Az ATM-ek elleni fizikai támadások megelőzése

EGY HATÉKONY MEGKÖZELÍTÉS KIDOLGOZÁSA

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.

”

KÖSZÖNETNYILVÁNÍTÁS

Ez a dokumentum az Európai Unió Bűnüldözési Együttműködési Ügynöksége (European Union Agency for Law Enforcement Cooperation, Europol) és az Európai Bűnmegelőzési Hálózat (European Crime Prevention Network, EUCPN) titkársága együttműködésének eredménye. Köszönetünket szeretnénk kifejezni azoknak a bankjegykiadó automaták (automated teller machine, ATM) elleni fizikai támadásokkal foglalkozó szakértőknek, akik időt és fáradtságot nem kímélve támogatták jelen ajánlás létrehozását, azáltal, hogy részt vettek az ATM-ek elleni fizikai támadások témájában rendezett konferencián (2019. január, Brüsszel), és alapvető információkat osztottak meg velünk. Külön köszönet illeti az EU-s és nem EU-S („harmadik") országok bűnüldöző ügynökségeit, a magánszektort, ideértve a bankautomata-ipar szakmai szervezetét (ATM Industry Association, ATMIA), a BPostot, a Holland Bűnmegelőzési és Biztonsági Központot (Centrum voor Criminaliteitspreventie en Veiligheid, CVV), Diebold Nixdorfot, a Biztonságos Tranzakciók Európai Szövetségének az ATM-ek és ATS-ek (automata széfek) elleni támadásokkal foglalkozó szakértői csoportját (European Association for Secure Transactions Expert Group on ATM and ATS Physical Attacks, EAST EGAP), az Európai Intelligens Pénzbiztonsági Szövetséget (European Intelligent Cash Protection Association, Euricpa), az ING-t, a Febelfint, az NCR-t, a Protectet, az SIOC Bankinget, a Spinnakert, a TMD Security-t, valamint Belgium, Horvátország, Németország és Spanyolország belügyminisztériumait.

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

TARTALOMJEGYZÉK

KERETEK

Mivel a bankjegykiadó automaták (ATM-ek) elleni fizikai támadások és az érintett európai országok száma folyamatosan növekszik, az Európai Bűnmegelőzési Hálózat (EUCPN) és az Europol rendezett egy konferenciát (2019. január), ahol a bűnmegelőzési szervezetek, valamint a köz- és magánszférába tartozó partnerek együtt tekintették át az ilyen típusú bűncselekmények megelőzésének lehetőségeit. Jelen ajánlás a konferencia következtetéseit foglalja össze annak érdekében, hogy felhívja a hatóságok figyelmét az ATM-ek elleni fizikai támadásokra és a megelőző intézkedésekre.

Az Európai Unió tagállamait korlátozott, de egyre nagyobb számban érintik az ATM-ek elleni fizikai támadások. A támadások okozta 2017-es pénzügyi veszteséget 30 millió euróra becsülik Európában. Néhány országban folyamatosan jelentős számú, ATM-ek elleni fizikai támadást tapasztaltak, más országokban pedig jelentősen nőtt az ilyen jellegű esetek száma az elmúlt 2 évben. A bűnözésnek ez a területe gyors fejlődést mutat. Bizonyos országok sikeres megközelítést alkalmaztak az ATM-ek elleni fizikai támadások kezelésére, és az elmúlt időszakban jelentős csökkenést tapasztaltak. Másrészt, korábban nem érintett országok voltak kénytelenek szembesülni az ATM-ek elleni fizikai támadások hirtelen megugrásával 2018-ban, ami a bűnszervezetek területeinek kiterjesztésével magyarázható. Ezek a bűncselekmények nem csak a bankokat érintik: független szolgáltatók ATM-jeit is egyre nagyobb számban éri támadás, mivel ezek gyakran sebezhetőbb területeken vagy helyszíneken vannak elhelyezve.

A bűnözők által az ATM-ek elleni támadásra alkalmazott különböző elkövetési módszerek (modi operandi, MO-k) két fő kategóriába sorolhatók: ATM-ek elleni fizikai támadások és ATM-hez köthető csalások (ideértve az ATM-ek logikai rendszere elleni és a vírusokkal történő támadásokat is). Jelen kiadvány az ATM-ek elleni fizikai támadásokkal foglalkozik, vagyis az ATM-ek fizikai eszközökkel történő erőszakos, a készpénz eltulajdonítását célzó feltörésével. Az erőszakos feltörést a következő eszközökkel lehet végrehajtani:

> **robbanóanyagok használatával:** a támadók gáz vagy szilárd halmazállapotú robbanóanyagokat használva fizikailag törik fel az ATM pénztartó rekeszét, és így férnek hozzá a készpénzhez;

> kirántásos támadások: a támadók fizikailag, gyakran egy csúcskategóriás jármű segítségével távolítják el az ATM-et a beépítési környezetéből;

> in-situ támadások: a támadók erőszakkal vágják át a pénzrekeszt, amihez gyakran használnak vágó- vagy törőszerszámokat, például sarokcsiszolót, kalapácsot vagy oxiacetilén hegesztőket.

01 AZ ATM-EK ELLENI FIZIKAI TÁMADÁSOK SIKERÉT MEGHATÁROZÓ TÉNYEZŐK

Az ATM-ek elleni sikeres támadások aránya alacsony: csak 1/3 részük sorolható ebbe a kategóriába. Sikertelen támadások esetén azonban az épületekben (pl. robbanóanyagok által) okozott kár ugyanolyan fontos, hiszen ilyenkor a bűnügyi helyszín közelében lévő környezet kockázatos marad az ott lakók, az elsőként beavatkozók és a járókelők számára.

A fizikai támadás sikere számos tényezőn múlik, ideértve az ATM jellemzőit, az ATM elleni támadás előkészítését, valamint az elkövetők tapasztalatát és szakértelmét.

1. Az ATM-ek sebezhetősége

A leginkább sebezhető ATM-ek azok, amelyek épületeken kívül (falba épített, TTW) találhatók vagy épületek belső terében állnak. Egy beltéri (önmagában álló) ATM megtámadásakor a bűnszervezetek inkább a kereskedelmi létesítményekben lévő ATM-eket részesítik előnyben, semmint a bankokban lévőket, ahol jellemzően megerősített felügyeletre kell számítaniuk. A bankok főként a bank épületén kívül vagy belül elhelyezett ATM-eket alkalmaznak. A távolabbi helyszíneken, utcákon, kereskedelmi létesítményekben, pl. benzinkutakon, szupermarketekben, szállodákban, kaszinókban, repülőtereken stb. telepített automaták a bankfiókok bezárásával egyre fontosabb szerephez

jutnak. A független szolgáltatók inkább önmagukban álló ATM-eket telepítenek. Az ő ATM-jeik gyakran üzlethelyiségekben, vendéglátóhelyeken, szabadidős létesítményekben, közlekedési csomópontokban (vasútállomások, repülőterek stb.), középületekben vagy utcákon találhatók.

Az online banki szolgáltatások egyre növekvő népszerűségével párhuzamosan a következő években valószínűleg sok bankfiókot fognak bezárni, ami az ATM-ek számának csökkenését is maga után vonja[1]. Ez azonban a sebezhetőbb helyszíneken lévő, bankoktól távoli és a független szolgáltatókhoz köthető ATM-ek számának növekedését is eredményezheti.

2. Az ATM-ek elleni támadások előkészítése

Egy támadás előkészítése több hetet vagy akár hónapot is felölelhet. A tetteseknek össze kell gyűjteniük a szükséges **eszközöket és erőforrásokat**, például járműveket, felszereléseket és kapcsolattartókat. A **járművek** alapvetően fontos szerepet játszanak az ATM-ek elleni fizikai támadásokban: az elkövetők főként autóval közlekednek és a támadás után is jellemzően gyors járművekkel menekülnek, amelyek gyakran lopottak vagy béreltek, de akár (pl. interneten) vásárolt autók is lehetnek. Az ATM-ek elleni fizikai támadásoknál használt **felszerelések** készen és legálisan, átlagos boltokban kaphatók, ami nem növeli az ilyen típusú bűncselekmények elkezdésének korlátait. Egy szerszám eredetének lekövetése nehéz feladat a bűnüldözők számára, így az elkövetők csak korlátozott kockázatot vállalnak. Az ATM-ek elleni támadásban aktívan résztvevő, nemzetközi szintű bűnszervezeteknek szinte minden alkalommal van a célországban kapcsolattartójuk (olyan személyek, akik egy bizonyos ideig ott tartózkodnak), vagy alternatív megoldásként rajtaütésszerűen is támadhatnak. Ezek a kapcsolattartók a logisztikai ügyintézésben segítik a bűnszervezeteket, például szállást bérelnek, beszerzik a szükséges járművet vagy más eszközöket, illetve becserkészik a célpontokat. Egyes nemzetközi elkövetők teljes mértékben ráhagyják a logisztikai ügyintézést és a becserkészési feladatokat a helyi kapcsolattartókra, és ők csak az ATM elleni támadás végrehajtására érkeznek meg közúton vagy repülővel.

A bűnszervezetek gyakran kiterjedt **becserkészési** műveleteket végeznek a megfelelő célpontok beazonosítása érdekében: kiderítik az ATM töltésének időpontját, felderítik az ATM környezetét, az automata technikai jellemzőit, a menekülési útvonalakat és a helyszínen lévő biztonsági intézkedéseket, pl. a videokamerás megfigyelőrendszereket (CCTV), a riasztóérzékelőket és a takarásokat.

Egyes bűnszervezetek bizonyos akciókkal **zavarják meg a bűnüldözők és biztonsági szolgálatok** tevékenységét még a támadás előtt. Manipulálják a riasztórendszereket és a közvilágítást, elterelési technikákat alkalmaznak, áthajtási akadályokat állítanak fel vagy manipulálják a bűnüldöző szervek autóit.

3. Az elkövetők tapasztalata és szakértelme

Az ATM-ek elleni fizikai támadások vonzóak a bűnözők számára, mivel a készpénz azonnal elérhető, és kiterjedt hálózatra sincs szükség a lopott áruk eladásához. Kényelmes megoldás azon bűnözők számára, akik már aktívak a vagyon elleni bűncselekmények területén.

A bűnszervezeteknek meg kell szerezniük a **szükséges tapasztalatot és szakértelmet**, mivel ezek meghatározó szerepet játszanak a támadások sikerében vagy sikertelenségében. Az, hogy milyen tapasztalatra és szakértelemre van szükség, nagy mértékben függ a **támadás típusától**. A kirántásos és az *in situ* támadásokban egyszerű elkövetési módszereket (főként vakmerőséget és nyers erőt) alkalmaznak, így ezekhez rendszerint nincs szükség speciális képességekre. Az éghető gázokat vagy szilárd robbanóanyagokat alkalmazó támadások már magasabb szintű szakértelmet kívánnak.

A támadók különböző **szintű kompetenciákkal** rendelkeznek. Egyrészt, a jól szervezett és nagy tapasztalattal bíró bűnszervezetek akár percek alatt képesek végrehajtani egy ATM elleni sikeres támadást. Urai a helyzetnek, és képesek a kockázatot csak saját magukra korlátozni, így a járulékos károkat is a minimálisra csökkenteni. Másrészt, a kevésbé szervezetten működő, inkább opportunista csoportoknak sokszor nem sikerül a támadás, és jelentős károkat okozhatnak a helyszínen és a környező épületekben. A kevésbé szervezetten működő bűnszervezetek némelyikéről úgy gondolják, hogy inkább visszatérnek a hagyományos, szervezett vagyon elleni bűncselekményekhez, mivel az ATM-ek elleni támadáskor nem képesek felülkerekedni a megelőző intézkedéseken, és ezek elbátortalanítják őket.

02 A MEGELŐZŐ MEGKÖZELÍTÉS IRÁNTI IGÉNY

Azok az országok, ahol az ATM-ek elleni fizikai támadások sikerének aránya alacsony, vagy ahol az ATM-ek elleni fizikai támadások száma csökken, kiváló példái annak, hogy az ATM-ek fizikai megtámadása elleni küzdelemre vonatkozó megközelítés sikere az operatív és a megelőző intézkedések együttes alkalmazásán múlik. Mivel a bűnözés ezen területén aktívan működő bűnszervezetek száma alacsony, a bűnszervezeti tagok letartóztatása és következményes büntetése jelentősen csökkenti a támadások számát. Azonban a szabadon engedésük után sok támadó újrakezdi tevékenységét. Sőt, a bűnözői csoport sokszor gyorsan megoldja a letartóztatott elkövető helyettesítését. Ezért nagy szükség van megelőző intézkedésekre, lehetőleg úgy, hogy azok illeszkedjenek a jogi keretrendszerbe. Sőt, a tapasztalatok azt mutatják, hogy az egyik országban bevezetett megelőző intézkedések a bűnszervezeteket más országok sebezhetőbb célpontjaiba irányítják. Így csak idő kérdése, hogy az egyik országban megjelenő elkövetési módszerek másik országokra is átterjedjenek. Mindez világosan mutatja, mekkora **szükség van a megelőző és operatív intézkedések európai szintű** elfogadására, a magán-, a közszférában és a bűnüldöző szerveknél dolgozó partnerek szoros együttműködésére

03 MEGELŐZÉS

Az ilyen típusú bűnözés megelőzése és az ellene való küzdelem érdekében világos stratégiára van szükség. Ebben a fejezetben áttekintjük azt a három lépést, amelyet általában megtesznek az ATM-ek elleni fizikai támadásokkal való szembekerüléskor, illetve a megelőzésükért tett előkészületek során.

Elsőként a **helyzet felmérése:** fel kell állítani az ATM-ek és környezetük kockázati profilját figyelembe véve a megszerezhető készpénzmennyiséget (a lehetséges zsákmányt), valamint a járulékos károk és a személyi sérülések kockázatát. Másodszor, a kockázatértékelés után ki kell alakítani egy **megelőzési stratégiát.** Végül, a **megelőző intézkedéseket** végre is kell hajtani.

1. A helyzet felmérése

A bűnszervezetek hajlamosak olyan, bizonyos típusú ATM-eket vagy bizonyos szolgáltatók ATM-jeit célpontként megjelölni, amelyek jellemzői lehetővé teszik az ATM elleni támadást. Ezért szükséges az ATM-ek elleni fizikai támadások kockázatát alaposan felmérni, amihez lehetőség szerint a teljes készpénzbiztonsági láncot figyelembe kell venni, az átvételtől az ATM-be történő leszállításig. Az egyes ATM-ek kockázati profiljának felállításához többek között az alábbi tényezők elemzése szükséges:

- Az ATM helyének és környezetének jellemzői; olyan tulajdonságok, mint például a városi vagy vidéki helyszín, a népsűrűség, a rendőrőrsök távolsága, az automata rendszámfelismerő (ANPR) kamerák megléte a környéken, CCTV a közelben stb.
- Az ATM elhelyezkedése:
  - egy épület, bankfiók belső területén vagy azon kívül, vagy távolabbi (pl. kereskedelmi) helyszínen; beépítve vagy egy épülethez illesztve,
  - önállóan álló ATM-ek esetében: rögzítve van-e vagy sem,
  - beépített vagy épülethez rögzített ATM-ek esetében: vannak-e építészeti gyenge pontok, hogyan szervezik meg a pénz tárolását stb.
- Az ATM típusa.
- Az ATM-be épített biztonsági funkciók.
- Az ATM-ben lévő készpénzmennyiség.
- Az ATM-ek elleni támadások várható típusa és elkövetési módszere, annak érdekében, hogy először a leginkább megfelelő megelőző intézkedést lehessen bevezetni.
- A már megtett biztonsági és megelőző intézkedések (intelligens bankjegy-érvénytelenítő rendszerek (IBNS), CCTV, biztonsági ködképző (láthatóság-csökkentő) rendszer stb.).

További felmérendő elem még a partnerekkel, további szereplőkkel, valamint a törvényhozással való együttműködés szintje. Fel kell mérni a bűnüldöző szerveknél, valamint a magán- és a közszférában dolgozó partnerek közötti együttműködés szintjét, és szövetségeket kell létrehozni a bűnözés elleni küzdelem érdekében. Valószínűleg mindegyik partner rendelkezik olyan információkkal, amelyekkel hozzájárulhat a helyzet felméréséhez. Ebben a keretrendszerben a helyi rendőrségek és a helyi hatóságok különösen fontos szerepet töltenek be. A jogszabályi környezetet is értékelni kell, mivel egy olyan jogi keretrendszert kell létrehozni, amely alkalmas a megelőzésre, a kötelező megelőző intézkedések bevezetésére, valamint ítélethozatalra az ATM-ek elleni támadások esetében stb.

2. Megelőző megközelítés kidolgozása

A helyzet felmérése, valamint az ATM-ek biztonságára vonatkozó kockázatok fő területei, az erősségek és a gyengeségek meghatározása után ki lehet dolgozni a (gyakran a köz- és magánszféra együttműködésére épülő) stratégiát, és be lehet vezetni a megelőző és operatív ellenintézkedéseket. A megelőző intézkedéseknek az elkövetők szándékainak és adottságainak csökkentését kell megcélozniuk. Ennek elérése érdekében a Clarke[2]-féle öt helyzeti bűnmegelőzési stratégiából hármat alapul véve, három tengelyt javasolunk megelőző intézkedésekre vonatkozóan: a jutalmak csökkentése, az elkövetőket érintő kockázatok növelése, és a zsákmány megszerzéséhez szükséges erőfeszítések növelése.

A bűnözök a várható megtérülést és a kapcsolódó kockázatokat mérlegelik (pl. egy ATM elleni támadás során). A könnyedén megszerezhető jutalom esélyének csökkentése és az elkövetőket érintő kockázatok növelése csökkenti a várakozásaikat és a vágyat arra, hogy fizikai támadást indítsanak egy ATM ellen. Az ATM-ekhez való hozzáféréshez szükséges erőfeszítések növelése irányába ható további intézkedések is befolyásolják az elkövetők adottságait. Az opportunista elkövetők, akik gyakran belebuknak a próbálkozásokba, leállnak az ATM-ek elleni támadásokkal, az ATM-ek elleni támadások profi elkövetői számára pedig csökken a sikerességi arány, ami szintén befolyásolja a megtérülés/kockázat arányt.

Sőt, a párhuzamos intézkedések, pl. egy hatásos médiastratégia, a korai szociális megelőzés, valamint az épületek járulékos károsainak esélyét és a helyi lakosok, segélyhívók és járókelők biztonságát szavatoló intézkedések kiegészítik a megelőzési stratégiát.

A megközelítés felépítésének más módjai is lehetségesek. A holland hatóságok az ún. korlátmodellt alkalmazzák[3]. Ez a modell beazonosítja azokat a lépéseket, amelyeket egy bűnözőnek meg kell tennie ahhoz, hogy elkövessen egy bűntényt. Azokat a partnereket és lehetőségeket is meghatározza, amelyek lehetővé teszik a bűntény elkövetését, és hasznos eszköznek bizonyul ahhoz, hogy meg lehessen

szervezni az információgyűjtési folyamatot a bűntény elkövetésének helyén. Az ATM-ek elleni fizikai támadások végrehajtásához szükséges lépések azonosításával a bűntényt akadályozó korlátokat és a korlátok felállításához legideálisabb partnereket is meg lehet határozni. A korlátmodell azokat a jeleket is beazonosítja, amelyekkel riasztani lehet a köz- és magánszférához tartozó partnereket az ATM-ek elleni fizikai támadáskor, de olyan jeleket is meghatároz, amelyeket ezek a partnerek maguk küldhetnek, hogy értesítsék a hatóságokat a gyanújukról.

A megelőzés megerősítésével együtt járó kockázatok csökkentése érdekében alaposan kidolgozott stratégiára van szükség. A megelőző intézkedéseknek, amelyek nagyon hatásosak az amatőrök és utánzók elbátortalanításában, néha nem várt hatásaik is lehetnek. Néhány bűnözői csoport a „próba-szerencse" módszerhez folyamodik a sebezhető ATM-ek megtalálásakor, és ezzel egy sor megrongált ATM-et hagy maga után. A veszélyesebb és könyörtelenebb bűnszervezetek elkezdenek erőszakosabb elkövetési módszereket alkalmazni, például a támadásaik során áttérnek a gáz robbanóanyagokról a szilárd halmazállapotúakra.

A hatékony megelőző intézkedések bevezetéséhez a legjobb módszer egy nemzeti hatóság felállítása, amely megfelelő hatáskörrel rendelkezik ahhoz, hogy – a helyzetet alaposan felmérve – speciális intézkedéseket hozzon a nagy kockázatot jelentő ATM-ekre vonatkozóan. Ez a megközelítés hatékonynak bizonyult Franciaországban, és akkor működik különösen jól, ha egy jogi keretrendszer is létrejön, illetve az intézkedések végrehajtása operatív intézkedésekkel együtt történik.

3. A megelőző intézkedések végrehajtása

Az ebben a fejezetben bemutatott, az ATM-ek elleni fizikai támadások megelőzését célzó intézkedések a különböző országokban már bizonyítottak. Ezek a megelőző intézkedések témájában megtartott konferencia következtetésein, valamint az ATM-ek biztonságával foglalkozó nemzetközi szervezetek által aktívan támogatott megelőző intézkedéseken alapulnak. Sok intézkedés már jól ismert, hiszen számos ország is sikerrel valósított már meg ezek közül többet is. Azonban a javasolt intézkedések gyakran csak részben valósulnak meg, és nem kerülnek be a jogszabályi környezetbe.

Ahogy korábban említettük, a megelőző intézkedésekre vonatkozóan három tengely alkalmazását javasoljuk: a jutalmak csökkentése, az elkövetőket érintő kockázatok növelése, valamint a zsákmány megszerzéséhez szükséges erőfeszítések növelése.

3.1 A jutalmak csökkentése

A bűncselekményekből származó jutalmak csökkentése az első az ATM-ek elleni fizikai támadások megelőzésére vonatkozó tengelyek közül. Amíg fennáll a könnyen megszerezhető pénzre vonatkozó felfogás, a bűnözők elkövetnek ilyen típusú bűncselekményeket. Az elérhető készpénz mennyiségének csökkentése, illetve a készpénz eltávolítása vagy megsemmisítése mind csökkenti az érdekes zsákmány megszerzésének lehetőségét. A csökkent várakozások az ilyen típusú bűncselekmények elkövetése iránti vágyat is csökkentik.

A készpénzmennyiség csökkentése

A jutalom csökkentését célzó egyik intézkedés az ATM-ekben található készpénz mennyiségének csökkentése. Ideális esetben ezt a mennyiséget az egy napi kereskedési mennyiségre kellene korlátozni**.** A költséghatékonyságot egy bankok közötti együttműködés biztosíthatná. Hollandiában több bank együttműködésével bankfüggetlen ATM-hálózatot hoztak létre, ez a „Geldmaat". Az együttműködés célja a készpénz elérhetőségének, hozzáférhetőségének és biztonságának garantálása. Mindez valószínűleg az ATM-ek számának csökkenését eredményezi majd. Az ATM-ek ugyanakkor nem tartalmaznak majd több készpénzt, csak gyakrabban lesznek újratöltve, az újratöltések számát pedig az igény határozza meg.

Mivel a tettesek főként 3:00 és 4:00 között támadják meg az ATM-eket, határozottan javasolt az önmagukban álló ATM-ek (amelyek a legtöbbször kereskedelmi létesítményekben vagy nyilvános helyeken találhatók meg) kiürítése, és a készpénz trezorban való elhelyezése a nap végén. Egy figyelmeztető jelzés tájékoztatná az embereket arról, hogy az ATM-ben éjszaka nincs készpénz. A következő nap pedig az ilyen automatákat a vásárlók látóterén kívül, bezárt létesítményben kell újratölteni. Ilyen rendszer működik Franciaországban, ahol a jogszabályi környezet arra kötelezi az üzletekben, önmagukban álló ATM-eket üzemeltető kereskedőket, hogy éjszakára vegyék ki a készpénz az ATM-ből, és hagyják nyitva azt. Egyéb ATM esetén a bennük lévő készpénzmennyiséget az újratöltési gyakoriság növelésével lehetne csökkenteni.

A zsákmány tönkretétele és a pénz nyomon követése

Az intelligens bankjegy-érvénytelenítő rendszerek (IBNS) alkalmazása a jutalom tönkretételének elsődleges módszere. Ezek a rendszerek tintával jelölik meg a bankjegyeket, amivel jelezhető, hogy az adott bankjegy lopott. Az IBNS-tintához nyomkövetők és jelölők adhatók. Jelenleg ezeket a jelölőket főként törvényszéki célokra használják, mivel ezek hozzákapcsolják az adott bankjegyet a bűncselekmény helyszínéhez, és növelik az elkövetők elfogásának esélyeit. Habár az IBNS hatékony megelőző intézkedés, felvet bizonyos aggályokat.

Az Európai Központi Bank nem téríti meg a megjelölt bankjegyek értékét [4] (2003 óta), azonban számos EU-tagállam központi bankja ezt még megteszi. A megjelölt bankjegyeket a kaszinókon keresztül is visszavezethetik a legális rendszerbe. Az IBNS külön akadályt jelent a bűnözők számára, de még hatékonyabb lehetne, ha a megjelölt bankjegyeket a bűnözők az EU teljes területén sehol sem használhatnák fel. Ennek elérése érdekében a nemzeti központi bankoknak nem lenne szabad elfogadniuk a megjelölt bankjegyeket, kivéve bizonyos speciális körülmények fennállása esetén, pl. ha a bankjegyek téves aktiválás miatt szennyeződtek be. A lakosságot is fontos tájékoztatni arról, hogy ne fogadjanak el megjelölt bankjegyeket. Még hosszabb távon a bankjegykezelő berendezéseknek észlelniük kell a megjelölt bankjegyeket, és ilyeneket el kell helyezni a bankokban és a kereskedelmi létesítményekben, pl. kaszinókban, autómosókban stb. A tinta észlelése nehéz és drága, azonban költséghatékony megoldás lehet olyan infravörös rendszerek telepítése, amelyek az infravörös jelölővel megjelölt bankjegyeket észlelik. Ezek a rendszerek már bizonyították a hatékonyságukat, és Belgiumban és Franciaországban már bevált gyakorlatnak számítanak. Ha infravörös jelölővel ellátott bankjegyeket visznek egy ATM-hez, az ATM elfogadja („elnyeli") a pénzt, de nem írja jóvá a számlán, sőt a megjelölt bankjegyeket bemutató személyt nyilvántartásba is vehetik.

Az IBNS megoldások telepítésekor más megfontolások is szerepet játszhatnak. Sok gyártó az aktiválási mechanizmusuk vagy a tintatípusuk szerint több különböző IBNS megoldás is kínál. Az egyik elsődleges megfontolandó elem, hogy nem mindegyik IBNS-aktiválási technológia képes az összes veszély elhárítására. Egyes IBNS-ek jól működnek a kirántásos vagy *in situ* támadás, illetve gáztámadás esetén, de szilárd robbanóanyaggal elkövetett támadás esetén hatástalanok maradnak – és fordítva. Ezért a kiválasztott technológiát alaposan meg kell fontolni.

Egy másik megfontolandó tényező a kiválasztandó tinta típusa. Belgiumban nemzeti minimumkövetelményeket (biztonság, a megjelölt bankjegyek százalékos aránya, nem mosható stb.) határoztak meg az IBNS-ekre vonatkozóan, és független vizsgálatok tanúsítják, hogy a rendszer megfelel a nemzeti szabványoknak, illetve hogy a gyártó állításainak megfelelően működik. Fontos, hogy a vizsgálatokat valódi bankjegyeken végezzék, mivel léteznek a piacon olcsóbb tinták, amelyek a hamisított/utánzat bankjegyekkel jól működnek, de a valódiakkal nem, vagyis a tinta az eredeti bankjegyekből mosással eltávolítható. Fentieken túl, ajánlatos a tintához törvényszéki jelölőt is hozzáadni, ami lehetővé teszi a megjelölt bankjegyek és egy adott bűnügyi helyszín közötti kapcsolat vizsgálatát.

A bevált gyakorlatok azt mutatják, hogy az IBNS megoldások nagyon hatékonyak lehetnek, különösen, ha más megelőző intézkedésekkel együtt alkalmazzák őket. 2015-ben Franciaország új jogszabályt fogadott el, ami az IBNS-ek telepítéséről és az egyedi DNS-sel ellátott tinta alkalmazásáról szóló cikkeket is tartalmaz. Azt, hogy az IBNS-eket és az egyéb intézkedéseket hol kell bevezetni, a francia katonai rendőrség (gendarmerie) dönti el kockázatértékelés alapján. Amióta az új jogszabályi környezet megerősítette a megelőzési és operatív megközelítést, a támadások száma a 2013-as 300-ról 2018-ra 50-re csökkent.

Egy másik fejlesztés alatt álló módszer a zsákmány tönkretételére a **ragasztó** alkalmazása. A ragasztó hatékonyságát Hollandiában már sikerült bizonyítani, de a megvalósítás és működtetés költségei egyelőre nagyon magasak. Sőt, a ragasztó akár tűzveszélyes is lehet, ha a rendszer nem aktiválódik egy támadás előtt, mivel a ragasztó részecskéi a levegőben szétszóródva gyúlékony elegyet képezhetnek. Ez a módszer egyelőre nem áll készen a piaci bevezetésre, de a jövőben jó megoldás lehet.

3.2 A kockázat növelése

Az ATM-ek elleni fizikai támadások megelőzésének második tengelye a potenciális elkövetők elrettentése a bűntények elkövetésétől a lelepleződés és a büntetés kockázatának növelése révén. Amellett, hogy a robbanóanyagok használata az ATM-ek elleni támadások során a fizikai sérülések kockázatát is magában hordozza, a bűnözők számára a fő kockázatot a börtönbüntetés jelenti, akár tetten érik az elkövetőt, akár egy nyomozás során kapják el. Ahhoz, hogy csökkenjen a potenciális tettesek elkövetés iránti vágya, a lelepleződés és a büntetés esélyét kell megnövelni. A társadalom számára

természetesen a bűnözők elkapása és elítélése is hatékony megelőzési módszer, feltéve, hogy meg is büntetik őket, ahogy ezt számos országban láthattuk.

Az információk megosztása

Az ATM-ek elleni támadások elkövetőinek leleplezése és megbüntetése szempontjából kulcsfontosságú az ATM-ek fizikai megtámadása elleni küzdelemben részt vevő összes szereplő közötti információmegosztás. Ezek közé a szereplők közé tartoznak az ATM-szolgáltatók, a bűnüldöző hatóságok (rendőrség, ügyészség stb.), a közhatóságok, az ATM-ek és a biztonsági és védelmi eszközök gyártói, a szakmai szervezetek, az ATM-szolgáltatók (bankok és független szolgáltatók), a biztonsági cégek és a riasztóközpontok. Ideális esetben az információmegosztás nemzeti és nemzetközi szinten is működik.

Egy ATM ellen tervezett fizikai támadás korai észlelése nehéz feladat, ami csak akkor sikerülhet, ha a bűnüldözésben részt vevők és a magánszférához tartozó partnerek (biztonsági cégek és ATM-szolgáltatók) közötti nemzetközi szintű információcsere tökéletesen működik. Mutatók széles körét kell nyomon követni, ideértve a bűnüldöző ügynökségek közötti korai figyelmeztető jelzéseket a mozgásban lévő bűnszervezetekről, az ATM-ek elleni támadásokban használt gyanús járművekről, a biztonsági cégektől vagy az ATM-ek közelében tapasztalt gyanús viselkedésről szóló polgárőri jelentésekből származó információkról, az ATM-szolgáltatók által észlelt gyanús tranzakciókról és egyéb észlelési módszerekről. A korai észlelés érdekében végzett rendőrségi intézkedés lehet még a lopott autók, a robbanóanyagokat gyártó és forgalmazó vállalatok, valamint a robbanóanyagok használatára jogosult cégek megfigyelése is. A korai észlelés elérése érdekében tett erőfeszítések bonyolultak, és nem garantálják a sikert, ezért a támadások előtti bűnüldözési beavatkozások ritkán fordulnak elő.

Ha a korai észlelés nem lehetséges, a riasztóközpontok gyorsan képesek figyelmeztetést kiadni egy ATM elleni fizikai támadás esetén. A beavatkozás lehetővé tétele érdekében meg kell állapodni a riasztóközpontok és a bűnüldöző ügynökségek közötti gyors kommunikációra vonatkozó nemzeti előírásokról és protokollokról, és ezeket meg is kell valósítani. Egy valós idejű információ bármilyen korai észlelése esetén a bűnüldözőknek mindig mérlegelniük kell a beavatkozás időzítését és a sikeresség esélyeit. A bűnözők tetten érése nagyon nehéz feladat, ami akár veszélyes helyzeteket is előidézhet, mivel sok bűnszervezet igen erőszakos és nehéz fegyvereket használ.

Az ATM elleni támadást követő sikeres nyomozás érdekében a bűnüldöző rendőröknek az összes szereplővel kommunikálniuk kell, hiszen közülük bárki szolgálhat olyan információval, ami hozzájárulhat a nyomozás sikeréhez. Természetesen az elsődleges áldozatokkal, vagyis a bankokkal vagy egyéb ATM-szolgáltatókkal való kommunikáció és együttműködés is szükséges: ők olyan adatokhoz férnek hozzá, amelyek fontosak a nyomozás szempontjából. Az ATM-szolgáltató számára a bűnüldöző ügynökségektől származó információk segítséget nyújthatnak a megelőző intézkedések javításában. Sőt, a szakmai szervezetekkel és a gyártókkal fennálló kapcsolatok is hasznosnak bizonyulnak: gyakran küldenek biztonsági-riasztási témájú üzeneteket, amelyekre a többi érdekelt fél is feliratkozhat. Az ATM-gyártók nagy rálátással rendelkeznek az ATM-ek elleni támadások típusaira, valamint a megelőző intézkedések kapcsolódó gyengeségeire és erősségeire. Nagyon is támogatják a rendőrséget az ATM-ek technikai jellemzőire és az elkövetési módszerekre vonatkozó információkkal.

A határokon átnyúló együttműködés is alapvető fontosságú: az országoknak meg kell osztaniuk egymás között (a gyanúsított, elítélt ATM-támadókra, az elkövetési módokra, a gyanús járművekre, a támadásokról készült képekre stb. vonatkozó) információkat, nemcsak a nyomozás elősegítése miatt, hanem azért is, mert a másik országban elítélt gyanúsítottak visszaesőként büntethetők.

Végül, egy európai szintű – a bűnüldözők számára elérhető és törvényszéki adatokat (pl. különböző típusú IBNS-tinták, nyomkövetők és jelölők vagy ATM védőüvegek) is tartalmazó – adatbázis létrehozása is nagyban segíthetné a nyomozásokat, és összekapcsolhatná a gyanúsítottakat egy adott bűnügyi helyszínnel. Sokszor a technológiák nemzetközi szintű standardizálása is hiányos: a 2019. januári konferencia résztvevői is megemlítették, hogy a tinták és a bűncselekmények jelölésének EU-szintű standardizálása nagyban elősegíthetné a nyomozásokat.

CCTV és lehallgatóeszközök

A CCTV-rendszerekből és lehallgatókészülékekből származó kép- és hanganyagok támogathatják egyrészt egy adott támadás valós idejű felderítését (pl. a bűntény helyszínén elsőként beavatkozók fizikai sérüléseinek

megelőzése érdekében), másrészt a későbbi nyomozást (pl. az elkövetők és elkövetési módszerük beazonosítása érdekében). A CCTV-ből származó képek használhatók együtt a nyilvános és az ATM közelében lévő egyéb CCTV-rendszerek képeivel, a traffipaxok felvételeivel ahhoz, hogy az elkövetőkről és elkövetési módszerükről teljesebb kép alakuljon ki.

Azonban a CCTV-képek gyakran gyenge minőségűek vagy rossz körülmények között tárolják őket. Egy személy beazonosításához megfelelő minőségű képekre van szükség. Itt is igaz, hogy a biztonsági CCTV-kre vonatkozó európai szabványok támogathatnák a nyomozásokat. És mivel az elkövetők gyakran kikapcsolják a CCTV-kamerákat a támadás előtt, meg kell fontolni a láthatatlan CCTV-k vagy valós idejű lehallgatókészülékek használatát.

Büntetés és az elkövetők rehabilitációja

A következetes és súlyos büntetés bizonyítottan megelőző hatással jár. Egy bűnszervezet letartóztatása azonnali hatással van az ATM-ek elleni támadások számára, azonban a szabadon engedésük után gyakran a támadások felfutása érzékelhető. Ez azt jelenti, hogy rövid büntetésekkel az elkövetők nagyon hamar ismét aktívakká válnak. Az ATM-ek elleni fizikai támadások elkövetőire kiszabható minimum és maximum büntetés mértéke változó az egyes tagállamokban. Néhányan úgy gondolják, hogy a nagyobb büntetések lehetősége elrettenti a potenciális elkövetőket, de kutatások[5] azt mutatják, hogy a büntetések súlyosbítása nem feltétlenül fokozza az elrettentő hatást. Ezért érdekes lenne megvizsgálni a korrekciós (elkövető alapú) rehabilitációs programok hatását a magas visszaesési arány csökkentésére.

3.3 Az erőfeszítések növelése

Az ATM-ek elleni fizikai támadások megelőzésének harmadik tengelye olyan intézkedéseket tartalmaz, amelyek megnehezítik a tettesek számára a bűntény elkövetését.

A bűnözésnek ellenálló környezet biztosítása

Ha a kockázatértékelés (lásd fent) azt mutatja, hogy egy ATM magas kockázatú környezetben található, az automatát le kell szerelni, és áthelyezni egy alacsony vagy közepes kockázatú területre. Olyan esetben biztosan ezt kell tenni, amikor az elemzés azt mutatja, hogy az épület összedőlhet, ha az ATM-et robbanóanyaggal támadják meg. A magas kockázatú esetekben az ilyen intézkedések érvényesítésére jogszabályokat lehet bevezetni. A magas kockázatú területeken lévő ATM-ek számának csökkentése mellett a készpénz nélküli fizetések lebonyolítását kell ösztönözni, hogy az ATM-ek iránti igény csökkenjen.

Ha az ATM áthelyezése nem lehetséges, a legmagasabb fokú biztonsági intézkedéseket kell bevezetni: pl. a kirántást megakadályozó cölöpöket, az épülethez való hozzáférést akadályozó lámpaoszlopokat vagy egyéb utcai bútorokat, járműleállító-rendszereket kell alkalmazni, illetve megfelelő utcai világítást, nyílt vagy rejtett megfigyelőrendszert és lopásgátló eszközöket (pl. bankjegy-érvénytelenítő rendszereket) kell elhelyezni. Amikor nem magas kockázatba sorolt helyen lévő ATM-et támadnak meg, ezt a helyet is ide kell sorolni, és extra biztonsági intézkedéseket kell alkalmazni. Az új tényezőket figyelembe kell venni a kockázatértékelés frissítésekor. A kockázatok újraértékelését rendszeresen el kell végezni.

Az ATM-ek megerősítése

Az ATM-gyártók az Európai Szabványügyi Bizottság (CEN) biztonsági minősítése szerint besorolt biztonsági funkciókkal rendelkező ATM-ek standard választékát kínálják. Általában az ATM-ek CEN1-től CEN14-ig terjedő CEN-jelzéssel vannak ellátva. A minősítést az automata felépítésének erőssége és a támadásokkal szembeni ellenállása határozza meg. A gázokkal szembeni ellenállás a legtöbb esetben opcionálisan választható elem (CEN-GAS). A standard modellek általában további védelmi elemekkel egészíthetők ki. Ezeket a funkciókat általában harmadik felek szerelik be, akik biztosítják a helyi jogszabályi előírásoknak való megfelelést, és az alapmodellnek a helyi ügyfelek igényei szerinti beállítását. Az extra biztonsági funkciók közé tartozhatnak a különböző érzékelők, amelyek egy gázsemlegesítő rendszert aktiválnak, illetve egy *in situ* vagy robbantásos támadás esetén az IBNS, valamint a megerősített pénzkiadó nyílások és széfzárak a trezorhoz való jogosulatlan hozzáférés megakadályozására, amikor a fő nyílást manipulálták. A szállítható, önállóan álló ATM-ek esetében fontos az olyan rögzítőrendszerek használata, amelyek extra védelmet nyújtanak a kirántásos támadások ellen. Az ATM-eket nyomkövető rendszerekkel is felszerelhetik, amelyek olyan esetekben segíthetik a nyomozást, amikor az ATM-et a kinyitás előtt más helyre viszik.

Építészeti intézkedések

Egy ATM telepítésekor javasolt olyan automatát választani, amelyhez hátulról lehet hozzáférni, mert ilyen esetben az elkövetőnek be kell lépnie az épületbe, és hozzá kell férnie a gép hátuljához, hogy ellophassa a pénzt. A szállítható, önállóan álló ATM-ek a leginkább sebezhetők, ezért az ilyen típusú ATM-ek számának csökkentésével a biztonság növekedne. Sőt, ha az ATM-eket csak betörésbiztos helyiségekben lehetne elhelyezni, az önállóan álló ATM-ek használata automatikusan csökkenne.

Ködképző rendszer

A ködágyú gyorsan sűrű ködöt borítja be a helyiséget, amitől a behatoló nem lát semmit, így a biztonsági köd gyakran ellehetetleníti az ATM-támadás végrehajtását. Végső esetben a rendszer lelassítja az elkövetőt, így a rendőrségnek több ideje marad beavatkozni. Ez a biztonsági ködképző rendszer össze van kötve a riasztórendszerrel, és kétféleképpen aktiválható. Vagy automatikusan aktiválódik riasztóérzékelők – például mozgásérzékelők (éjszaka) vagy az ATM pénzkiadó nyílásának manipulálását észlelő érzékelők – hatására. Vagy a hamis riasztások elkerülése érdekében egy riasztóközpont aktiválja őket. A falba épített, kültéri ATM-ek esetén a ködképző rendszer az ATM hátulján alkalmazható, vagyis az automata mögötti helyiséget borítja be ködöt, és csökkenti nullára az elkövető látótávolságát.

A ködképző rendszerek „egypontos" védelmet biztosíthatnak a nyitott térben, pl. benzinkutakon, szupermarketeknél lévő ATM-ek esetén, amivel elkerülhető a létesítmény teljes területének ködöt való beborítása. A ködöt biztosított védelem akkor igazán sikeres, amikor a köd különböző szögekből árad, vagy amikor teljesen megtölti az ATM mögötti teret egy

kirántásos támadás esetén. Vizsgálatok folynak arra vonatkozóan, hogy a ködágyúkat az ATM-nek helyet adó helyiség helyett be lehet-e szerelni magába az ATM-be. A ködhöz DNS-jelölőket is hozzá lehet adni, amelyek megjelölik az elkövetőket és ruháikat.

3.4 Párhuzamos intézkedések

A fent említett megelőző intézkedések eredményes és hatékony megvalósítása érdekében számos párhuzamos intézkedést is fontolóra kell venni. Ezek az intézkedések elengedhetetlenül szükségesek az ATM-ek elleni fizikai támadások kezelését célzó holisztikus megelőző és operatív megközelítések lehetővé tételéhez és megerősítéséhez.

Jogszabályi környezet

A jogszabályok számos országban arra kötelezik az ATM-szolgáltatókat, hogy gondoskodjanak megelőző intézkedésekről. Más országokban a bankok és bűnüldöző ügynökségek közötti egyezségek és megállapodások biztosítanak jól működő megközelítést az ATM-ek elleni fizikai támadásokra vonatkozóan. Többek között az alábbi területekre vonatkozóan érdemes megfontolni a szabályozási intézkedéseket:

- megelőző intézkedések beépítése;
- a bűnüldöző szervek, valamint a magán- és a közszférában dolgozó partnerek közötti együttműködést lehetővé tévő jogi keretrendszerek;
- a büntetések átdolgozása, ha az ATM-ek elleni fizikai támadások elkövetői túl enyhe büntetéseket kapnak.

Azonban a törvények vagy megállapodások gyakran csak a bankokra vonatkozóan fogalmaznak meg kötelezettségeket, a független ATM-szolgáltatókra ezek nem érvényesek. Ez egy gyakori gyenge pont a jogi keretrendszerekben.

Egyes országok semmilyen jogszabályt nem vezetnek be, csak az ATM-szolgáltatókat próbálják meggyőzni a megelőző intézkedések alkalmazásáról azáltal, hogy felhívják a figyelmüket a bűnözési területekre és trendekre: a sok független bankkal rendelkező országokban ez kifejezetten nehéznek bizonyul.

Feltétlenül szükséges gondoskodni arról, hogy a megelőző intézkedések hatékony megvalósításába beletartozzon a jogszabályok és rendeletek módosítása is mind nemzeti, mind pedig nemzetközi szinten, ami kötelező érvényű az ATM-szolgáltatók összes típusára. Ideális esetben a jogszabályokat EU-s szinten kell egymáshoz igazítani, hogy elkerülhető legyen a bűnszervezetek átáramlása a jogszabályaikkal erős megelőző intézkedéseket alkalmazó országokból az enyhébben szabályozott államokba.

Médiastratégia

A megelőző stratégia egy másik fontos tengelye az alaposan kidolgozott médiastratégia, ami a

várakozásokat és az ATM-eket megtámadók ilyen típusú bűncselekmények elkövetése iránti vágyát is csökkenti. Az alacsony sikerességi arányt és az elkövetőket érintő magas kockázatokat kell hangsúlyozni; a jutalmakról („zsákmányról") vagy az ATM elleni támadás részleteiről – például az érintett ATM típusáról –, vagy a megakadályozott elkövetési módszerről pedig közleményeket kell kiadni. Másrészről a gyanúsítottak letartóztatásáról és az elítélésük utáni büntetéséről szóló híreket széles körben nyilvánosságra kell hozni.

Fokozott együttműködés

A fokozott együttműködésről és az információcseréről már sok szó esett, de ezek fontosságát nem lehet eléggé hangsúlyozni. A nemzetközi szintű operatív információcsere az Europol tevékenységének központi eleme. A megelőzés témájában megtartott konferencián az információcsere fontossága mellett az is világosan kiderült, hogy multidiszciplináris és többszintű együttműködésre és információmegosztásra van szükség az összes releváns szereplő között, ideértve a bűnüldöző ügynökségeket, a közhatóságokat, az ATM-ek, valamint a biztonsági és védelmi eszközök gyártóit, a szakmai szervezeteket, az ATM-szolgáltatókat (bankok és független szolgáltatók), a biztonsági cégeket és a riasztóközpontokat. Mindennek helyi, nemzeti és nemzetközi szinten is meg kell valósulnia.

A járulékos károk kockázatának csökkentése

A szilárd robbanóanyaggal elkövetett támadások esetén a bűnszervezetek után maradék anyag maradhat, ami veszélyes helyzetet teremthet az elsőként beavatkozók vagy (a közelben lakó vagy járókelő) állampolgárok számára. Ezért gondoskodni kell az ő biztonságukról. Belgium esetéhez hasonlóan ki kell dolgozni az elsőként beavatkozók (mind a bűnüldözői, mind az ATM-szolgáltatói oldalról) által követendő protokollokat és eljárásokat, és ezeket össze kell hangolni egymással. Ebben az összefüggésben egy másik bevált gyakorlat Hollandia példája, ahol az ATM elleni támadásról készült CCTV-felvételt használják a helyzet felmérésére. Az ilyen képek azonnali elérhetővé tétele érdekében megállapodásokat kell kötni a riasztóközpontokkal.

Szociális megelőzés

A bűnszervezetek gyakran fiatal embereket keresnek és vesznek fel tagjaik közé. Ezért olyan projekteket kell megvalósítani, amelyek ezeket a felvételi folyamatokat már egy korai szakaszban meghiúsítják. A rendőrségnek vagy szociális munkásoknak oda kell figyelniük ezekre a folyamatokra, és be kellene avatkozniuk az elkövetők személyes megkeresése révén.

04 KÖVETKEZTETÉSEK

Az utóbbi két évben az ATM-ek elleni fizikai támadásokat elszenvedő európai országok száma nőtt. Ebben a vonatkozásban az Europol és az EUCPN közös munkával gyűjtötte össze az ilyen típusú bűncselekmények megelőzését és az ellenük való küzdelmet szolgáló legjobb intézkedéseket.

Az ATM-ek elleni fizikai támadások megakadályozását célzó sikeres megközelítés operatív és megelőző intézkedések összességéből áll. Annak elkerülésére, hogy az erősebb intézkedéseket alkalmazó országok bűnszervezetei másik, sebezhetőbb országokba tegyék át székhelyüket, ajánlott ezeket az intézkedéseket európai szinten elfogadni.

Az ilyen típusú bűncselekmények megelőzése és az ellenük való küzdelem érdekében világos stratégiát kell kidolgozni három lépésben: a helyzet felmérése, a kockázatértékelésen alapuló megelőző megközelítés kidolgozása, és a megelőző intézkedések megvalósítása.

Az ATM-ek elleni fizikai támadások kockázatértékelésének tartalmaznia kell az ATM és környezete jellemzőit, a partnerek és szereplők közötti, az ilyen típusú bűncselekmények elleni küzdelmet célzó szövetségek létrehozására irányuló együttműködéseket, valamint a megelőzési és jogi keretrendszer értékelését is. A helyzet felmérését követően a köz- és a magánszféra együttműködésére épülő stratégiát, valamint megelőző és operatív ellenintézkedéseket kell kidolgozni. A megelőző intézkedések célja az elkövetők ATM-ek elleni fizikai támadásra irányuló szándékának és adottságainak mérséklése. Ennek elérése érdekében a megelőző intézkedések vonatkozásában három tengelyt javaslunk: a jutalmak csökkentése, a kockázat növelése, valamint az erőfeszítések növelése. A megelőző stratégiát párhuzamos intézkedésekkel kell kiegészíteni. A legjobb gyakorlat egy olyan nemzeti hatóság felállítása, amely megfelelő hatáskörrel bír a szükséges intézkedések betartatásához.

A **jutalmak csökkentésével,** a bűnözők ilyen típusú bűncselekmények elkövetése iránti vágya is csökken. Az ATM-ekben lévő készpénzmennyiség csökkentése az újratöltött pénz mennyiségének korlátozásával annyira, hogy 1 napi kereskedésre legyen elegendő, vagy a (leginkább sebezhető) ATM-ek éjszakai kiürítésével olyan intézkedés, ami csökkenti a bűnözők várakozásait. Egy másik módszer a zsákmány tönkretétele és a pénz nyomon követhetőségének megoldása. Ilyen célra az IBNS alkalmazható, ami megjelöli a bankjegyeket, és jelzi, hogy lopottak. Ez a módszer akkor a leghatékonyabb, amikor lehetetlenné válik a bűnözők számára a pénz elköltése vagy visszaforgatása a legális pénzrendszerbe. Ez úgy érhető el, ha a bankok és az emberek nem fogadnak el megjelölt bankjegyeket, illetve bankjegykezelő berendezések telepítésével, amelyek észlelik és visszautasítják a megjelölt bankjegyeket. Ebből a szempontból az infravörös jelölővel megjelölt bankjegyeket észlelő infravörös rendszerekbe való beruházás bizonyult költséghatékony megoldásnak Belgiumban és Franciaországban. IBNS telepítésekor az országoknak alaposan meg kell fontolniuk, hogy melyik aktiváló mechanizmust választják, mik legyenek a bankjegyek érvénytelenítésének minimumkövetelményei és hogy adnak-e törvényszéki jelölőt a tintához.

Azok az intézkedések, amelyek a lelepleződés és a büntetés **kockázatának növelésével** rettentik el a potenciális elkövetőket a bűntények elkövetésétől, képezik az ATM-ek elleni fizikai támadások megelőzésének második tengelyét. Az ATM-ek elleni

támadások leleplezésének és megbüntetésének kulcseleme az információgyűjtés és -megosztás a szereplők között, mind nemzeti, mind nemzetközi szinten. A jó minőségű CCTV-képek és hanganyagok megosztása növelheti a korai észlelés esélyét és a sikeres nyomozást. Annak elkerülésére, hogy a CCTV-ket vagy a lehallgatóeszközöket kikapcsolják a támadás előtt, a láthatatlan CCTV-k vagy valós idejű lehallgatókészülékek telepítése lehet a megoldás. Egy törvényszéki adatbázis létrehozása, és a technológiák európai szintű standardizálása nagyban segítené a nemzetközi együttműködést és a nyomozásokat. Ha a tetteseket elkapják és elítélik, érdekes lehet megvizsgálni a korrekciós (elkövető alapú) rehabilitációs programok hatását a magas visszaesési arány csökkentésére.

Az ATM-ek elleni fizikai támadások megelőzésének harmadik tengelyébe a bűncselekmény elkövetéséhez szükséges **erőfeszítéseket növelő** intézkedések tartoznak. Ha egy ATM-et a bűnözésnek ellenálló környezetbe, maximális biztonsági intézkedések mellett telepítenek, a tetteseknek nehezebb feladat lesz az ATM megtámadása. Sőt, az ATM-ek általános védelmét további kiegészítő biztonsági funkciókkal lehet fokozni. A fenti intézkedéseken túl a ködképző rendszerek telepítése is elrettentheti az elkövetőket, vagy legalábbis lelassíthatja támadás elkövetését.

A fent említett intézkedéseket számos **párhuzamos intézkedés** is erősítheti. Ilyen lehet például egy olyan jogi keretrendszer kialakítása, amely a megelőző intézkedések bevezetésére kötelezi az ATM-szolgáltatókat; egy jól felépített médiastratégia kidolgozása; a fokozott együttműködés helyi, nemzeti és nemzetközi szinten; iránymutatás az elsőként beavatkozók számára azért, hogy csökkenteni lehessen a járulékos károk mértékét; valamint a befektetés a szociális megelőzésbe, ami aláássa a bűnözésbe való bevonás folyamatait.

Factsheet

A MEGELŐZŐ MEGKÖZELÍTÉSRE VONATKOZÓ AJÁNLÁSOK: ÁTTEKINTÉS

Hatékony válasz kidolgozása az ATM-ek elleni fizikai támadások ellen

A helyzet felmérése

> Az országban/régióban található ATM-ek kockázati profiljának meghatározása

> Partnerek és szereplők beazonosítása az ATM-ek fizikai megtámadása elleni küzdelemben, és az együttműködés értékelése

> Az ATM-ek fizikai megtámadása elleni küzdelemre vonatkozó jogi keretrendszer értékelése nemzeti és nemzetközi szinten

Megelőző megközelítés kidolgozása

> A kezelendő (fő) kockázatok és fontossági sorrendjük meghatározása

> Az ezen kockázatok kezelésére leginkább alkalmas megelőző intézkedések meghatározása a három tengely figyelembevételével

> A kiválasztott megelőző intézkedések megerősítéséhez szükséges párhuzamos megelőző intézkedések meghatározása

Az alábbi célok érdekében alkalmazható megelőző intézkedések:

01

A jutalmak csökkentése

> A készpénzmennyiség csökkentése.
  - Az ATM kiürítése éjszakára.
  - Az újratöltések számának/gyakoriságának növelése.
> A zsákmány tönkretétele.
  - Intelligens bankjegy-érvénytelenítő rendszerek (IBNS).
  - Infravörös jelölők az IBNS-tintában, amit a bankjegykezelő berendezések észlelni tudnak a megjelölt bankjegyeken.
  - Fejlesztés alatt: ragasztó.

02

A kockázat növelése

> Határokon átnyúló információmegosztás a következők érdekében:
  - egy lehetséges ATM-elleni támadás korai vagy valós idejű észlelése,
  - az operatív megközelítés megerősítése,
  - a visszaesők elítélése,
  - a törvényszéki adatok európai szintű megosztása.
> CCTV és lehallgatóeszközök.
> Büntetés és az elkövetők rehabilitációja.

03

Az erőfeszítések növelése

> A bűnözésnek ellenálló környezet biztosítása.
  - A magas kockázatú ATM-ek áthelyezése.
  - Biztonsági intézkedések: fizikai akadályok, megfigyelés stb.
> Az ATM-ek megerősítése pl. a gáz vagy szilárd robbanóanyagoknak ellenálló nyílásokkal
> Építészeti intézkedések, például olyan automaták, amelyekhez hátulról lehet hozzáférni
> Biztonsági ködképző rendszerek.

Párhuzamos intézkedések a megelőző megközelítés megerősítésére

> Hatékony jogszabályok, amelyek tartalmazzák az ATM-ek fizikai megtámadása elleni megelőző intézkedéseket, a büntetéseket stb.

> Hatékony, az elkövetőket elbátortalanító médiastratégia.

> A szereplők (közszféra, magánszféra, bűnüldözés) közötti fokozott együttműködés az ATM-ek fizikai megtámadása ellen.

> Az elsőként beavatkozók vagy civilek (pl. a közelben lakók vagy járókelők) járulékos káraira vonatkozó kockázatok csökkentése.

> A szociális megelőzés annak megakadályozására, hogy fiatalokat béreljenek fel (az ilyen típusú) bűntények elkövetésére.

ENDNOTES

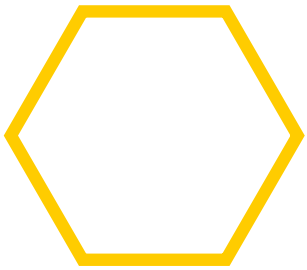
1 Willem Pieter de Groen, Zachary Kilhoffer és Roberto Musmeci, *The future of EU ATM markets: impacts of digitalisation and pricing policies on business models* [Az EU ATM-piacok jövője: a digitalizáció és árpolitikák hatásai az üzleti modellekre], CEPS-jelentés, 2018

2 Derek Cornish és Ronald V. Clarke, 'Opportunities, precipitators and criminal decisions: a reply to Wortley's critique of situational crime prevention' [Lehetőségek, kiváltó okok és bűnözői döntések: válasz a helyzeti bűnmegelőzésre vonatkozóan Wortley által megfogalmazott kritikára], *Crime prevention Studies* 16 (2003), 41-96.

3 Centrum voor Criminaliteitspreventie, barrieremodellen [Bűnmegelőzési és Biztonsági Központ, korlátmodellek], www.barrieremodellen.nl

4 Európai Központi Bank, az Európai Központi Bank döntése, The denominations, specifications, reproduction, exchange and withdrawal of euro banknotes [Az euróbankjegyek címletei, specifikációi, sokszorosítása, cseréje és visszavonása], 2003.

5 David Weisburd, David P. Farrington és Charlotte Gill, 'Conclusion: What Works in Crime Prevention Revisited' [Következtetés: A bűnmegelőzés működőképes elemeinek felülvizsgálata], David Weisburd, David P. Farrington és Charlotte Gill, *What works in Crime Prevention and Rehabilitation* [A bűnmegelőzés és a rehabilitáció működőképes elemei]. 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