Förebygga fysiska attacker mot bankomater

UTVECKLA EN EFFEKTIV STRATEGI

EUCPN
EUROPEAN CRIME PREVENTION NETWORK
EMPACT
EUROPOL

“

It is only a matter of time before MOs emerging in one country spread to other countries. This clearly indicates the need for adoption of the preventive and operational measures at the European level with private, public and law-enforcement partners working closely together.

”

TACK

Detta dokument är resultatet av ett samarbete mellan Europol, Europeiska unionens byrå för samarbete inom brottsbekämpning, och EUCPN-sekretariatet, det europeiska nätverket för förebyggande av brottslighet . Vi vill tacka experterna inom området fysiska attacker mot bankomater för deras tid och insatser i arbetet med att ta fram denna rekommendationsskrift. De har bidragit genom att närvara vid konferensen om förebyggande av fysiska attacker mot bankomater (januari 2019, Bryssel) och genom att tillhandahålla avgörande information. Framför allt vill vi tacka brottsbekämpande organ från EU-länder och från länder utanför EU (”tredjeländer”), den privata sektorn inklusive ATM Industry Association (ATMIA), BPost, Centrum voor Criminaliteitspreventie en Veiligheid (CCV), Diebold Nixdorf, European Association for Secure Transactions Expert Group on ATM och [serviceboxar för kontanträkning] ATS Physical Attacks (EAST EGAP), European Intelligent Cash Protection Association (Euricpa), ING, Febelfin, NCR, Protect, SIOC Banking, Spinnaker, TMD Security och inrikesministerierna i Belgien, Kroatien, Tyskland och Spanien.

This brochure was funded by the European Union’s Internal Security Fund — Police.

INNEHÅLL

INNEHÅLL

På grund av det ökande antalet fysiska bankomatattacker och det ökande antalet drabbade EU-länder organiserade det europeiska nätverket för förebyggande av brottslighet (EUCPN) och Europol en konferens (januari 2019) där brottsbekämpande samt offentliga och privata partner samlades för att gemensamt undersöka hur dessa brott kan förebyggas. Denna rekommendationsskrift sammanfattar resultaten av den här konferensen för att öka myndigheternas medvetenhet om fysiska bankomatattacker och förebyggande åtgärder.

Det är ett begränsat men trots allt växande antal länder inom EU som har problem med fysiska bankomatattacker. År 2017 beräknades den därav följande ekonomiska förlusten till över 30 miljoner euro i Europa. En del länder fortsätter att se ett signifikant antal fysiska bankomatattacker, och andra har sett en signifikant ökning av dem under de två senaste åren. Det här brottsområdet utvecklas snabbt. En del länder har varit framgångsrika i sin hantering av de fysiska bankomatattackerna och har på senare tid sett en markant minskning av dem. Å andra sidan har länder som tidigare inte drabbats upplevt en plötslig våg av fysiska bankomatattacker under 2018 till följd av att kriminella organisationer brett ut sig inom landet. Det är inte bara banker som drabbas utan även bankomater från oberoende leverantörer, eftersom dessa bankomater ofta är förlagda till mer sårbara byggnader eller platser.

De många olika tillvägagångssätt (modi operandi, MO) som brottslingar tillämpar för att attackera bankomater kan delas in i två huvudkategorier: fysiska bankomatattacker och bankomatrelaterade bedrägeriattacker (detta inkluderar attacker mot bankomatprogramvara och sabotageprogram). De här skriften fokuserar på fysiska attacker mot bankomater: fysiskt inbrott i bankomater för att tömma dem på pengar. Fysiskt inbrott kan ske med hjälp av:

> **sprängmedel:** angriparna använder gas eller fasta sprängämnen för att fysiskt bryta sig in i bankomaten och få tillgång till kontanterna,

> **utdragnings-/rammningsattacker:** angriparna avlägsnar bankomaten fysiskt från installationsplatsen, ofta med hjälp av en bil med hög kapacitet,

> **attacker på platsen:** angriparna bryter sig in i bankomaten med fysiskt våld, ofta med hjälp av kap- eller krossverktyg som vinkelslipar, släggor eller acetylensyrebrännare.

01 FAKTORER SOM AVGÖR FRAMGÅNGEN HOS EN FYSISK BANKOMATATTACK

Framgångstalen för bankomatattacker är låga – endast en tredjedel av attackerna lyckas. Men även om attacken inte lyckas så blir skadorna (exempelvis till följd av sprängning) på byggnaderna stora och miljön runt brottsplatsen blir en otrygg plats för lokalbefolkning, blåljuspersonal och förbipasserande.

Hur väl en bankomatattack lyckas är beroende av ett antal faktorer, däribland bankomatens utförande, planeringen av attacken och gärningsmännens erfarenhet och kunnande.

1. Bankomaternas sårbarhet

De mest sårbara bankomaterna är de som sitter utomhus (monterade genom väggen) och de som står placerade inuti byggnader. Vid attacker av fristående inomhusbankomater föredrar kriminella organisationer bankomater i köpcenter framför bankomater i bankanläggningar där bevakningen brukar vara hårdare. Banker driver framför allt bankomater som är placerade inuti eller utanför en bankbyggnad. Fjärrbelägna bankomater på gator eller på kommersiella anläggningar som bensinstationer, stormarknader, hotell, kasinon, flygplatser osv. blir alltmer vanliga i takt med att bankfilialer stänger ner. Oberoende leverantörer administrerar bankomater som en fristående tjänst. Deras bankomater är ofta placerade i butiksanläggningar, på hotell- och fritidsanläggningar, transportanläggningar (järnvägsstationer, flygplatser osv.), i offentliga byggnader och ute på gatan.

Eftersom bankärenden i allt högre grad sker online kommer troligen allt fler filialer att läggas ner under de kommande åren, vilket kommer att leda till en minskning av antalet bankomater[1]. Detta kan emellertid medföra ett större antal fjärrbelägna bankomater och bankomater från oberoende leverantörer på mer sårbara platser.

2. Planering av en bankomatattack

Förberedandet av en attack kan ta upp till flera veckor eller till och med månader. Gärningsmännen måste samla ihop nödvändiga **verktyg och resurser** som fordon, utrustning och kontaktpunkter. **Fordon** är nödvändiga redskap för de fysiska bankomatattackerna. Gärningsmännen förflyttar sig huvudsakligen i bil och efter attacken flyr de ofta undan i snabba fordon. Dessa är ofta stulna, men kan också ha hyrts eller köpts (t.ex. via internet). Det mesta av **utrustningen** för fysiska bankomatattacker är enkelt att få tag på eftersom det säljs i vanliga butiker. Det gör det ännu enklare att ta steget över till den här typen av brottslighet. Att spåra ursprunget för ett verktyg är svårt för de brottsbekämpande organen så riskerna för gärningsmännen är begränsade. Kriminella organisationer som är aktiva inom fysiska bankomatattacker på internationell nivå har alltid kontaktpunkter i landet som är föremål för attacken (personer som bor där under en viss period) eller kan det vara så att de tillämpar en hit-and-run-teknik. De här kontakterna hjälper de kriminella organisationerna med logistiken. De ordnar med övernattning, tillhandahåller ett fordon eller annan utrustning och identifierar målen. En del internationella gärningsmän lämnar över all logistik och rekognoscering till de lokala kontakterna och tar sig sedan bara till landet med bil eller flyg för att utföra bankomatattacken. Kriminella organisationer genomför omfattande **rekognoscering** för att identifiera lämpliga mål – de beräknar tidpunkt under dagen då bankomaten är full med kontanter, undersöker bankomatens omgivningar, bankomatens tekniska utformning, flyktvägar och säkerhetsåtgärder som finns inrättade, t.ex. intern kameraövervakning (CCTV), larmsensorer och jalusier. En del kriminella organisationer vidtar ett antal åtgärder för att **stressa de brottsbekämpande styrkorna och säkerhetspersonalen** före en attack. De manipulerar larmsystem och offentlig belysning, använder avledande tekniker, sätter upp vägavspärrningar eller försöker mixtra med de brottsbekämpande styrkornas fordon.

3. Gärningsmännens erfarenhet och kunnande

Fysiska attacker är attraktiva för kriminella eftersom de får tag på pengarna direkt och det behövs inget omfattande nätverk för att sälja stulna föremål. Det är ett bekvämt alternativ för kriminella som redan är aktiva inom organiserad brottslighet mot enskild egendom. Kriminella organisationer måste samla på sig **expertis och kunnande som krävs** eftersom det är en avgörande faktor för om attacken ska lyckas eller inte. Expertis och kunnande som krävs är i hög grad beroende av **typen av attack**. Utdragnings-/rammningsattacker och attacker som sker *på platsen* har enkla tillvägagångssätt (i stort sett är det djärvhet och råstyrka som krävs), så de kräver inte några specifika färdigheter. Attacker med brännbar gas och attacker med fasta sprängmedel kräver en högre grad av expertis. Angriparna uppvisar olika **kompetensnivåer**. Å ena sidan kan välorganiserade och erfarna grupper utföra en bankomatattack på några minuter. De är väl förtrogna med processen och kan begränsa risken till dem själva och därmed även begränsa de indirekta skadorna. Mindre organiserade och opportunistiska grupper, å andra sidan, misslyckas ofta med sina försök och kan orsaka avsevärd skada på anläggningarna och byggnaderna i det omkringliggande området. En del av de här mindre organiserade kriminella grupperna tros återgå till traditionell organiserad brottslighet mot enskild egendom eftersom de avskräcks av de förebyggande åtgärderna som de inte klarar av att avvärja vid bankomatattacker.

02 BEHOVET AV EN FÖREBYGGANDE STRATEGI

Länder där gärningsmännens framgångtal är låga vid fysiska bankomatattacker eller där antalet fysiska bankomatattacker minskar visar att en lyckad strategi för att motarbeta fysiska bankomatattacker består av en kombination av operationella och förebyggande åtgärder. Eftersom antalet kriminella organisationer inom detta brottsområde är begränsat reducerar gripanden och påföljande bestraffning av medlemmarna i de kriminella organisationerna avsevärt antalet attacker. Många bankomatrånare fortsätter emellertid med sina attacker så snart de blir frigivna. Dessutom kan en grupp kan ibland ersätta den gripne gärningsmannen snabbt. Därför finns det ett stort behov av förebyggande åtgärder, vilka helst bör vara inbäddade i en lagstiftningsram. Dessutom visar erfarenhet att förebyggande åtgärder i ett land kan driva kriminella organisationer mot mer sårbara mål i andra länder. Det är bara en tidsfråga innan tillvägagångssätt som framträder i ett land sprider sig vidare till andra länder. Det här är ett tydligt tecken på att **de förebyggande och operationella åtgärderna måste vidtas på den europeiska nivån** i ett tätt samarbete mellan privata, offentliga och brottsbekämpande partner.

03 FÖREBYGGANDE ARBETE

För att förebygga och tackla den här typen av brott behövs en tydlig strategi. I det här kapitlet kommer vi att ge en översikt över de tre steg som i regel tas när man ställs inför fysiska bankomatattacker eller förbereder för att förhindra dem.

Först har vi **situationsbedömningen**; en riskprofil över bankomaterna och deras omgivningar ska upprättas mot bakgrund av mängden tillgängliga kontanter (möjligt byte), risken för indirekt skada och risken för personskada. Därefter, baserat på riskbedömningen, ska en **förebyggande strategi** tas fram. Slutligen ska de **förebyggande åtgärderna** genomföras.

1. Bedöma situationen

Kriminella organisationer tenderar att antingen rikta in sig på specifika typer av bankomater eller bankomater från specifika leverantörer med funktioner som underlättar bankomatattacken. Därför är det nödvändigt att göra en grundlig bedömning av risken för fysiska bankomatattacker, helst innehållande hela säkerhetskedjan för kontanterna från transitering till leverans för förvaring i bankomaten. För att fastställa riskprofilen för varje bankomat måste ett antal poster analyseras inklusive följande.

- Hur det ser ut där bankomaten är placerad och i bankomatens omgivning, stads- eller landsortsplacering, befolkningstäthet, närhet till polisstationer, kameror för automatisk avläsning av registreringsskyltar (ANPR) i närheten, intern kameraövervakning i närheten osv.
- Bankomatens placering:
  - uti eller utanför en bank, i en bankfilial eller på en fjärrbelägen anläggning (t.ex. köpcentrum), inbyggd eller fastsatt på en byggnad,
  - för fristående bankomat: om den är förankrad eller ej,
  - för inbyggda bankomater eller bankomater fastsatta på en byggnad: om det föreligger arkitektoniska svagheter, hur kontantförvaringen är organiserad osv.
- Typen av bankomat.
- Säkerhetsfunktionerna som ingår i bankomaten.
- Mängden kontanter i bankomaten.
- Typen av fysiska bankomatattacker och förväntat tillvägagångssätt, så att man kan vidta de mest lämpliga förebyggande åtgärderna.
- Redan vidtagna säkerhetsåtgärder och förebyggande åtgärder (intelligent system för neutralisering av sedlar (IBNS), intern kameraövervakning, säkerhetsdimma (synlighetsreduktion) osv.).

Ytterligare aspekter som ska utvärderas är status för samarbetet med partner och intressenter samt lagstiftningen. Samarbetet mellan brottsbekämpande, privata och offentliga partner ska utvärderas för att man ska kunna bygga allianser för att motarbeta brott. Det är möjligt att varje partner sitter inne med intressant information som kan bidra till bedömningen av situationen. Lokal polis och lokala myndigheter är särskilt viktiga inom detta ramverk. Lagstiftningen måste utvärderas med avseende på inrättandet av ett juridiskt ramverk för förebyggande arbete, obligatoriska förebyggande åtgärder, straffpåföljd för bankomatattacker osv.

2. Utveckla en förebyggande strategi

När väl situationen har utvärderats och de huvudsakliga riskområdena samt styrkorna och svagheterna hos bankomatsäkerheten har fastställts kan en strategi utvecklas (ofta byggd på offentligt/privat samarbete) och förebyggande och operationella motåtgärder kan inrättas. Förebyggande åtgärder ska syfta till att avskräcka och inkapacitera brottslingarna. För att göra det föreslår den brittiske kriminologen Ronald V. Clarke tre axlar av förebyggande åtgärder baserade på tre av fem strategier för situationsbundet brottsförebyggande [2]; minska vinsten, öka risken för gärningsmännen och göra det mer besvärligt att lägga vantarna på bytet.

Brottslingarna väger den förväntade vinsten mot de relaterade riskerna (t.ex med en bankomatattack). Genom att minska chansen för ett enkelt byte och öka risken för gärningsmännen minskar man deras förväntningar och lust att ge sig på en fysisk bankomatattack. Fler åtgärder som ökar ansträngningen som krävs för att man ska lyckas med att bryta sig in i bankomaten påverkar gärningsmännens kapacitet. Opportunistiska gärningsmän som ofta misslyckas med sina försök slutar att ge sig på bankomater. För professionella bankomatrånare reduceras framgångstalen, vilket åter igen har inverkan på vinst-/riskbalansen.

Den förebyggande strategin kompletteras vidare av parallella åtgärder såsom effektiv mediastrategi, tidigt socialt förebyggande arbete samt åtgärder för att reducera risken för indirekt skada på byggnader och för att garantera säkerheten för lokalbefolkning, blåljuspersonal och förbipasserande.

Andra sätt att strukturera strategin är också möjliga. I Nederländerna tillämpar myndigheterna den så kallade barriärmodellen [3]. Den här modellen identifierar steg som en brottsling måste ta för att begå ett brott. Den identifierar också de partner och tillfällen som kan möjliggöra brottet och det är ett användbart verktyg för att organisera informationsinsamlingsprocessen vid brottsområdet. Genom att identifiera varenda steg som måste tas för att man ska genomföra en bankomatattack går det att identifiera barriärerna som förhindrar brottet och de bästa partnerna för att ställa upp dem. Den här barriärmodellen identifierar även signaler

för att varna offentliga och privata partner för fysiska bankomatattacker och signaler som de kan sända ut själva för att underrätta myndigheterna om deras misstankar.

En välutvecklad strategi behövs för att minska de risker som förknippas med förstärkande förebyggande arbete. Förebyggande åtgärder som är mycket effektiva genom att avskräcka amatörer och copycats har ibland oönskade effekter. En del grupper tillämpar trial-and-error-metoder för att hitta sårbara bankomater och lämnar efter sig en skörd av trasiga bankomater. Farligare och mer oförskräckta kriminella grupper börjar använda sig av mer våldsamma tillvägagångssätt som att gå över från gas till fasta sprängämnen i sina attacker.

För att fastställa en effektiv uppsättning av förebyggande åtgärder är den bästa metoden att inrätta en nationell myndighet med behörighet att ålägga specifika åtgärder för högriskbankomater vilka ska vara baserade på en noggrann situationsanalys. Den här metoden har visat sig effektiv i Frankrike, i synnerhet om ett rättsligt ramverk etableras och åtgärderna implementeras tillsammans med operationella åtgärder.

3. Implementera förebyggande åtgärder

Åtgärderna som introduceras i detta kapitel för att förhindra fysiska bankomatattacker har visat sig verkningsfulla i olika länder. De är baserade på slutsatserna från konferensen om förebyggande arbete och på förebyggande åtgärder som aktivt rekommenderas av internationella organisationer aktiva inom bankomatsäkerhet. Många åtgärder är välkända. Flera länder har redan implementerat ett antal åtgärder med framgång. Ofta implementeras emellertid de föreslagna åtgärderna endast delvis och införlivas inte i lagstiftningen.

Som vi beskrev ovanför föreslås tre axlar av förebyggande åtgärder: minska vinsten, öka risken för gärningsmännen och göra det besvärligare att lägga vantarna på bytet.

3.1 Minska vinsten

Att minska vinsten/belöningen av kriminellt agerande är den första axeln när man ska förebygga fysiska attacker. Så länge uppfattningen om ”lätta pengar” råder kommer kriminella att fortsätta begå den här typen av brott. Genom att minska mängden tillgängliga kontanter och antingen avlägsna eller förstöra kontanterna minskar man möjligheterna för att det ska finnas intressant byte som lockar. Sänkta förväntningar minskar lusten hos kriminella att begå den här typen av brott.

Minska mängden kontanter

Ett sätt att minska vinsten är att minska mängden kontanter som finns i bankomaten. Allra helst bör mängden kontanter vara begränsad till endast det belopp som behövs för en dags transaktioner. Samarbete mellan banker kan garantera kostnadseffektivitet. I Nederländerna har ett antal banker samarbetat för att inrätta ett bankoberoende bankomatnätverk som kallas ”Geldmaat”. Målet med samarbetet är att garantera tillgänglighet, åtkomlighet, överkomlighet och säkerhet med avseende på kontanter. Det här kommer troligen att leda till färre bankomater. Däremot kommer varje bankomat inte att innehålla mer kontanter, men den kommer att fyllas på oftare. Antalet påfyllningar kommer att behovsanpassas.

Eftersom de flesta attackerna sker mellan kl. 03.00 och 04.00 bör fristående bankomater (vilka oftast är belägna i kommersiella och offentliga byggnader, vilka är mer sårbara) tömmas i slutet av dagen, och därefter ska kontanterna placeras i ett kassaskåp. En varningsskylt kan informera allmänheten om att bankomaten inte innehåller några kontanter. Dagen därpå fylls bankomaten på innan byggnaden har öppnat för kunderna. Det här systemet har införts i Frankrike där lagen säger att alla butiksinnehavare med en fristående bankomat i butiken måste ta ut kontanterna på kvällen och lämna bankomaten öppen. För andra bankomater kan det tillgängliga kontantbeloppet minskas genom att man ökar påfyllningsfrekvensen.

Förstöra bytet och göra pengarna spårbara

Intelligenta system för neutralisering av sedlar (IBNS) är tekniker som tillämpas för att förstöra bytet vid bankomatattacker. Sådana system färgar sedlarna med bläck så att man kan se att de är stulna. Spårare och markörer kan läggas till IBNS-bläcket. För närvarande används dessa markörer framför allt för kriminaltekniska ändamål genom att länka sedeln till brottsscenen och öka risken för att gärningsmannen ska åka fast. Även om IBNS är en effektiv förebyggande åtgärd finns det en del överväganden.

Europeiska centralbanken betalar inte tillbaka fläckade sedlar [4] (sedan 2003) men ett antal av EU-medlemsstaternas nationella centralbankerna gör det fortfarande. Fläckade sedlar tar sig också tillbaka in i det lagliga systemet via kasinon. IBNS skapar extra svårigheter för kriminella men skulle vara mycket mer effektivt om det vore omöjligt för kriminella att använda fläckade sedlar inom EU. För att uppnå det borde fläckade sedlar inte accepteras av de nationella centralbankerna. Undantag kan göras för specifika omständigheter, till exempel när sedlar har fläckats genom falsk aktivering. Det är också viktigt att upplysa befolkningen om att fläckade sedlar inte får tas emot. I ett mer långsiktigt perspektiv ska sedelacceptorer kunna detektera fläckade sedlar och de ska installeras i banker och på kommersiella anläggningar som kasinon, biltvättar osv. Att detektera bläcket är svårt och dyrt, men en kostnadseffektiv lösning skulle kunna vara att installera infraröda system som detekterar sedlar som fläckats med infraröda markörer. Dessa system har visat sig vara effektiva och är standard i Belgien och Frankrike. När sedlar med infraröda markörer förs in i bankomaten accepterar (sväljer) bankomaten dem, men kontot krediteras inte. Personen som för in de fläckade sedlarna bör även registreras.

Vid installation av IBNS-lösningar finns en del andra överväganden. Många tillverkare tillhandahåller ett antal olika IBNS-lösningar med olika aktiveringsmekanismer och olika typer av bläck. Ett första övervägande gäller det faktum att inte alla typer av IBNS-aktiveringstekniker kan tackla alla hot. En del IBNS-tekniker fungerar mycket bra för utdragnings- och rammningsattacker, *på platsen*-attacker och gasattacker men fungerar inte vid en attack med fasta sprängämnen och omvänt. Därför måste man noga överväga vilken teknik som ska användas.

Ett annat övervägande är vilken typ av bläck som ska väljas. I Belgien är de nationella minimikraven för IBNS (säkerhet, fläckningsprocentandel, ej tvättbart osv.) fastställda och oberoende tester intygar att systemet uppfyller de nationella standarderna och fungerar i enlighet med tillverkarens anspråk. Det är viktigt att testa på riktiga sedlar för det finns billigare bläcksorter på marknaden vilka fungerar väl med förfalskade/falska sedlar men inte med äkta sedlar, vilket innebär att bläcket kan avlägsnas från äkta sedlar om man tvättar dem. Utöver detta rekommenderas att det till bläcket läggs en forensisk markör, vilken gör det möjligt att utreda en koppling mellan fläckade sedlar och en specifik brottsplats.

Bästa praxis visar att IBNS kan vara mycket effektivt speciellt i kombination med andra förebyggande åtgärder. År 2015 introducerade Frankrike ny lagstiftning innehållande paragrafer om installation av IBNS-teknik och användning av bläck med unikt DNA. Det är den franska militärpolisen (gendarmeriet) som, baserat på en riskbedömning, bestämmer var IBNS och andra åtgärder måste implementeras. Sedan den nya lagstiftningen förstärkte den förbyggande och operationella strategin minskad antalet attacker från 300 för 2013 till 50 för 2018.

En annan teknik som är under utveckling går ut på att bytet ska förstöras med **lim**. Effekten av lim har beprövats i Nederländerna, men implementerings- och driftskostnaderna är för närvarande höga. Dessutom kan lim utgöra en brandrisk om systemet inte aktiveras före en attack eftersom spridningen av limpartiklar i luften skulle kunna göra att det bildas en brännbar blandning. Den här metoden är inte marknadsredo ännu men skulle kunna vara en lösning i framtiden.

3.2 Öka risken

En andra axel för förebyggande av fysiska bankomatattacker är att avskräcka potentiella gärningsmän från att begå brott genom att öka risken för upptäckt och straffpåföljd. Utöver risken för fysisk skada vid användning av sprängmedel för bankomatattacker är den primära risken för en brottsling en fängelsedom efter gripandet på bar gärning eller efter en utredning. För att minska lockelsen för de potentiella gärningsmännen måste risken för upptäckt och straffpåföljd ökas. För samhället är förstås infångandet och dömandet av de kriminella också en mycket effektiv förebyggande metod om påföljden blir straff, precis som vi sett i ett antal länder.

Informationsdelning

För att bankomatråna re ska upptäckas och dömas till straffpåföljd är det avgörande med informationsdelning mellan alla intressenterna i kampen mot fysiska bankomatattacker, däribland bankomatleverantörer, brottsbekämpande myndigheter (polis, åklagare osv.), offentliga myndigheter, tillverkarna av både bankomater samt säkerhets- och skyddsanordningar, professionella sammanslutningar, bankomatleverantörer (banker och oberoende leverantörer), säkerhetsföretag och larmcentraler. I bästa fall bör detta ske både på nationell och internationell nivå.

Tidig upptäckt av en förestående bankomatattack är svårt. Endast när det råder näst intill perfekt fungerande informationsutbyte på internationell nivå mellan brottsbekämpande partner och privata partner (säkerhetsföretag och bankomatleverantörer) är tidig upptäckt möjligt. En mängd olika indikatorer måste övervakas, som t.ex. tidiga varningsmeddelanden mellan brottsbekämpande organ om kriminella gruppers förehavanden, information om (”heta”) fordon som använts i bankomatattacker, information från säkerhetsföretag eller vakter i närområdet om misstänkt beteende som upptäckts i området kring bankomaten, suspekta transaktioner som upptäckts av bankomatleverantörer eller andra avkänningsmetoder. Andra möjliga polisiära åtgärder för tidig upptäckt är övervakning av stulna bilar, av tillverkare och distributörer av sprängmedel och företag med tillstånd att använda sprängmedel. De insatser som krävs för att tidig upptäckt ska vara möjligt är krävande och det finns ingen garanti för att de lyckas, varför brottsbekämpande insatser före en attack är ovanliga.

Om tidig upptäckt inte är möjligt kan larmcentraler snabbt utfärda en varning vid en eventuell fysisk bankomatattack. För att göra det möjligt att ingripa måste nationella bestämmelser och protokoll för snabb kommunikation mellan larmcentraler och brottsbekämpande enheter avtalas och inrättas. Oavsett om det gäller tidig upptäckt eller realtidsinformation måste de brottsbekämpande enheterna bedöma bästa tidpunkt och läge för en insats. Att ta de kriminella på bar gärning är mycket svårt och kan leda till riskfyllda situationer eftersom en del kriminella grupper är mycket våldsamma och tungt beväpnade.

För att den utredning som följer efter en bankomatattack ska bli framgångsrik måste de brottsbekämpande enheterna kommunicera med alla intressenter, eftersom alla kan sitta inne med information som kan bidra till en lyckad utredning. Naturligtvis är kommunikation och samarbete med de primära offren, bankerna och de övriga bankomatleverantörerna nödvändigt – de har tillgång till data som är viktiga för utredningen. För bankomatleverantören kommer informationen från de brottsbekämpande enheterna att hjälpa till att förbättra de förebyggande åtgärderna. Därutöver har kontakter med professionella sammanslutningar och tillverkare visat sig vara verkningsfulla – de skickar ofta ut säkerhetsmeddelanden som andra intresserade aktörer kan abonnera på. Bankomattillverkare har god översikt över olika typer av bankomatattacker och över svagheter och styrkor hos de motsvarande förebyggande åtgärderna. De är villiga att stödja polisen med information om de tekniska aspekterna hos bankomaterna och de tillvägagångssätt som används.

Gränsöverskridande samarbete är av största betydelse: länder ska dela information (om misstänkta, dömda bankomatrånare, tillvägagångssätt, suspekta fordon, bilder på attacker osv.), inte bara som stöd för utredningen utan också för att misstänkta som dömts i andra länder ska kunna dömas för återfall i brott.

Slutligen kan upprättandet av en databas på europeisk nivå som är tillgänglig för brottsbekämpande myndigheter och innehåller forensiska data (t.ex. om olika typer av IBNS-bläck, spårare och markörer eller skyddsglas för bankomater) kraftfullt understödja utredningar och koppla misstänkta till en specifik brottsplats. Standardisering av tekniker på en internationell nivå är ofta inte tillräckligt. Under januari 2019-konferensen konstaterade deltagare att EU-nivåstandardisering av bläck och brottsmärkning avsevärt skulle kunna underlätta utredningarna.

Intern kameraövervakning och avlyssningsutrustning

Bild- och ljuddata från kameraövervakningssystem och avlyssningsutrustning kan vara till stöd för både realtidsdetektering av en attack (t.ex. för att förhindra att blåljuspersonal som kommer till brottsplatsen skadas fysiskt) och för de efterföljande utredningarna (t.ex. för att identifiera gärningsmännen och deras tillvägagångssätt). Kameraövervakningsbilderna kan kombineras med bilder från offentliga och övriga kameraövervakningssystem i närområdet runt bankomaten och med trafikradarinspelningar för att tillhandahålla en mer komplett bild av gärningsmännen och deras tillvägagångssätt. Kameraövervakningsbilder är emellertid ofta av ganska dålig kvalitet, och förvaringen av dem bristfällig. Bilderna måste vara av tillräckligt god kvalitet för att en person ska kunna identifieras. Som tidigare sagt skulle europeiska standarder för säkerhetskameraövervakning underlätta utredningarna. Eftersom gärningsmän ofta oskadliggör övervakningskameror före en attack skulle man dessutom kunna installera osynlig kameraövervaknings- eller realtidsavlyssningsutrustning.

Straffpåföljd och rehabilitering av brottslingar

Konsekventa och stränga straff har visat sig ha en förbyggande effekt. Gripandet av en kriminell

organisation har omedelbar effekt på antalet bankomatattacker. Frisläppandet av bankomatrånare leder emellertid också ofta till en ny våg av attacker. Det innebär att korta straff leder till att förövarna snabbt är aktiva på nytt. Min- och maxstraffen för brottslingar som döms för varje enskild typ av fysisk bankomatattack varierar bland medlemsstaterna. En del anser att strängare straff kommer att avskräcka potentiella gärningsmän. Vetenskaplig forskning [5] visar emellertid att strängare straff inte nödvändigtvis förstärker den avskräckande effekten. Därför kan det vara intressant att titta på korrigerande (och gärningsmansbaserade) rehabiliteringsprogram för att förhindra den höga återfallsfrekvensen.

3.3 Göra det mer besvärligt

Den tredje axeln för att förebygga bankomatattacker innehåller åtgärder som gör det mer besvärligt för en brottsling att genomföra brottet.

Garantera en miljö som är motståndskraftig mot brott

Om riskbedömningen (se ovan) visar att en bankomat är placerad i ett högriskområde ska den monteras ned och flyttas till ett låg- eller medelriskområde. Ett tydligt exempel på detta är ifall analysen visar att byggnaden kan kollapsa om en bankomatattack utförs med sprängmedel. Lagstiftning skulle kunna implementeras för att verkställa sådana åtgärder i högriskfall. Utöver att minska antalet bankomater i högriskmiljöer bör kontantlös betalning uppmuntras för att minska behovet av bankomater. Om det inte är möjligt att flytta bankomaten ska så många säkerhetsåtgärder som möjligt vidtas: t.ex. utplacering av skyddspollare, lampposter och andra trafikskydd för att begränsa åtkomsten till byggnaden, fordonsstoppande system, installation av adekvat gatubelysning, förbättrad öppen eller dold övervakning och stöldskyddsutrustning som ett system för sedelneutralisering. När en bankomat attackeras på en plats som inte har identifierats som högriskområde ska den identifieras som sådan och extra säkerhetsåtgärder ska vidtas. De nya faktorerna ska inkluderas i riskbedömningsverktyget för att uppdatera det. Omvärdering av den här risken ska ske regelbundet.

Förstärka bankomaterna

Bankomattillverkarna erbjuder ett standardsortiment av bankomater som är utrustat med ett antal säkerhetsfunktioner vilka är säkerhetsklassade enligt Europeiska standardiseringskommittén (CEN). I allmänhet har bankomater en CEN-märkning som sträcker sig från lägsta CEN1-klassen till högsta CEN4-klassen. Funktioner som styrka hos ytterhöljet och beständighet mot attacker är vad som bestämmer klassen. Beständighet mot gasattacker erbjuds vanligen som tillval (CEN-GAS). Standardmodulerna kan förstärkas med extra skyddsåtgärder. Vanligtvis är det tredjeparter som installerar dessa funktioner för att garantera samstämmighet med lokal lagstiftning och anpassning av basmodellerna efter de lokala kundernas behov. Extra säkerhetsfunktioner inkluderar olika sensorer för att aktivera ett gasneutraliserande system eller IBNS vid en eventuell *attack på platsen* eller attack med sprängmedel och förstärkta luckor och valvlås för att förhindra otillåten tillgång till kassaskåpet där den primära luckan hotas. För portabla, fristående bankomater är det viktigt att använda förankringssystem vilka erbjuder extra skydd mot utdragnings-/rammningsattacker. Spårningssystem kan inkluderas i bankomaten för att vara till stöd för utredarna när bankomaten transporteras till en annan plats innan den öppnas.

Arkitektoniska åtgärder

När en bankomat ska installeras rekommenderas maskiner med åtkomst på baksidan. Det innebär att gärningsmannen måste ta sig in i byggnaden för att komma åt maskinens baksida och stjäla kontanterna. Portabla, fristående bankomater är de mest sårbara. En minskning av antalet sådana bankomater skulle öka säkerheten. Att göra det obligatoriskt att bankomater ska monteras i inbrottssäkra rum skulle automatiskt minska användningen av fristående bankomater.

Dimsystem

En dimkanon fyller snabbt upp ett rum med tät dimma så att inkräktaren inte kan se något. Den här säkerhetsdimman gör det ofta omöjligt att genomföra en bankomatattack. Om inte annat så fördröjs attacken och polisen får mer tid att ingripa. Säkerhetsdimsystemet är kopplat till larmsystemet och kan aktiveras på två sätt. Det kan utlösas automatiskt med larmsensorer som rörelsedetektorer (på natten) eller manipuleringssensorer i bankomatluckan. Det kan också aktiveras via en

larmcentral om man vill undvika för många falskalarm. För vägginbyggda utomhusbankomater kan dimsystemet användas på bankomatens baksida för att fylla rummet med dimma och reducera gärningsmannens sikt till obefintlig. Dimsystemen kan ge punktskydd åt bankomater som är placerade i öppna utrymmen på bensinstationer, stormarknader osv. På det viset undviker man att hela området fylls med dimma. Dimskyddet är som mest effektivt när dimman kommer från olika vinklar eller när den fyller utrymmet bakom bankomaten vid en eventuell rammningsattack. Tester pågår där man undersöker om dimkanoner kan monteras inuti själva bankomaten, i stället för i rummet där bankomaten är placerad. DNA-märkning som fläckar gärningsmännen och deras kläder kan läggas till dimman.

3.4 Parallella åtgärder

För att garantera effektiv och verkningsfull implementering av de förebyggande åtgärder som nämnts ovan måste ett antal parallella åtgärder beaktas. Dessa åtgärder är oundgängliga för att möjliggöra eller förstärka en holistisk förebyggande och operationell strategi för att hantera fysiska bankomatattacker.

Lagstiftning

I ett antal länder måste bankomatleverantörerna enligt lag vidta förebyggande åtgärder. I andra länder garanterar upprättade villkor och avtal mellan banker och brottsbekämpande organ en välfungerande strategi för att hantera fysiska bankomatattacker. Områden inom vilka regelverk kan övervägas är:

- inbäddning av förebyggande åtgärder,
- juridiska ramverk för att tillåta samarbete mellan brottsbekämpande samt offentliga och privata partner,
- en omarbetning av straffutdömningen om straffen för gärningsmännen vid fysiska bankomatattacker är för låga.

Ofta är det emellertid bara bankinstitutionerna som tvingas till efterlevnad, medan oberoende bankomatleverantörer inte är bundna av dessa lagar eller avtal. Det här är en vanlig svag punkt i regelverken.

En del länder implementerar inte några lagar utan försöker övertala bankomatleverantörerna att vidta förebyggande åtgärder genom att öka deras medvetenhet kring brottsområdena och trenderna. I länder med ett stort antal oberoende banker visar detta sig speciellt svårt.

Det är nödvändigt att garantera att den resulterande implementeringen av de förebyggande åtgärderna inkluderar förändringar i lagstiftningen och bestämmelser både på nationell och internationell nivå vilka gäller för alla typer av bankomatleverantörer. I mest gynnsamma fall bör lagstiftningen harmoniseras på EU-nivå för att man ska undvika att kraftfulla lagstiftade förebyggande åtgärder i ett land driver de kriminella organisationerna vidare till andra länder med mindre sträng lagstiftning.

Mediastrategi

En annan viktig axel i den förebyggande strategin är en väletablerad mediastrategi som syftar till att sänka förväntningarna och minska lockelsen för bankomatrånarna att ge sig in på den här typen av brott. Låga framgångstal och den höga risken för gärningsmännen måste understrykas. Kommunikation om vinst (byte) eller detaljer kring bankomatattacken såsom typ av drabbad bankomat eller tillvägagångssätt som bör undvikas. Å andra sidan är det nödvändigt med omfattande kommunikation kring arresteringar av misstänkta och påföljande straff efter en fällande dom.

Förbättrat samarbete

Förbättrat samarbete och informationsutbyte har redan nämnts men kan inte nog understrykas. Operationellt informationsutbyte på den internationella nivån är Europols främsta uppgift. Utöver det här informationsutbytet visade konferensen om förberedande arbete tydligt på ett behov av utökat tvärvetenskapligt samarbete över flera nivåer och av informationsdelning mellan alla relevanta aktörer inklusive brottsbekämpande organ, offentliga myndigheter, bankomattillverkare samt säkerhets- och skyddsanordningar, professionella sammanslutningar, bankomatleverantörer (banker och oberoende leverantörer, säkerhetsföretag och larmcentraler. Detta måste omfatta de lokala, nationella och internationella nivåerna.

Minska risken för indirekt skada

Vid eventuella attacker med sprängämnen kommer en del kriminella organisationer att lämna efter sig material. Det kan skapa riskfyllda situationer för blåljuspersonal och civila (från närområdet eller som passerar förbi).

Deras säkerhet måste garanteras I Belgien till exempel måste protokoll och förfaranden som ska följas av blåljuspersonal (både de från brottsbekämpande organ och de från bankomatleverantörerna) utformas och samordnas med varandra. En annan bästa rutin i det sammanhanget är exemplet med Nederländerna där användning av kameraövervakningsmaterial från bankomatattacken används för att utvärdera situationen. Överenskommelser med larmcentraler kan inrättas för att göra dessa bilder omedelbart tillgängliga.

Socialt förebyggande arbete

Kriminella organisationer rekryterar ofta bland unga. Projekt kan inledas för att försvåra för de här rekryteringsprocesserna i ett tidigt skede. Polis och socialarbetare bör vara uppmärksamma på de här processerna och kan ingripa genom att personligen ta kontakta de potentiella gärningsmännen.

04 SLUTSATSER

Under de senaste två åren har antalet EU-länder som drabbas av fysiska bankomatattacker ökat. Därför har Europol och EUCPN samarbetat för att identifiera de bästa åtgärderna för att bekämpa och förebygga detta brott.

En framgångsrik strategi för att tackla fysiska bankomatattacker består av en kombination av operationella och förebyggande åtgärder, helst inbäddade i ett regelverk. För att undvika att kraftfulla metoder i ett land driver kriminella organisationer mot mer sårbara länder rekommenderas att dessa åtgärder antas på europeisk nivå.

För att förhindra och tackla den här typen av brott ska en tydlig strategi inrättas i tre steg: utvärdering av situationen, framtagning av en förebyggande strategi baserad på riskbedömningen och införande av de förebyggande åtgärderna.

Riskbedömningen för fysiska bankomatattacker bör inkludera uppgifter om bankomatens beskaffenhet och dess omgivningar, samarbetet med partner och intressenter för att bygga allianser för att bekämpa detta brott samt utvärdering av de förebyggande och rättsliga ramarna. När situationen väl utvärderats bör det etableras en strategi byggd på offentligt/privat samarbete samt förebyggande och operationella motåtgärder. Målet med de förebyggande åtgärderna är att minska lockelsen och kapaciteten hos gärningsmännen att ge sig på en fysisk bankomatattack. För att nå detta föreslås tre axlar med förebyggande metoder: minska vinsten, öka risken och göra det besvärligt för gärningsmännen. Parallella åtgärder ska komplettera den förebyggande strategin. Bästa praxis är att inrätta en nationell myndighet som har befogenhet att göra dessa nödvändiga åtgärder obligatoriska.

Genom att **reducera vinsten** minskar förbrytarens lust att ge sig in på den här typen av brottslighet. En åtgärd för att sänka förväntningarna för de kriminella är att minska mängden kontanter i bankomaterna till vad som är tillräckligt för en dags transaktioner, eller att tömma (de mest sårbara) bankomaterna på natten. En annan metod är att förstöra bytet och göra pengarna spårbara. I det här sammanhanget kan IBNS användas, vilket fläckar sedlarna och märker dem som stulna. Den här metoden är den mest effektiva när det är omöjligt för kriminella att betala med pengarna eller att återinföra dem i det lagliga kontantflödet. Det här kan åstadkommas genom att bankerna och allmänheten inte accepterar fläckade sedlar vid betalning och genom att man installera sedelacceptorer som kan detektera och neka fläckade sedlar. I det här avseendet har investeringar i infraröda system som detekterar fläckade sedlar med infraröda markörer visat sig vara en kostnadseffektiv lösning i Belgien och Frankrike. När länder installerar IBNS måste de noggrant överväga de valda aktiveringsmekanismerna, minimikraven för neutralisering av sedlarna och om man vill förse bläcket med en forensisk markör.

Åtgärder som avskräcker potentiella gärningsmän från att begå brott genom att öka risken för detektering och påföljande straff är den andra axeln för att förebygga fysiska bankomatattacker. Avgörande för att detektera och straffa bankomatrånare är informationsinsamling och -delning mellan alla intressenter, både på nationell och internationell nivå. Informationsutbyte av högkvalitativa övervakningsbilder och ljuddata kan öka chanserna för tidig upptäckt och framgångsrik utredning. För att

undvika att kameraövervaknings- eller avlyssningsenheter oskadliggörs före attacken kan installation av osynlig kameraövervaknings- eller realtidsavlyssningsutrustning övervägas. Skapandet av en forensisk databas och standardisering av tekniker på europeisk nivå skulle avsevärt underlätta för internationella samarbeten och utredningar. Om brottslingar arresteras och döms kan det vara intressant att undersöka korrigerande (och gärningsmansbaserade) rehabiliteringsprogram för att förhindra hög återfallsfrekvens.

Den tredje axeln för att förebygga fysiska bankomatattacker inkluderar åtgärder för att**försvåra för brottslingarna** att genomföra en kriminell gärning. Installation av en bankomat i en miljö som är motståndskraftig mot brott och har maximala säkerhetsåtgärder kommer att göra det besvärligare för brottslingarna att attackera en bankomat. Dessutom kan standardskyddet för bankomater förstärkas med ett antal ytterligare säkerhetsfunktioner. Utöver dessa åtgärder kan installation av ett dimsystem avskräcka gärningsmannen eller åtminstone fördröja attacken.

Ett antal **parallella åtgärder** kommer att understödja åtgärderna ovan, till exempel att skapa ett regelverk som ålägger alla bankomatleverantörer att implementera säkerhetsåtgärder, utveckla en välutvecklad mediastrategi, förbättra samarbetet på lokal, nationell och internationell nivå, ställa upp riktlinjer för blåljuspersonal för att minska risken för indirekt skada och investera i socialt förebyggande för att underminera rekryteringsprocessen av kriminella.

Factsheet

REKOMMENDATIONER FÖR EN FÖRBYGGANDE STRATEGI: ÖVERSIKT

Utveckla ett effektivt svar för att förhindra fysiska bankomatattacker

Bedöma situationen

> Etablera riskprofilen för bankomater i ditt land/din region.

> Identifiera partner och intressenter i kampen mot fysiska bankomatattacker och utvärdera samarbetet.

> Utvärdera regelverket för att ta itu med fysiska bankomatattacker på nationell och internationell nivå.

Utveckla en förebyggande strategi

> Fastställa de viktigaste riskerna som måste omfattas och prioriteterna.

> Fastställ de bästa förebyggande åtgärderna för att omfatta dessa risker genom att överväga tre huvudaxlar.

> Fastställa parallella förebyggande åtgärder som behövs för att förstärka de förebyggande åtgärder som.

Förebyggande åtgärder som kan vidtas för att

01

Minska vinsten

> Minska mängden kontanter.
  - Tömma bankomaten på natten.
  - Öka antalet/frekvensen av påfyllningar.

> Förstöra bytet.
  - Intelligenta system för neutralisering av sedlar (IBNS).
  - Infraröda markörer i IBNS-bläck så att fläckade sedlar kan.
  - Under utveckling: lim.

02

Öka risken

> Gränsöverskridande informationsdelning för:
  - tidig upptäckt eller realtidsupptäckt av en möjlig bankomatattack,
  - förstärkning av den operationella strategin,
  - bestraffning av återfallsbrottslingar,
  - utbyte av forensiska data på Europanivå.

> Intern övervakningskamera- och avlyssningsutrustning.

> Påföljande straff och rehabilitering av brottslingar.

03

Göra det besvärligare

> Garantera en miljö som är motståndskraftig mot brott.
  - Förflyttning av högriskbankomater till annan plats.
  - Säkerhetsåtgärder: fysiska hinder, övervakning osv.

> Förstärka bankomater med jalusier, beständiga mot gas och fasta sprängämnen osv.

> Arkitektoniska åtgärder såsom maskiner med åtkomst på baksidan.

> Säkerhetsdimsystem.

Parallella åtgärder för att förstärka den förebyggande strategin

> Effektiv lagstiftning inklusive förebyggande åtgärder mot fysiska bankomatattacker, påföljande domar osv.

> Effektiv mediastrategi som avskräcker gärningsmän.

> Förbättrat samarbete mellan intressenter (offentliga, privata, brottsbekämpande) i kampen mot fysiska bankomatattacker.

> Förbättrat samarbete mellan intressenter (offentliga, privata, brottsbekämpande) i kampen mot fysiska bankomatattacker.

> Socialt förbyggande för att undvika att unga rekryteras inom denna kriminella verksamhet.

ENDNOTES

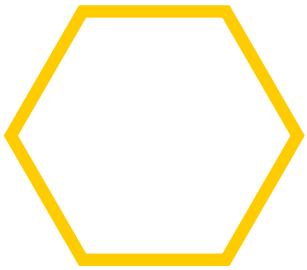
1 Willem Pieter de Groen, Zachary Kilhoffer and Roberto Musmeci, *The future of EU ATM markets: impacts of digitalisation and pricing policies on business models*, CEPS report, 2018

2 Derek Cornish and Ronald V. Clarke, 'Opportunities, precipitators and criminal decisions: a reply to Wortley's critique of situational crime prevention', *Crime prevention Studies* 16 (2003), 41-96.

3 Centrum voor Criminaliteitspreventie, barrieremodellen, www.barrieremodellen.nl

4 European Central Bank decision of the European Central Bank, The denominations, specifications, reproduction, exchange and withdrawal of euro banknotes, 2003.

5 David Weisburd, David P. Farrington and Charlotte Gill, 'Conclusion: *What Works in Crime Prevention Revisited*', David Weisburd, David P. Farrington and Charlotte Gill, *What works in Crime Prevention and Rehabilitation*. Cambridge: Springer, 2016, 311.



CONTACT DETAILS

EUCPN Secretariat
Phone: +32 2 557 33 30
Email: eucpn@ibz.eu
Website: www.eucpn.org, www.europol.europa.eu

TWITTER.COM/EUCPN
FACEBOOK.COM/EUCPN
LINKEDIN.COM/COMPANY/EUCPN