Publikation der deutschen Versicherer
(GDV e. V.) zur Schadenverhütung

Richtlinien zur Sicherung von Geldautomaten – Risikobewertung und Maßnahmen

Kompetent. Kostenlos. Neutral.

Wir danken der Polizei, insbesondere der Kommission Polizeiliche Kriminalprävention der Länder und des Bundes für die gute und konstruktive Zusammenarbeit bei der Erarbeitung dieser Richtlinien.

Ferner danken wir den Vertretern der Versicherungswirtschaft, der Deutschen Gesetzlichen Unfallversicherung (DGUV), der Kreditwirtschaft sowie den Herstellern von Geldautomaten für die gute und konstruktive Zusammenarbeit bei der Erarbeitung dieser Richtlinien.

Herausgeber: Gesamtverband der Deutschen Versicherungswirtschaft (GDV)

Verlag: VdS Schadenverhütung GmbH
Amsterdamer Str. 174
50735 Köln
Tel.: (0221) 77 66 0
Fax: (0221) 77 66 341

Das vorliegende Dokument ist nur verbindlich, sofern dessen Verwendung im Einzelfall vereinbart wird; ansonsten ist die Berücksichtigung dieses Dokuments unverbindlich. Die Vereinbarung zur Verwendung dieses Dokuments ist rein fakultativ. Dritte können im Einzelfall auch andere Anforderungen nach eigenem Ermessen akzeptieren, die diesem Dokument nicht entsprechen.

Um eine Beeinträchtigung des Textverständnisses zu vermeiden, verwendet VdS Schadenverhütung durchweg das generische Maskulinum. Eine Bevorzugung oder anderweitige Wertung des männlichen, weiblichen oder sonstigen Geschlechts geht damit ausdrücklich nicht einher.

Richtlinien zur Sicherung von Geldautomaten – Risikobewertung und Maßnahmen

INHALT

1 Allgemeines

1.1 Einleitung

Geldautomaten (GA) werden von Tätern auf vielfältige Weise angegriffen. Neben Angriffen mit thermisch oder mechanisch wirkenden Werkzeugen, ist insbesondere der täterseitige Einsatz von gasförmigen und festen Sprengmitteln, die Täuschung des Nutzers durch Manipulationen im und am Geldautomaten sowie die Manipulation von Geräteprozessen bekannt.

Dem Sprengen von Geldautomaten muss dabei besondere Aufmerksamkeit gewidmet werden. Die Vorgehensweise der Täter verursacht neben dem Schaden am GA zumeist erhebliche Sachschäden des unmittelbaren und mittelbaren Umfelds. Darüber hinaus muss bei jedem Angriff mit Sprengmitteln auch mit Personenschäden gerechnet werden.

Trotz präventiver Maßnahmen ist es unmöglich, Risiken beim Betrieb von GA völlig auszuschließen. Die Risiken ergeben sich aus unterschiedlichen Faktoren, die in ihrer Gesamtheit nur von geschulten Fachleuten zuverlässig bewertet werden können. Ein Restrisiko ist unvermeidbar. Um eine höchstmögliche Sicherheit bei vertretbarem Restrisiko zu erreichen, sind individuelle Sicherungskonzepte zu erstellen, umzusetzen und regelmäßig hinsichtlich aktueller Entwicklungen anzupassen.

Das vorliegende Druckstück wurde unter Mitarbeit einer aus Reihen der Polizei, der Versicherungswirtschaft, Vertretern der Kreditwirtschaft sowie von Herstellern von GA konstituierten Expertenrunde erarbeitet.

Die vorliegenden Richtlinien bieten den Verantwortlichen Hilfestellung bei der Beurteilung möglicher Gefährdungen und Risiken, die sich beim Betrieb von GA ergeben können.

In diesem Dokument werden Anforderungen u. a. dadurch beschrieben, dass auf in externen Regelwerken genannte Klassen, Grade und andere Einteilungen verwiesen wird. Im Sinne der einheitlichen Systematik des Gesamtwerkes der durch den GDV und VdS herausgegebenen VdS-Richtlinien wird daher im vorliegenden Papier auf bestehende VdS-Richtlinien und die darin beschriebenen Klassen, Grade usw. verwiesen.

Neben den VdS-Richtlinien existieren für einzelne Produkte und Dienstleistungen auch nationale und internationale Normen. Eventuell existierende, korrespondierende Norm-Klassen einschließlich der entsprechenden vergleichsweisen Einstufung können den Sicherungsrichtlinien Geschäfte und Betriebe, VdS 2333 sowie den Technischen Kommentaren, VdS 3134 entnommen werden.

Die Einstufungs- sowie Handlungsratschläge sind unverbindlich. Die Empfehlungen sind ausdrücklich als Hilfestellung zu verstehen. Die jeweils Verantwortlichen werden in keiner Weise von ihrer Entscheidungsverpflichtung und Verantwortung entbunden.

Die vorliegenden Richtlinien behandeln bisher bekannte Begehungsweisen, die Empfehlungen entsprechen dem aktuellen Stand der Technik. Über die vorliegenden Empfehlungen hinaus finden sich Anforderungen zum Schutz vor Angriffen auf Geldautomaten u. a. in den Sicherungsrichtlinien Bargeld (VdS 2472), den Technischen Kommentaren (VdS 3134) sowie im Vorschriften- und Regelwerk der gesetzlichen Unfallversicherungsträger.

1.2 Gültigkeit

Diese Richtlinien gelten ab dem 01.02.2022.

Sie ersetzen die Ausgabe VdS 5052 : 2017-01 (03).

2 Risikobetrachtung

2.1 Allgemeines

Beim Betrieb von GA ergeben sich unterschiedliche Risiken, denen, um eine Minimierung möglicher Schäden zu erreichen, individuell begegnet werden muss. Die in diesen Richtlinien enthaltenen Aufzählungen von Risiken sowie die Erläuterungen der Gegenmaßnahmen sind als Orientierungshilfe bei der Durchführung einer Gefährdungsanalyse sowie der Absicherung individueller Risiken zu verstehen. Sie kann aufgrund sich ändernder Techniken und sich entwickelnder Tätervorgehensweisen keinen Anspruch auf Vollständigkeit erheben.

Durch sich ändernde Tatbegehungsweisen, ermittelte Schwachstellen, geänderte Umfeldbedingungen u. v. m. können sich die Gegebenheiten, an denen sich das Sicherungskonzept orientiert, schnell und gravierend ändern. Ein kontinuierlicher Prozess zur wiederkehrenden Lageeinschätzung, Definition neuer oder geänderter Sicherungsmaßnahmen und Überprüfung der Wirksamkeit aller Maßnahmen ist daher unerlässlich. Zusätzliche Sicherheit entsteht, wenn diese Prozesse und Strukturen regelmäßig durch Dritte auditiert werden. VdS bietet im Rahmen der Richtlinien VdS 3406-1 die Zertifizierung

Bild 2-1: Tatort einer Geldautomatensprengung

des Sicherheitsmanagementprozesses für bauliche Objekte an.

Hinweis: Die Kommission Polizeiliche Kriminalprävention der Länder und des Bundes hat ein Raster für eine Risikoanalyse zur Sprengung von Geldautomaten entwickelt. Dieses ist Anhang F zu entnehmen.

2.2 Risikofaktoren beim Betrieb eines Geldautomaten

Ein Geldautomat stellt technisch gesehen keine Gefahr dar. Die technischen Abläufe beim Betrieb des GA sind sowohl für Betreiber als auch für den Nutzer risikofrei. Dennoch korreliert der reale Einsatz von GA mit einem relevanten Gefahrenpotenzial.

Durch die Auslagerung und Automatisierung von Geldgeschäften mit Endkunden erfolgt zeitgleich die Verlagerung des Risikos, welches Geschäften mit Bargeld innewohnt, von den Räumlichkeiten des Betreibers (z. B. Geldinstitut) hin zum Aufstellungsort des Automaten.

Geldautomaten bieten aufgrund des eingelagerten Bargelds für Täter einen erheblichen Anreiz, dieses Bargeld unmittelbar durch den Einsatz unterschiedlichster Angriffsmethoden oder durch am GA vorgenommene Manipulationen zu erlangen (vgl. Bild 2-1).

Denkbare Vorgehensweisen für einen Täter, der das Ziel verfolgt, unrechtmäßig Zugriff auf das im GA befindliche Bargeld zu erlangen, können u. a. die folgenden sein.

Direkte Angriffe

Direkte Angriffe nehmen eine Zerstörung des GA sowie eine großflächige Beschädigung der Umgebung billigend in Kauf. Hierzu zählen Angriffe, die es zum Ziel haben, direkten Zugriff auf die Geldkassetten bzw. das eingelagerte Bargeld zu erlangen, z. B. durch:

- Sprengung des GA
- heiße und kalte Angriffe auf den GA (Angriffe mit thermischen und mechanischen Werkzeugen)
- Totalentwendung des GA, um diesen zu einem späteren Zeitpunkt in einer für den Täter risikoarmen Umgebung aufzubrechen.

Indirekte Angriffe

Indirekte Angriffe richten sich im Wesentlichen auf die Manipulation des GA und/oder der Umgebung. In Bezug auf die den GA nutzenden Kunden besteht das Risiko, dass Täter Vorrichtungen am bzw. im GA oder seinem unmittelbaren Umfeld installieren, die z. B.

- der Erschleichung der PIN
- der Erschleichung der Kartendaten
- dem Abfangen von Bargeld
- dem Abfangen der Bankkarte

dienen.

Hierzu können u. a. zählen:

- Skimming,
  d. h. Auslesen der Daten vom Magnetstreifen der Bankkarte bei zeitgleicher Erschleichung der zugehörigen PIN
- Cash Trapping,
  d. h. Abfangen von Bargeld im Rahmen von Auszahlungsvorgängen
- Card Trapping,
  d. h. Abfangen der Bankkarte z. B. unter Einsatz einer sogenannten Kartenschlinge bei zeitgleicher Erschleichung der zugehörigen PIN
- Eavesdropping,
  d. h. Abhören von Kartendaten während der Übertragung
- Shimming, d. h. Angriffe auf die Chip-Schnittstelle der Bankkarte
- Reversal Fraud,
  d. h. Abbruch von Transaktionen zur wiederholten Durchführung derselben
- Jackpotting,
  d. h. Manipulation der Hardware/Software des Geldautomaten, um unberechtigte Auszahlungen bzw. eine Totalentleerung des Automaten auszulösen.

Vandalismus

Je nach Erreichbarkeit besteht das Risiko, dass der GA, sein Aufstellort oder die Umgebung im Rahmen von Vandalismus angegriffen und beschädigt werden.

Risiken durch Raub

Weiter können Kunden bei der Bedienung des GA durch Raub, Betrug oder Diebstahl unmittelbar geschädigt werden. Dies trifft insbesondere zu, wenn hohe Auszahlungsbeträge am GA angeboten werden und dies von Dritten (Tätern) beobachtet wird.

Ein Beraubungsrisiko besteht ebenfalls für Personen, die GA warten, bestücken bzw. Bargeld entsorgen. Diesem Beraubungsrisiko ist direkt bei der Gestaltung des Umfeldes zu begegnen, um risikominimierende Maßnahmen umzusetzen (z. B. durch entsprechende Gestaltung der GA-Einbausituation).

Die genannten Angriffsarten bezogen auf Raub werden im weiteren Verlauf dieses Dokuments nicht näher betrachtet.

2.3 Potenzielle Folgen von Angriffen auf Geldautomaten

Verschiedene Überlegungen sind für die Entscheidung, unter welchen Randbedingungen ein bestehender bzw. ein neu aufgestellter GA betrieben werden sollte relevant. Etliche Angriffsarten können nicht nur ausschließlich einen möglichen Bargeldverlust oder den Komplettverlust des Automaten bedeuten, sondern darüber hinaus weitreichende Folgeschäden nach sich ziehen.

Bei praktischen Sprengversuchen mit verschlossenen Automaten wurde die ca. 100 kg schwere Wertbehältnistür bis zu 14 m weit fortgeschleudert. Der gesamte Automat wurde dabei zerrissen. Wenn ein Angriff auf einen in oder an einem Gebäude installierten GA mit einem solchen Ablauf stattfindet, wird dies zu erheblichen baulichen Schäden führen. Auch Personenschäden können dabei nicht ausgeschlossen werden.

Wenn ein solcher Angriff innerhalb eines Foyers oder in der Kundenhalle eines Geldinstitutes stattfindet, muss u. a. mit folgenden Resultaten gerechnet werden:

- Zerstörungen des unmittelbaren Umfeldes aufgrund
  - entstehender Druckwellen
  - fortgeschleuderter schwerer Bestandteile des Automaten, z. B. der Wertbehältnistür oder Teile der Wandung
  - durcheinander geschleuderter Einrichtungsgegenstände
  - Glasbruch

- Zerstörung des unmittelbaren sowie mittelbaren Umfeldes aufgrund
  - der Entzündung von brennbarem Material
  - der Explosion/Verpuffung von Gasgemisch, das bei der Befüllung des Automaten ausgetreten ist
  - von verbliebenem, nicht gezündetem Sprengstoff (Gas/Festsprengstoff) im Gerät bzw. im Objekt, insbesondere bei abgebrochenen Delikten, sofern sich die Gefahr einer verzögerten und unkontrollierten Explosion realisiert.

Neben Schäden innerhalb und außerhalb des Gebäudes muss unter Umständen mit einem Totalverlust des Gebäudes gerechnet werden. Darüber hinaus sind, auch wenn die Gebäudeschäden sich als nicht verheerend herausstellen, ernsthafte Schäden an der IT-Landschaft (Arbeitsplatzrechner, Rechner in Automaten bis hin zur essenziellen Serverumgebung des Betreibers) durch den Explosionsdruck bzw. Verschmutzung durch Explosionsrückstände oder durch thermische Einwirkungen der Explosion zu erwarten.

Da nicht davon ausgegangen werden kann, dass sich die Schäden auf den inneren Bereich der Räumlichkeiten des Betreibers beschränken, müssen Personenschäden durch herumfliegende Trümmerteile und/oder Glas erwartet werden. Das gilt auch dann, wenn sich der GA in einem abgeschlossenen Innenraum, z. B. im Foyer oder in einem Vorraum zum Geldinstitut befindet.

Auch bei Angriffen mit schweren Baumaschinen oder Fahrzeugen, die eine Totalentwendung des GA zum Ziel haben, sind erhebliche Gebäudeschäden zu erwarten.

Grundsätzlich darf nicht damit gerechnet werden, dass die Schäden ausschließlich in einem eng begrenzten Bereich auftreten. Zumindest der an den Geldautomaten angrenzende öffentliche sowie angrenzender umbauter Raum ist unmittelbar mit bedroht und dort auch sämtliche in der Nähe befindliche Personen. Besonderen Gefährdungen sind auch Interventionskräfte ausgesetzt, insbesondere durch nicht oder nicht vollständig zur Detonation gekommene Sprengstoffe. Wenn es in Folge eines Angriffes zu einem Brand kommt, können neben den Räumlichkeiten des Betreibers auch weitere Räumlichkeiten oberhalb des Tatortes oder auch Nachbargebäude in Mitleidenschaft gezogen werden.

Auch durch Cyberangriffe können Schäden entstehen. Diese umfassen sowohl die mithilfe von Manipulation umgesetzte Komplettleerung der GA als auch gestohlene oder manipulierte Daten.

Alle genannten, nach außen hin – u. a. von der Kundschaft – wahrnehmbaren Folgen eines Angriffs auf Geldautomaten können deutliche Rückwirkungen auf die weitere Arbeitsfähigkeit des Betreibers haben und drastische Imageschäden verursachen (Reputationsrisiko). Eine auf einen Angriff folgende längere Betriebsunterbrechung kann zur dauerhaften Abwanderung von Kunden führen. Der Imageschaden, den der Betreiber durch einen Angriff erleiden kann, ist nur schwer zu prognostizieren, muss aber dennoch in die Gesamtbetrachtung einbezogen werden.

3 Konkrete Angriffsarten und Angriffsbeschreibungen

3.1 Allgemeines

In diesem Kapitel werden verschiedene Angriffe konkret beschrieben. Grundsätzlich kann zwischen zerstörenden und manipulativen Angriffen unterschieden werden. Ziel ist es, die Vorgehensweise der Täter und die relevanten Einflussfaktoren zu verstehen. Auf dieser Grundlage können dann im weiteren Verlauf die Gefährdungsanalyse, die Schutzzieldefinition und die Festlegung von Sicherungsmaßnahmen erfolgen.

Sicherungsmaßnahmen gegen die beschriebenen Angriffe sind in Kapitel 5 ff. erläutert. Die Gesamtheit der umgesetzten Gegenmaßnahmen ist entsprechend des individuellen Sicherungskonzeptes auf das Risiko abzustimmen.

3.2 Angriffe mit Werkzeugen

3.2.1 Aufkeilen

Unter hohem persönlichen Risiko (hohe Verletzungsgefahr) können Wertbehältnisse (WB) mithilfe von Metallkeilen und schweren, handgeführten Hämmern angegriffen werden (vgl. Bild 3-1). Dabei wird angestrebt, mehrere Keile in den Spalt zwischen Tür und Korpus des Behältnisses einzutreiben und so ein Versagen der Verriegelung herbeizuführen. Bei konstruktiv schwachen Wertbehältnissen lassen sich auf diese Weise die einzelnen Bauteile des Produktes so weit auseinander drücken, dass eine Öffnung erwirkt werden kann.

Bild 3-1: Aufgekeilter Geldautomat

Bild 3-2: Aufgespreizter Geldautomat

Bild 3-3: Angriff mit dem Winkelschleifer

3.2.2 Spreizen

Türen von Wertschutzschränken von GA können je nach Konstruktion mit Hydraulikspreizgeräten angegriffen werden. Dabei wird in der Regel zunächst versucht, den konstruktiv nicht vollständig vermeidbaren Türspalt an der Verriegelungsseite der Tür mithilfe eines Metallkeils zu erweitern. Sofern der erweiterte Spalt ausreichend Raum bietet, ein Spreizgerät einzusetzen, kann der Angriff erfolgen (vgl. Bild 3-2). Durch wiederholten Einsatz des Spreizgerätes und unterstützende Fixierung der erzeugten Spalte mit Keilen kann der Korpus des GA unter Umständen so weit deformiert werden, dass die Riegelbolzen des Riegelwerkes nicht mehr in den Korpus eingreifen und die Tür geöffnet werden kann.

3.2.3 Trennschleifen

Angriffe mit Trenn- oder Winkelschleifern auf GA haben zum Ziel, Öffnungen in den Korpus des Wertbehältnisses einzubringen oder dessen Tür zu überwinden (vgl. Bild 3-3).

Derartige Angriffe können prinzipiell an allen frei zugänglichen Punkten erfolgen. So ist es, sofern der Zugriff auf die Wandungen gegeben ist, unter Umständen möglich, Teile der Wertbehältniswandung großflächig herauszutrennen. Dies kann im Erfolgsfall die Möglichkeit gewähren, den Inhalt des GA komplett entwenden zu können.

Weitere potenzielle Angriffspunkte liegen im Bereich der Sperrstellen der Verschlusseinrichtung und an den Bändern bzw. Scharnieren. Wenn es möglich ist, die Riegelbolzen zu durchtrennen oder die Bänder zu entfernen, ist häufig (sofern keine Notverriegelung greift) ein Öffnen der Tür möglich.

3.2.4 Brennschneiden

Schneidbrenner arbeiten mit einem Gemisch aus Brenngas und Sauerstoff. Durch die Reaktion der beiden Gase werden hohe Temperaturen erzeugt, die ausreichend sind, metallische Bauteile von Wertbehältnissen (z. B. Wandung, Armierungen, Riegel) zu schmelzen und so zu zertrennen (vgl. Bild 3-4).

Ein Wertbehältnis, das lediglich eine einwandige metallische Hülle aufweist, lässt sich mit einem Schneidbrenner innerhalb weniger Sekunden öffnen. Die Dicke der Bleche ist dabei nicht von Bedeutung. Bei einfachen Behältnissen kommen mitunter Bleche von nur wenigen Millimetern Dicke zum Einsatz. Auch Bleche, deren Dicke im Zentimeterbereich liegt, lassen sich mit diesem Werkzeug schnell und einfach zerschneiden.

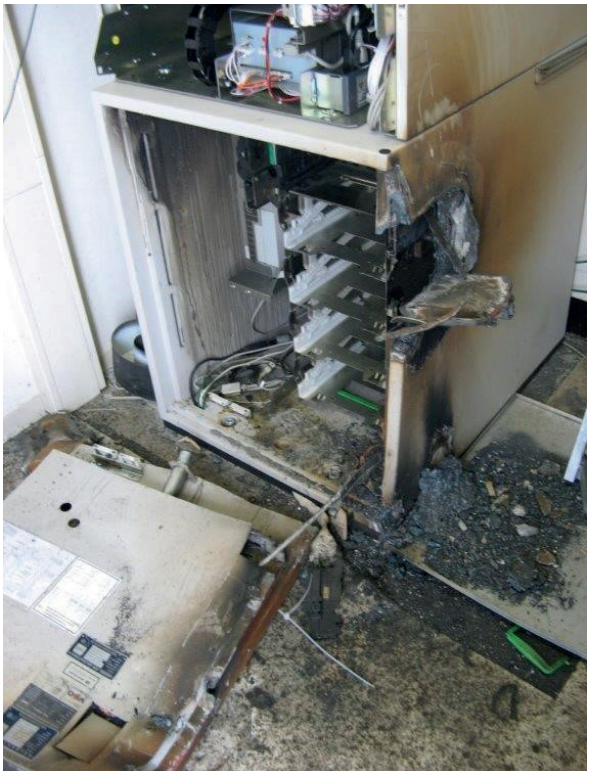

Bild 3-4: Türöffnung nach Brennschneiden

3.2.5 Sauerstofflanze

Die sogenannte Sauerstofflanze ist ein thermisches Schneidwerkzeug mit extrem hohem Energieumsatz. Sie ist geeignet, Metalle und andere Materialen (z. B. Beton) aufzuschmelzen und so zu zerstören. Die Arbeit mit der Sauerstofflanze erzeugt insbesondere bei höherwertigen Wertbehältnissen große Mengen an Rauch- und Abgasen. Diese Gase stellen schon nach wenigen Sekunden für den Täter eine deutliche Behinderung dar.

3.2.6 Gefährdungsanalyse

Die Gefährdungsanalyse, welche zum Ziel hat, das Risiko von Werkzeugangriffen zu beurteilen, muss sich im Wesentlichen mit dem Produkt, d. h. mit der Widerstandsfähigkeit des Wertschutzschrankes auseinandersetzen. Lediglich wenn sichergestellt ist, dass von einem Täter nicht auf einen konkreten GA zugegriffen werden kann (etwa, weil dieser sich in einem stark gesicherten Bereich im Gebäudeinneren befindet), kann die Bedeutung des Widerstandsgrades des Behältnisses in Bezug auf einen möglichen Aufbruch abweichend bewertet werden.

Eine besondere Gefährdung von GA kann sich aus der Aufstellung der Geräte im öffentlich zugänglichen bzw. in relativ leicht begehbaren Räumlichkeiten ergeben. Dies ist bei Geldautomaten, bedingt durch die erforderliche Bedienung durch Kunden, in aller Regel gegeben. Das bedeutet, auch potentielle Täter können sich dem GA und somit dem Wertbehältnis bis auf kurze Distanz nähern. Dies versetzt potenzielle Täter in die Lage, Einbruchwerkzeuge relativ schnell und effektiv einzusetzen.

Als besonders ungünstig ist auch die Aufstellung in Bereichen zu werten, welche einen leichten Zugriff auf erforderliche Werkzeuge ermöglichen. GA, die z. B. in Foyerbereichen von Bau- oder Werkzeugmärkten aufgestellt sind, könnten von Tätern bevorzugt angegriffen werden, weil die Werkzeuge direkt vor Ort verfügbar sind. Besonders risikoreich kann diese Konstellation sein, wenn sich der Markt zusätzlich in einem Gelände mit geringer Wohndichte befindet.

Wegen der heute verfügbaren Werkzeuge mit sehr leistungsfähigen Akkus oder Verbrennungsmotoren spielt das Vorhandensein einer Stromversorgung für die Risikobetrachtung keine oder nur noch eine sehr untergeordnete Rolle.

In Bezug auf heiße Angriffe sind die räumliche Situation sowie die Belüftung des Aufstellortes bedeutsam. In kleinen Räumen sind Angriffe mit einem Schneidbrenner u. ä. wegen der unmittelbaren Gefährdung für den Täter (Hitze, Funkenflug,

Rauchgase usw.) eher schlecht umzusetzen. Für Behältnisse, die in großen Räumen oder sogar im Freien positioniert sind, sind heiße Angriffe jedoch ein relevantes Risiko. Hier gilt, dass ein GA, der leicht erreichbar ist, einem höheren Angriffsrisiko ausgesetzt ist, als ein GA, der nur umständlich oder aufgrund weiterer Sicherungsmaßnahmen schwer erreichbar ist. Dies liegt nicht zuletzt daran, dass die Täter für heiße Angriffe eine relativ sperrige Ausrüstung zum Tatort bringen müssen (Gasflaschen, Schläuche, Brennaufsätze). Der Einsatz von Sauerstofflanzen erfordert zudem einen gewissen Bewegungsspielraum für die Täter.

In jüngerer Vergangenheit ist es (noch) nicht zu nennenswerten Schadenzahlen durch den Einsatz von Sauerstofflanzen gekommen. Wenn es für einen Täter jedoch möglich sein sollte, eine Sauerstofflanze zum Einsatz zu bringen, muss mit einem – unabhängig vom Diebesgut – hohen Schadenpotenzial gerechnet werden, da mit einer hohen lokalen Wärmeentwicklung sowie einem starken Funkenflug gerechnet werden muss. Damit einher geht eine erhöhte Brandgefährdung.

Zusammenfassend stellt sich die Gefährdungsanalyse in Bezug auf Werkzeugangriff so dar, dass ein GA einem umso höheren Risiko ausgesetzt ist, je leichter ein Täter Zugriff auf das Behältnis erhalten kann (z. B. GA freistehend) und je leichter somit der Täter den Antransport des erforderlichen Werkzeugs vornehmen kann. Für den Täter ungünstige Arbeitsbedingungen (z. B. räumliche Enge, lange Wege, um Werkzeug (manuell) heranzutransportieren) verringern das Risiko für den individuellen Automaten (vgl. Bild 3-5).

Bild 3-5: Risiko von Werkzeugangriffen

3.3 Sprengung

3.3.1 Allgemeines

Bei einem möglichen Einsatz von Sprengstoff resultieren Gefahren für das Gebäude und die Umgebung vor allem aus der enormen zu erwartenden Sprengkraft des Materials.

Bei einer Sprengung nimmt das Volumen der eingesetzten Ausgangsmaterialen schlagartig zu. Wenn diese Volumenvergrößerung in einem geschlossenen Behältnis erfolgt, wird Druck aufgebaut. Dadurch wirken sehr starke Kräfte auf die Außenwand des Wertbehältnisses. Sind die auftretenden Kräfte stark genug, reißt die Außenwand förmlich auf.

Abhängig von der Art und Stärke der Explosion, sowie von Konstruktion und Stabilität des Wertbehältnisses, kann der Schaden von einer unvollständigen Öffnung über eine erfolgreiche Öffnung der Tür bis hin zur totalen Zerstörung einschließlich großräumiger Schäden im Umfeld reichen. Zusätzlich resultiert aus dem Sprengangriff eine deutliche Brandgefahr. Komplettverluste von Häusern oder Hausteilen durch Explosion und/oder Brand hat es bereits gegeben.

Wenn sich zum Zeitpunkt der Explosion Personen in der Nähe des GA befinden, besteht Gefahr für Leib und Leben. Selbst Personen, die sich beabsichtigt oder zufällig im Umfeld des Explosionsherdes befinden, etwa weil sie zum Zeitpunkt der Sprengung das Foyer straßenseitig passieren, sind extrem gefährdet, da die Explosion kleine und größere Bruchstücke regelrecht in Geschosse verwandeln kann (vgl. Bild 3-6).

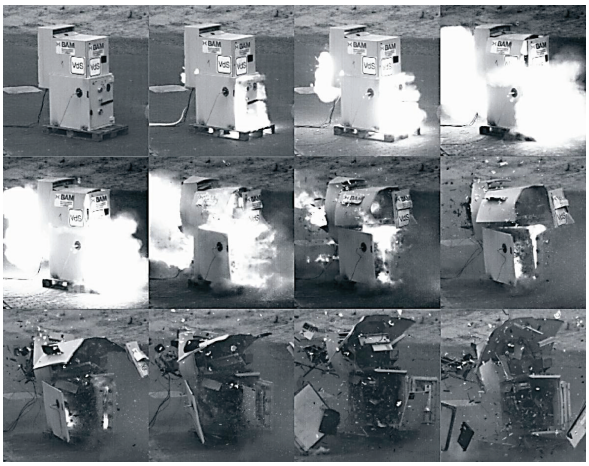

Bild 3-6: GA-Sprengung, Hochgeschwindigkeitsaufnahmen

Wenn die vom Täter vorgesehene, „kontrollierte" Zündung scheitert, besteht ein besonders hohes Risiko für unbeteiligte Dritte, für intervenierende Polizei-/Feuerwehrkräfte, Beschäftigte von Dienstleistern und Kreditinstituten sowie für die Gebäudesubstanz aber natürlich auch für die Täter selbst durch eine plötzlich und unkontrolliert hervorgerufene Detonation. Schon die minimale Energie eines statischen Entladungsfunkens kann die Explosion auslösen.

3.3.2 Gefährdungsanalyse

In den letzten Jahren ist die Anzahl von Sprengangriffen auf Geldautomaten unter Verwendung von Gas oder Festsprengstoff auf ein beträchtliches Maß angestiegen.

Die Angriffstechniken der professionellen Tätergruppen entwickeln sich dabei permanent weiter. Da auch Täter ohne besondere Kenntnisse Sprengung als Angriffsmethode einsetzen, fällt es schwer, hinreichend konkrete und gleichzeitig allgemeingültige Gefährdungsfaktoren abschließend zu benennen.

Darüber hinaus spielt die gerade in Deutschland sehr heterogene und individualisierte Struktur der Kreditinstitute eine Rolle, die das Erkennen von Mustern deutlich erschwert. Trotzdem lassen sich Präventionsansätze ableiten und zumindest fünf wesentliche Gefährdungsfaktoren erkennen. Diese Faktoren sind für eine Tatauswahl offenbar besonders relevant und sollten daher in die individuelle Gefährdungsanalyse des GA-Standortes mit einbezogen werden:

- systembedingte Geräteöffnungen, z. B. Shutter, Kabeldurchführungen zum Einbringen des Sprengmittels
- Umfeldbedingungen (unbemerkte Tatausführung möglich)
- Positionierung der Versorgungsöffnung/ bauliche Gegebenheiten (Zugriff auf GA-Inhalt nach erfolgreicher Sprengung möglich)
- Verkehrsanbindung/Intervention (erfolgreiche Flucht nach Tatausführung möglich)
- Gerätetyp des GA (individuelle, gerätespezifische Schwachstellen)

Systembedingte Öffnungen

Bauartbedingt verfügen GA über eine Vielzahl von systembedingten Öffnungen (z. B. Kabeldurchführungen oder Shutter). Sprengangriffe erfolgen häufig über die für den Täter einfach zu erreichenden Öffnungen des Wertbehältnisses. Diese Öffnungen sollten bestmöglich verschlossen oder der Zugang zu diesen behindert werden. Neben den systembedingten Öffnungen zum Wertbehältnis, stellt das GA-Gehäuse die erste Widerstandshülle dar. Leicht zu öffnende Türen/Hauben bzw. Schwachstellen in der Gehäusestruktur (Kamerablenden, Shutter bzw. Geldentnahmefach auf Kundenseite) können einen Angriff erleichtern.

Umfeldbedingungen

Die tatvorbereitenden Handlungen für eine GA-Sprengung sind auffällig. Täter versuchen, die Vorarbeiten unbeobachtet auszuführen. Häufig finden die Taten daher in der Zeit zwischen Mitternacht und dem Morgengrauen statt. Es werden Standorte gewählt, die in dieser Zeit nur vereinzelt genutzt werden. Es kann angenommen werden, dass Geldautomaten an Standorten, die auch in den Nachtstunden durchgängig einer visuellen Kontrolle des GA ermöglichen (z. B. personell besetzte Tankstelle mit 24-stündiger Öffnung), einer geringeren Gefährdung unterliegen.

Positionierung Versorgungsöffnung/bauliche Gegebenheiten

Der Angriff auf den Geldautomaten erfolgt im Regelfall über die gut erreichbare Kundenseite. Angriffe können z. B. über den Shutter, der sich im Wertbehältnis befindet oder über den Kopf des GA nach gewaltsamer Öffnung der vorderen Bedienfeldes erfolgen. Danach kann über die systembedingten Öffnungen der Sprengstoff eingebracht werden.

Für die Täter ist es weiter von entscheidender Bedeutung, dass sie nach einer Sprengung einen einfachen und möglichst schnellen Zugriff auf den GA-Inhalt bekommen. Das bedeutet im Normalfall, dass die Täter die Tür des Wertbehältnisses erreichen müssen. Am schnellsten kommen die Täter bei einem sog. Frontloader an die Beute, da sich die Tür zum Kunden (bzw. zum Täter) hin öffnet. Rearloader (Automaten, die von der Geräterückseite befüllt werden) stellen eine Taterschwernis dar, weil sich die Täter zusätzlich zur Sprengung auch noch Zugang zum hinteren Automatenbereich, zu dem sich die Tür des Wertbehältnisses öffnet, verschaffen müssen. Sind Wände und Zugänge zu diesem Raum nur in Leichtbauweise ausgeführt oder verfügt der Raum über Fenster ohne besondere Einbruchhemmung, können die Täter davon ausgehen, dass ein Zugang zum rückwärtigen Automatenbereich bereits im Zuge der Explosion mit geschaffen wird. Bisherige Erfahrungen legen nahe, dass Rearload-Automaten die in einem Raum in fester Bauweise (durchbruchhemmende Wandelemente, einbruchhemmen-

de Türen, nach Möglichkeit Verzicht auf Fenster) aufgestellt sind, für Täter weniger attraktiv sind. In diesem Fall müssten sie neben dem GA-Angriff noch in den Versorgungsraum einbrechen, was bei entsprechender Sicherung spezielle und andere Fertigkeiten erfordert, als der Angriff auf den GA.

Verkehrsanbindung/Intervention

Da spätestens nach der Sprengung eine Alarmierung der Polizei durch z. B. die vorhandene EMA zu erwarten ist und Interventionskräfte zum Objekt geschickt werden, sind für die Täter neben einer schnellen Tatausführung auch möglichst lange Interventionszeiten und gute Fluchtmöglichkeiten von Bedeutung.

Grundsätzlich kann daher davon ausgegangen werden, dass Täter die Standorte bevorzugen, die die o. g. Bedingungen erfüllen. Der erwartete Zeitaufwand für die schnelle Tatausführung und gute Fluchtmöglichkeiten führen zu Sprengangriffen auch in innerstädtischen Bereichen, wenn die Täter die Umfeldbedingungen als günstig eingeschätzt haben.

Gerätetyp GA

In der Vergangenheit häufig erfolgreich angegriffene Gerätetypen sollten gegen besser geschützte Modelle ausgetauscht oder mit präventiv wirkenden Schutzmaßnahmen nachgerüstet werden. Bei Anschaffung eines GA empfiehlt es sich, die bereits ab Werk erhältlichen zusätzlichen Sicherungsmaßnahmen installieren zu lassen.

Wertbehältnis

Die Behältnisse selber können – es gibt entsprechende Prüfverfahren – gegen den Einsatz von Sprengstoffen geprüft und anerkannt werden (siehe Kapitel 6.2).

3.3.3 Sprengung mit Gas

Ohne eine Anleitung zu geben, wie die Sprengung eines GA umgesetzt werden kann, wird im Folgenden eine mögliche Vorgehensweise beschrieben, um zu verdeutlichen, mit welchem – auf den ersten Blick – geringen Aufwand Täter vorgehen können.

Bei Sprengangriffen wird ein explosionsfähiges Medium in das Wertbehältnis eingebracht und gezündet. Sobald mit Luft oder Sauerstoff vermischtes Brenngas ins Wertbehältnis eingelassen wird, besteht höchste Explosionsgefahr, da sich das Gemisch bereits durch kleinste Funken bzw. elektrische Entladungen unbeabsichtigt entzünden kann. Sofort nach der Zündung reagiert das Brenngas mit dem Sauerstoff, dehnt sich schlagartig aus und drückt die Tür des im GA befindlichen Wertbehältnisses auf und/oder sprengt die Wände des Behältnisses auseinander. Der Täter kann nun, sofern ihm der Zugang zum GA noch möglich ist, auf die Geldkassetten, sofern diese nicht zu stark zerstört sind, zugreifen und fliehen.

Die bei der Explosion freiwerdende Druckkraft ist unter anderem stark abhängig von der Menge des explodierenden Gasgemisches. Je mehr zündfähiges Gasgemisch eingefüllt werden kann, desto stärker wird die Zerstörung des Behältnisses sowie der Umgebung ausfallen. Da unter realen Bedingungen eine exakte Mischung und Mengenregulierung des Explosivgases nicht möglich ist, lässt sich die Heftigkeit der Explosion kaum prognostizieren.

3.3.4 Sprengung mit Festsprengstoff

Neben der Verwendung explosiver Gasgemische sind auch Angriffe mit Festsprengstoffen unterschiedlicher Art und Herkunft bekannt. Ähnlich wie bei Angriffen mit gasförmigem Sprengstoff bringen die Täter bei dieser Tatbegehungsweise Festsprengstoff im Inneren des WB zur Detonation, den sie zuvor durch die bauartbedingten Öffnungen des WB dorthin eingebracht haben. Verwendet werden gewerbliche Sprengstoffe, z. B. Sprengschnüre, Feuerwerkskörper mit erheblicher Sprengwirkung ohne eine Zulassung in Deutschland, Plastiksprengstoffe und ähnliches. Die Einbringung erfolgt unter Zuhilfenahme von geeigneten Werkzeugen.

3.3.5 Widerstandsgrad des Wertbehältnisses im Geldautomaten

Weist das Wertbehältnis nicht mindestens den in Kapitel 7.5.2 beschriebenen Widerstandsgrad mit den entsprechenden Zusatzkennzeichen aus, besteht eine hohe Gefahr für die erfolgreiche Durchführung von Angriffen.

Es wird unterschieden zwischen dem Nachweis der Sicherungseigenschaften gegen die Auswirkungen von Sprengungen mit

- Festsprengstoff (EX) und
- gasförmigem Sprengstoff (GAS).

Beide Angriffsarten werden getrennt betrachtet, da der augenscheinlich ähnliche Angriffsvorgang in der Art der Kraftentfaltung und Wirkung deutlich voneinander abweichend ist.

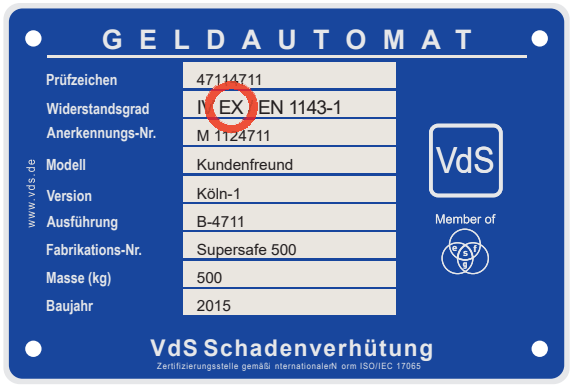

Bild 3-7: Anerkennungsplakette Wertbehältnis für GA mit nachgewiesener Wirkungshemmung gegen Sprengstoff

3.4 Totalentwendung

3.4.1 Möglicher Tathergang

Dieser Modus Operandi hat das Ziel, GA vom Aufstellungsort zu entfernen, abzutransportieren und die Geldschrankeinheit an einem Ort mit geringerem Entdeckungsrisiko zu öffnen. Bei diesen Angriffen (gewaltsames Überwinden der Verankerung und Abtransport) handelt sich in der Regel um einen Blitzeinbruch, d. h. die Täter führen den Einbruch ohne Rücksicht auf vorhandene Einbruchmelde- und Videotechnik durch.

Bild 3-8: Herausgerissener GA

Dazu werden freistehende GA mit Ketten, Stahlseilen oder Schwerlastgurten umschlungen und z. B. mit Fahrzeugen aus der Verankerung gerissen und abtransportiert, um sie an einem anderen Ort gefahrlos öffnen zu können (vgl. Bild 3-8).

Bei in der Wand eingelassenen GA erfolgt das Herausreißen in der Regel mit schweren fahrbaren Baumaschinen (z. B. Radlader oder Autokräne). Dabei wird die Einbauwand des GA mit der Baumaschine zerstört, anschließend erfolgt mit der Baumaschine das Herausreißen und der Abtransport des GA. Zusätzlich zum Verlust des GA und dem darin enthaltenen Bargeld, sind erhebliche Gebäudebeschädigungen zu verzeichnen. Besonders die im Verkaufsbereich oder Eingangsbereich von Verbrauchermärkten frei aufgestellten GA werden in dieser Weise angegriffen.

3.4.2 Gefährdungsanalyse

Überdurchschnittlich gefährdet sind frei aufgestellte GA in ländlichen Bereichen oder Stadtrandgebieten, da diese in der Regel in den Nachtstunden eine geringe Kundenfrequentierung aufweisen. Die bekannten Schadenfälle sind hauptsächlich diesen Örtlichkeiten zuzuordnen.

Weniger gefährdet bei Aufstellung – auch in ländlichen Bereichen – sind nur Standorte von GA, bei denen sich auf Grund der baulichen Gegebenheiten ein Herausreißen und der Abtransport selbst mit schweren Baumaschinen als schwierig erweisen würde (z. B. Höhenunterschiede zwischen Aufstellungsort des GA und dem Zugangsbereich zum GA).

Wandeinbaugeräte in Gebäuden in Massivbauweise sind nur mit schweren Baumaschinen angreifbar.

Insgesamt gibt es bezüglich der Schadenzahlen aus den vergangenen Jahren eine Verringerung der Angriffe mit Totalentwendung des GA durch die Verlagerung der Modi Operandi zu anderen Angriffsarten hin, z. B. Sprengung von GA.

3.5 Vandalismus

3.5.1 Möglicher Tathergang

Vandalismus ist eine bewusste illegale Handlung, die eine Beschädigung und/oder Zerstörung von Dingen (hier: vom GA oder vom Foyer bzw. von Foyereinrichtungen) zum Ziel hat. Konkrete Tatvorgehensweisen können sich spontan aus der jeweiligen Situation ergeben, sind aber teilweise auch geplant.

Vandalismus kann vielfältige Ursachen haben. Häufigste Auslöser dürften Verärgerung oder Böswilligkeit in Verbindung mit aggressiver Grundstimmung und entsprechendem Verhalten sowie Imponiergehabe – häufig unter Einfluss von Alkohol – sein.

Täter zerstören oder beschädigen z. B. GA durch Treten oder Schlagen. Teilweise kommen mechanische Hilfsmittel zum Einsatz. Verschiedentlich werden Einrichtungsgegenstände des SB-Bereichs zerstörerisch eingesetzt oder entsprechende Gegenstände vom Täter gezielt mitgebracht. Auch Flüssigkeiten mit aggressiver Wirkung, Farbsprays oder Feuerzeuge sowie zum Schneiden oder Kratzen geeignete Gegenstände, werden häufig verwendet. Beute ist weder das Ziel der Täter, noch kommt es bei Vandalismus zur Geldentwendung.

Die häufigsten Angriffe richten sich gegen Kartenleser, Tastatur, Beleuchtungs- und Diskretionselemente sowie das Display des GA. Nicht selten kommt es zu weiteren Beschädigungen im SB-Foyer. Auch Verunreinigungen, die aus dem unerwünschten Aufenthalt von Personen oder „Partys“ im Foyer resultieren, sind als Vandalismus zu verstehen und lassen sich durch eine wirksame Foyerüberwachung mit entsprechender Intervention reduzieren. Zielführend können ein Nachtverschluss und die Ansprache von Personen im SB-Foyer (ggf. unter Nutzung vorbereiteter Texte) aus einer NSL sein. Auch unregelmäßige Kontrollgänge im SB-Foyer sind hilfreich.

3.5.2 Gefährdungsanalyse

Für GA, die in Bereichen aufgestellt sind, für die aufgrund hoher Nutzungsfrequenzen eine soziale Kontrolle gegeben ist, wird das Risiko von Vandalismus eher gering bewertet. Auch GA, bei denen eine visuelle Kontrolle durch Personen gegeben ist, sind als minder gefährdet einzustufen.

Eine besondere Gefährdung für GA ergibt sich aus der Aufstellung dieser Geräte im öffentlich zugänglichen bzw. relativ leicht zugänglichen Raum und insbesondere zu Zeiten, während denen nur eine geringe Nutzung zu verzeichnen ist. Standorte in der Nähe von sozialen Brennpunkten oder Treffpunkten gewaltbereiter Personengruppen/Szenetreffs sowie Outdoorinstallationen sind besonders betroffen.

Das Risiko für GA kann sich zudem je nach der Aufstellsituation an Tagen mit Festveranstaltungen örtlich erhöhen.

4 Manipulation am GA

4.1 Allgemeines

Neben den geschilderten – vielfach brachialen – Angriffen auf das Wertbehältnis des Geldautomaten, sind die GA auch manipulativen Angriffen ausgesetzt. Im Unterschied zu den in den vorherigen Abschnitten genannten Angriffsarten wird bei den im Folgenden beschriebenen Manipulationen auch der Kunde geschädigt, da in einen Auszahlvorgang eingegriffen wird bzw. Kundendaten/-karten missbräuchlich erbeutet/verwendet werden. Grundsätzlich kann zwischen Delikten deren Ziel der Diebstahl einer einzelnen Karte oder der Banknoten eines einzelnen Auszahlvorgangs (Card- und Cash-Trapping) und dem sog. Skimming (massenhaften Abgreifen der Magnetstreifendaten und PIN) unterschieden werden. Derartige Manipulationen sind für Laien oft gar nicht oder nur sehr schwer zu erkennen (vgl. Bild 4-1).

Aufgrund der hohen Variabilität manipulativer Angriffe muss die Gefährdungsanalyse stets und in besonderem Maße die individuellen Gegebenheiten einer GA-Installation berücksichtigen. Von einer allgemeinen Gefährdungsanalyse, wie sie in diesen Richtlinien für eine Reihe anderer Bedrohungen formuliert ist, wird daher abgesehen.

Bild 4-1: Manipulationen sind schwer erkennbar: Geldautomat links mit, rechts ohne Manipulation

4.2 Abfangen von Bargeld beim Auszahlungsvorgang

Gerade in jüngster Vergangenheit ist diese vergleichsweise einfach anmutende Form der Manipulation vermehrt in das Blickfeld der Öffentlichkeit geraten. Beim sog. Cash-Trapping wird die finale Übergabe des Bargeldes an den Endkunden mit einer „Bargeldfalle" (engl. cash trap) verhindert. Diese Fallen können vor dem Geldausgabeschacht aber auch entlang des Geldausgabetransportweges im GA platziert werden. Bei ersterem manipulieren die Täter die Geldausgabeöffnung des Automaten mit einer nachgefertigten Blende. Diese Blende wird mit Hilfe von doppelseitigem Klebeband vor dem eigentlichen Geldausgabeschacht des Automaten (Shutter) angebracht. Bei einem anschließenden Bedienvorgang durch einen Kunden kommt es scheinbar zu keiner Auszahlung.

Beim zweiten bekannten Angriffsszenario platzieren die Kriminellen innerhalb des Gerätes im Transportweg des Geldes eine Transportsperre mit Klemmfunktion, die für den Benutzer von außen nicht erkennbar ist.

Tatsächlich stellt der Automat die Banknoten bereit. Durch die vor dem Auszahlschacht angebrachte manipulierte Blende ist dies für den Kunden allerdings nicht zu erkennen. Nach einer gewissen Zeit versucht der Automat die nicht entnommenen Banknoten wieder einzuziehen. Hierbei bleiben an der von den Tätern mit doppelseitigem Klebeband präparierten Blende zumeist einige Banknoten hängen. Diese werden von den Tätern, nachdem der Kunde den Automaten verlassen hat, entnommen.

4.2.1 Abfangen der Karte mit Erschleichung der PIN

Ähnlich wie beim Cash-Trapping handelt es sich beim sog. Card-Trapping um eine Tat, bei der die Täter nach jedem Manipulationsvorfall den Automaten neu präparieren müssen.

Beim Card-Trapping wird der Karteneingabeschlitz des Automaten mittels einer eingeführten Kunststoff- oder Metallschlinge derart manipuliert, dass die Karte zwar eingezogen und gelesen werden kann aber nicht mehr ausgegeben wird. Der Auszahlvorgang kann auch in diesem Fall nicht abgeschlossen werden, da dem Kunden eine Entnahme der Karte nicht möglich ist. Häufig tritt ein Täter in dieser Situation als vermeintlich hilfsbereiter Kunde auf und schlägt vor, die PIN nochmals einzugeben. Nach dem dies nicht erfolgreich war, verlässt der Karteneigentümer häufig den Automatenbereich. Diese Situation nutzt der Täter und entnimmt die Karte. Mit ihr und der ausgespähten PIN kann er nun bis zu den entsprechenden Limits der Karte bzw. des Kontos verfügen.

4.2.2 Auslesen der Karte mit Erschleichung der PIN

Skimming bezeichnet das illegale Ausspähen/Abgreifen der Kartendaten und PIN von Debit- bzw. Kreditkarten an Geldautomaten oder anderen Geräten die eine Karten- bzw. PIN-Eingabe erfordern.

Hierbei bringen die Täter – um den Inhalt des Magnetstreifens der Karte kopieren zu können – eine miniaturisierte Leseeinrichtung (nebst Speicher- oder Übertragungseinheit) am Karteneingabeschlitz oder im Kartenleser des Geldautomaten an. Beim Einführen einer Karte werden die jeweiligen Daten so unbemerkt kopiert. Die zusätzlich notwendige PIN wird häufig mittels einer im direkten Umfeld verdeckt platzierten Kamera aufgenommen. Teilweise werden von den Tätern auch täuschend echt nachgebildete Aufsatztastaturen angebracht, die die PIN-Eingabe protokollieren (siehe Bild 4-2).

Die gewonnenen Kartendaten lassen sich auf Rohlinge (sog. White-Cards) kopieren. Mit diesen Kartendubletten können an ausländischen Geldautomaten – überwiegend im außereuropäischen Raum – missbräuchliche Verfügungen vorgenommen werden.

Nachdem die Skimmingangriffe kontinuierlich angestiegen waren, sind sie seit der Umstellung auf Mikrochip-basierte Kartenkommunikation (sog. EMV-Einführung), die den Magnetstreifen ablöste und weiterer begleitender Maßnahmen (Geoblocking, SEPA, Liability Shift) deutlich zurückgegangen.

Bild 4-2: Manipulation am GA

4.2.3 Manipulation der Hardware/Software

Jackpotting, Blackboxing sowie Man in the Middle- und Reversal Fraud-Angriffe werden häufig als intelligente oder smarte Angriffe bezeichnet.

Beim **Jackpotting** wird eine Schadsoftware auf den Rechner des Geldautomaten eingespielt. Diese Malware wird entweder über zugängliche bzw. unzureichend geschützte Schnittstellen in den Rechner eingebracht, oder es wird versucht, das Auszahlmodul des Automaten direkt durch von den Tätern eingebrachte Hardware (Mini-PCs) anzusprechen. Anschließend erfolgt über den infizierten Rechner des Geldautomaten ein Zugriff auf das Auszahlungsmodul des GA mit dem Ziel, unautorisierte Bargeldauszahlungen zu veranlassen. Im In- und Ausland sind entsprechende Fälle bekannt.

Beim **Blackboxing** handelt es sich um eine Variante des Jackpotting, bei der die Täter den Geldautomaten öffnen, die Kommunikation zwischen dem Rechner des Geldautomaten und dem Auszahlungsmodul unterbrechen und anschließend einen „tätereigenen" Rechner (Blackbox) an das Auszahlungsmodul anschließen, um unautorisierte Bargeldauszahlungen zu veranlassen.

Beim **Man in the Middle-Angriff** hackt sich der Täter in die Kommunikation zwischen dem GA und dem Bankennetz. Er schafft sich so Zugriff auf den Datenverkehr und schaltet sich aktiv zwischen die Kommunikationspartner. So kann er die Daten einsehen und zu seinen Zwecken manipulieren.

Beim **Reversal Fraud-Angriff** wird während der Auszahlung ein Fehlerzustand im GA erzeugt, der dazu führt, dass das Geld nicht ausgegeben wird. Im Zuge dessen wird der belastete Betrag dem Kundenkonto wieder gutgeschrieben. Durch geeignete Mittel, die den Ausgabemechanismus manipulieren, wie z. B. das Montieren einer Kralle o. ä., sorgt der Täter dafür, dass das Geld nicht zurück in den Vorrat transportiert und später von ihm entnommen werden kann.

5 Grundsätzliche Empfehlungen

5.1 Allgemeines

Der Einsatz von Geldautomaten hat zur Folge, dass der Umgang und die Verwahrung von Banknoten in großem Umfang aus gesicherten Bereichen in den öffentlichen Raum verlagert werden. Bei potenziellen Tätern führt die Verlagerung zu einer Steigerung des Tatanreizes. Mögliche Tätervorgehensweisen wurden im vorangegangenen Kapitel dargestellt.

Bei der Erstellung wirksamer Schutzkonzepte spielen viele Faktoren eine Rolle. In diesem Kapitel werden der Einfluss der Aufstellsituation des GA sowie grundsätzliche Ausführungen zur Zielstellung von Sicherungsmaßnahmen beschrieben. Die Abschnitte 5.4 bis 5.7 greifen diese Aspekte auf und bilden auf dieser Grundlage Maßnahmenpakete gegen verschiedene Angriffsszenarien ab.

Der Einsatz von Sicherungsmaßnahmen sollte mit den jeweiligen Beteiligten und relevanten Akteuren abgestimmt sein. Vor dem Einsatz ist eine umfassende Risikobetrachtung durchzuführen.

Bei der Frage nach der Wirksamkeit einzelner Maßnahmen hinsichtlich konkreter Angriffsszenarien ist Kapitel 6 zurate zu ziehen.

Relevante Aspekte für die Umsetzung einzelner Maßnahmen sind in Kapitel 7 beschrieben.

5.2 Einfluss der Aufstellsituation des GA

Grundsätzlich ist jeder GA unabhängig von der Aufstellsituation potenziell gefährdet. Dennoch können Bedingungen gegeben sein, die Angriffe erschweren oder begünstigen. Die Kombinationen der Einbauumstände und möglicher Angriffsszenarien müssen analysiert werden, um daraus differenzierte Schadenverhütungsmaßnahmen für das konkrete Objekt abzuleiten und umzusetzen.

Bei der Gesamtbetrachtung der Angriffsszenarien wird offensichtlich, dass der gesicherte Wandeinbau (Rearload-Automaten in Verbindung mit einem mechanisch gesicherten und elektronisch überwachten Rückraum) eine spürbare Verringerung des Tatanreizes bewirkt. Für praktisch alle weiteren Aufstellungsvarianten ergeben sich ein erhöhtes oder sogar ein hohes Gefährdungspotenzial. Tatbegünstigende oder -erschwerende Konstellationen sind bezogen auf verschiedene Aufstellungsarten und Angriffsszenarien in Bild 5-1 dargestellt.

Abweichend von ortsfesten Aufstellvarianten kommen auch mobile Systeme zum Einsatz (z. B. in fahrbaren Geschäftsstellen oder als mobiler GA). Hierbei muss die Gefährdung in Abhängigkeit von der konkreten Nutzungs- und Aufstellungssituation individuell betrachtet und ein spezielles Sicherungskonzept mit dem Versicherer abgestimmt werden, um eine auf den individuellen Fall abgestimmte Gesamtlösung zu erhalten.

Das Gefährdungspotenzial für Manipulationen am GA, wie sie in Abschnitt 4 beschrieben sind, ist

Aufstellungsort	Einbausituation	FL/RL	Bereich entsprechend VdS 2472/ VdS 2311*	EMA	Angriffe mit mechanischen oder/und thermischen Angriffs-werkzeugen	Total-entwendung	Sprengung (Gas- oder Fest-sprengstoff)
in Bereichen mit 24 h-Bewirtschaftung und direkter ständiger Einsichtnahme*	Wandeinbau	Frontload	gesichert	mit EMA			
				ohne EMA			
			nicht gesichert	mit EMA			
				ohne EMA			
		Rearload	gesichert	mit EMA			
				ohne EMA			
			nicht gesichert	mit EMA			
				ohne EMA			
	frei aufgestellt	Frontload		mit EMA			
				ohne EMA			
Bankfiliale	Wandeinbau	Frontload	gesichert	mit EMA			
				ohne EMA			
			nicht gesichert	mit EMA			
				ohne EMA			
		Rearload	gesichert	mit EMA			
				ohne EMA			
			nicht gesichert	mit EMA			
				ohne EMA			
	frei aufgestellt	Frontload		mit EMA			
				ohne EMA			
in Containern/Pavillons (keine feste Bauweise)	Wandeinbau	Frontload	gesichert	mit EMA			
				ohne EMA			
			nicht gesichert	mit EMA			
				ohne EMA			
		Rearload	gesichert	mit EMA			
				ohne EMA			
			nicht gesichert	mit EMA			
				ohne EMA			
	frei aufgestellt	Frontload		mit EMA			
				ohne EMA			
Drittstandorte innerhalb von Gebäuden (z. B. Shopping Center oder Container/Pavillons in fester Bauweise)	Wandeinbau	Frontload	gesichert	mit EMA			
				ohne EMA			
			nicht gesichert	mit EMA			
				ohne EMA			
		Rearload	gesichert	mit EMA			
				ohne EMA			
			nicht gesichert	mit EMA			
				ohne EMA			
	frei aufgestellt	Frontload		mit EMA			
				ohne EMA			
Drittstandorte außerhalb von Gebäuden (z. B. Bahnhöfe)				mit EMA			
				ohne EMA			

*) überwachter gesicherter Bereich entsprechend der Richtlinien VdS 2472/VdS 2311

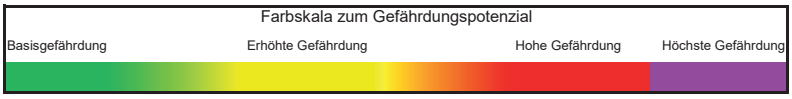

Bild 5-1: Gefährdungspotenzial von ortsfesten GA

getrennt von der o. g. Aufstellung einzuschätzen. Neben den Gerätetypen (die von den Tätern genutzten Manipulationswerkzeuge sind in der Regel automatenspezifisch) spielt in diesem Kontext vor allem eine hohe Nutzungsfrequenz eine Rolle, da die Täter in kurzer Zeit eine Vielzahl von Karten (-daten) erlangen bzw. Bargeld abfangen wollen.

5.3 Ziel der Sicherungsmaßnahmen

Alle Sicherungs- und Überwachungsmaßnahmen (vgl. Bild 5-2) sowohl unmittelbar am Geldautomaten als auch in dessen Umfeld haben zum Ziel, z. B.:

- Tatanreize herabzusetzen
- Zeit zu gewinnen, damit der Täter seinen Angriff abbricht
- mögliche Tatausführungen wesentlich zu erschweren
- Chancen zu erhöhen, Täter im Verlauf eines Tatversuchs zu ergreifen

Als Sicherungsebene, die unmittelbar gegen aktive Zugriffsversuche eines Täters auf Bargeld oder ähnliche Werte wirkt, dient die mechanische oder physikalische Sicherung. Zu nennen sind zum einen stabile, angemessenen technischen Kriterien genügende Wertbehältnisse. Weiter kommen bei den mechanischen Sicherungen die Konstruktion und Ausgestaltung relevanter Gebäude und Räume zum Tragen, die so ausgebildet sein sollten, dass der Zugang zu vorhandenen Werten von vornherein wirksam erschwert ist.

Bild 5-2: Zusammenspiel verschiedener Sicherungsmaßnahmen

Eine weitere Sicherungsebene stellt die elektronische Überwachung durch geeignete Technik (z. B. EMA, VÜA) dar. Diese erkennt einen bevorstehenden oder begonnenen Angriff und ermöglicht, situationsbezogen geeignete und im Vorfeld abgestimmte Interventionsmaßnahmen einzuleiten.

Die Zeit, die der Täter zur Überwindung der Sicherungsmaßnahmen benötigt, wird Widerstandszeit genannt. Sie sollte so bemessen sein, dass es mit der eingeleiteten Intervention möglich ist, den Täter noch im Verlauf des Zugriffsversuchs (in flagranti) zu ergreifen. Die Tatdauer und die individuelle Interventionszeit müssen somit aufeinander abgestimmt sein; die erforderliche Tatdauer sollte die Interventionsdauer unbedingt überschreiten (vgl. Bild 5-3).

Der zumeist langen Interventionsdauer bei Nacht stehen kurzen Tatbegehungszeiten bei Sprengungen (3–5 Minuten) aber auch bei hydraulischen Angriffen gegenüber. Dadurch erreichen Interventionskräfte selten den Tatort so zeitig, dass sie die Täter noch antreffen. Aus diesem Grunde ist es besonders bei diesen Tatbegehungsweisen notwendig, den Tatanreiz schon bei der Tatplanung so weit herabzusetzen, dass die Täter ihren Angriffsplan für diesen GA gar nicht erst weiterverfolgen.

Eine Maßnahme, den Tatanreiz zu verringern kann neben sichtbaren, baulich-mechanischen Maßnahmen beispielsweise auch der deutliche Hinweis auf umgesetzte, VdS-anerkannte elektronische Schutzmaßnahmen wie Einfärbungs- oder Nebelsysteme (vgl. Abschnitt 6.3) sein.

Um möglichst viel Zeitpuffer für die Interventionsmaßnahmen zu erreichen, ist es sinnvoll, dass

- mit gestaffelten Sicherungen gearbeitet wird, die dem Täter einen schnellen Zugriff verwehren (z. B. indem ein Wertbehältnis mit hohem Anerkennungsgrad mit Anbindung an die Einbruchmeldeanlage in einem mechanisch gesicherten und elektronisch überwachten Raum aufgestellt und verankert wird)
- die Tat frühzeitig, vorzugsweise unmittelbar nach Beginn der Überwindungsversuche, erkannt und gemeldet wird
- der Täter, möglichst viel Zeit auf die Überwindung mechanischer Sicherungen verwenden muss.

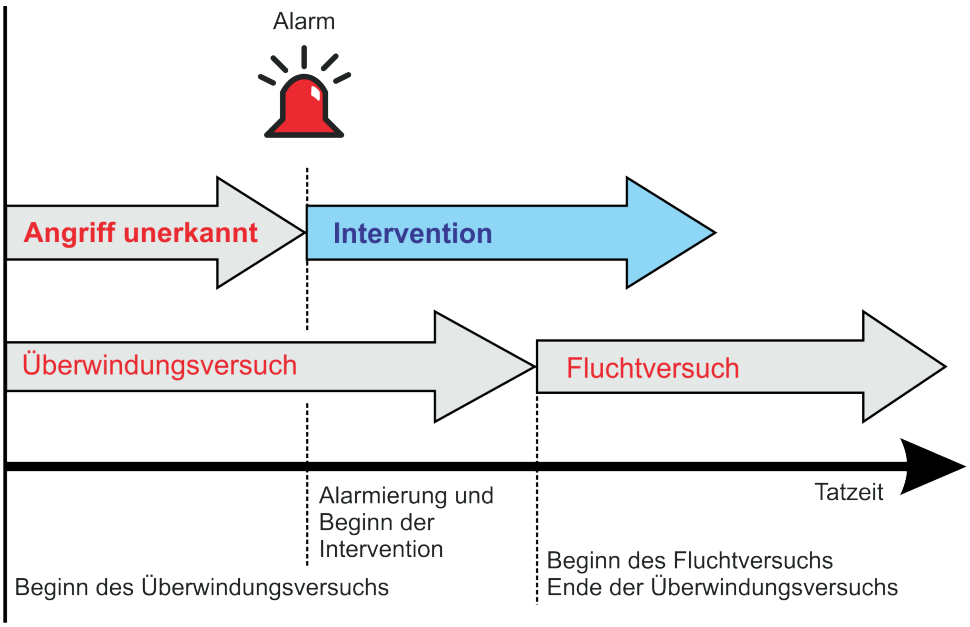

Bild 5-3: Zusammenspiel Tatvorgang und Intervention

Die technischen Maßnahmen sollten unbedingt umgesetzt und um organisatorische Maßnahmen, z. B. Foyerschließung zu betriebsarmen Zeiten ergänzt bzw. mit diesen kombiniert werden.

5.4 Maßnahmen gegen Sprengung

Um Sprengangriffen zu begegnen, bieten sich unter anderem die im Folgenden aufgeführten Maßnahmen an. Diese können gemeinsam oder, je nach ermittelter Risikolage, auch alternativ umgesetzt werden.

Mechanische Sicherungsmaßnahmen

- Einbau oder Nachrüstung solider Verschlüsse aller systembedingten Öffnungen zum Wertgelass – insbesondere der „leicht zugänglichen Öffnungen“ (Shutter, Kabeldurchführungen etc.)
- Einsatz von zertifizierten Wertbehältnissen, die einen hohen Widerstandswert besitzen und zudem über eine nachgewiesene Widerstandsfähigkeit gegen Sprengungen mit Gas bzw. Sprengstoff (vgl. Abschnitt 7.5) verfügen
- Einbau oder Nachrüstung von Verstärkungsmaßnahmen am Gehäuse (z. B. Haubenöffnungsmechanismus), sowie an der Tür oder sonstigen Schwachstellen, durch die jeweils systembedingte Öffnungen im Wertbehältnis zugänglich werden
- Äußere Gebäudehülle des GA Standortes, insbesondere Zugangs- und Foyertüren in verstärkter Ausführung, um bei gleichzeitigem Nacht-Verschluss einen erhöhten Widerstandszeitwert zu erreichen
- gesicherter Wandeinbau und der Einsatz von Rearload-GA
- Ausführung der Wände des Raumes in fester Bauweise (min. VdS-Klasse A), um Zugang zum Versorgungsraum und damit zur Rückseite des GA wirksam zu behindern
- Ausführung der Zugänge des Versorgungsraumes einbruchhemmend (min. VdS-Klasse A)
- vorhandene Fenster im Versorgungsraum mit Sichtschutz ausstatten
- vorhandene Fenster einbruchhemmend, mindestens in VdS-Klasse A ausführen
- alternativ zur einbruchhemmenden Ausführung ggf. Vergitterung des Fensters umsetzen (Vergitterung in zertifizierter Ausführung mindestens der VdS-Klasse A entsprechend)

Elektronische Überwachungs- und Sicherungsmaßnahmen

- Überwachung des GA bzw. des Aufstellortes mit Videotechnik, wobei diese den Angriff nicht verhindert bzw. behindert aber der Erkennung der Tat dient und für die Ergreifung der Täter dienlich sein kann (vgl. Abschnitt 7.11)
- Sofern die Videoüberwachung, die ein aktives Eingreifen ins Geschehen ermöglicht (z. B. direkte Ansprache des Täters über Lautsprecher), eröffnet die Chance, dass ein Abschreckungseffekt gegenüber dem Täter greift
- Einsatz von Vernebelungssystemen zur Verhinderung oder Verzögerung der Tatausführung
- Zargen-Einbau und Verwendung von Rearload-Geräten sowie Überwachung des GA-Versorgungsraums mit einer VdS-anerkannten Einbruchmeldeanlage Klasse C-SG 4
- Einbau oder Nachrüstung von technischen Vorrichtungen, die den Zugang zu systembedingten Öffnungen und somit das Einleiten von Gas/Festsprengstoffen
  - behindern (z. B. zusätzliche Verriegelungen, Verschluss systembedingter Öffnungen oder volumenreduzierende Maßnahmen)
  - verzögern (z. B. Bedienfeldverriegelungen, Kabeldurchführungsabdeckungen, Rollladen),
  - detektieren (z. B. Gasmelder)

  um Schäden zu minimieren. Die Kombination der oben genannten Maßnahmen mit elektronischer Überwachung (Einbruchmeldeanlage für GA und Rückraum sowie ggf. Foyerüberwachung) ermöglicht die frühzeitige Einleitung von Interventionsmaßnahmen.

Organisatorische Maßnahmen

- Zugänglichkeit zum GA außerhalb von Zeiten erhöhter personeller Präsenz möglichst einschränken (z. B. Nachtverschluss)
- schnelle Intervention

5.5 Maßnahmen gegen Totalentwendung

Die Täter müssen, um eine Chance auf Erfolg zu haben, Zugriff auf das Wertbehältnis erlangen. Mit Ausnahme des Angriffs mit schweren Baumaschinen können sämtliche Angriffe mit dem Ziel der Totalentwendung durch das Zusammenspiel mechanischer und elektronischer Sicherungsmaßnahmen wirksam erschwert werden.

Mechanische Sicherungsmaßnahmen

- Um die Möglichkeit, Zugseile o. ä. um den GA herumzulegen wirksam zu behindern, sollten ein Zargeneinbau bevorzugt werden (vgl. Bild 7-2 und Bild 7-3).
- Um den Zugang zum Versorgungsraum und damit zur Rückseite des GA wirksam zu behindern, sind die Wände des Raumes in fester Bauweise auszuführen.
- Die Zugänge des Versorgungsraumes sind einbruchhemmend mindestens in VdS-Klasse A auszuführen.
- Vorhandene Fenster im Versorgungsraum müssen über einen Sichtschutz verfügen

und sind einbruchhemmend, mindestens in VdS-Klasse A auszuführen. Alternativ zur einbruchhemmenden Ausführung kann eine Vergitterung des Fensters sinnvoll sein. Die Vergitterung muss in zertifizierter Ausführung mindestens der VdS-Klasse A entsprechen.
- Bei GA ist die fachgerechte Verankerung grundsätzlich erforderlich (siehe Zertifikat des GA).
- Geldautomaten sollten keinesfalls frei aufgestellt werden: ein gesicherter Wandbau ist zu empfehlen (Zugänge des Versorgungsraumes und Wände einbruchhemmend).
- Ist ein GA dennoch freistehend, sollte dieser so angeordnet werden, dass Angriffe mit Fahrzeugen wie Umstoßen oder Abreißen erschwert werden. Erreichbar ist das z. B. durch Erschwerung der Zufahrt und damit der Behinderung der Erreichbarkeit des GA mit einem Fahrzeug (z. B. durch Nutzung von Pollern, schweren Steinen, Blumenkübeln, Bäumen).

Eine fachgerechte Befestigung des GA und ggf. des Sockels wird durch die Verwendung der gem. Zertifikat vom Hersteller gelieferten bzw. vorgegebenen Montagematerialen und der Verankerung entsprechend der Herstellervorgaben erreicht. Bei der Montage ist insbesondere darauf zu achten, dass diese auf die Wand- bzw. Bodenkonstruktionen und -materialien abgestimmt ist.

Elektronische Überwachungs- und Sicherungsmaßnahmen
- Überwachung des GA durch EMA gemäß VdS 2311, u. a. auf Abriss, z. B. mittels Abrissmelder
- Die EMA-Absicherung des GA-Versorgungsraums sollte gemäß VdS-Klasse C-SG5 erfolgen.
- Ereignisgesteuerte Videoüberwachung mit Einbindung in die Einbruchmeldeanlage (und die damit verbesserten Interventionsmöglichkeiten)
- Das Foyer sollte in die Überwachung durch die EMA in Form einer „Perimeterüberwachung" einbezogen werden (siehe entsprechendes Mustersicherungskonzept im Leitfaden Perimeter, VdS 3143).
- Außerhalb der Geschäftszeiten sollte eine zeitgesteuerte Aktivierung der Foyerüberwachung gegeben sein, um Angriffe auf Teile des Foyers oder GA oder Vandalismus zu erkennen und Gegenmaßnahmen einleiten zu können. Da es sich bei den Angriffen auf GA sehr häufig um Blitzeinbrüche handelt, ist der Alarm aus dem Foyer mit höchster Priorität zu verfolgen. Bei gegebener ereignisgesteuerter Live-Bildübertragung aus dem Foyer kann die NSL unverzüglich eine Alarmverifikation vornehmen und entsprechende Interventionsmaßnahmen einleiten.
- Bei Geschäftsstellen, für die im Rahmen der Gefährdungsanalyse auch der Angriff mit schweren Fahrzeugen als realistische Bedrohung erkannt wird, sollten aufgrund dieser besonderen Sachlage zusätzliche Sicherungsmaßnahmen wie z. B. VdS-anerkannte Ortungs- und/oder Einfärbesysteme eingesetzt werden.

5.6 Maßnahmen gegen Vandalismus

Ausschlaggebend für die Auswahl wirkungsvoller Gegenmaßnahmen ist die Ermittlung der standortbezogenen Risiken (vgl. Abschnitt 3.5.2). Erst dann kann die Gefährdung durch den alternativen oder parallelen Einsatz unterschiedlicher Maßnahmen wirksam reduziert werden. Geeignet, um das gewünschte Schutzziel zu erreichen, ist der Einsatz von:

- Zutrittskontrollanlagen zum Foyer bzw. zum GA-Standort
- Zutrittskontrollanlagen in Verbindung mit Zeitfenstern
- Videotechnik mit
  - Portraitkamera im GA
  - Sensorik in bestimmten Zeitfenstern (z. B. 00:00 bis 05:00 Uhr)
  - Sensorik und/oder virtuellem Wächterrundgang
  - akustischer Ansprache von (potenziellen) Tätern
- personeller Bewachung/Kontrolle
- zeitlich befristete Schließung von SB-Foyers bzw. GA-Standorten
- 3D-Sensoren (Erkennung kundenuntypischen Verhaltens mittels 3D-Scanner)

5.7 Maßnahmen gegen indirekte Angriffe

Gegen Angriffe, die das Ziel haben, in den Besitz fremder Bankkarten sowie der entsprechenden Identifikationsnummern (PIN) zu gelangen, bieten die GA-Hersteller unterschiedliche Sicherheitsprodukte/-lösungen an. Darüber hinaus sollten die Kunden zu einem sorgfältigen Umgang mit den entsprechenden Karten angehalten werden.

Unter anderem sollten die Kunden

- die PIN stets verdeckt (z. B. unter der darüber gehaltenen Hand) eingeben
- die PIN nicht notieren (weder auf der Karte oder als Telefonnummer getarnt)
- die Karte stets sorgfältig verwahren.

Es wird empfohlen, an allen GA einen PIN-Sichtschutz gemäß den Sicherheitskriterien der Deutschen Kreditwirtschaft einzusetzen, um die Aus-

spähung der PIN durch Dritte zu erschweren und die Awareness der Kunden zu erhöhen.

Gegen Cyberangriffe bieten GA-Hersteller unterschiedliche Softwareprodukte an, unter anderem Festplattenverschlüsselung, Zugangskontrolle zum SB-System und Schutz gegen Malware (z. B. gegen Jackpotting oder Blackboxing).

6 Wirkung der Schutzmaßnahmen

6.1 Allgemeines

Um Angriffen zu begegnen, bieten sich die im Folgenden aufgeführten Maßnahmen an. Die Maßnahmen können gemeinsam oder, je nach ermittelter Risikolage, auch alternativ umgesetzt werden. Nicht alle Maßnahmen wirken gegen alle Angriffe. In den nachfolgenden Abschnitten wird daher die Wirksamkeit in Form von Tabellen dargestellt.

Dabei bedeuten

-	Keine Wirkung gegen diese Angriffsart gegeben
o	Bedingte oder mittelbare Schutzwirkung ggfs. gegeben
+	Unmittelbare Schutzwirkung gegen diese Angriffsart gegeben
++	Sehr gute und unmittelbare Schutzwirkung gegen diese Angriffsart gegeben

Die nachfolgende Wirksamkeitsbetrachtung besitzt nur dann Gültigkeit, wenn die in Kapitel 7 formulierten Anforderungen erfüllt sind.

Es wird empfohlen, die jeweilige Schutzmaßnahme vorab mit dem Versicherer abzustimmen. Rechtliche Aspekte bei der Auswahl von Schutzmaßnahmen sind durch den Betreiber zu prüfen und zu bewerten. Die nachfolgende Einstufung berücksichtigt diese Aspekte nicht, sondern beschränkt sich auf die Betrachtung der Wirkmechanik von Angriff und Gegenmaßnahme.

6.2 Mechanische Schutzmaßnahmen

6.2.1 Wertbehältnis Grad IV mit Zusatzkennzeichnung EX und GAS

Für Geldautomaten sind Wertbehältnisse des Widerstandsgrades VdS-Grad IV (VdS 2450) mit einem VdS-zertifizierten Schutz gegen Sprengangriffe (Zusatzkennzeichnung EX und GAS) erhältlich.

Schutzmaßnahme wirksam zur Verhinderung von:

Spreizen	Angriff mit Winkelschleifer	Thermische Angriffe	Totalentwendung	Sprengen mit Gas	Sprengen mit Festsprengstoff
o	+	+	-	+	+

Ab Widerstandsgrad VdS-Grad IV erschwert das Behältnis auch andere mechanische Angriffsarten signifikant.

6.2.2 Verriegelung systembedingter Öffnungen

Das einfache Öffnen/Aufhebeln der Verriegelung des Gerätekopfes wird durch mechanische Maßnahmen verhindert.

Durch elektromechanische Verriegelung der Geldausgabeöffnungen des Wertbehältnisses und dem stabilen Verschluss aller sonstigen systembedingten Öffnungen des Wertbehältnisses, z. B. mittels geeigneter Verblendungen, wird vorrangig die Einleitung von Sprengstoff verhindert.

Die Umsetzung ist in der Regel individuell und im Rahmen der Nachrüstung möglich. Eine Zertifizierung ist bisher nicht vorgesehen.

Schutzmaßnahme wirksam zur Verhinderung von:

Spreizen	Angriff mit Winkelschleifer	Thermische Angriffe	Totalentwendung	Sprengen mit Gas	Sprengen mit Festsprengstoff
-	-	-	-	+	+

6.2.3 Einbruchhemmender Rollladen

Zu Zeiten der Nichtbenutzung des Geldautomaten wird ein einbruchhemmender Rollladen heruntergelassen, der den Zugriff auf das Bedienfeld des Geldautomaten verhindert und ihn vor Angriffen schützt. Der Rollladen läuft in stabilen Führungsschienen und ist gemäß VdS 2534 bzw. DIN EN 1627 in der Klasse A ausgeführt sowie alarmgesichert.

Schutzmaßnahme wirksam zur Verhinderung von:

Spreizen	Angriff mit Winkelschleifer	Thermische Angriffe	Totalentwendung	Sprengen mit Gas	Sprengen mit Festsprengstoff
-	-	-	-	+	+

6.2.4 Gesicherter Bereich

Der Zutritt zum rückwärtigen Bereich wird dadurch erschwert, dass die Wand in durchbruchhemmender Qualität ausgeführt wird. Weitere Raumelemente wie Türen, Fenster und Vergitterungen werden in VdS Klasse A ausgeführt. Dazu zählt auch die Ausführung der Frontblende bzw. des Zargenelementes in durchbruchhemmender Qualität.

Schutzmaßnahme wirksam zur Verhinderung von:

Spreizen	Angriff mit Winkelschleifer	Thermische Angriffe	Totalentwendung	Sprengen mit Gas	Sprengen mit Festsprengstoff
+	+	+	+	+	+

6.3 Elektronische Schutzmaßnahmen

6.3.1 Einbruchmeldeanlage und Videoüberwachung

Die Einbruchmeldeanlage dient der frühzeitigen Erkennung eines Angriffes auf den Geldautomaten und der Einleitung zeitnaher Interventionsmaßnahmen. Durch eine Vorfeldüberwachung, z. B. verschlossenes SB-Foyer, kann die Intervention zwischen Detektion und Angriff wesentlich schneller eingeleitet werden.

In Kombination mit einer Videoüberwachungsanlage kann eine effiziente Alarmverifikation erreicht werden.

Eine eigenständige Videoüberwachung mit integrierter Videoanalytik zur Detektion kann ebenfalls zum frühzeitigen Erkennen und Verifizieren von Angriffen genutzt werden.

Schutzmaßnahme wirksam zur Verhinderung von:

Spreizen	Angriff mit Winkelschleifer	Thermische Angriffe	Totalentwendung	Sprengen mit Gas	Sprengen mit Festsprengstoff
o	o	o	o	o	o

Diese Maßnahme allein ist nicht gegen Angriffe wirksam, sondern dient der Prävention und Einleitung einer schnellen Intervention.

6.3.2 Zündsysteme für Explosivgase

Bei diesen Systemen wird innerhalb des Wertbehältnisses für Geldautomaten eine Vorrichtung installiert, die nach jeder Detektion explosiver Gase einen Zündfunken erzeugt. Dies soll sicherstellen, dass eingeleitetes, explosives Gasgemisch in kleinen, unschädlichen Mengen sofort (ggf. wiederkehrend) zur Zündung gebracht wird, so dass es sich nicht ansammeln und größeren Schaden verursachen kann.

Schutzmaßnahme wirksam zur Verhinderung von:

Spreizen	Angriff mit Winkelschleifer	Thermische Angriffe	Totalentwendung	Sprengen mit Gas	Sprengen mit Festsprengstoff
-	-	-	-	++	-

6.3.3 Antigas-Systeme

Ins Wertbehältnis eingebrachtes Sprenggas wird mit technischen Meldern erkannt, um in der Folge spezielle Gase oder Pulver freizusetzen. Diese greifen entweder in die chemische Reaktion zwischen dem Sprenggas und Sauerstoff ein, um die Zündung des Sprenggases zu unterbinden bzw. zu hemmen (Inertisierung) oder sie sorgen für einen Verdrängungseffekt, so dass sich kein explosives Gas ansammeln kann. Die Wirkungsdauer ist abhängig von der Füllmenge, die im Antigas-System gespeichert sein kann.

Schutzmaßnahme wirksam zur Verhinderung von:

Spreizen	Angriff mit Winkelschleifer	Thermische Angriffe	Totalentwendung	Sprengen mit Gas	Sprengen mit Festsprengstoff
-	-	-	-	+	-

6.3.4 Vernebelungstechnik

Bei der Vernebelungstechnik wird die Tatausführung erschwert bzw. unterbunden, indem ein Nebelgerät ausgelöst wird, welches innerhalb kürzester Zeit den Raum mit Sicherheitsnebel füllt. Dadurch wird dem Täter die Sicht genommen.

Teilautomatische Variante

Voraussetzung für den Einsatz ist, dass durch qualifizierte Bewertung der Sachlage eindeutig ein unmittelbar bevorstehender Angriff erkannt wird. Dies kann z. B. mittels Videoüberwachung realisiert werden, die auslöst, wenn das ansonsten verschlossene Foyer gewaltsam geöffnet wird. Das Alarmvideo wird an eine Notruf- und Serviceleitstelle übertragen. Der Sicherheitsmitarbeiter bewertet die Lage anhand dessen und steuert das Nebelsystem an.

Vollautomatische Variante

Im Gegensatz zur teilautomatischen Variante ist bei der vollautomatischen Lösung kein menschliches Handeln erforderlich. Durch Gas- oder Aufbruchmelder im Geldautomaten wird der Angriff vollautomatisch detektiert und in der Folge das Vernebelungsgerät angesteuert.

Der Einsatz von Vernebelungstechnik sollte mit allen Beteiligten (Polizei, Feuerwehr, Sicherheitsdienstleister, Betreiber) abgestimmt und Bewohner informiert sein.

Schutzmaßnahme wirksam zur Verhinderung von:

Spreizen	Angriff mit Winkelschleifer	Thermische Angriffe	Totalentwendung	Sprengen mit Gas	Sprengen mit Festsprengstoff
+	+	+	+	+	+

Diese Maßnahme allein ist nicht wirksam, sondern immer nur in Kombination mit zusätzlichen elektronischen Überwachungsmaßnahmen.

6.3.5 Einfärbungssysteme

Einfärbesysteme, auch Intelligent Banknote Neutralisation Systems genannt, färben im Alarmfall das in den Geldkassetten befindliche Bargeld mit Sicherheitstinte ein, wodurch dieses gekennzeichnet und dessen Verwendung erschwert wird.

Die Auslösung kann durch unterschiedliche Sensoren (Lage-/Schock-/Gas-/Temperatur-/Körperschall-, sonstige Sensorik) oder die unzulässige Entnahme der Geldkassetten erfolgen.

Einfärbesysteme, bei denen eine zuverlässige Auslösung auch durch Gas- oder Festsprengstoffexplosionen erfolgt, müssen dies in einer unabhängigen Prüfung und Zertifizierung nachweisen. IBNS wirken nur dann sicher gegen Sprengangriffe, wenn dies im Rahmen des Prüfverfahrens nachgewiesen wurde. In diesem Falle kann von einer unmittelbaren Schutzwirkung („+“) gegen sämtliche Angriffsarten ausgegangen werden. Darüber hinaus realisiert eine Einfärbung allenfalls sekundären Schutz, da der Angriff auf den Geldautomaten nicht unterbunden wird. Eine präventive Wirkung ist nur bei flächendeckend einheitlicher Ausstattung und Kennzeichnung zu erwarten.

Schutzmaßnahme wirksam zur Verhinderung von:

Spreizen	Angriff mit Winkelschleifer	Thermische Angriffe	Totalentwendung	Sprengen mit Gas	Sprengen mit Festsprengstoff
o	o	o	o	o	o

Diese Maßnahme allein kann den Angriff nicht unterbinden und sollte daher in Kombination mit weiteren Schutzmaßnahmen zum Einsatz kommen.

6.3.6 Klebesysteme

Klebesysteme verkleben im Alarmfall das in den Geldkassetten befindliche Bargeld. Derzeit liegen keine gesicherten Erkenntnisse in Bezug auf Qualitätskriterien, Einsatzgrenzen und gesundheitliche Gefährdung vor, die eine belastbare Bewertung von Nutzen und Risiken gestatten.

6.3.7 Ortungssysteme

Mittels unauffälliger Sender, die mit spezieller Funktechnik arbeiten, können Geldbündel oder Geldkassetten geortet und „verfolgt“ werden. Das Ortungssystem muss auf eine geeignete Interventionsstelle aufgeschaltet sein.

Sofern eine Intervention durch die Polizei beabsichtigt ist, sind die technischen Voraussetzungen aus dem von den Landeskriminalämtern der Länder formulierten Anforderungsprofil für Ortungsgeräte zu erfüllen.

Darüber hinaus realisiert ein Ortungssystem allenfalls sekundären Schutz, da der Angriff auf den Geldautomaten nicht unterbunden wird. Eine präventive Wirkung ist nur bei flächendeckend einheitlicher Ausstattung und Kennzeichnung zu erwarten.

Schutzmaßnahme wirksam zur Verhinderung von:

Spreizen	Angriff mit Winkelschleifer	Thermische Angriffe	Totalentwendung	Sprengen mit Gas	Sprengen mit Festsprengstoff
o	o	o	o	-	-

Diese Maßnahme allein ist nicht wirksam, sondern immer nur in Kombination mit zusätzlichen Schutzmaßnahmen.

Bild 7-1: Gesamtkonzept Sicherung (ohne Gewichtung der einzelnen Maßnahmen)

6.4 Organisatorische Schutzmaßnahmen

6.4.1 Zutrittsbeschränkung

In nutzungsschwachen Zeiten wird der Zugang zum SB-Foyer verschlossen. Dies sollte vorrangig in der Zeit von 22:00 Uhr bis 6:00 Uhr erfolgen und sollte mit weiteren Maßnahmen kombiniert werden. Dazu zählen vor allem der Einsatz von zertifizierter Einbruchmeldetechnik, Videotechnik und Vernebelungssystemen.

Schutzmaßnahme wirksam zur Verhinderung von:

Spreizen	Angriff mit Winkel-schleifer	Thermi-sche Angriffe	Totalent-wendung	Sprengen mit Gas	Sprengen mit Fest-spreng-stoff
+	+	+	+	+	+

7 Wirksame Umsetzung von Schutzmaßnahmen

7.1 Gesamtkonzept

Abgeleitet aus den in Kapitel 3 ff. genannten Risiken ergeben sich generelle Sicherungsempfehlungen, die als Basismaßnahmen für die Absicherung von GA zu verstehen sind. Individualisierungen bei den Sicherungsmaßnahmen sind für jeden Einzelfall zu berücksichtigen. Diese ergeben sich aus den individuellen Gegebenheiten und Besonderheiten eines jeden GA, besonderen Gefährdungen, Schwachstellen oder dergleichen.

Insgesamt sollten, um ein umfassendes Gesamtkonzept einer Absicherung zu realisieren, alle in Bild 7-1 genannten Einzelaspekte berücksichtigt werden.

Ein Sicherungskonzept könnte sich beispielsweise aus diesen Komponenten zusammensetzen:

- Einsatz von zertifizierten Wertbehältnissen, die einen hohen Widerstandswert besitzen und zudem über eine nachgewiesene Widerstandsfähigkeit gegen Sprengungen mit Gas bzw. Sprengstoff (vgl. Abschnitt 7.5) verfügen
- Zugänglichkeit zum GA außerhalb von Zeiten erhöhter personeller Präsenz möglichst einschränken
- Überwachung des GA bzw. des Aufstellortes innerhalb von Gebäuden mit Einbruchmeldetechnik (diese behindert nicht den Aufbruch, dient aber der Angriffserkennung und Interventionseinleitung); vgl. Abschnitt 7.6
- Überwachung des GA bzw. des Aufstellortes mit Videotechnik (diese behindert i.d.R. nicht den Aufbruch, dient aber der Erkennung der Tat und kann der Ergreifung der Täter dienlich sein)
- Einsatz von Videotechnik, die ein aktives Eingreifen ins Geschehen ermöglicht (z. B. direkte Ansprache des Täters über Lautsprecher)
- Nutzung der Chance, dass ein Abschreckungseffekt gegenüber dem Täter greift; vgl. Kapitel 7.11

7.2 Aufstellort

Risiken für Geldautomaten können sich unter anderem aus seinem Aufstellort sowie der Aufstellungsart ergeben. Das heißt umgekehrt, dass sich über Ort und Art der Aufstellung das Risiko für den Automaten günstig beeinflussen lässt.

Grundsätzlich sollte der Aufstellort des GA so gewählt werden, dass möglichst wenig Angriffsarten zum Erfolg führen. Mit Bild 7-1 wird hierzu eine erste Entscheidungshilfe zu verschiedenen Aufstellorten gegeben.

Vorzugsweise ist ein GA im inneren Bereich von Geldinstituten aufzustellen, weil diese außerhalb der Geschäftszeiten nicht zugänglich sind.

Aber auch bei rund um die Uhr zugänglichen Geldautomaten kann die Zugänglichkeit durch die Art der Montage eingeschränkt werden. Die erfolgreiche Umsetzung vieler Angriffsarten lässt sich erschweren, indem der GA nicht „frei aufgestellt" ist. Ein frei aufgestellter Geldautomat zeichnet sich dadurch aus, dass er von allen vier Seiten aus zugänglich ist. Wenn der Automat aber z. B. in einer Wand verbaut ist, ist es für den Täter nur schwer oder gar nicht möglich, die Wände des Wertbehältnisses anzugreifen.

Einer besonderen Gefährdung unterliegen freistehende GA z. B. auf Parkplätzen, Bahnhöfen und vielen anderen weitläufigen und zumindest zeitweise verlassenen Standorten.

Jedoch stellen Drittstandorte für sich genommen nicht automatisch eine signifikante Risikoerhöhung dar; manche Standorte, sofern sie sich in einem belebten und rund um die Uhr („24/7") bewirtschafteten Umfeld befinden (z. B. am Flughafen, an großen Tankstellen) sind als deutlich risikoärmer zu werten als die vorgenannten zeitweise einsamen Lokationen. Hier kann nach Abwägung von Vor- und Nachteilen ggf. der Einsatz freistehender GA verantwortet werden.

7.3 Einbau

Die Gefährdung von GA wird neben dem Aufstellort maßgeblich von der Einbausituation beeinflusst. In praktisch allen Fällen ist es sinnvoll, einen Einbau von GA so vorzunehmen, dass die Kundenbedienseite und die Seite zur Ver- und Entsorgung bzw. Wartung räumlich durch eine Wand in fester Bauweise getrennt sind.

Eine Montage von Automaten im „Fensterzargen-Einbau" (vgl. Bild 7-2) ist im Vergleich zu alternativen Aufstellungslösungen zu bevorzugen. Am vorteilhaftesten ist es, den GA in der Wand des Ver- bzw. Entsorgungsraums zu montieren. Eine gute Alternative zu dieser Montageart stellt, sofern eine sichere Versorgung des Automaten realisierbar ist, ein in die Wand integrierter „Vollzargen-Einbau" (vgl. Bild 7-3) dar.

Damit werden die Angriffsmöglichkeiten auf den GA deutlich eingeschränkt. Optimal ist ein Wandeinbau, der eine Ver-/Entsorgung aus einem separaten Raum heraus erfordert.

Unabhängig davon, ob eine freistehende Aufstellung oder ein Zargen-Einbau favorisiert wird, muss ein GA, um die Wegnahme oder einen Angriff mit Werkzeugen vor Ort zu erschweren, am Aufstellort stabil montiert werden. Hinweise dazu finden sich in Abschnitt 7.5.3.

7.4 Gesicherter Ver- und Entsorgungsraum

Das Wertbehältnis des Geldautomaten, insbesondere die Wertbehältnistür ist bestmöglich gegen Angriffe zu schützen. Der Raum muss gemäß VdS 2472 dem gesicherten Bereich zugeordnet und für den berechtigten Personenkreis ohne Gefährdung der eigenen Person erreichbar sein. Daher muss der Versorgungsraum mechanisch hohen Anforderungen genügen:

- Die Wände des Versorgungsraums sind in fester Bauweise auszuführen (die Wände können z. B. mit mindestens 120 mm Dicke in Kalksandstein gemauert oder als Betonwand oder aber als einbruchhemmende Verbundbauwand der VdS-Klasse A ausgeführt sein).
- Um Tätern den Zutritt wirksam zu erschweren, sind Türen selbstschließend, an der Außen- bzw. Zugangsseite mit einem nicht drehbaren Knauf (kein Drehknauf oder Türdrücker) sowie mindestens in einbruchhemmender Ausführung gemäß VdS-Klasse A auszuführen; sie sollten keine Verglasung aufweisen.
- Der Zutritt von Personen zum Versorgungsraum muss geregelt sein. Grundsätzlich ist eine Zutrittskontrollanlage der VdS-Klasse B mit der Möglichkeit zur Auslösung eines Überfallalarms vorzusehen. Alternativ darf der Raum nur nach entsprechender Autorisierung begehbar sein.
- Der Raum sollte fensterlos sein. Sind Fenster vorhanden, muss der Einblick auf die darin befindlichen Wertbehältnisse verhindert sein und die Fenster sind in einbruchhemmender Ausführung mindestens der VdS-Klasse A auszuführen.
- Alternativ zur einbruchhemmenden Ausführung kann eine Vergitterung des Fensters sinnvoll sein. Die Vergitterung muss in zertifizierter Ausführung mindestens der VdS-Klasse A erfolgen.

Um im Falle eines Angriffes im Verlauf der Ver- oder Entsorgung von GA mit Banknoten Hilfe herbeirufen zu können, sollte der Versorgungsraum mit einem Überfallmelder ausgestattet und ebenso wie der Vorraum in die Videoüberwachungsanlage eingebunden sein.

7.5 Wertbehältnisse

7.5.1 Prüfung und Zertifizierung

Eine wesentliche Maßnahme gegen Angriffe auf Geldautomaten ist der ausschließliche Einsatz von zertifizierten Wertbehältnissen.

Da es nicht möglich ist, durch bloße Inaugenscheinnahme des Wertbehältnisses dessen Qualität hinsichtlich seiner Aufbruchsicherheit zu erkennen, ist es dringend erforderlich, für den Einsatz in Geldautomaten nur solche Wertbehältnisse zu verwenden, die die Prüfung in einem unabhängigen Labor absolviert haben und eine Zertifizierung gemäß VdS 2450 bzw. EN 1143-1 aufweisen. Der Hersteller kann die Produktqualität mit dem verliehenen Zertifikat nachweisen. Für den Besitzer/Nutzer des Wertbehältnisses ist der Widerstandsgrad auf der an der Innenseite der Behältnistür angebrachten Anerkennungsplakette dokumentiert (vgl. Bild 7-4).

Anmerkung: Weiterführende Informationen können den Technischen Kommentaren von VdS (VdS 3134) entnommen werden.

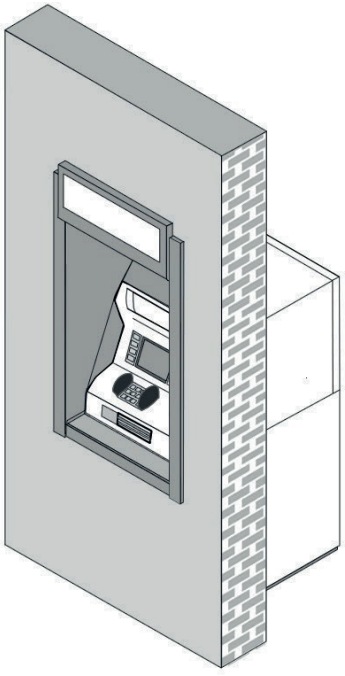

Bild 7-2: Fensterzargen-Einbau

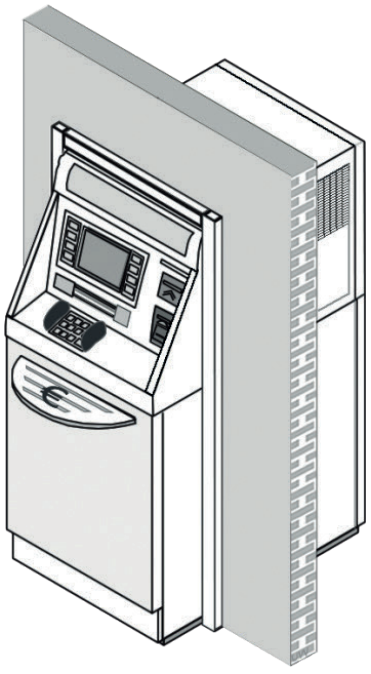

Bild 7-3: Vollzargen-Einbau

Bild 7-4 :GA-Plakette

7.5.2 Einsatzempfehlungen

Generell kann davon ausgegangen werden, dass das Risiko für einen Geldautomaten bzw. für das Wertbehältnis eines Geldautomaten mit Werkzeugen angegriffen zu werden, umso höher ist, je einfacher dieser erreichbar ist und umso einfacher sich ein potenzieller Transport und Einsatz von Werkzeugen gestalten würde. Je nach Lage und Erreichbarkeit des Geldautomaten sowie je nach Umfang der aufbewahrten Werte ist der Widerstandsgrad des Wertbehältnisses auszuwählen.

Für den Einsatz sind generell Geldautomaten mit Wertschutzschränken ab Grad IV geeignet. Geldautomaten ohne Zertifizierung gemäß VdS 2450 sind ungeeignet.

Die Widerstandsfähigkeit von Wertbehältnissen gegenüber Sprengangriffen ist Gegenstand besonderer Prüfungen. Wurden diese Merkmale geprüft, werden nachstehende Kennzeichnungen zusätzlich zum Widerstandsgrad auf der Plakette ausgewiesen.

Kennzeichnung	Bedeutung
GAS	Zertifizierte Widerstandsfähigkeit gegen Sprengangriffe mit gasförmigen Explosivstoffen
EX	Zertifizierte Widerstandsfähigkeit gegen Sprengangriffe mit festen Explosivstoffen

Tabelle 7-1: Zusatzkennzeichen bei Wertbehältnissen mit Widerstand gegen Sprengangriffe

Da sich Sprengangriffe mit gasförmigen und festen Sprengstoffen stark unterscheiden, bieten nur Wertbehältnisse mit beiden Kennzeichen Schutz gegen entsprechende Angriffe. Wertbehältnisse, die Grad IV entsprechen und dieser Empfehlung folgen, sind dementsprechend mit „IV EX GAS EN 1143-1" gekennzeichnet (vgl. Bild 7-5, Widerstandsgrad bzw. Grade).

7.5.3 Verankerung

Die Wegnahme (Totalentwendung) des GA muss verhindert werden, indem GA (bzw. die darin befindlichen Wertbehältnisse) am Aufstellungsort entsprechend den Herstellervorschriften sach- und fachgerecht verankert werden (vgl. VdS 2472). Die Montage ist zu dokumentieren (vgl. VdS-Attest zur Bestätigung der Montage eines Wertbehältnisses/Sockels, VdS 3540, Anhang E).

7.5.4 Sockelmontage

Falls Geldautomaten auf einem Sockel montiert werden, muss für den Sockel eine mit dem eigentlichen Automaten harmonierende VdS-Anerkennung vorliegen. Die Montage des Automaten am Sockel sowie die Montage des Sockels am Aufstel-

Bild 7-5: Anerkennungsplakette für Wertbehältnisse für Geldautomaten in der klassischen sowie in der Darstellungsweise bei Zertifizierung im Rahmen der EFSG

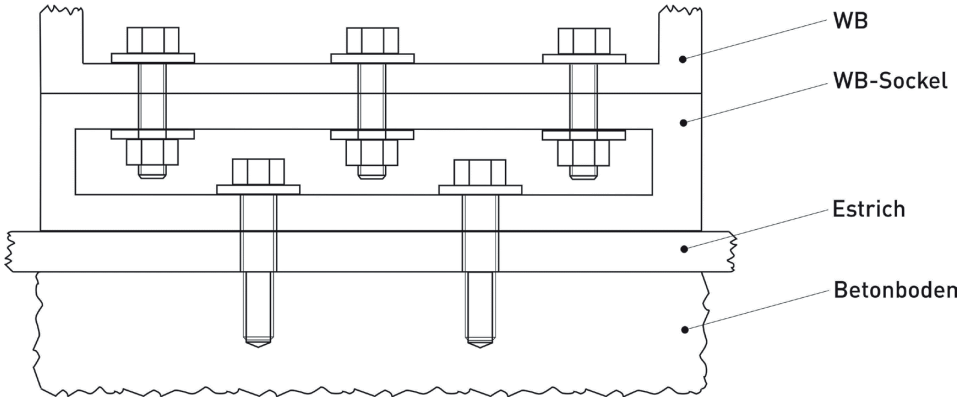

Bild 7-6: Prinzip der Verankerung von WB und Sockel

Bild 7-7: Anerkennungsplakette für Geldautomaten-WB und dazugehörigem Sockel

lungsort müssen sach- und fachgerecht nach den Vorgaben des Herstellers erfolgen. Der Sockel wird im Boden verankert und das Behältnis seinerseits wird mit dem Sockel verschraubt (vgl. Bild 7-6).

Damit sichergestellt ist, dass Sockel und Geldautomat für den gemeinsamen Einsatz anerkannt sind, muss der Eintrag in der Rubrik „Modell" auf der Plakette des GA sowie auf der Plakette des Sockels übereinstimmen (die Plaketten sind an der Innenseite der Wertbehältnistür bzw. am Sockel angebracht, Bild 7-7).

7.5.5 Fachunternehmen

Montage, Verankerung, Instandhaltung, Reparaturen oder Umbaumaßnahmen an Wertbehältnissen müssen sach- und fachgerecht ausgeführt werden, um die Schutzwirkung nicht zu beeinträchtigen und die Zertifizierung aufrecht zu erhalten. Diese Arbeiten sollten daher nur durch den Hersteller selbst oder VdS-anerkannte Service-Unternehmen für den Wartungs-, Reparatur- und Umrüstungsservice an Wertbehältnissen gemäß VdS 3529 durchgeführt werden.

7.6 Einbruchmeldetechnik

7.6.1 Überblick

Einbruchmeldetechnik dient dazu, den Einbruch oder Einbruchversuch eines Täters in einen Sicherungsbereich zu erkennen und zu melden (zu Planung und Einbau von Einbruchmeldeanlagen siehe VdS 2311). Als Sicherungsbereiche können bestimmte Gebäude, Gebäudeabschnitte, Räume oder Wertbehältnisse definiert werden.

Grundsätzlich können bei jeder Angriffsart eine frühzeitige Erkennung des Angriffs durch eine Einbruchmeldeanlage gewährleistet und Interventionsmaßnahmen ergriffen werden. Ziel ist es, den vom Täter verursachten Schaden zu minimieren und den Täter zu ergreifen. Für jedes Angriffsszenario ist deshalb eine Einbruchmeldeanlage mit nachgeschalteten Interventionsmaßnahmen zu empfehlen.

7.6.2 Einsatzempfehlungen

Generell sind GA mittels Einbruchmeldetechnik der Klasse C-SG 5 (vgl. VdS 2311) zu überwachen. Die Automaten bzw. deren Wertbehältnisse müs-

sen ggf. einen eigenständigen Sicherungsbereich bilden. Zusätzlich ist zu empfehlen, dass die Räume, in denen sich Wertbehältnisse befinden sowie Versorgungsräume von Geldautomaten, mit einer VdS-anerkannten Einbruchmeldeanlage überwacht werden.

Abhängig von der Aufstellungsvariante kann von einer Objektüberwachung des Geldautomaten abgesehen und eine fallenmäßige Überwachung des Raumes und der angrenzenden Bereiche nach VdS Klasse C-SG5 als ausreichend angesehen werden.

Mit der Planung und Ausgestaltung einer EMA ist ein qualifiziertes und zertifiziertes Fachunternehmen (VdS-anerkanntes Errichterunternehmen für Gefahrenmeldeanlagen, Fachrichtung Einbruchmeldeanlagen gemäß VdS 3403) zu beauftragen. Die EMA muss mit dem Attest VdS 2170 dokumentiert werden.

Es besteht die Möglichkeit, die EMA für dem Empfang und die Weiterleitung weiterer technischer Meldungen zu nutzen, wie sie bspw. in Abschnitt 7.8 beschrieben sind. Auch die Kombination von Einbruchmelde- und Videotechnik ist möglich.

7.7 Foyerüberwachung

Soll das Foyer auch außerhalb der Geschäftszeiten zugänglich sein, kann dieses nicht mit einer klassischen EMA überwacht werden, weil die ordnungsgemäße Scharf-/Unscharfschaltung unter Einhaltung der Zwangsläufigkeit nicht praktikabel ist.

Wenn in einem bestimmten Zeitfenster auch bei niedriger Nutzungsfrequenz das Betreten des Foyers dennoch zugelassen werden soll, bietet sich eine Perimeterdetektion an. Eine Lösung ist die Videoüberwachung des Foyers kombiniert mit einer Zutrittsüberwachung der Foyertür. Ein schlüssiges Konzept ist z. B., dass die Videoüberwachung des Foyers bei einem Zutritt (ausgelöst z. B. durch einen Bewegungsmelder im Raum oder durch einen Magnetkontakt an der Tür) aktiviert wird und die Meldungen und Bilder an eine NSL übertragen werden. Meldungen innerhalb eines definierten Zeitfensters (z. B. von 22:00 Uhr bis 06:00 Uhr; mit der NSL sind entsprechende Absprachen zu treffen) können dann durch einen qualifizierten Bediener überprüft werden. Anhand der Videobilder wird im Normalfall gut erkennbar sein, ob es sich um einen Kunden handelt oder ob ggf. ein Angriff auf den Geldautomaten durchgeführt oder vorbereitet wird.

Technische Auswertung und Übermittlung der Meldung können über die EMA erfolgen. Sofern es sich um eine Anschaltung an eine Meldegruppe Perimeterüberwachung handelt, bleibt die Attestierfähigkeit der VdS-EMA erhalten (weitere Voraussetzungen siehe VdS 2311).

Details zur Überwachung von Foyerzonen sind dem Sicherungsleitfaden Perimeter, VdS 3143, zu entnehmen.

7.8 Weitere Sensorik

Neben den in den Richtlinien VdS 2311 zur Planung und Einbau von Einbruchmeldeanlagen bezeichneten Möglichkeiten kann im oder am GA verbaute Sensorik zusätzliche Möglichkeiten zur Unterstützung frühzeitiger und differenzierter Detektion bieten.

Das kann beispielsweise sein:

- Gasdetektion im Wertbehältnis
- Öffnungsüberwachung des GA-Gehäuses zusätzlich zur Überwachung des Wertbehältnisses auf Öffnen und Durchbruch
- Überwachung des GA-Kartenslots auf Manipulation und Vorsatzgeräte
- Überwachung des GA-Kartenslots im Zusammenspiel mit der Videoüberwachung, ob innerhalb eines vorgegeben Zeitintervalls tatsächlich eine Karte eingeführt wurde
- Überwachung der Geldausgabeeinheit auf Manipulation
- Überwachung der GA Meldung (bzw. Fehlermeldungen) auf atypische Meldungen sowie typische angriffsrelevante Meldungen

Aus der Verknüpfung mehrerer relevanter Kriterien ergibt sich damit eine möglichst frühzeitige und dennoch zuverlässige Indikation für das Vorliegen eines Angriffs.

7.9 Vernebelungstechnik

Vernebelungssysteme können durch die Sichteinschränkung erhebliche Irritationen beim Täter auslösen und diesen damit veranlassen, von seinem Vorhaben abzusehen. Vorzugsweise kann ein Vernebelungssystem zum Einsatz kommen, wenn der Raum, in dem der GA zugänglich ist, verschlossen und mit einer Bewegungsdetektion und Kameraüberwachung ausgestattet ist. Das Kamerabild wird bei Bewegungsdetektion an eine NSL übertragen. Die NSL-Fachkraft entscheidet aufgrund der übertragenen Mediendaten, ob eine Auslösung des Vernebelungssystems erfolgt. Eine automatische Auslösung in öffentlich zugänglichen Berei-

chen wird nicht empfohlen. Die Polizei wird von der NSL über die Auslösung benachrichtigt.

Die Polizei ist über die Installation eines Vernebelungssystems zu informieren. Sofern das Nebelsystem im Überwachungsbereich einer Brandmeldeanlage installiert ist, muss dies mit dem Errichter der Brandmeldeanlage abgestimmt werden, um ungewollte Falschauslösungen weitestgehend zu vermeiden. Ebenso ist die Installation eines Vernebelungssystems der Feuerwehr anzuzeigen, damit diese in evtl. vorhandenen Einsatzplänen aufgenommen werden kann.

Eine Information von Hausbewohnern über die Installation eines Vernebelungssystems wird empfohlen. Grundsätzlich sollte bzw. darf der Einsatz von Nebelsystemen nicht in Räumen erfolgen, die von Hausmitbewohnern mitgenutzt werden, z. B. als Durchgang zur Straße oder als Fluchtweg.

7.10 Aufschaltung und Intervention

Um den Erfolg elektronischer Sicherungsmaßnahmen zu gewährleisten, muss eine qualifizierte Alarmintervention durch die Polizei oder eine VdS-anerkannte Notruf- und Serviceleitstelle mit Interventionsstelle (NSL mit IS; früher als Wach- und Sicherheitsunternehmen bezeichnet) sichergestellt sein. Interventionsmaßnahmen für unterschiedliche Alarmierungsfälle (Einbruch, Überfall, Vandalismus usw.) sind im Vorfeld mit der NSL abzustimmen. Hierzu ist immer das Alarmdienst- und Interventionsattest (VdS 2529) zu verwenden.

7.11 Videotechnik

7.11.1 Überblick

Videoüberwachungssysteme werden mit den unterschiedlichsten technischen Leistungsmerkmalen angeboten und sind heutzutage sehr vielseitig einsetzbar. Sie können verschiedene Aufgaben erfüllen, z. B.:

- Livebildübertragung und –betrachtung
- Aufzeichnung zum Zweck späterer Nachvollziehbarkeit (z. B. Beweissicherung)
- Erkennung von Angriffen, unerwünschten Zuständen oder Anomalien im Rahmen von Videoanalytik (z. B. Erkennung herumlungernder Personen, sog. Loitering-Detection oder Erkennung von anderem kundenuntypischen Verhalten)

Während demnach einerseits Videoanlagen nur als „verlängertes Auge“ zum Einsatz kommen sollen, werden andererseits Videoanlagen eingesetzt, die mittels mehrerer Kameras eine dreidimensionale Erkennung von Personen sowie Objekten durch Höhenmessung umsetzen.

Moderne Videosysteme ermöglichen es, unerwünschte Ereignisse zu erkennen, um unmittelbar und zielgerichtet reagieren zu können, z. B. durch direktes Ansprechen der Täter oder Übergabe der vorliegenden Informationen an die Interventionskräfte.

Realisiert wird dies z. B. durch:

- selektive Livebildübertragung
- Automatische Bildanalyse und Meldungserzeugung
- visuelle Alarmvorprüfung
- Referenzbildabgleich (z. B. SB-Zone und GA)

Daher ist es unerlässlich, für die Konzeption der VÜA eine genaue Ziel- und Aufgabendefinition vorzunehmen.

Weitere Informationen finden sich in den Richtlinien Planung und Einbau von Videoüberwachungsanlagen (VdS 2366) sowie Alarmverifikation (VdS 3415).

7.11.2 Einsatzempfehlungen

Planung und Einbau der Videoüberwachung hat gemäß VdS 2366 unter Berücksichtigung der gesetzlichen Vorschriften (z. B. Datenschutz) zu erfolgen.

In Abhängigkeit vom ermittelten Schutzziel müssen die Bildqualität, der Sabotageschutz und die Speicherdauer festgelegt werden.

Eine ereignisgesteuerte Übertragung der Bilddaten und Sabotagemeldungen an eine ständig besetzte Stelle kann für eine zeitnahe Intervention genutzt werden.

Wenn Videotechnik zum Einsatz kommt, sollten die Tatabläufe bzw. Phasen eines GA-Angriffes erfasst und aufgezeichnet werden. Für eine geeignete Beleuchtung (siehe auch nachfolgender Abschnitt) ist zu sorgen.

Videobasierte Detektion kann eingesetzt werden, um den Einbau illegaler Bauteile, wie z. B. Überbautastaturen, Cash Traps oder Skimmern an den Bedienflächen des GA, zu erkennen.

Mit der Planung und Ausgestaltung einer VÜA ist ein qualifiziertes und zertifiziertes Fachunternehmen (VdS-anerkanntes Errichterunternehmen für Ge-

fahrenmeldeanlagen, Fachrichtung Videoüberwachungsanlagen gemäß VdS 3403) zu beauftragen.

7.12 Beleuchtung

Eine vollständige, dauerhafte und ausreichende Ausleuchtung der Bereiche mindert den Tatanreiz. Zudem begünstigt eine positive Beleuchtungssituation das persönliche Sicherheitsgefühl des Bankkunden bzw. Nutzers. Es ist sinnvoll, auch den Außenbereich des Foyers hinreichend auszuleuchten, um Kunden so die Möglichkeit zu geben, die Umgebung vor dem Verlassen des Foyers einzusehen und zu überblicken.

Alle Bereiche, die von Kunden oder anderen Personen genutzt werden, sind daher ausreichend zu beleuchten. Es wird empfohlen, den diesbezüglichen Regelungen für Arbeitsstätten zu folgen.

7.13 Auswahlempfehlungen

Generell wird empfohlen, VdS-anerkannte Systeme und Produkte einzusetzen, da die technischen Eigenschaften sowie die allgemeine Produktqualität im Rahmen einer unabhängigen Prüfung bestätigt wurden.

Bei anderen oder nicht anerkannten Produkten ist eine Beurteilung von Produktqualität und Produkteignung ggf. nur basierend auf Aussagen des Anbieters möglich und kann sich dadurch problematisch gestalten.

Anhang A Begriffe

Fahrbare Geschäftsstelle: in einem Fahrzeug untergebrachte Geschäftsstelle, um Kundengeschäfte ohne örtliche Bindung an das Geldinstitut anzubieten

Hinweis: Fahrbare Geschäftsstellen können z. B. im Rahmen von temporären Veranstaltungen für den Zeitraum der Veranstaltung eingesetzt werden.

Geldautomat (GA): Vorrichtung zur automatisierten Ausgabe und Annahme von Geld mit einer gesicherten Aufbewahrungseinheit (Wertbehältnis).

Gefährdung: Wahrscheinlichkeit, dass eine zunächst abstrakte Bedrohung unter Ausnutzung von Schwachstellen eine konkreten Schaden verursacht (sich ein Risiko realisiert)

Risiko: Möglichkeit, dass ein erwünschtes Ereignis nicht eintritt oder ein unerwünschtes Ereignis eintritt; abstrakte Risiken können mit der konkreten Gefährdung quantifiziert werden

Sicherungsbereich: spezieller, geschlossener Raum, der so gestaltet ist, dass ein ausreichender Schutz gegen gewaltsames Eindringen sowie gegen den Einblick von außen gegeben ist

Sicherungsbereich (in Zusammenhang mit Einbruchmeldetechnik): das von einer Einbruchmeldeanlage (EMA) überwachte Areal (i. d. R. einschließlich der Umgrenzung bzw. der Außenhaut)

Systembedingte Öffnung: funktionsbedingt erforderliche Öffnung eines Produktes, welches generell darauf ausgerichtet ist, in geschlossenem Zustand keine Durchlässe bzw. Durchgriffmöglichkeiten aufzuweisen, um die darin befindlichen Dinge vor unbefugtem Zugriff zu schützen

Hinweis: In einem Wertbehältnis für Geldautomaten befinden sich z. B. systembedingte Öffnungen für Kabeldurchlässe, die zur Anschaltung einer im Inneren des WB befindlichen elektronischen Überwachung dienen sowie Öffnungen zum Transport von Bargeld aus dem WB heraus oder in das WB hinein.

Anhang B Abkürzungen

DGUV: Deutsche Gesetzliche Unfallversicherung e. V.

EMA: Einbruchmeldeanlage

EMV: Europay International, MasterCard und VISA; Spezifikation für Zahlungskarten

EFSG: European Fire and Security Group

GA: Geldautomat

NSL: Notruf- und Serviceleitstelle

VdS: VdS Schadenverhütung GmbH

VÜA: Videoüberwachungsanlage

WB: Wertbehältnis

Anhang C Normative Verweisungen

Diese Richtlinien enthalten datierte und undatierte Verweise auf andere Regelwerke. Die Verweise erfolgen in den entsprechenden Abschnitten, die Titel werden im Folgenden aufgeführt. Änderungen oder Ergänzungen datierter Regelwerke gelten nur, wenn sie durch Änderung dieser Richtlinien bekannt gegeben werden. Von undatierten Regelwerken gilt die jeweils letzte Fassung.

DIN EN 1143-1 Wertbehältnisse, Anforderungen; Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Einbruchdiebstahl, Teil 1: Wertschutzschränke, Wertschutzschränke für Geldautomaten, Wertschutzraumtüren und Wertschutzräume

EN 1300 Wertbehältnisse – Klassifizierung von Hochsicherheitsschlössern nach ihrem Widerstandswert gegen unbefugtes Öffnen

VdS 2170 VdS-Attest bzw. Anlagenbeschreibung zur Dokumentation von Überfall- und/oder Einbruchmeldeanlagen

VdS 2333 Sicherungsrichtlinien für Geschäfte und Betriebe
Hinweis: Verweisungen im Text beziehen sich auf die Ausgabe VdS 2333 : 2014-09 (04)

VdS 2366 VdS-Richtlinien für Videoüberwachungsanlagen; Planung und Einbau

VdS 2450 VdS-Richtlinien für mechanische Sicherungseinrichtungen; Wertschutzschränke, Wertschutzschränke für Geldautomaten, Wertschutzraumwandungen und Wertschutzraumtüren; Anforderungen, Klassifizierung und Prüfmethoden

VdS 2472 Sicherungsrichtlinien Bargeld
Hinweis: Verweisungen im Text beziehen sich auf die Ausgabe VdS 2472 : 2020-01

VdS 2529 Alarmdienst- und Interventionsattest

VdS 3134 Technische Kommentare

VdS 3143 Sicherungsleitfaden Perimeter

VdS 3403 VdS-Richtlinien für die Anerkennung von Errichterunternehmen für Gefahrenmeldeanlagen (GMA)

VdS 3406-1 VdS-Richtlinien für das Sicherheitsmanagement; Bauliche Objekte, Teil 1, Verfahren

VdS 3415 VdS-Richtlinien für Sicherheitsdienstleistungen, Alarmverifikation

VdS 3529 Anerkennung von Service-Unternehmen für den Wartungs-, Reparatur- und Umrüstungsservice an Wertbehältnissen

VdS 3540 Bestätigung der Montage eines Wertbehältnisses/Sockels (Montageattest)

VdS 5473 VdS-Broschüre Videoüberwachung

Anhang D Bezugsquellen und Institutionen

VdS-Richtlinien
VdS Schadenverhütung GmbH
Verlag
Amsterdamer Straße 174
50735 Köln
www.vds-shop.de

Publikationen des Gesamtverbandes der Deutschen Versicherungswirtschaft e. V. im Bereich Schadenverhütung und Technik
VdS Schadenverhütung GmbH
Verlag
Amsterdamer Straße 174
50735 Köln
www.vds-shop.de

Publikationen der Unfallversicherungsträger Deutsche Gesetzliche Unfallversicherung (DGUV), die zuständigen Unfallversicherungsträger
Deutsche Gesetzliche Unfallversicherung e. V. (DGUV)
Glinkastraße 40
10117 Berlin
Tel.: +49 30 13001-0 (Zentrale)
Fax: +49 30 13001-9876
E-Mail: info@dguv.de
www.dguv.de

European Fire and Security Group, EFSG Anerkennungslisten und Informationen EFSG Sekretariat
EFSG Secretariat
c/o CNPP Cert.
Ms Sylvie Jalin
Route de la Chapelle Réanville
F-27950 Saint-Marcel
Phone: +33 (0)2 76 76 70 00
www.efsg.org

Anhang E Atteste

Zur Dokumentation umgesetzter bzw. vereinbarter Sicherungsmaßnahmen stehen standardisierte und teilweise bundesweit einheitliche Formulare zur Verfügung, auf die an den jeweiligen Stellen im Text verwiesen wurde. Aus Gründen der Übersichtlichkeit sind diese nachstehend nochmals zusammenfassend dargestellt.

Muster und weitere Informationen wie Ausfüllhinweise sind den Technischen Kommentaren, VdS 3134 zu entnehmen.

Druckstück-Nr.	Verwendung
VdS 2170	Einbruch-/Überfallmeldeanlagen
VdS 3426	Videoüberwachungsanlagen
VdS 2529	Alarmdienst und Intervention
VdS 3540	Verankerung von Wertbehältnissen
VdS 3863	Dienstleistungen an Wertbehältnissen

Tabelle E-1: Übersicht der Atteste

Anhang F Bundesweit einheitliches Raster für eine Risikoanalyse zur Sprengung von Geldautomaten (GA-S)

Erläuterungen zur Anwendung des bundesweit einheitlichen Rasters für eine Risikoanalyse zur Sprengung von Geldautomaten (GA-S)

1. Das vorliegende Dokument wurde auf Basis der von der Ständigen Konferenz der Innenminister und -senatoren der Länder (IMK) am 02.10.2019 beschlossenen „Maßnahmen zur Sicherung von Geldautomaten“ (Stand: 11.03.2019) sowie nach Institutsvorlagen unter Einbindung der Versicherungswirtschaft und der Projektgruppe „Geldautomatensprengungen“ (BLPG GA-S) der Kommission Polizeiliche Kriminalprävention der Länder und des Bundes zum Schutz vor GA-Sprengungen entwickelt.

2. Das bundesweit einheitliche Raster für eine Risikoanalyse wurde in neun Kategorien von Sicherungsparametern gegliedert. Eine darauf aufsetzende institutsindividuelle Gesamtbewertung erfolgt unter Würdigung aller umgesetzten Maßnahmen.

3. Die aufgeführten Maßnahmen umfassen die wesentlichen, heute möglichen und von der Polizei als wirksam eingeschätzten Maßnahmen im Sinne der Sprengprävention. Dabei ist zu berücksichtigen, dass nicht alle Maßnahmen eine gleichgerichtete und gleichwertige Schutzwirkung zur Erreichung der Schutzziele (siehe Blatt Schutzziele) haben.

4. Das Ergebnis kann eine Indikation dafür sein, ob der bestehende Maßnahmen-Mix einen ausreichenden Schutz für den GA-Standort darstellt oder ob weiterer Handlungsbedarf besteht. Die Entscheidungshoheit für eine Umsetzung obliegt dem GA-Betreiber.

Schutzziele:

Primärziele:

Verhinderung von Geldautomatensprengungen
Verhinderung von Personenschäden durch Geldautomatensprengungen
Verhinderung von Sachschäden durch Geldautomatensprengungen
Verhinderung der Beuteerlangung

Sekundärziel:

Erschwerung und Verhinderung der Beuteverwertung

Bundesweit einheitliches Rasters für eine Risikoanalyse zur Sprengung von Geldautomaten (GA-S)

Vers-1.0 vom 24.11.2020

Legende:
0 = Entspricht nicht der derzeitigen Empfehlungspraxis der Polizei
1 = Entspricht der derzeitigen Empfehlungspraxis der Polizei

Ausfüllanleitung:
- Alle Kategorien sind auszufüllen
- Die mit (* gekennzeichneten Fußnoten mit technischen Erläuterungen sind zu beachten!

1. Aufstellort des Geldautomaten (GA)(*1

Institutsbezeichnung: (z. B. BIC) Standortbezeichnung: (z.B. Filialnummer) Id.-Nr. des GA: (z.B. TID)

PLZ/Ort: Straße: Hausnummer:

[1] Geschäftsgebäude(*2 [0] kombiniertes Wohn-Geschäftsgebäude [0] Container/SB-Pavillon

[1] 24 h gesicherter Aufstellort(*3 [0] Drittstandort (z.B. Baumarkt/Einkaufszentrum) [0] Sonstige:(*4

[1] im Gebäude [0] außerhalb(*5 [1] Wandeinbau [0] freistehend [0] EG(*6 [1] OG/UG(*7

2. Nachtverschluss

Nachtverschluss des Foyers(*2: [0] nein [1] ja(*1 Zeit: _____ Uhr - _____ Uhr

3. Ausführung des GA

[0] Frontloader

[1] Rearloader:
- Serviceraum hinter GA [1] Ja [0] Nein
- Serviceraum(*1 gesichert [1] Ja [0] Nein
- EMA im Serviceraum vorhanden [1] Ja [0] Nein

4. Widerstandsklasse (WK) des GA

[0] UL / CEN L bis CEN IV [1] Gas/Ex zertifiziert in der WK CEN IV / CEN III (*1

5. Mechanische Sicherungstechnik am GA(*1

Zusätzliche Kopfsicherung(*2 [1] Ja [0] Nein

Zusätzlicher Shutterverschluss(*3 [1] Ja [0] Nein

Abdeckung technischer Wertbehältnisöffnungen(*4 [1] Ja [0] Nein

6. Alarmsicherung / Einbruchmeldeüberwachung(*1

am Geldautomatengehäuse [0] Nein [1] Ja z.B. Haubenöffnungskontakt (*2

im SB-Bereich [0] Nein [1] Ja z.B. Bewegungsmelder(*3

Tür/Fenster zum SB Bereich [0] Nein [1] Ja z.B. Magnetkontakt(*4

7. Alarmaufschaltung(*1

[1] Notruf-Serviceleitstelle (NSL)/Alarmzentrale [1] Polizei [1] Sonst. Zentralen [0] Nicht 24/7 [0] Keine

8. Interventionssysteme(*1

8.1 Ein Videosystem(*2 im SB-Bereich / Foyer vorhanden. [1] Ja [0] Nein

Aufzeichnung erfolgt: [1] Ja [0] Nein

Übertragung im Alarmfall erfolgt an:(*3 [1] Polizei/NSL/Alarmzentrale [0] Sonst. Zentralen [0] Nicht 24/7 [0] Keine

8.2 Nebelsystem

Nebelsystem im SB-Bereich vorhanden: [1] Ja [0] Nein

- Nebelsystem verdeckt eingebaut (*4 [1] Ja [0] Nein
- mehrere Auslass-/Blinddüsen vorhanden (*5 [1] Ja [0] Nein

Nebelsystem im Serviceraum vorhanden: [1] Ja [0] Nein

Aktivierung durch: Technik (automatisiert) [1] Ja [0] Nein

Alarmzentrale/NSL [1] Ja [0] Nein

8.3 Optisch/Akustisches System(*6 vorhanden: [1] Ja [0] Nein

9. Mittelbar wirkende Sicherungstechnik(*1

Gasverdrängung (Neutralisation)(*2 [1] Ja [0] Nein Piezozündung(*3 [1] Ja [0] Nein

Einfärbesystem in der Geldkassette(*4 [1] Ja [0] Nein Klebetechnik (*5 [1] Ja [0] Nein

Sprengmatten(*6 [1] Ja [0] Nein Ortungssysteme(*7 [1] Ja [0] Nein

Bundesweit einheitliches Rasters für eine Risikoanalyse zur Sprengung von Geldautomaten (GA-S)

Fußnoten mit technischen Erläuterungen zu den Kategorien 1 bis 9

1. Aufstellort des Geldautomaten (GA)

(*1 Mehrfachnennungen sind möglich und erforderlich.

(*2 Keine Personen befinden sich Nachts regulär im Gebäude (Bereich des GA ausgenommen)
Typisch: SB Zone des Geldinstituts und Rotunden mit sprengfester Umhausung
Hintergrund: Keine Personengefährdung im Gebäude bei nächtlicher Sprengung

(*3 GA-Standort im Sicherheitsbereich (z.B. Flughafenterminal, Werksgelände, Krankenhaus mit besetztem Empfang)

(*4 z.B. Rotunde ohne sprengfeste Umhausung oder GA-Standorte im ÖPNV (U- und S-Bahnhöfe)

(*5 Tastatur des GA befindet sich direkt im öffentlichen Bereich (= "Bürgersteig" oder gleichwertig)

(*6 Sofern der Standort des GA durch entsprechende Sicherungsmaßnahmen (bspw. Verpollerung) nicht mit einem PKW erreichbar und dadurch "Rammen" ausgeschlossen ist, sind auch EG Standorte geeignet.

(*7 Standort des GA nicht mit einem PKW erreichbar (Eindringen durch "Rammen" ist ausgeschlossen)

2. Nachtverschluss

(*1 Nachtverschluss sollte den möglichen Tatzeitraum abdecken.
Empfehlung Polizei: 22.00 Uhr bis 06.00 Uhr.
Hintergrundinformation: Aktuelle Tatzeiten (Ende Q2 2020): 24.00 Uhr bis 06.00 Uhr
Für Geldautomaten, die vollständig in einer Filiale stehen (Bedienung nur während der Filialzeiten möglich) gelten die Schliesszeiten der Filiale als Nachtverschlusszeiten.

(*2 Gleichlautende Empfehlungen gelten auch für Drittstandorte (z.B. Tankstelle, Bürogebäude, Baumärkte)

3. Ausführung des GA

(*1 Empfehlung Polizei: Serviceraum gesichert in durchbruchhemmender Ausführung.
Die Filiale eines Geldinstitutes kann ebenfalls als Serviceraum zur Sprengpärvention angesehen werden, wenn sie in durchbruchhemmender Ausführung gesichert ist und der GA als Wandeinbau ausgeführt ist.

4. Widerstandsklasse (WK) des GA

(*1 Empfehlung Polizei: Bei Neuanschaffungen sollten Wertschutzschränke für GA die Anforderung gegen Gas- und Explosionssprengungen (Gas/Ex) erfüllen und mindestens der Widerstandsklasse CEN IV oder höher entsprechen.

5. Mechanische Sicherungstechnik am GA

(*1 Mehrfachnennungen sind möglich.

(*2 Zusätzliche Sicherungmaßnahme, die ein gewaltsames Öffnen/Abheben der GA-Haube oder des GA-Kopfs verhindert.
Hintergrund: Wertbehältnisöffnungen zur Einleitung (Shutter, techn. Öffnungen) sind nach Öffnung i.d.R. frei zugänglich.

(*3 Zusätzlicher Shutterverschluss bedeutet, dass die Öffnung, durch die das Geld unmittelbar aus dem Wertbehältnis heraustransportiert wird (Cash-Gate), durch eine Metallplatte separat mechanisch verschlossen ist.
Der "Shutter" des Geldausgabeschachts im GA-Kopf/ in der GA-Haube, den der Kunde bei der Geldausgabe nutzt, bietet hingegen nur eine geringe zusätzliche Schutzwirkung.

(*4 Technische Wertbehältnisöffnungen sind alle sonstigen GA-Öffnungen, die unmittelbar in das Wertbehältnis führen.
Soweit diese nach Öffnen oder Zerstören der GA-Haube bzw. des GA Rahmens zugänglich sind, bieten sie den Tätern die Möglichkeit zur Einleitung von Gas oder Einführung von Sprengstoff.
Beispiele: Kabeldurchführungen, Lüftungen etc.

Bundesweit einheitliches Rasters für eine Risikoanalyse zur Sprengung von Geldautomaten (GA-S)

Fußnoten mit technischen Erläuterungen zu den Kategorien 1 bis 9

6. Alarmsicherung / Einbruchmeldeüberwachung

Für alle Alamsicherungen gilt, dass unmittelbar eine Alarmierung/Information an eine ständig besetzte Stelle erfolgt, die somit unmittelbar reagieren kann (Einleitung der Intervention).

(*1 Mehrfachnennungen sind möglich.

(*2 Öffnungskontakt oder gleichwertig, durch den die Öffnung des GA-Kopfs/ der GA-Haube detektiert wird.

(*3 Bewegungsmelder oder gleichwertig, die eine Bewegung von Personen in der SB-Zone detektieren.

(*4 Sensoren, die ein Öffnen von Türen und/oder Fenstern detektieren.

7. Alarmaufschaltung

(*1 NSL (gem. VdS) und Alarmzentrale (gem. EN) werden als gleichwertig betrachtet. Soweit in einigen Bundesländern ein Konzessionär-Betrieb anstelle einer Polizeiaufschaltung erfolgt, sind diese wie eine NSL oder Alarmzentrale zu werten.
Als "Sonstige Zentralen" gelten Stellen, die außerhalb der Öffnungszeiten besetzt sind.
Aufschaltungen, bei denen eine ständige Besetzung über den gesamten Tatzeitraum nicht garantiert ist und/oder die nicht unmittelbar auf einen Alarm reagieren können (Intervention einleiten), gelten hier als "keine Aufschaltung".

8. Interventionssysteme

(*1 Mehrfachnennungen sind möglich.

(*2 Aufgrund der abgestuften Wirksamkeit wird zwischen einem Videosystem mit Aufzeichnung und einem Videosystem mit zusätzlicher Bildübertragung im Alarmfall unterschieden.

(*3 Begrifflichkeiten siehe 7. Alarmaufschaltung.

(*4 Systeme, die eine Manipulation der Austrittsdüse mit hoher Wahrscheinlichkeit detektieren oder verhindern, sind als gleichwertig zu einer verdeckten Installation zu bewerten.

(*5 Maßnahmen, die den Täter nicht erkennen lassen, aus welchen Düsen/Ausgängen Nebel entweichen wird, so dass eine Tatvorbereitung (Auslassmanipulation) erschwert oder unmöglich wird.

(*6 z.B. lauter Alarmton, Ansprache der Täter, Außensirene, grelle Lichter (Stroposkopblitz)
Das Anschalten der SB-Beleuchtung wird nicht als Alarmintervention angesehen (wird vom Täter nicht als Intervention wahrgenommen).

9. Mittelbar wirkende Sicherungstechnik

(*1 Mehrfachnennungen sind möglich.

(*2 Gasneutralisation kann bei Gasangriffen wirken und nicht bei Festsprengstoff.

(*3 Piezozündung kann bei Gasangriffen wirken und nicht bei Festsprengstoff.

(*4 Einfärbesysteme sind in vielfältigen Produktvarianten verfügbar.

(*5 Verklebesysteme können zukünftig eine Alternative zu Einfärbesystemen sein.

(*6 Sprengmatten/energieabsorbierende Matten reduzieren die Sprengwirkung (passiv).

(*7 Ortungssysteme (in einer Geldkassette) können eine Beutelokalisierung ermöglichen. Eine Abstimmung mit der Polizei wird empfohlen.

Anhang G Änderungen zur Vorversion

- Umstrukturierung der Inhalte (vgl. Inhaltsverzeichnis)
- redaktionelle Änderungen bei verbliebenen bzw. angepassten Textpassagen
- Erläuterung zur einheitlichen Verweisung auf VdS-Klassen und -Grade (vgl. 1.1)
- Erläuterung zur korrespondierenden Normen (vgl. 1.1)
- Klärung, dass die vorliegenden Richtlinien auf dem aktuellen Stand der Technik fußen (vgl. 1.1)
- Überarbeitung der Risikobetrachtung (vgl. 2ff)
- Überarbeitung der Angriffsarten (vgl. 3ff)
- Aktualisierung des Themas Sprengung (vgl. 3.3)
- Bearbeitung der Gefährdungsanalysen auf die konkreten Risiken bezogen (vgl. z. B. 3.3.2)
- Ergänzung der Ausführungen zu Festsprengstoff (vgl. 3.3.4)
- Formulierung von Angaben zur Wirkung der (unterschiedlichen) Schutzmaßnahmen (vgl. 6ff)
- Überarbeitete Erläuterung zur Umsetzung von Schutzmaßnahmen (vgl. 7ff)
- Vorstellung der neu erstellten Anerkennungsplakette für WB im Rahmen einer Anerkennung durch EFSG (vgl. 7.5.2)

Raum für Ihre Notizen

Raum für Ihre Notizen

Herausgeber: Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GDV)

Verlag: VdS Schadenverhütung GmbH • Amsterdamer Str. 174 • D-50735 Köln
Telefon: (0221) 77 66 - 0 • Fax: (0221) 77 66 - 341