Prevenirea atacurilor fizice asupra bancomatelor

DEZVOLTAREA UNEI ABORDĂRI EFICIENTE

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.

”

MULȚUMIRE

Acest document este rodul unei colaborări între Agenția Uniunii Europene pentru cooperare în aplicarea legii (Europol) și secretariatul Rețelei europene de prevenire a criminalității (EUCPN). Dorim să mulțumim experților în atacurile fizice asupra bancomatelor (ATM) care au investit timp și efort în susținerea creării acestei lucrări de recomandare. Au contribuit prin participarea la conferința privind prevenirea atacurilor fizice asupra bancomatelor (ianuarie 2019, Bruxelles) și furnizarea de informații cruciale. În special, am dori să mulțumim agențiilor de aplicare a legii din U.E. și din țările („terțe") ce nu aparțin de U.E., sectorului privat, inclusiv Asociației industriei de bancomate (ATMIA), BPost, Centrum voor Criminaliteitspreventie en Veiligheid (CCV), Diebold Nixdorf, Asociației Europene pentru Grupuri de experți în tranzacții securizate pe bancomate și atacuri fizice asupra ATS [seifuri] (EAST EGAP), Asociației europene pentru protecția inteligentă a banilor în numerar (Euricpa), ING, Febelfin, NCR, Protect, SIOC Banking, Spinnaker, TMD Security și ministerelor de interne din Belgia, Croația, Germania și Spania.

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

CUPRINS

CONTEXT

Odată cu numărul atacurilor fizice asupra bancomatelor (ATM) și numărul de țări europene afectate în creștere, Rețeaua europeană de prevenire a criminalității (EUCPN) și Europol au organizat o conferință (ianuarie 2019), care aduce serviciile de aplicare a legii împreună cu partenerii publici și privați pentru a examina prevenirea acestei forme de criminalitate. Această lucrare de recomandare rezumă concluziile acestei conferințe pentru a crește gradul de conștientizare în rândul autorităților cu privire la atacurile fizice asupra bancomatelor și la măsurile preventive.

Un număr limitat, dar tot mai mare de țări din Uniunea Europeană, are probleme cu atacurile fizice asupra bancomatelor. În 2017, pierderea financiară cauzată a fost de peste 30 de milioane de euro în Europa. Unele țări continuă să asiste la un număr semnificativ de atacuri fizice asupra bancomatelor, altele au cunoscut o creștere semnificativă a numărului acestor incidente în ultimii doi ani. Această zonă a criminalității evoluează rapid. Unele țări au avut succes în abordarea acestora de a soluționa atacurile fizice asupra bancomatelor și au observat recent o scădere semnificativă a atacurilor. Pe de altă parte, țările neafectate anterior s-au confruntat cu o creștere bruscă a atacurilor fizice asupra bancomatelor în 2018, din cauza grupurilor de criminalitate organizată (OCG) care își extind teritoriul. Nu numai băncile sunt afectate, tot mai multe bancomate de la furnizori independenți sunt atacate, deoarece acestea sunt adesea situate în spații sau locații mai vulnerabile.

Gama largă de diferite metode [moduri de operare (MO)] pe care infractorii le folosesc pentru a ataca bancomatele pot fi împărţite în două categorii majore: atacuri fizice asupra bancomatelor şi atacuri prin fraudă asociate bancomatelor (acestea includ atacuri logice şi malware asupra bancomatelor). Această lucrare se concentrează pe atacurile fizice asupra bancomatelor: intrarea forţată cu mijloace fizice în bancomate pentru a fura banii din acestea. Intrarea forţată poate fi realizată astfel:

> **utilizarea explozivilor:** atacatorii folosesc gaz sau explozivi solizi pentru a încălca fizic seiful bancomatului şi pentru a avea acces la banii în numerar;

> **atacuri prin smulgere/folosirea unui obiect ca berbec:** atacatorii îndepărtează fizic bancomatul din mediul de instalare, folosind adesea un vehicul de ultimă generaţie;

> **atacuri la faţa locului:** atacatorii taie materialul seifului cu ajutorul unei forţe brute, folosind deseori instrumente de tăiere sau de rupere, cum ar fi polizoarele unghiulare, baroase sau flacără oxiacetilenică.

01 FACTORI CARE DETERMINĂ SUCCESUL UNUI ATAC FIZIC ASUPRA BANCOMATULUI

Rata de succes a atacurilor asupra bancomatelor este scăzută; doar o treime din atacuri au succes. Cu toate acestea, chiar şi atunci când atacul nu reuşeşte, daunele cauzate (de exemplu, de explozivi) structurilor clădirilor sunt la fel de importante, lăsând un mediu nesigur în vecinătatea locului infracţiunii pentru localnici, echipele de intervenţie şi trecători.

Succesul unui atac fizic depinde de o serie de factori, inclusiv; caracteristicile unui bancomat, aranjamentul unui atac asupra bancomatului şi experienţa şi cunoştinţele făptuitorilor.

1. Vulnerabilitatea bancomatelor

Cele mai vulnerabile bancomate sunt cele situate în exterior [prin perete (TTW)] sau cele care se află în interiorul clădirilor. Atunci când atacă un bancomat aflat în interior (independent), OCG-urile preferă bancomatele situate în spaţii comerciale în detrimentul celor situate în spaţiile bancare unde supravegherea este de obicei mai strictă. Băncile operează în principal bancomate situate în interiorul sau în afara unei clădiri a băncii. Locaţiile izolate ale băncilor („bancă de la distanţă”) de pe stradă sau din spaţiile comerciale ale comercianţilor, cum ar fi benzinăriile, supermarketurile, hotelurile, cazinourile, aeroporturile etc. devin treptat mai importante, odată cu

închiderea sucursalelor bancare. Furnizorii independenți operează bancomate ca un serviciu independent. Bancomatele acestora sunt adesea amplasate în locații de vânzare cu amănuntul, locații ale hotelurilor și de agrement, locații de transport (gări, aeroporturi etc.), clădiri publice și în stradă.

Odată cu popularitatea din ce în ce mai mare a serviciilor bancare online, este posibil ca multe sucursale bancare să fie închise în următorii ani, ceea ce duce la o scădere generală a numărului de bancomate.[1] Cu toate acestea, acest lucru ar putea implica o creștere a numărului de bancomate de tip bancă de la distanță și bancomate ale furnizorilor independenți, situate în locații mai vulnerabile.

2. Aranjamentul unui atac asupra bancomatului

Pregătirea unui atac poate dura până la câteva săptămâni sau chiar luni. Infractorii trebuie să colecteze **instrumentele și resursele** necesare, cum ar fi vehicule, echipamente și puncte de contact. **Vehiculele** sunt un instrument esențial pentru atacurile fizice asupra bancomatelor; făptuitorii se deplasează în principal cu mașina și după atac reușesc deseori să scape cu ajutorul vehiculelor rapide. Acestea sunt de multe ori furate, dar pot fi, de asemenea, închiriate sau achiziționate (de exemplu, prin intermediul internetului). Majoritatea **echipamentelor** pentru atacurile fizice asupra bancomatelor sunt ușor accesibile și disponibile în mod legal în magazinele normale. Acest lucru reduce în continuare numărul pragului de trecere în această zonă a criminalității. Urmărirea originii unui instrument este dificilă pentru aplicarea legii, astfel încât riscurile pentru făptuitori sunt limitate. OCG-urile care activează în atacuri fizice asupra bancomatelor la nivel internațional au aproape întotdeauna puncte de contact în țara țintă (persoane care locuiesc acolo pentru o anumită perioadă) sau, alternativ, pot folosi o tehnică de părăsire a locului infracțiunii. Aceste contacte susțin OCG-urile cu servici de logistică, cum ar fi închirierea spațiilor de cazare, procurarea unui vehicul sau a altor echipamente și cercetarea țintelor. Unii făptuitori internaționali lasă logistica și cercetarea în întregime în mâinile contactele locale și doar călătoresc pe cale rutieră sau aeriană pentru executarea atacului asupra bancomatelor.

OCG-urile efectuează deseori **cercetări** extinse pentru a identifica ținte adecvate; evaluează perioada din zi în care bancomatul este alimentat, împrejurimile bancomatului, specificațiile tehnice ale bancomatului, rutele de evacuare și măsurile de securitate care există, cum ar fi televiziunea cu circuit închis (CCTV), senzorii de alarmă și obloane.

Unele OCG-uri întreprind o serie de acțiuni pentru a **frustra serviciile de aplicare a legii și de securitate** înainte de atac. Acestea manipulează sistemele de alarmă și iluminatul public, folosesc tehnici de diversiune, creează blocaje rutiere sau încearcă să manipuleze vehiculele serviciilor de aplicare a legii.

3. Experienţa şi cunoştinţele făptuitorilor

Atacurile fizice asupra bancomatelor sunt atractive pentru infractori, deoarece banii sunt disponibili imediat și nu este nevoie de o rețea extinsă pentru a vinde mărfurile furate. Este o alternativă convenabilă pentru infractorii care activează deja în criminalitatea organizată asupra proprietăților.

OCG-urile trebuie să adune **expertiza și cunoștințele necesare**, deoarece acestea sunt un factor determinant în succesul sau eșecul unui atac. Expertiza și cunoștințele necesare depind foarte mult de **tipul atacului**. Atacurile prin smulgere/folosirea unui obiect ca berbec și cele *la fața locului* au un mod de operare simplu (în principal, curajul și utilizarea forței brute), deci, în general, nu necesită abilități specifice. Atacurile cu gaz combustibil și atacurile cu explozivi solizi necesită un nivel mai ridicat de expertiză.

Atacatorii prezintă diferite **niveluri de competență**. Pe de o parte, grupurile extrem de organizate și experimentate pot executa un atac fizic asupra bancomatului cu succes în doar câteva minute. Acestea controlează procesul și sunt capabile să limiteze riscul la care sunt expuse limitând, de asemenea, daunele colaterale. Pe de altă parte, grupurile mai puțin organizate și oportuniste eșuează adesea în încercările lor și pot provoca daune semnificative în spațiile și clădirile din cartier. Se consideră că unele dintre OCG-urile mai puțin organizate vor reveni la activități tradiționale de criminalitate organizată asupra proprietăților, fiind descurajate de măsurile preventive pe care nu sunt în măsură să le depășească în atacurile asupra bancomatelor.

02 NECESITATEA UNEI ABORDĂRI PREVENTIVE

Țările în care făptuitorii au o rată scăzută de succes în atacurile fizice asupra bancomatelor sau unde numărul de atacuri fizice asupra bancomatelor scade, ilustrează faptul că o abordare de succes pentru combaterea atacurilor fizice asupra bancomatelor constă într-o combinație de măsuri operaționale și preventive. Deoarece numărul OCG-urilor active în această zonă a criminalității este limitat, arestările și pedepsirea pentru daune ale membrilor OCG reduc semnificativ numărul de atacuri. Cu toate acestea, odată eliberați, mulți atacatori de bancomate își reiau activitățile. Mai mult, uneori, un grup poate înlocui rapid făptuitorul arestat. Prin urmare, există o mare nevoie de măsuri preventive, de preferat încorporate într-un cadru legislativ. Mai mult, experiența arată că măsurile preventive dintr-o țară pot determina deplasarea OCG-urile către ținte mai vulnerabile din alte țări. Este doar o chestiune de timp înainte ca modurile de operare emergente dintr-o țară să se răspândească în alte țări. Acest lucru indică în mod clar **necesitatea adoptării măsurilor preventive și operaționale la nivel european** cu partenerii privați, publici și de aplicare a legii care colaborează îndeaproape.

03 PREVENIREA

Pentru a preveni şi combate acest tip de criminalitate, este necesară o strategie clară. În acest capitol vom oferi o imagine de ansamblu asupra celor trei paşi care sunt în general întreprinşi atunci când ne confruntăm cu atacuri fizice asupra bancomatelor sau atunci când ne pregătim să le prevenim.

În primul rând, **evaluarea situaţiei**; trebuie stabilit un profil de risc al bancomatelor şi a împrejurimilor acestora, luând în considerare cantitatea de bani în numerar disponibilă (pradă posibilă), riscul de daune colaterale şi riscul de vătămare corporală. În al doilea rând, pe baza evaluării riscurilor, trebuie elaborată o **strategie preventivă**. În ultimul rând, trebuie aplicate **măsurile preventive**.

1. Evaluarea situaţiei

OCG-urile tind să vizeze fie tipuri specifice de bancomate, fie bancomate ale unor furnizori specifici, cu caracteristici care facilitează atacul asupra bancomatelor. Prin urmare, este necesară efectuarea unei evaluări detaliate a riscului de atacuri fizice asupra bancomatelor, incluzând de preferat întregul lanț de securitate a banilor în numerar de la transport la livrare la depozitare în bancomat. Pentru a stabili profilul de risc al fiecărui bancomat, trebuie analizate o serie de elemente, inclusiv următoarele.

- Caracteristicile locației și a împrejurimilor bancomatului; caracteristici, cum ar fi localitatea din oraș sau locația rurală, densitatea populației, proximitatea secțiilor de poliție, camerele de recunoaștere automată a plăcuțelor de înmatriculare (ANPR) din cartier, televiziunea cu circuit închis din apropiere etc.
- Locația bancomatului:
  - în interiorul sau la exteriorul unei clădiri, într-o sucursală a unei bănci sau într-un spațiu la distanță (de ex., comercial), integrat sau atașat unei clădiri,
  - pentru bancomatul independent: fie că este ancorat sau nu,
  - pentru bancomatele integrate sau atașate unei clădiri: dacă există puncte slabe arhitecturale, cum este organizată depozitarea banilor în numerar etc.
- Tipul bancomatului.
- Funcționalitățile de securitate incluse în bancomat.
- Suma de bani în numerar din bancomat.
- Tipul de atacuri fizice asupra bancomatului și modul de operare la care să ne așteptăm pentru a adopta mai întâi cele mai adecvate măsuri preventive.
- Măsurile de securitate și prevenire luate deja [sisteme inteligente de neutralizare a bancnotelor (IBNS), televiziune cu circuit închis, sistem de securitate cu ceață (reducerea vizibilității) etc.].

Alte elemente care trebuie evaluate sunt starea de cooperare cu partenerii și părțile interesate și legislația. Colaborarea dintre serviciile de aplicare a legii, partenerii privați și publici trebuie evaluată pentru a construi alianțe privind combaterea criminalității. Este posibil ca fiecare partener să dețină informații interesante pentru a contribui la evaluarea situației. Poliția locală sau autoritățile locale sunt deosebit de importante în cadrul respectiv. Legislația trebuie evaluată în ceea ce privește stabilirea unui cadru legal pentru prevenire, luarea de măsuri preventive obligatorii, condamnarea pentru atacuri asupra bancomatelor etc.

2. Dezvoltarea unei abordări preventive

Odată ce situația a fost evaluată și principalele zone de risc, precum și punctele forte și slabe ale securității bancomatului, se poate elabora o strategie (se bazează adesea pe colaborarea publică și privată) și pot fi puse în aplicare măsuri preventive și operaționale. Măsurile de prevenire ar trebui să vizeze reducerea intenției și a capacităților făptuitorilor. Pentru a realiza acest lucru, trei axe ale acțiunilor preventive sunt propuse pe baza a trei din cele cinci strategii de prevenire a criminalității situaționale de către Clarke[2]; reducerea recompenselor, creșterea riscului pentru făptuitori și creșterea efortului de acces la pradă.

Infractorii fac un echilibru între rentabilitatea preconizată și riscurile asociate (de exemplu, cu un atac asupra bancomatului). Reducerea șanselor de a obține o recompensă ușoară și creșterea riscului pentru făptuitori scad așteptările și dorința acestora de a se implica într-un atac fizic asupra bancomatului. Măsurile suplimentare care cresc efortul necesar pentru a obține accesul la bancomat afectează capacitățile făptuitorilor. Făptuitorii oportuniști, care adesea eșuează în încercările lor, încetează să se implice în atacuri asupra bancomatelor. Pentru atacatorii profesioniști de bancomate, rata de succes este redusă, afectând din nou echilibrul rentabilitate/risc.

În plus, măsuri paralele, cum ar fi o strategie media eficientă, prevenirea socială timpurie și măsuri pentru a reduce riscul de daune colaterale pentru clădiri și pentru a asigura siguranța rezidenților locali, a echipelor de intervenție și a trecătorilor completează strategia preventivă.

Sunt posibile și alte metode de structurare a abordării. În Olanda, autoritățile aplică așa-numitul model de barieră[3]. Acest model identifică pașii pe care trebuie să-i facă un infractor pentru săvârșirea unei infracțiuni. De asemenea, identifică partenerii și oportunitățile care permit infracțiunea și este un instrument util prin care se poate organiza procesul de colectare a informațiilor privind zona de criminalitate. Identificând fiecare etapă necesară pentru a executa un atac fizic asupra bancomatului, se pot identifica barierele pentru obstrucționarea infracțiunii

și cei mai buni parteneri pentru a stabili barierele. Modelul de barieră identifică, de asemenea, semnale pentru a avertiza partenerii publici și privați cu privire la atacurile fizice asupra bancomatelor și semnalele pe care le pot transmite singuri pentru a notifica autoritățile cu privire la suspiciunile acestora.

O strategie bine dezvoltată este necesară pentru atenuarea riscurilor care vin împreună cu consolidarea prevenirii. Măsurile preventive care sunt foarte eficiente pentru a descuraja amatorii și imitatorii, au uneori efecte nedorite. Unele grupuri apelează la metode de încercare și eroare pentru a găsi bancomatele vulnerabile, lăsând o urmă de bancomate deteriorate. OCG-urile mai periculoase și nemiloase încep să folosească moduri de operare mai violente, cum ar fi trecerea de la gaz la explozivi solizi în atacurile acestora.

Pentru a stabili un set eficient de măsuri preventive, cea mai bună practică este instaurarea unei autorități naționale care are puterea de a impune măsuri specifice pentru bancomatele cu risc ridicat, pe baza unei analize detaliate a situației. Această abordare s-a dovedit eficientă în Franța, mai ales dacă este stabilit un cadru legal și măsurile sunt puse în aplicare împreună cu măsurile operaționale.

3. Aplicarea măsurilor preventive

Măsurile introduse în acest capitol pentru prevenirea atacurilor fizice asupra bancomatelor s-au dovedit a fi utile în diferite țări. Acestea se bazează pe concluziile conferinței de prevenire și pe măsurile preventive promovate în mod activ de organizațiile internaționale active în securitatea bancomatelor. Multe măsuri sunt bine cunoscute. Multe țări au aplicat deja cu succes un număr de măsuri. Cu toate acestea, deseori măsurile propuse sunt aplicate doar parțial și nu sunt încorporate în legislație.

După cum am menționat mai sus, sunt propuse trei axe ale acțiunilor preventive: reducerea recompenselor, creșterea riscului pentru făptuitori și creșterea efortului necesar pentru a avea acces la pradă.

3.1 Reducerea recompenselor

Reducerea recompenselor din infracțiuni este prima axă în prevenirea atacurilor fizice asupra bancomatelor. Atât timp cât persistă percepția „bani obținuți ușor”, infractorii se vor implica în acest tip de infracțiune. Reducerea sumei disponibile de bani în numerar și eliminarea sau distrugerea banilor în numerar, reduc posibilitățile existenței unei prăzi interesante. Așteptările reduse scad dorința infractorului de a se implica în acest tip de infracțiune.

Reducerea sumei de bani în numerar

O măsură de reducere a recompensei este reducerea sumei de bani în numerar disponibile într-un bancomat. În mod ideal, această sumă ar trebui să fie limitată la suma necesară numai pentru o zi de tranzacționare. Colaborarea dintre bănci ar putea asigura rentabilitatea. În Olanda, o serie de bănci au colaborat la crearea unei rețele de bancomate independente de bancă, numită „Geldmaat”. Scopul colaborării este de a asigura disponibilitatea, accesibilitatea, caracterul rezonabil și securitatea banilor în numerar. Acest lucru va duce probabil la o reducere a numărului de bancomate. Cu toate acestea, fiecare bancomat nu va conține mai mulți bani în numerar, dar va fi alimentat mai des. Numărul de alimentări va fi adaptat în funcție de necesitate.

Întrucât infractorii atacă în mare parte bancomatele între orele 03:00 și 04:00, este recomandat cu tărie ca bancomatele independente (în mare parte situate în spații comerciale și publice, care sunt mai vulnerabile) să fie golite la sfârșitul zilei, iar banii să fie mutați într-un seif. Un semn de avertizare poate informa publicul că bancomatul nu deține bani în timpul nopții. A doua zi, bancomatul trebuie alimentat ferit de privirea clienților și cu spațiul închis. Acest sistem este implementat în Franța, unde legislația obligă comercianții cu un bancomat independent în magazin să scoată numerarul noaptea și să lase bancomatul deschis. Pentru alte bancomate, sumele deținute pot fi reduse prin intermediul creșterii frecvenței de alimentare.

Dezvăluirea prăzii şi marcarea banilor

Sistemele inteligente de neutralizare a bancnotelor (IBNS) reprezintă o primă tehnică pentru dezvăluirea recompenselor. Aceste sisteme pătează bancnotele cu cerneală pentru a fi recunoscute ca furate. Marcatorii și markerele pot fi adăugate în cerneala IBNS-urilor. În acest moment, acești marcatori sunt folosiți în principal în scop criminalistic, asociind bancnota cu locul infracțiunii și crescând riscul făptuitorilor de a fi prinși. Deși IBNS este o măsură preventivă eficientă, există câteva aspecte de luat în considerare.

Banca Centrală Europeană nu rambursează bancnotele pătate[4] (din 2003), însă o serie de bănci centrale naționale ale statelor membre ale U.E. încă fac acest lucru. Bancnotele pătate sunt, de asemenea, reintroduse în sistemul juridic prin intermediul cazinourilor. Un IBNS creează un obstacol suplimentar pentru infractori, dar ar fi mult mai eficient dacă ar fi imposibil ca infractorii să folosească bancnote pătate în U.E. Pentru a realiza acest lucru, bancnotele pătate nu ar trebui să fie acceptate de către băncile centrale naționale. Excepții pot fi făcute pentru circumstanțe specifice, cum ar fi bancnotele pătate în timpul unei activări false. De asemenea, este important să sfătuim populația să nu accepte bancnote pătate. Într-o perspectivă mai îndelungată, acceptoarele de bancnote ar trebui să detecteze bancnotele pătate și ar trebui instalate în bănci și în spații comerciale, cum ar fi cazinouri, spălătorii auto etc. Detectarea cernelii este dificilă și costisitoare, cu toate acestea, o soluție rentabilă ar putea fi instalarea sistemelor cu infraroșu care detectează bancnotele pătate cu markere infraroșii. Aceste sisteme și-au dovedit eficiența și sunt o bună practică în Belgia și Franța. Când bancnotele cu markere infraroșii sunt introduse în bancomat, bancomatul va accepta („înghiți") banii, dar nu îi va credita într-un cont. Trebuie să fie înregistrată și persoana care introduce bancnotele pătate.

Există câteva aspecte ce trebuie luate în considerare atunci când sunt instalate soluții IBNS. Mai mulți producători oferă o serie de soluții IBNS diferite cu mecanisme de activare diferite și diferite tipuri de cerneală. Un prim aspect se referă la faptul că nu toate tipurile de tehnologii de activare IBNS pot contracara toate amenințările. Unele IBNS-uri își fac treaba foarte bine pentru atacurile prin smulgere sau prin folosirea unui obiect ca berbec, atacurile *la fața locului* și atacurile cu gaze, dar nu funcționează în cazul unui atac cu exploziv solid sau invers. Prin urmare, tipul de tehnologie ales ar trebui să fie bine luat în considerare.

Un alt aspect de luat în considerare este alegerea tipului de cerneală. În Belgia, sunt stabilite cerințele minime naționale pentru IBNS (siguranță, procentul de pătare, nu poate fi spălată etc.), iar testele independente certifică faptul că sistemul îndeplinește standardele naționale și funcționează conform pretențiilor producătorului. Este importantă testarea pe bancnotele reale, deoarece există pe piață tipuri mai ieftine de cerneală care funcționează bine cu bancnotele falsificate/false, dar nu și cu bancnotele reale: ceea ce înseamnă că cerneala poate fi îndepărtată de pe bancnotele veritabile prin spălare. În plus, se recomandă adăugarea în cerneală a unui marker folosit în criminalistică, ceea ce face posibilă investigarea unei legături între bancnotele pătate și o anumită scenă a infracțiunii.

Bunele practici arată că IBNS poate fi foarte eficient, în special în combinație cu alte măsuri preventive. În 2015, Franța a introdus noi legislații, inclusiv articole privind instalarea IBNS-urilor și utilizarea de cerneală cu ADN unic. Poliția militară franceză (jandarmeria) este cea care, pe baza unei evaluări a riscurilor, decide unde trebuie puse în aplicare IBNS-ul și alte măsuri. Întrucât noua legislație a consolidat abordarea preventivă și operațională, numărul atacurilor a scăzut de la 300 în anul 2013 la 50 în anul 2018.

O altă tehnică în curs de dezvoltare pentru a dezvălui prada este folosirea **lipiciului**. Eficacitatea lipiciului a fost dovedită în Olanda, dar costurile de implementare și de funcționare sunt în prezent ridicate. Mai mult decât atât, lipiciul poate reprezenta un pericol de incendiu dacă sistemul nu este activat înainte de un atac, deoarece dispersia particulelor de lipici în aer ar putea produce un amestec de combustibil. Această metodă nu este încă pregătită pentru piață, dar ar putea fi o soluție pentru viitor.

3.2 Creşterea riscului

O a doua axă pentru prevenirea atacurilor fizice asupra bancomatelor este de a descuraja potențialii făptuitori privind săvârșirea infracțiunilor prin creșterea riscului de depistare și pedepsire. Pe lângă riscul de vătămare corporală atunci când se utilizează explozivi pentru atacuri asupra bancomatelor, principalul risc pentru un infractor este o pedeapsă cu închisoarea atunci când este prins fie în flagrant („în fapt"), fie după o investigație. Pentru a reduce dorința potențialilor făptuitori, riscul depistării și pedepsirii trebuie crescut. Pentru societate, prinderea și condamnarea infractorilor este desigur și o metodă de prevenire foarte eficientă dacă există pedepse ulterioare, după cum am văzut în mai multe țări.

Schimbul de informaţii

Cheia depistării și pedepsirii atacatorilor de bancomate este schimbul de informații între toate părțile interesate în lupta împotriva atacurilor fizice asupra bancomatelor, inclusiv furnizorii de bancomate, autoritățile de aplicare a legii (poliție, procuror etc.), autoritățile publice, producătorii atât de bancomate, cât și de dispozitive de securitate și de protecție, asociațiile profesionale, furnizorii de bancomate (bănci și furnizori independenți),

companiile de securitate și centrele de alarmă. În mod ideal, acest lucru ar trebui să se întâmple atât la nivel național, cât și la nivel internațional.

Detectarea timpurie a unui atac fizic viitor asupra bancomatului este dificilă. Numai în cazurile schimburilor de informații aproape ireproșabile, la nivel internațional, între partenerii de aplicare a legii și partenerii privați (companiile de securitate și furnizorii de bancomate) este posibilă detectarea timpurie. Trebuie monitorizată o gamă largă de indicatori, inclusiv mesaje de avertizare timpurie între agențiile de aplicare a legii cu privire la OCG-uri în mișcare, informații despre vehicule („vizate") care au fost utilizate în atacuri asupra bancomatelor, informații de la companii de securitate sau paza de cartier cu privire la un comportament suspect detectat în zona care înconjoară bancomatul, tranzacțiile suspecte detectate de furnizorii de bancomate și alte metode de detectare. Alte măsuri posibile ale poliției pentru detectarea timpurie sunt monitorizarea mașinilor furate, a producătorilor și distribuitorilor de explozivi și a companiilor autorizate să utilizeze explozivi. Eforturile necesare pentru obținerea depistării timpurie sunt solicitante și nu au nicio garanție de succes, prin urmare intervențiile de aplicare a legii înainte de atac sunt rare.

Dacă nu este posibilă detectarea timpurie, centrele de alarmă pot emite rapid un avertisment în caz de atacuri fizice asupra bancomatelor. Pentru a permite intervenția, reglementările și protocoalele naționale pentru comunicarea rapidă între centrele de alarmă și serviciile de aplicare a legii trebuie să fie convenite și stabilite. În cazul detectării timpurii sau a informațiilor în timp real, forțele de ordine vor trebui să evalueze întotdeauna sincronizarea și cea mai bună oportunitate de intervenție. Prinderea în fapt a infractorilor este foarte dificilă și poate duce la situații periculoase, deoarece unele OCG-uri sunt foarte violente și folosesc armament greu.

Pentru o investigație de succes după atacul fizic asupra unui bancomat, ofițerii de aplicare a legii trebuie să comunice cu toate părțile interesate, deoarece oricare dintre acestea ar putea deține informații care să contribuie la succesul unei investigații. Desigur, comunicarea și colaborarea cu victimele principale, băncile sau alți furnizori de bancomate sunt necesare: aceștia au acces la date importante pentru investigație. Pentru furnizorul de bancomate, informațiile din partea serviciilor de aplicare a legii vor ajuta la îmbunătățirea măsurilor preventive. Mai mult, legăturile cu asociațiile profesioniste și producătorii se dovedesc a fi utile: acestea trimit adesea mesaje de alertă privind securitatea la care se pot abona și alte părți interesate. Producătorii de bancomate au o imagine de ansamblu bună asupra diferitelor tipuri de atacuri asupra bancomatelor și a punctelor slabe și forte corespunzătoare ale măsurilor preventive. Aceștia sunt foarte dispuși să susțină poliția cu informații despre aspectele tehnice ale bancomatelor și cu privire la modurile de operare utilizate.

Cooperarea transfrontalieră este esențială: țările ar trebui să facă schimb de informații (cu privire la suspecți, atacatori de bancomate condamnați, moduri de operare, vehicule suspecte, imagini cu atacuri etc.), nu numai pentru susținerea investigației, ci și pentru că suspecții condamnați într-o altă țară pot fi condamnați pentru reluarea atacurilor/recidivă.

În cele din urmă, crearea unei baze de date la nivel european, disponibilă serviciilor de aplicare a legii și care conține date criminalistice (de exemplu, privind diferite tipuri de cerneală pentru IBNS, marcatori și markere sau privind sticla de protecție pentru bancomate) ar putea susține puternic investigațiile și conecta suspecții de o anumită scenă a crimei. Standardizarea tehnologiilor la nivel internațional este adesea insuficientă: în cadrul conferinței din ianuarie 2019, participanții au menționat că standardizarea la nivel european a cernelii și etichetelor privind criminalitatea ar putea facilita considerabil investigațiile.

Televiziune cu circuit închis şi dispozitive de ascultare

Datele imaginilor și sunetelor din sistemele televiziunii cu circuit închis și dispozitivele de ascultare pot ajuta atât la detectarea în timp real a unui atac (de exemplu, pentru a preveni vătămarea corporală a echipelor de intervenție care ajung la locul infracțiunii), cât și la investigațiile ulterioare (de exemplu, pentru a identifica făptuitorii și modul de operare). Imaginile televiziunii cu circuit închis pot fi combinate cu imaginile din sistemele publice și din alte sisteme de televiziune cu circuit închis din vecinătatea bancomatului și a înregistrărilor dispozitivelor radar pentru a oferi o imagine mai completă a făptuitorilor și a modului de operare.

Cu toate acestea, imaginile televiziunii cu circuit închis au adesea de calitate slabă sau nu sunt stocate corespunzător. Imaginile trebuie să aibă o calitate suficient de bună pentru a permite identificarea unei persoane. Din nou, stabilirea standardelor europene pentru televiziunea cu circuit închis pentru securitate ar facilita investigațiile. De asemenea, întrucât făptuitorii dezactivează adesea televiziunea cu circuit închis înainte

de atac, ar putea fi luată în considerare și instalarea televiziunii cu circuit închis sau a dispozitivelor de ascultare în timp real astfel încât să nu fie vizibile.

Pedepsirea și reabilitarea infractorilor

Pedeapsa consecventă și severă se dovedește a avea un efect preventiv. Arestarea unui OCG are un efect imediat asupra numărului de atacuri asupra bancomatelor. Cu toate acestea, eliberarea din închisoare a atacatorilor de bancomate duce adesea la un nou val de atacuri. Aceasta înseamnă că sentințele scurte duc la reluarea rapidă a atacurilor de către infractori. Sancțiunile minime și maxime pentru infractorii condamnați pentru fiecare tip de atac fizic asupra bancomatelor variază în funcție de statele membre. Unele persoane cred că sancțiunile mai mari îi vor descuraja pe potențialii făptuitori. Cu toate acestea, cercetările științifice[5] arată că mărirea severității sentințelor nu intensifică neapărat efectul de descurajare. Prin urmare, ar putea fi interesant să analizăm programele de reabilitare corecțională (și speciale pentru infractori) pentru a reduce nivelul ridicat al recidivei.

3.3 Creşterea efortului

Cea de-a treia axa pentru prevenire a atacurilor fizice asupra bancomatelor include acțiuni care fac mai solicitantă efectuarea infracțiunii pentru infractor.

Asigurarea unui mediu rezistent la infracţiuni

Dacă evaluarea riscurilor (conform celor de mai sus) arată că un bancomat este situat într-un mediu cu risc ridicat, locația ar trebui desființată și bancomatul transferat într-o zonă cu risc scăzut sau mediu. Acesta este cu siguranță cazul în care analiza demonstrează că există posibilitatea prăbușirii clădirii dacă un bancomat este atacat utilizând explozivi. Legislația ar putea fi implementată pentru a aplica astfel de măsuri în cazuri cu risc ridicat. Pe lângă reducerea numărului de bancomate în medii cu risc ridicat, ar trebui încurajate plățile fără numerar pentru a reduce nevoia de bancomate.

Dacă nu este posibilă transferarea bancomatului, trebuie luat un număr maxim de măsuri de securitate: de ex., utilizarea unor stâlpi de oprire pentru atacurile prin folosirea unui obiect ca berbec, stâlpi de iluminat și alte piese de mobilier stradal pentru a restricționa accesul în clădire, sisteme de oprire a vehiculelor, instalarea de sisteme adecvate pentru iluminatul stradal, un nivel mai strict al supravegherii normale sau sub acoperire și dispozitive anti-furt, cum ar fi un sistem de degradare a bancnotelor. Atunci când o locație este atacată într-o locație care nu a fost identificată cu risc ridicat, aceasta trebuie identificată ca atare și trebuie adăugate măsuri suplimentare de securitate. Noii factori trebuie luați în considerare în instrumentul de evaluare a riscurilor pentru a-l putea actualiza. Reevaluarea acestui risc trebuie să fie o operațiune recurentă.

Consolidarea bancomatelor

Producătorii de bancomate oferă o gamă standard de bancomate care dețin o serie de caracteristici de siguranță, care sunt evaluate conform gradelor de securitate ale Comitetului European de Standardizare (CEN). În general, bancomatele au un marcaj CEN care variază de la gradul inferior CEN1 la cel mai înalt, CEN4. Caracteristici precum rezistența corpului și rezistența la atacuri determină gradul. Rezistența la gaz este oferită ca opțiune în majoritatea cazurilor (CEN-GAS). Modelele standard pot fi îmbunătățite cu măsuri de protecție suplimentare. De obicei, terții instalează aceste caracteristici pentru a asigura respectarea legislației locale și ajustarea modelului de bază la cerințele clienților locali. Caracteristicile suplimentare de securitate includ diverși senzori pentru a activa un sistem de neutralizare a gazelor sau un IBNS în cazul unui atac *la fața locului* sau a unui atac cu explozivi și obloane îmbunătățite și încuietori pentru seif pentru a împiedica accesul neautorizat la seif unde oblonul principal este compromis. Pentru bancomatele portabile, independente, este important să folosiți sisteme de ancorare care oferă o protecție suplimentară împotriva atacurilor prin smulgere/prin folosirea unui obiect ca berbec. Sistemele de urmărire pot fi incluse în bancomate pentru a ajuta investigatorii atunci când acestea sunt transportate într-o altă locație înainte de deschidere.

Măsuri la nivel arhitectural

La instalarea unui bancomat, se recomandă folosirea aparatelor la care accesul se face în partea din spate. În acest caz, făptuitorul trebuie să intre în clădire și să obțină acces în partea din spate a aparatului pentru a fura numerarul. Bancomatele portabile și independente sunt cele mai vulnerabile. O reducere a numărului acestor bancomate ar crește nivelul de securitate. Obligația de a instala bancomatele într-o cameră antiefracție ar reduce automat folosirea bancomatelor independente.

Sistem cu ceaţă

Un tun de ceață umple rapid o cameră cu o ceață densă, astfel încât intrusul să nu poată vedea nimic. Această ceață pentru securitate face deseori imposibilă executarea atacului asupra bancomatului. În cel mai rău caz, sistemul încetinește făptuitorul, oferind timp serviciilor de poliție pentru a interveni. Sistemul de securitate cu ceață este conectat la sistemul de alarmă și poate fi activat în două moduri. Poate fi declanșat automat de senzori de alarmă, cum ar fi detectoare de mișcare (noaptea) sau senzori de manipulare a obloanelor bancomatelor. Poate fi activat și de un centru de alarmă pentru a evita prea multe alarme false. Pentru bancomatele exterioare din perete, sistemul cu ceață poate fi aplicat în partea din spate a bancomatului, pentru a umple încăperea din spate cu ceață și pentru a reduce vizibilitatea făptuitorilor la zero.

Sistemele cu ceață pot asigura protecție într-un anume punct unui bancomat amplasat în spații deschise în benzinării, supermarketuri etc. Astfel, se evită umplerea întregii zone cu ceață. Protecția cu ceață are cel mai mare succes atunci când ceața este emisă din unghiuri diferite sau când umple spațiul din spatele bancomatului, în cazul

unui atac prin folosirea unui obiect ca berbec.. Se desfășoară teste pentru a vedea dacă tunurile de ceață pot fi instalate în bancomatul propriu-zis și nu în camera în care este amplasat bancomatul. Markerele ADN care pătează făptuitorii și îmbrăcămintea acestora pot fi adăugate cerii.

3.4 Măsuri paralele

Pentru a asigura implementarea eficientă și eficace a măsurilor preventive menționate mai sus, trebuie luate în considerare o serie de măsuri paralele. Aceste măsuri sunt indispensabile pentru a permite sau consolida o abordare holistică preventivă și operațională pentru a aborda atacurile fizice asupra bancomatelor.

Legislaţia

Într-o serie de țări, legislația obligă furnizorii de bancomate să ia măsuri preventive. În alte țări, stabilirea de clauze și acorduri între bănci și agențiile de aplicare a legii asigură o abordare corectă pentru a aborda atacurile fizice asupra bancomatelor. Zonele în care pot fi luate în considerare măsurile de reglementare includ:

- integrarea măsurilor preventive;
- cadre legale care să permită colaborarea dintre serviciile de aplicare a legii și partenerii publici și privați;
- o reelaborare a sentințelor dacă sancțiunile pentru făptuitorii de atacuri fizice asupra bancomatelor sunt prea mici.

Cu toate acestea, de multe ori numai instituțiile bancare sunt obligate să se conformeze, iar furnizorii independenți de bancomate nu sunt obligați să respecte aceste legi sau acorduri. Acesta este un punct slab comun într-un cadru de reglementare.

Anumite țări nu pun în aplicare nicio reglementare, dar încearcă să convingă furnizorii de bancomate să ia măsuri preventive prin creșterea gradului de conștientizare a zonelor de criminalitate și a tendințelor: în țările cu un număr mare de bănci independente, acest lucru se dovedește a fi deosebit de dificil.

Este imperativ să ne asigurăm că punerea în aplicare eficientă a măsurilor preventive include modificări ale legislației și reglementărilor atât la nivel național, cât și la nivel internațional care obligă toate tipurile de furnizori de bancomate. În mod ideal, legislația trebuie să fie aliniată la nivelul U.E. pentru a evita ca măsurile preventive dure integrate în legislația unei țări să determine deplasarea OCG-urilor către alte țări cu reglementări mai puțin stricte.

Strategie media

O altă axă importantă a strategiei preventive este o strategie media bine pusă la punct, care are drept scop reducerea așteptărilor și dorinței atacatorilor de bancomate de a se implica în această infracțiune. Trebuie subliniate ratele scăzute de succes și riscurile mari pentru făptuitori; comunicarea cu privire la recompense („pradă”) sau la detaliile despre atacul asupra bancomatului, cum ar fi tipul de bancomat afectat sau modul de operare. Pe de altă parte, este necesară o comunicare extinsă cu privire la arestarea suspecților și la pedeapsa consecventă după o condamnare.

Colaborare îmbunătăţită

Colaborarea îmbunătățită și schimbul de informații au fost menționate pe larg, dar nu pot fi suficient de evidențiate. Schimbul de informații operaționale la nivel

internațional este principala activitate a Europol. Pe lângă acest schimb de informații, conferința de prevenire a arătat nevoia clară de creștere a nivelului de cooperare multidisciplinară și pe mai multe niveluri și a schimbului de informații între toate părțile interesate relevante, inclusiv agențiile de aplicare a legii, autoritățile publice, producătorii de bancomate și dispozitive de securitate și protecție, asociațiile profesionale, furnizorii de bancomate (bănci și furnizori independenți), companiile de securitate și centrele de alarmă. Aceasta trebuie să includă nivelul local, național și internațional.

Reducerea riscului de daune colaterale

În cazul atacurilor cu explozivi solizi, unele OCG-uri vor lăsa materiale în urmă. Acest lucru poate crea situații periculoase pentru echipele de intervenție sau civili (fie pentru cei care locuiesc în cartier, fie pentru trecători). Siguranța acestora trebuie asigurată. Așa cum se întâmplă în Belgia, protocoalele și procedurile care trebuie urmate de echipele de intervenție (atât cele furnizate de serviciile de aplicare a legii, cât și cele din partea furnizorilor de bancomate) trebuie să fie dezvoltate și aliniate împreună. O altă bună practică în acest context este exemplul Olandei, în care se utilizează imagini ale televiziunii cu circuit închis de la atacul asupra bancomatului pentru a evalua situația. Se pot stabili acorduri cu centrele de alarmă pentru ca aceste imagini să fie puse la dispoziție imediat.

Prevenţie socială

Adesea, OCG-urile caută tineri pentru a-i recruta. Proiectele ar putea fi create pentru a frustra aceste procese de recrutare într-o etapă timpurie. Poliția sau asistenții sociali trebuie să fie atenți la aceste procese și pot interveni prin abordarea personală a potențialilor făptuitori.

04 CONCLUZII

În ultimii doi ani, numărul țărilor europene afectate de atacurile fizice asupra bancomatelor a crescut. În acest sens, Europol și EUCPN au lucrat împreună pentru a aduna cele mai bune măsuri pentru combaterea și prevenirea acestei infracțiuni.

O abordare de succes pentru combaterea atacurilor fizice asupra bancomatelor constă într-o combinație de măsuri operaționale și preventive, de preferat integrate într-un cadru legislativ. Pentru a evita ca măsurile dure dintr-o țară să determine deplasarea OCG-urilor către țări mai vulnerabile, se recomandă adoptarea acestor măsuri la nivel european.

Pentru prevenirea și combaterea acestui tip de infracțiune, ar trebui stabilită o strategie clară în trei etape: evaluarea situației, dezvoltarea unei abordări preventive bazate pe evaluarea riscurilor și punerea în aplicare a măsurilor preventive.

Evaluarea riscurilor pentru atacurile fizice asupra bancomatelor ar trebui să includă caracteristicile bancomatului și a împrejurimilor acestuia, cooperarea cu partenerii și părțile interesate pentru a construi alianțe pentru combaterea acestei infracțiuni și evaluarea cadrului preventiv și legal. Odată evaluată situația, ar trebui stabilită o strategie bazată pe colaborarea publică și privată și măsurile preventive și operaționale. Scopul măsurilor preventive este de a reduce intenția și capacitățile făptuitorului de a se implica într-un atac fizic asupra bancomatului. Pentru realizarea acestui lucru, sunt propuse trei axe ale acțiunilor preventive: reducerea recompenselor, creșterea riscului și creșterea efortului. Măsurile paralele ar trebui să finalizeze strategia preventivă. Instaurarea unei autorități naționale care are puterea de a impune aceste măsuri necesare este cea mai bună practică.

Prin **reducerea recompenselor,** dorința infractorului de a se implica în acest tip de infracțiune scade. Reducerea sumei de numerar din bancomat prin limitarea numerarului alimentat la cel suficient pentru o zi de tranzacționare sau golirea bancomatelor (a celor mai vulnerabile) noaptea este o măsură pentru a reduce așteptările infractorului. O altă metodă este dezvăluirea prăzii și marcarea banilor. În acest context, poate fi aplicat sistemul IBNS, care pătează bancnotele și le marchează ca fiind furate. Această metodă este cea mai eficientă atunci când este imposibil ca infractorii să cheltuiască acești bani sau să reintroducă aceste bancnote în sistemul juridic de numerar. Acest lucru poate fi obținut de către bănci și public prin neacceptarea bancnotelor pătate pentru plată și instalând acceptoare de bancnote care pot detecta și refuza bancnotele pătate. În această privință, investiția în sisteme cu infraroșu care detectează bancnotele colorate cu markere infraroșii s-a dovedit a fi o soluție rentabilă în Belgia și Franța. Atunci când instalează sisteme IBNS, țările ar trebui să ia în considerare în detaliu mecanismele de activare alese, cerințele minime pentru neutralizarea bancnotelor și adăugarea unui marker folosit în criminalistică în cerneală.

Măsurile care îi determină pe potențialii făptuitori de săvârșire a infracțiunilor prin **creșterea riscului** de depistare și pedeapsă, reprezintă a doua axă pentru prevenirea atacurilor fizice asupra bancomatelor. Cheia depistării și pedepsirii atacatorilor de bancomate

este colectarea și schimbul de informații între toate părțile interesate, atât la nivel național, cât și la nivel internațional. Schimbul de informații privind imaginile de înaltă calitate și datele sonore ale televiziunii cu circuit închis poate crește șansele de detectare timpurie și investigare reușită. Pentru a evita dezactivarea înainte de atac a televiziunii cu circuit închis sau a dispozitivelor de ascultare, poate fi luată în considerare instalarea televiziunii cu circuit închis sau a dispozitivelor de ascultare în timp real astfel încât să nu fie vizibile. Crearea unei baze de date criminalistice și standardizarea tehnologiilor la nivel european ar putea facilita în mare măsură cooperarea și investigațiile la nivel internațional. Dacă infractorii sunt prinși și condamnați, ar putea fi interesant să analizăm programele de reabilitare corecțională (și speciale pentru infractori) pentru a reduce nivelul ridicat al recidivei.

A treia axa de prevenire a atacurilor fizice asupra bancomatelor include măsuri pentru **creșterea efortului** necesar unui infractor pentru a efectua infracțiunea. Instalarea unui bancomat într-un mediu rezistent la infracțiuni, cu un număr maxim de măsuri de securitate, va face atacarea acestuia de către un infractor mult mai solicitantă. În plus, protecția standard pentru bancomate poate fi îmbunătățită cu o serie de caracteristici suplimentare de securitate. Pe lângă aceste măsuri, instalarea unui sistem cu ceață poate descuraja făptuitorul sau, în cel mai rău caz, poate încetini atacul.

Un număr de **măsuri paralele** va consolida măsurile menționate mai sus, cum ar fi crearea unui cadru legal care obligă toți furnizorii de bancomate să pună în aplicare măsurile preventive, dezvoltarea unei strategii media bine stabilite, colaborarea îmbunătățită la nivel local, național și internațional, orientările pentru echipele de intervenție pentru a reduce riscul de daune colaterale și investiția în prevenția socială pentru a submina procesele de recrutare în activități infracționale.

RECOMANDĂRI PENTRU O ABORDARE PREVENTIVĂ: PREZENTARE GENERALĂ

Dezvoltarea unui răspuns eficient pentru a preveni atacurile fizice asupra bancomatelor

Evaluarea situaţiei

> Stabiliţi profilul de riscuri al bancomatelor din ţara/ regiunea dvs.

> Identificaţi partenerii şi părţile interesate în lupta împotriva atacurilor fizice asupra bancomatelor şi evaluaţi colaborarea.

> Evaluaţi cadrul legal pentru combaterea atacurilor fizice asupra bancomatelor la nivel naţional şi internaţional.

Dezvoltarea unei abordări preventive

> Determinaţi (principalele) riscuri ce trebuie acoperite şi priorităţile.

> Determinaţi cele mai bune măsuri preventive pentru a acoperi aceste riscuri luând în considerare trei axe principale.

> Determinaţi măsurile preventive paralele necesare pentru a întări măsurile preventive luate.

Măsuri preventive ce pot fi luate pentru a

01

Reduce recompensele

> Reducerea sumei de bani în numerar.
  - Golirea bancomatelor noaptea.
  - Creşterea numărului/frecvenţei de alimentări.
> Dezvăluirea prăzii.
  - Sisteme inteligente de neutralizare a bancnotelor (IBNS).
  - Markere infraroşii în cerneala sistemelor IBNS pentru a detecta bancnotele pătate cu ajutorul acceptoarelor de bancnote.
  - În curs de dezvoltare: lipici.

02

Creşte riscul

> Schimb de informaţii transfrontalier pentru:
  - detectarea timpurie sau în timp real a unui atac posibil asupra bancomatului,
  - consolidarea abordării operaţionale,
  - condamnarea infractorilor revidivişti,
  - schimbul de date criminalistice la nivel european.
> Televiziune cu circuit închis şi dispozitive de ascultare.
> Pedepsirea consecventă şi reabilitarea infractorilor.

03

Creşte efortul

> Asigurarea unui mediu rezistent la infracţiuni.
  - Schimbarea locaţiilor bancomatelor cu risc ridicat.
  - Măsuri de securitate: obstacole fizice, supraveghere etc.
> Consolidarea bancomatelor cu obloane, făcându-le rezistente la gaz sau explozivi solizi etc.
> Măsuri la nivel arhitectural, precum aparate cu acces în partea din spate.
> Sisteme de securitate cu ceaţă.

Măsuri paralele pentru consolidarea abordării preventive

> Legislaţie eficientă, inclusiv măsuri preventive împotriva atacurilor fizice asupra bancomatelor, condamnarea consecventă etc.

> Strategie media eficientă pentru descurajarea făptuitorilor.

> Colaborare îmbunătăţită între toate părţile interesate (publice, private, serviciile de aplicare a legii) în lupta împotriva atacurilor fizice asupra bancomatelor.

> Reducerea riscului de daune colaterale în rândul echipelor de intervenţie sau a civililor (de ex., cei care trăiesc în cartier sau trecătorii).

> Prevenţia socială pentru a evita recrutarea tinerilor pentru (acest tip de) infracţiuni.

ENDNOTES

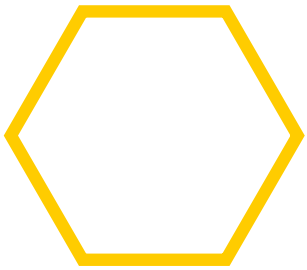
1 () Willem Pieter de Groen, Zachary Kilhoffer and Roberto Musmeci, The future of EU ATM markets: impacts of digitalisation and pricing policies on business models, CEPS report, 2018

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