Geldautomatenkriminalität

August | 09

Überblick über die Situation in Europa und die wichtigsten Regeln, um Straftaten zu verhindern

enisa
European Network and Information Security Agency

Die ENISA

Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) ist eine Einrichtung der Europäischen Union, die mit dem Ziel errichtet wurde, die Funktionsfähigkeit des Binnenmarktes zu fördern. Als Kompetenzzentrum berät die ENISA die Mitgliedstaaten und die Organe der Europäischen Union über Netz- und Informationssicherheit, spricht Empfehlungen aus und dient als zentrale Anlaufstelle für Informationen über bewährte Praktiken. Darüber hinaus fördert diese Einrichtung die Kontakte zwischen den europäischen Institutionen, den Mitgliedstaaten und den Akteuren aus Wirtschaft und Industrie.

Kontakt:

Allgemeine Anfragen zu Sensibilisierungsmaßnahmen zur Informationssicherheit richten Sie bitte an:

E-Mail: Isabella Santa, Leitende Sachverständige für Sensibilisierungsfragen — awareness@enisa.europa.eu

Internet: http://www.enisa.europa.eu/

Geldautomatenkriminalität:
Überblick über die Situation in Europa und die wichtigsten Regeln, um Straftaten zu verhindern

August 2009

Danksagung

An der Erstellung dieser Veröffentlichung haben verschiedene Beteiligte direkt oder indirekt mitgewirkt. Der Veröffentlichung liegen unter anderem Beiträge von Mitgliedern der ENISA-Plattform für die Zusammenarbeit bei der Sensibilisierung (AR Community) zugrunde.

Die ENISA dankt den Mitgliedern der ENISA-Plattform für die Zusammenarbeit bei der Sensibilisierung und ihren Einrichtungen, ADICAE, Arjen de Landgraaf von E-Secure-IT, Daniel Blander von InfoSecurityLab Inc., David Barroso von S21sec, Fabio Guasconi von @ Mediaservice.net S.r.l., Fabrizio Cirilli, Gerasimos Ntouskas von KPMG Limited, INTECO, Joao Brites Moita, Lachlan Gunn von European ATM Security Team Ltd, Neal Ysart von PwC, Sissel Thomassen von InfoSecure, William Beer von PwC, Yves Le Roux von CA für ihre großzügige Unterstützung, ihre wertvollen Beiträge und die Materialien, die sie für diese Veröffentlichung zur Verfügung gestellt haben.

Schließlich bedanken wir uns bei den Personen, die sich an dieser Veröffentlichung mit ihren Korrekturen, hilfreichen Hinweisen, Kommentaren und Anregungen beteiligt haben. Ganz besonders bedanken wir uns bei den Mitgliedern des European ATM Security Team. Auch wenn diese Liste sicherlich nicht vollständig ist, wäre diese Veröffentlichung ohne ihre Unterstützung unvollständig und nicht korrekt.

Inhalt

Zusammenfassung

Die Zahl der Geldautomaten nimmt in Europa jedes Jahr zu. Geldautomaten finden sich zunehmend auch an anderen Orten als Banken wie Supermärkten, Flughäfen, Tankstellen, Bahnhöfen, Kaufhäusern usw. Mit der Zunahme der Geldautomaten in Europa steigt auch der Umfang der gemeldeten Geldautomatenkriminalität, die im Jahr 2008 zu Verlusten in Höhe von 485,15 Mio. EUR führte. Für zahlreiche dieser Angriffe ist die organisierte Kriminalität verantwortlich und die Rezession wird als mögliche Ursache für diesen Anstieg vermutet. Die Geldautomatenindustrie räumt der Sicherheit der Benutzer und der Bekämpfung von Betrug eine hohe Priorität ein, um das Vertrauen der Benutzer in das System zu bewahren.

Durch eine Reihe von Empfehlungen soll dieses Weißbuch die Benutzer für die unterschiedlichen Gefahren bei der Benutzung von Geldautomaten sensibilisieren. Zudem bietet es Tipps für deren Erkennung und Bekämpfung. Die ENISA ist der Ansicht, dass ein zunehmendes Risikobewusstsein der Benutzer den ersten Schritt zur Bekämpfung der Geldautomatenkriminalität darstellt und zu einem signifikanten Rückgang der Angriffe und Betrugsversuche auf Geldautomaten führen kann. Die Bürger müssen aufgeklärt werden, wie sie zur Verringerung dieser Gefahren beitragen können, indem sie die nötigen Vorsichtsmaßnahmen bei der Nutzung von Bankautomaten treffen, wie die Abdeckung ihrer PIN-Nummer bei der Eingabe oder die Wachsamkeit für eventuell manipulierte Geldautomaten oder ungewöhnliche Aktivitäten.

Geldautomatenkriminalität verändert sich ständig, daher müssen auch die entsprechenden Gegenmaßnahmen beständig angepasst werden. In dieser Veröffentlichung können weder alle mit der Benutzung von Geldautomaten verbundenen Risiken behandelt werden noch können sämtliche Tipps für einen sicheren Umgang dargestellt werden. Diese Veröffentlichung ist vielmehr als hilfreicher und notwendiger Anfang zu verstehen, das Bewusstsein der Benutzer für die Problematik bei der Nutzung von Geldautomaten in der Europäischen Union und weltweit zu erhöhen sowie auf die Thematik der Datensicherheit und die bewährten Verfahren der Branche hinzuweisen. Die ENISA setzt sich dafür ein, die Benutzer von Geldautomaten auf die möglichen Schwächen hinzuweisen, und stellt sicher, dass auf nationaler Ebene in den Mitgliedstaaten der EU weiterführende Informationen und Hinweise von Seiten der Banken, Finanzinstitutionen, Zahlungssysteme und Exekutivorgane verbreitet werden.

Diese Veröffentlichung befasst sich nicht mit den rechtlichen Voraussetzungen für die Aufstellung, den Betrieb und die Wartung von Geldautomaten oder der Verarbeitung von Transaktionen und Ausgabe von Banknoten.

In dieser Veröffentlichung werden schließlich auch keine Empfehlungen für die Eignung, Verfügbarkeit und Effektivität einzelner Systeme oder Geräte für den Einsatz zur Vermeidung oder Verhinderung von Angriffen auf Geldautomaten ausgesprochen.

TEIL 1:

GELDAUTOMATEN UND ENTSPRECHENDE SICHERHEITSMAßNAHMEN

Geldautomaten

Eine Definition

Ein Geldautomat (auch Bankautomat), ist ein EDV-gestütztes Gerät, das dem Kunden eines Kreditinstitutes ermöglicht, Transaktionen ohne Hilfe eines Bankmitarbeiters oder Kassenmitarbeiters auszuführen.

Die meisten modernen Bankautomaten identifizieren den Bankkunden durch die Plastikkarte, die der Kunde in den Bankautomaten einführt. Die Plastikkarte kann mit einem Magnetstreifen oder einem integrierten Schaltkreis ausgestattet sein, der die Kartennummer und einige Sicherheitsinformationen wie Ablaufdatum und Kartenprüfnummer (CVC) umfasst. Die Prüfung des Benutzers erfolgt durch die Eingabe einer persönlichen Geheimzahl (PIN).

Über einen Geldautomaten können Kunden Barabhebungen von ihrem Bankkonto (oder Barabhebungen mit einer Kreditkarte) vornehmen, ihren Kontostand zu prüfen, die Prepaid-Karte ihres Mobiltelefons aufzuladen, Rechnungen begleichen usw.

Die Nutzung von Geldautomaten: ein Überblick über die Situation in Europa

Nach einer Schätzung des European ATM Security Team (EAST) gab es 2008 in Europa 383 951 Geldautomaten und mehr als 1,5 Mio. Geldautomaten weltweit([1]). 72 % aller Geldautomaten in Europa befinden sich in fünf Staaten: Vereinigtes Königreich, Spanien, Deutschland, Frankreich und Italien. Gegenüber dem Vorjahr ist die Gesamtzahl der Geldautomaten in Europa um 6 % gestiegen.

([1]) *https://www.european-atm-security.eu/Welcome%20to%20EAST/*
Nach einer im Mai/Juni 2009 durchgeführten Erhebung von EAST zur Nutzung von Geldautomaten verfügten 49 % der Befragten über Grundkenntnisse zu den möglichen Risiken und Gefahren, benötigten aber weiterführende Informationen und 14 % der Befragten waren sich über Risiken und Gefahren unsicher und würden Leitlinien zu deren Erkennung begrüßen.

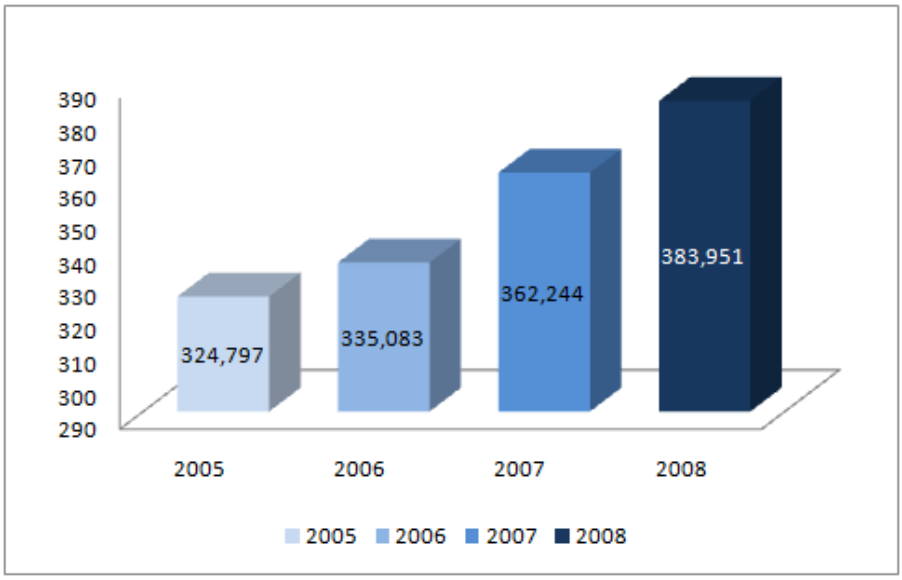
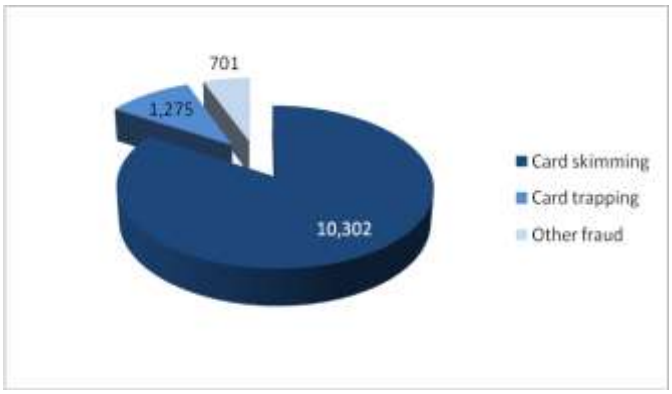


Abbildung 1: Zahl der Geldautomaten in Europa Quelle: EAST & EPC

Geldautomatenkriminalität und ihre finanziellen Auswirkungen in Europa

Mit dem Anstieg der Zahl der Geldautomaten ist auch eine drastische Zunahme der Geldautomatenkriminalität zu verzeichnen. Nach einem aktuellen Bericht der EAST stieg die betrügerische Geldautomatenkriminalität in Europa im Jahr 2008 um 149 % gegenüber dem Vorjahr an. Dem Bericht zufolge ist dieser Anstieg vor allem auf die dramatische Zunahme von sogenannten Skimming-Vorfällen zurückzuführen. Im Jahr 2008 waren insgesamt 10 302 nachgewiesene Skimming-Vorfälle in Europa zu verzeichnen. Noch bedenklicher sind hingegen jüngste Berichte über Angriffe, bei denen die Netzwerke der Geldautomaten und die Geldautomaten selbst mit einfach verfügbarer moderner Malware([2]) infiziert wurden.



Nach diesem Bericht sind die körperlichen Übergriffe auf die Benutzer von Geldautomaten in Europa hauptsächlich aufgrund eines Rückgangs der angezeigten Raubüberfälle um 29 % gesunken. Die Zahl der tätlichen Angriffe auf Geldautomaten selbst hat jedoch um 32 % zugenommen. Obwohl die finanziellen Verluste durch diese Angriffe geringer sind als bei anderen kriminellen Handlungen an Geldautomaten, stellen derartige Angriffe nach wie vor ein ernst zu nehmendes Problem für die Branche dar.

Abbildung 2: Betrügerische Geldautomatenkriminalität nach Zahl der Vorfälle 2008 (Gesamtjahr)
Quelle: EAST & EPC

([2]) Malware ist Software, deren Zweck in der Infizierung oder Schädigung eines Computersystems ohne Wissen des Eigentümers besteht.

Trotz des drastischen Anstiegs der Vorfälle nahmen die tatsächlichen Verluste aufgrund von Betrug im Vergleich zum Vorjahr nur um 11 % zu. Die Verluste aufgrund von Betrugsfällen waren nach wie vor erheblich, und trotz aller in den europäischen Staaten eingeleiteten Gegenmaßnahmen belief sich der Gesamtverlust auf knapp 500 Mio. EUR. In Abbildung 3 wird dieser Verlust ausführlicher dargestellt.

Knapp 400 Mio. EUR dieses Verlustes entstanden im Ausland aufgrund von Betrug außerhalb der Landesgrenzen durch Kriminelle, die Kartendaten gestohlen hatten. Aufgrund der Einführung der EMV([3])-Technik in Europa treten diese Verluste meist außerhalb Europas auf.

Abbildung 3: Betrügerische Geldautomatenkriminalität nach gemeldetem Gesamtverlust 2008 (Gesamtjahr) Quelle: EAST & EPC

Geschätzte Verluste weltweit

Nach Schätzungen des US-Geheimdiensts beliefen sich im Jahr 2008 die Verluste aufgrund von Geldautomatenbetrug auf 1 Mrd. USD im Gesamtjahr bzw. 350 000 USD täglich.

Im Jahr 2007 betrugen die Kosten für Kredit- und Debitkartenbetrug im Vereinigten Königreich die Rekordsumme von 535 Mio. GBP. APACS berichtet, dass im Jahr 2008 eine Zunahme des Kartenbetrugs um 14 % auf knapp 610 Mio. GBP zu verzeichnen war. Der Betrug an Geldautomaten nahm um 31 % zu und belief sich im Jahr 2008 auf 45,7 Mio. GBP.

Aktuelle Vorfälle weltweit

Fälle von Geldautomatenkriminalität treten nach wie vor weltweit auf. Es wurden nicht nur Vorfälle aus Europa, sondern auch aus dem asiatisch-pazifischen Raum, Nord- und Südamerika, Afrika, Russland sowie dem Nahen und Mittleren Osten gemeldet. Einige Beispiele:

- ✓ Durch ein an einem Geldautomaten in Melbourne angebrachtes Skimming-Gerät wurden einer australischen Bank 500 000 USD gestohlen([4]).
- ✓ An einem Geldautomaten im Außenbereich eines Supermarktes im Vereinigten Königreich wurden Geräte zum Einlesen von Bank- und Kreditkartendaten angebracht([5]).

([3]) EMV bezeichnet einen Standard für die Interoperation von Zahlungskarten und geeigneten POS-Terminals sowie Geldautomaten' zur Authentifizierung von Zahlungen mit Kreditkarten und Debitkarten. Die Buchstaben EMV stehen für die drei Gesellschaften, die den Standard ursprünglich gemeinsam entwickelt hatten: *Europay*, *MasterCard* und *VISA*.
([4]) „ATM scam nets Melbourne thieves $ 500,000" (*Geldautomatendiebe erbeuten 500 000 USD*), 24. März 2009, verfügbar unter *http://www.atmmarketplace.com/article.php?id=10808* (zuletzt besucht am 20. April 2009)
([5]) „Shoppers are targeted in ATM scam" (*Einkaufende werden Opfer von Geldautomatenbetrug*), BBC News, 11. März 2006, verfügbar unter *http://news.bbc.co.uk/2/hi/uk_news/england/tees/4796002.*stm (zuletzt besucht am 20. April 2009)

- ✓ In Melbourne wurden zehn Geldautomaten zum Kopieren von Karten verwendet und ein Betrag im Wert von mehr als 1 Mio. USD von Bankkonten gestohlen([6]).
- ✓ In Staten Island wurde von mehr als 250 Opfern ein Betrag von 500 000 USD erbeutet, indem Kameras an der Tastatur eines Geldautomaten angebracht und die Opfer bei der Eingabe ihrer PIN-Nummern gefilmt wurden([7]).
- ✓ Auf einem Computer im Besitz von Kriminellen wurden etwa 4 000 Seiten mit Daten zu zypriotischen Kreditkarten gefunden ([8]).

Arten der Geldautomatenkriminalität

Eine Definition

Geldautomaten sind für Kriminelle besonders interessant, da sie einen direkten Zugang zu Banknoten und in einigen Fällen sogar zu persönlichen Daten des Benutzers ermöglichen, die für einen Diebstahl der Identität verwendet werden können. Während sich in Bankautomaten große Mengen an Bargeld befinden können, ermöglichen Bankkarten den Kriminellen den Zugang zu den Bankkonten des Kunden, die häufig Summen enthalten, die den in einem einzelnen Bankautomaten befindlichen Betrag leicht übersteigen können. Eine gestohlene Karte kann, sofern die PIN-Nummer bekannt ist, so lange von Kriminellen zur Abhebung von Geld von einem Bankkonto verwendet werden, bis der tägliche Höchstbetrag ausgeschöpft ist oder die Karte vom Eigentümer gesperrt wird. Obwohl die Kriminellen nach wie vor auf Geldautomaten und das darin befindliche Geld zielen, richten sie ihre Energien zunehmend auf den Erhalt von Daten zu Bankkarten und damit auf die Ausdehnung ihrer Gewinne.

Im Wesentlichen gibt es drei unterschiedliche Arten von Angriffen auf Geldautomaten:

- ✓ Versuche, die Daten zur Bankkarte eines Kunden zu stehlen;
- ✓ Computer- und Netzwerkangriffe auf Geldautomaten, um Daten zu Bankkarten zu erhalten;
- ✓ tätliche Angriffe auf Geldautomaten.

Diebstahl der Bankkartendaten von Kunden

Geldautomatenkriminalität zielt hauptsächlich auf den Diebstahl der auf einer Bankkarte gespeicherten Daten. Bis vor Kurzem wurden Magnetstreifen zur Speicherung der Informationen zur Identifizierung eines Kunden und ein PIN-Code zur Authentifizierung dieser Informationen bzw. Durchführung von Transaktionen an einem Geldautomaten eingesetzt. Leider sind die auf einem Magnetstreifen gespeicherten Informationen leicht zu kopieren und zu fälschen. Kriminelle konzentrieren sich daher auf Methoden zur Erfassung dieser Daten.

([6]) „Australian police suspect Romanian gang behind $ 1 million ATM scam" (*Australische Polizei vermutet rumänische Gruppe hinter einem Geldautomatenbetrug von 1 Mio. USD*), 14. April 2009, verfügbar unter *http://www.atmmarketplace.com/article.php?id=10883* (zuletzt besucht am 20. April 2009)

([7]) „ATMs on Staten Island rigged for identity theft; bandits steal $500G" (*Geldautomaten auf Staten Island manipuliert, Banditen stehlen 500 000 USD*), 11. Mai 2009, verfügbar unter http://www.nydailynews.com/news/ny_crime/2009/05/11/2009-05-11_automated_theft_bandits_steal_500g_by_rigging_atms_with_pinreading_gizmos.html#ixzz0J8qBVdar&D

([8]) „ATM scam targets hundreds of credit cards" (*Hunderte von Kreditkarten wurden Ziel von Geldautomatenbetrug*), New Europe, Ausgabe: 793, 4. August 2008, verfügbar unter *http://www.neurope.eu/articles/89221.php* (zuletzt besucht am 20. April 2009)

Diesem Schwachpunkt wurde teilweise durch die Einführung der EMV-Smartcards (auch als Chip und PIN-Karten oder Chipkarten bekannt) begegnet. Nach EAST arbeiten 90 % der europäischen Geldautomaten nun unter Einhaltung des EMV-Standards.

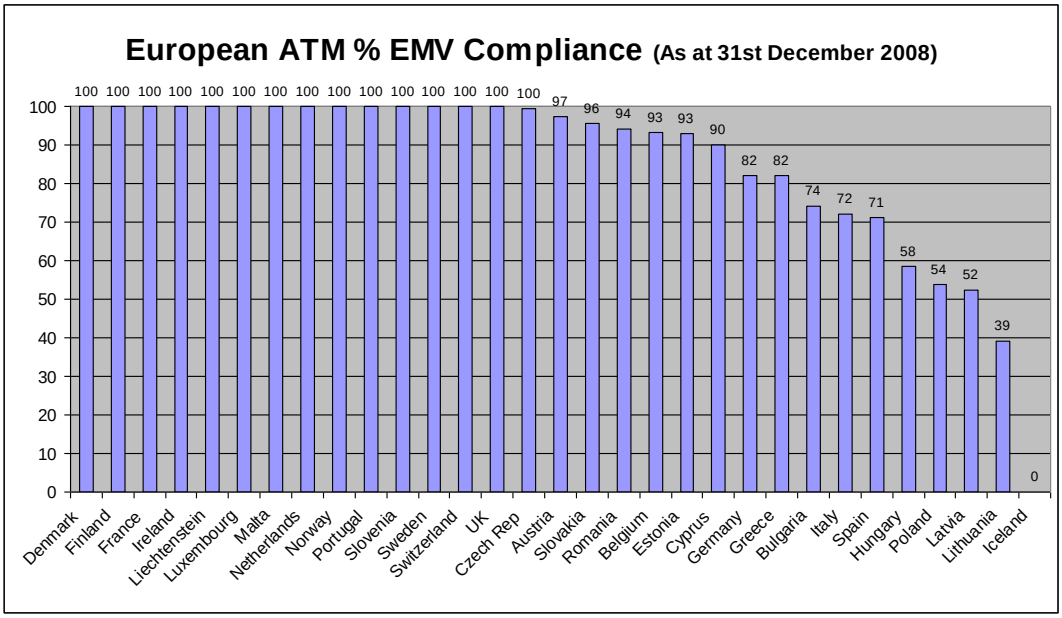


Abbildung 4: Prozentsatz der EMV-fähigen Geldautomaten in Europa, Quelle: EAST & EPC

Obwohl auch diese Karten mit einem Magnetstreifen ausgestattet sind, genügt der Magnetstreifen allein nicht, um eine Transaktion an einem Geldautomaten mit einem Kartenlesegerät, das für das Einlesen eines EMV-Chips ausgestattet ist, auszuführen (außer der Kartenemittent erlaubt eine derartige Transaktion). Fälschungen von EMV-Karten können daher nicht verwendet werden, um Bargeld von einem EMV-fähigen Geldautomaten abzuheben.

Da bis Ende des Jahres 2010 die meisten Europäer über EMV-fähige Karten verfügen werden, müssen die Kriminellen die gefälschten Karten außerhalb Europas und in Ländern einsetzen, in denen die Geldautomaten nicht EMV-fähig sind. Bis dahin besteht jedoch weiterhin die Gefahr gefälschter Bankkarten.

Skimming von Karten

An einem Geldautomaten werden die auf dem Magnetstreifen einer Karte gespeicherten Daten und die Geheimzahl durch einen modifizierten Kartenleser, ein sogenanntes Skimming-Gerät, erfasst. Das Skimming-Gerät wird unauffällig an einem Geldautomaten angebracht und erfasst die auf dem Magnetstreifen gespeicherten Daten sowie die Eingabe der Geheimzahl des Kunden. Der Kunde führt seine Karte in den mit einem Skimming-Gerät manipulierten Geldautomat ein, führt eine normale Transaktion aus und entnimmt die Karte. Der Kunde entfernt sich vom Geldautomaten und bemerkt nicht, dass seine Karte kopiert wurde. Die erfassten Daten werden dann zur Herstellung gefälschter Karten für betrügerische Abhebungen verwendet. Der Kunde bemerkt diese Tatsache erst, wenn unerlaubte Geldabhebungen/Transaktionen von seinem Bankkonto ausgeführt werden. Da Skimming-Geräte sehr ausgeklügelt und häufig schwer zu erkennen sind, sind zahlreiche Karten betroffen.

Von den Kriminellen werden verschiedene Methoden eingesetzt und die Geheimzahlen werden entweder durch den Einsatz kleiner Überwachungskameras oder eine Auflage auf die PIN-Eingabetastatur (falsche PIN-Eingabetastatur) ausgespäht. Mehr und mehr wird auch die Bluetooth-Wireless-Technologie([9]) verwendet, um Kartendaten und PIN-Nummern zu einem Laptop in der Nähe zu übermitteln. Diese Informationen können leicht an jeden Punkt der Welt versandt werden und ermöglichen die schnelle Herstellung gefälschter Karten.

Typische Methoden, die zum Skimming von Karten eingesetzt werden

Ein kleines Skimming-Gerät, das über dem Einzugsschlitz des Kartenlesers angebracht wird, (oder ein gefälschtes Bedienungsfeld auf dem Kartenlesegerät) mit einer Auflage auf der PIN-Eingabetastatur (bzw. einer kleinen Überwachungskamera) zum Ausspähen der PIN.

Abbildung 5: Die Abbildung wurde freundlicherweise von EAST zur Verfügung gestellt.

Abbildung 6: Die Abbildung wurde freundlicherweise von EAST zur Verfügung gestellt.

Über dem Instrumentenbrett des Geldautomaten wird eine vollständige falsche Front angebracht.

Abbildung 7: Die Abbildung wurde freundlicherweise von EAST zur Verfügung gestellt.

([9]) Die Bluetooth-Technologie ermöglicht die Kommunikation zwischen elektronischen Geräten über kurze Entfernungen mithilfe einer Funkverbindung.

Ein Skimming-Gerät wird in den Kartenleser zum Öffnen der Tür des Bankvorraums angebracht (die Kamera zum Ausspähen der PIN befindet sich üblicherweise über dem Geldautomaten im Vorraum der Bank).

Abbildung 8: Die Abbildung wurde freundlicherweise von EAST zur Verfügung gestellt.

Skimming-Geräte können sich auch neben dem normalen Kartenschlitz des Geldautomaten befinden und mit einer Aufschrift versehen sein, wonach die Karte zunächst durch das Gerät gezogen werden soll. Diese Methode ist jedoch in Europa nicht so verbreitet.

Abbildung 9: Die Abbildung wurde freundlicherweise von der Polizeiabteilung Neapel zur Verfügung gestellt.

Falsche Geldautomaten

Es wurden Fälle bekannt, in denen Kriminelle falsche Geldautomaten in- und außerhalb von Einkaufszentren und an anderen öffentlichen Orten aufgestellt hatten. Diese sehen aus wie echte Geldautomaten und einige von ihnen geben sogar Bargeld aus. Sämtliche in diese Automaten eingeführten Karten werden kopiert und die PIN-Informationen werden über die PIN-Eingabetastatur ausgespäht. Da diese Automaten nicht an ein Netzwerk angeschlossen werden, können die Kriminellen sie an jedem Ort aufstellen, an dem sich eine Stromversorgung befindet.

Aktueller Skimming-Vorfall an einem Geldautomaten

Im April 2009 ging ein in New York lebender 33-jähriger Mitarbeiter von Microsoft in die nächstgelegene Filiale der Chase Bank, um Geld für den Besuch beim Friseur abzuheben. Als er seine Karte in den Geldautomaten einführte, bemerkte er einen leichten Widerstand. Es wurde angezeigt, dass der Automat seine Karte nicht lesen konnte. Er versuchte es daher erneut. Beim zweiten Mal zeigte der Automat eine Fehlermeldung an.

Er wollte aufgeben und einen anderen Automaten verwenden, als ihm ein Gedanke kam. Er hatte von Geräten gehört, die von Betrügern an den Kartenlesern von Geldautomaten angebracht werden, und überlegte, obwohl es ihm unwahrscheinlich erschien, ob dies der Grund für sein Problem sein könnte. Er versuchte, die grüne Kunststoffabdeckung des Karteneinzugsschlitzes zu entfernen, und stellte fest, dass sie sich abnehmen ließ. Hinter einem an dem Automaten angebrachten Spiegel fand er zudem eine versteckte Kamera, die genau auf das Eingabefeld gerichtet war, um die Geheimzahlen der Opfer bei der Eingabe der PIN auszuspähen([10]).

Abbildung 10: Skimming-Vorfall

Einziehen der Karte

Hier wird eine Karte von einem Geldautomaten eingezogen und eine Reihe von Methoden eingesetzt, um an die Geheimzahl des Kunden zu gelangen. Verlässt der Kunde den Geldautomaten ohne seine Karte, wird die Karte von den Kriminellen entnommen und zur betrügerischen Abhebung von Bargeld oder zum Einkauf (in Geschäften, per Telefon oder online) verwendet. Üblicherweise wird bei jedem Angriff nur eine Karte entwendet. Die Kriminellen müssen jedes Mal, wenn eine Karte eingezogen wird, das gesamte Gerät abnehmen, obwohl kürzlich auch Geräte zum Einziehen von Karten entdeckt wurden, die über einen längeren Zeitraum angebracht werden und das Herausnehmen der Karten ermöglichen, ohne das Gerät zu entfernen.

Die meist verbreitete Variante ist unter der Bezeichnung „Libanesische Schlinge" bekannt. Die Diebe bringen am Kartenleser des Geldautomaten eine Schlinge, einen Draht oder einen starken Faden an. Dadurch kann die Karte in den Geldautomaten eingeführt und gelesen werden, wird jedoch nicht mehr ausgegeben. Die Kriminellen erspähen die Geheimzahl durch Beobachtung des Benutzers bei der Eingabe seiner PIN (visuelle Datenausspähung) und entnehmen die Karte, nachdem das Opfer die Bank in dem Glauben, die Karte wurde aus anderen Gründen vom Automaten eingezogen, verlassen hat.

Es werden zahlreiche Techniken zur Ermittlung der Geheimzahl des Kunden eingesetzt wie der Einsatz von Videokameras, das Anbieten von Hilfe oder das Ablenken des Kunden während der Eingabe der Geheimzahl. Eine weitere Form des Einziehens der Karte ist unter der Bezeichnung Algerian V bekannt.

Diebstahl durch Ablenkung oder „manuelles" Skimming

Ähnlich wie das Einziehen der Karte liegt der Unterschied nur darin, dass die Karte dem Besitzer von Kriminellen direkt entwendet wird. Nachdem sie die Eingabe der Geheimzahl beobachtet haben, lenkt eine Gruppe von Kriminellen den Benutzer ab und storniert die Transaktion. Während zwei Kriminelle den Benutzer beschäftigen (häufig durch Fallenlassen einer Banknote und Fragen des Benutzers, ob dies sein Geld sei), drückt ein Krimineller die Taste „Abbrechen" und entnimmt die Karte des Kunden. Wenn sich der Benutzer wieder dem Geldautomaten zuwendet, wird er informiert, dass der Geldautomat nicht funktioniert und seine Karte nicht zurückgeben wird.

Visuelle Datenausspähung

([10]) http://abcnews.go.com/Technology/Business/story?id=7434509&page=1

Dies bezeichnet eine von Betrügern angewandte Technik zum Erhalt einer Geheimzahl, die üblicherweise beim Einzug der Karte oder beim Stehlen der Karte durch Ablenkung eingesetzt wird. Hinter dem Opfer stehend liest der Kriminelle die Geheimzahl während der Eingabe und merkt sich diese, schreibt diese auf oder gibt sie direkt in ein Mobiltelefon ein.

Fortführung der Transaktion

Hier setzt ein Krimineller eine nicht abgeschlossene Transaktion fort, nachdem das Opfer den Geldautomaten verlassen hat. Dies geschieht üblicherweise, indem das Opfer mitten während einer Transaktion in dem Glauben gelassen wird, der Geldautomat funktioniere nicht oder durch andere Methoden dazu bewegt wird, sich während des Abhebens von Bargeld vom Automaten zu entfernen.

Ein aktueller Vorfall aus den USA

Innerhalb einer halben Stunde, nachdem sie Bankkarten während einer Transaktion gestohlen hatten, beraubten zwei Männer nichts ahnende Kunden um 1 800 USD Bargeld. In einem von drei bekannten Fällen ist die Polizei der Ansicht, die Kriminellen entfernten sich weniger als zwei Meter zu einem benachbarten Geldautomaten und hoben in drei verschiedenen Transaktionen 900 USD ab, während die Opfer in der Bank ihre Karten sperren ließen. In einem anderen Fall stahl ein Paar innerhalb einer halben Stunde nach dem Diebstahl der Bankkarte 900 USD durch Kreditkartentransaktionen und Bargeldabhebungen.

Nach den Vermutungen der Polizei beobachtet der erste Angreifer einen Bankkunden bei der Eingabe der Geheimzahl in den Automaten und gibt die Nummer in ein Mobiltelefon ein. Der zweite Angreifer lenkt dann den Kunden durch das Fallenlassen eines 20 USD-Scheins ab und hält ihn an der Schulter fest, während der erste Angreifer die Karte stiehlt, nachdem sie vom Geldautomaten ausgegeben wurde. Die gestohlene Karte wird dann an einem anderen Geldautomaten eingesetzt, während sich der Kunde wundert, warum der Geldautomat seine Karte nicht zurückgibt([11]).

Entnahme von Bargeld

Kriminelle bringen ein Gerät am Geldausgabeschlitz an, durch das die Banknoten im Inneren des Geldautomaten bleiben, wenn ein Kunde eine Abhebung vornimmt. Der Kunde verlässt den Automaten in der Annahme, der Geldautomat funktioniere nicht, und betritt die Bank, um den Vorfall zu melden, während die Diebe die Banknoten entnehmen.

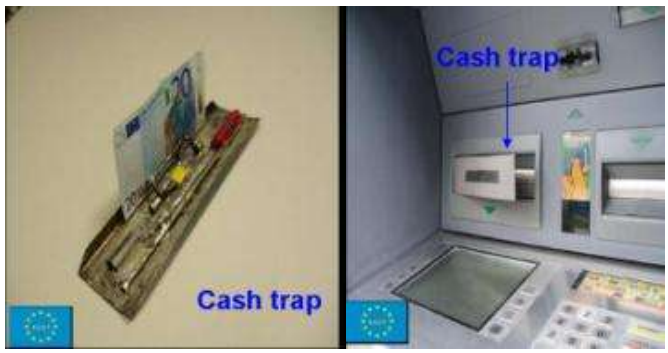


Abbildung 11: Die Abbildung wurde freundlicherweise von EAST zur Verfügung gestellt.

Computer- und Netzwerkangriffe

Das Internet bietet weltweiten Zugang und Konnektivität. Es ermöglicht jedem von uns den Zugang zu Menschen in der ganzen Welt. Es bietet jedoch auch Kriminellen den Zugang zu Systemen und Menschen. Auch diese Bedrohung zeigt sich auf diese Weise.

Netzwerkangriffe auf Geldautomaten

([11]) Robinson G., „Bondi banks scam: ATM alert" *(Betrug der Banken in Bondi: Geldautomatenwarnung*), *The Sydney Morning Herald*, Oktober 2008, verfügbar unter http://www.smh.com.au/news/national/bondi-banks-scam-atm-alert/2008/10/09/1223145514492.html?sssdmh=dm16.338950 (zuletzt besucht am 2. Juli 2009)

Geldautomaten kommunizieren über eine Netzwerkverbindung mit den Systemen der Banken. Einige dieser Verbindungen verwenden private Netzwerke und eigene Netzwerkprotokolle. Häufiger werden diese Verbindungen jedoch über das Internet hergestellt und Standardnetzwerkprotokolle eingesetzt. Die Betrüger verwenden Computerprogramme (Malware), um Geldautomaten anzugreifen und sich über Software oder eine Sicherheitslücke des Computers Zugang zu verschaffen. Sobald sie Zugang zu einem Geldautomaten haben, installieren die Betrüger eine Software, die Kartendaten und PIN-Nummern erfasst. Ein infizierter Geldautomat unterscheidet sich optisch nicht von einem normalen Geldautomaten und die Benutzer sind sich der Gefahr nicht bewusst.

Viren und bösartige Software

Geldautomaten verwenden häufig öffentlich zugängliche Betriebssysteme und Standardhardware und sind daher anfällig für eine Infektion mit Viren oder anderer schädlicher Software. Die schädliche Software gelangt über Netzwerkangriffe oder andere infizierte Geräte in den Geldautomaten. Nach ihrer Installation auf dem Geldautomaten sammelt die schädliche Software Kartendaten und Geheimzahlen.

Aktueller Vorfall

Im April 2009 wurden in Russland Geldautomaten entdeckt, die mit einer ausgeklügelten bösartigen Software infiziert waren (Malware). Die Software war in der Lage, nicht nur die Kartendaten, sondern auch die Geheimzahl zu erfassen. Während ein bestimmter Geldautomat erfolgreich infiziert wurde, ließen im März eingegangene Geheimberichte vermuten, dass auch andere Geldautomaten angegriffen wurden([12]).

Phishing

Seit vielen Jahren gibt es Betrugsversuche über schriftliche Kommunikation. Mit der Verbreitung von E-Mails und Internet hat sich diese Betrugsform weltweit verbreitet und den Namen „Phishing" erhalten. Durch Phishing soll der Nutzer dazu aufgefordert werden, seine Kartennummer und Geheimzahl anzugeben. Die Betrüger versenden eine E-Mail, die sie als Bank ausgibt, und geben an, die Kontoangaben seien unvollständig oder der Benutzer habe seine Kontoinformationen zu aktualisieren, um sein Konto weiterhin nutzen zu können. Der Benutzer wird aufgefordert, einen Link anzuklicken und die dort angegebenen Eingaben auszuführen. Dieser Link führt jedoch zu einer von den Betrügern eingerichteten Site, die der Site der Bank ähnelt. Dort soll der Benutzer vertrauliche Informationen wie die Kartenummer und die Geheimzahl eingeben. Diese Informationen werden von den Betrügern erfasst und zur Herstellung gefälschter Karten, zur Abhebung von Bargeld vom Konto des Benutzers und zum Einkaufen verwendet.

Angriffe für Dritte

Betrüger setzen ausgeklügelte Programmierungsmethoden([13]) ein, um auf die Websites in den Netzwerken von Finanzinstitutionen zu gelangen. Über diesen Zugang erhalten die Betrüger Zugriff auf die Banksysteme und die Datenbank der Geldautomaten. Die Betrüger erfassen Kartennummern und ändern gegebenenfalls die Geheimzahlen der Karten, die sie einsetzen wollen. Anschließend verkaufen sie die Karten mit den zugehörigen Daten an andere Betrüger. Diese Betrüger erstellen Bankkarten mit den gestohlenen Informationen und verwenden diese Karten zum Abheben von Bargeld von Bankkonten. Die ursprünglichen Betrüger erhalten üblicherweise einen Prozentsatz an den Gewinnen.

([12]) http://www.atmsecurity.com/monthly-digest/atm-security-monthly-digest/atm-fraud-and-security-digest-march-2009.html
([13]) Durch die Verwendung von SQL-Techniken

Aktueller Vorfall

Im Januar und Februar 2008 gab der US-Geheimdienst bekannt, er ermittle in zwei Fällen. Der eine betraf die OmniAmerican Credit Union und der andere die Global Cash Card. Im April und Mai 2008 traten derartige Fälle auch bei Symmetrex, einem Abwickler von Zahlungstransaktionen, und 1st Source Bank auf. Die Karten von Symmetrex wurden von der MetaBank eingesetzt. Allein diese beiden Institutionen erlitten Verluste in Höhe von 4 Mio. USD([14]).

Tätliche Angriffe auf Geldautomaten

Durch tätliche Angriffe auf Geldautomaten wollen die Täter sich Zugang zum Bargeld im Tresor oder in den Sicherheitseinrichtungen eines Geldautomaten verschaffen Einige der häufigsten Methoden sind dabei Raubüberfälle durch das Rammen eines Fahrzeugs, Explosionen (mit Gas oder anderen Mitteln) und Aufschneiden (z. B. mithilfe von Kreissägen, Schneidbrennern, Sauerstofflanzen oder Diamantbohrern). Raubüberfälle sind auch beim Auffüllen oder der Wartung von Geldautomaten möglich. Die Mitarbeiter werden entweder überfallen, während sie Bargeld vom oder zum Geldautomaten bringen oder während der Tresor des Geldautomaten geöffnet und die Geldkassette ausgetauscht wird.

Sicherheitsmaßnahmen

Was passiert, wenn die Daten eines Kunden ausgespäht wurden?

Wenn Kriminelle einmal die Kartennummern und Geheimzahlen in ihrem Besitz haben, können diese Informationen auf unterschiedliche Weise verwendet werden. Die Kartendaten können entweder zum Abheben von Bargeld vom Bankkonto des Kunden oder zum Einkaufen über das Internet oder Telefon verwendet werden. Gefälschte Kredit- und Debitkarten können für die Verwendung durch andere Personen hergestellt werden.

Die Kriminellen arbeiten normalerweise in gut organisierten Gruppen und können im Auftrag größerer krimineller Vereinigungen tätig sein. Derzeit nimmt die Zahl krimineller Gruppen aus dem Ausland bei diesen Betrugsfällen zu.

Risiken und Gefahren

Die Erläuterung der möglichen Risiken und Gefahren für die Bürger nach erfolgreicher Geldautomatenkriminalität stellt eine wichtige Aufgabe dar. Dies liegt hauptsächlich daran, dass durch Geldautomatenkriminalität nicht nur der Zugang zum Bankkonto eines Opfers ermöglicht wird, sondern die Kriminellen auch über Informationen und Instrumente verfügen, um weitergehenden Betrug zu begehen, wie das Auftreten als eine andere Person bis zur Übernahme eines Bankkontos.

Dies lässt sich vielleicht am besten anhand der zunehmenden Zahl der Dienstleistungen erläutern, die über den üblichen Bankautomaten für ein Bankkonto angeboten werden. Wurden beispielsweise die Informationen zu Ihrer Debitkarte zusammen mit der Geheimzahl ausgespäht, hat der Betrüger nicht nur den Zugang zum Geld auf einem Konto, sondern kann eine Reihe von Verwaltungsfunktionen durchführen, die speziell auf die Ausführung weitergehender Betrüge zielen.

Die Zahl der Risiken und Gefahren sind daher beinahe unendlich. Zwei Kategorien von Risiken stechen jedoch besonders hervor:

([14]) http://garwarner.blogspot.com/2009/03/bank-hacking-exposed-analyzer-affadavit.html

Die erste Risikokategorie betrifft direktere Angriffe wie das Einbehalten von Banknoten, die libanesische Schlinge, bei der die Karte sofort in den Besitz des Betrügers gelangt, oder körperliche Angriffe auf die Benutzer von Geldautomaten bzw. tätliche Angriffe auf die Geldautomaten selbst, durch Taschendiebstahl oder Rammen des Automaten durch ein Fahrzeug.

Die zweite Risikokategorie zielt eher auf langfristigere Schädigungen und dürfte aufgrund ihrer Unterschiedlichkeiten zu den häufiger verbreiteten Gefahren zählen. Diese Form der Kriminalität führt immer zur nachfolgenden Nutzung der Informationen und Identität des Opfers, auch wenn sie häufig zu sofortigen Gewinnen wie dem direkten Zugang zu Barmitteln führt. Die Reihe der möglichen Betrugsfälle umfasst den Diebstahl der Identität, die Übernahme des Kontos und Erpressung und hat für das Opfer neben den finanziellen Verlusten häufig weitere unerwünschte Folgen wie eine Verschlechterung der Kreditwürdigkeit oder Gerichtsverhandlungen.

Künftig wird Geldautomatenkriminalität für Kriminelle vermutlich noch attraktiver, da die Dienstleistungen und Produkte, die über die neueste Generation von Geldautomaten zur Verfügung stehen, noch weiter ausgedehnt und entwickelt werden. Zum einen wird eine zunehmende Zahl von Geldautomaten für die Einzahlung von Bargeld und Schecks entwickelt und zum anderen werden viele Geldautomaten jetzt für die Ausgabe anderer Produkte eingesetzt wie Briefmarken, die auch für Kriminelle attraktiv sind. Unter diesen Umständen ist davon auszugehen, dass sich auch die verschiedenen Arten von Angriffen weiterentwickeln und die Geldautomatenkriminalität in all ihren verschiedenen Formen weiterhin Anlass zur Besorgnis geben wird, weshalb die Sensibilisierung der Öffentlichkeit noch notwendiger wird.

Sicherheitsmaßnahmen für Geldkarteninhaber

Der Geldautomatenbetrug wird zunehmend ausgeklügelter und die Kriminellen haben neue und innovative Formen entdeckt, mit gefälschten Karten, die die Daten von realen Karteninhabern aufweisen, Geld von Bankkonten abzuheben. Auch wenn die kriminellen Methoden, um an Geld zu gelangen, technisch ausgereifter sind, sind die Probleme der Karteninhaber die gleichen wie zu Beginn des Geldautomatenbetrugs.

Wichtigstes Ziel eines Kontoinhabers ist die Sicherheit seines Geldes auf der Bank. Informationssicherheit hat sich zu lange nur auf technische Lösungen zur Maximierung des Schutzes beschränkt. In Zusammenhang mit den Vorfällen im Bereich Geldautomatensicherheit wird dem menschlichen Faktor in den vergangenen Jahren mehr Aufmerksamkeit gewidmet. Die Karteninhaber müssen sich der Risiken, denen sie ausgesetzt sind, bewusst sein und müssen wissen, wie sie Betrug verhindern oder Schaden begrenzen können, wenn ihre Kartendaten in die falschen Hände gelangen. Geldautomaten werden von Betrügern sowohl für den Erhalt der Kartendaten als auch zur betrügerischen Abhebung von Geld von den Konten der Kunden eingesetzt. Die Karteninhaber sollten sich dieser Problematik stets bewusst sein, wenn sie ihre Karten verwenden, Menschen beim Geldabheben beobachten oder ihre eigenen Kontoauszüge prüfen.

Schutz der Karten

Die Karteninhaber sollten sich der mit ihren Karten verbundenen Risiken sowie der Möglichkeiten zur Vermeidung von betrügerischen Abhebungen von Bankkonten anderer Karteninhaber bewusst sein.

Die ersten Zeichen, dass etwas nicht in Ordnung ist, zeigen sich beim Besuch des Geldautomaten. Es ist wichtig, dass die Karteninhaber auf die Umgebung achten, nahe am Geldautomaten stehen und das

Eingabefeld so abdecken, dass niemand die Eingabe der PIN beobachten kann. Die beste Möglichkeit, die eigene Karte und die Kartendaten zu schützen, besteht in der Aufmerksamkeit bei der Nutzung eines Geldautomaten. Durch die regelmäßige Verwendung des gleichen Geldautomaten wissen Karteninhaber beispielsweise, wie dieser auszusehen hat, und können normale und zu erwartende Verhaltensweisen abschätzen. Sollte etwas an dem Automaten ungewohnt sein, dürfen die Karteninhaber diesen nicht verwenden und sollten ihre Bank über ihre Beobachtungen oder den Verdacht informieren.

Persönlicher Schutz

Sollten Karteninhaber verdächtige Verhaltensweisen in der Nähe von Geldautomaten beobachten, ist umgehend die Bank zu unterrichten, sofern dies möglich ist. Wichtig ist es auch, niemals einen verdächtig aussehenden oder einen nicht normal funktionierenden Geldautomaten weiter zu untersuchen, da die Betrüger sich häufig in der Nähe aufhalten und möglicherweise eingreifen, wenn jemand den Geldautomaten genauer prüft. In einigen Fällen wurden die Karteninhaber körperlich angegriffen, als sie herausfinden wollten, was mit dem Geldautomaten nicht in Ordnung war. Achten Sie auf andere Menschen in der Nähe des Geldautomaten. Falls sich jemand verdächtig verhält oder die Nutzung des Geldautomaten ein ungutes Gefühl auslöst, informieren Sie bitte die Bank über Ihren Verdacht und verwenden Sie einen anderen Geldautomaten.

Schutz der Geheimzahl

Betrüger setzen zahlreiche unterschiedliche Methoden ein, um an Kartendaten zu gelangen. Der wichtigste Schutz der Karteninhaber vor Betrug ist daher die Geheimhaltung der PIN. Ist den Betrügern die Geheimzahl bekannt, haben sie leichten Zugang zu dem Geld. Geldautomaten verfügen nicht weltweit über die gleichen Sicherheitsvorkehrungen. Nach einer Reise ins Ausland sollten Karteninhaber daher ihre PIN ändern. Die Betrüger werden auch versuchen, die ihnen bekannte PIN für den Zugriff auf andere Karten zu verwenden, daher werden für unterschiedliche Karten nachdrücklich verschiedene Geheimzahlen empfohlen.

Geldkartendaten und das Internet

Einen weiteren Zugang zu persönlichen Bank- und Authentifizierungsinformationen wie beispielsweise Geheimzahlen bietet das Internet. Sobald die Informationen bekannt sind, können gefälschte Karten hergestellt werden. Phishing-Vorfälle nehmen zu, bei denen die Karteninhaber eine E-Mail mit der Aufforderung erhalten, auf einen Link zu klicken und persönliche Daten und Bankangaben einzugeben. Die E-Mails werden häufig von authentisch wirkenden Absendern verschickt, da die Betrüger sehr ausgeklügelte Methoden entwickelt haben, um die Korrespondenz der Banken nachzuahmen. Daher ist das Erkennen betrügerischer Nachrichten teilweise schwierig. Eine wichtige Regel ist daher, niemals auf Hyperlinks in E-Mails zu klicken, in denen zur Bestätigung von Bankinformationen aufgefordert wird. Eine weitere Vorsichtsmaßnahme ist der Einsatz guter Antiviren- und Firewall-Programme auf dem für das Internet-Banking eingesetzten PC.

Weitere Sicherheitsmaßnahmen

Eine weitere Sicherheitsmaßnahme könnte in der Verwendung von aufladbaren Bankkarten bestehen, über die nur ein begrenzter Geldbetrag zur Verfügung steht. Auf diese Weise können Betrüger keine größere Beträge abheben, die ein Karteninhaber möglicherweise auf seinem Bankkonto hat.

Die Verbraucher sollten auch wachsam sein, wenn sie Bankinformationen über das Telefon weitergeben, da jemand in der Nähe das Gespräch belauschen könnte. Telefongespräche mit der Bank sollten daher ausschließlich an ruhigen Orten geführt werden.

Um betrügerische Geldabhebungen entdecken zu können, sollten Karteninhaber ihre Banktransaktionen und Kontoauszüge regelmäßig überprüfen.

Notfallnummern der Bank bereitlegen

Nachdem sich Betrüger den Zugang zu den Kartendaten und Geheimzahlen verschafft haben, werden sie versuchen, so schnell wie technisch möglich Geld von den Konten abzuheben. Die Bank und gegebenenfalls die örtlichen Behörden sind daher so schnell wie möglich zu informieren, wenn ein Karteninhaber vermutet, seine Geheimzahl und/oder Kartendaten wurden ausgespäht, damit die Bank das Konto bzw. die Konten sperren und so betrügerische Geldabhebungen verhindern kann. Dabei ist es entscheidend, die Notfallnummern der Bank jederzeit bei der Hand zu haben. Es ist daran zu denken, dass beim Verlust der Karte auch die Notfallnummer verloren geht, wenn sie nicht auch an anderer Stelle notiert wird. Informieren Sie sich zudem über die aus dem Ausland zu wählende Notfallnummer, da sie sich möglicherweise unterscheiden kann.

TEIL 2: WICHTIGE REGELN

Verhaltensregeln zur Bekämpfung von Geldautomatenkriminalität

Diese Sicherheitstipps sind das Resultat von Datenauswertungen und verfügbaren Forschungsergebnissen. In diesem Abschnitt werden die Empfehlungen für die Sensibilisierung gegenüber den unterschiedlichen Arten von Betrug sowie die entsprechenden Gegenmaßnahmen übersichtlich dargestellt.

Diese Verhaltensregeln bieten ein Höchstmaß an Schutz bei geringstmöglichem Aufwand. Durch die Einhaltung dieser Verhaltensregeln können die Benutzer von Geldautomaten ihre Sicherheit erhöhen.

Kategorie	#	Empfehlungen	Beschreibung
Auswahl eines sicheren Geldautomaten	1.	Benutzen Sie keine Geldautomaten, die mit spezieller Beschilderung oder Warnungen versehen sind.	Benutzen Sie keine Geldautomaten, an denen besonders viele Schilder und Warnhinweise angebracht sind, da diese häufig von Betrügern eingesetzt werden, um den Eindruck zu erwecken, der manipulierte Geldautomat sei sicher. Besondere Vorsicht ist angeraten, wenn ungewohnte Bedienhinweise für den Geldautomaten angegeben sind.
	2.	Benutzen Sie die Geldautomaten in den Innenräumen der Bank.	Falls möglich, sollten eher die Geldautomaten in Banken, anderen Gebäuden oder abgeschlossenen Räumen als die Bankautomaten auf der Straße genutzt werden. Die an der Straße angebrachten Geldautomaten bieten Kriminellen einen einfacheren Zugang.
	3.	Benutzen Sie keine freistehenden Geldautomaten.	Vermeiden Sie die Nutzung freistehender Geldautomaten. Die Geldautomaten sollten an der Wand eines Gebäudes angebracht sein oder sich innerhalb einer Anlage befinden. Bietet der Geldautomat keinen Schutz, ist jedoch an einem Gebäude angebracht und funktioniert ordnungsgemäß, haben Sie vermutlich nichts zu befürchten.
Beobachtung der Umgebung	4.	Achten Sie auf die Umgebung des Geldautomaten.	Achten Sie stets auf Ihre Umgebung. Benutzen Sie einen Geldautomaten, der gut sichtbar und gut ausgeleuchtet ist. In dunklen Bereichen und an schlecht geschützten oder überwachten Orten ist besondere Vorsicht angeraten.
	5.	Achten Sie auf einen ausreichenden Abstand der anderen Kunden am Geldautomat.	Achten Sie darauf, dass sich andere Personen in einem ausreichenden Sicherheitsabstand befinden. Es ist Vorsicht geboten, falls Fremde Ihnen an einem Geldautomaten Hilfe anbieten, selbst wenn die Karte nicht ausgegeben wird oder Sie andere Schwierigkeiten haben. Lassen Sie sich von niemandem ablenken.
	6.	Schützen Sie Ihre PIN, indem Sie nahe am Geldautomaten stehen und das Eingabefeld	Decken Sie das Eingabefeld bei der Eingabe der PIN mit der Hand ab, damit Ihre Daten nicht von einer Kamera oder einer anderen Person eingesehen werden können. Geben Sie niemals

		abdecken.	ihre Geheimzahl an andere weiter.
Prüfung des Geldautomaten	7.	Achten Sie auf die Vorderseite der Automaten.	Sollte die Vorderseite des Geldautomaten sich von anderen Automaten unterscheiden (z. B. durch einen zusätzlichen Spiegel), über Klebespuren (möglicherweise von einem angebrachten Gerät) oder zusätzliche Beschilderungen verfügen, ist ein anderer Automat zu verwenden und die Bank über die Beobachtungen zu unterrichten.
	8.	Achten Sie auf den Karteneinzugsschlitz.	Wenn Sie einen Ihnen unbekannten Geldautomaten benutzen, der sich nicht innerhalb einer Bank befindet, untersuchen Sie das Gerät sorgfältig. Selbst wenn Ihnen der Geldautomat bekannt ist, sollten Sie auf etwaige Unterschiede oder ungewohnte Eigenschaften des Kartenlesegeräts achten. Sieht der Einzugsschlitz ungewohnt oder zu groß aus, drücken Sie mit der Hand dagegen. Wenn ein Gerät über dem Lesegerät angebracht wurde, sitzt dieses locker oder lässt sich sogar entfernen. Vorrichtungen zur Einziehung der Karten oder des Bargelds müssen am Kartenlesegerät oder Geldausgabeschlitz befestigt werden. Verwenden Sie den Geldautomaten nicht, wenn etwas am Karteneinzugsschlitz oder Eingabefeld befestigt wurde. Brechen Sie die Transaktion ab und entfernen Sie sich vom Geldautomaten. Versuchen Sie niemals, verdächtige Geräte zu entfernen.
	9.	Untersuchen sie die PIN-Eingabetastatur sorgfältig.	Selbst wenn Ihnen der Geldautomat bekannt ist, achten Sie auf etwaige Unterschiede oder ungewohnte Eigenschaften der PIN-Eingabetastatur. Sollte eine falsche PIN-Eingabetastatur über der echten Tastatur angebracht sein, wird sie sich bei leichten Vor- und Rückbewegungen verschieben lassen.
	10.	Achten Sie auf zusätzliche Kameras.	Achten Sie darauf, ob neben den üblichen Sicherheitskameras an Geldautomaten noch weitere Kameras angebracht sind.
	11.	Melden Sie eingezogene Karten sofort.	Melden Sie eingezogene Karten sofort. Falls möglich, entfernen Sie sich dabei nicht vom Geldautomaten. Rufen Sie stattdessen die Bank von dem Geldautomaten aus an, der Ihre Karte eingezogen hat. Vertrauen Sie niemals auf die Hilfe von Fremden beim Wiedererhalt einer eingezogenen Karte. Informieren Sie zusätzlich die örtlichen Polizei- und Sicherheitskräfte.
	12.	Seien Sie vorsichtig, wenn der Geldautomat kein Geld ausgibt oder keine Gebühr erhoben wird.	Sollte der Geldautomat kein Bargeld ausgeben, handelt es sich vermutlich um Betrug und Sie sollten Ihre Bank über die möglichen Gefahren für Ihr Bankkonto unterrichten. Bei Verwendung eines Geldautomaten, der nicht an eine Bank angeschlossen ist (häufig an Tankstellen oder in Bars), ist besondere Vorsicht geboten, wenn keine Gebühr erhoben wird. Für private Geldautomaten, die nicht zu einer Bank gehören, werden Gebühren erhoben. Wird keine Gebühr erhoben, ist dies ein Hinweis darauf, dass es sich möglicherweise um einen falschen Geldautomaten handelt.

Überprüfung der Kontoauszüge	13.	Überprüfen Sie regelmäßig Ihre Kontoauszüge.	Überprüfen Sie ihre Kontoauszüge regelmäßig auf Transaktionen, die Ihnen nicht bekannt sind. Obwohl die meisten Betrugsfälle unverzüglich nach dem Ausspähen der Informationen auftreten, können einige auch erst Wochen oder Monate später ausgeführt werden. Durch die häufige Überprüfung der Kontoauszüge können die Folgen möglicher Betrugsfälle begrenzt werden.
Melden verdächtiger Aktivitäten	14.	Melden Sie eingezogene Karten sofort.	Melden Sie eingezogene Karten sofort. Falls möglich, entfernen Sie sich dabei nicht vom Geldautomaten. Rufen Sie stattdessen die Bank von dem Geldautomaten aus an, der Ihre Karte eingezogen hat. Vertrauen Sie niemals auf die Hilfe von Fremden beim Wiedererhalt einer eingezogenen Karte. Informieren Sie zusätzlich die örtlichen Polizei- und Sicherheitskräfte.
	15.	Melden Sie sofort jegliche auffälligen Aktivitäten.	Der Verlust oder Diebstahl der Bankkarte oder betrügerische Aktivitäten auf Ihrem Bankkonto sollten unverzüglich gemeldet werden, um weitere Verluste zu verhindern.

Schlussfolgerungen

Geldautomaten sind ein wichtiger Teil des Handels in Europa und bieten ihren Kunden wertvolle Dienstleistungen. Mit der zunehmenden Nutzung von Geldautomaten ist ein dramatischer Anstieg von Angriffen auf Geldautomaten und Betrugsfällen zu beobachten. Methoden wie Skimming, Phishing und Netzwerkangriffe auf Geldautomaten haben im vergangenen Jahr zu Verlusten von fast 500 Mio. EUR in Europa geführt. Die Methoden werden immer ausgeklügelter und haben zu einem Anstieg der Angriffe auf Geldautomaten von 149 % im Jahr 2008 geführt.

In dieser Veröffentlichung werden zahlreiche Formen beschrieben, wie Geldautomaten angegriffen werden, sowie Methoden und Hinweise zum Schutz für die Nutzer von Geldautomaten dargestellt.

Die ENISA ist der Ansicht, dass die Sensibilisierung für mögliche Gefahren und Gegenmaßnahmen einen wichtigen Schritt zur Bekämpfung von Geldautomatenbetrug darstellt.

Diese Informationen können das Auftreten und die finanziellen Folgen von Angriffen auf Geldautomaten signifikant senken und zu einem größeren Vertrauen in den Einsatz von Geldautomaten führen.

ANHANG

Nutzung und Betrug von Geldautomaten: Fallstudien

Der ENISA liegen Fallstudien und Erfahrungsberichte aus mehreren europäischen Staaten vor, die sich mit unterschiedlichen Fällen der Nutzung und des Betrugs von Geldautomaten befassen. Dem Leser sollen anhand dieser Studien die wesentlichen Probleme und Lösungen vorgestellt und die empfohlenen Verhaltensweisen effektiv und konkret verdeutlicht werden.

Zypern

Derzeit sind auf der Insel (in dem von der Republik Zypern kontrollierten Gebiet) etwa 560 Geldautomaten aufgestellt. Es liegen keine Informationen zur Zahl oder Art der im türkisch besetzten Gebiet der Insel vorhandenen Geldautomaten vor. Die meisten der 560 Geldautomaten sind fest an Wänden installiert. Zwei bis drei Geldautomaten sind an sogenannten Geldkiosken angebracht. Eine beträchtliche Zahl der auf der Insel befindlichen Geldautomaten ist an den Karteneinzugsschlitzen mit besonderen Kunststoffschildern und einem Gerät zum Schutz vor Skimming versehen, um das Anbringen derartiger Geräte (und damit das Erfassen der Informationen auf dem Magnetstreifen) zu verhindern. Dies könnte eine wichtige Rolle bei der Bekämpfung von Geldautomatenbetrug durch Skimming spielen([15]).

Aktuelle Vorfälle in Zypern

Die folgenden Informationen wurden vom System für Betrugsüberwachung der JCC Payments System Ltd. erfasst.

Fall Nr. 1:

Von mehreren Personen wurden gefälschte und neu codierte Karten an Geldautomaten benutzt. Es wurden 26 Karten eingesetzt und insgesamt ein Betrag von 2 310,00 EUR abgehoben. Das System zur Betrugsüberwachung ermittelte die betrügerischen Handlungen und informierte die zyprische Polizei. Einer der Betrüger wurde am Flughafen festgenommen.

Fall Nr. 2:

Zwei Personen verwendeten gefälschte Karten an Geldautomaten. Es wurden 131 Karten eingesetzt und insgesamt ein Betrag von 15 830,00 EUR abgehoben. Nach ihrer Identifizierung durch das System zur Betrugsüberwachung wurden die Personen bei der Benutzung der gefälschten Karten von der Polizei verhaftet.

Fall Nr. 3:

Eine Person verwendete gefälschte Karten an Geldautomaten. Es wurden 43 Karten eingesetzt und insgesamt ein Betrag von 1 860,00 EUR abgehoben. Das System zur Betrugsüberwachung ermittelte die betrügerischen Handlungen und informierte die zyprische Polizei. Der Betrüger wurde festgenommen.

Fall Nr. 4:

Zwei Personen verwendeten gefälschte Karten an Geldautomaten. Es wurden 76 Karten eingesetzt und insgesamt ein Betrag von 7 950,00 EUR abgehoben. Das System zur Betrugsüberwachung ermittelte die betrügerischen Handlungen und informierte die zyprische Polizei. Die Betrüger wurden verhaftet.

([15]) Sämtliche Informationen wurden von der Abteilung Risikomanagement von JCC Payments Systems Ltd, dem einzigen Acquirer/Processor von VISA, MasterCard, AMEX und Diners in Zypern, zur Verfügung gestellt.

Fall Nr. 5:

Von mehreren Personen wurden gefälschte Karten an Geldautomaten verwendet. Es wurden 53 Karten eingesetzt und insgesamt ein Betrag von 10 700,00 EUR abgehoben. Das System zur Betrugsüberwachung ermittelte die betrügerischen Handlungen und informierte die zyprische Polizei. Ein Betrüger wurde festgenommen.

Fall Nr. 6:

Zwei Personen verwendeten gefälschte Karten an Geldautomaten. Es wurden 122 Karten eingesetzt und insgesamt ein Betrag von 21 980,00 EUR abgehoben. Nach ihrer Identifizierung durch das System zur Betrugsüberwachung wurden die Personen bei der Benutzung der gefälschten Karten von der Polizei verhaftet.

Fall Nr. 7:

Eine Person verwendete gefälschte Karten an Geldautomaten. Es wurden 41 Karten eingesetzt und insgesamt ein Betrag von 28 340,00 EUR abgehoben. Nach ihrer Identifizierung durch das System zur Betrugsüberwachung wurde die Person bei der Benutzung der gefälschten Karten von der Polizei verhaftet.

Fall Nr. 8:

Eine Person verwendete gefälschte Karten an Geldautomaten. Es wurden 82 Karten eingesetzt und insgesamt ein Betrag von 12 330,00 EUR abgehoben. Das System zur Betrugsüberwachung ermittelte die betrügerischen Handlungen und informierte die zyprische Polizei. Der Betrüger wurde festgenommen.

Fall Nr. 9:

Zwei Personen verwendeten gefälschte Karten an Geldautomaten. Es wurden 21 Karten eingesetzt und insgesamt ein Betrag von 10 980,00 EUR abgehoben. Das System zur Betrugsüberwachung ermittelte die betrügerischen Handlungen und informierte die zyprische Polizei. Die Betrüger wurden verhaftet.

Risiken und Gefahren

Entwicklung des Geldautomatenbetrugs

Im Jahr 2009 war ein kontinuierlicher Rückgang des Geldautomatenbetrugs zu verzeichnen, der hauptsächlich auf die Einführung des EMV-Chips in Europa und die in Zypern eingesetzten wirkungsvollen Antibetrugsmaßnahmen zurückzuführen ist.

Eine zunehmende Zahl von Betrügern kann identifiziert werden. Dies ist hauptsächlich darauf zurückzuführen, dass Betrüger fälschlicherweise davon ausgehen, Zypern sei ein technisch wenig entwickeltes Land (wenige EMV-Terminals und unzulängliche Systeme zur Kartenüberwachung) und sie könnten auf der abgelegensten Insel in Europa nicht gefasst werden. Tatsächlich ist in Zypern nur ein Acquirer tätig, sodass die Identifizierung von Betrügern sehr viel einfacher ist. Im Vereinigten Königreich oder in Griechenland sind hingegen fünf oder sechs verschiedene Acquirer tätig, unter denen kein Datenaustausch stattfindet, sodass sich das Fassen von Betrügern sehr viel schwieriger gestaltet.

Fähigkeiten der Geldautomatenbetrüger

Die auf der Insel identifizierten Betrüger zeichneten sich durch eine intelligente Vorgehensweise bei der Durchführung des Betrugs aus und zeigten große Fähigkeiten beim Umgehen der Sicherheitsvorkehrungen der Banken. Zudem zeigen sie Einfallsreichtum und scheinen gut organisiert zu sein. Darüber hinaus sind die Skimming-Methoden der Betrüger ausgereifter als die Techniken der Händler (z. B. „Jitter", „FDI").

Folgen des Geldautomatenbetrugs

Durch die Betrugsfälle wird derzeit die „Integrität der Marke" und das Vertrauen der Karteninhaber beeinträchtigt. Durch Vorkehrungen in den Kartensystemen, die auf wirksamen Gegenangriffen auf die Aktivitäten der Betrüger bei der Durchführung eines Kreditkartenbetrugs beruhen, wird dies jedoch ausgeglichen.

Italien

In Italien werden an Geldautomaten vorwiegend Debitkarten benutzt, mit denen eine umgehende Abhebung von Bargeld von einem Bankkonto möglich ist und die darüber hinaus über Zahlungs- und Abfragefunktionen, wie für das Aufladen von Telefonen, den Abruf von Daten über das persönliche Konto, Spenden, usw. verfügen. Das System BANCOMAT (wichtigstes italienische Debitkartensystem) und seine Protokolle wurden vor mehr als zwanzig Jahren konzipiert. Doch trotz ihrer Weiterentwicklung in Richtung neue Konzepte bestehen nach wie vor Sicherheitsprobleme in Zusammenhang mit ihrer Konzeption und den für die Lösungen gewählten Methoden, die heute durch modernere Varianten ersetzt werden.

Die ersten Karten dieser Art, die nach wie vor weit verbreitet sind, beruhen auf einem Magnetstreifen, auf dem verschiedene Daten gespeichert sind. Die Authentifizierung erfolgt anhand einer fünfstelligen Geheimzahl, die direkt von der Bank vergeben wird. In den letzten Jahren versuchen allerdings die Gesellschaften, die das System betreiben, diese Karten durch Karten der neuen chipbasierten Generation (Smart Cards) zu ersetzen, da diese schwerer zu kopieren sind. Im gesamten Umfeld sind Weiterentwicklungen zu verzeichnen: Alte Geldautomaten, die eigene Systeme verwenden, werden ersetzt und die neuen Geräte verfügen über modernere Funktionen, wie multimedialer Inhalt, Zahlungen mit automatischer Erkennung von Banknoten, Touchscreen, Tastatur und weitere umfangreiche Funktionen zur individuellen Anpassung der Betriebssoftware.

Alle Geldautomaten sind mit einer Videoüberwachungsanlage ausgestattet, um tätliche Angriffe wie die Verwendung von Kränen zur Entfernung der Geldautomaten von ihrer Befestigung oder von gestohlenen Fahrzeugen zum Rammen oder zur Anbringung von Sprengstoff zu verhindern. Bei ausgefeilten Angriffsmethoden wird eine falsche Frontseite mit einem „Skimmer" zum Kopieren der Karte verwendet. Zur Begrenzung des Schadens durch Diebstahl (zusätzlich zu den nach wie vor hohen Kosten für Geldautomaten) füllen italienische Banken die Geldautomaten nur mit den unbedingt erforderlichen Barbeträgen auf und statten diese mit Geräten aus, die die Banknoten dauerhaft verändern (Färbung, usw.).

Bislang waren die in Italien zu verzeichnenden Betrugsfälle auf die vorstehend erläuterten Kategorien beschränkt, es liegt noch kein dokumentierter Datenangriff auf Geldautomaten vor. Dennoch kann angenommen werden, dass sich dieser Trend kurzfristig dramatisch ändern wird.

Eines der wichtigsten Probleme in Bezug auf die Sicherheit von Geldautomaten ist mit der Zahl der Akteure in dem Bereich verbunden: Häufig ist die Kommunikation zwischen diesen Parteien unzureichend und es ist nicht einfach zu ermitteln, ob ein Fehler auf den Hardwarehersteller (Geldautomatenanbieter), den Softwarehersteller, die verwendeten Protokolle oder die Konfiguration der Infrastruktur des Geldautomaten zurückzuführen ist.

Für Angriffe verwendete Methoden

Bei der neuesten Generation von Geldautomaten handelt es sich im Wesentlichen um Industrie-PCs mit besonderen seriellen Anschlüssen oder USB-Geräte (PINPAD-Geräte, Automaten für Banknoten, individuell angepasste Tastaturen, usw.), die über IP- oder SNA-Protokolle (jetzt IP-gekapselte Pakete) mit der Bank verbunden sind. Zudem sparen die Banken durch eine Senkung der Investitionen in Standleitungen zur Datenübertragung Kosten, wodurch die Sicherheit der Geldautomatensysteme verringert wird. Es wird häufig darauf hingewiesen, dass diese Geräte direkt mit dem internen Netzwerk (LAN) der Bank oder dem Netzwerk der Filiale verbunden sind und selten vom Netzwerksegment der anderen Systeme des Unternehmens getrennt sind (von den Arbeitsstationen bis zu den Serversystemen).

Im Allgemeinen werden Geldautomaten als Industrieanlage und nicht als gewöhnliche Computer verwendet. Aus diesem Grund werden sie nach ihrer Installation auch selten aktualisiert und mangelhaft gewartet. Als Industrieanlagen müssen darüber hinaus Patches des Betriebssystems (hauptsächlich Microsoft Windows) zuerst getestet, lizenziert und vom Hersteller verteilt werden, sodass ein zusätzliches Hindernis entsteht. Dadurch werden die Geldautomatensysteme verschiedenen bekannten Gefahren ausgesetzt, wie Würmer und Viren, die die Infrastruktur schädigen können, sodass diese nicht mehr zur Verfügung steht (z. B. Crash der Geldautomaten von Diebold im Jahr 2003 aufgrund des Wurms Slammer). Sofern bestimmte Bedingungen erfüllt sind, besteht die Gefahr, dass externe oder interne Angreifer der Bank auch Angriffe auf die Systeme durchführen können, bei denen die Schwachstellen des Betriebssystems, der Software oder der Kennwortverwaltung (häufig „bekannt") genutzt werden, um auf den Geldautomaten zuzugreifen und die Software zum Abheben höherer Bargeldbeträge zu verändern.

Darüber hinaus wurden bei den analysierten Verbindungsprotokollen zahlreiche Sicherheitslücken festgestellt. Obwohl in letzter Zeit neuere und unter stärkerer Berücksichtigung von Sicherheitsaspekten erarbeitete Spezifikationen herausgegeben wurden, werden diese üblicherweise nicht vollständig umgesetzt. Beispielsweise erfolgt die Kommunikation zwischen dem Geldautomaten und dem Backend (Mainframe, usw.) häufig nicht verschlüsselt und es bestehen keine Funktionen, mit denen die Zulässigkeit der Daten gewährleistet wird. Im Rahmen von Angriffssimulationen wurde belegt, wie es möglich ist, diese Meldungen abzufangen und zu bearbeiten, sodass der Angreifer mehr Geld abheben kann, als auf dem Konto verfügbar ist, oder den Abhebungsbetrag ändern kann.

Bei unterschiedlichen Analysen wurde ein weiteres ernstes Problem ermittelt (wodurch die Ergebnisse früherer Untersuchungen noch verschärft wurden), nämlich die Platzierung der Geldautomaten: Bei mobilen Geldautomaten in ungeschützten Bereichen sind die Strom- und Netzwerkverbindungen häufig für Endbenutzer zugänglich (selbst wenn der Geldautomat in der Bank aufgestellt ist). Ein künstlicher Stromausfall führt zu einem Neustart des Systems, wodurch ein Angreifer verschiedene Informationen einsehen kann. Andererseits kann bei einem möglichen Zugriff auf die Netzwerkkabel ein System installiert werden, das den Netzverkehr abfängt und ihn über ein drahtloses Netzwerk weiterleitet.

Um die zahlreichen möglichen Sicherheitsprobleme, nicht nur in Bezug auf technische Aspekte, besser zu verstehen, ist der unterschiedliche Einsatz von Geldautomaten zu bedenken. Sie befinden sich im ganzen Land, sind häufig nicht mit den Hauptsitzen der Banken verbunden und werden direkt in den Filialen oder anderen Stellen von externen Anbietern installiert, denen die Verschlüsselungscodes bereitgestellt werden.

Die Verwaltungsverfahren für diese Systeme sind üblicherweise weniger genau als für EDV-Systeme, obwohl heute zunehmend vergleichbare Plattformen verwendet werden: Wir sprechen von Sicherheitstests nach der Implementierung, der Kennwortverwaltung, Sicherheitsüberwachung und Alarmierung, Schwachstellen und Patch-Verwaltung, Malware-Schutz, usw.

Es muss nachdrücklich darauf hingewiesen werden, dass zahlreiche dieser Angriffe nicht nur auf Debitkarten abzielen, sondern auch bei der Verwendung von Kreditkarten an Geldautomaten funktionieren können, selbst wenn eine Bewertung der spezifischen Auswirkungen noch aussteht.

Sicherheitsprobleme in Verbindung mit Geldautomaten werden häufig nicht erkannt, nahezu keine Bank hat eine formelle und vollständige Bewertung der Sicherheitsrisiken für ihre Geldautomateninfrastruktur durchgeführt. Die Verwendung des Konzepts „Sicherheit durch Geheimhaltung", das lange Zeit für die entsprechenden Geräte zugrunde gelegt wurde, ist konzeptionell falsch und wird es weiter sein, solange der weltweite Trend zu Bankbetrug zunimmt. Immer mehr Menschen befassen sich mit diesen Infrastrukturen, um Sicherheitslücken zu finden, die Zugang zu Geldautomaten und dem eigentlichen Ziel dieser neuen Formen des organisierten Verbrechens bieten: Banknoten.

Künftig wird nahezu sicher ein Anstieg der Datenangriffe auf Geldautomaten zu verzeichnen sein: Ein Ignorieren dieser Risiken in dieser schwierigen Übergangsphase wird in der Praxis zur Folge haben, dass der zweifellos wichtige Kampf, der für die nationale Sicherheit jedes Staates und das Weltwirtschaftssystem von großer Bedeutung ist, verloren wird.

Portugal

In Portugal ist eine der höchsten Verbreitungsraten von Geldautomaten pro Kopf in Europa zu verzeichnen. Dies ist größtenteils auf die modernen Funktionen zurückzuführen, die der Bevölkerung im Allgemeinen zur Verfügung stehen. Neben den traditionelleren Finanzdienstleistungen wie das Abheben von Bargeld oder die Abfrage des Kontostands zählen zu diesen die Zahlung von öffentlichen und privaten Dienstleistungen (wie Gas, Wasser, Steuern oder Mobilfunkdienstleistungen) oder die Möglichkeit zum Kauf von Konzerttickets.

Im Folgenden bieten wir eine Übersicht über das Geldautomatennetz in Portugal, die wichtigsten Risiken und Betrugsarten sowie die eingeleiteten und noch erforderlichen Maßnahmen für eine Verbesserung der Sicherheit von Geldautomaten.

Geldautomatennetz

Das Geldautomatennetz in Portugal wird von SIBS verwaltet, einer Gesellschaft, die sich im Eigentum der meisten auf dem Markt präsenten Banken befindet. SIBS ist die sechstgrößte Clearingstelle in Europa und verarbeitet mehr als 2 Mrd. Transaktionen pro Jahr über einen Wert von insgesamt etwa 6 000 000 Mio. EUR. Sie ist für die Entwicklung eines integrierten Geldautomaten- und POS-Netzwerks für alle auf dem Markt befindlichen Banken verantwortlich.

Hinsichtlich der Verwendung von Kredit- und Debitkarten liegen die portugiesischen Indikatoren über dem Durchschnitt der EU, sowohl für Karten, Geldautomaten als auch POS-Terminals pro Kopf. Darüber hinaus weist Portugal mit 60 % aller Transaktionen die höchste Nutzungsquote von Karten gegenüber anderen Zahlungsarten in Europa auf.

Sämtliche Geldautomaten sowie 83 % der POS-Terminals sind jetzt landesweit EMV-fähig (Europay, Mastercard und Visa). Auch die Finanzinstitute bemühen sich um die Bereitstellung EMV-fähiger Kredit- und Debitkarten, die 2008 44 % der landesweit eingesetzten Karten ausmachten.

Das Geldautomatennetz wird durch Standleitungen (VPN) über SSL mit zusätzlichen Sicherheitsmechanismen wie 3DES-Verschlüsselung und MAC (Message Authentication Code) unterstützt. Darüber hinaus wird bei der Entwicklung des Geldautomatennetzes ein Sicherheitskonzept berücksichtigt, nach dem keine Anlage direkt eine Verbindung mit einem Geldautomaten herstellen kann. Vielmehr nimmt der Geldautomat die Verbindung mit anderen Anlagen (einschließlich SIBS-Systeme) auf.

PayWatch

Ende 2008 wurde eine neue Gesellschaft – Paywatch – gegründet, die für die Überwachung des Geldautomatennetzes rund um die Uhr, die Identifizierung von Kartenbenutzungsmustern und die Aufdeckung von Betrugsmustern bei Geldautomaten und POS-Terminals verantwortlich ist.
Dadurch kann PayWatch Betrugsfälle mit portugiesischen Karten und/oder an Geldautomaten/im POS-Netz in Echtzeit feststellen und schnell den Schaden begrenzen. Dies ist nur aufgrund der vorstehend erläuterten Tatsache möglich, dass das Netzwerk integriert ist und insgesamt als Gegenentwurf zu einem fragmentierten Netzwerk gesehen werden kann. Vor nicht allzu langer Zeit wurden diese Überwachungstätigkeiten von der Bevölkerung im Allgemeinen als eine Art „Big Brother" gesehen und bestand wenig Verständnis für die Prüfung der Transaktionen. Vermutlich aufgrund der steigenden Zahl von Fällen, die jedes Jahr bekannt werden (nicht nur in Portugal, sondern weltweit), hat sich die Einstellung in den letzten Jahren jedoch geändert und die Bevölkerung erkennt jetzt die Vorteile des Systems und den Schutz für sich selbst und ihr Geld.

Durch die Analyse von Kryptogrammen kann PayWatch in Echtzeit feststellen, wenn eine kopierte Karte im Geldautomatennetz verwendet wird – dies ist auf portugiesische Karten und Geldautomaten begrenzt. Wenn eine Karte als EMV-Karte gilt, jedoch nur der Magnetstreifen (Fallback) verwendet wird, handelt es sich höchstwahrscheinlich um eine Kopie der Karte und der Vorgang wird abgebrochen.

PayWatch verfügt über eine Übersicht über die Nutzung von portugiesischen Kredit-/Debitkarten, und zwar sowohl im portugiesischen Geldautomatennetz als auch im Ausland. Daher können PayWatch und SIBS bestimmte Karten sperren bzw. Vorgänge in einem bestimmten Gebiet in der Welt sperren, wenn eine betrügerische Verwendung festgestellt wird - beispielsweise können Umsätze mit portugiesischen Karten in Barcelona gesperrt werden.

Wenn PayWatch eine kopierte Karte oder eine andere betrügerische Verwendung in Echtzeit feststellt, können SIBS oder die Bank den Kunden umgehend benachrichtigen und es können die geeigneten Maßnahmen eingeleitet werden, um die Risiken zu begrenzen.

Risiken und Umfang der Betrugsfälle

Generell werden in Portugal nur wenige Betrugsfälle festgestellt, ein oder zwei Fälle werden pro Jahr gemeldet. Tätliche Angriffe auf Geldautomaten stellen das größte Risiko dar, wobei 2008 ein deutlicher Anstieg zu verzeichnen war, der auf die Spezialisierung einer Gruppe aus Osteuropa auf diese Art von Angriffen zurückging.

Allerdings ist auch bei der Zahl der erfolglosen Angriffe eine deutliche Zunahme festzustellen. Dies ist darauf zurückzuführen, dass eine zunehmende Zahl von Geldautomaten jetzt über Färbungssysteme für Banknoten verfügt und am Boden befestigt ist.

Hinsichtlich der Angriffe auf Karten bildet Skimming nach wie vor die größte Gefahr. Das Kopieren der Karte erfolgt am Geldautomat oder in den Vorräumen der Banken, in denen bisweilen Geldautomaten aufgestellt sind, bei denen die Kunden eine Karte zum Öffnen der Tür durchziehen müssen. Dies entspricht 10 % bis 20 % der Fälle. Die Geheimzahl wird üblicherweise durch die

Anbringung einer Kamera oberhalb des Geldautomaten, eine gefälschte Tastatur oder „Shoulder Surfing" ausgespäht.

Sämtliche Geldautomaten verfügen landesweit über eine Art von Anti-Skimming-Mechanismus. Am häufigsten ist die Verwendung eines Lesegeräts, durch das der Einzug der Karte verlangsamt und das Lesen der Karte für ein gefälschtes Lesegerät schwieriger wird.

Aus technischer Sicht ist es möglich, eine integrierte Kamera über dem Geldautomaten anzubringen, um möglicherweise feststellen zu können, wenn eine Person ein gefälschtes Gerät an einem Geldautomaten anbringt. Nach Angaben der nationalen Kommission für den Datenschutz ist dies in Portugal aus Gründen des Schutzes der Privatsphäre jedoch nicht möglich.

Obwohl die SIBS und die Polizei sehr kooperativ und vertrauensvoll zusammenarbeiten, kann dies nicht über die Justiz gesagt werden. Personen, die wiederholt des Betrugs überführt werden, werden manchmal nur für ein bestimmtes Vergehen verurteilt und die Tatsache, dass es sich um eine Wiederholung handelt, wird nicht berücksichtigt. Des Weiteren werden nach den portugiesischen Rechtsvorschriften nur Personen verurteilt, die mit kopierten Kreditkarten gefasst werden. Dies gilt nicht für Debitkarten, was angesichts der Zahl dieser Art von Karten (Visa Electron) im Land als Problem betrachtet wird.

Angesichts der Einführung von EMV-Karten wird tendenziell ein Anstieg der Nutzung kopierter portugiesischer Karten im Ausland, und zwar in Ländern, in denen EMV noch nicht vollständig eingeführt ist, erwartet.

Für eine sicherere Umgebung

Auf der Website von SIBS finden sich Hinweise auf Sicherheitsvorkehrungen, die die Bürger bei der Nutzung von Geldautomaten oder POS-Terminals zu beachten haben, unter anderem ist darauf zu achten, die Karte nicht aus den Augen zu lassen, Vorgänge nicht zu wiederholen, sofern das Terminal nicht eine Meldung anzeigt, dass der erste Versuch erfolglos war, und die PIN-Nummer nicht an Dritte weiterzugeben. Diesbezüglich wird am Geldautomat selbst eine Meldung zum Schutz des Benutzers angezeigt, in der dieser darauf hingewiesen wird, die Eingabe der PIN so durchzuführen, dass sie nicht von Dritten ausgespäht werden kann.
Die Einführung der Färbungssysteme für Banknoten war dabei hilfreich, tätliche Angriffe auf Geldautomaten zu verhindern. Die Händler werden dafür sensibilisiert, dass es sich bei einer angefärbten Banknote um eine gestohlene Banknote handelt - bislang wurde nur ein Fall gemeldet, in dem eine angefärbte Banknote bei einem Händler vorgelegt wurde.

Angesichts der Mechanismen, mit denen die Geldautomaten ausgestattet werden, konzentrieren sich die Angreifer auf die Türen in den Vorräumen von Banken, in denen sich Geldautomaten befinden. Die Tür kann mit jeder Karte mit einem Magnetstreifen geöffnet werden, sodass der Mechanismus in Bezug auf die Kontrolle des Zugangs zu dem Vorraum nutzlos ist und ein neues Sicherheitsrisiko für Skimming entsteht. Durch einen Knopf zum Öffnen der Tür, der dieselbe Kontrolle wie heute bieten würde, könnte dieses Sicherheitsrisiko beseitigt werden. Solange die Karte für den Zugang zum Vorraum erforderlich ist, wird empfohlen, eine Karte zum Öffnen der Tür zu verwenden und die Transaktion am Geldautomaten mit einer anderen Karte vorzunehmen.

Des Weiteren wird empfohlen, sofern möglich, immer denselben Geldautomaten zu verwenden, um ungewöhnliche Veränderungen

(wie falsche Tastaturen oder Kartenlesegeräte) leichter feststellen können.

Zudem wird eine Zunahme der Betrugsversuche in der virtuellen Welt erwartet. Zur Bekämpfung dieses Problems entwickelte SIBS ein System – MBNet – das die Zuordnung eines MBNet-Konto zu einem Bankkonto ermöglicht, ein Vorgang, der in der Bank vorgenommen werden kann. Bei einer Online-Zahlung ist es dann möglich, auf die Website von MBNet zuzugreifen und eine virtuelle Visa-Kartennummer zu erstellen, die auf einen bestimmten verfügbaren Betrag begrenzt ist und nach einem Monat abläuft.

Quellen und weiterführende Literatur

„ATM scam nets Melbourne thieves $ 500,000" (*Geldautomatendiebe erbeuten 500 000 USD*), 24. März 2009, verfügbar unter *http://www.atmmarketplace.com/article.php?id=10808* (zuletzt besucht am 20. April 2009)

„ATM scam targets hundreds of credit cards" (*Geldautomatenbetrug zielt auf Hunderte von Kreditkarten*), New Europe, Ausgabe: 793, 4. August 2008, verfügbar unter *http://www.neurope.eu/articles/89221.php* (zuletzt besucht am 20. April 2009)

„ATMs on Staten Island rigged for identity theft; bandits steal $500G" (*Geldautomaten auf Staten Island manipuliert, Banditen stehlen 500 000 USD*), 11. Mai 2009, verfügbar unter http://www.nydailynews.com/news/ny_crime/2009/05/11/2009-05-11_automated_theft_bandits_steal_500g_by_rigging_atms_with_pinreading_gizmos.html#ixzz0J8qBVdar&D

„Australian police suspect Romanian gang behind $ 1 million ATM scam" (*Australische Polizei vermutet rumänische Gruppe hinter einem Geldautomatenbetrug von 1 Mio. USD*), 14. April 2009, verfügbar unter *http://www.atmmarketplace.com/article.php?id=10883* (zuletzt besucht am 20. April 2009)

http://abcnews.go.com/Technology/Business/story?id=7434509&page=1

http://cert.inteco.es

http://garwarner.blogspot.com/2009/03/bank-hacking-exposed-analyzer-affadavit.html

http://www.adicae.net/

http://www.atmsecurity.com/monthly-digest/atm-security-monthly-digest/atm-fraud-and-security-digest-march-2009.html

http://www.computerworld.com/securitytopics/security/story/0,10801,111158,00.html

http://www.denverpost.com/headlines/ci_12276447 (zuletzt besucht am 5. Mai 2009)

http://www.europol.europa.eu/index.asp?page=news&news=pr090731_2.htm

http://www.mydigitallife.info/2006/09/25/atm-hacking-and-cracking-to-steal-money-with-atm-backdoor-default-master-password/

http://www.theregister.co.uk/2006/11/18/mp3_player_atm_hack/

http://www.wired.com/threatlevel/2009/04/pins/

https://www.european-atm-security.eu/Welcome%20to%20EAST/

Marks P., „Cash machines hacked to spew out card details" (*Hackerangriff auf Geldautomaten, um Kartendaten zu erhalten*), *NewScientist Magazine*, Ausgabe Nr. 2713, verfügbar unter http://www.newscientist.com/article/mg20227135.700-cash-machines-hacked-to-spew-out-card-details.html?full=true (zuletzt besucht am 8. Juli 2009)

McGlasson L., „ATM Fraud: 7 Growing Threats to Financial Institutions"*, (Geldautomatenbetrug: sieben zunehmende Gefahren für Finanzinstitutionen) BankInfoSecurity*, verfügbar unter http://www.bankinfosecurity.com/articles.php?art_id=1523 (zuletzt besucht am 9. Juni 2009)

Peretti K. K., „Data Breaches: What The Underground World of "Carding" Reveals" (*Datenkriminalität: was die „Carding"-Kriminalität aufzeigt*), *Santa Clara Computer & High Technology Law Journal*, Volumen 25, Ausgabe 2, verfügbar unter http://www.chtlj.org/volumes/v25 (zuletzt besucht am 2. Juli 2009)

Reuters, *„Cyberthieves steal millions from banks" (Cyber-Diebe erbeuten Millionen von Banken)*, Mai 2009, verfügbar unter http://uk.reuters.com/article/idUKTRE54I6CK20090520 (zuletzt besucht am 20. Mai 2009)

Robinson G., „Bondi banks scam: ATM alert" (*Betrug der Banken in Bondi: Geldautomatenwarnung*), *The Sydney Morning Herald*, Oktober 2008, verfügbar unter http://www.smh.com.au/news/national/bondi-banks-scam-atm-alert/2008/10/09/1223145514492.html?sssdmh=dm16.338950 (zuletzt besucht am 2. Juli 2009)

„Shoppers are targeted in ATM scam" (*Gezielter Betrug von Einkaufenden an Geldautomaten*), *BBC News*, 11. März 2006, verfügbar unter *http://news.bbc.co.uk/2/hi/uk_news/england/tees/4796002.stm* (zuletzt besucht am 20. April 2009)

SIBS, „Relatório e Contas 2008", *SIBS*, 2009, verfügbar unter http://www.sibs.pt/export/sites/sibs_publico/pt/documentos/relatorioecontas/Contas_SA_2008.pdf (zuletzt besucht am 5. Mai 2009)

The Sydney Morning Herald, Oktober 2008, verfügbar unter http://www.smh.com.au/news/national/bondi-banks-scam-atm-alert/2008/10/09/1223145514492.html?sssdmh=dm16.338950

Trustwave, *Automated Teller Machine (ATM) Malware Analysis Briefing*, 28. Mai 2009, verfügbar unter https://www.trustwave.com/pressReleases.php (zuletzt besucht am 13. Juli 2009)

VISA Business News, *Data Security Alert – Compromise of ATM PIN Transactions*, 3. Juni 2009

Zetter K., „ATM Vendor Halts Researcher's Talk on Vulnerability", *WIRED*, Juni 2009, verfügbar unter http://www.wired.com/threatlevel/2009/06/atm-vendor-halts-talk/ (zuletzt besucht am 8. Juli 2009)

Geldautomatenkriminalität: Überblick über die Situation in Europa und die wichtigsten Regeln, um Straftaten zu verhindern

ISBN-13: 978-92-9204-042-0

Katalognummer: TP-80-09-736-DE-N

DOI : 10.2824/16934

TP-80-09-736-DE-N

ISBN-13 978-92-9204-042-0

PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu