Swedsec

ÅKU 2025

ÅRLIG KUNSKAPSUPPDATERING

2024-10-09

Innehåll

Inledning

Den årliga kunskapsuppdateringens funktion

För att ha en aktiv Swedsec-licens krävs att licenshavaren varje år gör en årlig kunskapsuppdatering (ÅKU) inom ämnen som Swedsecs prövningsnämnd har valt ut. Kunskapskraven för ÅKU innehåller såväl nya företeelser eller regler som repetition av ämnen från de olika licensieringstesterna.

Struktur för ÅKU

Swedsec har ett system med yrkesanpassade licensieringstester. Även ÅKU ska vara anpassad till yrkesroll. ÅKU 2025 innehåller totalt 14 ämnen.

För att säkerställa att licenshavarna både uppdaterar befintliga kunskaper och tar del av nyheter i såväl kunskapskraven som generella nyheter på marknaden är ämnena för ÅKU 2025 indelade i tre avsnitt:

- Repetitionsämnen, det vill säga ämnen från kunskapskraven för licensieringstesterna som Swedsecs prövningsnämnd bedömt bör repeteras av licenshavarna.
- Nyheter: Nya ämnen i kunskapskraven, det vill säga ämnen som har föranlett förändringar i kunskapskraven för licensieringstesterna i samband med de senaste uppdateringarna, och andra aktuella ämnen som bedöms vara relevanta, men som inte ingår i kunskapskraven för licensieringstesterna.
- 2025 ersätts etikfallet med ett tema med inriktningen risker och sårbarheter i det finansiella systemet. Syftet är att licenshavaren ska tillägna sig viss elementär kunskap, främst om de aktuella begreppen och brottsmetoderna. Härutöver är tanken att licenshavaren ska få uppslag för att reflektera över risker som kan uppstå i olika arbetssituationer och för hur man ska agera och förhålla sig till dessa, exempelvis om det inte finns några instruktioner eller något givet rätt eller fel.

Varje licenshavare ska genomföra kunskapsuppdatering av de ämnen som är markerade för respektive yrkesroll i matrisen nedan. Den som arbetar med till exempel både investeringsrådgivning och bolån ska genomföra ämnen för båda rollerna.

Kognitiva nivåer

Kunskapskraven för ÅKU ska fungera som stöd vid utformning av utbildningar och uppgiftskonstruktion. Förutom utbildningsmoment ska ÅKU innehålla kontrollfrågor. I beskrivningen till varje ämne framgår vilken kognitiv nivå licenshavaren förväntas ha uppnått efter att ha genomfört kunskapsuppdateringen. I tabellen nedan beskrivs olika kognitiva nivåer.

Nivå	Förklaring
Känna till (K)	Licenshavaren ska känna till och komma ihåg begrepp, definitioner och faktauppgifter.
Förstå (F)	Licenshavaren ska förstå och kunna förklara olika samband och sammanhang.
Tillämpa (T)	Licenshavaren ska kunna använda till exempel formler, regler, lagar och metoder.

Ämnen ÅKU 2025

Ämne	Ledning och kontroll-funktioner[A]	Rådgivare[B]	Specialister[C]	Bolån[D]	Informations-givare[E]
Repetitionsämnen					
Kreditprövning – brister i kontroll dokumentation				x	
Dokumentation av bolånerådgivning				x	
Egendomsförhållanden och bolån				x	
Olika typer av ränteplaceringar		x	x		x
Aktivt och passivt förvaltade fonder	x	x	x		x
Regelverk kring hållbarhet	x	x			
Röjande av insiderinformation och analytikermassage	x		x		
Nyheter					
Kundens hållbarhetspreferenser i rådgivningen, inklusive PAI	x	x			
Flexibelt uttag av tjänstepension		x			
Skattenyheter		x	x	x	x
Dora/cybersäkerhet	x				
Värdering av onoterade tillgångar – utmaningar och frågeställningar			x		
Kapitaltäckning – nya regler 2025	x				
Tema					
Risker och sårbarhet i det finansiella systemet	x	x	x	x	x

[A] Personer som arbetar med olika typer av ledning och kontrollfunktioner inom finansmarknaden med särskild inriktning mot bank, fondverksamhet, värdepappersrörelse och försäkringsrörelse, t ex verkställande direktörer och andra ansvariga chefer samt utövare i kontrollfunktioner såsom funktioner för regelefterlevnad, riskkontroll och internrevision.

[B] Personer som arbetar med finansiell rådgivning till konsumenter eller investeringsrådgivning till kunder och/eller personer som arbetar med försäkringsdistribution avseende livförsäkringar med sparmoment till privatpersoner och företag, till exempel privatrådgivare, företagsrådgivare och Private Banking-rådgivare.

[C] Personer som arbetar inom olika typer av specialistfunktioner inom värdepappersområdet, till exempel fond- och portföljförvaltare, analytiker och aktiemäklare.

[D] Personer som arbetar med att sätta samman, erbjuda, bevilja, förmedla eller ge råd om bostadskrediter till konsumenter, till exempel bolånerådgivare och kredithandläggare.

[E] Personer som ger information om finansiella instrument, investeringstjänster eller sidotjänster utan att ge investeringsrådgivning.

Repetition

Kreditprövning – brister i kontroll och dokumentation

I samband med en låneansökan och kreditprövning kan en rådgivare behöva ta in kompletterade dokument som är en del av dokumentationen av ett låneärende, det kan till exempel vara underlag som styrker kundens inkomst eller värdet på bostaden. Rådgivaren ska förstå varför dokumentationen krävs, varför det är viktigt att kontrollera handlingarnas äkthet och vad det finns för riskfaktorer. Hur man gör en rimlighetsbedömning om värdena och när kan det krävas att ytterligare underlag tas in samt hur utförda kontroller ska dokumenteras och arkiveras. *Exakt hur dessa processer går till skiljer sig mellan bankerna men på övergripande nivå finns likheter.*

Licenshavaren ska:

- förstå vilken information som rådgivaren behöver inhämta om kunden för att kunna göra kreditbedömning och lämna ett lämpligt råd samt övergripande förstå vad risk innebär för kunden och för banken.
- förstå vad som ska dokumenteras av lånehandlingarna och av underlaget i rådgivningen. Licenshavaren ska också förstå varför dokumentation krävs och kunna förklara för kunden varför handlingar, som låneansökan, kreditupplysning, rådgivning, ESIS och kreditavtalet dokumenteras och vad de innebär.
- förstå när och varför en värdering ska göras och vad en värdering används till hos kreditgivaren. Dessutom ska licenshavaren kunna ange vilka krav som ställs på den utförda värderingen och vem som får utföra värdering. Licenshavaren ska känna till vikten av oberoende mellan värderingen och kreditbeslutsprocessen.
- kunna tolka och bedöma rimligheten i en värdering och skälen till värderingen samt kunna förklara värderingen för kunden.

Läsanvisningar:

FFFS 2023:20, 2 kap Kreditprövning 2023:20 | Finansinspektionen

Bolån - Kunskap för Swedsecs licensiering av Anette Ridder, kapitel 9 Kreditprövning

Dokumentation av bolånerådgivning

Många kunder har frågor om vilken räntebindningstid som passar dem bäst och då är det viktigt att rådgivarna vet vad fördelarna och nackdelarna är med rörlig respektive bunden ränta samt om dessa skiljer sig i en uppåtgående respektive nedåtgående räntemarknad. Vad avgör om en rådgivningssituation uppstår och hur dokumenteras den i så fall?

Frågor som ofta uppkommer:

- Vad är fördelarna och nackdelarna med rörlig respektive bunden ränta? Vad är fördelen med att kombinera rörlig och bunden ränta?
- Skiljer sig för- och nackdelarna i uppåtgående respektive nedåtgående räntemarknad? Kan det var bra att binda räntan även i en nedåtgående marknad?

Licenshavaren ska:

- förstå innebörden av rörlig och bunden ränta, räntetak och räntesäkring samt olika räntebindningsalternativ. Licenshavaren ska förstå innebörden av villkorsändring och kunna förklara vad som gäller om kunden vill lösa lån i förtid samt förstå hur ränteskillnadsersättning beräknas.
- förstå när en rådgivningssituation uppstår och kunna skilja den från situationer då handläggaren lämnar generell information och/eller då marknadsföring förekommer. Licenshavaren ska känna till vilka krav som ställs beträffande licenshavarens kompetens. Licenshavaren ska också förstå vilken information som rådgivaren behöver inhämta om kunden för att kunna göra kreditbedömning och lämna ett lämpligt råd samt

övergripande förstå vad risk innebär för kunden och för banken. Licenshavaren ska kunna anpassa förklaringarna/råden så att kunden kan bedöma om kreditavtalet lämpar sig för dennes behov och ekonomiska situation.

- Licenshavaren ska förstå vad som ska dokumenteras av lånehandlingarna och av underlaget i rådgivningen. Licenshavaren ska också förstå varför dokumentation krävs och kunna förklara för kunden varför handlingar, som låneansökan, kreditupplysning, rådgivning, ESIS och kreditavtalet dokumenteras och vad de innebär.

Läsanvisningar:

Boränta - viktigt att tänka på | Konsumenternas

Rörlig eller bunden boränta? - Tips och råd - Finansportalen

Konsumentkreditlag (2010:1846) | Sveriges riksdag (riksdagen.se) Rådgivning om bostadskrediter § 51-54

Egendomsförhållanden och bolån

Licenshavaren ska känna vilka negativa familjerättsliga konsekvenser som kan uppstå av att makar/sambor upptar en gemensam kredit med en bostad som säkerhet vilken utgör enskild egendom/ej bodelningsbar egendom. Licenshavaren ska känna till att det är olämpligt att en kund står med som medlåntagare till sin make/maka/sambos kredit om egendomen som pantsatts som säkerhet för krediten till sin helhet ägs av den andra maken/makan/sambon och bostaden i fråga ej är bodelningsbar egendom. Licenshavaren bör vidare känna till att i majoriteten av ovan nämnda situationer behöver kompletterande familjerättsliga avtal upprättas för att skydda den part som ej äger bostaden vid en eventuell separation eller dödsfall.

Läsanvisningar:

Ekonomisk Familjerätt, Folke Grauers, upplaga 10, 2022

Olika typer av ränteplaceringar

När vi lämnat perioden med noll eller negativa räntor har olika typer av ränteplaceringar åter blivit aktuella för många sparare. Det finns stora skillnader mellan olika typer av ränteplaceringar inte minst vad gäller risk och potentiell avkastning. Val av ränteplacering kan få stor betydelse för framtida avkastning varför det är viktigt att som rådgivare förstå de olika placeringarnas egenskaper.

Licenshavaren ska förstå de grundläggande faktorer som skapar skillnader mellan ränteplaceringar, främst duration och kreditrisk samt hur de påverkar risk och avkastning. Licenshavaren ska känna till de huvudsakliga skillnaderna mellan kontosparande och sparande i räntefonder. Licenshavaren ska också känna till de vanligaste typerna av räntefonder samt vilka typer av obligationer dessa fonder vanligtvis innehåller. Licenshavaren ska förstå skillnaderna mellan obligationer med fast respektive rörlig kupong (FRN) samt hur det påverkar risk och avkastning i obligationen/fonden som placerar i dessa obligationer.

Aktivt och passivt förvaltade fonder

Under ett antal år har intresset för så kallade passivt förvaltade fonder ökat stadigt, på bekostnad av aktivt förvaltade. De passivt förvaltade fonderna finns också i huvudsak i två olika varianter, indexfonder och börshandlade fonder, ETF:er. De passiva fonderna speglar ett specifikt index, de aktiva fonderna har oftast ett index som referens. Det är därför viktigt att förstå hur olika index är konstruerade då exempelvis två indexfonder som investerar på Stockholmsbörsen kan ha olika innehåll och utveckling.

Licenshavaren ska förstå skillnaden mellan en ETF och en värdepappersfond och vilka effekter de kan få för en placerare. Licenshavaren ska vidare förstå den grundläggande skillnaden mellan passivt och aktiv förvaltade fonder. Licenshavaren ska känna till hur val av indexkonstruktion kan påverka en passiv fonds avkastning i relationen till den underliggande marknaden och de vanligaste typerna av avvikelser från underliggande marknadsindex som förekommer (främst exkludering av etiska eller hållbarhetsrelaterade skäl). Vidare ska licenshavaren känna till de vanligaste index som förekommer på Stockholmsbörsen samt hur de skiljer sig.

Regelverk kring hållbarhet

Under de senaste åren har det publicerats och implementerats en mängd regler på hållbarhetsområdet i relation till dem som tillhandahåller finansiella produkter, de finansiella produkterna som sådana samt själva distributionen av produkter som bygger på eller tar hänsyn till hållbarhetsfaktorer på olika sätt.

Från ett värdekedjeperspektiv har lagstiftaren skapat en komplex struktur av olika krav som totalt sett omfattar framtagande av finansiella produkter, förvaltning av dem, transparens kring hållbarhetsarbete, distribution av produkter som innefattar hållbarhetsfaktorer samt slutligen löpande rapportering av hållbarhetsarbete.

Givet att reglerna återfinns i olika lagar och förordningar är det viktigt att licenshavarna har en förståelse för hur regelverken samverkar och hur de kommer in vid rådgivning om finansiella produkter.

Licenshavaren ska:

- känna till vad Taxonomiförordningen är och vilka typer av bolag och branscher som omfattas idag och vad som utgör en miljömässigt hållbar investering.
- känna till Disclosureförordningens syfte och vilka produkter och tjänster som omfattas. Förstå definitionen av finansiella produkter som 1. främjar miljörelaterade eller sociala egenskaper enligt artikel 8 eller 2. har hållbar investering som mål enligt artikel 9. Förstå samverkan med Taxonomiförordningen på det sätt att dessa typer av produkter också kan innehålla miljömässigt hållbara investeringar. Och till sist förstå vad som menas med att produkter beaktar huvudsakliga negativa konsekvenser för hållbarhetsfaktorer, så kallad Principle Adverse Impact (PAI).
- känna till var man kan hitta fonders och IBIPs hållbarhetsinformation och känna till att utfallet av fondförvaltningens hållbarhetsarbete redovisas i fondernas årsrapporter.
- förstå distributörens roll och hur hållbarhetsaspekter ska inkluderas vid rådgivning av finansiella produkter.

Läsanvisningar:

Finansinspektionen:

https://www.fi.se/sv/hallbarhet/regler/taxonomi/

https://www.fi.se/sv/hallbarhet/regler/upplysningar/

Taxonomiförordningen 2020/852 artikel 2(2), 3 och 5 – 7 & 9

SFDR 2019/2088 artikel 2, 6, 8 – 9, 10 – 11

MiFIDs delegerade förordning 2017/565 artikel 54(2) och 2021/1253 artikel 1(6)

IDDs delegerade förordning 2017/2359 artikel 9(2) och 2021/1257 artikel 2(3)

Röjande av insiderinformation och analytikermassage

Eftersom börsbolag är kunder hos banker och andra värdepappersinstitut får vissa av institutens licenshavare inte sällan tillgång till insiderinformation, det vill säga (något förenklat) information som inte är offentliggjord och som, om den offentliggjordes, skulle påverka priset på bolaget aktier och andra värdepapper väsentligt.

Det är förbjudet att utnyttja insiderinformation för att handla aktier eller tipsa andra att handla. Det är även, såsom huvudregel, förbjudet att över huvud taget röja insiderinformation. Detta får endast ske om röjandet, med lagstiftarens vokabulär, sker som ett normalt led i fullgörandet av tjänst, verksamhet eller åligganden. Detta är exempelvis fallet om ett uppgiftslämnande sker i samband med en så kallad marknadssondering.

Om undantagen inte är uppfyllda gör sig röjaren skyldig till brottet obehörigt röjande av insiderinformation. Om röjandet inte sker med uppsåt (avsikt) utan av oaktsamhet är det inte brottsligt men det utgör likväl en överträdelse av den så kallade Marknadsmissbruksförordningen. Detsamma gäller om agerandet förvisso skett med avsikt men endast kan betraktas som ringa. I sådana fall beivras dock röjandet genom sanktionsavgifter eller andra så kallade administrativa sanktioner från Finansinspektionen.

Undantaget från röjandeförbudet ska tolkas restriktivt; i korthet gäller att den som får informationen ska ha ett nödvändigt behov av informationen för att kunna utföra sina arbetsuppgifter eller andra nödvändiga åtgärder. Att det mer allmänt kan vara värdefullt eller intressant för en medarbetare att känna till uppgifterna, till exempel för att man arbetar inom samma enhet, är inte tillräckligt.

Aktieanalytiker har, av fullt naturliga skäl, ofta upparbetade kontakter med de noterade börsbolag som analytikerna följer. Det är emellertid viktigt att analytikerna bidrar till att en sund relation med börsbolaget upprätthålls och till att börsbolaget inte lämnar insiderinformation till analytikern (vare sig i konkret och uttrycklig eller i mera inlindad och underförstådd form). Om så ändå skulle ske måste analytikern vara noga med att inte obehörigen röja uppgifterna vidare eller utnyttja dem på annat sätt, till exempel genom att lämna investeringstips grundat på informationen eller ge information om reviderade estimat rörande börsbolaget till vissa utvalda kunder innan analysen gjorts tillgänglig för hela marknaden.

Licenshavaren ska känna till reglerna om obehörigt röjande av insiderinformation i lagen om straff för marknadsmissbruk på värdepappersmarknaden och i marknadsmissbruksförordningen.

Läsanvisningar:

Prop. 2016/17:22 s 281-285.

Finansinspektionens skrivelse 2024-05-29 med titeln Esmas uttalande om ”pre-close calls”, se
https://www.fi.se/contentassets/b38e0a0fc6a044baa89fe3016c35e04e/esma-uttalande-pre-close-calls-sve.pdf

Nyheter

Kundens hållbarhetspreferenser i rådgivningen, inklusive PAI

Kraven runt integrering av hållbarhet i rådgivning från myndigheter såväl som intresset från kunder för hållbara investeringar har ökat de senaste åren. Mot denna bakgrund är det viktigt att licenshavare har rätt förutsättningar för att kunna förstå och bedöma kunders hållbarhetspreferenser och därigenom kunna ge lämpliga råd.

För att säkerställa att finansiella produkter på ett relevant sätt matchas med kunders individuella preferenser och investeringsmål finns det på distributionssidan krav i MiFID (LVPM) och IDD (LFD) om att man vid rådgivning till kund ska inkludera kunders hållbarhetspreferenser som ett led i lämplighetsbedömningen.

En kunds hållbarhetspreferenser definieras utifrån att kunden ska ange om något av följande ska utgöra en del av kundens placeringar:

a) En viss minimiandel som ska investeras i en produkt som gör miljömässigt hållbara investeringar;
b) En viss minimiandel som ska investeras i en produkt som gör hållbara investeringar enligt SFDRs definition;
c) En produkt som beaktar PAI och där kunden bestämmer vilka kvalitativa eller kvantitativa inslag av PAI som produkten ska ha

Denna information ska rådgivaren inhämta från kund som ett led i lämplighetsbedömningen, i samband med att man diskuterar investeringsmål, tidshorisont, risktolerans etc. Till skillnad från övriga parametrar i lämplighetsbedömningen är hållbarhetspreferenserna helt baserade på kundens önskemål och vilja. Därav finns det inte samma typ av avrådansplikt i de fall där rådgivaren inte har produkter som helt matchar kundens preferenser. Istället finns det möjlighet för kund att ändra sina preferenser inom ramen för vad som kan anses som en i övrigt lämplig produktrekommendation.

Rådgivare ska kunna tillämpa reglerna om hållbarhetspreferenser och integrera dem i rådgivningen genom frågor till kund samt kunna hantera situationer där det inte går att matcha en kunds hållbarhetspreferenser med tillgängligt produktutbud, både vad gäller produkter som omfattas av SFDR och produkter som inte lyder under det regelverket.

Läsanvisningar:

MiFIDs delegerade förordning 2017/565 artikel 54 och 2021/1253 preambel 5-8 samt artikel 1(1) och 1(6)

IDDs delegerade förordning 2017/2359 artikel 9(2) och 2021/1257 preambel 9-15 samt artikel 2(1) och 2(3)

ESMAs riktlinjer för vissa aspekter av lämplighetskraven i MiFID II

- Allmän riktlinje 2, p. 26 – 29
- Allmän riktlinje 8, p. 81 – 85 och 88

FI-tillsyn – Svårt med hållbara råd vid sparande, Nr 29, 28 mars 2024 (Dnr 23-17298)

Flexibelt uttag av tjänstepension

Förslag om flexiblare regler för utbetalning av pension från pensionsförsäkring och pensionssparkonto ska beslutas av riksdagen den 23 oktober.

Idag kan man göra uppehåll med utbetalning av den allmänna pensionen. Detta har dock inte varit möjligt i fråga om utbetalning av tjänstepension och privat pensionssparande, eftersom den så kallade femårsregeln i inkomstskattelagen innebär att en pensionsförsäkring inte får betalas ut under kortare tid än fem år och att utbetalningarna då ska ske med samma eller stigande belopp. Kravet innebär att en pensionär som börjar arbeta igen riskerar att drabbas ekonomiskt av höjd skatt på grund av tjänstepensionen. Framöver blir det dock möjligt att

under de första fem åren göra uppehåll i en påbörjad utbetalning av ålderspension och efterlevandepension från en pensionsförsäkring och att förlänga utbetalningstiden efter att utbetalning har påbörjats. Femårsregeln kompletteras med undantagsbestämmelser som anger hur kommande utbetalningar ska göras om den försäkrade gör ett sådant uppehåll. Vidare ges nya bestämmelser om hur utbetalningstiden ska bestämmas om den försäkrade väljer att förlänga utbetalningstiden efter att utbetalning har påbörjats. Motsvarande ändringar kommer även att gälla för utbetalning från pensionssparkonto. De nya bestämmelserna träder i kraft den 1 januari 2025.

Licenshavaren ska förstå att de nya reglerna innebär att det blir möjligt att under de första fem åren göra uppehåll i en påbörjad utbetalning av ålderspension och efterlevandepension från en pensionsförsäkring och att förlänga utbetalningstiden efter att utbetalning har påbörjats, samt att detsamma gäller utbetalning från pensionssparkonto.

Läsanvisning:

Flexiblare regler för utbetalning från pensionsförsäkring och pensionssparkonto, prop 2023/24:159 (pdf 229 kB)

Skattenyheter

Licenshavaren ska känna till vissa förändringar i budgetpropositionen inom skatteområdet från och med 2025.

Avtrappat ränteavdrag för lån utan säkerheter

Det föreslås att ränta ska dras av bara på lån som uppfyller särskilda förutsättningar gällande värdering av ställda säkerheter och maximal belåningsgrad. Ränta ska dras av på lån med säkerhet i bostad, värdepapper, fordon, båt, skepp eller luftfartyg, samt på lån som har lämnats av en pantbank. Ränta ska också dras av om lånet avser finansiering av ny-, till- eller ombyggnad av en byggnad och avsikten är att lånet när byggprojektet är färdigt ska omvandlas till ett lån med säkerhet i bostad.

Enligt förslaget ska rätten till avdrag för ränteutgifter trappas av på två år. Det innebär att avdrag för beskattningsåret 2025 får göras med 50 procent av ränteutgifter på lån som inte omfattas av avdragsrätten.

Skattefritt sparande på ISK, i kapitalförsäkring och i så kallad PEPP-produkt

Det föreslås en skattefri grundnivå för sparande på investeringssparkonto, i kapitalförsäkring och i så kallad PEPP-produkt som uppgår till 150 000 kronor år 2025 och höjs till 300 000 kronor år 2026.

DORA/Cybersäkerhet

Den 17 januari 2025 ska EU-förordningen för digital operativ motståndskraft (DORA-förordningen) börja tillämpas. Förordningen utgör EU:s mest omfattande regelverk om operativ motståndskraft och cybersäkerhet inom den finansiella sektorn och syftar till att säkerställa att deltagare i det finansiella systemet har vidtagit de skyddsåtgärder som krävs för att motverka cyberattacker och andra it-relaterade risker. DORA innebär nya krav på banker och andra kreditinstitut, försäkringsbolag, värdepappersföretag och övriga företag inom den finansiella sektorn. Utöver detta omfattas även kritiska IKT[1]-leverantörer, inklusive molntjänstleverantörer (CSP:er). DORA utökar även mandatet för EU:s finansiella tillsynsmyndigheter (ESA), vars huvudsakliga uppgift blir att säkerställa att företag blir finansiellt motståndskraftiga och kan upprätthålla verksamheten vid allvarliga driftstörningar. ESA kommer ha befogenhet att begära information, utföra inspektioner samt utfärda rekommendationer, administrativa sanktioner och avhjälpande åtgärder.

DORA innebär omfattande och detaljerade krav på styrelsen och ledningen i finansiella företag att tillse:

- Hantering och styrning av IKT-risker
- Klassificering och rapportering av IKT-relaterade incidenter

[1] IKT - förkortning för informations- och kommunikationsteknik

- Testning av sin digitala operativa motståndskraft
- Hantering av IKT-tredjepartsrisker

Förordningen kompletteras av ett flertal tekniska standarder som närmare specificerar kraven i DORA-förordningen.

Underlåtenhet att följa regelverket medför risk för sanktionsavgift om 1 procent av den genomsnittliga dagliga omsättningen (högst sex månader) för varje dag som reglerna inte uppfylls.

Licenshavaren ska känna till de krav som DORA innebär.

Läsanvisningar:

DORA-förordningen: https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32022R2554

Finansdepartementets faktapromemoria: https://data.riksdagen.se/fil/00B543B1-2CA8-46CD-B386-50BAF0A28282

Värdering av onoterade tillgångar – utmaningar och frågeställningar

Värdering av tillgångar som handlas på en likvid kapitalmarknad är normalt inget större problem rent analytiskt, eftersom marknadspriset på tillgången i fråga är lätt att observera och inte kräver några värderingsantaganden. När det gäller värdering av onoterade tillgångar är situationen däremot mer komplicerad. Två områden där frågan om värdering av onoterade tillgångar är särskilt relevanta är dels då det gäller företag som upprättar koncernredovisning enligt IFRS, dels då det gäller värdering av onoterade aktieinnehav i riskkapitalfonder och investmentbolag.

Koncernredovisningen i noterade bolag följer idag redovisningsprinciperna i det internationella regelverket *International Financial Reporting Standards* (IFRS). Detta regelverk är mycket omfattande och relativt detaljerat, men en standard är av särskilt intresse för externa bedömare på de finansiella marknaderna, nämligen IFRS 13. IFRS 13 handlar om redovisning av verkligt värde, och är särskilt viktigt för noterade fastighetsbolag och noterade bolag som äger skogstillgångar.

Licenshavaren ska känna till principerna bakom redovisning av verkligt värde enligt IFRS 13. Licenshavaren ska känna till varför denna standard infördes, det vill säga. vilka redovisningsmässiga och värderingsmässiga problem som den antas lösa. Licenshavaren ska förstå varför redovisade ”verkliga” värden enligt detta regelverk kan skilja sig från kapitalmarknadens implicita värdering av samma tillgångar vid ett visst tillfälle. Licenshavaren ska även förstå vilka analytiska problem och utmaningar som uppstår då diskrepansen mellan dessa två olika sätt att värdera blir betydande, såsom exemplifieras av situationen för noterade fastighetsbolag under år 2023-2024 .

Vad gäller värdering av onoterade aktieinnehav i riskkapitalfonder och investmentbolag ska licenshavaren på ett övergripande sätt förstå hur sådana innehav brukar värderas. Det innebär att licenshavaren ska förstå grunderna i kassaflödesvärdering, det vill säga. värdering av diskonterade framtida fria kassaflöden med en vägd kapitalkostnad som diskonteringsränta. Licenshavaren ska dessutom förstå hur de vanligaste värderingsmultiplarna är definierade och hur de används som komplement eller alternativ till värdering av fria kassaflöden i värderingssammanhang.

Licenshavaren ska slutligen förstå den viktiga principiella skillnaden mellan ett noterat marknadspris på en tillgång och ett bedömt värde på samma tillgång enligt någon värderingsmodell, det vill säga. skillnaden mellan ”pris” och ”värde”. Licenshavaren ska särskilt förstå vilka antaganden om marknadens funktionssätt, informationshantering och effektivitetsgrad man måste göra för att kunna basera sina placeringsbeslut på skillnader mellan en tillgångs ”pris” och ett bedömt ”värde” enligt en egen värderingsmodell.

Kapitaltäckningsregler för kreditinstitut och vissa värdepappersbolag

Från 1 januari 2025 träder ändrade regler om kapitaltäckning för kreditinstitut och vissa värdepappersbolag i kraft. Nu gällande kapitaltäckningsdirektiv (2013/36/EU) och tillsynsförordning (575/2013/EU) har uppdaterats. Förslag till hur direktivet ska genomföras i svensk rätt kommer att publiceras under hösten 2024.

De nya reglerna ställer, liksom dagens regler, vissa minimikrav på ett instituts kapital. Det görs ändringar i nuvarande metoder för att beräkna kapitalkrav och helt nya metoder införs. Ändringarna innebär att kapitalkrav för operativa risker inte längre får beräknas med interna modeller. De nya reglerna innehåller även krav på att institut som använder en intern modell för att beräkna kapitalkrav för kreditrisk och/eller marknadsrisk ska uppfylla ett minimikapitalkrav baserat på schablonmetoderna.

Licenshavaren ska därför förstå innebörden av dessa nya och ändrade metoder för att beräkna kapitalkrav för kreditrisker, marknadsrisker respektive operativa risker.

Läsanvisningar:

EU publicerar andra bankpaketet | Finansinspektionen

Tema – risker och sårbarheter i det finansiella systemet

1. Inledning

Det finansiella systemet är en väl integrerad del av såväl medborgarnas vardag som samhällsekonomin i stort. De risker som det finansiella systemet och dess användare utsätts för speglar vid var tid samhällsutvecklingen i stort. Systemet har, liksom samhället i övrigt, under senare år blivit mer sårbart och utsatt för olika relativt nya typer eller nya varianter av brottslighet. Brottsligheten är i hög grad sammankopplad med den tekniska utvecklingen, exempelvis vad gäller metoden för betalningar och överföring av pengar. En annan del av utvecklingen är att brottsligheten i allt större omfattning har blivit organiserad och kopplad till kriminella nätverk med stora resurser.

Brottsligheten riskerar att allvarligt skada såväl de enskilda medborgarna som samhället – inklusive det finansiella systemet – i stort. Mot den bakgrunden finns det nu skäl att i denna årliga kunskapsuppdatering belysa delar av den kriminalitet som riktas mot det finansiella systemet och huvudriskerna med denna.

De företeelser som beskrivs nedan träffas ofta av olika regelverk, vilka exempelvis kan ställa detaljerade krav på hur de finansiella företagen eller deras anställda ska agera i vissa situationer. Här bör särskilt nämnas EU:s förordning för digital operativ motståndskraft (DORA-förordningen), som ska börja tillämpas i hela EU den 17 januari 2025, och som bland annat innebär ökade krav på finansiella företag inom EU att övervaka och rapportera sina risker inom informations- och kommunikationsteknologi.

Syftet med genomgången är inte att licenshavarna ska få detaljkunskap om dessa regelverk utan att licenshavarna ska tillägna sig viss elementär kunskap, främst om de aktuella begreppen och brottsmetoderna. Härutöver är tanken att licenshavaren ska få uppslag för att reflektera över risker som kan uppstå i olika arbetssituationer och för hur man ska agera och förhålla sig till dessa, exempelvis om det inte finns några instruktioner eller något givet rätt eller fel. Materialet lämpar sig därför för olika pedagogiska grepp. Utöver den webbaserade utbildningen får företagen gärna komplettera med till exempel workshops eller diskussionsseminarier, anpassade efter den verksamhet som varje företag bedriver. Med hänsyn till detta har vi inte angett några exakta kunskapsmål. Under varje avsnitt har vi dock formulerat några punkter som kan vara till stöd för läsaren. Tanken är även att de webbaserade utbildningarna ska genomföras i sin helhet för att ge licenshavarna möjlighet att reflektera kring dessa frågor.

Det bör nämnas att penningtvätt och terrorismfinansiering endast berörs i förbigående i redogörelsen.

2. Kort om det finansiella systemets roll i samhället

Det finansiella systemet spelar en central roll i samhället och är en samhällsviktig funktion. Systemet möjliggör bland annat snabba och effektiva betalningar och en effektiv allokering av pengar och andra tillgångar. Det gör det möjligt för företag och allmänheten att spara på bankkonton, investera i värdepapper eller att hitta finansiering genom att uppta lån. Vidare kan företag och staten/kommuner kapitalisera sig genom att ge ut värdepapper på värdepappersmarknaden.

Det är mot den bakgrunden viktigt för såväl enskilda privatpersoner som för företag och samhället i stort att det finansiella systemet är stabilt, effektivt och tryggt samt att samtliga aktörer känner ett stort förtroende för systemet.

3. Allmänt om risker inom det finansiella systemet samt om detta dokument

Det finansiella systemet har i alla tider varit utsatt för olika typer av hot. Hotbilden har sett olika ut under olika tider, inte minst beroende på den tekniska utvecklingen i samhället. Under det senaste decenniet har hotbilden i hög grad förändrats, till följd av den snabba utvecklingen inom IT. Riskerna har i stor utsträckning förflyttats från den fysiska till den digitala världen. En rad tekniker och funktioner har utvecklats för att underlätta och effektivisera kundernas och de finansiella aktörernas hantering av transaktioner och övriga dispositioner i det finansiella systemet och även hos olika betaltjänstleverantörer på internet. Detta har i grunden förändrat kundernas beteenden och har i hög grad medfört en snabbare och smidigare hantering. Utvecklingen går snabbt och kunderna förväntar sig att företagen erbjuder nya lösningar i takt med den.

Utvecklingen har dock även gjort de finansiella företagen och kunderna mer exponerade för olika typer av bedrägerier och integritetsintrång. Bankerna och de övriga finansiella företagen har byggt upp omfattande säkerhetsfunktioner mot detta. Det har gjort att bedragarna, snarare än att utnyttja säkerhetsbrister i betaltjänsterna, i stället har kommit att främst inrikta sig på att manipulera kunderna. Riskerna har därmed i hög grad inte bara förflyttats från den fysiska till den digitala världen utan även från de finansiella företagen till kunderna. Bedrägerier genom sådan så kallad social manipulation har också ökat mest under senare år och står i dag för den största delen av de belopp som bedragarna lurar till sig.

För de finansiella företagen innebär utvecklingen, mot denna bakgrund, också att det löpande måste ske en avvägning mellan smidighet och kundvänlighet å ena sidan och tröghet och ökad säkerhet å andra sidan.

Att bli utsatt för ett bedrägeri kan innebära stora ekonomiska förluster för den som blir bedragen samtidigt som de ekonomiska vinsterna från bedrägerierna göder den kriminella ekonomin. Det är ofta äldre personer som drabbas av bedrägerierna. Utöver den ekonomiska förlusten som bedrägeriet innebär, upplever brottsoffren ofta skam och skuldkänslor. Att motverka bedrägerier är därför en viktig uppgift för de finansiella företagen.

Nedan redogörs för olika typer av bedrägerier och andra risker som förekommer inom det finansiella systemet.

Redogörelsen är inte uttömmande. Avsnitt 4 och 5 har främst utgått från de risker en investeringsrådgivare kan beröras av i sitt arbete, varvid huvudfokus har legat på risker som kan drabba företagets kunder, det vill säga risker ur ett kundperspektiv. Det kan även röra sig om risker som främst är kopplade till kunderna och som kan få återverkningar på kundernas situation och därmed även på de finansiella företagens arbete.

I avsnitt 6 behandlas kreditbedrägerier. Avsnittet är främst relevant för de som arbetar direkt med kreditfrågor men även övriga yrkeskategorier kan beröras och bör ha en grundläggande kännedom om riskerna på området.

Förutom kunskap om de typer av bedrägerier och liknande som kan drabba kunder är det viktigt att licenshavarna även har en god allmän bild av de mer generella och systemhotande risker som finns, varför även vissa sådana berörs. De handlar dels om avsnitt 7, Möjliggörare och brottslighet kopplad till kriminella nätverk, dels om avsnitt 8, Välfärdsbrottslighet.

4. Viktiga bedrägerirelaterade risker (utom kreditbedrägerier)

Allmänt

Den gemensamma nämnaren för ett bedrägeriupplägg är försöket och viljan att påverka och förmå kunden att göra något: exempelvis klicka på en länk, genomföra en betalning eller ringa ett telefonnummer.

Bedragaren har ofta kontakt med brottsoffret under en längre tid för att bygga förtroende. Ofta använder bedragarna sig av tillgänglig publik information för att kartlägga sina brottsoffer. De har många gånger god kännedom om det aktuella finansiella företagets (exempelvis kundens banks) säkerhetssystem, vilket ger dem ökad trovärdighet hos brottsoffren.

Ett bedrägeri genomförs antingen genom att bedragaren förmår brottsoffret att själv göra transaktionen, som då blir en så kallad behörig transaktion, eller genom att bedragaren genomför transaktionen utan samtycke från konsumenten, så kallad obehörig transaktion, eller manipulerar konsumentens transaktion på något sätt. Det är alltså fråga om bedrägeri genom så kallad social manipulation.

Om en kund har förmåtts att självmant genomföra en behörig transaktion genom social manipulation, får konsumenten i dag (hösten 2024) ofta ingen ersättning. Majoriteten av förlusterna som uppstår genom bedrägerier bärs därför i dagsläget av konsumenter. Äldre konsumenter är särskilt drabbade.

En betalning eller annan åtgärd som är signerad av kunden med så kallad stark kundautentisering är som huvudregel en behörig transaktion. Med stark kundautentisering avses förenklat en autentisering som grundas på användning av två eller flera komponenter – exempelvis vetskap om något som bara användaren känner till eller något som bara användaren har – och som är fristående från varandra så att förhållandet att någon obehörig har kommit över en av komponenterna inte äventyrar de andra komponenternas tillförlitlighet.

Flera av de risker som beskrivs nedan har inte, eller har inte alltid, en direkt påverkan på kundens mellanhavanden med det finansiella företaget. Eftersom riskerna i hög grad är relaterade till kundens ekonomi och ekonomiska trygghet är det likväl viktigt att företagets medarbetare känner till riskerna.

Vishing (telefonbedrägeri)

Bedragaren ringer upp en kund som under telefonsamtalet blir lurad att antingen lämna ifrån sig koder från sin säkerhetsdosa eller att identifiera sig eller signera uppdrag med sin e-legitimation. Kunderna luras idag ofta att utföra transaktionerna själva, exempelvis under förevändning att pengar behöver föras över till ett ”säkert konto”. Det förekommer även att kunder luras att signera nytt BankID för bedragaren som sedan har access till kundens Internetbank och kan ansöka om krediter och genomföra transaktioner.

Bedragare döljer sig ofta bakom ”spoofade” telefonnummer, det vill säga maskerade nummer där bedragaren själv väljer vilket telefonnummer som ska uppvisas i offrets display, för att det ska framstå som att det exempelvis är en bank som kontaktar sina kunder.

Det finns i dag (hösten 2024) inga krav på att myndigheter eller banker ska kunna styrka sin identitet och behörighet i ett telefonsamtal, så att det går att verifiera vem som ringer. Detta möjliggör för bedragare att hävda att de ringer från till exempel en bank.

Smishing-bedrägeri (falska sms)

Bedragaren skickar ett sms till en konsument med information som ska få kunden att göra något. Bedragarens avsikt är att skapa en stressad situation där kunden måste agera snabbt. Antingen ska kunden ringa ett telefonnummer, installera programvara eller följa en länk och lämna ut information. Vanliga upplägg är sms med information om ”misstänkt aktivitet på kort eller konto”, eller sms från ”mamma som har bytt telefon och behöver hjälp”.

Det är vanligt att ett vishing/telefonbedrägeri kombineras med smishing/falska sms. Detta sker ofta genom att ett sms från en fejkad aktör 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”. Härefter kan kunden exempelvis förmås att godkänna en viss transaktion via internet. I samband med detta kan kunden luras att installera fjärrstyrningsprogramvara på sin telefon eller dator, vilket ger bedragaren full access och kontroll över skärm och tangentbord. Bedragaren kan därefter lägga upp transaktioner i kundens bank som kunden sedan luras att signera.

Investeringsbedrägeri

Bedragaren kontaktar en konsument och erbjuder en påhittad investeringsmöjlighet, alltid med inslag av hög avkastning till låg risk, ofta på kort tid. Kontakten sker ofta genom telefonsamtal men erbjudanden kan även lämnas via sms, e-post eller sociala medier.

Inte sällan blir kunden utsatt för ett så kallat återvinningsbedrägeri, det vill säga att kunderna luras på nytt, antingen på samma sätt eller genom att de vilseleds att de kan få tillbaka pengar från ett tidigare investeringsbedrägeri.

Romansbedrägeri

Konsumenten blir kontaktad och uppvaktad av en bedragare. För bedragaren handlar det om att nå människor i situationer där de är sårbara, och kärlek är en stark drivkraft.

Bedrägerier med stöd av artificiell intelligens och deep fakes

Genom den senaste tekniken inom artificiell intelligens är det möjligt att framställa förfalskade videor, bilder eller ljud som är så genomarbetade att de framstår som äkta, så kallade ”deep fakes”. Användningen av deep fakes för bedrägliga syften är ett växande hot i samhället. Deep fakes skulle exempelvis kunna användas som ett verktyg för att imitera kunder eller personer i ledande position gentemot exempelvis bankpersonal inom betalningsområdet. Målet skulle kunna vara att genomföra bedrägliga betalningar. Detta hotområde är sannolikt bara i sin linda, men det förekommer redan att bedragare använder sig av ett automatiserat och robotiserat arbetssätt, exempelvis att automatiserade konversationer förekommer i vissa bedrägeriupplägg via sociala medier och chat-appar.

En deep fake innebär förstås inte i sig att ett bedrägeri genomförs. Eftersom det kan vara ett effektivt verktyg för en bedragare har vi dock här inkluderat en text om detta.

Uppslag för reflektion och övningar:

- Vilka huvudsakliga risker skulle kunna uppstå för företagets kunder, relaterade till dina arbetsuppgifter och i den verksamhet du arbetar?
- Kan du och företaget göra något för att förebygga riskerna? Kan man göra något för att lindra konsekvenserna av en realiserad risk, till exempel ett bedrägeri mot en kund?

5. Att tänka på vid misstankar om bedrägeri mot kund

När det gäller att förebygga bedrägerier så bör man hålla i huvudet att många kunder, inte minst äldre personer, har bristande kunskap om IT och hur det tekniska fungerar. Det innebär att företaget bör försöka skapa sig en bild av kundens kunskap och kompetens samt, om sådan saknas, tydligt utbilda och informera kunden om hur produkter och tjänster fungerar och hur företaget arbetar (det är exempelvis vanligt att företag inte ber en kund identifiera sig utan att kunden först kontaktat företaget).

Detta är främst företagets ansvar men även den enskilda rådgivaren bör sträva efter att uppfylla det, exempelvis genom att inte dra sig för att fråga kunden om dennes kunskaper eller ge grundläggande råd och tips om tekniken. Rådgivaren kan även hänvisa kunden till de etablerade hemsidor mm som finns för att hjälpa konsumenter, såsom den egna bankens hemsida, bankernas gemensamma hemsida Svårlurad, https://www.svarlurad.se.

När det gäller investeringsbedrägerier innehåller Finansinspektionens hemsida bra information om hur ett bedrägeri kan gå till i praktiken och hur kunder ska undvika att bli lurade, se https://www.fi.se/sv/konsument-skydd/investeringsbedragerier/sa-kan-det-ga-till/. Finansinspektionen har även en varningslista som bland annat omfattar företag som används för investeringsbedrägerier, se https://www.fi.se/sv/vara-register/fis-varningslista/

I övrigt gäller att rådgivaren bör visa uppmärksamhet (på engelska används ofta begreppet awareness) och bör ha ett kritiskt förhållningssätt, det vill säga att rådgivaren ska fråga sig om agerandet är rimligt utifrån kundens förutsättningar, historik med mera samt vid behov ska ställa kontrollfrågor till kunderna, allt för att säkerställa att kundens transaktioner är korrekta.

Det är alltså viktigt att vara uppmärksam på och tolka kundernas beteende, för att på så sätt kunna upptäcka ett avvikande beteende.

Uppslag för reflektion och övningar:

- Hur skulle du agera om du ser tecken på att en kund utsätts för ett bedrägeri? Om bedrägeriet riktas mot det egna företaget?
- Hur skulle du och din arbetsgivare kunna på bästa sätt informera kunderna (exempelvis om företagets arbetsrutiner) för att minska risken för att de luras av bedragare?
- Vad är centralt för ett kritiskt förhållningssätt just för dina arbetsuppgifter?

6. Kreditbedrägerier

Allmänt

Ett kreditbedrägeri innebär att någon ansöker och beviljas en kredit på felaktiga grunder, främst så att personens kreditvärdighet framstår som väsentligt bättre än den i själva verket är. Det är sedan lång tid en mycket vanligt förekommande företeelse, som numera underlättas av snabba digitala förfaranden för låneansökning, ofta inom ramen för de framväxande snabb- och blancolånemarknaderna.

En rad olika uppgifter kan påverka utfallet av en kunds kreditansökan, exempelvis falska arbetsgivarintyg eller lönespecifikationer samt manipulerade kontoutdrag. Att knyta samman förståelsen för de olika uppläggen av kreditbedrägerier i alla delar av kreditens förlopp – från ansökan till återbetalning – är därför ofta utmanande.

Ett vanligt förekommande upplägg innebär 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. Bedragaren drar nytta av att de olika kreditgivarna inte kan utbyta information, det vill säga före den tidpunkt uppgifter börjar synas i kreditupplysningarna. Det kan gälla såväl regelrätta lån som kreditköp.

Idag (hösten 2024) är det möjligt för bedragare att registrera falska uppgifter om inkomst hos svenska myndigheter, vilket kan försvåra möjligheten för kreditgivarna att förlita sig på och bedöma tillförlitligheten i uppgifterna rörande identiteter och familjeförhållanden.

Det finns även risker kopplade till betalning, avbetalning och lösen av krediter. All betalning av krediter bör kontrolleras mot uppgifterna avseende kundkännedom. Om medlens ursprung är tvivelaktigt finns det risk att kreditgivaren tar emot medel från penningtvättsupplägg och då hamnar kreditgivaren i en svår situation för hur kundförhållandet ska hanteras.

När det gäller företagskrediter handlar det ofta om att företaget tar många parallella olikartade krediter under den tid företaget kan användas som brottsverktyg, det vill säga under den tid som felaktiga uppgifter om kreditvärdighet uppges i de kontroller som genomförs av kreditgivare. Det är fråga om att ta regelrätta företagslån, andra snabbare företagskrediter, genomföra stora kreditinköp av dyra varor såsom maskiner, redskap eller fordon. Det är i allmänhet en målvakt som står som företrädare för det företag som tar krediten.

Uppslag för reflektion och övningar:

- Har ska du och den verksamhet du arbetar i kunna identifiera tecken på att det kan vara fråga om ett försök till kreditbedrägeri? Vilka förhandskontroller kan genomföras och vad bör ett kritiskt förhållningssätt inbegripa?
- Vad kan vara tecken på att någon bolagsföreträdare är målvakt?

7. Möjliggörare och brottslighet kopplad till kriminella nätverk

Allmänt om möjliggörare och kriminella nätverk

Organiserad brottslighet med stort våldskapital påverkar idag i princip alla delar av samhället och därigenom även finansiella företag. Vissa moment i den kriminella verksamheten förutsätter eller underlättas väsentligt av att så

kallade möjliggörare anlitas. Med en möjliggörare avses en person som utnyttjar sin anställning för att hjälpa kriminella nätverk. En möjliggörare kan finnas såväl i statlig, kommunal som privat sektor.

Ibland används även begreppet insiders. Insiders för dock även associationerna till insiderbrott, det vill säga där personer använt så kallad insiderinformation för att göra vinster på värdepappersmarknaden. (En sådan person kan vara, men är inte alltid, en möjliggörare.) Nedan används därför endast termen möjliggörare.

När det gäller finansiella företag kan en möjliggörare utnyttja sin insyn i företaget för att exempelvis genomföra olagliga transaktioner eller manipulera finansiella flöden, på uppdrag av kriminella. Det finns ett flertal exempel där bankanställda tros ha hjälpt kriminella att utforma trovärdiga ansökningar för olika typer av krediter med hjälp av felaktiga inkomstuppgifter. Möjliggörare kan även bidra med att hantera och använda brottsvinster samt göra dessa svårare att spåra, och minska risken att transaktioner fastnar i kontroller.

Beträffande stora systemviktiga finansiella företag, såsom de så kallade storbankerna, kan det även tänkas att främmande stater försöker använda möjliggörare för att samla underrättelser, destabilisera ekonomin eller påverka politiska beslut.

Möjliggörares handlingar kan alltså underlätta, effektivisera och diversifiera den kriminella affärsverksamheten. Det medför att fler personer riskerar att drabbas av brott och kan bidra till att upptäcktsrisken minskar, vilket innebär att brottsligheten kan pågå under längre tid. Det förstärker även de kriminella nätverken, vilket ger dem möjligheter att fortsätta och utöka sin brottsliga verksamhet, inte minst genom att rekrytera fler möjliggörare och ytterligare infiltrera myndigheter och företag.

En möjliggörare kan användas för en specifik del av ett brottsupplägg. Rollen kan även innebära att möjliggöraren samarbetar med andra möjliggörare, exempelvis om en banktjänsteman och en mäklare hjälps åt för att möjliggöra fastighetsköp med brottsvinster.

Det är självklart inte tillåtet för någon anställd att medvetet möjliggöra eller underlätta kriminell verksamhet. Om så sker är det inte givet att agerandet är brottsligt men tröskeln för brottslig och straffbar medverkan till andras brottslighet är tämligen låg – det räcker att personen har, som det heter, främjat den brottsliga gärningen med råd eller dåd. Medhjälpen kan bestå i praktiskt bistånd (som varken behöver vara av nödvändig eller väsentlig art) men det kan i vissa fall räcka med mentalt stöd som uppmuntrar gärningsmannen att begå brottet. Det betyder att exempelvis en banktjänsteman som rent praktiskt utför en betalning på uppdrag av någon och förstår att pengarna kommer från kriminell verksamhet gör sig skyldig till brottslig medverkan till penningtvätt.

Vem blir möjliggörare?

Det går inte att enkelt karaktärisera vem som är eller riskerar att bli en möjliggörare. I många fall finns en tydlig social koppling. Möjliggöraren kan då exempelvis tillhöra samma familj eller släkt eller vara barndomsvän till personer i kriminella nätverk. Möjliggöraren behöver dock inte alltid ha någon sådan koppling. Istället för sociala lojaliteter kan det handla om att personen har andra sårbarheter – såsom ekonomiska problem eller olika former av kostsamma missbruk (av till exempel narkotika eller spel) – vilka kan göra individen mer sårbar för förfrågningar, hot och påtryckningar från kriminella nätverk. Möjliggörarna kan ha en livsstil där de spenderar pengarna snabbt, men det är heller inte givet. Oavsett konsumtionsnivå skapar ersättningen dock ofta nya behov av pengar och blir ett tydligt motiv till att fortsätta som möjliggörare.

Förebyggande arbete

För att upptäcka potentiella möjliggörare genomför flera olika offentliga och privata verksamheter i dag bakgrundskontroller av de sökande redan innan de börjar på arbetsplatsen. Det handlar exempelvis om att kontrollera den sökandes identitet, arbetslivserfarenhet och utbildning.

För arbetsgivare är det viktigt att ha beaktat kriminella nätverks potentiella intresse av möjliggörare i sin risk- eller säkerhetsskyddsanalys. De risker som identifieras behöver kopplas till typer av befattningar, och omsättas i kravprofiler för nya tjänster och uppdragsbeskrivningar. Riskbedömningen bör styra vilka behörigheter som funktionerna ges, både i fysiska lokaler och i informationssystem. Det inkluderar exempelvis en översyn av vilka

personer som har tillgång till lokaler, it-system, utrustning, information och möten. Man bör även se över om det finns yrkesroller, tjänster eller positioner som skulle kunna vara intressanta för personer i kriminella nätverk.

En av möjliggörarnas främsta uppgifter är att lämna ut information. Inte sällan är den informationen av skyddsvärd karaktär. Att se över tillgången till information inom en verksamhet är därför centralt, till exempel genom åtkomstbegränsning och loggning av vem som tagit del av vilken information.

Det kan vidare vara viktigt att se över tjänster där ensamarbete förekommer och vilka arbetsuppgifter som lämpar sig för distansarbete. Ensamarbete utgör inte bara en högre risk för felaktigheter, det gör även enskilda medarbetare extra sårbara för närmanden från personer i kriminella nätverk. På samma sätt innebär även ökat distansarbete en högre risk. Det kan här exempelvis vara befogat med begränsningar som innebär att alla uppgifter inte går att komma åt vid distansarbete.

En vanlig förebyggande åtgärd mot korruption är fyraögonsprincipen eller dualitetsprincipen. Det kan vara ett bra verktyg mot möjliggörare. Om åtminstone en annan person gör en reell granskning av det ifrågavarande beslutet och underlaget kan det försvåra att den först inblandade vinklar beslutet, till kriminella nätverks fördel. Även rotering av anställda inom eller mellan närliggande funktioner kan utgöra ett skydd mot att någon agerar som möjliggörare, i och med att den ansvariga byts ut med jämna mellanrum.

Det kan också ha en förebyggande effekt om otillåtna slagningar och sökningar kan flaggas och utredas skyndsamt.

Möjliggörare kan vara duktiga på sitt jobb, och dessutom trevliga och omtyckta. Trots att möjliggörare många gånger frångår riktlinjer och ordinarie arbetsrutiner kan det därför krävas ett mönster av flera små avsteg för att arbetsgivaren ska kunna identifiera felaktigheterna.

När det gäller förmågan att förebygga och förhindra att kriminella nätverk utnyttjar möjliggörare är det, på ett allmänt plan, viktigt att arbetsgivare dels stärker sin egen kunskap om företeelsen, dels sprider kunskapen till både chefer och medarbetare.

Genom utbildning om företeelsen kan företaget medvetandegöra arbetstagare och chefer, så att de kan känna igen oegentligheter och interna brott och vågar agera på signaler om dessa. Om personalen har fått god kännedom blir det svårare för såväl möjliggöraren som dennes kollegor att påstå att de inte visste vad som gällde.

För vissa yrkesroller med nära och återkommande kontakt med personer som skulle kunna tillhöra kriminella nätverk kan utbildningen lämpligen innehålla moment där de får öva på dessa kontakter för att öka sin motståndskraft mot manipulation.

Utbildningar kan också handla om att förbättra verksamhetens säkerhetskultur eller öka kunskapen om yrkesrollens värdegrund och mål. Genom att arbeta kontinuerligt med värdegrundsfrågor kan arbetsgivare påverka medarbetarnas syn på företaget och dess roll i samhället. Det handlar om att skapa gemensamma sätt att tänka och agera när det gäller risk och säkerhet i de komplexa situationer där misstankar om otillåten påverkan eller om möjliggörare uppstår. Med en tydlig värdegrund kan medarbetare i högre grad än annars även vägledas i hur de ska agera i situationer där det inte finns förbestämda rutiner att följa.

Det är vidare viktigt att ansvars- och rutinbeskrivningar innehåller tydliga beslutskedjor och tydlig ansvarsfördelning, eftersom det försvårar för möjliggöraren att hitta bortförklaringar och lägga skulden på något annat.

Ytterligare en betydelsefull faktor är ett gott och tryggt arbetsklimat. Ett sådant brukar öka känslan av lojalitet till företaget, vilket minskar sårbarheten för att bli möjliggörare.

Upptäckt och rapportering

Att upptäcka möjliggörare kan ta lång tid och misstankar är ofta svåra att bevisa. Upptäckt torde ofta förutsätta att företaget systematiskt granskar och kontrollerar verksamheten utifrån sin riskanalys rörande möjliggörare.

Inte sällan har uppmärksamma kollegor och chefer i verksamheten bäst förutsättningar för att uppmärksamma möjliggörare. Rutiner bör finnas för intern incidentrapportering och hantering av incidenter som rör möjliggörare. (Att det dessutom kan vara en känslig fråga när kollegor agerar på ett felaktigt sätt förstärker förstås behovet av

tydliga rutiner). Vissa typer av signaler, exempelvis om mutor, utpressning, hot, jäv och olämpliga relationer kan lämpa sig för visselblåsarsystem.

När det finns skäl att anta att brott har begåtts kan det finnas anledning (och ibland skyldighet, såsom vid misstanke om penningtvätt och insiderbrott eller marknadsmanipulation) att anmäla det till polisen, men även andra myndigheter kan vara aktuella, som Ekobrottsmyndigheten, Finansinspektionen och Skattebrottsenheten inom Skatteverket.

Även när ingen brottsanmälan görs finns möjligheter att uppmärksamma rättsväsendet om handlingen. Exempelvis kan möjliggörare som misstänks bistå kriminella med penningtvätt rapporterats till Finanspolisen med stöd av penningtvättslagstiftningen.

Beträffande anställda som innehar Swedsec-licens, för närvarande runt 25 000 anställda i olika befattningar i finanssektorn, har de anslutna företagen även en skyldighet att anmäla regelöverträdelser som är kopplade till arbetsuppgifter som kräver licens till Swedsec. Swedsec prövar därefter frågan och om agerandet bedöms vara en överträdelse påförs den anställde sanktioner. Besluten fattas av Swedsecs disciplinnämnd och blir offentliga.

Uppslag för reflektion och övningar:

- Skulle en möjliggörare kunna användas till något brottsligt i den verksamhet där du arbetar? Kopplat till dina arbetsuppgifter?
- Vilka beslut och ageranden är särskilt känsliga och samtidigt svåra att upptäcka eller kontrollera?
- Kan företaget eller du själv göra något mer för att förebygga att möjliggörare får inflytande i verksamheten?
- Har företaget (och du själv) en tydlig värdegrund? Fungerar den som hjälpmedel mot illojala eller brottsliga ageranden? Är den en viktig del i företagets arbetskultur? Finns det brister eller förbättringspotential?
- Finns det i företaget goda och tillförlitliga rutiner för intern rapportering av misstänkta oegentligheter? Vad kan göras för att göra processen smidigare och säkrare för den som anmäler?

8. Välfärdsbrottslighet

När nya bidrag eller stöd från det allmänna inrättas drar det till sig intresse från kriminella – något som tydligt visat sig vid exempelvis utbetalningarna av ekonomiska stöd under covidpandemin, elstöd samt olika ekonomiska stöd relaterade till miljöbefrämjande åtgärder.

Rent praktiskt kan det exempelvis handla om att myndigheter har lurats att fatta och verkställa beslut om felaktiga utbetalningar av sjukpenning och andra bidrag eller ersättningar samt om mervärdesskatt. Kanske står det helt klart för exempelvis en bank att en kund som är egen företagare har utfört arbete samtidigt som denne uppbär ersättning på grund av sjukfrånvaro, vård av barn eller vård av sjukt barn.

Ofta sker brottet med stöd av en möjliggörare som även aktivt konstruerat ärenden och underlag så att det verkar som om besluten fattats på korrekta grunder. I vissa enskilda fall kan det röra sig om utbetalningar i mångmiljonklassen och sammantaget omfattar kriminellas utnyttjande av välfärdssamhället – välfärdsbrottsligheten – mycket stora summor.

Välfärdsbrottsligheten utgör en särskild utmaning för banker och andra finansiella företag eftersom utbetalningarna kommer från myndigheter, det vill säga avsändare med högt förtroende.

Det är svårt för finansiella företag att kontrollera om det rör sig om en bakomliggande brottslighet där myndigheter har lurats till utbetalning på felaktiga grunder. Mottagarna är dessutom i allmänhet vanliga personer eller företag, varför det saknas anledning att misstänka att de inte skulle ha rätt att ta emot pengarna.

Kontrollerna måste därför i första hand göras av den beslutande eller utbetalande myndigheten. Från och med 2024 har en ny myndighet, Utbetalningsmyndigheten, inrättats. Utbetalningsmyndigheten ska kontrollera utbetal-

ningar från välfärdssystemen och kan därmed förväntas bidra till ökad övervakning och kontroll av välfärdsbrottslighet.

De finansiella företagen har inte någon laglig skyldighet att anmäla exempelvis misstänkta bidragsbrott till myndigheterna. (På begäran av vissa myndigheter måste banker och andra penninginrättningar dock lämna ut annars sekretessbelagda uppgifter, som exempelvis har relevans i ärenden om bostadsbidrag och bostadstillägg.)

Företagen och dess medarbetare bör ändå så lång möjligt ändå bidra i kampen mot välfärdsbrottsligheten. En central fråga är här hur detta förhåller sig till banksekretessen (eller motsvande för andra finansiella företag). Den är som bekant mycket stark. Den är dock inte absolut - kundens förhållanden får röjas om det inte sker obehörigen. En polisanmälan utgör förstås inte något obehörigt röjande om det, såsom vid misstanke om marknadsmissbruk (insiderbrott eller marknadsmanipulation) eller penningtvätt, finns en lagstadgad skyldighet för företaget att anmäla misstankar.

Inte heller när sådan skyldighet saknas sträcker sig banksekretessen så långt att den skyddar personer som enligt företagets vetskap eller misstanke har begått ett brott. Om misstankarna är väl grundande kan det inte anses obehörigt att göra en brottsanmälan och överlämna nödvändiga upplysningar om en kund. (se Per-Ola Jansson, Banksekretess och annan Finansiell sekretess, s 149).

Det innebär inte att företaget har en underförstådd generell skyldighet att anmäla brottsmisstankar till myndigheterna. Att sådan skyldighet inte finns innebär emellertid inte att det i alla tänkbara situationer - oavsett omständigheter och typ av brottsmisstanke - förefaller givet att företagets inställning bör vara att det inte är företagets uppgift att upptäcka och anmäla brott, och att någon myndighetskontakt följaktligen inte ska tas. I den bedömningen synes såväl etiska som kommersiella aspekter (exempelvis kopplade till företagets renommé eller status som tillståndspliktigt företag) kunna komma att aktualiseras. Det är mot den bakgrunden fördelaktigt om företaget är förberett på denna typ av ställningstaganden, exempelvis genom att företagets förhållningssätt klargörs i en intern riktlinje eller en policy.

Uppslag för reflektion och övningar:

- Innebär dina arbetsuppgifter eller ditt företags tjänster att du/företaget får del av information som kan tyda på att en kund ägnar sig år välfärdbrottslighet?
- Kan den som begår välfärdbrottslighet utnyttja företagets tjänster för att underlätta brottsligheten?
- Kan du eller företaget förändra arbetsmetoderna så att det blir svårare att för kunderna att begå välfärdsbrottslighet?
- Vilka krav bör här ställas på företaget, internt och från samhällets sida, när det gäller att anmäla misstänkt brottslighet (i de fall där det saknas regler om anmälningsplikt)? Vilka hinder reser banksekretessen?
- Finns det inom företaget instruktioner eller rutiner för hur personalen ska agera vid misstankar om välfärdsbrottslighet?

9. Informations- och cybersäkerhet

I detta avsnitt beskrivs några risker relaterade till informationssäkerhet och cybersäkerhet. (Här kan påminnas om att DORA-förordningen, som ska tillämpas fr o m 17 januari 2025, kommer medföra högre krav på de finansiella företagen att hantera och rapportera risker inom informations- och kommunikationsteknologi.)

Ransomware-attacker

En ransomware-attack, eller utpressningsangrepp, är ett program där aktören krypterar sina offers data tills en lösensumma är betald. Det förekommer även att kriminella inte bara krypterar data utan även stjäl data i samband med attacken och hotar med att lägga ut informationen publikt på internet om inte lösensumman betalas. Ransomware-attacker kan vidare medföra informationsförluster.

Under senare år har ransomware-attacker drabbat ett stort antal verksamheter både i Sverige och internationellt och därmed fått stor uppmärksamhet i media. Bland de drabbade är it-bolaget TietoEvry. Attacken mot det bolaget fick omfattande följder för ett stort antal kunder till bolaget. Fallet exemplifierar vad som kan inträffa när koncentrationer av kritiska tjänster byggs upp hos enskilda leverantörer.

Omfattande ransomware-attacker mot finansiell sektor skulle kunna få mycket stor påverkan. Studier och analyser från bland annat Riksbanken visar att en tillräckligt stor cyberattack mot finansiell sektor skulle kunna hota den finansiella stabiliteten.

De finansiella företagen behöver löpande bevaka och utvärdera ransomware-hotet och att förbättra sina skyddsåtgärder. Om en attack skulle ske måste företaget ha utvecklat åtgärder för att kunna upptäcka, hantera och återställa verksamheten. TietoEvry-fallet understryker att företaget behöver ha en god förståelse rörande vilka koncentrationsrisker de är utsatta för, om de har lagt ut delar av sin it-verksamhet.

Mer information samt tips och råd finns i Nationellt cybersäkerhetscentrums Temafördjupning Utpressningsangrepp Juni 2024, se https://www.ncsc.se/siteassets/publikationer/utpressningsangrepp---temafordjupning.pdf

Överbelastningsattacker

Nätverk och enheter som är kopplade till internet utsatts ofta för konstanta angrepp. En sådan vanlig typ är överbelastningsattacker, det vill säga attacker för att påverka internettjänsters och webbplatsers tillgänglighet, exempelvis genom att man överbelastar uppkopplingar och webb med trafik så att systemen går i baklås.

Attackerna genomförs i regel av ideologiskt motiverade hotaktörer. Dessa är organisationer, enskilda individer eller grupper som utför attackerna för att ta parti för någon sida i en konflikt eller samhällshändelse. Att protestera med överbelastningsattacker är då ett billigt och effektivt sätt att orsaka störning i det samhället och skapa uppmärksamhet för sin fråga.

Aktörerna kan även ha anknytning till främmande makt och kriminella organisationer. Syftet med attackerna kan då vara mer övergripande, att påverka medborgarna genom att försöka visa att samhällsviktiga finansiella tjänster är i fara. Attackerna har hittills haft en begränsad effekt men utgör likväl ett hot mot samhället och de finansiella företagen.

De många påverkade verksamheterna visar dock hur sårbart samhället är och hur viktigt det är att myndigheter och företag skyddar system och har förberedelser att åtgärda det som inträffar.

Phishing

Att använda e-post för att genomföra angrepp kallas Phising (nätfiske) eller, i de fall angreppet är riktat mot en eller ett fåtal individer, spearphishing (riktat nätfiske). Syftet är att få en användare att agera på ett sätt som hjälper angriparen. Angriparen skickar e-postmeddelanden som ska verka legitima och på så sätt få användaren att klicka på en länk i meddelandet, öppna ett bifogat dokument eller tillåta innehåll i e-postmeddelandet, exempelvis en bild, att hämtas från internet. Gör användaren något av detta hjälper det angriparen på något sätt att uppnå sitt syfte. Angreppet kan handla om att lura mottagaren att lämna ifrån sig ett lösenord, kreditkortsuppgifter, delta i penningtvätt eller installera skadlig kod.

I det fall hotaktören är ute efter att samla in vissa uppgifter behöver användaren inte alltid aktivt ange sina uppgifter för att hotaktören ska få tag på det den är ute efter - det kan ske i bakgrunden utan att användaren är medveten om att så sker. Phishing och spearphishing är framgångsrikt eftersom det i stor utsträckning utnyttjar mänskliga egenskaper, exempelvis nyfikenhet.

I regel riktas phishing mot en bredare målgrupp och har som mål att träffa så många offer som möjligt. När angripare använder phishing är det därför mycket ovanligt att dessa inkluderar några personliga detaljer.

För att motverka phising är det viktigt att användarna är medvetna om hotet och är uppmärksamma på att inte klicka på länkar eller öppna dokument som de inte förväntar sig.

Ett spearphishing-angrepp inkluderar personliga detaljer som exempelvis ett namn eller referenser till något som är av intresse för mottagaren och skickas vanligtvis till ett begränsat antal mottagare. Detta kräver att hotaktören

har kartlagt organisationen eller personen. Spearphishing förekommer ofta i cyberangrepp som genomförs av statliga aktörer. Dessutom använder även kriminella spearphishing i allt större utsträckning.

Det har förekommit att spearphishing har riktats mot medarbetare i banker som kan tänkas ha högre it-behörigheter. LinkedIn har använts för att kartlägga bankernas it-medarbetare, vilka sedan har fått falska jobberbjudanden med länkar till skadlig kod. Syftet med denna typ av spearphishing är troligen att hotaktörerna ser detta som ett snabbt sätt att etablera fotfäste i bankernas infrastruktur. Phishing mot it-leverantörers personal som ett sätt att potentiellt attackera företag förekommer också. Spridning av skadlig kod i finansiella företag via phishing kan mot denna bakgrund vara en hög risk för företagen. De är därför viktigt att företagen dels utbildar personalen så att de ska kunna upptäcka phishing-mejl, dels implementerar tekniska lösningar för att blockera phishing-mejl.

Uppslag för reflektion och övningar:

- Finns det inom företaget en god allmän medvetenhet om dessa företeelser?
- Vet du som anställd om du kan göra något för att minska risken för ransomware-attacker eller överbelastningsattacker mot företaget eller för att sådana drabbar företagets kunder? Kan riskerna för att kunder drabbas få allvarliga återverkningar för din arbetsgivare”?
- Finns det god medvetenhet om phisingangrepp? Finns det risk för att kriminella falskeligen använder företagets namn i samband med angreppen? Finns det i så fall god beredskap inom företaget för att informera oroliga kunder?

Läsanvisningar:

Avsnitt 2-4 och 7-8: Hotbildsbedömning för Sveriges Banker, Svenska Bankföreningen maj 2024, se

https://www.swedishbankers.se/fragor-vi-arbetar-med/banksakerhet/sakerhet/hotbildsbedomning-for-sveriges-banker-2024/ (En ny version förväntas bli publicerad under våren 2025.)

Avsnitt 6:

Finansinspektionens föreskrifter, FFFS, 2023:20, 2 kap Kreditprövning

Bolån - Kunskap för Swedsecs licensiering av Anette Ridder, kapitel 9 Kreditprövning

Avsnitt 7-8:

Möjliggörare för kriminella nätverk - Rapport från Brottsförebyggande rådet, 2024:2

Avsnitt 9

Nationellt cybersäkerhetscentrums rapport Cybersäkerhet i Sverige 2022 - hot, metoder, brister och beroenden, se https://www.ncsc.se/siteassets/publikationer/ncsc-rapport-2-cybersakerhet-i-sverige-2022-rekommenderade-sakerhetsatgarder.pdf

Nationellt cybersäkerhetscentrums Temafördjupning Utpressningsangrepp Juni 2024, se https://www.ncsc.se/siteassets/publikationer/utpressningsangrepp---temafordjupning.pdf

Finansdepartementets promemoria om digital operativ motståndskraft för finanssektorn:

https://www.regeringen.se/contentassets/58784e2692fd44dcb665af7bfaace3d7/digital-operativ-motstandskraft-for-finanssektorn.pdf

DORA-förordningen: https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX%3A32022R2554