Verhinderung physischer Angriffe auf Geldautomaten

Entwicklung eines effektiven Ansatzes

Danksagungen
Dieses Dokument ist das Ergebnis einer Zusammenarbeit zwischen der Agentur der EU für die Zusammenarbeit der Strafverfolgungsbehörden (Europol) und dem Sekretariat des Europäischen Netzes für Kriminalprävention (EUCPN). Wir möchten den Experten für physische Angriffe auf Geldautomaten danken, die Zeit und Mühe investiert haben, um die Erstellung dieses Empfehlungspapiers zu unterstützen. Sie leisteten einen Beitrag, indem sie an der Konferenz über die Verhinderung von physischen Angriffen auf Geldautomaten (Januar 2019, Brüssel) teilnahmen und wichtige Informationen zur Verfügung stellten. Unser besonderer Dank gilt den Strafverfolgungsbehörden aus EU- und Nicht-EU-Ländern („Drittländern"), dem Privatsektor einschließlich der ATM Industry Association (ATMIA), BPost, Centrum voor Criminaliteitspreventie en Veiligheid (CCV), Diebold Nixdorf, der European Association for Secure Transactions Expert Group on ATM and [automatic teller safes] ATS Physical Attacks (EAST EGAP), der European Intelligent Cash Protection Association (Euricpa), ING, Febelfin, NCR, Protect, SIOC Banking, Spinnaker, TMD Security und den Innenministerien von Belgien, Kroatien, Deutschland und Spanien.

Rechtlicher Hinweis
Der Inhalt dieser Veröffentlichung spiegelt nicht notwendigerweise die offizielle Meinung eines EU-Mitgliedstaates oder einer Behörde oder Institution der EU oder der Europäischen Gemeinschaft wider.

Inhalt

1 Kontext 4
2 Faktoren, die den Erfolg eines physischen Angriffs auf einen Geldautomaten bestimmen 5
2.1 Verwundbarkeit von Geldautomaten 5
2.2 Vorgehensweise bei einem Angriff auf einen Geldautomaten 6
2.3 Erfahrung und Know-how der Täter 6
3 Notwendigkeit eines präventiven Ansatzes 8
4 Prävention 9
4.1 Beurteilung der Situation 9
4.2 Entwicklung eines präventiven Ansatzes 10
4.3 Umsetzung von Präventivmaßnahmen 12
4.3.1 Verringerung der Lukrativität 12
4.3.2 Erhöhung der Risiken 15
4.3.3 Erhöhung des Aufwands 18
4.3.4 Parallele Maßnahmen 20
5 Schlussfolgerungen 23
6 Empfehlungen für einen präventiven Ansatz: Übersicht 26

1 Kontext

Angesichts der steigenden Zahl von physischen Angriffen auf Geldautomaten und der zunehmenden Zahl der betroffenen europäischen Länder organisierten das Europäische Netz für Kriminalprävention (EUCPN) und Europol eine Konferenz (Januar 2019), die Strafverfolgungsbehörden mit öffentlichen und privaten Partnern zusammenbrachte, um sich mit der Prävention dieses Verbrechens zu befassen. Dieses Empfehlungspapier fasst die Schlussfolgerungen dieser Konferenz zur Sensibilisierung der Behörden für physische Angriffe auf Geldautomaten und Präventivmaßnahmen zusammen.

Die Fülle unterschiedlicher Methoden (*modi operandi* (MO)), die Kriminelle bei Angriffen auf Geldautomaten anwenden, lässt sich in zwei Hauptkategorien einteilen: physische Geldautomatenangriffe und Betrugsangriffe im Zusammenhang mit Geldautomaten (dazu gehören Logikangriffe auf Geldautomaten und Malware). In diesem Papier geht es um physische Angriffe auf Geldautomaten: das erzwungene Eindringen mit physischen Mitteln in Geldautomaten, um ihnen ihr Bargeld zu entnehmen. Erzwungenes Eindringen kann erreicht werden durch:

- Verwendung von Sprengstoffen: Angreifer verwenden Gas oder feste Explosivstoffe, um den Geldautomatentresor physisch zu knacken und Zugang zum Bargeld zu erhalten;
- Rip-Out-/Ram-Raid-Angriffe: Die Angreifer entfernen den Geldautomaten physisch aus der Installationsumgebung, oft unter Verwendung eines High-End-Fahrzeugs;
- In-situ-Angriffe: Angreifer öffnen den Tresor mit roher Gewalt, oft unter Verwendung von Schneid- oder Brechwerkzeugen wie Winkelschleifer, Vorschlaghammer oder Schneidbrenner.

In einer begrenzten, jedoch wachsenden Zahl von Ländern in der Europäischen Union stellen physische Angriffe auf Geldautomaten ein Problem dar. Für das Jahr 2017 wurde der verursachte finanzielle Schaden in Europa auf über 30 Millionen Euro geschätzt. In einigen Ländern kommt es nach wie vor zu einer beträchtlichen Anzahl physischer Angriffe auf Geldautomaten, während in anderen Ländern die Zahl dieser Vorfälle in den letzten zwei Jahren erheblich zugenommen hat. Dieser Kriminalitätsbereich entwickelt sich schnell. Einige Länder waren in ihrem Vorgehen gegen physische Angriffe auf Geldautomaten erfolgreich und verzeichneten kürzlich einen deutlichen Rückgang der Angriffe. Andererseits sahen sich bisher nicht betroffene Länder 2018 mit einem plötzlichen Anstieg physischer Angriffe auf Geldautomaten konfrontiert, da organisierte Banden ihr Territorium ausdehnten. Nicht nur Banken sind betroffen, auch Geldautomaten unabhängiger Anbieter werden zunehmend angegriffen, da sie sich häufig in anfälligeren Räumlichkeiten oder an verwundbaren Standorten befinden.

2 Faktoren, die den Erfolg eines physischen Angriffs auf einen Geldautomaten bestimmen

Die Erfolgsquote von Angriffen auf Geldautomaten ist gering; nur ein Drittel der Angriffe sind erfolgreich. Aber selbst wenn der Angriff erfolglos bleibt, ist der Schaden (z.B. durch Sprengstoff) an Gebäudestrukturen ebenso erheblich, sodass für Anwohner, Ersthelfer und Passanten in der Nähe des Tatorts eine unsichere Umgebung entsteht.

Der Erfolg eines physischen Angriffs hängt von einer Reihe von Faktoren ab, u.a. von den Merkmalen eines Geldautomaten, der Vorgehensweise beim Angriffs und der Erfahrung und dem Know-how der Täter.

2.1 Verwundbarkeit von Geldautomaten

Die am stärksten gefährdeten Geldautomaten sind diejenigen, die sich außerhalb (in die Wand eingebaut (TTW)) oder innerhalb von Gebäuden befinden. Bei Angriffen auf einen (eigenständigen) Geldautomaten in einem Gebäude bevorzugen organisierte Banden Geldautomaten, die sich in Geschäftsräumen befinden, gegenüber Geldautomaten in Bankgebäuden, wo die Überwachung in der Regel stärker ist. Banken betreiben hauptsächlich Geldautomaten, die sich innerhalb oder außerhalb eines Bankgebäudes befinden. Bankferne Standorte („bank remote“) auf der Straße oder in den Geschäftsräumen von Händlern wie Tankstellen, Supermärkten, Hotels, Kasinos, Flughäfen usw. gewinnen angesichts der Schließung von Bankfilialen allmählich an Bedeutung. Unabhängige Anbieter betreiben Geldautomaten als eigenständige Dienstleistung. Ihre Geldautomaten befinden sich häufig an Einzelhandelsstandorten, in Bewirtungsbetrieben und in Freizeiteinrichtungen, an Verkehrsstandorten (Bahnhöfe, Flughäfen usw.), in öffentlichen Gebäuden und auf der Straße.

Angesichts der zunehmenden Beliebtheit des Online-Bankings werden in den kommenden Jahren wahrscheinlich viele Bankfilialen geschlossen werden, was zu einem allgemeinen Rückgang der Zahl der Geldautomaten führen wird. ([1]) Dies könnte jedoch einen Anstieg der Zahl der bankfernen Geldautomaten und der Geldautomaten unabhängiger Anbieter an anfälligeren Standorten nach sich ziehen.

([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

2.2 Vorgehensweise bei einem Angriff auf einen Geldautomaten

Die Vorbereitung eines Angriffs kann mehreren Wochen oder gar Monate in Anspruch nehmen. Die Täter müssen die notwendigen **Werkzeuge und Ressourcen** wie Fahrzeuge, Ausrüstung und Kontaktstellen zusammentragen. **Fahrzeuge** sind ein wesentliches Mittel für physische Angriffe auf Geldautomaten; die Täter reisen hauptsächlich mit dem Auto und nach dem Angriff flüchten sie meist mit schnellen Fahrzeugen. Diese werden oft gestohlen, können aber auch gemietet oder gekauft werden (z.B. über das Internet). Die meisten **Ausrüstungsgegenstände** für physische Angriffe auf Geldautomaten sind in normalen Geschäften leicht und legal erhältlich. Dies senkt die Schwelle für den Einstieg in diesen Kriminalitätsbereich weiter. Die Rückverfolgung des Ursprungs eines Werkzeugs ist bei der Strafverfolgung schwierig, sodass die Risiken für die Täter begrenzt sind. Organisierte Banden, die auf internationaler Ebene bei physischen Angriffen auf Geldautomaten aktiv sind, verfügen fast immer über Kontaktstellen im Zielland (Personen, die sich dort für einen bestimmten Zeitraum aufhalten), oder alternativ dazu können sie sich einer Hit-An-Run-Vorgehensweise bedienen. Diese Kontakte unterstützen die organisierten Banden bei der Logistik, wie z.B. bei der Anmietung von Unterkünften, der Beschaffung eines Fahrzeugs oder anderer Ausrüstungsgegenstände sowie beim Ausspähen von Zielen. Einige internationale aktive Täter überlassen Logistik und Ausspähen vollständig den lokalen Kontakten und reisen nur zur Durchführung des Angriffs auf den Geldautomaten per Auto oder Flugzeug an.

Organisierte Banden führen oft umfangreiche **Erkundungen** durch, um geeignete Ziele zu identifizieren, die Tageszeit zu ermitteln, zu der der Geldautomat gefüllt wird, die Umgebung des Geldautomaten, die technischen Besonderheiten des Geldautomaten, die Fluchtwege und die vorhandenen Sicherheitsmaßnahmen, wie z.B. Videoüberwachung (CCTV), Alarmsensoren und Blenden.

Einige organisierte Banden ergreifen eine Reihe von Maßnahmen, um **Strafverfolgungsbehörden und Sicherheitsdienste vor dem Angriff zu behindern**. Sie manipulieren Alarmsysteme und die öffentliche Beleuchtung, verwenden Umgehungstechniken, errichten Straßensperren oder versuchen, Fahrzeugen der Strafverfolgungsbehörden zu manipulieren.

2.3 Erfahrung und Know-how der Täter

Physische Angriffe auf Geldautomaten sind für Kriminelle attraktiv, weil das Geld sofort verfügbar ist und kein umfangreiches Netzwerk für den Verkauf gestohlener Waren benötigt wird. Sie stellen eine bequeme Alternative für Kriminelle dar, die bereits im Bereich der organisierten Eigentumsdelikte aktiv sind.

Die organisierten Banden müssen das **erforderliche Fachwissen und Know-how** erwerben, da diese für den Erfolg oder Misserfolg eines Angriffs entscheidend sind. Erforderliches Fachwissen und Know-how hängen stark von der **Art des Angriffs** ab. Rip-out-/Ram-raid- und *In-situ*-Angriffe haben einen simplen MO (hauptsächlich Kühnheit und die Anwendung von roher Gewalt), sodass sie im Allgemeinen keine besonderen Fähigkeiten erfordern. Angriffe mit brennbaren Gasen und festen Sprengstoffen erfordern ein höheres Maß an Fachwissen.

Die Angreifer weisen unterschiedliche **Kompetenzniveaus** auf. Einerseits können hochgradig organisierte und erfahrene Banden innerhalb von Minuten einen erfolgreichen physischen Angriff auf einen Geldautomaten durchführen. Sie haben den Prozess unter Kontrolle und sind in der Lage, das Risiko für sich selbst und damit auch den Kollateralschaden zu begrenzen. Andererseits scheitern weniger organisierte und opportunistische Gruppen oft bei ihren Versuchen und können den Räumlichkeiten und Gebäuden in der Nachbarschaft erheblichen Schaden zufügen. Man geht davon aus, dass einige der weniger gut organisierten Banden zu den traditionellen Aktivitäten organisierter Eigentumskriminalität zurückkehren werden, entmutigt durch die Präventivmaßnahmen, die sie bei Angriffen auf Geldautomaten nicht überwinden können.

3 Notwendigkeit eines präventiven Ansatzes

Länder, in denen die Täter geringe Erfolgsraten bei physischen Angriffen auf Geldautomaten haben oder in denen die Zahl der physischen Angriffe auf Geldautomaten abnimmt, zeigen, dass ein erfolgreicher Ansatz zur Abwehr physischer Angriffe auf Geldautomaten aus einer Kombination von operativen und präventiven Maßnahmen besteht. Da die Zahl der in diesem Kriminalitätsbereich tätigen organisierten Banden begrenzt ist, wird die Zahl der Angriffe durch Verhaftungen und die daraus folgende Bestrafung von Mitgliedern organisierter Banden erheblich reduziert. Viele Geldautomatenangreifer nehmen jedoch ihre Aktivitäten wieder auf, sobald sie freigelassen sind. Außerdem kann eine Gruppe den verhafteten Täter manchmal schnell ersetzen. Daher besteht ein großer Bedarf an präventiven Maßnahmen, vorzugsweise in einen gesetzlichen Rahmen eingebettet. Darüber hinaus zeigt die Erfahrung, dass Präventionsmaßnahmen in einem Land organisierte Banden auf anfälligere Ziele in anderen Ländern lenken können. Es ist nur eine Frage der Zeit, bis sich die in einem Land entstehenden MO auf andere Länder ausbreiten. Dies zeigt deutlich die **Notwendigkeit der Einführung präventiver und operativer Maßnahmen auf europäischer Ebene**, wobei private, öffentliche und Strafverfolgungspartner eng zusammenarbeiten.

4 Prävention

Um diese Art von Kriminalität zu verhindern und zu bekämpfen, ist eine klare Strategie erforderlich. In diesem Kapitel werden wir einen Überblick über die drei Schritte geben, die im Allgemeinen unternommen werden, wenn man mit physischen Angriffen auf Geldautomaten konfrontiert wird oder sich auf deren Prävention vorbereitet.

Zunächst die **Beurteilung der Situation**: Es sollte ein Risikoprofil der Geldautomaten und ihrer Umgebung erstellt werden, das die Menge des verfügbaren Bargeldes (mögliche Beute), das Risiko von Kollateralschäden und das Risiko von Personenschäden berücksichtigt. Zweitens sollte auf der Grundlage der **Risikobewertung** eine Präventionsstrategie entwickelt werden. Zuletzt müssen die **präventiven Maßnahmen** umgesetzt werden.

4.1 Beurteilung der Situation

Organisierte Banden tendieren dazu, entweder bestimmte Arten von Geldautomaten oder Geldautomaten bestimmter Anbieter mit Merkmalen, die den Angriff erleichtern, ins Visier zu nehmen. Daher ist es notwendig, eine gründliche Bewertung des Risikos physischer Geldautomatenangriffe durchzuführen, vorzugsweise unter Einbeziehung der gesamten Bargeld-Sicherheitskette vom Transit über die Lieferung bis zur Lagerung im Geldautomaten. Um das Risikoprofil jedes Geldautomaten zu ermitteln, muss eine Reihe von Elementen analysiert werden, darunter die folgenden.

- Merkmale des Standortes und der Umgebung des Geldautomaten; Merkmale wie städtische oder ländliche Lage, Bevölkerungsdichte, Nähe von Polizeistationen, Kameras mit automatischer Kennzeichenerkennung in der Nachbarschaft, Videoüberwachung in der Umgebung usw.
- Der Standort des Geldautomaten:
    - innerhalb oder außerhalb eines Gebäudes, in einer Bankfiliale oder ausgelagert (z.B. in Gewerbegebäuden), eingebaut oder an einem Gebäude angebracht,
    - bei isoliert stehenden Geldautomaten: Ist der Automat verankert oder nicht,
    - bei Geldautomaten, die in ein Gebäude eingebaut oder an einem Gebäude angebracht sind: Gibt es architektonische Schwachstellen, wie ist die Bargeldlagerung organisiert usw.
- Der Typ des Geldautomaten.
- Die im Geldautomaten enthaltenen Sicherheitsfunktionen.

- Die Bargeldmenge im Geldautomaten.
- Die Art der zu erwartenden physischen Angriffe auf Geldautomaten und die zu erwartende Vorgehensweise, um zuerst die am besten geeigneten Präventivmaßnahmen zu ergreifen.
- Die bereits getroffenen Sicherheits- und Präventivmaßnahmen (intelligente Banknoten-Neutralisationssysteme (IBNS), Videoüberwachung, Sicherheitsnebelanlage (Verringerung der Sicht) usw.).

Weitere zu evaluierende Elemente sind der Stand der Zusammenarbeit mit Partnern und Interessenvertretern sowie die Gesetzgebung. Die Zusammenarbeit zwischen Strafverfolgungsbehörden, privaten und öffentlichen Partnern sollte evaluiert werden, um Allianzen zur Verbrechensbekämpfung aufzubauen. Möglicherweise verfügt jeder Partner über interessante Informationen, die zur Beurteilung der Situation beitragen können. Lokale Polizei oder lokale Behörden sind in diesem Rahmen besonders wichtig. Die Gesetzgebung muss hinsichtlich der Schaffung eines rechtlichen Rahmens für die Prävention, das Ergreifen verbindlicher Präventivmaßnahmen, das Strafmaß für Angriffe auf Geldautomaten usw. bewertet werden.

4.2 Entwicklung eines präventiven Ansatzes

Nachdem die Lage beurteilt und die Hauptrisikobereiche sowie die Stärken und Schwächen der Geldautomatensicherheit bestimmt wurden, kann eine Strategie entwickelt werden (häufig auf der Grundlage einer öffentlich-privaten Zusammenarbeit), und es können präventive und operative Gegenmaßnahmen ergriffen werden. Präventionsmaßnahmen sollten der Verringerung der Absicht und der Fähigkeiten der Täter dienen. Um dies zu erreichen, werden drei Achsen präventiver Maßnahmen vorgeschlagen, die auf drei von fünf Strategien der situativen Kriminalitätsprävention von Clarke ([2]) basieren: Reduzierung der Attraktivität, Erhöhung des Risikos für die Täter und Erhöhung des Aufwandes beim Zugang zur Beute.

Kriminelle bilanzieren die zu erwartende Rendite und die damit verbundenen Risiken (z.B. bei einem Geldautomatenangriff). Die Verringerung der Chancen auf leichte Beute und die Erhöhung des Risikos für die Täter hemmt ihre Erwartungen und ihren Wunsch, einen physischen Geldautomatenangriff durchzuführen. Weitere Maßnahmen, die den Aufwand für den Zugang zum Geldautomaten erhöhen, wirken sich auf die Fähigkeiten der Täter aus. Opportunistische Täter, die

([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.

bei ihren Versuchen oft scheitern, hören auf, sich an Geldautomatenangriffen zu beteiligen. Bei professionellen Geldautomatenangreifern verringert sich die Erfolgsquote, was sich wiederum auf das Verhältnisse zwischen Rendite und Risiko auswirkt.

Darüber hinaus vervollständigen parallele Maßnahmen wie eine wirksame Medienstrategie, frühzeitige soziale Prävention und Maßnahmen zur Verringerung des Risikos von Kollateralschäden an Gebäuden und zur Gewährleistung der Sicherheit von Anwohnern, Ersthelfern und Passanten die Präventionsstrategie.

Weitere Methoden zur Strukturierung des Ansatzes sind möglich. In den Niederlanden wenden die Behörden das so genannte Barrierenmodell ([3]) an. Dieses Modell identifiziert die Schritte, die ein Krimineller unternehmen muss, um ein Verbrechen zu begehen. Es zeigt auch die Partner und die Gelegenheiten auf, die die Straftat ermöglichen, und ist ein nützliches Instrument, um den Prozess der Informationsbeschaffung über den Kriminalitätsbereich zu organisieren. Durch Identifizierung der einzelnen Schritte, die zur Durchführung eines physischen Geldautomatenangriffs erforderlich sind, können die Barrieren, die das Verbrechen behindern, und die besten Partner zur Errichtung dieser Barrieren ermittelt werden. Das Barrierenmodell identifiziert auch Signale, um die öffentlichen und privaten Partner vor physischen Geldautomatenangriffen zu warnen, sowie Signale, die sie selbst aussenden können, um die Behörden über ihren Verdacht zu informieren.

Eine gut entwickelte Strategie ist notwendig, um die Risiken zu mindern, die mit der Stärkung der Prävention einhergehen. Präventivmaßnahmen, die bei der Abschreckung von Amateuren und Nachahmern sehr wirksam sind, haben manchmal unerwünschte Auswirkungen. Einige Gruppen wenden Trial-and-Error-Methoden an, um verwundbare Geldautomaten aufzuspüren, wobei sie eine Spur von beschädigten Geldautomaten hinterlassen. Gefährlichere und skrupellosere organisierte Banden beginnen, bei ihren Angriffen gewaltsamere Mittel anzuwenden, indem sie etwa von Gas zu festen Sprengstoffen wechseln.

Um ein effizientes Paket von Präventivmaßnahmen zu schnüren, ist die Einrichtung einer nationalen Behörde, die befugt ist, auf der Grundlage einer gründlichen Analyse der Situation spezifische Maßnahmen für gefährdete Geldautomaten vorzuschreiben, die beste Praxis. Dieser Ansatz hat sich in Frankreich als wirksam erwiesen, insbesondere, wenn ein rechtlicher Rahmen geschaffen wird und die Maßnahmen zusammen mit operativen Maßnahmen umgesetzt werden.

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

4.3 Umsetzung von Präventivmaßnahmen

Die in diesem Kapitel vorgestellten Maßnahmen zur Verhinderung physischer Geldautomatenangriffe haben sich in verschiedenen Ländern als wirksam erwiesen. Sie basieren auf den Schlussfolgerungen der Präventionskonferenz und auf Präventivmaßnahmen, die von internationalen Organisationen, die im Bereich der Sicherheit von Geldautomaten tätig sind, aktiv gefördert werden. Viele Maßnahmen sind gut bekannt. Mehrere Länder haben bereits eine Reihe von Maßnahmen erfolgreich umgesetzt. Oft werden die vorgeschlagenen Maßnahmen jedoch nur teilweise umgesetzt und nicht in die Gesetzgebung eingebettet.

Wie bereits erwähnt, werden drei Achsen von Präventivmaßnahmen vorgeschlagen: Verringerung der Lukrativität, Erhöhung des Risikos für die Täter und Erhöhung des Aufwands, der erforderlich ist, um an die Beute zu gelangen.

4.3.1 Verringerung der Lukrativität

Die Verringerung der Lukrativität krimineller Handlungen ist die erste Achse bei der Verhinderung physischer Geldautomatenangriffe. Solange die Vorstellung von „schnellem Geld“ fortbesteht, werden sich Kriminelle auf derartige Verbrechen einlassen. Wenn man die Menge des verfügbaren Bargeldes verringert und das Bargeld entweder entfernt oder vernichtet, verringert man die Möglichkeiten der Verfügbarkeit lohnenswerter Beute. Geringere Erwartungen verringern den Wunsch des Kriminellen, sich auf derartige Verbrechen einzulassen.

4.3.1.1 *Verringerung der Bargeldmenge*

Eine Maßnahme zur Verringerung der Lukrativität ist die Reduzierung der in einem Geldautomaten verfügbaren Bargeldmenge. Im Idealfall sollte dieser Betrag auf die für einen Handelstag notwendige Menge beschränkt werden. Die Zusammenarbeit zwischen Banken könnte die Kosteneffizienz gewährleisten. In den Niederlanden baute eine Reihe von Banken gemeinsam ein bankenunabhängiges Netz von Geldautomaten namens „Geldmaat“ auf. Ziel der Zusammenarbeit ist es, die Verfügbarkeit, Zugänglichkeit, Erschwinglichkeit und Sicherheit von Bargeld zu gewährleisten. Dies wird wahrscheinlich zu einer Verringerung der Zahl der Geldautomaten führen. Jeder

Geldautomat wird jedoch nicht mehr Bargeld enthalten, sondern öfter aufgefüllt werden. Die Häufigkeit der Auffüllungen wird dem Bedarf angepasst.

Da Täter die Geldautomaten meist zwischen 03.00 und 04.00 Uhr angreifen, wird dringend empfohlen, bei freistehenden Geldautomaten (meist in gewerblichen und öffentlichen Räumlichkeiten, die anfälliger sind), den Geldautomaten zu leeren und das Bargeld am Ende des Tages in einem Tresor zu lagern. Ein Warnhinweis kann die Öffentlichkeit darüber informieren, dass der Geldautomat nachts kein Bargeld enthält. Am nächsten Tag sollte der Geldautomat für Kunden unsichtbar und bei verschlossenen Räumlichkeiten wieder aufgefüllt werden. Dieses System wird in Frankreich umgesetzt, wo die Gesetzgebung Einzelhändler mit einem isoliert stehendem Geldautomaten im Geschäft verpflichtet, das Bargeld nachts zu entnehmen und den Geldautomaten offen zu lassen. Bei anderen Geldautomaten können die enthaltenen Beträge durch Erhöhung der Auffüllhäufigkeit gesenkt werden.

4.3.1.2 *Die Beute unbrauchbar und das Geld rückverfolgbar machen*

Intelligente Banknoten-Neutralisationssysteme (IBNS) sind eine erste Technik, um die Beute unbrauchbar zu machen. Diese Systeme färben die Banknoten mit Tinte ein, um sie als gestohlen zu kennzeichnen. Indikatoren und Marker können der IBNS-Tinte beigefügt werden. Gegenwärtig werden diese Marker hauptsächlich für forensische Zwecke verwendet, um die Banknote mit dem Tatort in Verbindung zu bringen und für die Täter das Risiko, gefasst zu werden zu erhöhen. Auch wenn IBNS eine wirksame Präventivmaßnahme ist, gibt es einige Überlegungen.

Die Europäische Zentralbank erstattet gefärbte Banknoten ([4]) nicht zurück (seit 2003), einige nationale Zentralbanken der EU-Mitgliedstaaten tun dies aber noch. Eingefärbte Banknoten werden auch über Kasinos wieder in das legale System eingeführt. Ein IBNS schafft ein zusätzliches Hindernis für Kriminelle, wäre aber viel effektiver, wenn es für Kriminelle unmöglich ist, in der EU gefärbte Banknoten zu verwenden. Um dies zu erreichen, sollten eingefärbte Banknoten von den nationalen Zentralbanken nicht akzeptiert werden. Ausnahmen können unter bestimmten Umständen gemacht werden, z.B. bei Banknoten, die aufgrund einer versehentlichen Aktivierung eingefärbt wurden. Es ist auch wichtig, der Bevölkerung zu raten, eingefärbte Banknoten nicht zu akzeptieren. Auf längere Sicht sollten Einzahlungsautomaten eingefärbte Banknoten erkennen und in Banken und Geschäftsräumen wie Kasinos, Autowaschanlagen usw. installiert werden. Die Erkennung der Tinte ist schwierig und teuer, eine kostengünstige Lösung könnte jedoch die Installation von

([4]) Entscheidung der Europäischen Zentralbank, Stückelungen, Spezifikationen, Reproduktion, Umtausch und Einzug von Euro-Banknoten, 2003.

Infrarotsystemen sein, die mit Infrarot-Markern gefärbte Banknoten erkennen. Diese Systeme haben sich als wirksam erwiesen und stellen in Belgien und Frankreich eine bewährte Praxis dar. Wenn Banknoten mit Infrarot-Markern in den Geldautomaten eingeführt werden, akzeptiert („schluckt“) der Geldautomat das Geld, schreibt es aber nicht einem Konto gut. Die Person, die die markierten Banknoten einführt, sollte ebenfalls registriert werden.

Es gibt einige weitere Überlegungen bei der Installation von IBNS-Lösungen. Mehrere Hersteller bieten eine Reihe verschiedener IBNS-Lösungen mit unterschiedlichen Aktivierungsmechanismen und unterschiedlichen Tintentypen an. Eine erste Überlegung betrifft die Tatsache, dass nicht alle Arten von IBNS-Aktivierungstechnologien allen Bedrohungen entgegenwirken können. Einige IBNS funktionieren sehr gut bei Rip-Out-, Ram-Raid-, *In-situ*- und Gasangriffen, sie funktionieren jedoch nicht im Falle eines Angriffs mit festen Explosivstoffen oder umgekehrt. Daher sollte die Technologie gut überlegt gewählt werden.
Eine weitere Überlegung ist die Art der zu wählenden Tinte. In Belgien werden die nationalen Mindestanforderungen an das IBNS (Sicherheit, Prozentsatz der Einfärbung, nicht abwaschbar usw.) festgelegt, und unabhängige Tests bescheinigen, dass das System den nationalen Normen entspricht und gemäß den Angaben des Herstellers funktioniert. Es ist wichtig, mit echten Banknoten zu testen, da es billigere Tinten auf dem Markt gibt, die gut bei gefälschten Banknoten, aber nicht bei echten Banknoten funktionieren: Das bedeutet, dass die Tinte durch Waschen von echten Banknoten entfernt werden kann. Darüber hinaus wird empfohlen, der Tinte einen forensischen Marker beizufügen, der es ermöglicht, eine Verbindung zwischen eingefärbten Banknoten und einem bestimmten Tatort zu ermitteln.

Bewährte Verfahren zeigen, dass IBNS vor allem in Kombination mit anderen Präventivmaßnahmen sehr effektiv sein kann. 2015 führte Frankreich eine neue Gesetzgebung ein, die Artikel über die Installation von IBNS und die Verwendung von Tinte mit einzigartiger DNA enthält. Die französische Gendarmerie entscheidet auf der Grundlage einer Risikobewertung, wo das IBNS und andere Maßnahmen umgesetzt werden müssen. Da die neue Gesetzgebung den präventiven und operativen Ansatz stärkte, sank die Zahl der Angriffe von 300 im Jahr 2013 auf 50 im Jahr 2018.

Eine weitere Technik, die derzeit entwickelt wird, um die Beute unbrauchbar zu machen, ist die Verwendung von **Klebstoff**. Die Wirksamkeit von Klebstoff wurde in den Niederlanden nachgewiesen, aber die Implementierungs- und Betriebskosten sind derzeit hoch. Darüber hinaus kann Klebstoff eine Brandgefahr darstellen, wenn das System nicht vor einem Angriff aktiviert wird,

da durch die Verbreitung von Klebstoffpartikeln in der Luft ein brennbares Gemisch entstehen könnte. Diese Methode ist noch nicht marktreif, könnte aber eine Lösung für die Zukunft sein.

4.3.2 Erhöhung der Risiken

Eine zweite Achse zur Verhinderung physischer Geldautomatenangriffe ist die Abschreckung potentieller Täter von der Begehung von Straftaten, indem das Risiko der Aufdeckung und Bestrafung erhöht wird. Neben dem Verletzungsrisiko bei der Verwendung von Sprengstoffen für Angriffe auf Geldautomaten besteht das Hauptrisiko für einen Kriminellen in einer Haftstrafe, wenn er entweder auf frischer Tat oder nach einer Ermittlung gefasst wird. Um das Verlangen der potentiellen Täter zu verringern, muss das Risiko der Aufdeckung und Bestrafung erhöht werden. Für die Gesellschaft ist die Ergreifung und Verurteilung der Kriminellen natürlich auch eine sehr wirksame Präventionsmethode, wenn es zu einer anschließenden Bestrafung kommt, wie wir in mehreren Ländern gesehen haben.

4.3.2.1 *Austausch von Informationen*

Entscheidend für die Aufdeckung und Bestrafung von Geldautomatenangreifern ist der Informationsaustausch zwischen allen Beteiligten im Kampf gegen physische Geldautomatenangriffe, darunter Geldautomatenanbieter, Strafverfolgungsbehörden (Polizei, Staatsanwaltschaft usw.), Behörden, die Hersteller sowohl von Geldautomaten als auch von Sicherheits- und Schutzvorrichtungen, Berufsverbände, Geldautomatenanbieter (Banken und unabhängige Anbieter), Sicherheitsunternehmen und Alarmzentralen. Im Idealfall würde dies sowohl auf nationaler als auch auf internationaler Ebene geschehen.

Die Früherkennung eines bevorstehenden physischen Geldautomatenangriffs ist schwierig. Nur in Fällen mit nahezu einwandfreiem Informationsaustausch auf internationaler Ebene zwischen Strafverfolgungspartnern und privaten Partnern (Sicherheitsfirmen und Geldautomatenanbieter) ist eine Früherkennung möglich. Zahlreiche Indikatoren müssen überwacht werden, darunter Frühwarnmeldungen zwischen den Strafverfolgungsbehörden über in Bewegung befindliche organisierte Banden, Informationen über („heiße“) Fahrzeuge, die bei Geldautomatenangriffen benutzt wurden, Informationen von Sicherheitsfirmen oder Nachbarschaftswachen über verdächtiges Verhalten, das in der Umgebung des Geldautomaten beobachtet wurde, verdächtige

Transaktionen, die von Geldautomatenanbietern entdeckt wurden, und andere Erkennungsmethoden. Weitere mögliche polizeiliche Maßnahmen zur Früherkennung sind die Überwachung gestohlener Autos, von Herstellern und Vertreibern von Sprengstoff sowie von Unternehmen, die zur Verwendung von Sprengstoff berechtigt sind. Die Anstrengungen, die für eine Früherkennung notwendig sind, sind anspruchsvoll und bieten keine Erfolgsgarantie, daher sind Interventionen der Strafverfolgungsbehörden vor einem Angriff selten.

Wenn eine Früherkennung nicht möglich ist, können Alarmzentralen im Falle eines physischen Geldautomatenangriffs schnell eine Warnung ausgeben. Um ein Eingreifen zu ermöglichen, müssen nationale Regelungen und Protokolle für eine schnelle Kommunikation zwischen Alarmzentralen und Strafverfolgungsbehörden vereinbart und eingerichtet werden. Im Falle einer Früherkennung oder von Echtzeitinformationen müssen die Strafverfolgungsbehörden immer den Zeitpunkt und die beste Gelegenheit für ein Eingreifen bewerten. Die Kriminellen auf frischer Tat zu fassen, ist sehr schwierig und kann zu gefährlichen Situationen führen, da einige organisierte Banden sehr gewalttätig sind und schwere Waffen einsetzen.

Für eine erfolgreiche Ermittlung nach einem physischen Geldautomatenangriff müssen die Strafverfolgungsbeamten mit allen Beteiligten kommunizieren, da jeder von ihnen über Informationen verfügen könnte, die zum Ermittlungserfolg beitragen. Natürlich ist die Kommunikation und Zusammenarbeit mit den Hauptopfern, den Banken oder anderen Geldautomatenanbietern notwendig: Sie haben Zugang zu Daten, die für die Ermittlung wichtig sind. Für den Geldautomatenanbieter werden die Informationen der Strafverfolgungsbehörden dazu beitragen, die Präventionsmaßnahmen zu verbessern. Darüber hinaus erweisen sich Kontakte mit Fachverbänden und Herstellern als nützlich: Sie versenden häufig Sicherheitswarnungen, die andere interessierte Akteure abonnieren können. Geldautomatenhersteller haben einen guten Überblick über die verschiedenen Arten von Geldautomatenangriffen und die entsprechenden Schwächen und Stärken von Präventivmaßnahmen. Sie sind gern bereit, die Polizei mit Informationen über die technischen Aspekte der Geldautomaten und über die verwendeten MO zu unterstützen.

Grenzüberschreitende Zusammenarbeit ist unerlässlich: Die Länder sollten Informationen austauschen (über Verdächtige, verurteilte Geldautomatenangreifer, MO, verdächtige Fahrzeuge, Bilder von Angriffen usw.), nicht nur zur Unterstützung der Ermittlungen, sondern auch, weil Verdächtige, die in einem anderen Land verurteilt wurden, wegen erneuter Straftaten/Rückfälligkeit verurteilt werden können.

Schließlich könnte die Einrichtung einer Datenbank auf europäischer Ebene, die den Strafverfolgungsbehörden zur Verfügung steht und forensische Daten (z.B. zu verschiedenen Arten von IBNS-Tinten, Indikatoren und Markern oder Geldautomatenschutzglas) enthält, Ermittlungen stark unterstützen und Verdächtige mit einem bestimmten Tatort in Verbindung bringen. Die Standardisierung von Technologien auf internationaler Ebene ist oft unzureichend: Während der Konferenz im Januar 2019 erwähnten die Teilnehmer, dass eine Standardisierung von Tinten und Tatortmarkierungen auf EU-Ebene die Ermittlungen erheblich erleichtern könnte.

4.3.2.2 *Videoüberwachung und Abhörgeräte*

Die Bild- und Tondaten von Videoüberwachungssystemen und Abhörgeräten können sowohl die Echtzeit-Erkennung eines Angriffs (z.B. zur Verhinderung physischer Schädigung der am Tatort eintreffenden Ersteinsatzkräfte) als auch nachfolgende Ermittlungen (z.B. zur Identifizierung der Täter und ihrer Vorgehensweise) unterstützen. Die Überwachungsbilder können mit Bildern von öffentlichen und anderen Überwachungssystemen in der Nachbarschaft des Geldautomaten und mit Verkehrsradaraufnahmen kombiniert werden, um ein vollständigeres Bild der Täter und ihrer Vorgehensweise zu erhalten.

Aufnahmen von Videoüberwachungssystemen sind jedoch oft von schlechter Qualität oder unsachgemäß gespeichert. Die Bilder sollten von ausreichender Qualität sein, um die Identifizierung einer Person zu ermöglichen. Auch hier würde die Festlegung europäischer Standards für die Sicherheits-Videoüberwachung die Ermittlungen erleichtern. Da außerdem die Täter vor einem Angriff oft die Überwachungskameras deaktivieren, könnte auch die Installation von nicht sichtbaren Überwachungskameras oder von Echtzeit-Abhörgeräten in Betracht gezogen werden.

4.3.2.3 *Bestrafung und Wiedereingliederung der Täter*

Eine konsequente und harte Bestrafung beweist ihre präventive Wirkung. Die Verhaftung einer organisierten Bande wirkt sich unmittelbar auf die Zahl der Geldautomatenangriffe aus. Die Haftentlassung von Geldautomatenangreifern führt aber auch oft zu einer neuen Welle von Angriffen. Das bedeutet, dass kurze Strafen dazu führen, dass die Täter sehr schnell wieder aktiv werden. Die Mindest- und Höchststrafen für Kriminelle, die für jede Art von physischem Geldautomatenangriff verurteilt werden, sind von Mitgliedstaat zu Mitgliedstaat unterschiedlich.

Einige sind der Meinung, dass höhere Strafen potentielle Täter abschrecken werden. Wissenschaftliche Untersuchungen ([5]) zeigen jedoch, dass eine Erhöhung des Strafmaßes nicht unbedingt die abschreckende Wirkung erhöht. Daher könnte es interessant sein, sich mit strafvollzugs- (und täterbasierten) Rehabilitationsprogrammen zu befassen, um die hohe Rückfallquote zu verringern.

4.3.3 Erhöhung des Aufwands

Die dritte Achse zur Prävention physischer Geldautomatenangriffe umfasst Maßnahmen, die es für einen Täter schwieriger machen, die kriminelle Handlung auszuführen.

4.3.3.1 *Gewährleistung einer kriminalitätsresistenten Umgebung*

Wenn die Risikobeurteilung (siehe oben) ergibt, dass sich ein Geldautomat in einer Umgebung mit hohem Risiko befindet, sollte der Standort abgebaut und der Geldautomat in einen Bereich mit geringem oder mittlerem Risiko verlegt werden. Dies gilt vor allem, wenn die Analyse zeigt, dass das Gebäude einstürzen könnte, wenn ein Geldautomat unter Verwendung von Sprengstoff angegriffen wird. In Fällen mit hohem Risiko könnten Gesetze zur Durchsetzung solcher Maßnahmen erlassen werden. Abgesehen von der Verringerung der Anzahl der Geldautomaten in risikoreichen Umgebungen sollte der bargeldlose Zahlungsverkehr gefördert werden, um den Bedarf an Geldautomaten zu verringern.

Wenn es nicht möglich ist, den Geldautomaten zu verlegen, sollte ein Höchstmaß an Sicherheitsmaßnahmen ergriffen werden: z.B. die Verwendung von Anti-Rammschutzpollern, Laternenpfählen und anderem Straßenmobiliar, um den Zugang zum Gebäude zu beschränken, Fahrzeugauffangsysteme, die Installation einer angemessenen Straßenbeleuchtung, verstärkte offene oder verdeckte Überwachung und Diebstahlschutzvorrichtungen wie z.B. ein Banknotenzerstörungssystem. Wenn ein Geldautomat an einem Ort angegriffen wird, der nicht als risikoreich identifiziert wurde, sollte er entsprechend eingestuft und zusätzliche Sicherheitsmaßnahmen getroffen werden. Die neuen Faktoren sollten bei der Aktualisierung des

([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.

Risikobewertungsinstruments berücksichtigt werden. Die Neubewertung dieses Risikos sollte regelmäßig wiederholt werden.

4.3.3.2 *Verstärkung der Geldautomaten*

Die Hersteller von Geldautomaten bieten eine Standardauswahl von Geldautomaten an, die eine Reihe von Sicherheitsmerkmalen aufweisen, die nach den Sicherheitsstufen des Europäischen Komitees für Normung (CEN) eingestuft sind. Im Allgemeinen haben Geldautomaten eine CEN-Kennzeichnung, die von der unteren Stufe CEN1 bis zur höchsten Stufe CEN4 reicht. Merkmale wie Stabilität des Gehäuses und Widerstandsfähigkeit gegen Angriffe bestimmen den Grad. Gasbeständigkeit wird meist als Option angeboten (CEN-GAS). Die Standardmodelle können mit zusätzlichen Schutzmaßnahmen aufgewertet werden. Gewöhnlich werden diese Funktionen von Dritten installiert, um die Einhaltung der lokalen Gesetzgebung und die Anpassung des Basismodells an die Anforderungen der Kunden vor Ort zu gewährleisten. Zu den zusätzlichen Sicherheitsmerkmalen gehören verschiedene Sensoren zur Aktivierung eines Gas-Neutralisationssystems oder IBNS im Falle eines *In-Situ*-Angriffs oder eines Angriffs mit Sprengstoff sowie verbesserte Blenden und Tresorschlösser, die den unbefugten Zugang zum Tresor verhindern, wenn die Hauptblende beschädigt ist. Bei transportablen, autonomen Geldautomaten ist es wichtig, Verankerungssysteme zu verwenden, die zusätzlichen Schutz gegen Rip-out-/Ram-Raid-Angriffe bieten. Tracking-Systeme können in den Geldautomaten integriert werden, um die Ermittler zu unterstützen, wenn der Geldautomat vor der Öffnung an einen anderen Ort transportiert wird.

4.3.3.3 *Architektonische Maßnahmen*

Bei der Installation eines Geldautomaten wird empfohlen, Geräte mit rückseitigem Zugang zu verwenden. In diesem Fall muss der Täter das Gebäude betreten und sich Zugang zur Rückseite des Automaten verschaffen, um das Geld zu stehlen. Transportable, isoliert stehende Geldautomaten sind am verwundbarsten. Eine Verringerung der Zahl dieser Geldautomaten würde die Sicherheit erhöhen. Die Verpflichtung, Geldautomaten in einem einbruchsicheren Raum zu installieren, würde automatisch die Nutzung isoliert stehender Geldautomaten verringern.

4.3.3.4 *Nebelanlage*

Eine Nebelkanone füllt einen Raum schnell mit einem dichten Nebel, sodass der Eindringling nichts sehen kann. Dieser Sicherheitsnebel macht es oft unmöglich, den Geldautomatenangriff auszuführen. Zumindest verlangsamt das System den Täter und verschafft der Polizei Zeit, einzugreifen. Die Sicherheitsnebelanlage ist mit dem Alarmsystem verbunden und kann auf zwei Arten aktiviert werden. Sie kann automatisch durch Alarmsensoren wie Bewegungsmelder (nachts) oder Geldautomaten-Blenden-Manipulationssensoren ausgelöst werden. Sie kann auch von einer Alarmzentrale aktiviert werden, um zu viele Fehlalarme zu vermeiden. Bei TTW-Geldautomaten im Freien kann die Nebelanlage auf der Rückseite des Geldautomaten angebracht werden, um den dahinter liegenden Raum mit Nebel zu füllen und die Sicht der Täter auf Null zu reduzieren.

Nebelanlagen können einen punktuellen Schutz für einen Geldautomaten bieten, der sich auf einer freien Fläche in Tankstellen, Supermärkten usw. befindet. Dadurch wird vermieden, dass der Nebel den gesamten Bereich füllt. Der Nebelschutz ist am wirksamsten, wenn der Nebel aus verschiedenen Winkeln kommt oder wenn er den Raum hinter dem Geldautomaten füllt, im Fall
eines Ram-Raid-Angriffs. Derzeit wird geprüft, ob Nebelkanonen im Geldautomaten selbst installiert werden können, anstatt in dem Raum, in dem sich der Geldautomat befindet. Dem Nebel können DNA-Marker beigefügt werden, die auf die Täter und ihre Kleidung gelangen.

4.3.4 Parallele Maßnahmen

Um die effiziente und effektive Umsetzung der oben genannten Präventivmaßnahmen zu gewährleisten, muss eine Reihe paralleler Maßnahmen in Betracht gezogen werden. Diese Maßnahmen sind unerlässlich, um einen ganzheitlichen präventiven und operativen Ansatz zur Bekämpfung physischer Geldautomatenangriffe zu ermöglichen oder zu unterstützen.

4.3.4.1 *Gesetzgebung*

In einigen Ländern verpflichtet die Gesetzgebung Geldautomatenanbieter zu präventiven Maßnahmen. In anderen Ländern sorgen Vereinbarungen und Abkommen zwischen Banken und Strafverfolgungsbehörden für einen gut funktionierenden Ansatz bei physischen Geldautomatenangriffen. Zu den Bereichen, in denen regulatorische Maßnahmen in Betracht gezogen werden können, gehören:

- Einbettung von Präventivmaßnahmen;

- rechtliche Rahmenbedingungen, die eine Zusammenarbeit zwischen Strafverfolgungsbehörden und öffentlichen und privaten Partnern ermöglichen;
- eine Überarbeitung des Strafmaßes, wenn die Strafen für die Täter bei physischen Geldautomatenangriffen zu niedrig sind.

Häufig sind jedoch nur Bankinstitute zur Einhaltung dieser Gesetze oder Vereinbarungen verpflichtet, während unabhängige Geldautomatenanbieter nicht an diese Gesetze oder Vereinbarungen gebunden sind. Dies ist eine häufige Schwachstelle eines Regulierungsrahmens.

Einige Länder führen keine Regulierung ein, sondern versuchen, die Anbieter von Geldautomaten zu Präventivmaßnahmen zu bewegen, indem sie ihr Bewusstsein für Kriminalitätsbereiche und Trends schärfen: In Ländern mit einer hohen Anzahl unabhängiger Banken erweist sich dies als besonders schwierig.

Es muss unbedingt sichergestellt werden, dass die wirksame Umsetzung der Präventivmaßnahmen Änderungen der Gesetzgebung und der Vorschriften sowohl auf nationaler als auch auf internationaler Ebene umfasst, die für alle Arten von Geldautomatenanbietern bindend sind. Idealerweise sollte die Gesetzgebung auf EU-Ebene angeglichen werden, um zu vermeiden, dass wirksame Präventivmaßnahmen, die in der Gesetzgebung eines Landes verankert sind, organisierte Banden in andere Länder mit weniger strengen Vorschriften treiben.

4.3.4.2 *Medienstrategie*

Eine weitere wichtige Achse der Präventionsstrategie ist eine gut etablierte Medienstrategie, mit der die Erwartungen und der Wunsch der Angreifer von Geldautomaten, sich auf solche Verbrechen einzulassen, verringert werden. Geringe Erfolgsquoten und die hohen Risiken für die Täter sind hervorzuheben; Kommunikation über die Lukrativität („Beute“) oder Details über den Geldautomatenangriff, etwa die Art des betroffenen Geldautomaten oder den MO sind zu vermeiden. Andererseits ist eine umfassende Kommunikation über die Festnahme von Verdächtigen und die daraus folgende Bestrafung nach einer Verurteilung notwendig.

4.3.4.3 *Verstärkte Zusammenarbeit*

Verstärkte Zusammenarbeit und Informationsaustausch wurden ausgiebig erwähnt, können aber nicht genug betont werden. Der operative Informationsaustausch auf internationaler Ebene ist das

Kerngeschäft von Europol. Neben diesem Informationsaustausch zeigte die Präventionskonferenz die klare Notwendigkeit einer verstärkten multidisziplinären und mehrstufigen Zusammenarbeit und des Informationsaustauschs zwischen allen relevanten Akteuren auf, darunter Strafverfolgungsbehörden, Behörden, Hersteller von Geldautomaten und Sicherheits- und Schutzvorrichtungen, Berufsverbände, Geldautomatenanbieter (Banken und unabhängige Anbieter), Sicherheitsunternehmen und Alarmzentralen. Dies muss die lokale, nationale und internationale Ebene einschließen.

4.3.4.4 *Verminderung des Risikos von Kollateralschäden*

Bei Angriffen mit festen Sprengstoffen hinterlassen einige organisierte Banden Material. Dies kann zu gefährlichen Situationen für Einsatzkräfte oder Zivilisten (die entweder in der Nachbarschaft wohnen oder vorbeikommen) führen. Ihre Sicherheit muss gewährleistet sein. Wie in Belgien müssen Protokolle und Verfahren, die von den Einsatzkräften (sowohl von den Strafverfolgungsbehörden als auch von den Geldautomatenanbietern) einzuhalten sind, entwickelt und aufeinander abgestimmt werden. Eine weitere bewährte Praxis in diesem Zusammenhang ist das Beispiel der Niederlande, wo zur Beurteilung der Situation auf Videoaufnahmen des Geldautomatenangriffs zurückgegriffen wird. Es können Vereinbarungen mit Alarmzentralen getroffen werden, um diese Aufnahmen sofort verfügbar zu machen.

4.3.4.5 *Soziale Prävention*

Oft suchen organisierte Banden nach jungen Leuten, die sie rekrutieren können. Es könnten Projekte ins Leben gerufen werden, um diese Rekrutierungsprozesse in einem frühen Stadium zu vereiteln. Polizei oder Sozialarbeiter sollten diese Prozesse aufmerksam beobachten und könnten eingreifen, indem sie persönlich auf die potentiellen Täter zugehen.

5 Schlussfolgerungen

In den letzten 2 Jahren hat die Zahl der europäischen Länder, die von physischen Geldautomatenangriffen betroffen sind, zugenommen. In diesem Zusammenhang haben Europol und das EUCPN zusammengearbeitet, um die besten Maßnahmen zur Bekämpfung und Verhütung dieses Verbrechens zusammenzutragen.

Ein erfolgreicher Ansatz zur Abwehr physischer Geldautomatenangriffe besteht in einer Kombination von operativen und präventiven Maßnahmen, die vorzugsweise in einen gesetzlichen Rahmen eingebettet sind. Um zu vermeiden, dass starke Maßnahmen in einem Land organisierte Banden in anfälligere Länder treiben, wird empfohlen, diese Maßnahmen auf europäischer Ebene zu verabschieden.

Zur Prävention und Bekämpfung dieser Art von Kriminalität sollte eine klare Strategie in drei Schritten festgelegt werden: Beurteilung der Situation, Entwicklung eines Präventionsansatzes auf der Grundlage der Risikobewertung und Umsetzung der Präventivmaßnahmen.

Die Risikobewertung für physische Angriffe auf Geldautomaten sollte die Merkmale des Geldautomaten und seiner Umgebung, die Zusammenarbeit mit Partnern und Interessengruppen zur Bildung von Allianzen zur Bekämpfung dieses Verbrechens und die Bewertung des präventiven und rechtlichen Rahmens umfassen. Sobald die Situation beurteilt worden ist, sollte eine Strategie festgelegt werden, die auf öffentlich-privater Zusammenarbeit sowie präventiven und operativen Gegenmaßnahmen beruht. Ziel der Präventivmaßnahmen ist es, die Absicht und die Fähigkeiten des Täters zur Durchführung eines physischen Geldautomatenangriffs zu verringern. Um dies zu erreichen, werden drei Achsen präventiver Maßnahmen vorgeschlagen: Verringerung der Lukrativität, Erhöhung des Risikos und Erhöhung des Aufwands. Parallele Maßnahmen sollten die Präventivstrategie vervollständigen. Die Einrichtung einer nationalen Behörde, die befugt ist, diese notwendigen Maßnahmen durchzusetzen, ist die beste Praxis.

Durch **Reduzierung der Lukrativität** sinkt die Bereitschaft des Kriminellen, sich an dieser Art von Verbrechen zu beteiligen. Die Verringerung der Bargeldmenge in den Geldautomaten durch Begrenzung des aufgefüllten Bargeldes auf die Menge, die nur für einen Handelstag ausreicht, oder die Leerung der (am stärksten gefährdeten) Geldautomaten in der Nacht ist eine Maßnahme, um die Erwartungen der Kriminellen zu verringern. Eine andere Methode besteht darin, die Beute unbrauchbar und das Geld rückverfolgbar zu machen. In diesem Zusammenhang kann das IBNS eingesetzt werden, das die Banknoten einfärbt und als gestohlen markiert. Diese Methode ist am effektivsten, wenn es für Kriminelle unmöglich ist, dieses Geld auszugeben oder diese Scheine wieder

in den legalen Geldkreislauf einzuführen. Dies kann dadurch erreicht werden, dass Banken und die Öffentlichkeit keine eingefärbten Banknoten zur Zahlung akzeptieren und Einzahlungsautomaten installiert werden, die gefärbte Banknoten erkennen und ablehnen können. In dieser Hinsicht hat sich die Investition in Infrarot-Systeme, die mit Infrarot-Markern gefärbte Banknoten erkennen, in Belgien und Frankreich als eine kostengünstige Lösung erwiesen. Bei der Installation des IBNS sollten die Länder die gewählten Aktivierungsmechanismen, die Mindestanforderungen für die Neutralisierung der Banknoten und das Hinzufügen eines forensischen Markers zur Tinte gründlich prüfen.

Maßnahmen zur Abschreckung potentieller Täter von der Begehung von Straftaten, indem das **Risiko der Aufdeckung und Bestrafung erhöht** wird, sind die zweite Achse zur Prävention physischer Geldautomatenangriffe. Der Schlüssel zur Überführung und Bestrafung von Geldautomatenangreifern ist die Sammlung und der Austausch von Informationen zwischen allen Beteiligten, sowohl auf nationaler als auch auf internationaler Ebene. Der Informationsaustausch von qualitativ hochwertigen Videoüberwachungsbildern und Tondaten kann die Chancen auf Früherkennung und erfolgreiche Ermittlungen erhöhen. Um zu vermeiden, dass Videoüberwachungs- oder Abhörgeräte vor dem Angriff deaktiviert werden, kann die Installation von nicht sichtbaren Videoüberwachungsanlagen oder Echtzeit-Abhöranlagen in Betracht gezogen werden. Die Schaffung einer forensischen Datenbank und die Standardisierung der Technologien auf europäischer Ebene könnten die internationale Zusammenarbeit und die Ermittlungen erheblich erleichtern. Wenn Täter gefasst und verurteilt werden, könnte es interessant sein, sich mit strafvollzugs- (und täterbasierten) Rehabilitationsprogrammen zu befassen, um die hohe Rückfallquote zu verringern.

Die dritte Achse zur Verhinderung physischer Geldautomatenangriffe umfasst Maßnahmen zur **Erhöhung der Anstrengungen**, die ein Täter zur Ausführung der Straftat unternehmen muss. Die Installation eines Geldautomaten in einer kriminalitätsresistenten Umgebung mit einem Höchstmaß an Sicherheitsvorkehrungen wird es für Straftäter schwieriger machen, einen Geldautomaten anzugreifen. Darüber hinaus kann der Standardschutz von Geldautomaten durch eine Reihe zusätzlicher Sicherheitsmerkmale erweitert werden. Zusätzlich zu diesen Maßnahmen kann die Installation einer Nebelanlage den Täter abschrecken oder zumindest den Angriff verzögern.

Eine Reihe **paralleler Maßnahmen** wird die oben genannten Maßnahmen verstärken, wie z.B. die Schaffung eines Rechtsrahmens, der alle Anbieter von Geldautomaten verpflichtet, die Präventivmaßnahmen umzusetzen, die Entwicklung einer gut etablierten Medienstrategie, die verstärkte Zusammenarbeit auf lokaler, nationaler und internationaler Ebene, Leitlinien für

Einsatzkräfte, um das Risiko von Kollateralschäden zu verringern, und die Investition in soziale Prävention, um die kriminellen Rekrutierungsprozesse zu untergraben.

6 Empfehlungen für einen präventiven Ansatz: Übersicht

Entwicklung einer wirksamen Antwort zur Verhinderung physischer Angriffe auf Geldautomaten

Beurteilung der Situation

Erstellen des Risikoprofils der Geldautomaten in Ihrem Land/Ihrer Region
Identifizierung von Partnern und Beteiligten im Kampf gegen physische Geldautomatenangriffe und Bewertung der Zusammenarbeit
Evaluierung des rechtlichen Rahmens für die Bekämpfung physischer Geldautomatenangriffe auf nationaler und internationaler Ebene.

Entwicklung eines präventiven Ansatzes

Bestimmung der abzudeckenden (Haupt-)Risiken und der Prioritäten
Bestimmung der besten Präventivmaßnahmen zur Abdeckung dieser Risiken unter Berücksichtigung von drei Hauptachsen.
Bestimmung der parallelen Präventivmaßnahmen, die zur Stärkung der getroffenen Präventivmaßnahmen erforderlich sind.

Präventivmaßnahmen, die getroffen werden können, zur		
Verringerung der Lukrativität	Erhöhung der Risiken	Erhöhung des Aufwands
– Verringerung der Bargeldmenge. ○ Leeren des Geldautomaten bei Nachts. ○ Erhöhen der Anzahl/Häufigkeit der Nachfüllungen. – Unbrauchbarmachen der Beute. ○ Intelligente Banknoten-Neutralisationssysteme (IBNS). ○ Infrarot-Marker in IBNS-Tinte zur Erkennung von gefärbten Banknoten durch Einzahlungsautomaten. ○ In Entwicklung: Klebstoff.	– Grenzüberschreitender Informationsaustausch für: ○ Früh- oder Echtzeit-Erkennung eines möglichen Geldautomatenangriffs, ○ Stärkung des operativen Ansatzes, ○ Verurteilung von Wiederholungstätern, ○ Austausch von forensischen Daten auf europäischer Ebene. – Videoüberwachung und Abhörgeräte. – Konsequente Bestrafung und Wiedereingliederung der Täter.	– Gewährleistung einer kriminalitätsresistenten Umgebung. ○ Wechseln des Standortes von Geldautomaten mit hohem Risiko. ○ Sicherheitsmaßnahmen: physische Hindernisse, Überwachung usw. – Verstärkung von Geldautomaten mit Blenden, die Gas oder festen Sprengstoffen usw. standhalten. – Architektonische Maßnahmen wie Geräte mit Zugang von hinten – Sicherheitsnebelanlagen.

Parallele Maßnahmen zur Stärkung des präventiven Ansatzes

- Wirksame Gesetzgebung einschließlich Präventivmaßnahmen gegen physische Geldautomatenangriffe, konsequente Verurteilung usw.
- Wirksame Medienstrategie zur Abschreckung von Tätern.
- Verstärkte Zusammenarbeit zwischen allen Beteiligten (öffentlich, privat, Strafverfolgung) im Kampf gegen physische Geldautomatenangriffe.
- Verringerung des Risikos von Kollateralschäden für Einsatzkräfte oder Zivilisten (z.B. Nachbarn oder Passanten).
- Soziale Prävention, um zu vermeiden, dass Jugendliche für (diese Art von) Kriminalität rekrutiert werden.