2026-11-03

ju.remissvar@regeringskansliet.se
ju.L4@regeringskansliet.se

Betänkandet Effektiva ingripanden i cybermiljö

Svenska Bankföreningen har beretts tillfälle att yttra sig över betänkandet SOU 2026:45 Effektiva ingripanden mot brott i cybermiljö och lämnar härmed sina synpunkter.

Bakgrund och övergripande ställningstagande

Bankföreningen har under de senaste åren i ett antal framställningar till regeringen lyft fram behovet av ett mer offensivt och resursstarkt agerande från brottsbekämpande myndigheters sida i förhållande till cyberrelaterad brottslighet riktad mot den finansiella sektorn.

I en framställan från maj 2024 hemställde Bankföreningen om att brottsbekämpande myndigheter ges ett uppdrag och tillräckliga resurser för att kunna ligga i framkant och besitta den senaste tekniken och it-kompetens för att effektivt kunna ingripa mot pågående ekonomisk brottslighet i cybermiljön.[1] Detta oavsett om sådana ingripanden kan antas leda till slutlig lagföringen eller ej. Framställan pekade vidare på att oklarheter beträffande jurisdiktion inte ska förhindra effektiva polisiära ingripanden i Sverige. Lagstiftaren uppmanades därför att modernisera lagstiftningen för att kunna angripa nuvarande och framtida ekonomisk brottslighet, som blir alltmer avancerad.

I en framställan från januari 2025 uppmärksammade Bankföreningen att ingen av de i Nationellt Cybersäkerhetscenter (NCSC) ingående myndigheterna föreföll ha något tydligt ansvar eller mandat att ingripa eller för att stötta i avhjälpandet av cyberangrepp[2]. Styrning och ledning från myndigheterna vid de överbelastnings-attacker som drabbade bankerna under hösten 2024 upplevdes som otydlig.

Mot denna bakgrund välkomnar Bankföreningen att utredningen föreslår en ny rättslig ram för sådana ingripanden. Förslagen i utredningen svarar mot de behov Bankföreningen har identifierat; att brottsbekämpande myndigheter ges ett tydligt legalt mandat att agera offensivt och proaktivt i cybermiljön. Bankföreningen är

[1] Upptrappade åtgärder mot aktiva bedrägerinätverk, Svenska Bankföreningen 2024-05-07.
[2] Stärkt krishantering vid stora cyberangrepp, Svenska Bankföreningen 2025-01-14.

Besök (Visit):
Blasieholmsgatan 4B
Stockholm
Sverige (Sweden)

Post:
Box 7603
SE-103 94 Stockholm
Sverige (Sweden)

+46 (0)8 453 44 00
info@financesweden.se

www.financesweden.se

positiv till utredningens förslag och välkomnar inriktningen att ge brottsbekämpande myndigheter ändamålsenliga verktyg för att kunna förhindra och avbryta brottslighet i cybermiljön.

Finanssektorn och bankerna är i dag föremål för sofistikerade och storskaliga cyberangrepp. Det är viktigt för det finansiellstabilitet och allmänhetens förtroende att staten kan erbjuda ett effektivt svar på dessa hot.

Bankföreningen vill framhålla att de föreslagna befogenheterna behöver utformas med omsorg om de specifika förutsättningar som gäller för finansiella företag, digital forensisk, informationsdelning och ansvarsfördelning. Bankföreningen lämnar därför ett antal konkreta synpunkter i syfte att stärka förslagets ändamålsenlighet och rättssäkerhet i förhållande till den finansiella sektorn.

Otillräcklig analys av förhållandet till banksekretessen

Utredningen saknar en uttrycklig analys av hur de föreslagna ingripandebefogenheterna förhåller sig till banksekretessen i 1 kap. 10 § lagen (2004:297) om bank- och finansieringsrörelse (LBF). En banks it-system innehåller mycket stora mängder uppgifter om enskilda kunder och deras mellanhavanden med institutet, vilket på goda grunder åtnjuter ett starkt sekretesskydd.

Svenska Bankföreningen noterar att undantaget i 1 kap. 11 § LBF medger att sekretessbelagda uppgifter lämnas till en myndighet om det finns en uppgiftsskyldighet eller befogenhet som följer av lag. Det är därför tänkbart att den föreslagna lagen i princip kan utgöra det lagstöd som krävs för att ett röjande av banksekretessbelagda uppgifter ska anses behörigt i lagens mening.
Det kvarstår dock viktiga frågor som utredningen inte besvarar:

- *Proportionalitet och avgränsning:* Utredningen föreslår att ingripanden bara får riktas mot uppgifter i de delar av informationssystemet som har samband med relevant brottslighet. Vid en faktisk systemåtkomst är det i praktiken svårt, ofta omöjligt, att på förhand avgränsa vilka uppgifter polispersonal exponeras för. En bred systemåtkomst riskerar att innebära att Polisen tar del av ett mycket stort antal kunduppgifter utan att dessa har koppling till brottsligheten, vilket faller utanför ingripandelagens ramar och därmed även utanför undantaget i 1 kap. 11 § LBF. Även om det kan vara svårt att på förhand förordna om en systemåtkomst med tillräcklig precision för att ingripandet ska vara effektivt, kan säkerhetsgarantier ges genom lag. Utredningen bör närmare överväga hur sådana garantier bör utformas. En möjlig lösning kan vara förordande i lag om att enbart de förhållanden som är av direkt relevans för ingripandet får dokumenteras i varje ärende.

- *Bankens ansvar:* Banksekretessen är en skyldighet för institutet och dess anställda. Det är inte tillräckligt klart i utredningen om, och i så fall hur, den föreslagna lagen befriar banken från ansvar för det röjande av kunduppgifter som en polisiär systemåtkomst faktiskt medför. Banker genomför ingen självständig materiell prövning och saknar annars möjligheter att hindra eller påverka en verkställighet av ett beslut om ingripande. Det bör därför tydligt framgå att en bank inte kan ådra sig skadeståndsansvar gentemot sin kund till följd av ett sådant ingripande.

- *Avsaknad av jämförelse med andra skyddade uppgifter:* Utredningen innehåller uttryckliga förbud mot ingripanden som rör advokaters och läkares tystnadsplikt. Att banksekretessen, som torde vara den i praktiken mest förekommande typen av sekretess vid ifrågavarande ingripande, inte omfattas av en jämförelse i detta sammanhang förefaller inkonsekvent och skapar en otydlighet. Utredningen bör överväga ett förtydligande i denna del.

Utnyttjande av tekniska sårbarheter

Utredningens förslag: Enligt 17 § i förslaget till lag om polisiära ingripanden i cybermiljö får systemskydd brytas eller kringgås och tekniska sårbarheter utnyttjas vid verkställigheten. Det kan handla om att utnyttja tekniska brister, att installera program för att kringgå inloggning, eller att använda ett användarnamn och lösenord som har kommit till myndighetens kännedom. Rätten att bereda sig tillgång till informationssystem framgår av 3 § i lagförslaget.

Bankföreningens synpunkt: Bankföreningen förstår att möjligheten att utnyttja tekniska sårbarheter kan vara nödvändig för att brottsbekämpande myndigheter ska kunna ingripa effektivt mot antagonistiska cyberangrepp, inte minst i de situationer där angriparen redan befinner sig i ett finansiellt företags it-infrastruktur.

Bankföreningen vill uppmärksamma att befogenheten kan komma i konflikt med de krav som följer av DORA (Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn). Artiklarna 6, 8, 9, 10, 11 och 25 i DORA ålägger finansiella företag att fortlöpande identifiera, klassificera och hantera tekniska sårbarheter i sin infrastruktur samt att genomföra regelbunden sårbarhetstestning.

Om en myndighet utnyttjar en teknisk sårbarhet i ett finansiellt företags it-system utan att företaget informeras, riskerar företaget att stå kvar med en ohanterad sårbarhet i strid med sina skyldigheter enligt DORA. Felaktig identifiering av informationssystem, infrastrukturtjänster eller digitala resurser kan få betydande konsekvenser för bankerna genom exempelvis blockeringar, avstängningar, tillgänglighetsstörningar, dataförlust eller andra verksamhetspåverkande åtgärder. Ju

mer offensiva befogenheter som införs, desto högre blir kraven på precision och kontrollmekanismer.

Bankföreningen förordar därför att lagstiftningen kompletteras med en reglerad process för att informera den berörda verksamheten om den utnyttjade sårbarheten efter ingripandets slut.

Avsaknad av krav på återställning av informationssäkerheten

Utredningens förslag: Utredningen överväger ett krav motsvarande 25 § andra stycket lagen om hemlig dataavläsning, som ålägger den verkställande myndigheten att vidta de åtgärder som behövs för att informationssäkerheten i det berörda systemet ska hålla minst samma nivå som vid verkställighetens början, borde gälla även för ingripanden i cybermiljö. Utredningen avvisar ett sådant krav med motiveringen att ingripanden i cybermiljö är kortvariga, att raderingsbeslut till sin natur är oåterkalleliga och att kravet vid hemlig dataavläsning har visat sig problematiskt i praktiken. Det enda återställningskrav som föreslås är att installerade tekniska hjälpmedel ska tas bort eller göras obrukbara så snart ingripandet har genomförts eller beslutet upphört att gälla, enligt 19 § i lagförslaget.

Bankföreningens synpunkt: DORA artikel 11 kräver att finansiella entiteter har interna regler för IKT-kontinuitet, samt åtgärds- och återställningsplaner som möjliggör återgång till normal drift. Artikel 12 föreskriver säkerhetskopierings- och återställningsförfaranden som ska kunna aktiveras och anger att kontroller och avstämningar ska genomföras för att säkerställa hög dataintegritet efter återställning. Att lagförslaget inte innehåller något krav på att informationssäkerheten återställs till den nivå som gällde före ingripandet innebär att banken kan lämnas med ett försämrat eller förändrat säkerhetsläge utan att myndigheterna har ett rättsligt ansvar för att åtgärda detta. Bankföreningen förordar att ett uttryckligt krav på teknisk verifiering av att berörda it-system har återställts efter ingripandets slut införs i lagstiftningen. Företagen bör också ges möjlighet att genomföra en kompletterande säkerhetsgranskning i direkt anslutning till ingripandet**.**

Radering, ändring eller blockering av data

Utredningens förslag: Myndigheterna får enligt 3 § i lagförslaget ändra eller blockera uppgifter som ger tillgång till eller behandlas i det berörda informationssystemet. Radering regleras i 5 § i lagförslaget, men enbart om det är av synnerlig vikt för att förhindra eller avbryta brott med minst ett år i straffskalan. Beslut om radering fattas normalt av åklagare efter ansökan enligt 12 § och i brådskande fall interimistiskt av en behörig befattningshavare enligt 13–14 §§, varefter beslutet omgående ska prövas av åklagare. Kopior av raderade uppgifter ska förstöras senast sex månader efter prövningen.

Bankföreningens synpunkt: DORA artikel 9 kräver att data skyddas avseende tillgänglighet, äkthet, integritet och konfidentialitet och att risken för förvanskning eller förlust minimeras. Artikel 17 kräver att finansiella företag registrerar samtliga IKT-relaterade incidenter och inför en incidenthanteringsprocess som ger fullständig spårbarhet. Artikel 19 föreskriver att allvarliga IKT-relaterade incidenter ska rapporteras till behöriga myndigheter genom en första anmälan, delrapporter och en slutrapport, i vilken grundorsaken analyseras. Dessa rapporteringskrav förutsätter att incidentunderlag, säkerhetsloggar och revisionsspår bevaras intakta.

En myndighetsåtgärd som raderar, ändrar eller blockerar uppgifter kan direkt motverka bankens möjlighet att genomföra incidentutredningar, fastställa grundorsaker och fullgöra sin rapporteringsskyldighet enligt DORA artikel 19. Bankföreningen rekommenderar ett uttryckligt krav på att ett ingripande inte får omöjliggöra framtida incidentutredning eller regulatorisk granskning, om detta inte är absolut nödvändigt för ingripandets ändamål. Det bör också övervägas om lagstiftningen behöver innehålla tydligare principer eller minimikrav för forensiskt bevarande av digital bevisning innan åtgärder som radering eller störning genomförs.

Frivilligt samarbete, ansvarsfördelning och spårbarhet

Utredningens förslag: Utredningen konstaterar att ett tillträdesbeslut inte krävs om den som råder över ett informationssystem förväntas samarbeta frivilligt, och att ingripanden i sådana fall kan genomföras med samtycke. Denna ordning lämnas emellertid i allt väsentligt oreglerad. Beslutanderätten vid formella ingripanden regleras i 11 § och läggs på särskilt utsedda och kompetensgranskade befattningshavare. Av 2 § i förordningsförslaget framgår att befattningshavarna ska ha dokumenterad it-kompetens och ha befunnits lämpliga. Enligt 23 § ska beslut och verkställighetsåtgärder dokumenteras, men myndigheterna är inte skyldiga att i efterhand informera den berörda verksamheten om ett genomfört ingripande.

Bankföreningens synpunkt: Bankföreningen vill lyfta fram två sammanhängande brister i förslaget som tillsammans berör bankens ställning och handlingsutrymme i förhållande till de brottsbekämpande myndigheterna, dels under ett ingripande, dels i dess efterskede.

Under ingripandet är frivilligt samarbete sannolikt den vanligaste formen av interaktion när det gäller ingripanden i ett finansiellt företags it-miljö. Ett finansiellt företag har starka operativa, rättsliga och affärsmässiga skäl att vilja kontrollera hur och i vilken utsträckning externa parter ges åtkomst till dess system. Det är naturligt att en bank i en sådan situation önskar att dess egen personal visar Polisen de relevanta delarna av systemet och gör eventuella utdrag av information, snarare än att polispersonal självständigt ansluter till och navigerar i it-systemen. Utredningen ger inget svar på hur ett samtycke ska dokumenteras och avgränsas, om banken har rätt att ställa villkor för sin medverkan, och hur övergången från frivillig samverkan till

formella tvångsåtgärder ska hanteras. Avsaknaden av en reglerad ordning för frivilligt samarbete riskerar att skapa otydlighet och tvister i den praktiska tillämpningen.

Efter ingripandet uppstår en problematik i förhållande till DORA. Artikel 13 förutsätter att hela händelseförloppet vid en incident kan rekonstrueras och analyseras i efterhand. En situation där Polisen genomför tekniska åtgärder i ett finansiellt företags it-system utan att företaget i efterhand informeras om vad som gjorts innebär att banken bär det regulatoriska ansvaret men saknar informationen som krävs för att fullgöra sina skyldigheter avseende IKT-riskhantering, incidentklassificering och intern styrning.

Bankföreningen förordar att den fortsatta beredningen resulterar i tydliga riktlinjer för både formerna. Den första handlar om frivilligt samarbete medan den andra handlar om myndighetens skyldighet att efter avslutat ingripande lämna relevant information till den berörda verksamheten, i den mån säkerhetsskäl medger detta.

SVENSKA BANKFÖRENINGEN

Hans Lindberg

Magnus Jacobson