Fizinių bankomatų atakų prevencija

Veiksmingo požiūrio kūrimas

Pripažinimas
Šis dokumentas yra Europos Sąjungos teisėsaugos bendradarbiavimo agentūros (Europolo) ir Europos nusikalstamumo prevencijos tinklo (EUCPN) sekretoriato bendradarbiavimo rezultatas. Norėtume padėkoti fizinių bankomatų (ATM) atakų ekspertams, kurie investavo laiką ir jėgas remdami šio rekomendacinio darbo kūrimą. Jie prisidėjo dalyvaudami fizinių bankomatų atakų prevencijos konferencijoje (2019 m. sausio mėn., Briuselis) ir teikdami svarbią informaciją. Ypač norėtume padėkoti teisėsaugos agentūroms iš ES ir ne ES („trečiųjų“) šalių, privačiajam sektoriui, įskaitant bankomatų pramonės asociaciją (ATMIA), „BPost“, „Centrum voor Criminaliteitspreventie en Veiligheid“ (CCV), Diebold Nixdorf, Europos saugių operacijų asociacijos bankomatų ir [automatinių kasų seifų] ATS fizinių atakų (EAST EGAP) ekspertų grupei, Europos intelektualiųjų grynųjų pinigų apsaugos asociacijai („Euricpa“), ING, „Febelfin“, NCR, „Protect“, „SIOC Banking“, „Spinnaker“, „TMD Security“ ir Belgijos, Kroatijos, Vokietijos ir Ispanijos vidaus reikalų ministerijoms.

Teisinis įspėjimas
Šio leidinio turinys nebūtinai atspindi oficialią bet kurios ES valstybės narės ar bet kurios ES ar Europos Bendrijų agentūros ar institucijos nuomonę.

Turinys

1 Kontekstas

Didėjant fizinių bankomatų (ATM) atakų ir nukentėjusių Europos šalių skaičiui, Europos nusikalstamumo prevencijos tinklas (EUCPN) ir Europolas surengė konferenciją (2019 m. sausio mėn.), sukviesdami teisėsaugą kartu su viešaisiais ir privačiaisiais partneriais aptarti šio nusikaltimo prevenciją. Šiame rekomendaciniame dokumente apibendrinamos šios konferencijos išvados, siekiant atkreipti valdžios institucijų dėmesį į fizines bankomatų atakas ir prevencines priemones.

Daugybę skirtingų metodų (*modi operandi* (MO)), kuriuos nusikaltėliai naudoja puolant bankomatus, galima suskirstyti į dvi pagrindines kategorijas: fizines bankomatų atakas ir su bankomatais susijusias sukčiavimo atakas (tai apima bankomatų loginius ir kenkėjiškų programų išpuolius). Straipsnyje dėmesys sutelkiamas į fizines bankomatų atakas: priverstinį patekimą į bankomatus fizinėmis priemonėmis norint išimti grynųjų. Priverstinis patekimas gali būti įvykdytas šiomis priemonėmis:

- sprogmenų naudojimas: užpuolikai naudoja dujas ar kietus sprogmenis, kad fiziškai pažeistų bankomatų seifą ir gautų grynųjų pinigų;
- „rip-out/ram-raid“ išpuoliai: užpuolikai fiziškai pašalina bankomatą iš įrengimo aplinkos, dažnai naudodamiesi aukščiausios klasės transporto priemone;
- „in situ“ atakos: užpuolikai, naudodamiesi brutalia jėga, perpjauna seifą, dažnai naudodami pjovimo ar laužymo įrankius, tokius kaip kampiniai šlifuokliai, plaktukai ar oksiacetileno degikliai.

Ribotas, tačiau vis didėjantis, Europos Sąjungos šalių skaičius susiduria su fizinėmis bankomatų atakomis. Manoma, kad 2017 m. padarytas finansinis nuostolis Europoje viršys 30 mln. EUR. Kai kurios šalys ir toliau patiria nemažai fizinių atakų prieš bankomatus, kitose per pastaruosius 2 metus labai padaugėjo tokių incidentų. Ši nusikalstamumo sritis greitai vystosi. Kai kurios šalys sėkmingai taikė fizinių bankomatų atakų problemą ir pastaruoju metu pastebėjo, kad išpuolių sumažėjo. Kita vertus, šalys, kurios anksčiau nebuvo paveiktos, susidūrė su staigiu 2018 m. fizinių bankomatų atakų padaugėjimu dėl organizuoto nusikalstamumo grupuočių (ONG), plečiančių savo teritoriją. Tai paveikia ne tik bankus. Vis dažniau puolama nepriklausomų tiekėjų bankomatų, nes jie dažnai yra pažeidžiamose patalpose ar vietose.

2 Veiksniai, lemiantys fizinės bankomatų atakos sėkmę

Bankomatų atakų sėkmės procentas yra žemas; tik trečdalis atakų būna sėkmingos. Tačiau net tada, kai užpuolimas nesėkmingas, ne mažiau svarbi yra ir pastatų konstrukcijoms padaryta žala (pvz., sprogmenys), todėl vietos gyventojai, pirmosios pagalbos teikėjai ir praeiviai nepalieka nesaugios aplinkos nusikaltimo vietoje.

Fizinės atakos sėkmė priklauso nuo daugelio veiksnių, įskaitant; bankomatų ypatybes, bankomatų atakų sąranką ir nusikaltėlių patirtį bei žinias.

2.1 Bankomatų pažeidžiamumas

Labiausiai pažeidžiami yra išorėje (einantys per sieną (angl. „through the wall“, TTW)) arba pastatuose įrengti bankomatai. Atakuodami vidinį (atskirą) bankomatą, organizuoto nusikalstamumo grupuotės renkasi bankomatus, esančius komercinėse patalpose, o ne bankomatus, esančius banko patalpose, kur paprastai stebėjimas yra stipresnis. Bankai daugiausia valdo bankomatus, esančius banko pastate arba už jo ribų. Bankų nutolusios vietos („banko nuotolinė vieta“) gatvėje arba prekybininkų komercinėse patalpose, tokiose kaip degalinės, prekybos centrai, viešbučiai, kazino, oro uostai ir kt., pamažu tampa vis svarbesnės uždarant banko skyrius. Nepriklausomi paslaugų teikėjai bankomatus valdo kaip savarankišką paslaugą. Jų bankomatai dažnai būna mažmeninės prekybos vietose, svetingumo ir laisvalaikio vietose, transporto vietose (geležinkelio stotyse, oro uostuose ir kt.), viešuose pastatuose ir gatvėse.

Augant internetinės bankininkystės populiarumui, tikėtina, kad ateinančiais metais daugelis bankų skyrių bus uždaryti, dėl to bendras bankomatų skaičius sumažės. ([1]) Tačiau dėl to gali padidėti nutolusių bankomatų ir nepriklausomų teikėjų bankomatų, esančių pažeidžiamose vietose, skaičius.

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

2.2 ATM atakos nustatymas

Pasirengimas atakai gali užtrukti keletą savaičių ar net mėnesių. Pažeidėjai turi surinkti reikiamus **įrankius ir išteklius**, tokius kaip transporto priemonės, įranga ir kontaktiniai punktai. **Transporto priemonės** yra svarbi fizinių bankomatų atakų priemonė; nusikaltėliai dažniausiai keliauja automobiliu ir po išpuolio dažniausiai pabėga greitosiomis transporto priemonėmis. Jos dažnai yra vogtos, tačiau jas taip pat galima išsinuomoti ar įsigyti (pvz., internetu). Daugelį fizinių bankomatų atakų **įrangos** galima lengvai ir teisėtai įsigyti įprastose parduotuvėse. Tai dar labiau sumažina patekimo į šią nusikalstamą sritį slenkstį. Teisėsaugai sunku atsekti įrankio kilmę, todėl kaltininkams rizika yra nedidelė. Organizuoto nusikalstamumo grupuotės, aktyviai dalyvaujančios fizinėse ATM atakose tarptautiniu lygiu, beveik visada turi kontaktinius centrus tikslinėje šalyje (žmonės, kurie ten gyvena tam tikrą laiką) arba, priešingai, jie gali naudoti „smok ir bėk“ techniką. Šie kontaktai palaiko vietines organizuoto nusikalstamumo grupuotes logistikos klausimais, tokiais kaip būsto nuoma, transporto priemonės ar kitos įrangos įsigijimas ir žvalgymo tikslai. Kai kurie tarptautiniai nusikaltėliai visiškai palieka logistiką ir žvalgybą vietiniams kontaktams ir tiesiog keliauja keliais ar oru, kad įvykdytų bankomatų ataką.

Organizuoto nusikalstamumo grupuotės dažnai vykdo intensyvią **žvalgybą**, kad nustatytų tinkamus taikinius; įvertintų bankomato pildymo dienos laiką, bankomato aplinką, bankomatų techninę specifiką, evakuacijos kelius ir galiojančias saugumo priemones, tokias kaip uždarosios grandinės televizija (CCTV), aliarmo jutikliai ir užraktai.

Kai kurios organizuoto nusikalstamumo grupuotės imasi daugybės veiksmų, kad prieš ataką **suklaidintų teisėsaugos ir saugumo tarnybas**. Jie pažeidžia signalizacijos sistemas ir viešąjį apšvietimą, naudoja nukreipimo techniką, nustato kelio blokus ar bando sugadinti teisėsaugos transporto priemones.

2.3 Nusikaltėlių patirtis ir praktinės žinios

Fizinės bankomatų atakos yra patrauklios nusikaltėliams, nes pinigai yra iškart prieinami ir nereikia plėsti tinklo pavogtoms prekėms. Tai yra patogi alternatyva nusikaltėliams, jau vykdantiems organizuotus su nuosavybe susijusius nusikaltimus.

Organizuoto nusikalstamumo grupuotės turi sukaupti **reikiamos patirties ir praktinių žinių**, nes tai yra lemiamas atakos sėkmės arba nesėkmės veiksnys. Reikalingos žinios ir reikiama patirtis labai priklauso nuo **atakos tipo**. „Rip-out/ram-raid“ ir „*in situ*“ atakos turi paprastą MO (daugiausia įžūlumas ir žiaurios jėgos panaudojimas), todėl jiems paprastai nereikia specialių įgūdžių. Degiųjų dujų ir kietų sprogmenų atakos reikalauja aukštesnio lygio žinių.

Užpuolikai demonstruoja skirtingą **kompetencijos lygį**. Viena vertus, gerai organizuotos ir patyrusios grupės per kelias minutes gali įvykdyti sėkmingą fizinę bankomatų ataką. Jie kontroliuoja procesą ir sugeba apriboti riziką patys, taip sumažindami ir papildomą žalą. Kita vertus, mažiau organizuotos ir oportunistinės grupės dažnai žlunga bandydamos ir gali padaryti didelę žalą kaimynystėje esančioms patalpoms ir pastatams. Manoma, kad kai kurios mažiau organizuotos nusikalstamos grupuotės grįžta prie tradicinės organizuoto nusikalstamumo, susijusios su nuosavybe, kurių atgraso prevencinės priemonės, kurių neįmanoma įveikti užpuolus bankomatams.

3 Prevencinio požiūrio poreikis

Šalys, kuriose smurtautojai patiria mažą fizinių bankomatų atakų sėkmės procentą arba kuriose fizinių bankomatų atakų skaičius mažėja, rodo, kad sėkmingą kovos su fizinėmis bankomatų atakomis metodą sudaro operatyvinių ir prevencinių priemonių derinys. Kadangi šioje nusikalstamoje srityje aktyvių organizuotų organizuotų nusikalstamų grupuočių skaičius yra ribotas, areštai ir iš to išplaukiančios bausmės gali smarkiai sumažinti išpuolių skaičių. Tačiau išleidę daug bankomatų užpuolikų, jie pradeda savo veiklą. Be to, grupė kartais gali greitai pakeisti areštuotą nusikaltėlį. Todėl labai reikia prevencinių priemonių, kurias geriausia būtų įtraukti į teisinę sistemą. Be to, patirtis rodo, kad prevencijos priemonės vienoje šalyje gali paskatinti organizuotas organizuotas organizacijas nukreipti labiau pažeidžiamus tikslus kitose šalyse. Tik laiko klausimas, kol vienoje šalyje atsirandančios MO išplito į kitas šalis. Tai aiškiai rodo, kad **reikia priimti prevencines ir operatyvines priemones Europos lygiu**, glaudžiai bendradarbiaujant su privačiais, viešaisiais ir teisėsaugos partneriais.

4 Prevencija

Norint užkirsti kelią šio tipo nusikaltimams ir kovoti su jais, reikalinga aiški strategija. Šiame skyriuje apžvelgsime tris veiksmus, kurių paprastai imamasi susidūrus su fizinėmis bankomatų atakomis arba ruošiantis jų išvengti.

Pirmiausia **situacijos vertinimas**; bankomatų ir jų aplinkos rizikos pobūdis turėtų būti nustatytas atsižvelgiant į turimų grynųjų pinigų kiekį (galimą laimikį), netiesioginės žalos riziką ir asmens sužalojimo riziką. Antra, remiantis rizikos vertinimu, turėtų būti parengta **prevencinė strategija**. Galiausiai turėtų būti įgyvendintos **prevencinės priemonės**.

4.1 Įvertinkite situaciją

ONG yra linkę nukreipti arba į konkretaus tipo bankomatus, arba į konkrečių tiekėjų bankomatus, turinčius funkcijas, palengvinančias bankomatų ataką. Todėl būtina atlikti išsamų fizinių bankomatų išpuolių rizikos vertinimą, geriausia įtraukti visą grynųjų pinigų apsaugos grandinę nuo tranzito iki pristatymo iki saugojimo bankomate. Norint nustatyti kiekvieno bankomato rizikos profilį, reikėtų išanalizuoti keletą elementų, įskaitant šiuos elementus.

- Vietos ir bankomato aplinkos ypatybės; miesto ar kaimo vietovių, gyventojų tankio, policijos nuovadų artumo, automatinių valstybinių numerių atpažinimo (ANPR) kamerų kaimynystėje, vaizdo stebėjimo kamerų netoliese ir kt.
- Bankomato vieta:
    - pastato viduje arba išorėje, banko skyriuje arba atokiose (pvz., komercinėse) patalpose, įmontuotose ar pritvirtintose prie pastato,
    - autonominiam bankomatui: ar jis yra pritvirtintas, ar ne,
    - įmontuotiems ar pritvirtintiems prie pastato bankomatams: ar nėra architektūrinių trūkumų, kaip organizuojamas grynųjų pinigų saugojimas ir pan.
- Bankomato tipas.
- Į bankomatą įtrauktos saugos funkcijos.
- Grynųjų pinigų kiekis bankomate.
- Fizinių bankomatų išpuolių rūšis ir MO tikimasi, kad pirmiausia būtų imtasi tinkamiausių prevencinių priemonių.

– Jau įgyvendintos apsaugos ir prevencinės priemonės (intelektualiosios banknotų neutralizavimo sistemos (IBNS), vaizdo stebėjimo sistema, apsauginė rūko (matomumo sumažinimo) sistema ir kt.).

Kiti vertintini elementai yra bendradarbiavimo su partneriais ir suinteresuotosiomis šalimis padėtis ir teisės aktai. Reikėtų įvertinti teisėsaugos, privačių ir viešųjų partnerių bendradarbiavimą kuriant aljansus kovai su nusikalstamumu. Gali būti, kad kiekvienas partneris turi įdomios informacijos, kuri padėtų įvertinti situaciją. Vietos policija ar vietos valdžia šioje srityje yra ypač svarbi. Teisės aktai turi būti vertinami nustatant prevencinę teisinę bazę, imantis privalomų prevencinių priemonių, skiriant bausmes už bankomatų išpuolius ir kt.

4.2 Sukurti prevencinį požiūrį

Įvertinus situaciją ir išsiaiškinus pagrindines bankomatų saugumo stipriąsias ir silpnąsias puses, galima sukurti strategiją (dažnai paremtą viešojo ir privačiojo sektorių bendradarbiavimu) ir imtis prevencinių bei operatyvinių atsakomųjų priemonių. Prevencijos priemonėmis turėtų būti siekiama sumažinti kaltininkų ketinimus ir galimybes. Šiam tikslui pasiekti siūlomos trys prevencinių veiksmų kryptys, pagrįstos trimis iš penkių Clarke situacijomis pagrįstų nusikaltimų prevencijos strategijų ([2]); sumažinant atlygį, padidinant riziką nusikaltėliams ir padidinant pastangas apiplėšimui įvykdyti.

Nusikaltėliai subalansuoja laukiamą grąžą ir susijusią riziką (pvz., Su bankomatų išpuoliu). Sumažėjus šansams gauti lengvą atlygį ir padidinant nusikaltėlių riziką, sumažėja jų lūkesčiai ir noras įsitraukti į fizinę bankomatų ataką. Kitos priemonės, padidinančios pastangas norint patekti į bankomatą, daro įtaką nusikaltėlių galimybėms. Oportunistiniai nusikaltėliai, dažnai nesėkmingi, bando nutraukti bankomatų atakas. Profesionaliems bankomatų užpuolikams sėkmės procentas sumažėja, o tai vėlgi daro įtaką grąžos ir rizikos pusiausvyrai.

Be to, prevencinę strategiją papildo lygiagrečios priemonės, tokios kaip veiksminga žiniasklaidos strategija, ankstyva socialinė prevencija ir priemonės, kuriomis siekiama sumažinti užstato žalos pastatams riziką ir užtikrinti vietos gyventojų, pirmosios pagalbos teikėjų ir praeivių saugumą.

([2]) Derek Cornish ir 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.

Galimi ir kiti metodai, kaip susisteminti požiūrį. Nyderlanduose valdžios institucijos taiko vadinamąjį barjerinį modelį ([3]). Šis modelis nustato veiksmus, kuriuos nusikaltėlis turi atlikti padarydamas nusikaltimą. Tai taip pat nustato partnerius ir galimybes, kurios sudaro sąlygas nusikalstamumui, ir tai yra naudinga priemonė organizuoti informacijos rinkimo procesą nusikalstamumo srityje. Nustačius kiekvieną žingsnį, reikalingą įvykdyti fizinę bankomatų ataką, galima nustatyti kliūtis, trukdančias įvykdyti nusikaltimą, ir geriausius partnerius nustatyti kliūtis. Barjerinis modelis taip pat nustato signalus, įspėjančius viešuosius ir privačius partnerius apie fizines bankomatų atakas, ir signalus, kuriuos jie gali išsiųsti patys, kad praneštų valdžios institucijoms apie savo įtarimus.

Norint sušvelninti riziką, kylančią kartu su prevencijos stiprinimu, reikia gerai parengtos strategijos. Prevencinės priemonės, kurios labai veiksmingos siekiant atgrasyti mėgėjus ir kopijas, kartais sukelia nepageidaujamą poveikį. Kai kurios grupės, norėdamos surasti pažeidžiamus bankomatus, naudoja bandymo ir klaidų metodus, palikdami pėdsaką sugadintiems bankomatams. Pavojingesni ir negailestingesni ONG išpuoliuose pradeda naudoti žiauresnius MO, pavyzdžiui, pereidami iš dujų į kietus sprogmenis.

Norint sukurti veiksmingą prevencinių priemonių rinkinį, geriausia praktika yra nacionalinės valdžios institucijos, kuri yra įgaliota įvesti specialias priemones didelės rizikos bankomatams, remiantis išsamia padėties analize, pavyzdys. Šis požiūris pasirodė esąs efektyvus Prancūzijoje, ypač jei nustatyta teisinė sistema ir priemonės įgyvendinamos kartu su operatyvinėmis priemonėmis.

4.3 Įgyvendinkite prevencines priemones

Šiame skyriuje pateiktos fizinių bankomatų išpuolių prevencijos priemonės įrodė savo naudingumą įvairiose šalyse. Jie grindžiami prevencijos konferencijos išvadomis ir prevencinėmis priemonėmis, kurias aktyviai skatina tarptautinės organizacijos, veikiančios bankomatų saugumo srityje. Daugelis priemonių yra gerai žinomos. Kelios šalys jau sėkmingai įgyvendino keletą priemonių. Tačiau dažnai siūlomos priemonės įgyvendinamos tik iš dalies ir nėra įtrauktos į teisės aktus.

Kaip minėta pirmiau, siūlomos trys prevencinių veiksmų kryptys: sumažinti atlygį, padidinti nusikaltėlių riziką ir padidinti pastangas, reikalingas norint pasiekti plėšikavimą.

([3]) Centrum voor Criminaliteitspreventie, barrieremodellen, www.barrieremodellen.nl

4.3.1 Sumažinkite atlygį

Atostogų nuo nusikalstamų veikų sumažinimas yra pirmoji fizinių bankomatų atakų prevencijos kryptis. Kol išliks supratimas apie „lengvus pinigus“, nusikaltėliai užsiims tokio tipo nusikaltimais. Sumažinus turimų grynųjų pinigų kiekį arba pašalinus arba sunaikinant grynuosius, sumažėja įdomių plėšikavimo galimybių. Sumažėję lūkesčiai sumažina nusikaltėlio norą įsitraukti į tokio tipo nusikaltimus.

4.3.1.1 *Mažesnis grynųjų pinigų kiekis*

Viena priemonė atlygiui sumažinti yra bankomate esančių grynųjų pinigų sumažinimas. Idealiu atveju ši suma turėtų būti apribota iki reikiamos sumos tik vienai prekybos dienai. Bankų bendradarbiavimas galėtų užtikrinti ekonominį efektyvumą. Nyderlanduose keli bankai bendradarbiavo kurdami nuo bankų nepriklausomą bankomatų tinklą, vadinamą „Geldmaat“. Bendradarbiavimo tikslas - užtikrinti grynųjų pinigų prieinamumą, prieinamumą, prieinamumą ir saugumą. Tai greičiausiai sumažins bankomatų skaičių. Tačiau kiekviename bankomate nebus daugiau grynųjų, o jie bus papildomi dažniau. Pripildymų skaičius bus pritaikytas pagal poreikį.

Kadangi nusikaltėliai dažniausiai puola bankomatus nuo 03.00 iki 04.00 valandos, griežtai rekomenduojama atskirame bankomate (dažniausiai esančiame komercinėse ir viešosiose vietose, kurie yra labiau pažeidžiami) ištuštinti bankomatą ir perkelti grynuosius pinigus į seifą. dieną. Įspėjamasis ženklas gali informuoti visuomenę, kad bankomatas naktį neturi grynųjų. Kitą dieną bankomatas turėtų būti papildytas, nepastebint klientų ir užrakinus patalpas. Ši sistema įdiegta Prancūzijoje, kur įstatymai įpareigoja mažmenininkus, turinčius parduotuvėje atskirą bankomatą, išimti grynuosius pinigus naktį ir palikti bankomatą atidarytą. Kitų bankomatų atveju turimas sumas galima sumažinti padidinant papildymo dažnį.

4.3.1.2 *Sutrukdymas apiplėšimui ir pinigų atsekamumo užtikrinimas*

Pažangios banknotų neutralizavimo sistemos (IBNS) yra pirmoji premijų sugadinimo technika. Šios sistemos dažo banknotus rašalu, kad pažymėtų juos kaip pavogtus. Prie IBNS rašalo galima pridėti žymeklių ir žymeklių. Šiuo metu šie žymekliai daugiausia naudojami teismo medicinos tikslams, susiejant banknotą su nusikaltimo vieta ir padidinant nusikaltėlių riziką būti sugauti. Nors IBNS yra veiksminga prevencinė priemonė, yra keletas aplinkybių.

Europos centrinis bankas nekompensuoja dažytų banknotų ([4]) (nuo 2003 m.), tačiau nemažai ES valstybių narių nacionalinių centrinių bankų tai vis dar daro. Dažyti užrašai taip pat vėl įvedami į teisinę sistemą per kazino. IBNS sukuria papildomą kliūtį nusikaltėliams, tačiau būtų daug efektyvesnė, jei nusikaltėliams neįmanoma naudoti dažytų banknotų ES. Tam tikslui nacionaliniai centriniai bankai neturėtų sutikti su beicuotais vekseliais. Išimtys gali būti padarytos konkrečioms aplinkybėms, tokioms kaip užrašai, įspausti netikro aktyvavimo metu. Taip pat svarbu patarti gyventojams nepriimti dažytų užrašų. Žvelgiant iš ilgalaikės perspektyvos, banknotų priėmėjai turėtų aptikti beicuotus banknotus ir turėtų būti montuojami bankuose bei komercinėse patalpose, tokiose kaip kazino, automobilių plovyklos ir kt. Aptikti rašalą yra sunku ir brangu, tačiau ekonomiškas sprendimas gali būti įdiegti infraraudonųjų spindulių sistemas, kurios aptinka užrašus, nuspalvintus infraraudonųjų spindulių žymekliais. Šios sistemos įrodė savo veiksmingumą ir yra geriausia praktika Belgijoje ir Prancūzijoje. Kai bankomatai įvedami užrašai su infraraudonųjų spindulių žymekliais, bankomatas priims („praryja“) pinigus, bet neperves jų į sąskaitą. Asmuo, pristatantis dažytus banknotus, taip pat turėtų būti registruotas.

Diegiant IBNS sprendimus yra keletas kitų aspektų. Keli gamintojai teikia daugybę skirtingų IBNS sprendimų su skirtingais aktyvinimo mechanizmais ir skirtingų tipų rašalu. Pirmiausia atsižvelgiama į tai, kad ne visų rūšių IBNS aktyvinimo technologijos gali kovoti su visomis grėsmėmis. Kai kurios IBNS veikia labai gerai, kai yra „rip-out ram-raid“ atakos, *in situ* atakos ir dujų atakos, tačiau neveikia, jei įvyksta ataka naudojant kietuosius sprogmenis ar atvirkščiai. Todėl turėtų būti gerai apsvarstyta pasirinkta technologija.
Kitas aspektas yra rašalo tipas, kurį reikia pasirinkti. Belgijoje nustatyti nacionaliniai minimalūs IBNS reikalavimai (sauga, dažymas procentais, negalima plauti ir tt), o nepriklausomi testai patvirtina, kad sistema atitinka nacionalinius standartus ir veikia pagal gamintojo reikalavimus. Svarbu išbandyti tikrus banknotus, nes rinkoje yra pigesnių dažų, kurie gerai dirba su suklastotais / padirbtais banknotais, bet ne su tikrais banknotais: tai reiškia, kad rašalą iš tikrųjų banknotų galima pašalinti plaunant. Be to, į rašalą rekomenduojama pridėti teismo ekspertizės ženklą, kad būtų galima ištirti ryšį tarp dažytų banknotų ir konkrečios nusikaltimo vietos.

Geriausia praktika rodo, kad IBNS gali būti labai veiksmingas, ypač kartu su kitomis prevencinėmis priemonėmis. 2015 m. Prancūzija priėmė naujus teisės aktus, įskaitant straipsnius dėl IBNS diegimo ir rašalo su unikalia DNR naudojimo. Prancūzijos karinė policija (žandarmerija), remdamasi rizikos

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

vertinimu, nusprendžia, kur turi būti įgyvendintos IBNS ir kitos priemonės. Kadangi nauji teisės aktai sustiprino prevencinį ir operatyvinį požiūrį, atakų skaičius sumažėjo nuo 300 2013 m. Iki 50 2018 m.

Kita plėtojama technika, kaip sutrukdyti apiplėšimui, yra **klijų** naudojimas. Klijų efektyvumas buvo įrodytas Nyderlanduose, tačiau šiuo metu jų įgyvendinimas ir eksploatavimo išlaidos yra dideli. Be to, klijai gali sukelti gaisro pavojų, jei sistema nebus suaktyvinta prieš ataką, nes klijų dalelės pasklidus ore gali sudaryti degų mišinį. Šis metodas dar nėra parengtas rinkoje, tačiau gali būti sprendimas ateityje.

4.3.2 Padidinkite riziką

Antroji fizinių bankomatų atakų prevencijos kryptis yra atgrasyti potencialius kaltininkus nuo nusikaltimų, padidinant jų nustatymo ir bausmės riziką. Be fizinio sužeidimo, naudojant sprogmenis ATM priepuoliams, pagrindinė rizika nusikaltėliui yra kalėjimo bausmė, pagauta už padarytą veiką („raudonųjų ranką“) arba atlikus tyrimą. Norint sumažinti potencialių nusikaltėlių norą, reikia padidinti aptikimo ir bausmės riziką. Visuomenei nusikaltėlių gaudymas ir nuteisimas, be abejo, taip pat yra labai efektyvus prevencijos būdas, jei bus numatytos vėlesnės bausmės, kaip mes matėme keliose šalyse.

4.3.2.1 *Dalijimasis informacija*

Bankomatų užpuolikų aptikimo ir nubaudimo pagrindas yra dalijimasis informacija tarp visų kovojant su fizinėmis bankomatų išpuoliais, įskaitant bankomatų tiekėjus, teisėsaugos institucijas (policiją, prokurorą ir kt.), Valdžios institucijas, bankomatų gamintojus ir saugumą. ir apsaugos įtaisai, profesinės asociacijos, bankomatų tiekėjai (bankai ir nepriklausomi tiekėjai), apsaugos įmonės ir signalizacijos centrai. Idealiu atveju tai būtų tiek nacionaliniu, tiek tarptautiniu lygmeniu.

Anksti aptikti artėjančią fizinę bankomatų ataką sunku. Ankstyvą aptikimą įmanoma padaryti tik tais atvejais, kai teisėsaugos partneriai ir privatūs partneriai (apsaugos bendrovės ir bankomatų tiekėjai) keičiasi beveik nepriekaištinga informacija tarptautiniu lygiu. Turi būti stebimas platus rodiklių spektras, įskaitant išankstinio perspėjimo pranešimus tarp teisėsaugos institucijų apie judančias ONG, informaciją apie („karštas“) transporto priemones, kurios buvo naudojamos bankomatų išpuoliuose, informaciją iš saugumo kompanijų ar kaimynystės stebėjimų apie aptiktą įtartiną elgesį. bankomatų

apylinkėse, bankomatų teikėjų aptikti įtartini sandoriai ir kiti stebėjimo metodai. Kitos galimos policijos priemonės ankstyvam aptikimui yra vogtų automobilių stebėjimas, sprogmenų gamintojai ir platintojai bei įmonės, turinčios leidimą naudoti sprogmenis. Pastangos, reikalingos ankstyvam aptikimui, reikalauja daug ir negarantuoja sėkmės, todėl teisėsaugos intervencijos prieš išpuolį yra retos.

Jei ankstyvo aptikimo neįmanoma, signalizacijos centrai gali greitai pateikti įspėjimą, jei įvyktų fizinė bankomatų ataka. Kad būtų galima įsikišti, reikia susitarti ir sudaryti nacionalines greito ryšio tarp aliarmo centrų ir teisėsaugos institucijų taisykles ir protokolus. Ankstyvo aptikimo arba realiu laiku gautos informacijos atveju teisėsauga visada turės įvertinti laiką ir geriausią intervencijos galimybę. Sugauti nusikaltėlius, kuriems netaikomos raudonos rankos, yra labai sunku ir tai gali sukelti pavojingų situacijų, nes kai kurios organizuotos nusikalstamos grupuotės yra labai smurtinės ir naudoja sunkiuosius ginklus.

Po sėkmingo tyrimo po fizinės bankomatų atakos teisėsaugos pareigūnai turi bendrauti su visomis suinteresuotosiomis šalimis, nes bet kuris iš jų galėjo turėti informacijos, prisidedančios prie tyrimo sėkmės. Žinoma, būtina bendrauti ir bendradarbiauti su pagrindinėmis aukomis, bankais ar kitais bankomatų teikėjais: jie turi prieigą prie duomenų, kurie yra svarbūs tyrimui. Bankomatų teikėjui teisėsaugos teikiama informacija padės pagerinti prevencijos priemones. Be to, kontaktai su profesinėmis asociacijomis ir gamintojais yra naudingi: jie dažnai siunčia saugos pavojaus pranešimus, kuriuos gali užsiprenumeruoti kiti suinteresuoti subjektai. Bankomatų gamintojai turi gerą įvairių bankomatų atakų rūšių apžvalgą ir atitinkamus prevencinių priemonių trūkumus bei stipriąsias puses. Jie labai nori suteikti paramą policijai, teikdami informaciją apie bankomatų ir naudojamų MO techninius aspektus.

Tarpvalstybinis bendradarbiavimas yra būtinas: šalys turėtų keistis informacija (apie įtariamuosius, nuteistus bankomatų užpuolikus, operatyvinius vienetus, įtartinas transporto priemones, atakų vaizdus ir tt) ne tik palaikydamos tyrimą, bet ir todėl, kad kitoje šalyje nuteistiems įtariamiesiems gali būti skiriamos bausmės už pakartotinis nusikalstamumas/recidyvas.

Galiausiai duomenų bazės sukūrimas Europos lygiu, prieinamas teisėsaugai ir turintis teismo ekspertizės duomenis (pvz., apie įvairių tipų IBNS rašmenis, atsekamuosius žymeklius ar žymenis ar bankomatų apsaugos stiklą), galėtų stipriai paremti tyrimus ir susieti įtariamuosius su konkrečia nusikaltimo vieta. Technologijų standartizavimas tarptautiniu lygmeniu dažnai nėra pakankamas:

2019 m. sausio mėn. konferencijos dalyviai minėjo, kad rašalo ir nusikaltimų etikečių standartizavimas ES lygiu galėtų labai palengvinti tyrimus.

4.3.2.2 *Vaizdo stebėjimo ir klausymo įrenginiai*

Vaizdo ir garso duomenys iš vaizdo stebėjimo sistemų ir klausymosi prietaisų gali padėti aptikti išpuolį realiuoju laiku (pvz., užkirsti kelią fizinei žalai pirmiausia į įvykio vietą atvykusiems reagavusiems asmenims) ir vėlesnius tyrimus (pvz., nustatyti kaltininkus ir jų MO). Vaizdo įrašus galima sujungti su vaizdais iš viešųjų ir kitų vaizdo stebėjimo sistemų, esančių šalia bankomatų, ir eismo radarų kadrus, kad būtų išsamesnis nusikaltėlių ir jų MO vaizdas.

Tačiau CCTV vaizdai dažnai būna prastos kokybės arba blogai saugomi. Vaizdai turi būti pakankamos kokybės, kad būtų galima atpažinti asmenį. Europos saugumo CCTV standartų nustatymas vėl palengvintų tyrimus. Be to, kadangi nusikaltėliai prieš išpuolį dažnai išjungia vaizdo stebėjimo kameras, taip pat būtų galima apsvarstyti galimybę įrengti nematomą vaizdo stebėjimo arba realiojo laiko klausymo prietaisus.

4.3.2.3 *Bausmė ir pažeidėjo reabilitacija*

Nuoseklios ir griežtos bausmės turi prevencinį poveikį. ONG areštas daro tiesioginį poveikį bankomatų išpuolių skaičiui. Tačiau bankomatų užpuolikų paleidimas iš kalėjimo taip pat dažnai sukelia naują išpuolių bangą. Tai reiškia, kad dėl trumpų sakinių nusikaltėliai vėl tampa labai aktyvūs. Valstybėse narėse skirtingos minimalios ir maksimalios bausmės nusikaltėliams, nuteistiems už kiekvieno tipo fizinius bankomatų išpuolius. Kai kurie mano, kad didesnės baudos atgrasys potencialius kaltininkus. Tačiau moksliniai tyrimai ([5]) rodo, kad sakinių griežtumo didinimas nebūtinai sustiprina atgrasomąjį poveikį. Todėl gali būti įdomu pažvelgti į pataisos (ir nusikaltėlių pagrįstas) reabilitacijos programas, siekiant sumažinti didelį recidyvą.

4.3.3 Padidinkite pastangas

([5]) David Weisburd, David P. Farrington ir Charlotte Gill, 'Conclusion: What Works in Crime Prevention Revisited', David Weisburd, David P. Farrington ir Charlotte Gill, *What works in Crime Prevention and Rehabilitation*. Kembridžas: „Springer", 2016, 311.

Trečiojoje fizinių bankomatų išpuolių prevencijos kryptyje yra veiksmų, dėl kurių nusikalstamą veiką padaro nusikaltėliui griežtesnį.

4.3.3.1 *Nusikalstamumui atsparios aplinkos užtikrinimas*

Jei rizikos vertinimas (plg. aukščiau) rodo, kad bankomatas yra didelės rizikos aplinkoje, vieta turėtų būti išmontuota ir bankomatas perkeltas į mažos ar vidutinės rizikos zoną. Tai tikrai yra tuo atveju, jei analizė rodo, kad pastatas gali sugriūti, jei bankomatas užpuolamas naudojant sprogmenis. Galėtų būti įgyvendinami teisės aktai, skirti užtikrinti tokių priemonių įgyvendinimą didelės rizikos atvejais. Be bankomatų skaičiaus mažinimo padidintos rizikos aplinkoje, reikėtų skatinti ir grynųjų pinigų mokėjimą, kad sumažėtų bankomatų poreikis.

Jei neįmanoma perduoti bankomato, reikia imtis maksimalių saugumo priemonių: pvz. priešgaisrinių stulpų, šviestuvų ir kitų gatvės baldų naudojimas siekiant apriboti patekimą į pastatą, transporto priemonių arešto sistemas, tinkamo gatvių apšvietimo įrengimą, padidintą atvirą ar slaptą stebėjimą ir apsaugos nuo vagysčių priemones, tokias kaip banknotų ardymo sistema. Kai vieta užpuola toje vietoje, kuri nebuvo nustatyta kaip didelė rizika, ji turėtų būti nustatyta kaip tokia ir pridėta papildomų saugumo priemonių. Norint atnaujinti riziką, reikėtų atsižvelgti į naujus veiksnius. Pakartotinis šios rizikos vertinimas turėtų būti pasikartojanti operacija.

4.3.3.2 *Bankomatų sustiprinimas*

Bankomatų gamintojai siūlo standartinį bankomatų asortimentą, turinčią daugybę saugos funkcijų, kurios yra įvertintos pagal Europos standartizacijos komiteto (CEN) saugos laipsnius. Paprastai bankomatai turi CEN ženklą: nuo žemesnio lygio CEN1 iki aukščiausio, CEN4. Tokios savybės kaip kūno stiprumas ir atsparumas priepuoliams lemia pažymį. Atsparumas dujoms dažniausiai siūlomas kaip papildomas pasirinkimas (CEN-GAS). Standartinius modelius galima patobulinti papildomomis apsaugos priemonėmis. Paprastai trečiosios šalys diegia šias funkcijas, kad užtikrintų vietos įstatymų laikymąsi ir pagrindinio modelio pritaikymą vietinių klientų poreikiams. Papildomos apsaugos funkcijos apima įvairius jutiklius, skirtus suaktyvinti dujų neutralizavimo sistemą arba IBNS *in situ* atveju ar atakos sprogmenimis bei patobulintais užraktais ir skliautų spynomis, siekiant užkirsti kelią neteisėtam patekimui į seifą, kuriame pažeistas pagrindinis užraktas. Nešiojamiems, autonominiams bankomatams svarbu naudoti tvirtinimo sistemas, kurios siūlo papildomą apsaugą nuo išpuolių /

išpuolių. Stebėjimo sistemos gali būti įtrauktos į bankomatą, kad palaikytų tyrėjus, kai bankomatas prieš atidarant yra gabenamas į kitą vietą.

4.3.3.3 *Architektūrinės priemonės*

Diegdami bankomatą, siūloma naudoti galinės prieigos automatus. Tokiu atveju nusikaltėlis turi patekti į pastatą ir patekti į mašinos galą, kad pavogtų grynuosius pinigus. Labiausiai pažeidžiami nešiojamieji, autonominiai bankomatai. Sumažinus šių bankomatų skaičių padidėtų saugumas. Pareiga įrengti bankomatus apsaugos nuo įsilaužimo kambaryje automatiškai sumažintų autonominių bankomatų naudojimą.

4.3.3.4 *Rūko sistema*

Rūko patranka greitai užpildo kambarį tankiu rūku, todėl įsibrovėlis nieko nemato. Dėl tokio saugumo rūko bankomatų atakos įvykdyti neįmanoma. Bent jau dėl to sistema lėtina kaltininką paliekant laiko policijos tarnyboms įsikišti. Apsaugos rūko sistema yra sujungta su signalizacijos sistema ir gali būti įjungiama dviem būdais. Jį gali automatiškai įjungti aliarmo jutikliai, tokie kaip judesio jutikliai (naktį) arba ATM langinių manipuliavimo jutikliai. Jį taip pat gali suaktyvinti signalizacijos centras, kad būtų išvengta per daug melagingų aliarmų. Per sieninius lauko bankomatus rūko sistema gali būti pritaikyta bankomato gale, kad užpildytų kambarį rūku, o kaltininkų matomumas būtų lygus nuliui.

Rūko sistemos gali užtikrinti bankomatų, esančių atvirose vietose degalinėse, prekybos centruose, apsaugą nuo taškų. Taip išvengiama rūko, kuris užpildo visą teritoriją. Apsauga nuo rūko yra sėkmingiausia, kai rūkas kyla iš skirtingų kampų arba kai jis užpildo erdvę už bankomato
siautėjimo .. Tęsiami bandymai, siekiant nustatyti, ar rūko patrankas galima įrengti pačiame bankomate, o ne kambaryje, kuriame yra bankomatas. Prie rūko gali būti pridėti DNR žymekliai, kurie dažo nusikaltėlius ir jų drabužius.

4.3.4 Lygiagrečios priemonės

Norint užtikrinti veiksmingą ir rezultatyvų minėtų prevencinių priemonių įgyvendinimą, reikia apsvarstyti keletą lygiagrečių priemonių. Šios priemonės yra būtinos norint sudaryti sąlygas ar sustiprinti holistinį prevencinį ir operatyvinį požiūrį į fizinių bankomatų išpuolius.

4.3.4.1 *Teisės aktai*

Daugelyje šalių įstatymai įpareigoja bankomatų teikėjus imtis prevencinių priemonių. Kitose šalyse susitarimų ir susitarimų tarp bankų ir teisėsaugos institucijų sudarymas užtikrina gerai valdytą požiūrį į fizinių bankomatų išpuolius. Sritys, kuriose gali būti svarstomos reguliavimo priemonės:

- prevencinių priemonių įdėjimas;
- teisinės sistemos, leidžiančios bendradarbiauti teisėsaugai ir viešiesiems bei privatiems partneriams;
- pertvarkyti bausmes, jei bausmės fizinių bankomatų išpuoliams yra per mažos.

Tačiau dažnai tik bankų įstaigos yra įpareigotos laikytis taisyklių, o nepriklausomi bankomatų teikėjai nėra saistomi šių įstatymų ar susitarimų. Tai yra bendroji silpnoji vieta reguliavimo sistemoje.

Kai kurios šalys neįgyvendina jokio reguliavimo, tačiau bando įtikinti bankomatų teikėjus imtis prevencinių priemonių, geriau informuodamos apie nusikalstamumo sritis ir tendencijas: šalyse, kuriose yra daug nepriklausomų bankų, tai pasirodyti ypač sudėtinga.

Būtina užtikrinti, kad veiksmingas prevencinių priemonių įgyvendinimas apimtų įstatymų ir kitų teisės aktų pakeitimus tiek nacionaliniu, tiek tarptautiniu lygmeniu, privalomus visų rūšių bankomatų teikėjams. Idealiu atveju teisės aktai turėtų būti suderinti ES lygiu, kad būtų išvengta griežtų prevencinių priemonių, įtvirtintų vienos šalies teisės aktuose, vietinių organizuotų darbo grupių nukreipimo į kitas šalis, kuriose ne toks griežtas reglamentavimas.

4.3.4.2 *Žiniasklaidos strategija*

Kita svarbi prevencinės strategijos ašis yra nusistovėjusi žiniasklaidos strategija, kuria siekiama sumažinti bankomatų užpuolikų lūkesčius ir norą įsitraukti į šį nusikaltimą. Reikia pabrėžti žemą sėkmės lygį ir didelę nusikaltėlių riziką; komunikacija apie atlygį („plėšikavimas“) arba išsami informacija apie bankomatų ataką, pvz., paveikto bankomatų tipas arba vengta pinigų. Kita vertus, būtina išsamiai bendrauti apie įtariamųjų areštus ir už tai nubaudžiant nuosprendį.

4.3.4.3 *Glaudesnis bendradarbiavimas*

Glaudesnis bendradarbiavimas ir keitimasis informacija buvo plačiai paminėti, tačiau to negalima pabrėžti pakankamai. Operatyvinis keitimasis informacija tarptautiniu lygmeniu yra pagrindinė Europolo veikla. Be šio keitimosi informacija, prevencijos konferencija parodė aiškų poreikį plėsti daugiadalykį ir daugiapakopį bendradarbiavimą ir dalijimąsi informacija tarp visų susijusių suinteresuotųjų šalių, įskaitant teisėsaugos institucijas, valdžios institucijas, bankomatų ir apsaugos bei apsaugos priemonių gamintojus, profesines asociacijas, bankomatų teikėjus (bankus). ir nepriklausomi teikėjai), apsaugos kompanijos ir signalizacijos centrai. Tai turi apimti vietos, nacionalinis ir tarptautinis lygmuo.

4.3.4.4 *Sumažinti papildomos žalos riziką*

Atakų su kietaisiais sprogmenimis atveju kai kurios ONG medžiagos paliks medžiagą. Tai gali sukelti pavojingų situacijų pirmosios pagalbos teikėjams ar civiliams žmonėms (gyvenantiems kaimynystėje arba pravažiuojantiems pro šalį). Turi būti užtikrintas jų saugumas. Kaip ir Belgijoje, protokolai ir procedūros, kurių turi laikytis pirmosios pagalbos teikėjai (tiek teisėsaugos, tiek bankomatų teikėjai), turi būti sukurti ir suderinti tarpusavyje. Kita geriausia praktika šiame kontekste yra Nyderlandų pavyzdys, kai situacijai įvertinti naudojami vaizdo bankomatų užfiksuoti vaizdo įrašai. Galima sudaryti sutartis su signalizacijos centrais, kad šie vaizdai būtų nedelsiant prieinami.

4.3.4.5 *Socialinė prevencija*

Dažnai organizuotos darbo grupės ieško jaunų žmonių, kurie galėtų įdarbinti. Galima būtų rengti projektus, kurie pradiniame etape suklaidintų šiuos įdarbinimo procesus. Policija ar socialiniai darbuotojai turėtų būti dėmesingi šiems procesams ir galėtų įsikišti asmeniškai kreipdamiesi į galimus kaltininkus.

5 Išvados

Per pastaruosius 2 metus padidėjo fizinių bankomatų išpuolių paveiktų Europos šalių skaičius. Šiuo atžvilgiu Europolas ir EUCPN dirbo kartu rinkdami geriausias kovos su šiuo nusikaltimu ir jo prevencijos priemones.

Sėkmingas kovos su fizinėmis bankomatų išpuoliais būdas susideda iš operatyvinių ir prevencinių priemonių, pageidautina įterptų į teisinę sistemą, derinio. Siekiant išvengti, kad vienos šalies griežtos priemonės skatintų organizuotas organizuotas organizacijas nukreipti labiau pažeidžiamas šalis, rekomenduojama šias priemones patvirtinti Europos lygiu.

Siekiant užkirsti kelią tokio tipo nusikaltimams ir su jais kovoti, turėtų būti nustatyta aiški strategija trimis etapais: įvertinant situaciją, parengiant prevencinį požiūrį, pagrįstą rizikos vertinimu, ir įgyvendinant prevencines priemones.

Fizinių bankomatų išpuolių rizikos vertinimas turėtų apimti bankomatų ir jo apylinkių ypatybes, bendradarbiavimą su partneriais ir suinteresuotosiomis šalimis siekiant sukurti aljansus kovai su šiuo nusikaltimu ir prevencinės bei teisinės sistemos vertinimą. Įvertinus situaciją, turėtų būti sukurta strategija, paremta viešojo ir privačiojo sektorių bendradarbiavimu, ir turėtų būti sukurtos prevencinės bei operatyvinės atsakomosios priemonės. Prevencinių priemonių tikslas yra sumažinti kaltininko ketinimus ir galimybes įsitraukti į fizinę bankomatų ataką. Norint tai pasiekti, siūlomos trys prevencinių veiksmų kryptys: sumažinti atlygį, padidinti riziką ir padidinti pastangas. Lygiagrečios priemonės turėtų užbaigti prevencinę strategiją. Geriausia praktika yra nacionalinės valdžios institucijos, turinčios galią nustatyti šias būtinas priemones, įsteigimas.

Sumažinus **atlygį**, sumažėja nusikaltėlio noras užsiimti tokio tipo nusikaltimais. Sumažinti grynųjų pinigų kiekį bankomate apribojant, kad papildytų grynųjų pinigų pakaktų tik vienai prekybos dienai, arba ištuštinti (pažeidžiamiausius) bankomatus naktį - viena iš priemonių, leidžiančių sumažinti nusikaltėlio lūkesčius. Kitas būdas yra sugadinti plėšikavimą ir padaryti pinigus atsekamus. Šiame kontekste gali būti taikoma IBNS, kuri dažo užrašus ir pažymi juos pavogtais. Šis metodas yra efektyviausias, kai nusikaltėliams neįmanoma išleisti šių pinigų ar iš naujo įvesti šių banknotų į legalią grynųjų pinigų sistemą. Tai gali pasiekti bankai ir visuomenė, nepriimdami dažytų banknotų mokėjimui ir įdiegę banknotų priėmėjus, kurie gali aptikti ir atsisakyti dažytų banknotų. Šiuo atžvilgiu investicijos į infraraudonųjų spindulių sistemas, kurios aptinka dažytus užrašus su infraraudonųjų spindulių žymekliais, pasirodė esąs ekonomiškas sprendimas Belgijoje ir Prancūzijoje. Diegdamos IBNS, šalys turėtų nuodugniai apsvarstyti pasirinktus aktyvinimo mechanizmus, būtiniausius reikalavimus banknotams neutralizuoti ir į rašalą įtraukti teismo ekspertizės ženklą.

Priemonės, kurios atgraso potencialius nusikaltėlius nuo nusikaltimų **padidinant nustatymo ir bausmės riziką**, yra antroji fizinių bankomatų išpuolių prevencijos kryptis. ATM užpuolikų aptikimo ir nubaudimo pagrindas yra informacijos rinkimas ir dalijimasis tarp visų suinteresuotųjų šalių tiek nacionaliniu, tiek tarptautiniu lygiu. Keitimasis informacija apie aukštos kokybės vaizdo stebėjimo vaizdo ir garso duomenis gali padidinti ankstyvo aptikimo ir sėkmingo tyrimo galimybes. Norint išvengti, kad prieš užpuolimą būtų išjungti vaizdo stebėjimo arba klausymo įrenginiai, galima apsvarstyti galimybę įrengti nematomus vaizdo stebėjimo arba realiojo laiko klausymo įrenginius. Kriminalistinės duomenų bazės sukūrimas ir technologijų standartizavimas Europos lygiu galėtų labai palengvinti tarptautinį bendradarbiavimą ir tyrimus. Jei pažeidėjai bus sugauti ir nuteisti, gali būti įdomu pažvelgti į pataisos (ir nusikaltėliu pagrįstas) reabilitacijos programas, kad būtų sumažintas didelis recidyvas.

Trečioji kryptis, kuria siekiama užkirsti kelią fiziniams bankomatų išpuoliams, apima priemones, skirtas **padidinti nusikaltėlio pastangas** atlikti nusikalstamą veiką. diegus bankomatą nusikaltimams atsparioje aplinkoje, naudojant maksimalias saugumo priemones, nusikaltėliams bus lengviau reikalauti pulti bankomatą. Be to, standartinę ATM apsaugą galima patobulinti naudojant keletą papildomų saugumo funkcijų. Be šių priemonių, sumontavus rūko sistemą, kaltininkas gali būti atgrasomas arba bent jau sustabdytas puolimas.

Kelios **lygiagrečios priemonės** sustiprins minėtas priemones, tokias kaip teisinės sistemos, įpareigojančios visus bankomatų teikėjus įgyvendinti prevencines priemones, sukūrimas, nusistovėjusios žiniasklaidos strategijos sukūrimas, glaudesnis bendradarbiavimas vietos, nacionaliniu ir tarptautiniu lygmeniu, gairės pirmosios pagalbos teikėjams siekiant sumažinti netiesioginės žalos riziką ir investicijas į socialinę prevenciją, siekiant pakenkti kriminalinio įdarbinimo procesams.

6 Prevencinio požiūrio rekomendacijos: apžvalga

Sukurkite veiksmingą atsakymą, kaip išvengti fizinių bankomatų atakų

Įvertinkite situaciją

Sukurkite bankomatų rizikos profilį savo šalyje/regione
Nurodykite partnerius ir suinteresuotuosius subjektus, kovojančius su fizinėmis bankomatų išpuoliais, ir įvertinkite bendradarbiavimą
Įvertinti kovos su fizinėmis bankomatų išpuoliais teisinę bazę nacionaliniu ir tarptautiniu lygiais.

Sukurti prevencinį požiūrį

Nustatykite (pagrindinę) draudžiamą riziką ir prioritetus
Apsvarstykite tris pagrindines kryptis, kad nustatytumėte geriausias prevencines priemones šiai rizikai padengti.
Nustatykite lygiagrečią prevencinę priemonę, reikalingą sustiprintoms prevencinėms priemonėms.

Prevencinės priemonės, kurių galima imtis		
Sumažinkite atlygį	Padidinkite riziką	Padidinkite pastangas
– Mažinkite grynųjų pinigų sumą. ○ Naktį ištuštinkite bankomatą. ○ Padidinkite pakartotinių pakartojimų skaičių/dažnį. – Sugadink plėšiką. ○ intelektualiosios banknotų neutralizavimo sistemos (IBNS). ○ Infraraudonųjų spindulių žymekliai IBNS rašalu, kad aptiktų banknotų priėmėjų dažytus užrašus. ○ Vystoma: klijai.	– Keitimasis tarpvalstybine informacija: ○ ankstyvas ar realiu laiku aptiktas galimas bankomatų išpuolis, ○ veiklos metodo stiprinimas, ○ kaltinamųjų nuteisimas, ○ keitimasis kriminalistikos duomenimis Europos lygiu. – Vaizdo stebėjimo ir klausymo įrenginiai. – Paskesnė bausmė ir pažeidėjo reabilitacija.	– Nusikaltimams atsparios aplinkos užtikrinimas. ○ Keičiama didelės rizikos bankomatų vieta. ○ Saugumo priemonės: fizinės kliūtys, sekimas ir kt. – ATM sutvirtinimas su langinėmis, atsparus dujoms ar kietiems sprogmenims ir kt. – Architektūrinės priemonės, tokios kaip galinės prieigos mašinos – Apsaugos rūko sistemos.

Lygiagrečios prevencinio požiūrio stiprinimo priemonės

- Veiksmingi teisės aktai, įskaitant prevencines priemones prieš fizinius bankomatų išpuolius, dėl to kylančias bausmes ir kt.
- Efektyvi žiniasklaidos strategija, atgrasanti nusikaltėlius.
- Glaudesnis visų suinteresuotųjų šalių (valstybinių, privačių, teisėsaugos) bendradarbiavimas kovojant su fizinėmis bankomatų išpuoliais.
- Sumažinkite pirmosios pagalbos teikėjų ar civilių asmenų (pvz., Gyvenančių kaimynystėje ar pro šalį einančių asmenų) įkaito riziką.
- Socialinė prevencija, vengianti jaunuolių būti verbuojamiems dėl (tokio tipo) nusikaltimų.