalningar utgöra endast en viss andel av de totala pengaflödena.

Att förhindra att personer med brottsliga syften får tillgång till ett företag är en utmaning för samhället. Så snart en sådan tillgång finns ökar riskerna för andra aktörer, till exempel banker, som då måste försöka upptäcka riskerna utifrån företagets beteende och därefter vidta åtgärder.

Behov av åtgärder från politik och myndigheter

- Banker måste kunna lita på uppgifter och betalningar från svenska myndigheter. Staten behöver därför ta ansvar för att kontrollera och verifiera de uppgifter som finns i statliga register för att minska risken för att myndigheterna utnyttjas av den organiserade brottsligheten.
- Bolagsverket måste skärpa sina kontroller för att uppnå tillräcklig effektivitet och precision i de registrerade uppgifterna. Bankföreningen välkomnar det arbete som påbörjats inom ramen för regeringens uppdrag till Bolagsverket, samt de pågående utredningar som syftar till att ge verket de verktyg och legala förutsättningar som är nödvändiga.
- Redovisningskonsulternas verksamhet måste regleras. Statlig auktorisation bör bli obligatorisk, för att motverka kriminellas tillgång till bokföringstjänster.
- Företagsförmedlare måste regleras. Statlig auktorisation eller annan reglering med liknande verkan bör införas, för att motverka att kriminella får snabb och alltför enkel tillgång till befintliga eller nya företag.

Bedömningen är att det för bankerna innebär en utmaning att upptäcka risker för brottslighet som involverar företagskonton, trots bankernas avancerade tekniska lösningar och informationsutbyte sinsemellan och med myndigheter. Ändamålsenliga och fördjupade granskningar i samband med att banker inleder affärsförbindelser med företag, särskilt inom högriskbranscher, kan verka brottsförebyggande. Grundläggande är dock att det inom samhällsstrukturerna införs effektiva förhandskontroller av företag.

Finansiering av terrorism har ofta samband med välfärdsbrott.

8 Finansiering av terrorism

Finansiering av terrorism innebär att pengar eller annan egendom hanteras i syfte att användas till olika typer terroristrelaterad verksamhet. För bankernas del handlar det ofta om att privat- eller företagskunderna använder bankens tjänster på ett otillåtet sätt genom att överföra pengar i dessa illegala syften. Det sker i allmänhet under falska förespeglingar och kan därför vara svårt att upptäcka.

På administrativ nivå regleras finansiering av terrorism i samma regelverk som penningtvätt, men det är normalt sett fråga om skilda fenomen sett till modus och motiv.

En ökande överlappning mellan organiserad brottslighet och terrorfinansiering noteras i omvärldsbevakningen. Omfattande och komplex internationell skattebrottslighet (till exempel momskaruseller som under senare år har drabbat det svenska skattesystemet i stor omfattning), kräver avsevärd organisation och stora initiala investeringar. Inte sällan är det fråga om tio- eller hundratals miljoner kronor. Investeringarna kan komma från internationella kriminella nätverk som i sin tur kan misstänkas ha kopplingar till terrorism. Brottsvinsterna går på olika sätt tillbaka till de internationella kriminella nätverken i utlandet och är därmed svåra att spåra. Bankerna har svårt att upptäcka riskerna, bland annat eftersom omsättningen förefaller legitim och utbetalaren i detta fall är Skatteverket. Detsamma gäller organiserad välfärdsbrottslighet av olika slag.

De senaste åren har antalet fall av misstänkt finansiering av terrorism via kryptovalutor ökat. Exempel på andra finansieringsformer för terrorism kan vara kreditbedrägerier, missbruk av humanitär hjälp och kontantsmuggling.

Även crowdfunding används för finansiering av terrorism. En stor grupp individer med samma intressen finansierar då med små summor en verksamhet eller ett projekt. Plattformar för crowdfunding möjliggör för privatpersoner att starta olika typer av insamlingar på internationell nivå via internet. För banken är det mycket svårt att skilja legitima insamlingar från sådana som sker med bakomliggande intentioner att finansiera terrorism.

Internationell terrorism är den grundläggande orsaken till många av världens sanktionsregimer. Tillämpning av sanktioner utfärdade av till exempel Office of Foreign Assets Control (OFAC; USA:s primära sanktionsmyndighet) medför i praktiken starkt minskade risker för banker att oavsiktligt medverka till finansiering av terrorism.

En viktig riskfaktor i fråga om finansiering av terrorism är att bankerna i vissa fall saknar tillgång till tillräcklig och aktuell information om hur sådan finansiering går till samt vilka personer och företag som är inblandande. Vet bankerna inte vad de ska reagera på eller leta efter blir det svårt att upptäcka misstänkt terrorfinansiering.

Bedömningen är att genom ökad samverkan och informationsdelning om tillvägagångssätt och aktörer, kan bankernas risker för att medverka till finansiering av terrorism minska. Det krävs dessutom en mer omfattande tillsyn av kryptoområdet.

9 Internationella sanktioner

Internationella sanktioner – eller restriktiva åtgärder – är en del av EU:s gemensamma utrikes- och säkerhetspolitik. I och med en mer komplex konfliktbild och tilltagande geopolitiska spänningar i olika delar av världen har sanktioner med tiden blivit ett allt viktigare utrikespolitiskt påtryckningsmedel.

Syftet med att utfärda sanktioner är att påverka beteendet hos den som sanktionerats enligt en viss agenda hos den som sanktionerar. Det kan gälla exempelvis mänskliga rättigheter eller freds-bevarande syften. Sanktionerna kan skapa förändringar på politisk eller statlig nivå.

Sanktioner är ett alternativ till mer ingripande åtgärder såsom väpnad intervention. De kan även vara ett förstadium till mer ingripande åtgärder, det vill säga om sanktionerna inte fått önskad effekt. Sanktionernas effekter är oftast inte omedelbara, utan det krävs långsiktighet och uthållighet.

En rad olika länder utfärdar sanktioner. Viktiga internationella aktörer är FN, EU, USA och Storbritannien. Sverige utfärdar inga egna sanktioner, utan genomför sanktioner som är beslutade av FN eller EU. I praktiken behöver svenska banker även ta hänsyn till sanktioner utfärdade av tredje land, såsom USA, för att undvika allvarliga affärsrisker, och i förlängningen risker för det svenska samhällets behov av en fungerande bankverksamhet.

Sanktioner kan riktas mot

- regeringar i länder utanför EU.
- enheter (företag) som finansiellt stöder den politik som sanktionerna är riktade mot.
- grupper eller organisationer, till exempel terroristgrupper.
- enskilda personer som antingen stöder den politik som sanktionerna är riktade mot, eller är inblandade i terroristverksamhet etc.

Sanktionsområdet har blivit mer oförutsebart och komplext.

Sanktioner omfattar inte bara listade enheter, utan även enheter med anknytning till listade enheter. För att efterleva internationella sanktionerna behöver bankerna därför analysera vem som äger eller har kontroll över en sanktionerad enhet. Sanktioner kan också ta sikte på en viss typ av vara eller tjänst som i sig är legitim men som den som sanktionerats kan använda i oönskade syften. I dessa sammanhang omnämns ofta produkter med dubbla användningsområden (s.k. dual use), det vill säga som kan användas både i civila och militära syften. Det kan vara till exempel kemikalier, elektronik eller mjukvara. Handel med sådana produkter innebär särskilda utmaningar att upptäcka och förhindra.

Sanktionerna har under senare år blivit allt svårare att överblicka och tillämpa på ett enhetligt och effektivt sätt. Det är inte bara bankerna som behöver förhålla sig till sanktionerna. Till exempel behöver industrisektorn ständigt vara uppmärksam för att inte riskera att bryta mot sanktioner.

Det har under senare år också uppstått en större nyckfullhet och oförutsebarhet inom sanktionsområdet, bland annat i förhållande till USA:s utrikespolitiska hållning, som skiftar snabbt. Som exempel kan nämnas USA:s utfärdande av sanktioner i vedergällningssyfte mot företrädare för den internationella brottmålsdomstolen (ICC) i Haag, som bidrar ytterligare till svårhanterad komplexitet.

Utvecklingen inom sanktionsområdet och Rysslandssanktionerna

Sedan Rysslands olagliga annektering av Krimhalvön 2014 och invasionskrig i Ukraina 2022 har EU i aldrig tidigare skådad omfattning utfärdat sanktioner mot ryska intressen. Sanktionerna är i huvudsak avsedda att begränsa Rysslands militära förmåga och markera att landets beteende är oacceptabelt. Sanktionerna omfattar bland annat reseförbud, frysningar av betydande ryska tillgångar och ett oljepristak för rysk oljeexport. När denna rapport skrivs (maj 2026) har EU beslutat om sammanlagt 20 sanktionspaket mot Ryssland. Under 2026 förväntas fler och utökade sanktioner mot Ryssland.

Ryssland hittar dock nya vägar att systematiskt kringgå sanktionerna. Ryska aktörer har med hjälp av utländska intressen hittat sätt att till exempel importera avancerad teknologi som kan användas inom krigsindustrin eller få ut marknadspris på olja. Genom namnbyten på bolag, förfalskningar av handlingar, bulvaner, med mera försöker man dölja vem eller vilka personer som i själva verket äger eller styr företag. Rysslandssanktionerna syftar nu i många delar till att försöka komma till rätta med undandraganden och kringgåenden, vilket sannolikt kommer fortsätta vara prioriterat inom EU under 2026.

Samverkan inom sanktionsområdet

Storskaliga, komplexa och systematiska sanktionskringgåenden ställer ökade krav på såväl verksamhetsutövare som myndigheter inom EU. Förståelse för problemet är grundläggande. Alltmer omfattande sanktioner och en alltmer komplex och riskabel kontext medför stora utmaningar när det gäller samverkan kring sanktionerna.

För att verksamhetsutövare ska förstå sin riskexponering och kunna tillämpa sanktionerna på ett ändamålsenligt sätt, behöver de både stöd från myndigheter och ha möjlighet till dialog sinsemellan.

Internationella sanktioner kan dessutom samverka med komplicerade strukturer av handels- och exportrestriktioner i allt högre grad, vilket kräver information och analys.

På nationell nivå gav regeringen under 2024 polisen i uppdrag att stärka efterlevnaden av internationella sanktioner genom inrättande av ett samverkansråd. Rådet är nu verksamt och omfattar ett antal myndigheter.

Bedömningen är att en ökad konfliktbild och allt större geopolitiska spänningar i olika delar av världen medför alltmer omfattande och komplexa sanktioner. För att tillämpningen av sanktionerna ska vara effektiv och syftet med sanktionerna ska uppnås samt att överträdelser av sanktionerna ska kunna bekämpas krävs utökad samverkan och dialog mellan aktörerna på sanktionsområdet.

10 Bank- och värdetransportrån och angrepp mot uttagsautomater

Sedan 2020 har det inte inträffat något bankrån i Sverige. En sådan lång period utan denna typ av angrepp har inte noterats sedan mätningarna startade för 45 år sedan. Förklaringen till den varaktiga nedgången 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.

Under 2025 inträffade heller inga värdetransportrån. De tio senaste åren har inneburit en markant minskning av antal värdetransportrån jämfört med decenniet innan. Förklaringen till minskningen är effektivare skyddssystem, sedelinfärgning, färre transporter samt bättre samverkan och förebyggande åtgärder mellan värdetransportbolagen och Polisen.

Inga angrepp mot Bankomat AB:s uttagsautomater inträffade heller under 2025. Statistiken omfattar sprängda och uppsågade uttagsautomater, däremot inte skimming av kort (stöld av kortinformation).

Låg

Bedömningen är att hotbilden avseende bank- och värdetransportrån består men att antalet rån kommer fortsätta att ligga på en låg nivå 2026, liksom antalet angrepp mot uttagsautomater.

Det senaste bankrånet i Sverige inträffade 2020.

Foto: www.bankomat.se pressbilder

11 Utmaningarna med kontanter

Sverige hör till de länder som har allra lägst efterfrågan på kontanter och faktisk användning av kontantbetalningar. En väl utbyggd kortinfrastruktur och digitala betallösningar, som exempelvis Swish, har en extremt hög nyttjandegrad. Kontantanvändningen i Sverige bedöms fortsätta som de senaste åren, det vill säga minska cirka 10 procent årligen.

Det förs i allt större utsträckning diskussioner om huruvida kontantanvändningen bör öka i samhället. Det finns en ambition att säkerställa kontanternas fortlevnad för olika syften. Det syns i regleringar (främst lagstiftningen om kontanter i betaltjänstlagen), Riksbankens ansvar (exempelvis föreskriftsrätten inom beredskap för betalningar i RBFS 2023:3) samt olika utredningar (Betalningsutredningen och Kontantutredningen).

Mer kontanthantering i samhället ökar riskerna för personalen och för penningtvätt eftersom spårbarheten är låg.

Kontanter som beredskapslösning

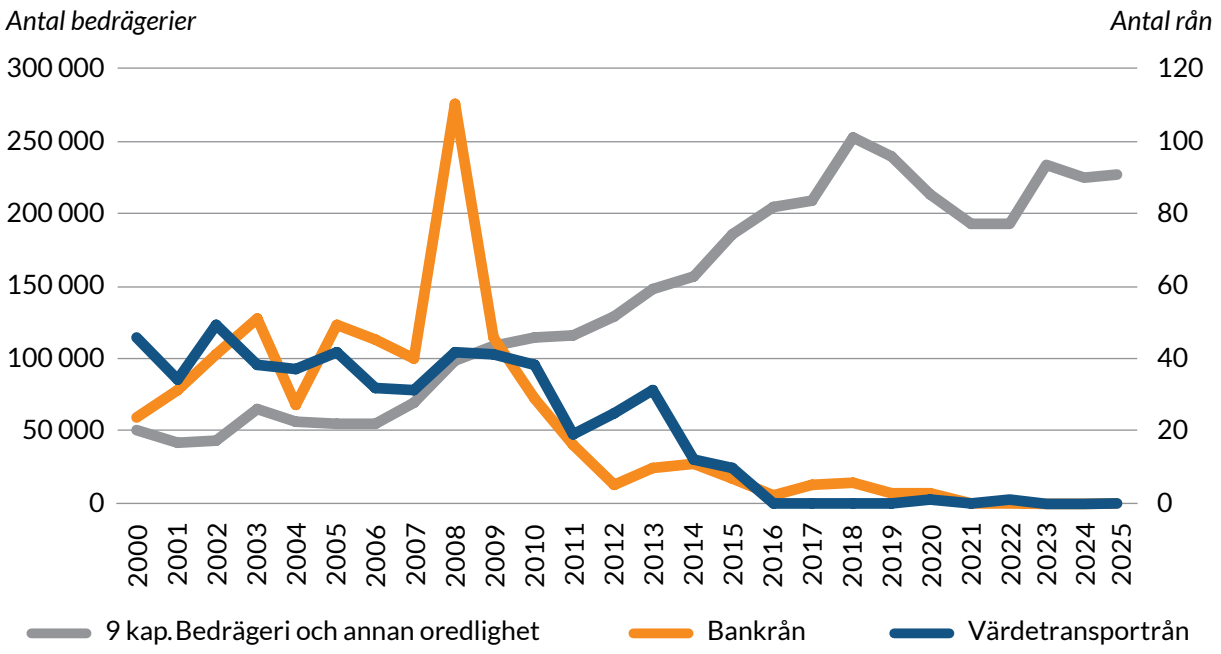
Eftersom kontanter används i så liten omfattning i normalläget är det inte en realistisk lösning att kontanter kan ha en avgörande betydelse vid kris eller krigshändelse. Kontantutbud och kontantinfrastruktur kommer helt enkelt inte att kunna skalas upp för att snabbt ersätta stora digitala betalningsvolymer. De slutsatserna har dragits av utredningar i såväl Danmark som Norge, samt av erfarenheterna från Ukraina.

Fokus för kontinuitets- och beredskapslösningar behöver därför ligga på ökad motståndskraft i de betalsystem som faktiskt används och i grundläggande infrastruktur som elförsörjning och telekommunikation.

Säkerheten för personalen

Kontantintensiv verksamhet skapar risker för de som arbetar med kontanter. För bankerna är säkerheten för personalen den viktigaste aspekten av kontantfrågan. Tack vare att allt mindre kontanter används har antal bank- och värdetransportrån minskat drastiskt från höga nivåer för 15–20 år

Antal polisanmälda bedrägerier och antal bank- och värdetransportrån (2000–2025).



Källa: Bankföreningen och BRÅ.

sedan. Senaste bankrånet i Sverige skedde 2020, och antalet värdetransportrån har också minskat markant det senaste decenniet. När antalet rån var som högst 2008 rånades två bankkontor och en värdetransport i veckan, med stort lidande för den drabbade personalen. Kontantutredningen underskattar de säkerhetsrisker som kontanter medför. Om kontantanvändandet ökar hos vissa handlare kommer både rånrisken och risken för internbedrägerier att öka.

Kontanter skapar penningtvättsrisker

Kontantintensiv verksamhet är också förknippad med hög risk för penningtvätt. Spårbarheten för kontanter är låg eller obefintlig, vilket är en avgörande nackdel i de flesta typer av brottsbekämpning. Kontanter är därför fortfarande ett attraktivt betalningsmedel i den illegala ekonomin. Stora delar av handeln med narkotika och illegala tjänster betalas med kontanter. Trots att kontantanvändningen överlag minskar i hela EU så ökar behovet av sedlar, vilket visar att kontanter fortfarande är ett viktigt verktyg som värdebevarare.

Bankerna har generellt sett bra kontroll över de direkta insättningar och 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 förstå var insättningarna kommer ifrån.

När kontanter växlas in i länder med stor kontantanvändning och dåliga kontroller, och sedan förs över till ett svenskt bankkonto är det mycket svårt för banken att kunna göra nödvändiga kontroller. Vid misstankar om penningtvätt kan bankerna behöva vidta åtgärder såsom att vägra ta emot kontanter från vissa utländska valutaväxlare.

Svårigheten består i att det i princip är omöjligt att spåra kontanta transaktionsflöden bakåt och påvisa misstänkta transaktioner och transaktionsflöden. Med olika typer av legala skyldigheter att acceptera kontanter kommer alltså risken för penningtvätt att öka, och möjligheten att hitta kriminella aktörer kommer att minska.

Bedömningen är att en ökad kontanthantering höjer riskerna för personalen och ökar risken för penningtvätt.

12 Hotbilden mot säkerhetskänslig verksamhet

Säkerhetskänslig verksamhet är verksamhet som är av betydelse för Sveriges säkerhet. Endast vissa av Sveriges banker bedriver säkerhetskänslig verksamhet. I de fall en bank bedriver säkerhetskänslig verksamhet, utgör den verksamheten enbart en begränsad del av bankens alla verksamhetsdelar. Hot mot säkerhetskänslig verksamhet kan många gånger likna hot mot annan verksamhet, både gällande bakomliggande hotaktörer och tänkbara metoder för angrepp. Det gör att detta avsnitt kan upplevas överlappa andra delar av rapporten.

Notera att detta avsnitt, till skillnad från resten av rapporten, beskriver hoten mot en mycket begränsad och specifik del av vissa av bankernas verksamhet. Bedömningarna som görs nedan utgår från dagens förhållanden men är framåtblickande, med en till två års horisont. De kan dock behöva omprövas löpande. Avsnittet bygger endast på de svenska säkerhetsmyndigheternas lägesbilder samt andra öppna och kommersiellt tillgängliga källor, och utgör en sammanfattning av en längre rapport som finns tillgänglig för de banker som bedriver säkerhetskänslig verksamhet.

Säkerhetskänslig verksamhet

Skyddet av säkerhetskänslig verksamhet kallas säkerhetsskydd, och är reglerat i säkerhetsskyddslagstiftningen, säkerhetsskyddsförordningen och i föreskrifter från olika myndigheter, däribland Säkerhetspolisen.

Avgörande för om en verksamhet ska anses vara av betydelse för Sveriges säkerhet är om en fientlig handling i form av spionerі, sabotage, terroristbrott eller andra brott, eller röjande av viss information som kan medföra skadekonsekvenser på nationell nivå. Nationella skadekonsekvenser kan till exempel vara störningar i eller bortfall av leveranser, tjänster och funktioner som är nödvändiga ur ett nationellt perspektiv.

Allmänt om säkerhetshoten mot den finansiella sektorn i Sverige

Enligt Riksbanken kommer det största hotet mot det finansiella systemets aktörer och infrastruktur från statliga och statsunderstödda hotaktörer. I en rapport från 2021 skriver Riksbanken att ”statliga aktörer söker idag insteg i digital infrastruktur som är kritisk för det svenska samhället för att ha möjlighet att slå ut den i det fall avsikten uppstår.” Statliga eller statsunderstödda hotaktörer kan med andra ord framgent ha en tilltagande avsikt och förmåga att utföra cyberattacker och sabotage som kan skada centrala samhällsfunktioner i Sverige. Varken organiserad brottslighet eller ideologiskt motiverade grupperingar bedöms vara dimensionerande hotaktörer för den säkerhetskänsliga verksamheten.

Främmande makt använder en hel arsenal av metoder för att nå sina mål men för finansiell sektor bedöms cyberdomänen vara den plattform som i högsta grad förekommer vid angrepp.

Ryssland som hotaktör mot säkerhetskänslig verksamhet i finansiell sektor

Ryssland är en aktör med en avancerad cyberförmåga, som är en integrerad del av landets underrättelsetjänster. Cyberoperationer används bland annat som ett verktyg för underrättelseinhämtning, påverkansoperationer och strategisk positionering. Det kan till exempel vara motiv som långsiktig åtkomst, dold informationsinhämtning, sabotage och utnyttjande av tredjepartsberoenden.

Till skillnad från mer öppna destruktiva cyberangrepp som förekommer i Ukraina bedöms cyberattackerna utanför Ukraina i huvudsak beröra dold informationsinhämtning. Ännu har det inte i bred bemärkelse framkommit exempel på destruktiva cyberangrepp i finansiell sektor utanför Ukraina. Wiper-skadlig kod, såsom ZEROLOT, har däremot använts i mot energisektorn i Ukraina och vid ett försämrat säkerhetspolitiskt läge skulle sådana förmågor kunna användas mot kritisk infrastruktur i Sverige.

Under de närmsta åren bedöms Ryssland i ökande grad förlita sig på nyttjande av organiserad brottslighet, ransomware-aktörer och hacktivistiska fasader för att kunna förneka inblandning i sabotage.

Kina som hotaktör mot säkerhetskänslig verksamhet i finansiell sektor

Kina bedöms som en aktör med fokus på långsiktig underrättelseinhämtning, strategisk positionering och förberedelser för åtkomst, snarare än destruktiva angrepp. Aktiviteten riktas främst mot statliga aktörer, forskning och akademi samt högteknologisk utveckling. Finansiell sektor kan däremot utsättas för indirekt exponering via tredjepartskomprometteringar, incidenter hos moln- eller telekomleverantörer.

Säkerhetskänslig verksamhet är verksamhet som är av betydelse för Sveriges säkerhet.

Iran som hotaktör mot säkerhetskänslig verksamhet i finansiell sektor

Irans säkerhetshotande verksamhet i Sverige utgörs av både underrättelseinhämtning och påverkansförsök. Irans prioriterade mål i Sverige bedöms bestå av israeliska och amerikanska verksamheter samt enstaka individer och organisationer från diasporan som antas utgöra ett hot mot den iranska regimen. Iran bedöms därför inte ha en avsikt och förmåga att angripa säkerhetskänslig verksamhet i svensk finansiell sektor.

Säkerhetshot mot svenska bankers säkerhetskänsliga verksamhet

De största hoten mot svenska bankers säkerhetskänsliga verksamhet bedöms återfinnas bland statliga eller statsunderstödda aktörer, där Ryssland bör ses som den dimensionerande hotaktören. Ryssland är den aktör som med störst sannolikhet kan tänkas ha eller utveckla en avsikt att försöka destabilisera Sverige som nation genom exempelvis angrepp på centrala punkter i det svenska finansiella systemet.

Att Ryssland har mycket avancerade förmågor inom såväl cyber- som underrättelsedomänen får anses vara välbelagt. Förmågor på den nivån är emellertid sannolikt mycket få, och således förbehållna de allra viktigaste målen.

Den svenska bankmarknaden är diversifierad, men ett stort antal banker tillhandahåller likartade tjänster, och det finns ett mått av utbytbarhet bankerna emellan. Bankerna har därutöver ett välutvecklat säkerhetsarbete och förmåga till återställning. Ett angrepp mot en viss bank torde således få en i sammanhanget begränsad effekt.

Det är därför inte troligt att säkerhetskänslig verksamhet vid svenska banker skulle utsättas för riktade cyberangrepp byggt på zero-day-sårbarheter, specialoperationer från kvalificerade sabotageförband eller infiltration från de ryska underrättelsetjänsterna genom strategisk placering av illegalister. Det troliga i sammanhanget bedöms vara angrepp av något mindre kvalificerad art. Sådana angrepp kan ske med egna resurser eller via proxys, exempelvis genom att nyttja olika kriminella aktörer. Det senare försvårar bedömningen av vem som ligger bakom ett angrepp.

Sammanfattande bedömning

- **Informationssäkerhetsrelaterade hot:** Bedömningen är att det inom cyberdomänen torde finnas avsikt och en god förmåga till tämligen avancerade destruktiva angrepp i form av omfattande och långvariga DDOS-attacker eller angrepp med malware som snabbt utnyttjar nyligen upptäckta sårbarheter. Det bedöms också finnas avsikt och en god förmåga att nyttja upptäckta sårbarheter för att bedriva dold informationsinhämtning.
- **Personalsäkerhetsrelaterade hot:** Även om avsikten finns, bedöms förmågan att genomföra angrepp med insiders vara begränsad. Bedömningen är att insiderhotet i första hand utgörs av opportunistiskt nyttjande av personer som vanligen saknar detaljerade kunskaper eller högre fysiska eller logiska åtkomsträttigheter. Dessa personer kan användas som möjliggörare eller utförare av angrepp mot informationssystem eller fysiska installationer såväl i spionage- som sabotagesyfte. Det

kan dock inte uteslutas att även personer som deltar i säkerhetskänslig verksamhet kan utgöra ett insiderhot.

- **Hot relaterade till fysisk säkerhet:** Även om avsikten finns, bedöms förmågan att genomföra sabotage eller fysiska angrepp för att komma över skyddsvärd information vara avsevärt mer begränsad än inom cyberdomänen. De resurser som rimligen kan avdelas för angrepp mot svenska banker bedöms i huvudsak utgå från nyttjande av lokala proxys. Dessa bedöms sakna god planerings- och samordningsförmåga och inte ha en särskilt långsiktig uthållighet. De praktiska förmågorna bedöms vara begränsade till enklare former av fysiska angrepp.

Behov av åtgärder från politik och myndigheter

- Sveriges banker stödjer Post- och telestyrelsen (PTS) förslag att Säkerhetspolisen ges i uppdrag att utreda möjligheten till normering avseende bedömning av nationella skadekonsekvenser inom det civila området.

  PTS noterade i en rapport till regeringen 2024 att en övervägande del av verksamhetsutövarna har betydande svårigheter dels att beskriva vilka skadekonsekvenser på Sveriges säkerhet som kan uppstå om den egna verksamheten drabbas av antagonistiska handlingar, dels att bedöma hur allvarliga skadekonsekvenserna är. PTS noterade flera problem som hängde samman med detta, bland annat att det förekommer att tillsynsmyndigheterna ger motstridiga signaler avseende deras bedömning av verksamhetsutövarens betydelse för Sveriges säkerhet.

  PTS föreslog med anledning av det att Säkerhetspolisen får i uppdrag att utreda möjligheten till normering avseende bedömning av nationella skadekonsekvenser inom det civila området. Sveriges banker stöder PTS förslag.

  Sveriges banker efterlyser en strukturerad samverkan avseende säkerhetsskydd i den finansiella sektorn. En sådan samverkan bör vara myndighetsledd.

- Den finansiella sektorn är komplex, och beroendet mellan olika aktörer är stort. Det är svårt för en enskild aktör att överblicka alla faktorer som behövs för att göra vissa bedömningar. Finansinspektionen beskrev detta förhållande i en rapport från 2022, och pekade på behovet av en bred och omfattande analys i syfte att identifiera vilka företag och processer som är mest skyddsvärda ur ett nationellt perspektiv.

  Även om säkerhetsskyddsregelverket träffar varje aktör var för sig finns sannolikt stora fördelar att vinna för Sveriges säkerhet genom att skapa en strukturerad samverkan för säkerhetsskyddsarbetet i sektorn. En sådan samverkan bör inte endast inkludera banker, utan även andra aktörer i den finansiella sektorn som bedriver säkerhetskänslig verksamhet, såväl företag som myndigheter.

  Exempel på konkreta sektorgemensamma aktiviteter är analyser av:

  - vilka tjänster, leveranser, funktioner och förmågor i sektorn (på sektornivå) som är av betydelse för Sveriges säkerhet.
  - vilka skadekonsekvenser för Sveriges säkerhet som kan uppstå vid en antagonistisk påverkan på ovan nämnda tjänster, leveranser, funktioner och förmågor samt när i tid efter ett angrepp sådana skador uppkommer.
  - säkerhetshot mot säkerhetskänslig verksamhet i sektorn.

  Sveriges banker efterlyser samverkansinitiativ från Finansinspektionen, Riksbanken och Riksgälden i denna fråga. Om verksamhetsutövare inte samverkar kan aktörer dra olika slutsatser, vilket medför att sektorns samlade säkerhetsskydd blir sämre än nödvändigt.

Bedömningen är att det finns ett hot mot bankernas säkerhetskänsliga verksamhet, och att det kommer att bestå under 2026.

Hotnivåer och trendindikatorer

Hotnivåer

Låg
Hotet bedöms som lågt, det finns inga eller få rapporterade incidenter. Påverkan på verksamheten är begränsad. Befintliga processer och kontroller bedöms ändamålsenliga för att hantera hotet.

Förhöjd
Hotet bedöms som förhöjt, det finns tydliga indikatorer på ökad aktivitet alternativt att incidenter blir mer avancerade och svåra att skydda sig mot. Hotbilden kräver ökad vaksamhet och i vissa fall förstärkta kontroller eller tillfälliga säkerhetsåtgärder. Regelbunden lägesuppföljning och tätare övervakning rekommenderas. Resursbehov och prioriteringar kan behöva justeras.

Hög
Hotet bedöms som högt, det finns en risk för incidenter som kan få allvarliga konsekvenser för verksamheten om inte åtgärder vidtas. Flera faktorer pekar på ett läge som kräver direkta åtgärder och kontinuerlig lägesuppföljning inom organisationen och med samarbetspartners.

Trendindikatorer

Ökar
Hotbilden visar tydliga tecken på att intensifieras över tid. Aktiviteten från relevanta aktörer stiger, eller så ökar risken för allvarligare konsekvenser för verksamheten. Situationen kräver ökad uppmärksamhet och ofta förstärkta kontroller eller beredskapshöjande åtgärder. Om trenden fortsätter kan hotnivån behöva höjas inom kort.

Oförändrad
Hotbilden är oförändrad och ligger på en jämn nivå över tid utan tecken på snabb förändring. Aktiviteten från hotaktörer är förväntad och följer tidigare mönster. Situationen kräver fortsatt monitorering men inga akuta förändringar i beredskap eller säkerhetsåtgärder. En stabil trend innebär dock inte att hotbilden är låg, endast att den är konstant.

Minskar
Hotbilden minskar jämfört med tidigare perioder och indikationerna blir färre eller mindre allvarliga. Det finns tecken på att åtgärder och yttre omständigheter har haft önskad effekt. Situationen bör fortsatt följas, men lägesbilden är mindre pressad än tidigare. Om den sjunkande trenden håller i sig kan hotnivån på sikt justeras ned.

Formgivning och grafisk produktion: www.luxlucid.com Stockholm, maj 2026

Svenska Bankföreningen
Finance Sweden

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