Finanspolisen informerar

• DECEMBER 2019

Penningtvätt efter VD-bedrägerier / Business E-mail Compromise (BEC)

En relativt vanlig och uppmärksammad bedrägeriform är så kallade VD-bedrägerier eller Business E-mail Compromise Fraud (BEC-fraud). Bedrägeriet riktar sig mot företag och består i att få företaget att göra en felaktig utbetalning till ett konto som kontrolleras av bedragarna.

Bedrägerierna drabbar både företag i Sverige och utomlands. Vanligtvis sker den felaktiga utbetalningen till ett annat land än det land där bedrägeriet ägt rum. Det innebär att den penningtvätt som sker i Sverige till följd av dessa brott i princip uteslutande har skett utomlands. Bedrägeriformen drabbar även företag i Sverige men den påföljande penningtvätten sker då vanligtvis i ett annat land.

Finanspolisen har under en längre tid följt utvecklingen, vilket resulterat i ett större antal brottsanmälningar och att avsevärda summor belagts med dispositionsförbud. Bedrägerierna ligger dock på en fortsatt hög nivå, och Finanspolisens bedömning är att förövarna till största delen består av internationella brottssyndikat.

Modus

Bedrägerier som föregår den här typen av penningtvätt kan utföras på flera olika sätt. Vanligtvis sker någon form av dataintrång men även rena s.k. social engineering-attacker förekommer. Syftet är att få tillgång till information som möjliggör bedrägeriet, och ibland även direkt tillgång till offrens datasystem. Tillgång till datasystem och information används sedan för att utföra bedrägerierna. Det kan vara att bedragarna genom manipulerade fakturor styr betalningen till ett annat mottagarkonto, eller skapar en faktura med en fiktiv mottagare som förefaller normal för företaget och för den anställde som godkänner fakturan.

Vad de olika tillvägagångssätten har gemensamt är att en betalning som ska till en viss mottagare genom bedragarnas agerande styrs till en annan mottagare. Den nya mottagaren är i princip alltid en målvakt och inte bedragaren själv. Oaktat om mottagarna är inblandade i bedrägeriet eller inte så medverkar de till en transaktioner som utgör en del av penningtvätt.

Efter en betalning är utförd kommer bedragarna att verka för att brottsvinsten säkerställs och tvättas. Dessa steg sker vanligtvis simultant och penningtvätten påbörjas redan när brottsvinsten anländer på den första målvaktens konto. Pengarna flyttas därför vidare, oftast i direkt anslutning till att de anlänt på kontot, till nästa målvakt. Det är vanligt att brottsvinsten i detta led delas upp mellan flera andra linjens målvakter. Swish är det vanligast transaktionssättet då en sådan överföring blir omedelbart tillgänglig hos mottagaren men även bank- och postgirobetalningar förekommer. Det förekommer också att brottsvinsten flyttas vidare till ett annat land direkt från den första målvaktens konto men det vanligaste är överföringar i flera led.

Efter ett antal transaktioner som syftar till att omöjliggöra att brottsvinsten återtas sker någon form av transaktion som slutligt skiljer brottet från brottsvinsten. Det kan vara kontantuttag, köp av varor som levereras, köp av kryptovalutor, eller överföringar till en jurisdiktion där spårning inte är möjlig. Därefter återstår endast att integrera pengarna i den legala ekonomin för att brottsvinsten ska vara tvättat.

Finanspolisen informerar

• DECEMBER 2019

Indikationer

Den vanligaste och starkaste indikationen att ett bedrägeri och påföjande penningtvätt av det här slaget sker är att namnet på mottagaren inte överensstämmer med namnet på konto-innehavaren. Vanligtvis sker betalning enligt en faktura till en företag, vars namn vanligtvis anges även i transaktionsinformationen. Det mottagande kontot tillhör dock inte det angivna företaget utan en privatperson.

Ytterligare indikationer är att utlandsbetalningar direkt vid ankomst skickas vidare till andra mottagare. Är det en större summa pengar som överförts fördelas den vanligtvis i mindre poster mellan flera mottagare.

Omständigheten att en privatperson får en större summa pengar från utlandet till ett privatkonto kan i sig vara en indikator. Många av de målvakter som Finanspolisen identifierat har innan den misstänkta transaktionen endast använt sitt konto till en ren vardagsenonomi. I andra fall har kontona varit nyöppnade. Generellt avviker transaktionen både genom att summan avviker från vad man kan förvänta sig givet personens ekonomi i övrigt samt att det inte finns ett tidigare mönster av liknande transaktioner.

Vissa målvakterna har varit inblandade i flera bedrägerier på samma konto. När den drabbade banken har avslutat kundrelationen har vissa målvakterna vänt sig till en annan bank där de medverkar till ytterligare transaktioner. Finanspolisen ser ett mönster hos dessa individer där de börjar med de största aktörerna och sedan vänder sig till nisch- och mellanbanker och till slut sparbanker. Det finns därför särskild anledning att vara uppmärksam på nya kunders utlandstransaktioner.

Åtgärder och rekommendationer

Den mest effektiva åtgärden är att verksamhetsutövaren har rutiner för att kontrollera avvikelser mellan namn på mottagare och namn på mottagande kontoinnehavare. En sådan avvikelse torde i sig vara tillräckligt stark indikation för att inte fullfölja transaktionen. Om transaktionen redan i detta skeda kan stoppas och returneras till avsändaren förhindrar man att bedrägeriet fullbordas. En penningtvättsrapport ska dock ändå inges till Finanspolisen avseende den nekade transaktionen och de inblandade personerna.

Även om det inte möjligt var att avbryta transaktionen ska en penningvättsrapport vid misstanke inges till Finanspolisen. Finns medel fortfarande kvar på kontot bör dessa frysas och kontakt via telefon tas med Finanspolisen för ett eventuellt dispositionsförbud

Vid inrapportering till Finanspolisen underlättar det om rapporten tydlig anger vilka åtgärder som vidtagits, inklusive eventuella utökade kundkännedomsåtgärder. Om kundrelationen avslutats eller en brottsanmälan ingetts bör det framgå.

Andra åtgärder kan vara att begränsa kundens möjlighet att använda de tjänster som är centrala i denna typ av brottslighet, främst då utlandsbetalningar och Swish.

Tidigare utskick från Finanspolisen avseende Swish och kryptovalutor innehåller också information som kan utgöra vägledning för att identifiera led i penningtvätt av detta slag.

Finanspolisen
Telefon: 010 56 368 00
E-post: fipo@polisen.se