Fyysisten pankkiautomaatti-hyökkäysten estäminen

TEHOKKAAN LÄHESTYMISTAVAN KEHITTÄMINEN

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.

”

KIITOKSET

Tämä asiakirja on Euroopan unionin lainvalvontayhteistyön (Europol) ja eurooppalaisen rikoksentorjuntaverkoston (EUCPN) sihteeristön yhteistyön tulosta. Haluamme kiittää fyysisten pankkiautomaattien luona tapahtuvien hyökkäysten asiantuntijoita, jotka panostivat aikaa ja vaivaa tukemaan tämän suositusasiakirjan luomista. He avustivat osallistumalla fyysisten pankkiautomaattihyökkäysten ehkäisyä käsittelevään konferenssiin (tammikuu 2019, Bryssel) ja tarjoamalla tärkeätä tietoa. Erityisesti haluamme kiittää EU:n ja EU:n ulkopuolisten (”kolmansien”) maiden lainvalvontaviranomaisia, yksityistä sektoria mukaan lukien ATM Industry Association (ATMIA), BPost, Centrum voor Criminaliteitspreventie en Veiligheid (CCV), Diebold Nixdorf, the European Association for Secure Transactions Expert Group on ATM and [automatic teller safes] ATS Physical Attacks (EAST EGAP), European Intelligent Cash Protection Association (Euricpa), ING, Febelfin, NCR, Protect, SIOC Banking, Spinnaker, TMD Security sekä Belgian, Kroatian, Saksan ja Espanjan sisäministeriöt.

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

SISÄLLYSLUETTELO

TAUSTA

Fyysisten pankkiautomaattihyökkäysten ja niistä kärsineiden Euroopan maiden määrän kasvaessa Euroopan rikoksentorjuntaverkosto (EUCPN) ja Europol järjestivät konferenssin (tammikuussa 2019), joka toi lainvalvontaviranomaiset yhteen julkisten ja yksityisten kumppaneiden kanssa pohtimaan tämän rikoksen ehkäisemistä. Tässä suositusasiakirjassa esitetään tiivistelmä konferenssin päätelmistä lisätä viranomaisten tietoisuutta fyysisistä pankkiautomaattihyökkäyksistä ja ennaltaehkäisevistä toimenpiteistä.

Rajoitettu, mutta yhä kasvava määrä Euroopan unionin maita on huolissaan fyysisistä pankkiautomaattihyökkäyksistä. Vuonna 2017 aiheutuneen taloudellisen vahingon arvioitiin olevan Euroopassa yli 30 miljoonaa euroa. Jotkut maat kokevat edelleen huomattavia määriä fyysisiä hyökkäyksiä pankkiautomaatteihin, ja jotkut maat ovat kokeneet näiden tapahtumien määrän lisääntyneen huomattavasti viimeisen kahden vuoden aikana. Tämä rikollisuusalue kehittyy nopeasti. Jotkut maat ovat menestyneet lähestymistavassaan pankkiautomaatteihin kohdistuvien fyysisten hyökkäysten hallintaan ja hyökkäysten määrä on vähentynyt äskettäin merkittävästi. Toisaalta maat, joihin hyökkäykset eivät ole aiemmin vaikuttaneet, joutuivat äkilliseen pankkiautomaattien fyysisten hyökkäysten kohteeksi vuonna 2018, koska järjestäytyneet rikollisryhmät laajensivat alueitaan. Tämä ei koske vain pankkeja, ja hyökkäyksiä tapahtuu yhä useammin riippumattomien palveluntarjoajien pankkiautomaateista, koska ne sijaitsevat usein haavoittuvammissa tiloissa tai paikoissa.

Laaja joukko erilaisia menetelmiä (menettelytavat), joilla rikolliset hyökkäävät pankkiautomaatteihin, voidaan jakaa kahteen pääluokkaan: fyysiset pankkiautomaattihyökkäykset ja pankkiautomaatteihin liittyvät petoshyökkäykset (tämä sisältää pankkiautomaattien loogiset ja haittaohjelmahyökkäykset). Tämä artikkeli keskittyy pankkiautomaatteihin kohdistuviin fyysisiin hyökkäyksiin: fyysinen murtautuminen pankkiautomaatteihin käteisvarojen poistamiseksi. Murto voidaan suorittaa:

> **räjähteillä:** hyökkääjät käyttävät kaasua tai kiinteitä räjähteitä rikkoakseen fyysisesti pankkiautomaatin turvallisuuden ja saadakseen käteisvaroja;

> **ulosveto- / törmäyshyökkäykset:** hyökkääjät poistavat fyysisesti pankkiautomaatin asennusympäristöstä, usein käyttämällä huippuluokan ajoneuvoa;

> **paikan päällä tapahtuvat hyökkäykset:** hyökkääjät leikkaavat kassakaapin läpi raa'alla voimalla, usein käyttämällä leikkaus- tai murtotyökaluja, kuten kulmahiomakoneita, lekoja tai happiasetyleenihitsauspillejä.

01 PANKKIAUTOMAATTIEN FYYSISEN HYÖKKÄYKSEN ONNISTUMISTA MÄÄRITTELEVÄT TEKIJÄT

Pankkiautomaattihyökkäysten onnistumisaste on alhainen; vain kolmasosa hyökkäyksistä onnistuu. Vaikka hyökkäys epäonnistuu, rakennukselle aiheutuvat vahingot (esim. räjähteillä) ovat kuitenkin yhtä tärkeitä, jolloin jää vaarallinen ympäristö rikospaikan läheisyyteen paikallisille asukkaille, ensihoitajille ja ohikulkijoille.

Fyysisen hyökkäyksen onnistuminen riippuu monista tekijöistä, mukaan lukien pankkiautomaatin ominaisuudet, pankkiautomaatin hyökkäyksen valmistelu ja tekijöiden kokemus ja tietämys.

1. Pankkiautomaattien haavoittuvuus

Haavoittuvimpia pankkiautomaatteja ovat ne, jotka sijaitsevat ulkopuolella (rakennuksen seinän takana, tai ne, jotka ovat erillään rakennusten sisällä. Kun järjestäytyneet rikollisryhmät hyökkäävät sisäisiin (erillisiin) pankkiautomaatteihin, ne valitsevat mieluummin kaupallisissa tiloissa sijaitsevat pankkiautomaatit kuin pankkitiloissa sijaitsevat pankkiautomaatit, joissa valvonta on yleensä vahvempaa. Pankit käyttävät pääasiassa pankkiautomaatteja, jotka sijaitsevat pankkirakennuksen sisällä tai ulkopuolella. Pankkien etäsijainneista kaduilla tai kauppiaiden kaupallisissa tiloissa, kuten huoltoasemat, supermarketit, hotellit, kasinot, lentokentät jne., tulee

vähitellen tärkeämpiä pankkikonttoreiden sulkemisen myötä. Riippumattomat palveluntarjoajat käyttävät pankkiautomaatteja itsenäisenä palveluna. Niiden pankkiautomaatit sijaitsevat usein kaupallisissa kohteissa, hotelleissa, vapaa-ajan kohteissa, rautatieasemilla, lentokentillä jne., julkisissa rakennuksissa ja kadulla.

Verkkopankkien suosion kasvaessa monet pankkikonttorit suljetaan todennäköisesti tulevina vuosina, mikä johtaa pankkiautomaattien kokonaismäärän laskuun[1]. Tämä saattaa kuitenkin aiheuttaa useampien pankkien etäautomaattien ja riippumattomien palveluntarjoajien pankkiautomaattien siirtymisen haavoittuvampiin paikkoihin.

2. Pankkiautomaattihyökkäyksen valmistelu

Hyökkäyksen valmistelu voi viedä useita viikkoja tai jopa kuukausia. Rikollisten on kerättävä tarvittavat **työkalut ja resurssit**, kuten ajoneuvot, välineet ja yhteyshenkilöt. **Ajoneuvot** ovat välttämätön työkalu pankkiautomaattien fyysisissä hyökkäyksissä; rikoksentekijät matkustavat pääasiassa autolla ja hyökkäyksen jälkeen he pakenevat useimmiten nopeilla ajoneuvoilla. Ajoneuvot varastetaan usein, mutta niitä saatetaan myös vuokrata tai ostaa (esim. internetin kautta). Suurin osa pankkiautomaattien fyysisten hyökkäysten **välineistä** on helposti ja laillisesti saatavissa normaaleissa kaupoissa. Tämä alentaa entisestään kynnystä siirtyä tälle rikosalueelle. Työkalun alkuperän jäljittäminen on vaikeaa lainvalvonnalle, joten rikoksentekijöiden riskit ovat vähäiset. Kansainvälisellä tasolla pankkiautomaattien fyysisiä hyökkäyksiä suorittavilla järjestäytyneillä rikollisryhmillä on melkein aina yhteyksiä kohdemaassa (ihmisiä, jotka oleskelevat siellä tietyn ajanjakson ajan) tai vaihtoehtoisesti, he voivat käyttää liikennepakotekniikkaa. Nämä yhteyshenkilöt tukevat järjestäytyneitä rikollisryhmiä logistiikan kanssa, kuten asunnon vuokraus, ajoneuvon tai muiden välineiden hankinta ja partiointikohteet. Jotkut kansainväliset rikolliset jättävät logistiikan ja tiedustelun täysin paikallisten yhteyshenkilöiden varaan ja matkustavat vain maanteitse tai lentoteitse pankkiautomaattihyökkäyksen toteuttamiseksi.

Järjestäytyneet rikollisryhmät suorittavat usein kattavan **tiedustelun** tunnistaakseen sopivia kohteita ja arvioidakseen pankkiautomaatin täyttöajan, ympäristön, teknisiä yksityiskohtia, poistumisreittejä ja olemassa olevia turvatoimia, kuten valvontakamera, hälytysanturit ja ikkunaluukut.

Jotkut järjestäytyneet rikollisryhmät ryhtyvät toimiin **lainvalvonnan ja turvallisuuspalveluiden estämiseksi** ennen hyökkäystä. He peukaloivat hälytysjärjestelmiä ja julkista valaistusta, käyttävät vääristystekniikoita, perustavat tiesulkuja tai yrittävät peukaloida lainvalvontaviranomaisten ajoneuvoja.

3. Rikoksentekijöiden kokemus ja tietämys

Fyysiset pankkiautomaattihyökkäykset ovat houkuttelevia rikollisille, koska rahat ovat heti käytettävissä eikä varastetun tavaran myyntiin tarvita laajaa verkostoa. Se on kätevä vaihtoehto rikollisille, jotka ovat jo aktiivisia järjestäytyneessä omaisuusrikollisuudessa.

Järjestäytyneiden rikollisryhmien on kerättävä **tarvittava asiantuntemus ja tietotaito**, koska nämä ovat määräävä tekijä hyökkäyksen onnistumisessa tai epäonnistumisessa. Tarvittava asiantuntemus ja tarvittava osaaminen riippuvat paljon **hyökkäyksen tyypistä**. Ulosveto-/törmäyshyökkäyksillä ja *paikan päällä tapahtuvilla* hyökkäyksillä on yksinkertainen menettelytapa (lähinnä uhkarohkeus ja raa'an voiman käyttö), joten ne eivät yleensä vaadi erityisiä taitoja. Hyökkäykset, joissa käytettään palavia kaasuja ja räjähteitä, vaativat edistyneempää asiantuntemusta.

Hyökkääjien **pätevyystaso vaihtelee**. Toisaalta erittäin organisoidut ja kokenut ryhmät voivat suorittaa onnistuneen pankkiautomaatin fyysisen hyökkäyksen muutamassa minuutissa. He hallitsevat prosessia ja kykenevät rajoittamaan itselleen kohdistuvan riskin rajoittaen samalla myös sivuvahinkoja. Toisaalta vähemmän järjestäytyneet ja opportunistiset ryhmät epäonnistuvat usein yrityksissään ja voivat aiheuttaa merkittäviä vahinkoja viereisille tiloille ja rakennuksille. Joidenkin vähemmän järjestäytyneiden rikollisryhmien uskotaan palaavan perinteiseen järjestäytyneeseen omaisuusrikollisuuteen johtuen ennaltaehkäisevistä toimenpiteistä, joita he eivät pysty päihittämään pankkiautomaattihyökkäyksissä.

02 ENNALTAEHKÄISEVÄN LÄHESTYMISTAVAN TARVE

Maat, joissa rikoksentekijöiden menestysprosentti on alhainen pankkiautomaattien fyysisten hyökkäysten kohdalla tai joissa pankkiautomaattien fyysisten hyökkäysten määrä vähenee, osoittavat, että menestyvä toimintatapa pankkiautomaattien fyysisten hyökkäysten torjumiseksi koostuu operatiivisten ja ennalta ehkäisevien toimenpiteiden yhdistelmästä. Koska tällä rikollisuuden alueella toimivien järjestäytyneiden rikollisryhmien määrä on rajoitettu, järjestöjen jäsenten pidätykset ja niistä johtuvat rangaistukset vähentävät huomattavasti hyökkäysten määrää. Vapauduttuaan pankkiautomaattihyökkääjät aloittavat kuitenkin toimintansa uudelleen. Lisäksi ryhmä voi joskus korvata pidätetyn rikoksentekijän nopeasti. Siksi ennaltaehkäiseviä toimenpiteitä, jotka mieluiten sisällytetään lainsäädäntökehykseen, tarvitaan erittäin paljon. Lisäksi kokemus osoittaa, että yhden maan ennaltaehkäisytoimenpiteet voivat johtaa järjestäytyneitä rikollisryhmiä kohti haavoittuvampia kohteita muissa maissa. On vain ajan kysymys, ennen kuin yhdessä maassa ilmenevät menettelytavat leviävät muihin maihin. Tämä osoittaa selvästi, että **ennaltaehkäiseviä ja operatiivisia toimenpiteitä on toteutettava Euroopan tasolla** yksityisten, julkisten ja lainvalvontaviranomaisten kanssa tiiviissä yhteistyössä

03 ENNALTAEHKÄISY

Tämän tyyppisen rikollisuuden estämiseksi ja torjumiseksi tarvitaan selkeä strategia. Tässä luvussa annamme yleiskuvan kolmesta vaiheesta, jotka yleensä suoritetaan kohdattaessa pankkiautomaattien fyysisiä hyökkäyksiä tai valmistautuessa estämään niitä.

Ensinnäkin **tilanteen arviointi**; pankkiautomaattien ja niiden ympäristön riskiprofiili olisi määritettävä ottaen huomioon käytettävissä olevan käteismäärän (mahdollinen ryöstösaalis), vakuusvahinkojen ja henkilövahinkojen riski. Toiseksi riskinarvioinnin perusteella olisi kehitettävä **ennaltaehkäisevä strategia**. Lopuksi **ennalta ehkäisevät toimenpiteet** olisi pantava täytäntöön.

1. Tilanteen arvioiminen

Järjestäytyneet rikollisryhmät kohdentavat yleensä joko erityyppisiä pankkiautomaatteja tai tiettyjen palveluntarjoajien pankkiautomaatteja, joiden ominaisuudet helpottavat pankkiautomaatin hyökkäystä. Siksi on välttämätöntä suorittaa perusteellinen arvio pankkiautomaattien fyysisten hyökkäysten riskistä, mukaan lukien mieluiten koko käteisvarmuusketju kuljetuksesta pankkiautomaattiin toimitukseen. Kunkin pankkiautomaatin riskiprofiilin määrittämiseksi on analysoitava joukko elementtejä, mukaan lukien seuraavat.

- Paikan sijainti ja pankkiautomaatin ympäristö; ominaisuudet, kuten kaupunki- tai maaseutuympäristö, väestötiheys, poliisiasemien läheisyys, ympäristössä oleva automaattinen rekisterikilpien tunnistus, läheisyydessä olevat valvontakamerat jne.
- Pankkiautomaatin sijainti:
  - rakennuksen sisällä tai ulkopuolella, pankkikonttorissa tai syrjäisissä (esim. kaupallisissa) tiloissa, sisäänrakennettu tai kiinnitetty rakennukseen,
  - itsenäinen pankkiautomaatti: riippumatta siitä, onko se ankkuroitu tai ei,
  - sisäänrakennettujen tai rakennukseen kiinnitettyjen pankkiautomaatien osalta: onko arkkitehtonisia heikkouksia, miten käteisvarojen varastointi järjestetään jne.
- Pankkiautomaatin tyyppi.
- Pankkiautomaattiin sisältyvät turvatoiminnot.
- Käteismäärä pankkiautomaatissa.
- Pankkiautomaattien fyysisten hyökkäysten tyyppi ja menettelytapa, joita voidaan odottaa soveltuvimpien ehkäisevien toimenpiteiden toteuttamiseksi ensin.
- Jo toteutetut turvatoimet ja ennaltaehkäisevät toimenpiteet (älykkäät setelinsuojausjärjestelmät (IBNS), valvontakamerat, turvasumu (näkyvyyden vähentäminen) jne.).

Lisäksi arvioitavia tekijöitä ovat yhteistyön tila kumppaneiden ja sidosryhmien kanssa sekä lainsäädäntö. Lainvalvonnan, yksityisten ja julkisten kumppaneiden välistä yhteistyötä tulisi arvioida liittoutumien luomiseksi rikollisuuden torjumiseksi. On mahdollista, että jokaisella kumppanilla on mielenkiintoista tietoa tilanteen arvioimiseksi. Paikallinen poliisi tai paikallisviranomaiset ovat erityisen tärkeitä tässä yhteydessä. Lainsäädäntöä on arvioitava oikeudellisen kehyksen luomisessa ennaltaehkäisylle, pakollisten ennaltaehkäisevien toimenpiteiden toteuttamiselle, pankkiautomaattihyökkäysten rangaistuksiin jne.

2. Ennaltaehkäisevän lähestymistavan luominen

Kun tilanne on arvioitu ja pankkiautomaatin turvallisuuden tärkeimmät riskialueet ja vahvuudet ja heikkoudet on määritetty, voidaan kehittää strategia (perustuu usein julkisen ja yksityisen sektorin yhteistyöhön) ja toteuttaa ehkäiseviä ja operatiivisia vastatoimenpiteitä. Ennaltaehkäisytoimenpiteet pitäisi suunnata vähentämään tekijöiden aikomusta ja mahdollisuuksia. Tämän saavuttamiseksi ehdotetaan kolmea ennaltaehkäisevän toimintalinjaa, jotka perustuvat kolmeen Clarken viidestä tilannerikollisuuden ehkäisystrategiasta[2]; palkintojen vähentäminen, rikoksentekijöiden riskin lisääminen ja saaliiseen käsiksi pääsemiseen tarvittavien ponnistelujen lisääminen.

Rikolliset punnitsevat odotettavissa olevan palkkion ja siihen liittyvien riskien suhdetta (esim. pankkiautomaattihyökkäys). Helpon saaliin saamisen mahdollisuuksien vähentäminen ja rikoksentekijöiden riskien lisääminen heikentävät heidän odotuksiaan ja haluaan osallistua pankkiautomaattien fyysisiin hyökkäyksiin. Lisätoimenpiteet, jotka lisäävät pankkiautomaattiin pääsyyn tarvittavia ponnisteluja, vaikuttavat tekijöiden kykyihin. Opportunistiset rikoksentekijät, jotka epäonnistuvat usein yrityksissään, lopettavat osallistumisen pankkiautomaattihyökkäyksiin. Ammattimaisille pankkiautomaattihyökkääjille onnistumisaste heikkenee, mikä taas vaikuttaa tuoton ja riskin väliseen tasapainoon.

Lisäksi ennaltaehkäisevää strategiaa täydentävät rinnakkaistoimet, kuten tehokas mediastrategia, varhainen sosiaalinen ennaltaehkäisy ja toimenpiteet rakennusten lisävahinkojen vähentämiseksi ja paikallisten asukkaiden, ensihoitajien ja ohikulkijoiden turvallisuuden varmistamiseksi.

On olemassa muita tapoja jäsentää lähestymistapaa. Alankomaissa viranomaiset soveltavat ns. estemallia[3]. Tämä malli yksilöi vaiheet, jotka rikollisen on suoritettava rikoksen tekemiseksi. Se tunnistaa myös kumppanit ja mahdollisuudet, jotka mahdollistavat rikoksen, ja se on hyödyllinen väline rikosalueen tiedonkeruuprosessin järjestämiseksi. Kun kukin pankkiautomaattien fyysisten hyökkäysten toteuttamiseen tarvittava askel tunnistetaan,

tällöin voidaan myös tunnistaa rikoksen estämisen esteet ja parhaat kumppanit esteiden asettamiseksi. Estemalli tunnistaa myös signaalit, jotka varoittavat julkisia ja yksityisiä kumppaneita pankkiautomaattien fyysisistä hyökkäyksistä, ja signaalit, joita he voivat itse lähettää ilmoittamaan viranomaisille epäilyistään.

Ennaltaehkäisyn tehostamiseen liittyvien riskien lieventämiseksi tarvitaan hyvin kehitetty strategia. Ennaltaehkäisevillä toimenpiteillä, jotka ovat erittäin tehokkaita lannistamaan amatöörejä ja jäljitteleviä rikollisia, on joskus ei-toivottuja vaikutuksia. Jotkut ryhmät etsivät haavoittuvia pankkiautomaatteja yrityksen ja erehdyksen kautta jättäen peräänsä vaurioituneita pankkiautomaatteja. Vaarallisemmat ja armottomat järjestäytyneet rikollisryhmät alkavat käyttää väkivaltaisempia menettelytapoja, kuten siirtymistä kaasusta räjähteisiin hyökkäyksissään.

Jotta voitaisiin laatia tehokkaat ennaltaehkäisevät toimenpiteet, paras käytäntö on perustaa kansallinen viranomainen, jolla on valtuudet määrätä erityistoimenpiteitä korkean riskin omaaville pankkiautomaateille perusteellisella tilanneanalyysillä. Tämä lähestymistapa on osoittautunut tehokkaaksi Ranskassa, varsinkin jos luodaan oikeudellinen kehys ja toimenpiteet pannaan täytäntöön yhdessä operatiivisten toimenpiteiden kanssa.

3. Ennaltaehkäisevien toimenpiteiden suorittaminen

Tässä luvussa esitetyt toimenpiteet pankkiautomaattien fyysisten hyökkäysten estämiseksi ovat osoittautuneet hyödyllisiksi eri maissa. Ne perustuvat ennaltaehkäisykonferenssin päätelmiin ja ennalta ehkäiseviin toimiin, joita pankkiautomaattiturvallisuuden alalla toimivat kansainväliset organisaatiot edistävät aktiivisesti. Monet toimenpiteet tunnetaan hyvin. Useat maat ovat jo toteuttaneet joukon toimenpiteitä menestyksekkäästi. Ehdotetut toimenpiteet pannaan kuitenkin usein täytäntöön vain osittain, eikä niitä ole sisällytetty lainsäädäntöön.

Kuten edellä mainittiin, ehdotetaan ennaltaehkäisevien toimien kolmea akselia: palkkioiden vähentäminen, rikoksentekijöiden riskin lisääminen ja ryöstösaaliiseen käsiksi pääsemiseksi tarvittavien ponnistelujen lisääminen.

3.1 Palkintojen vähentäminen

Rikoksista saatavien palkkioiden vähentäminen on ensimmäinen akseli pankkiautomaattien fyysisten hyökkäysten estämisessä. Niin kauan kuin käsitys ”helposta rahasta” jatkuu, rikolliset osallistuvat tällaiseen rikokseen. Käytettävissä olevan käteismäärän vähentäminen ja käteisen poistaminen tai tuhoaminen vähentävät kiinnostavan ryöstösaaliin houkutusta. Vähentyneet odotukset vähentävät rikollisen halua osallistua tällaiseen rikokseen.

Käteisen määrän vähentäminen

Yksi toimenpide palkkion vähentämiseksi on pankkiautomaatissa olevan käteismäärään vähentäminen. Ihannetapauksessa tämä määrä tulisi rajoittaa vain yhden päivän setelitarpeeseen. Pankkien välinen yhteistyö voisi varmistaa kustannustehokkuuden. Alankomaissa useat pankit tekivät yhteistyötä perustaakseen pankeista riippumattoman pankkiautomaattiverkon, nimeltään Geldmaat. Yhteistyön tavoitteena on varmistaa käteisvarojen saatavuus, tavoitettavuus, kohtuuhintaisuus ja turvallisuus. Tämä johtaa todennäköisesti pankkiautomaattien määrän vähenemiseen. Pankkiautomaatit eivät kuitenkaan sisällä enempää käteisvaroja, vaan ne täytetään useammin. Uudelleentäyttöjen määrä mukautetaan tarpeeseen.

Koska rikoksentekijät hyökkäävät useimmiten pankkiautomaatteihin kello 03.00–04.00 välisenä aikana, on suositeltavaa tyhjentää erilliset pankkiautomaatit (jotka sijaitsevat pääosin kaupallisissa ja julkisissa tiloissa, jotka ovat haavoittuvammassa asemassa) ja siirtää käteinen tallelokeroon päivän lopuksi. Varoitusmerkillä voidaan ilmoittaa, että pankkiautomaatissa ei ole käteisvaroja yöllä. Seuraavana päivänä pankkiautomaatti olisi täydennettävä asiakkaiden ulottumattomissa ja lukitussa tilassa. Järjestelmä on otettu käyttöön Ranskassa, jossa lainsäädäntö velvoittaa vähittäiskauppiaat, joilla on erillinen pankkiautomaatti kaupassa, poistamaan käteisen yöllä ja jättämään pankkiautomaatin auki. Muiden pankkiautomaattien hallussa olevia määriä voidaan pienentää lisäämällä täyttötiheyttä.

Saaliin tärveleminen ja rahojen tekeminen jäljitettäväksi

Älykkäät setelinsuojausjärjestelmät (IBNS) ovat ensimmäinen tekniikka palkkion tärvelemiseksi. Nämä järjestelmät värjäävät setelit musteella niiden

merkitsemiseksi varastetuksi. Jäljitysaineita ja merkkejä voidaan lisätä IBNS-musteeseen. Tällä hetkellä näitä merkintöjä käytetään pääasiassa rikosteknisiin tarkoituksiin, seteleiden yhdistämiseksi rikospaikalle ja rikoksentekijöiden kiinniottoriskin lisäämiseksi. Vaikka IBNS on tehokas ennaltaehkäisevä toimenpide, tiettyjä asioita on huomioitava.

Euroopan keskuspankki ei korvaa värjättyjä seteleitä[4] (vuodesta 2003), mutta useat EU:n jäsenvaltioiden kansalliset keskuspankit korvaavat vielä niitä. Värjättyjä seteleitä palautetaan myös liikkeeseen kasinoiden kautta. IBNS luo lisäesteen rikollisille, mutta olisi paljon tehokkaampaa, jos rikollisten on mahdotonta käyttää värjättyjä seteleitä EU:ssa. Tämän saavuttamiseksi kansallisten keskuspankkien ei pitäisi hyväksyä värjättyjä seteleitä. Poikkeuksia voidaan tehdä tietyissä tilanteissa, kuten väärän aktivoinnin aikana tahratut setelit. On myös tärkeää neuvoa ihmisiä olemaan hyväksymättä tahrattuja seteleitä. Pidemmällä tähtäimellä setelien hyväksymislaitteiden tulisi havaita tahratut setelit, ja näitä laitteita tulisi asentaa pankkeihin ja kaupallisiin tiloihin, kuten kasinoihin, autopesuloihin jne. Musteen havaitseminen on vaikeaa ja kallista, mutta kustannustehokas ratkaisu voisi kuitenkin olla infrapunajärjestelmien asentaminen, jotka havaitsevat infrapunamerkeillä värjätyt setelit. Nämä järjestelmät ovat osoittautuneet toimiviksi ja ovat parhaita käytäntöjä Belgiassa ja Ranskassa. Kun pankkiautomaattiin lisätään infrapunamerkittyjä seteleitä, pankkiautomaatti hyväksyy ("nielee") rahat, mutta ei hyvitä niitä tilille. Värjätyt setelit lisännyt henkilö olisi myös rekisteröitävä.

IBNS-ratkaisujen asentamisessa on joitain muita näkökohtia. Useat valmistajat tarjoavat useita erilaisia IBNS-ratkaisuja, joilla on erilaisia aktivointimekanismeja ja erityyppisiä musteita. Ensimmäinen huomio koskee sitä, että kaikki tyypit IBNS-aktivointitekniikkatyypit eivät pysty torjumaan kaikkia uhkia. Jotkut IBNS:t toimivat erittäin hyvin ulosveto- ja törmäyshyökkäyksissä, *paikan päällä* tapahtuvissa hyökkäyksissä ja kaasuhyökkäyksissä, mutta eivät toimi, jos räjähdyshyökkäyksissä tai päinvastoin. Siksi tekniikkaa tulisi harkita huolellisesti ennen sen valintaa.

Toinen näkökohta on valittava mustetyyppi. Belgiassa on asetettu IBNS-järjestelmän kansalliset vähimmäisvaatimukset (turvallisuus, värjätty prosenttiosuus, ei pestävä jne.) ja riippumattomat testit todistavat, että järjestelmä täyttää kansalliset standardit ja että se toimii valmistajan vaatimusten mukaisesti. On tärkeää testata oikeita seteleitä, koska markkinoilla on halvempia musteita, jotka toimivat hyvin väärennettyjen / väärien seteleiden kanssa, mutta eivät oikeiden setelien kanssa: tarkoittaen, että muste voidaan poistaa aidoista seteleistä pesemällä. Tämän lisäksi suositellaan, että musteeseen lisätään oikeudellinen merkki, jotta voidaan tutkia yhteys värjättyjen setelien ja tietyn rikoksen välillä.

Parhaat käytännöt osoittavat, että IBNS voi olla erittäin tehokas etenkin yhdessä muiden ehkäisevien toimenpiteiden kanssa. Vuonna 2015 Ranska esitteli uuden lainsäädännön, joka sisältää artikkeleita setelinsuojausjärjestelmien (IBNS) asentamisesta ja ainutlaatuisen musteen käytöstä. Ranskan sotilaspoliisi (santarmisto) päättää riskinarvioinnin perusteella, missä IBNS ja muut toimenpiteet on toteutettava. Koska uusi lainsäädäntö vahvisti ennaltaehkäisevää ja operatiivista lähestymistapaa, hyökkäysten määrä laski 300:sta vuonna 2013 50:een vuonna 2018.

Toinen kehitteillä oleva tekniikka ryöstösaaliin pilaamiseksi on **liiman** käyttö. Liiman tehokkuus todistettiin Alankomaissa, mutta toteutuskustannukset ja juoksevat kustannukset ovat tällä hetkellä korkeat. Liima voi lisäksi aiheuttaa palovaaran, jos järjestelmää ei aktivoida ennen hyökkäystä, koska liimahiukkasten leviäminen ilmaan voisi tuottaa palavan seoksen. Menetelmä ei ole vielä valmis markkinoille, mutta se voisi olla ratkaisu tulevaisuudessa.

3.2 Riskin lisääminen

Toinen akseli pankkiautomaattien fyysisten hyökkäysten estämiselle on ehkäistä potentiaalisia rikoksentekijöitä tekemästä rikoksia lisäämällä havaitsemisen ja rankaisemisen riskiä. Fyysisten loukkaantumisriskien lisäksi, kun räjähteitä käytetään pankkiautomaattihyökkäyksiin, rikoksen tekijän suurin riski on vankeusrangaistus, kun hänet vangitaan joko itse teossa tai tutkinnan jälkeen. Mahdollisten rikoksentekijöiden halun vähentämiseksi tunnistamisriskiä ja rangaistuksia on lisättävä. Yhteiskunnan kannalta rikollisten kiinniottaminen ja tuomitseminen on tietysti myös erittäin tehokas ennaltaehkäisymenetelmä, jos rangaistus langetetaan myöhemmin, kuten olemme nähneet useissa maissa.

Tietojen jakaminen

Pankkiautomaattihyökkääjien havaitsemisen ja rankaisemisen avain on tietojen jakaminen kaikkien pankkiautomaattien fyysisten hyökkäysten torjunnassa toimivien sidosryhmien välillä, mukaan lukien pankkiautomaatin tarjoajat, lainvalvontaviranomaiset

(poliisi, syyttäjä jne.), viranomaiset, sekä pankkiautomaattien valmistajat että turvallisuus- ja suojalaitteiden valmistajat, ammattiyhdistykset, pankkiautomaattien tarjoajat (pankit ja riippumattomat palveluntarjoajat), turvayritykset ja hälytyskeskukset. Ihannetapauksessa tämä tapahtuisi sekä kansallisella että kansainvälisellä tasolla.

Pankkiautomaattien fyysisten hyökkäysten varhainen havaitseminen on vaikeaa. Varhainen havaitseminen on mahdollista vain tapauksissa, joissa lainvalvontaviranomaisten ja yksityisten kumppaneiden (turvayhtiöt ja pankkiautomaattipalvelujen tarjoajat) välinen kansainvälinen tietojenvaihto on sujuvaa. Monia erilaisia indikaattoreita on seurattava, mukaan lukien varhaisvaroitusviestit lainvalvontaviranomaisten välillä liikkuvista OCG-yhdisteistä, tiedot pankkiautomaattihyökkäyksissä käytetyistä (”kuumista”) ajoneuvoista, tiedot turvayhtiöiltä tai naapurivalvonnalta havaituista epäilyttävistä käytöksistä pankkiautomaatin ympäröivällä alueella, pankkiautomaatin tarjoajien havaitsemia epäilyttäviä tapahtumia ja muita tunnistusmenetelmiä. Muita mahdollisia poliisin toimenpiteitä varhaiseksi havaitsemiseksi ovat varastettujen autojen, räjähdevalmistajien ja jakelijoiden sekä räjähteiden käyttöluvan saaneiden yritysten seuranta. Varhaisen havaitsemisen edellyttämät ponnistelut ovat vaativat, eikä niillä ole mitään takeita menestyksestä, joten lainvalvontatoimet ennen hyökkäystä ovat harvinaisia.

Jos varhainen havaitseminen ei ole mahdollista, hälytyskeskukset voivat antaa varoituksen nopeasti pankkiautomaatin fyysisen hyökkäyksen sattuessa. Intervention mahdollistamiseksi on sovittava ja perustettava kansalliset säännökset ja protokollat nopeaa viestintää varten hälytyskeskusten ja lainvalvonnan välillä. Jos havaitaan varhainen tieto tai tosiaikaista tietoa, lainvalvonnan on aina arvioitava ajoitus ja paras mahdollisuus puuttua asiaan. Rikollisten kiinniottaminen itse teossa on erittäin vaikeaa ja voi johtaa vaarallisiin tilanteisiin, koska jotkut järjestäytyneet rikollisryhmät ovat erittäin väkivaltaisia ja käyttävät raskaita aseita.

Pankkiautomaatin fyysisten hyökkäyksen jälkeisen onnistuneen tutkinnan suorittamiseksi lainvalvontaviranomaisten on kommunikoitava kaikkien sidosryhmien kanssa, koska jollakin niistä voi olla tietoja, jotka auttavat tutkinnan onnistumisessa. Tietysti on tarpeen kommunikoida ja tehdä yhteistyötä ensisijaisten uhrin, pankkien tai muiden pankkiautomaatin tarjoajien kanssa: heillä on pääsy tutkinnan kannalta tärkeisiin tietoihin. Lainvalvonnasta saatavat tiedot auttavat pankkiautomaatin tarjoajia parantamaan ennaltaehkäisytoimenpiteitä. Lisäksi yhteydet ammattijärjestöihin ja valmistajiin osoittautuvat hyödyllisiksi: ne lähettävät usein turvahälytysviestejä, joita muut kiinnostuneet voivat tilata. Pankkiautomaattien valmistajilla on hyvä yleiskatsaus pankkiautomaattihyökkäysten eri tyypeistä ja vastaavista ennalta ehkäisevien toimenpiteiden heikkouksista ja vahvuuksista. Ne ovat erittäin halukkaita tukemaan poliisia ilmoittamalla pankkiautomaattien teknisiä tietoja ja käytettyjä menettelytapoja.

Rajat ylittävä yhteistyö on välttämätöntä: maiden tulisi jakaa tietoja (epäillyistä, tuomituista pankkiautomaattihyökkääjistä, menettelytavoista, epäilyttävistä ajoneuvoista, hyökkäyskuvista jne.) tutkimuksen tukena ja sen vuoksi, että toisessa maassa tuomitut epäillyt voidaan tuomita rikoksen uusimisesta/uusintarikollisuudesta.

Lopuksi lainvalvontaviranomaisten tietokannan luominen, jota lainvalvonta voi käyttää ja joka sisältää rikosteknisiä tietoja (esimerkiksi erityyppisistä IBNS-musteista, merkkiaineista ja merkitsimistä tai pankkiautomaattien suojalasista), voisi tukea vahvasti tutkimuksia ja yhdistää epäiltyjä tiettyyn rikospaikkaan. Teknologioiden standardisointi kansainvälisellä tasolla on usein riittämätöntä: tammikuussa 2019 pidetyssä konferenssissa osallistujat mainitsivat, että muste- ja rikostunnisteiden standardointi EU:n tasolla voisi helpottaa huomattavasti tutkimuksia.

Valvontakamerat ja kuuntelulaitteet

Valvontakamerajärjestelmien ja kuuntelulaitteiden kuva- ja äänitiedot voivat tukea sekä hyökkäyksen reaaliaikaista havaitsemista (esim. rikospaikalle saapuvien pelastustyöntekijöiden fyysisen vahingon estämiseksi) että myöhempiä tutkimuksia (esim. rikoksentekijöiden ja heidän menettelytapansa tunnistamiseksi). Valvontakamerakuvia voidaan yhdistää julkisten ja muiden pankkiautomaatin läheisyydessä olevien valvontakamerajärjestelmien kuviin sekä liikennekamerakuviin, jotta saadaan täydellisempi kuva tekijöistä ja heidän menettelytavastaan.

Valvontakamerakuvat ovat kuitenkin usein heikkolaatuisia tai huonosti tallennettuja. Kuvien on oltava riittävän laadukkaita, jotta henkilö voidaan tunnistaa. Jälleen eurooppalaisten standardien asettaminen valvontakameraturvallisuudelle helpottaisi tutkintaa. Koska tekijät poistavat valvontakamerat usein käytöstä

ennen hyökkäystä, ei-näkyvien valvontakameroiden tai reaaliaikaisten kuuntelulaitteiden asentamista voidaan harkita.

Rangaistus ja rikoksentekijän kuntoutus

Johdonmukaisella ja ankaralla rangaistuksella on ennaltaehkäisevä vaikutus. Järjestäytyneen rikollisryhmän pidättämisellä on välitön vaikutus pankkiautomaattihyökkäysten määrään. Pankkiautomaattihyökkääjien vapauttaminen vankilasta johtaa kuitenkin usein myös uusiin hyökkäyksiin. Tämä tarkoittaa, että lyhyet tuomiot johtavat rikoksentekijöiden aktiivisuuteen jälleen nopeasti. Jokaisesta pankkiautomaatin fyysisestä hyökkäyksestä tuomittujen rikollisten vähimmäis- ja enimmäisrangaistukset vaihtelevat jäsenvaltioittain. Jotkut maat uskovat, että ankarammat rangaistukset estävät potentiaalisia tekijöitä. Tieteellinen tutkimus[5] osoittaa kuitenkin, että tuomioiden ankaruuden lisääminen ei välttämättä paranna pelotevaikutusta. Siksi saattaa olla mielenkiintoista tutkia korjaavia (ja rikoksentekijöihin perustuvia) kuntoutusohjelmia korkean uusiutumisen vähentämiseksi.

3.3 Ponnistelujen lisääminen

Kolmas akseli pankkiautomaattien fyysisten hyökkäysten estämiseksi sisältää toimia, jotka tekevät rikoksen suorittamisesta vaativampaa.

Rikostenkestävän ympäristön varmistaminen

Jos riskinarviointi (vrt. supra) osoittaa, että pankkiautomaatti sijaitsee korkean riskin ympäristössä, sijainti olisi purettava ja pankkiautomaatti siirrettävä matalan tai keskitason riskialueelle. Näin on varmasti, jos analyysi osoittaa, että rakennus voisi romahtaa, jos pankkiautomaattiin hyökättäisiin käyttämällä räjähteitä. Lainsäädäntö voitaisiin panna täytäntöön tällaisten toimenpiteiden täytäntöön panemiseksi korkean riskin tapauksissa. Pankkiautomaattien määrän vähentämisen ohella riskialttiissa ympäristöissä olisi myös rohkaistava käteisettömiä maksuja, pankkiautomaattien tarpeen vähentämiseksi.

Jos pankkiautomaatin siirtäminen ei ole mahdollista, on toteutettava mahdollisimman paljon turvatoimenpiteitä: esim. törmäykseltä suojaavien esteiden, lyhtypylväiden ja muiden katukalusteiden käyttö rakennukseen pääsyn rajoittamiseksi, ajoneuvojen pysäyttämisjärjestelmiä, riittävän katuvalaistuksen asentamista, lisääntynyttä avointa tai peiteltyä valvontaa sekä varkaudenestolaitteita, kuten seteleiden turmelemisjärjestelmä. Kun sijaintiin hyökätään paikassa, jota ei tunnistettu suureksi riskiksi, se olisi tunnistettava sellaiseksi ja ylimääräisiä turvatoimenpiteitä on lisättävä. Uudet tekijät olisi otettava huomioon riskinarviointityökalussa sen päivittämiseksi. Tämän riskin uudelleenarvioinnin tulisi olla toistuva toimenpide.

Pankkiautomaattien vahvistaminen

Pankkiautomaattivalmistajat tarjoavat vakiovalikoiman pankkiautomaatteja, joilla on useita turvaominaisuuksia, jotka on luokiteltu Euroopan standardointikomitean (CEN) turvallisuusluokkien mukaan. Yleensä pankkiautomaateissa on CEN-merkintä, joka vaihtelee alemmasta CEN1-luokasta korkeimpaan, CEN4-luokkaan. Ominaisuudet, kuten rungon vahvuus ja hyökkäyskestävyys, määräävät luokan. Kaasunkestävyys tarjotaan enimmäkseen lisävarusteena (CEN-GAS). Vakiomalleja voidaan parantaa lisäsuojatoimenpiteillä. Yleensä kolmannet osapuolet asentavat nämä ominaisuudet varmistaakseen paikallisen lainsäädännön noudattamisen ja perusmallin mukauttamisen paikallisten asiakkaiden vaatimuksiin. Lisävarusteisiin sisältyy erilaisia antureita kaasun neutralointijärjestelmän tai IBNS:n aktivoimiseksi *paikan päällä* tapahtuvassa hyökkäyksessä tai hyökkäyksessä, jossa käytetään räjähteitä ja parannettuja luukkuja ja holvilukkoja luvattoman pääsyn estämiseksi kassakaappiin, jossa pääluukku on vaurioitunut. Siirrettävissä, itsenäisissä pankkiautomaateissa on tärkeää käyttää ankkurointijärjestelmiä, jotka tarjoavat lisäsuojaa ulosveto- / törmäyshyökkäyksiä vastaan. Seurantajärjestelmiä voidaan sisällyttää pankkiautomaatteihin tutkijoiden tukemiseksi, kun pankkiautomaatti siirretään toiseen paikkaan ennen sen avaamista.

Arkkitehtoniset toimenpiteet

Pankkiautomaattia asennettaessa on suositeltavaa käyttää automaatteja, joihin päästään käsiksi niiden takapuolelta. Tällöin tekijän on päästävä sisään rakennukseen ja käsiksi koneen takaosaan varastaakseen käteisvaroja. Siirrettävät, itsenäiset pankkiautomaatit ovat haavoittuvimpia. Näiden pankkiautomaattien määrien vähentäminen lisäisi turvallisuutta. Velvollisuus asentaa pankkiautomaatteja murtovarmaan huoneeseen vähentäisi automaattisesti erillisten pankkiautomaattien käyttöä.

Sumujärjestelmä

Sumutykki täyttää nopeasti huoneen tiheällä sumulla, jotta tunkeilija ei näe mitään. Tämä turvasumu tekee pankkiautomaattihyökkäyksen toteuttamisen usein mahdottomaksi. Ainakin järjestelmä hidastaa rikoksentekijää jättäen aikaa poliisin puuttumiseen. Turvasumujärjestelmä on kytketty hälytysjärjestelmään ja voidaan aktivoida kahdella tavalla. Hälytysanturit, kuten liiketunnistimet (yöllä) tai pankkiautomaattiluukun peukalointianturit, voivat laukaista järjestelmän automaattisesti. Se voidaan aktivoida myös hälytyskeskuksessa, jotta vältetään liian monta väärää hälytystä. Seinän läpi ulottuvissa ulkoautomaateissa sumujärjestelmää voidaan käyttää pankkiautomaatin takana täyttämään takana oleva huone sumulla ja heikentämään näkyvyyttä.

Sumujärjestelmät voivat tarjota avoimissa tiloissa, kuten huoltoasemilla ja supermarketeissa sijaitsevien pankkiautomaattien täsmäytetyn suojauksen. Tämä välttää koko alueen täyttämistä sumulla. Sumusuojaus onnistuu parhaiten, kun sumu tulee eri kulmista tai kun se täyttää pankkiautomaatin takana olevan tilan

törmäyshyökkäysten tapauksessa. Testejä suoritetaan sen selvittämiseksi, voidaanko sumutykkejä asentaa itse pankkiautomaatteihin huoneen sijaan, jossa pankkiautomaatti sijaitsee. Sumuun voidaan lisätä DNA-merkitsimiä, jotka värjäävät tekijät ja heidän vaatteensa.

3.4 Rinnakkaiset toimenpiteet

Edellä mainittujen ennalta ehkäisevien toimenpiteiden tehokkaan ja vaikuttavan täytäntöönpanon varmistamiseksi on harkittava useita rinnakkaisia toimenpiteitä. Nämä toimenpiteet ovat välttämättömiä kokonaisvaltaisen ennaltaehkäisevän ja operatiivisen lähestymistavan mahdollistamiseksi tai vahvistamiseksi fyysisten pankkiautomaattihyökkäysten torjumiseksi.

Lainsäädäntö

Monissa maissa laki velvoittaa pankkiautomaattitarjoajat toteuttamaan ennaltaehkäiseviä toimenpiteitä. Muissa maissa pankkien ja lainvalvontaviranomaisten väliset sopimukset takaavat hyvin hoidetun lähestymistavan pankkiautomaattien fyysisiin hyökkäyksiin. Alat, joilla sääntelytoimenpiteitä voidaan harkita, ovat:

- ennalta ehkäisevien toimenpiteiden sisällyttäminen;
- oikeudelliset puitteet, jotka mahdollistavat lainvalvontaviranomaisten sekä julkisten ja yksityisten kumppanien välisen yhteistyön;
- rangaistuksen uudelleenkäsittely, jos pankkiautomaattien fyysisiin hyökkäyksiin osallistuvien rangaistukset ovat liian alhaiset.

Usein vain pankkilaitokset ovat kuitenkin velvollisia noudattamaan vaatimuksia, ja nämä lait tai sopimukset eivät sido riippumattomia pankkiautomaattipalvelujen tarjoajia. Tämä on yleinen heikko kohta sääntelyjärjestelmässä.

Jotkut maat eivät pane täytäntöön mitään asetusta, mutta yrittävät saada pankkiautomaattipalveluntarjoajat ryhtymään ennaltaehkäiseviin toimiin lisäämällä tietoisuutta rikollisuuden alueista ja suuntauksista: tämä osoittautuu erityisen vaikeaksi maissa, joissa on paljon riippumattomia pankkeja.

On ehdottoman välttämätöntä varmistaa, että ennalta ehkäisevien toimenpiteiden tehokas täytäntöönpano sisältää muutoksia lainsäädännössä ja säännöksissä sekä kansallisella että kansainvälisellä tasolla, mikä sitoo kaikenlaisia pankkiautomaattitarjoajia. Ihannetapauksessa lainsäädäntö olisi yhdenmukaistettava EU:n tasolla, jotta vältetään se, että yhden maan lainsäädäntöön sisältyvät vahvat ennaltaehkäisevät toimenpiteet saavat järjestäytyneitä rikollisryhmiä siirtymään muihin maihin, joissa on vähemmän tiukka lainsäädäntö.

Mediastrategia

Toinen tärkeä ennaltaehkäisevän strategian akseli on vakiintunut mediastrategia, jolla pyritään vähentämään pankkiautomaattihyökkääjien odotuksia ja halua osallistua tähän rikokseen. Alhaisia onnistumisasteita ja tekijöiden suuria riskejä on korostettava. Viestintä palkinnoista (saalis) tai pankkiautomaattihyökkäyksen yksityiskohdat, kuten kyseessä oleva pankkiautomaattityyppi tai vältetty menettelytapa. Toisaalta tarvitaan laaja-alaista viestintää epäiltyjen pidättämisistä ja tuomion jälkeisiä rangaistusseuraamuksia.

Parannettu yhteistyö

Tiiviimpää yhteistyötä ja tiedonvaihtoa on ehdotettu paljon, mutta sitä ei voida korostaa tarpeeksi. Operatiivinen tietojenvaihto kansainvälisellä tasolla on osa Europolin ydintoimintaa. Tämän tiedonvaihdon

lisäksi ennaltaehkäisykonferenssi osoitti selvän tarpeen lisätä monitieteistä ja monitasoista yhteistyötä ja tiedon jakamista kaikkien asiaankuuluvien sidosryhmien, kuten lainvalvontaviranomaisten, viranomaisten, pankkiautomaattien ja turvallisuus- ja suojauslaitteiden valmistajien, ammattijärjestöjen, pankkiautomaatin tarjoajien (pankit ja riippumattomat tarjoajat), turvayhtiöiden ja hälytyskeskusten välillä. Tähän pitää kuulua paikallinen, kansallinen ja kansainvälinen taso.

Lisävahinkojen riskin vähentäminen

Kiinteillä räjähteillä tapahtuvien hyökkäysten yhteydessä jotkut järjestäytyneet rikollisryhmät jättävät materiaalia jälkeensä. Tämä voi luoda vaarallisia tilanteita pelastustyöntekijöille tai siviileille (paikalliset asukkaat ja ohikulkijat). Heidän turvallisuutensa on varmistettava. Kuten Belgiassa, protokollia ja menettelyjä, joita pelastustyöntekijöiden (sekä lainvalvontaviranomaisten että pankkiautomaatin tarjoajien) on noudatettava, on kehitettävä ja yhdenmukaistettava keskenään. Toinen paras käytäntö tässä yhteydessä on esimerkki Alankomaista, jossa pankkiautomaattihyökkäyksestä peräisin olevaa valvontakamerakuvaa käytetään tilanteen arviointiin. Hälytyskeskusten kanssa voidaan tehdä sopimuksia, jotta nämä kuvat olisivat välittömästi saatavissa.

Sosiaalinen ehkäisy

Järjestäytyneet rikollisryhmät rekrytoivat usein nuoria. Hankkeita voitaisiin perustaa tukahduttamaan nämä rekrytointiprosessit varhaisessa vaiheessa. Poliisin tai sosiaalityöntekijöiden tulisi olla valppaana näiden prosessien suhteen, ja he voivat puuttua asiaan henkilökohtaisesti ottamalla yhteyttä mahdollisiin tekijöihin.

04 PÄÄTELMÄT

Viimeisen kahden vuoden aikana pankkiautomaattien fyysistä hyökkäyksistä kärsivien maiden määrä kasvoi Euroopassa. Tältä osin Europol ja EUCPN työskentelivät yhdessä parhaiden toimenpiteiden keräämiseksi tämän rikoksen torjumiseksi ja estämiseksi.

Menestyvä lähestymistapa pankkiautomaattien fyysisten hyökkäysten torjumiseksi koostuu operatiivisten ja ennalta ehkäisevien toimenpiteiden yhdistelmästä, mieluiten sisällytettynä lainsäädäntökehykseen. Jotta vältetään se, että yhdessä maassa toteutettavat vahvat toimenpiteet johtavat järjestäytyneitä rikollisryhmiä kohti haavoittuvampia maita, suositellaan näiden toimenpiteiden toteuttamista Euroopan tasolla.

Tämän tyyppisen rikollisuuden estämiseksi ja torjumiseksi olisi laadittava selkeä strategia kolmessa vaiheessa: tilanteen arviointi, riskien arviointiin perustuvan ennaltaehkäisevän lähestymistavan kehittäminen ja ennalta ehkäisevien toimenpiteiden toteuttaminen.

Pankkiautomaattien fyysisten hyökkäysten riskinarvioinnin tulisi sisältää pankkiautomaattien ja niiden ympäristön ominaispiirteet, yhteistyö kumppaneiden ja sidosryhmien kanssa liittoutumien luomiseksi tämän rikoksen torjumiseksi sekä ennaltaehkäisevän ja oikeudellisen kehyksen arviointi. Kun tilanne on arvioitu, julkisen ja yksityisen sektorin yhteistyöhön perustuva strategia sekä ennaltaehkäisevät ja operatiiviset vastatoimet olisi luotava. Ennaltaehkäisevien toimenpiteiden tarkoituksena on vähentää tekijän aikomusta ja mahdollisuuksia osallistua pankkiautomaatin fyysiseen hyökkäykseen. Tämän saavuttamiseksi ehdotetaan ennaltaehkäisevien toimien kolmea akselia: palkkioiden vähentäminen, riskin lisääminen ja tarvittavien ponnistelujen lisääminen. Rinnakkaistoimenpiteiden tulisi täyttää ennaltaehkäisevä strategia. Kansallisen viranomaisen perustaminen, jolla on valtuudet määrätä nämä tarpeelliset toimenpiteet, on paras käytäntö.

Kun **palkkioita vähennetään,** rikollisen halu osallistua tällaiseen rikokseen vähenee. Pankkiautomaatin käteismäärän vähentäminen rajoittamalla täydennettävän käteisrahan määrää vain yhden päivän tarpeeseen tai (haavoittuvimpien) pankkiautomaattien tyhjentäminen yöksi, on yksi keino vähentää rikollisten odotuksia. Toinen tapa on turmella saalis ja tehdä rahat jäljitettäviksi. Tässä yhteydessä voidaan käyttää setelinsuojausjärjestelmää (IBNS), joka värjää setelit ja merkitsee ne varastetuiksi. Tämä menetelmä on tehokkain, kun rikollisten on mahdotonta käyttää tätä rahaa tai palauttaa nämä setelit lailliseen käteisrahaa käyttävään järjestelmään. Pankit ja yleisö voivat saavuttaa tämän kieltäytymästä värjättyjä seteleitä maksua varten, ja asentamalla setelien hyväksymislaitteita, jotka voivat havaita ja hylätä värilliset setelit. Tässä suhteessa investointi infrapunajärjestelmiin, jotka havaitsevat infrapunamerkeillä merkityt setelit, on osoittautunut kustannustehokkaaksi ratkaisuksi Belgiassa ja Ranskassa. IBNS-järjestelmää asennettaessa maiden tulisi harkita perusteellisesti valittuja aktivointimekanismeja, seteleiden neutraloinnin vähimmäisvaatimuksia ja rikosteknisen merkinnän lisäämistä musteeseen.

Toimenpiteet, jotka estävät potentiaalisia tekijöitä tekemästä rikoksia **lisäämällä** havaitsemis- ja rangaistusriskiä, ovat toinen akseli pankkiautomaattien fyysisten hyökkäysten estämiseksi. Pankkiautomaattihyökkääjien havaitsemisen ja rankaisemisen avain on tiedonkeruu ja jakaminen kaikkien sidosryhmien välillä, sekä kansallisella että kansainvälisellä tasolla. Laadukkaiden

valvontakamerakuvien ja äänitietojen vaihto voi lisätä varhaisen havaitsemisen ja onnistuneen tutkinnan mahdollisuuksia. Valvontakameroiden tai kuuntelulaitteiden käytöstä poistamisen ehkäisemiseksi ennen hyökkäystä, ei-näkyvien valvontakameroiden tai reaaliaikaisten kuuntelulaitteiden asentamista voidaan harkita. Oikeustieteellisen tietokannan luominen ja tekniikoiden standardointi Euroopan tasolla voisi helpottaa suuresti kansainvälistä yhteistyötä ja tutkimuksia. Jos rikoksentekijät vangitaan ja tuomitaan, saattaa olla mielenkiintoista tutkia korjaavia (ja rikoksentekijöihin perustuvia) kuntouttavia ohjelmia korkean uusiutumisen vähentämiseksi.

Kolmas akseli pankkiautomaattien fyysisten hyökkäysten estämiseksi sisältää toimia, jotka **lisäävät** rikoksen suorittamiseen vaadittuja ponnisteluja. Kun pankkiautomaatti asennetaan rikoksia kestävään ympäristöön, jossa on enimmäismäärä turvallisuustoimenpiteitä, rikoksentekijöiden on haastavampaa suorittaa fyysisiä pankkiautomaattihyökkäyksiä. Lisäksi tavallista pankkiautomaattisuojausta voidaan parantaa useilla lisäsuojausominaisuuksilla. Näiden toimenpiteiden lisäksi sumujärjestelmän asentaminen voi estää tekijää tai ainakin hidastaa hyökkäystä.

Useat **rinnakkaistoimet** vahvistavat edellä mainittuja toimenpiteitä, kuten sellaisen oikeudellisen kehyksen luominen, joka velvoittaa kaikki pankkiautomaattitarjoajat toteuttamaan ennaltaehkäiseviä toimenpiteitä, vakiintuneen tiedotusstrategian kehittäminen, tehostettu yhteistyö paikallisella, kansallisella ja kansainvälisellä tasolla, ohjeet ensihoitajille lisävahinkojen välttämiseksi ja sosiaaliseen ennaltaehkäisyyn tehtävät investoinnit rikollisen rekrytoinnin vähentämiseksi.

Factsheet

SUOSITUKSET ENNALTAEHKÄISEVÄÄN LÄHESTYMISTAPAAN: YLEISKATSAUS

Kehitä tehokas vastaus pankkiautomaattien fyysisten hyökkäysten estämiseksi

Arvioi tilanne

> Luo pankkiautomaattien riski-profiili maassasi / alueellasi.

> Tunnista kumppanit ja sidos-ryhmät pankkiautomaattien fyysisten hyökkäysten torjun-nassa ja arvioi yhteistyötä.

> Arvioi oikeudellinen kehys pankkiautomaattien fyysisten hyökkäysten torjumiseksi kansallisella ja kansainvälisellä tasolla.

Kehitä ennaltaehkäisevä lähestymistapa

> Määritä (tärkeimmät) riskit ja prioriteetit.

> Määritä parhaat ehkäisevät toimenpiteet näiden riskien kattamiseksi ottamalla huomioon kolme pääakselia.

> Määritä tarvittavat rinnakkaiset ennaltaehkäisevät toimenpiteet toteutettujen ennaltaehkäisevien toimenpiteiden vahvistamiseksi.

Ennaltaehkäisevät toimenpiteet, joihin voidaan ryhtyä

01

Palkintojen vähentäminen

> Käteismäärän vähentäminen.
  - Pankkiautomaattien tyhjentäminen yöllä.
  - Täyttömäärien / -tiheyksien lisääminen.

> Ryöstösaaliin tärveleminen.
  - Älykkäät setelinsuojausjärjestelmät (IBNS).
  - Infrapunamerkit (IBNS-muste) värjättyjen setelien havaitsemiseksi setelien vastaanottajien toimesta.
  - Kehitteillä: liima.

02

Riskin lisääminen

> Rajat ylittävä tiedonvaihto seuraaville:
  - mahdollisen pankkiautomaattihyökkäyksen varhainen tai reaaliaikainen havaitseminen,
  - operatiivisen lähestymistavan vahvistaminen,
  - rikoksenuusijoiden tuomitseminen,
  - rikosteknisten tietojen vaihto Euroopan tasolla.

> Valvontakamerat ja kuuntelulaitteet.

> Seuraamukselliset rangaistukset ja rikoksentekijän kuntoutus.

03

Ponnistelujen lisääminen

> Rikoksilta suojatun ympäristön varmistaminen.
  - Korkean riskin pankkiautomaattien sijainnin vaihtaminen.
  - Turvatoimenpiteet: fyysiset esteet, valvonta jne.

> Pankkiautomaattien lujittaminen ikkunoilla, suojaus kaasua, räjähteitä yms. vastaan.

> Arkkitehtoniset toimenpiteet, kuten takaa käytettävät koneet.

> Turvasumujärjestelmät.

Rinnakkaistoimet ennaltaehkäisevän lähestymistavan vahvistamiseksi

> Tehokas lainsäädäntö mukaan lukien toimenpiteet pankkiautomaattien fyysisten hyökkäysten ennalta ehkäisemiseksi, seuraamukselliset tuomiot jne.

> Tehokas mediastrategia, joka estää rikoksentekijöitä.

> Laajennettu yhteistyö kaikkien sidosryhmien (julkiset, yksityiset, lainvalvontaviranomaiset) välillä pankkiautomaattien fyysisten hyökkäysten torjunnassa.

> Vähennä ensihoitajille tai siviileille (esim. paikalliset asukkaat ja ohikulkijat) aiheutuvien mahdollisten vahinkojen riskiä.

> Sosiaalinen ehkäisy, jolla vältetään nuorten palkkaaminen (tämän tyyppisiin) rikoksiin.

ENDNOTES

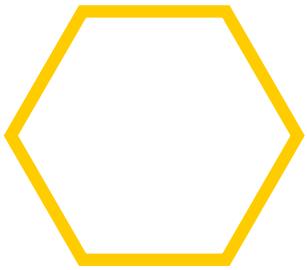
1 Willem Pieter de Groen, Zachary Kilhoffer and Roberto Musmeci, *The future of EU ATM markets: impacts of digitalisation and pricing policies on business models*, CEPS report, 2018

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 Euroopan keskuspankki Euroopan keskuspankin päätös euro-seteleiden nimellisarvoista, selitelmistä, vaihtamisesta, käytöstä poistamisesta ja seteliaiheen käytöstä, 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