Prevenir los asaltos a cajeros automáticos

Desarrollo de un enfoque eficaz

Agradecimientos
El presente documento es fruto de la colaboración entre la Agencia de la Unión Europea para la Cooperación Policial (Europol) y la secretaría de la Red Europea de Prevención de la Delincuencia (REPD). Queremos agradecer a los expertos en asaltos a cajeros automáticos que invirtieron tiempo y esfuerzo prestando apoyo a la creación de este documento de recomendación. Ellos contribuyeron asistiendo a la conferencia sobre la prevención de asaltos a cajeros automáticos (enero de 2019, Bruselas) y proporcionando información crucial. En particular, queremos agradecer a los organismos encargados de hacer cumplir la ley de los países de la UE y de países no pertenecientes a la UE («terceros»), al sector privado, incluida la asociación del sector de cajeros automáticos (ATMIA), BPost, el Centro holandés para la Prevención del Delito y la Seguridad (CCV), Diebold Nixdorf, el grupo de expertos de la Asociación Europea de Transacciones Seguras sobre asaltos a cajeros automáticos y cajas fuertes de cajeros automáticos (EAST EGAP), la Asociación Europea de la Protección Inteligente de Fondos (EURICPA), ING, Febelfin, NCR, Protect, SIOC Banking, Spinnaker, TMD Security y los Ministerios del Interior de Bélgica, Croacia, Alemania y España.

Aviso legal
El contenido de esta publicación no refleja necesariamente la opinión oficial de ningún Estado miembro de la UE ni de ningún organismo o institución de la UE o de las Comunidades Europeas.

Índice

1 Contexto

Ante el aumento del número de ataques a cajeros automáticos y el incremento del número de países europeos afectados, la Red Europea de Prevención de la Delincuencia (REPD) y Europol organizaron una conferencia (enero de 2019) en la que se reunieron los organismos encargados de la aplicación de la ley y los socios públicos y privados para examinar la prevención de estos delitos. En el presente documento de recomendación se resumen las conclusiones de esta conferencia para sensibilizar a las autoridades sobre los asaltos a cajeros automáticos y las medidas preventivas.

La amplia gama de métodos diferentes (*modus operandi*) utilizados por los delincuentes para atacar cajeros automáticos puede dividirse en dos categorías principales: asaltos a cajeros automáticos y ataques de fraude relacionados con los cajeros automáticos (estos incluyen los ataques lógicos a cajeros automáticos y los ataques de malware) Este documento se centra en los asaltos a cajeros automáticos: la entrada forzada con medios físicos a los cajeros para sacar su dinero. La entrada forzada se puede realizar mediante:

- el uso de explosivos: los atacantes utilizan explosivos de gas o sólidos para abrir físicamente la caja fuerte del cajero automático y acceder al dinero;
- ataques que consisten en «arrancar/empotrar»: los atacantes sacan el cajero físicamente del entorno de la instalación, a menudo utilizando un vehículo de alta gama;
- ataques in situ: los atacantes cortan la caja fuerte por medio de la fuerza bruta, a menudo utilizando herramientas de corte o rotura como amoladoras angulares, mazos o sopletes de oxiacetileno.

Un número limitado pero creciente de países de la Unión Europea está preocupado por los asaltos a cajeros automáticos. Se estima que en 2017 las pérdidas financieras causadas en Europa superaron los 30 millones de euros. Algunos países siguen siendo testigos de un número importante de asaltos contra cajeros automáticos, otros han experimentado un aumento significativo en el número de estos incidentes en los últimos dos años. Esta área de delincuencia evoluciona rápidamente. Algunos países han tenido éxito con su enfoque para abordar los asaltos a cajeros automáticos y han visto una disminución significativa de los ataques recientemente. Por otro lado hay países que no se habían visto afectados anteriormente y que han experimentado una repentina oleada de asaltos a cajeros en 2018 debido a la expansión del territorio de grupos delincuenciales organizados (GDO). No sólo se ven afectados los bancos; crece el número de ataques a cajeros automáticos de proveedores independientes porque suelen estar situados en locales o lugares más vulnerables.

2 Factores que determinan el éxito de un asalto a un cajero automático

La tasa de éxito de los ataques a cajeros es baja; sólo un tercio de los ataques tienen éxito. Sin embargo, incluso cuando el ataque no tiene éxito, los daños causados a las estructuras de los edificios (por ejemplo por los explosivos) son igualmente importantes; dejan un entorno inseguro en las proximidades del lugar del delito para los residentes locales, las unidades de primera intervención y los transeúntes.

El éxito de un asalto depende de varios factores, entre ellos: las características del cajero automático, la organización del ataque y la experiencia y los conocimientos de los autores.

2.1 Vulnerabilidad de los cajeros automáticos

Los cajeros automáticos más vulnerables son los situados en el exterior (en la pared) o los que están dentro de edificios. Para atacar un cajero automático (independiente) situado dentro de un edificio, los GDO prefieren los cajeros situados en locales comerciales a los que se encuentran dentro de una oficina bancaria, donde la vigilancia suele ser más fuerte. Los bancos operan principalmente cajeros automáticos ubicados dentro o fuera de una oficina bancaria. Las ubicaciones remotas de los bancos, en la calle o en locales comerciales como gasolineras, supermercados, hoteles, casinos, aeropuertos, etc., se están volviendo cada vez más importantes con el cierre de las sucursales bancarias. Los proveedores independientes operan cajeros automáticos como servicio independiente. Sus cajeros suelen estar situados en comercios, lugares de hostelería y ocio, lugares de transporte (estaciones de ferrocarril, aeropuertos, etc.), edificios públicos y en la calle.

Con la creciente popularidad de la banca electrónica, es probable que muchas sucursales bancarias se cierren en los próximos años, lo que provocará una disminución general del número de cajeros automáticos. ([1]) Sin embargo, esto podría suponer un aumento del número de cajeros automáticos en ubicaciones remotas de bancos y de cajeros automáticos de proveedores independientes situados en lugares más vulnerables.

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

2.2 Organización de un ataque a un cajero automático

La preparación de un ataque puede llevar hasta varias semanas o incluso meses. Los delincuentes necesitan reunir los **instrumentos y recursos** necesarios, como vehículos, equipamiento y puntos de contacto. Los **vehículos** son una herramienta esencial para los asaltos a cajeros automáticos; los autores viajan principalmente en coche y después del ataque suelen escapar con vehículos rápidos. Estos a menudo son robados, pero también pueden ser alquilados o comprados (por ejemplo a través de Internet). La mayor parte del **equipamiento** para los asaltos a cajeros automáticos está disponible legalmente en tiendas normales. Esto reduce aún más el umbral para entrar en esta área de delincuencia. Rastrear el origen de un instrumento es difícil para los organismos de aplicación de la ley, por lo que los riesgos para los autores son limitados. Los GDO activos en asaltos a cajeros automáticos a nivel internacional casi siempre tienen puntos de contacto en el país objetivo (personas que residen allí durante un determinado período) o, alternativamente, pueden utilizar una técnica de ataque y fuga. Estos contactos apoyan a los GDO con logística como alquilar un alojamiento, conseguir un vehículo u otro equipamiento y explorar objetivos. Algunos delincuentes internacionales dejan la logística y la exploración totalmente en manos de los contactos locales y sólo viajan por carretera o por aire para la ejecución del ataque al cajero automático.

Los GDO suelen realizar una **exploración** exhaustiva para identificar objetivos adecuados y evaluar la hora del día a la que se llena el cajero, los alrededores, los detalles técnicos del cajero, las rutas de escape y las medidas de seguridad presentes, como sistemas de videovigilancia, sensores de alarma y persianas.

Algunos GDO toman una serie de medidas para **obstaculizar el trabajo de las fuerzas del orden y los servicios de seguridad** antes del ataque. Alteran los sistemas de alarma y el alumbrado público, utilizan técnicas de desviación, establecen bloqueos de carreteras o intentan alterar los vehículos de las fuerzas del orden.

2.3 La experiencia y los conocimientos de los autores

Los asaltos a cajeros automáticos son atractivos para los delincuentes porque el dinero está disponible de inmediato y no hay necesidad de una amplia red para vender los bienes robados. Es

una alternativa cómoda para los delincuentes que ya están activos en la delincuencia organizada contra la propiedad.

Los GDO deben reunir la **pericia y los conocimientos necesarios**, ya que son un factor determinante para el éxito o el fracaso de un ataque. La pericia y los conocimientos necesarios dependen en gran medida del **tipo de ataque**. Los ataques que consisten en arrancar/empotrar *in situ* tienen un modus operandi sencillo (principalmente la audacia y el uso de la fuerza bruta), por lo que generalmente no requieren habilidades específicas. Los ataques con gas combustible o con explosivos sólidos requieren un mayor nivel de pericia.

Los atacantes muestran diferentes **niveles de competencia**. Por un lado, los grupos altamente organizados y experimentados pueden ejecutar un asalto a un cajero automático con éxito en cuestión de minutos. Tienen el proceso controlado y son capaces de limitar el riesgo para sí mismos, limitando así también los daños colaterales. Por otro lado, los grupos menos organizados y más oportunistas a menudo fracasan en sus intentos y pueden causar daños importantes a los locales y edificios del barrio. Se cree que algunos de los GDO menos organizados vuelven a las actividades tradicionales de delincuencia organizada contra la propiedad, desalentados por las medidas preventivas que no son capaces de sortear en los ataques a cajeros automáticos.

3 Necesidad de un enfoque preventivo

Los países en los que los autores experimentan bajas tasas de éxito en los asaltos a cajeros automáticos o en los que el número de asaltos a cajeros automáticos está disminuyendo ilustran que un enfoque exitoso para contrarrestar los asaltos a cajeros automáticos consiste en una combinación de medidas operativas y preventivas. Dado que el número de GDO activos en esta área de delincuencia es limitado, la detención y el consiguiente castigo de miembros de los GDO reduce significativamente el número de ataques. Sin embargo, una vez liberados, muchos atacantes de cajeros automáticos retoman sus actividades. Además, a veces un grupo es capaz de reemplazar rápidamente al autor detenido. Por esta razón, hay una gran necesidad de medidas preventivas, preferiblemente integradas en un marco legislativo. Además, la experiencia demuestra que las medidas de prevención en un país pueden conducir a los GDO hacia objetivos más vulnerables en otros países. Es sólo cuestión de tiempo que los modus operandi que surgen en un país se extiendan a otros países. Esto indica claramente la **necesidad de adoptar las medidas preventivas y operativas a nivel europeo** con la estrecha colaboración de los socios privados, públicos y de las fuerzas del orden.

4 Prevención

Para prevenir y abordar este tipo de delito se necesita una estrategia clara. En este capítulo explicaremos los tres pasos que generalmente se dan en caso de enfrentarse a asaltos a cajeros automáticos o en la preparación de su prevención.

En primer lugar, la **evaluación de la situación**; se debe establecer un perfil de riesgo de los cajeros automáticos y sus alrededores, teniendo en cuenta la cantidad de efectivo disponible (posible botín), el riesgo de daños colaterales y el riesgo de lesiones personales. En segundo lugar, sobre la base de la evaluación de los riesgos, se debe elaborar una **estrategia preventiva**. Por último, deben aplicarse las **medidas preventivas**.

4.1 Evaluar la situación

Los GDO tienden a dirigirse a tipos específicos de cajeros automáticos o a cajeros automáticos de proveedores específicos con características que facilitan el ataque. Por este motivo, es necesario realizar una evaluación exhaustiva del riesgo de asaltos a cajeros automáticos, preferiblemente incluyendo toda la cadena de seguridad del efectivo, desde el tránsito hasta la entrega y el almacenamiento en el cajero. Para establecer el perfil de riesgo de cada cajero automático se deben analizar una serie de elementos, entre los que se encuentran los siguientes.

- Las características de la ubicación y los alrededores del cajero; características como la ubicación en la ciudad o en el campo, la densidad de población, la proximidad de comisarías de policía, las cámaras de reconocimiento automático de matrículas (ANPR) en el vecindario, los sistemas de videovigilancia en las proximidades, etc.
- La ubicación del cajero automático:
    - dentro o fuera de un edificio, en una sucursal bancaria o en una ubicación remota (por ejemplo un local comercial), incorporado en un edificio o montado contra la pared,
    - en el caso de un cajero independiente: si está anclado o no,
    - para cajeros incorporados en o montados contra un edificio: si hay debilidades arquitectónicas, cómo está organizado el almacenamiento de efectivo, etc.
- El tipo de cajero automático.
- Las funciones de seguridad incluidas en el cajero automático.
- La cantidad de efectivo en el cajero automático.

- El tipo de asalto y el modus operandi que se puede esperar para adoptar primero las medidas preventivas más adecuadas.
- Las medidas de seguridad y prevención ya adoptadas (sistemas inteligentes de neutralización de billetes (IBNS), sistemas de videovigilancia, sistemas de niebla de seguridad (reducción de la visibilidad), etc.).

Otros elementos que deben evaluarse son el estado de la cooperación con los socios y los interesados y la legislación. Debería evaluarse la colaboración entre los organismos de aplicación de la ley y los socios privados y públicos para crear alianzas para luchar contra la delincuencia. Es posible que cada socio posea información interesante para contribuir a la evaluación de la situación. La policía local o las autoridades locales son particularmente importantes en este contexto. La legislación debe evaluarse en términos de establecer un marco legal para la prevención, tomar medidas preventivas obligatorias, penas por ataques a cajeros automáticos, etc.

4.2 Desarrollar un enfoque preventivo

Una vez que se haya evaluado la situación y se hayan determinado las principales áreas de riesgo y los puntos fuertes y débiles de la seguridad de los cajeros automáticos, se podrá elaborar una estrategia (a menudo basada en la colaboración entre los sectores público y privado) y se podrán establecer contramedidas preventivas y operativas. Las medidas de prevención deben tener por objeto reducir la intención y la capacidad de los autores. Para lograr esto, se proponen tres ejes de acciones preventivas basadas en tres de las cinco estrategias de prevención del delito situacional de Clarke ([2]): reducir las recompensas, aumentar el riesgo para los autores y aumentar el esfuerzo para acceder al botín.

Los delincuentes hacen un balance del rendimiento esperado y los riesgos asociados (por ejemplo de un ataque a un cajero automático). Reduciendo las posibilidades de obtener una recompensa fácil y aumentando el riesgo para los autores se disminuyen sus expectativas y su deseo de participar en un asalto a un cajero. Otras medidas que aumentan el esfuerzo necesario para acceder al cajero automático afectan a la capacidad de los autores. Los delincuentes oportunistas, que a menudo fracasan en sus intentos, dejan de participar en ataques a cajeros automáticos. En el caso de los

([2]) Derek Cornish y 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.

atacantes de cajeros profesionales, la tasa de éxito se reduce, lo cual a su vez afecta el balance entre rendimiento y riesgo.

Además, la estrategia preventiva se completa con medidas paralelas, como una estrategia eficaz de medios de comunicación, la prevención social temprana y medidas para reducir el riesgo de daños colaterales a los edificios y garantizar la seguridad de los residentes locales, las unidades de primera intervención y los transeúntes.

Hay otras formas posibles de estructurar el enfoque. En los Países Bajos, las autoridades aplican el llamado modelo de barreras ([3]). Este modelo identifica los pasos que un delincuente tiene que dar para cometer un delito. También identifica los socios y las oportunidades que permiten el delito y es un instrumento útil para organizar el proceso de recopilación de información sobre el área de delincuencia. Identificando cada paso necesario para ejecutar un asalto a un cajero se pueden identificar las barreras para obstaculizar el delito y los mejores socios para establecer las barreras. El modelo de barreras también identifica señales para alertar a los socios públicos y privados sobre los asaltos a cajeros automáticos y señales que pueden enviar ellos mismos para notificar sus sospechas a las autoridades.

Se necesita una estrategia bien desarrollada para mitigar los riesgos asociados al refuerzo de la prevención. Las medidas preventivas que son muy eficaces para desalentar a los aficionados y a los imitadores a veces tienen efectos indeseados. Algunos grupos recurren a métodos de ensayo y error para encontrar cajeros automáticos vulnerables, dejando un rastro de cajeros dañados. Los GDO más peligrosos y despiadados empiezan a usar modus operandi más violentos, como pasar de explosivos de gas a explosivos sólidos en sus ataques.

Para establecer un conjunto eficiente de medidas preventivas, la instalación de una autoridad nacional que tenga la facultad de imponer medidas específicas para los cajeros automáticos de alto riesgo en base a un análisis exhaustivo de la situación es una mejor práctica. Este enfoque ha demostrado su eficacia en Francia y es especialmente eficaz cuando se establece un marco jurídico y las medidas se aplican junto con medidas operativas.

([3]) Centro holandés para la Prevención del Delito y la Seguridad, Barrièremodellen, www.barrieremodellen.nl

4.3 Aplicar medidas preventivas

Las medidas presentadas en este capítulo para prevenir asaltos a cajeros automáticos han demostrado su utilidad en varios países. Se basan en las conclusiones de la conferencia sobre la prevención y en las medidas preventivas promovidas activamente por las organizaciones internacionales que trabajan en la seguridad de los cajeros automáticos. Muchas medidas son bien conocidas. Varios países ya han aplicado algunas medidas con éxito. Sin embargo, a menudo las medidas propuestas sólo se aplican parcialmente y no se incorporan a la legislación.

Como ya se ha mencionado, se proponen tres ejes de acciones preventivas: reducir las recompensas, aumentar el riesgo para los autores y aumentar el esfuerzo necesario para acceder al botín.

4.3.1 Reducir las recompensas

La reducción de las recompensas de los actos delictivos es el primer eje para prevenir los asaltos a cajeros automáticos. Mientras persista la percepción del «dinero fácil», los delincuentes se dedicarán a este tipo de delitos. La reducción de la cantidad de efectivo disponible y la retirada o destrucción del dinero reducen las posibilidades de que haya un botín interesante. La reducción de las expectativas disminuye el deseo del delincuente de participar en este tipo de delito.

4.3.1.1 *Reducir la cantidad de efectivo*

Una medida para reducir la recompensa es reducir la cantidad de dinero disponible en un cajero automático. Lo ideal sería que esta cantidad se limitara a la necesaria para un solo día de negocio. La colaboración entre los bancos podría garantizar una buena relación coste-eficacia. En los Países Bajos, varios bancos han colaborado para establecer una red de cajeros automáticos independiente de los bancos, llamada «Geldmaat». El objetivo de la colaboración es garantizar la disponibilidad, accesibilidad, asequibilidad y seguridad del dinero en efectivo. Esto probablemente llevará a una reducción en el número de cajeros automáticos. Sin embargo, cada cajero automático no contendrá más dinero, sino que se llenará más a menudo. El número de veces que se llena se adaptará a la necesidad.

Dado que los delincuentes realizan sus ataques a cajeros automáticos mayormente entre las 3 y las 4 de la madrugada, se recomienda encarecidamente que los cajeros automáticos independientes

(situados sobre todo en locales comerciales y lugares públicos, que son más vulnerables) se vacíen al final del día, trasladando el dinero a una caja fuerte. Una señal de advertencia podría informar al público de que el cajero automático no tiene efectivo por la noche. Al día siguiente, el cajero debe llenarse fuera de la vista de los clientes y con el local cerrado. Este sistema se aplica en Francia, donde la legislación obliga a los minoristas que tienen un cajero automático independiente en la tienda a sacar el dinero por la noche y dejar el cajero abierto. Para otros cajeros automáticos, las cantidades disponibles pueden reducirse aumentando la frecuencia de llenado.

4.3.1.2 *Estropear el botín y hacer que el dinero sea rastreable*

Los sistemas inteligentes de neutralización de billetes (IBNS) son una primera técnica para estropear las recompensas. Estos sistemas manchan los billetes con tinta para marcarlos como robados. Se pueden añadir trazadores y marcadores a la tinta del IBNS. En la actualidad, estos marcadores se utilizan principalmente con fines forenses, vinculando el billete al lugar del delito y aumentando el riesgo de que los autores sean capturados. Aunque los IBNS son una medida preventiva efectiva, hay algunas consideraciones.

El Banco Central Europeo no reembolsa los billetes manchados ([4]) (desde 2003), pero varios de los bancos centrales nacionales de los Estados miembros de la UE siguen haciéndolo. Los billetes manchados también se vuelven a introducir en el sistema legal a través de los casinos. Un IBNS crea un obstáculo adicional para los delincuentes, pero sería mucho más eficaz si fuera imposible que los delincuentes utilizaran billetes manchados en la UE. Para conseguir esto, los billetes manchados no deberían ser aceptados por los bancos centrales nacionales. Se pueden hacer excepciones en circunstancias específicas, por ejemplo para billetes manchados durante una activación en falso. También es importante aconsejar a la población que no acepte billetes manchados. Más a largo plazo, los lectores de billetes deberían detectar los billetes manchados e instalarse en bancos y en locales comerciales como casinos, lavaderos de coches, etc. La detección de la tinta es difícil y costosa; sin embargo, una solución rentable podría ser la instalación de sistemas de infrarrojos que detecten los billetes manchados con marcadores infrarrojos. Estos sistemas han demostrado su eficacia y son mejor práctica en Bélgica y Francia. Cuando se introducen billetes marcados con marcadores infrarrojos en el cajero automático, éste aceptará («tragará») el dinero pero no lo acreditará en una cuenta. La persona que introduce los billetes manchados también debería ser registrada.

([4]) Banco Central Europeo, Decisión del Banco Central Europeo sobre las denominaciones, especificaciones, reproducción, canje y retirada de los billetes en euros, 2003.

Hay algunas otras consideraciones al instalar soluciones IBNS. Varios fabricantes ofrecen diferentes soluciones IBNS con diferentes mecanismos de activación y diferentes tipos de tinta. Una primera consideración se refiere al hecho de que no todos los tipos de tecnologías de activación del IBNS son capaces de contrarrestar todas las amenazas. Algunos IBNS funcionan muy bien para ataques que consisten en arrancar/empotrar, ataques *in situ* y ataques con gas, pero no funcionan en caso de un ataque con explosivos sólidos, o viceversa. Por lo tanto, se debe estudiar cuidadosamente la tecnología a elegir.
Otra consideración es el tipo de tinta a elegir. En Bélgica se establecen requisitos mínimos nacionales para el IBNS (seguridad, porcentaje de manchado, no lavable, etc.) y pruebas independientes certifican que el sistema cumple las normas nacionales y funciona de acuerdo con las afirmaciones del fabricante. Es importante hacer pruebas con billetes reales porque hay tintas más baratas en el mercado que funcionan bien con los billetes falsos pero no con los reales, es decir que la tinta puede eliminarse de los billetes auténticos lavándolos. Además, se recomienda añadir un marcador forense a la tinta, lo que permite investigar la relación entre los billetes manchados y un lugar del delito específico.

Las mejores prácticas demuestran que el IBNS puede ser muy eficaz, especialmente en combinación con otras medidas preventivas. En 2015 Francia introdujo una nueva legislación que incluía artículos sobre la instalación de IBNS y el uso de tinta con un ADN único. Es la policía militar francesa (gendarmería) la que, sobre la base de una evaluación de riesgos, decide dónde hay que aplicar el IBNS y otras medidas. Desde que la nueva legislación reforzó el enfoque preventivo y operativo, el número de ataques disminuyó de 300 en 2013 a 50 en 2018.

Otra técnica que se está desarrollando para estropear el botín es el uso de **pegamento**. La eficacia del pegamento se ha demostrado en los Países Bajos, pero por ahora el coste de su introducción y uso es alto. Además, el pegamento puede ser un peligro de incendio si el sistema no se activa antes de un ataque, ya que la dispersión de las partículas de pegamento en el aire podría producir una mezcla combustible. Este método no está listo para el mercado todavía, pero podría ser una solución para el futuro.

4.3.2 Aumentar el riesgo

Un segundo eje para la prevención de los asaltos a cajeros automáticos es disuadir a los posibles autores de cometer delitos aumentando el riesgo de detección y castigo. Además del riesgo de lesiones físicas cuando se utilizan explosivos en ataques a cajeros automáticos, el principal riesgo para un delincuente es una sentencia de prisión cuando es sorprendido en el acto («in fraganti») o detenido después de una investigación. Para reducir el deseo de los posibles autores, es preciso aumentar el riesgo de detección y castigo. Para la sociedad, atrapar y condenar a los delincuentes es, por supuesto, también un método de prevención muy eficaz si hay un castigo posterior, como hemos visto en varios países.

4.3.2.1 *Compartir información*

Para detectar y castigar a los atacantes de cajeros automáticos es fundamental el intercambio de información entre todos los interesados en la lucha contra los asaltos a cajeros, incluidos los proveedores de cajeros automáticos, las autoridades encargadas de hacer cumplir la ley (policía, fiscal, etc.), las autoridades públicas, los fabricantes tanto de cajeros como de dispositivos de seguridad y protección, las asociaciones profesionales, los proveedores de cajeros automáticos (bancos y proveedores independientes), las empresas de seguridad y las centrales de alarma. Idealmente, esto debería hacerse tanto a nivel nacional como a nivel internacional.

La detección temprana de un inminente asalto a un cajero es difícil. La detección temprana sólo es posible cuando existe un intercambio de información casi perfecto a nivel internacional entre los socios encargados de hacer cumplir la ley y los socios privados (empresas de seguridad y proveedores de cajeros automáticos). Es preciso vigilar una amplia gama de indicadores, entre ellos los mensajes de alerta temprana entre los organismos encargados de hacer cumplir la ley sobre los movimientos de los GDO, la información sobre los vehículos («calientes») que se han utilizado en ataques a cajeros automáticos, la información de las empresas de seguridad o las patrullas vecinales sobre comportamientos sospechosos detectados en la zona que rodea el cajero, las transacciones sospechosas detectadas por los proveedores de cajeros automáticos y otros métodos de detección. Otras posibles medidas policiales para la detección temprana son la vigilancia de coches robados, fabricantes y distribuidores de explosivos y empresas autorizadas a utilizar explosivos. Los esfuerzos necesarios para lograr una detección temprana son exigentes y no tienen ninguna garantía de éxito, por lo que las intervenciones de las fuerzas del orden antes de un ataque son poco frecuentes.

Si no es posible una detección temprana, las centrales de alarma pueden emitir un aviso rápidamente en caso de un asalto a un cajero. A fin de permitir la intervención, es preciso acordar y establecer reglamentos y protocolos nacionales para la comunicación rápida entre las centrales de alarma y las fuerzas del orden. En caso de detección temprana o de información en tiempo real, las fuerzas del orden siempre tendrán que evaluar el momento y la mejor oportunidad de intervención. Sorprender a los delincuentes in fraganti es muy difícil y puede llevar a situaciones peligrosas porque algunos GDO son muy violentos y usan armas pesadas.

Para que la investigación tras un asalto a un cajero tenga éxito, los agentes de la ley tienen que comunicarse con todas las partes interesadas, ya que cualquiera de ellas puede tener información que contribuya al éxito de una investigación. Por supuesto, es necesaria la comunicación y la colaboración con las víctimas primarias, los bancos u otros proveedores de cajeros automáticos: ellos tienen acceso a datos que son importantes para la investigación. Al proveedor del cajero automático la información de las fuerzas del orden le sirve de ayuda para mejorar las medidas de prevención. Además, resultan útiles los contactos con las asociaciones profesionales y los fabricantes: a menudo envían mensajes de alerta de seguridad a los que pueden suscribirse otros interesados. Los fabricantes de cajeros tienen una buena visión general de los diferentes tipos de ataques a cajeros automáticos y de las debilidades y fortalezas de las medidas preventivas en cada caso. Están muy dispuestos a dar apoyo a la policía con información sobre los aspectos técnicos de los cajeros automáticos y los modus operandi utilizados.

La cooperación transfronteriza es esencial: los países deben compartir información (sobre sospechosos, atacantes de cajeros automáticos condenados, modus operandi, vehículos sospechosos, imágenes de ataques, etc.), no sólo en apoyo de la investigación sino también porque los sospechosos condenados en otro país pueden ser condenados por reincidencia.

Por último, la creación de una base de datos a nivel europeo, a disposición de los organismos encargados de hacer cumplir la ley y que contenga datos forenses (por ejemplo sobre diferentes tipos de tintas, trazadores y marcadores usados en los IBNS o sobre cristales de protección de cajeros automáticos), podría apoyar fuertemente las investigaciones y vincular a los sospechosos a un lugar del delito concreto. La normalización de las tecnologías a nivel internacional suele ser insuficiente: durante la conferencia de enero de 2019 los participantes mencionaron que la normalización a nivel de la UE de la tinta y las etiquetas usadas para marcar delitos podría facilitar en gran medida las investigaciones.

4.3.2.2 *Videovigilancia y dispositivos de escucha*

Las imágenes y el sonido grabados por los sistemas de videovigilancia y los dispositivos de escucha pueden servir de apoyo tanto para la detección en tiempo real de un ataque (por ejemplo para evitar daños físicos a las unidades de primera intervención que lleguen al lugar del delito) como para las investigaciones posteriores (por ejemplo para identificar a los autores y su modus operandi). Las imágenes del sistema de videovigilancia pueden combinarse con las imágenes de sistemas de videovigilancia públicos y de otros sistemas de videovigilancia en las proximidades del cajero y con las imágenes del radar de tráfico para proporcionar una imagen más completa de los autores y su modus operandi.

Sin embargo, las imágenes de los sistemas de videovigilancia suelen ser de mala calidad o mal almacenadas. Las imágenes deben ser de calidad suficiente para permitir la identificación de una persona. Una vez más, el establecimiento de normas europeas para los sistemas de videovigilancia facilitaría las investigaciones. Además, dado que los delincuentes a menudo desactivan las cámaras de vigilancia antes de un ataque, también podría considerarse la instalación de cámaras de vigilancia ocultas o de dispositivos de escucha en tiempo real.

4.3.2.3 *Castigo y rehabilitación del delincuente*

El castigo consecuente y severo demuestra tener un efecto preventivo. La detención de un GDO tiene un efecto inmediato en el número de ataques a cajeros automáticos. Sin embargo, la salida de prisión de atacantes de cajeros también suele provocar una nueva oleada de ataques. Esto significa que las sentencias cortas llevan a los delincuentes a volver a actuar muy rápidamente. Las penas mínimas y máximas para los delincuentes condenados por cada tipo de asalto a un cajero varían entre los Estados miembros. Algunos creen que las penas más altas disuadirán a los posibles autores. Sin embargo, las investigaciones científicas ([5]) demuestran que el aumento de la severidad de las sentencias no aumenta necesariamente el efecto disuasorio. Por lo tanto, podría ser interesante estudiar los programas de rehabilitación (centrados en el delincuente) para reducir la alta reincidencia.

([5]) David Weisburd, David P. Farrington y Charlotte Gill, «Conclusion: What Works in Crime Prevention Revisited», David Weisburd, David P. Farrington y Charlotte Gill, *What works in Crime Prevention and Rehabilitation*. Cambridge: Springer, 2016, 311.

4.3.3 Aumentar el esfuerzo

El tercer eje para prevenir los asaltos a cajeros contiene acciones que hacen que sea más difícil para un delincuente llevar a cabo el acto delictivo.

4.3.3.1 *Garantizar un entorno resistente a la delincuencia*

Si la evaluación del riesgo (véase más arriba) muestra que un cajero automático está situado en un entorno de alto riesgo, la ubicación debe ser desmantelada y el cajero trasladado a una zona de riesgo bajo o medio. Este es el caso, sin duda, cuando el análisis muestra que el edificio podría derrumbarse en caso de un ataque a un cajero con explosivos. Se podrían aplicar leyes para hacer cumplir este tipo de medidas en los casos de alto riesgo. Además de reducir el número de cajeros automáticos en los entornos de alto riesgo, se debería fomentar el pago sin efectivo para reducir la necesidad de cajeros automáticos.

Si no es posible trasladar el cajero automático, deben adoptarse las máximas medidas de seguridad: por ejemplo el uso de bolardos anti-alunizaje, farolas y otro mobiliario urbano para restringir el acceso al edificio, sistemas de detención de vehículos, la instalación de un alumbrado público adecuado, el aumento de la vigilancia visible u oculta y dispositivos antirrobo, como un sistema de degradación de billetes. Cuando una ubicación en una zona que no se ha identificado como de alto riesgo es atacada, debe identificarse como tal y deben aplicarse medidas de seguridad adicionales. Los elementos nuevos deben tenerse en cuenta en el instrumento de evaluación de riesgos para actualizarlo. La reevaluación de este riesgo debería ser una acción recurrente.

4.3.3.2 *Reforzar los cajeros automáticos*

Los fabricantes de cajeros automáticos ofrecen una gama estándar de cajeros automáticos que tienen una serie de características de seguridad que están clasificadas según los grados de seguridad del Comité Europeo de Normalización (CEN). Generalmente los cajeros automáticos tienen un clasificación CEN que va desde el grado más bajo CEN1 hasta el más alto, CEN4. Características como la fuerza de la estructura y la resistencia a los ataques determinan el grado. La resistencia al gas se suele ofrecer como una opción (CEN-GAS). Los modelos estándar pueden mejorarse con medidas de protección adicionales. Por lo general, terceros instalan estas características para garantizar el cumplimiento de la legislación local y el ajuste del modelo básico a los requisitos de los clientes

locales. Las características de seguridad adicionales incluyen varios sensores para activar un sistema de neutralización de gas o IBNS en caso de un ataque *in situ* o con explosivos y persianas y cerraduras de caja fuerte mejoradas para evitar el acceso no autorizado a la caja fuerte cuando la persiana principal está dañada. Para los cajeros automáticos portátiles e independientes es importante utilizar sistemas de anclaje que ofrezcan una protección adicional contra los ataques que consisten en arrancar/empotrar. Se pueden incluir sistemas de rastreo en el cajero automático para ayudar a los investigadores cuando el cajero se traslada a otro lugar antes de abrirlo.

4.3.3.3 *Medidas arquitectónicas*

Cuando se instala un cajero automático se sugiere usar máquinas de acceso trasero. De esta manera el delincuente tiene que entrar en el edificio y acceder a la parte trasera de la máquina para robar el dinero. Los cajeros portátiles e independientes son los más vulnerables. Una reducción del número de estos cajeros aumentaría la seguridad. La obligación de instalar los cajeros automáticos en una sala a prueba de ladrones disminuiría automáticamente el uso de cajeros independientes.

4.3.3.4 *Sistema de niebla*

Un generador de niebla llena una espacio rápidamente con una densa niebla, por lo que el intruso no puede ver nada. Esta niebla de seguridad a menudo hace imposible ejecutar el ataque al cajero automático. Como mínimo, el sistema hace que el delincuente actúe más despacio, lo que da más tiempo a los servicios de policía para intervenir. El sistema de niebla de seguridad está conectado al sistema de alarma y puede ser activado de dos maneras. Puede ser activado automáticamente por sensores de alarma como los detectores de movimiento (por la noche) o sensores de manipulación de las persianas del cajero. También puede ser activado por una central de alarma para evitar un exceso de falsas alarmas. En los cajeros exteriores, el sistema de niebla puede aplicarse en la parte trasera del cajero para llenar el espacio de niebla y reducir la visibilidad de los delincuentes a cero.

Los sistemas de niebla pueden proporcionar una protección puntual para un cajero automático ubicado en espacios abiertos en gasolineras, supermercados, etc. Esto evita que la niebla llene toda la zona. La protección con niebla tiene más éxito cuando la niebla viene de diferentes ángulos o cuando llena el espacio detrás del cajero automático en el caso de un ataque que consiste en empotrar. Se están realizando pruebas para ver si los generadores de niebla pueden instalarse

dentro del propio cajero automático en lugar de en el espacio donde se encuentra el cajero. A la niebla se pueden añadir marcadores de ADN que manchan a los delincuentes y su ropa.

4.3.4 Medidas paralelas

Para garantizar la aplicación eficiente y eficaz de las medidas preventivas mencionadas, es preciso considerar una serie de medidas paralelas. Estas medidas son indispensables para permitir o reforzar un enfoque preventivo y operativo integral para hacer frente a los asaltos a cajeros automáticos.

4.3.4.1 *Legislación*

En varios países la legislación obliga a los proveedores de cajeros automáticos a adoptar medidas preventivas. En otros países, el establecimiento de pactos y acuerdos entre los bancos y los organismos encargados de hacer cumplir la ley garantiza un enfoque bien organizado para hacer frente a los asaltos a cajeros automáticos. Se pueden considerar medidas de reglamentación en los siguientes ámbitos (entre otros):

- la incorporación de medidas preventivas;
- marcos jurídicos que permitan la colaboración entre los organismos de aplicación de la ley y los socios públicos y privados;
- una revisión de las penas aplicadas a los autores de asaltos a cajeros si estas son demasiado bajas.

Sin embargo, a menudo sólo las instituciones bancarias están obligadas a cumplir con estas leyes o acuerdos y estos no vinculan a los proveedores independientes de cajeros automáticos. Este es un punto débil habitual en un marco reglamentario.

Algunos países no aplican ninguna reglamentación, pero tratan de persuadir a los proveedores de cajeros automáticos de adoptar medidas preventivas mediante la sensibilización sobre las áreas de delincuencia y las tendencias. En los países con un gran número de bancos independientes esto resulta particularmente difícil.

Es fundamental asegurar que la aplicación efectiva de las medidas preventivas incluya cambios en la legislación y la reglamentación, tanto a nivel nacional como internacional, que vinculen a todos los tipos de proveedores de cajeros automáticos. Lo ideal sería que la legislación se armonizara a nivel

de la UE para evitar que las fuertes medidas preventivas incorporadas en la legislación de un país lleven a los GDO a otros países con una reglamentación menos estricta.

4.3.4.2 *Estrategia de medios de comunicación*

Otro eje importante de la estrategia preventiva es una sólida estrategia de medios de comunicación que tiene por objeto disminuir las expectativas y el deseo de los atacantes de cajeros automáticos de participar en este delito. Se deben destacar las bajas tasas de éxito y los altos riesgos para los autores y evitar comunicar información sobre las recompensas («botín») o detalles sobre los ataques, como el tipo de cajero afectado o el modus operandi. Por otra parte, es necesario que se comuniquen ampliamente las detenciones de sospechosos y el consiguiente castigo después de una condena.

4.3.4.3 *Colaboración mejorada*

Se ha mencionado mucho la mejora de la colaboración y el intercambio de información, pero no se puede insistir lo suficiente en ello. El intercambio de información operativa a nivel internacional es la actividad principal de Europol. Además de este intercambio de información, la conferencia sobre prevención mostró la clara necesidad de aumentar la cooperación multidisciplinaria y a varios niveles y el intercambio de información entre todos los interesados pertinentes, incluidos los organismos encargados de hacer cumplir la ley, las autoridades públicas, los fabricantes de cajeros automáticos y de dispositivos de seguridad y protección, las asociaciones profesionales, los proveedores de cajeros automáticos (bancos y proveedores independientes), las empresas de seguridad y las centrales de alarma. Esto debe incluir el nivel local, nacional e internacional.

4.3.4.4 *Reducir el riesgo de daños colaterales*

En caso de ataques con explosivos sólidos, algunos GDO dejarán material. Esto puede crear situaciones peligrosas para las unidades de primera intervención o ciudadanos (ya sean residentes o transeúntes). Su seguridad debe ser garantizada. Como es el caso en Bélgica, es preciso elaborar y armonizar los protocolos y procedimientos que han de seguir las unidades de primera intervención (tanto las de los organismos de aplicación de la ley como las de los proveedores de los cajeros automáticos). Otra buena práctica en este contexto es el ejemplo de los Países Bajos, donde se utiliza la grabación del sistema de videovigilancia del ataque al cajero para evaluar la situación. Se pueden

establecer acuerdos con las centrales de alarma para que estas imágenes estén disponibles de forma inmediata.

4.3.4.5 *Prevención social*

A menudo los GDO buscan jóvenes para reclutarlos. Se podrían establecer proyectos para frustrar estos procesos de reclutamiento en una etapa temprana. La policía o los trabajadores sociales deberían estar atentos a estos procesos y podrían intervenir acercándose personalmente a los potenciales delincuentes.

5 Conclusiones

En los últimos 2 años, el número de países europeos afectados por asaltos a cajeros automáticos ha aumentado. En este contexto, Europol y la REPD han trabajado juntos para reunir las mejores medidas para combatir y prevenir este delito.

Un enfoque exitoso para contrarrestar los asaltos a cajeros automáticos consiste en una combinación de medidas operativas y preventivas, preferiblemente integradas en un marco legislativo. A fin de evitar que unas medidas contundentes en un país empujen a los GDO hacia países más vulnerables, se recomienda adoptar estas medidas a nivel europeo.

Para prevenir y hacer frente a este tipo de delito se debe establecer una estrategia clara en tres etapas: la evaluación de la situación, la elaboración de un enfoque preventivo basado en la evaluación de los riesgos y la aplicación de las medidas preventivas.

La evaluación de riesgos de asaltos a cajeros automáticos debe incluir las características del cajero y sus alrededores, la cooperación con los socios y las partes interesadas para crear alianzas para combatir este delito y la evaluación del marco preventivo y jurídico. Una vez evaluada la situación, se debe establecer una estrategia basada en la colaboración entre los sectores público y privado y en la adopción de contramedidas preventivas y operativas. El objetivo de las medidas preventivas es reducir la intención y la capacidad del delincuente de participar en un asalto a un cajero automático. Para lograr esto, se proponen tres ejes de acciones preventivas: reducir las recompensas, aumentar el riesgo y aumentar el esfuerzo. Unas medidas paralelas deben completar la estrategia preventiva. La instalación de una autoridad nacional que tenga la facultad de imponer estas medidas necesarias es buena práctica.

Al **reducir las recompensas**, el deseo del delincuente de cometer este tipo de delito disminuye. Reducir la cantidad de efectivo en los cajeros automáticos limitándola a la necesaria para un solo día de negocio, o vaciar los cajeros automáticos (más vulnerables) por la noche, es una medida para reducir las expectativas del delincuente. Otro método es estropear el botín y hacer que el dinero sea rastreable. En este contexto, se puede aplicar el sistema IBNS, que mancha los billetes y los marca como robados. Este método es más eficaz cuando les es imposible a los delincuentes gastar este dinero o reintroducir los billetes en el sistema de efectivo legal. Esto puede lograrse si los bancos y el público no aceptan billetes manchados para el pago y si se instalan lectores de billetes que puedan detectar y rechazar los billetes manchados. A este respecto, la inversión en sistemas de infrarrojos que detectan los billetes manchados con marcadores infrarrojos ha demostrado ser una solución rentable en Bélgica y Francia. Al instalar sistemas IBNS, los países deben considerar detenidamente

los mecanismos de activación elegidos, los requisitos mínimos para la neutralización de los billetes y la adición de un marcador forense a la tinta.

Las medidas que disuaden a los posibles autores de cometer delitos porque **aumentan el riesgo** de detección y castigo son el segundo eje para la prevención de asaltos a cajeros automáticos. La recopilación y el intercambio de información entre todas las partes interesadas, tanto a nivel nacional como internacional, es clave para la detección y el castigo de atacantes de cajeros automáticos. El intercambio de información obtenida de imágenes de alta calidad grabadas por los sistemas de videovigilancia y de datos de sonido puede aumentar las posibilidades de una detección temprana y una investigación exitosa. Para evitar que se desactiven las cámaras de vigilancia o los dispositivos de escucha antes del ataque, se puede considerar la instalación de cámaras de vigilancia ocultas o dispositivos de escucha en tiempo real. La creación de una base de datos forenses y la normalización de las tecnologías a nivel europeo podrían facilitar enormemente la cooperación y las investigaciones internacionales. Si los delincuentes son detenidos y condenados, podría ser interesante estudiar los programas de rehabilitación (centrados en el delincuente) para reducir la alta reincidencia.

El tercer eje para prevenir los asaltos a cajeros incluye medidas para **aumentar el esfuerzo** que necesita el delincuente para llevar a cabo el acto delictivo. La instalación de un cajero automático en un entorno resistente a la delincuencia con las máximas medidas de seguridad hará que sea más difícil para los delincuentes atacar un cajero automático. Además, la protección estándar de los cajeros automáticos puede mejorarse con una serie de características de seguridad adicionales. Además de estas medidas, la instalación de un sistema de niebla puede disuadir al delincuente o al menos ralentizar el ataque.

Una serie de **medidas paralelas** fortalecerá las medidas mencionadas, como la creación de un marco jurídico que obligue a todos los proveedores de cajeros automáticos a aplicar las medidas preventivas, la elaboración de una sólida estrategia de medios de comunicación, una colaboración mejorada a nivel local, nacional e internacional, directrices para las unidades de primera intervención a fin de reducir el riesgo de daños colaterales y la inversión en prevención social para socavar los procesos de reclutamiento de delincuentes.

6 Recomendaciones para un enfoque preventivo: resumen

Desarrollar una respuesta efectiva para prevenir los asaltos a cajeros automáticos

Evaluar la situación

Establezca el perfil de riesgo de los cajeros automáticos en su país/región.
Identifique a los socios y partes interesadas en la lucha contra los asaltos a cajeros automáticos y evalúe la colaboración.
Evalúe el marco jurídico para hacer frente a los asaltos a cajeros automáticos a nivel nacional e internacional.

Desarrollar un enfoque preventivo

Determine los (principales) riesgos a cubrir y las prioridades.
Determine las mejores medidas preventivas para cubrir estos riesgos considerando tres ejes principales.
Determine las medidas preventivas paralelas necesarias para reforzar las medidas preventivas adoptadas.

Medidas preventivas que pueden adoptarse para		
Reducir las recompensas	Aumentar el riesgo	Aumentar el esfuerzo
– Reducir la cantidad de efectivo. o Vaciar el cajero por la noche. o Aumentar la frecuencia de llenado. – Estropear el botín. o Sistemas inteligentes de neutralización de billetes (IBNS). o Marcadores infrarrojos en la tinta del IBNS para detectar billetes manchados mediante lectores de billetes. o En desarrollo: pegamento.	– Intercambio de información internacional para: o detección temprana o en tiempo real de un posible ataque a un cajero, o fortalecer el enfoque operativo, o condenar a los reincidentes, o intercambio de datos forenses a nivel europeo. – Videovigilancia y dispositivos de escucha. – Castigo consecuente y rehabilitación del delincuente.	– Garantizar un entorno resistente a la delincuencia. o Cambiar la ubicación de cajeros de alto riesgo. o Medidas de seguridad: obstáculos físicos, vigilancia, etc. – Reforzar los cajeros con persianas, resistentes al gas o a los explosivos sólidos, etc. – Medidas arquitectónicas, por ej. máquinas de acceso trasero. – Sistemas de niebla de seguridad.

Medidas paralelas para reforzar el enfoque preventivo

- Legislación eficaz que incluya medidas preventivas contra los asaltos a cajeros automáticos, condenas consecuentes, etc.
- Estrategia eficaz de medios de comunicación para desalentar a los autores.
- Colaboración mejorada entre todos los interesados (públicos, privados, fuerzas del orden) en la lucha contra los asaltos a cajeros automáticos.
- Reducir el riesgo de daños colaterales para las unidades de primera intervención o ciudadanos (ya sean residentes o transeúntes).
- Prevención social para evitar que los jóvenes sean reclutados para (este tipo de) delitos.