



Finanzbetrug und Internet-Banking: Bedrohungen und Gegenmaßnahmen

François Paget, McAfee® Avert® Labs

Inhalt

Einige Daten für die USA	3
Statistik der US-amerikanischen Bundeshandelskommission	3
CyberSource	4
Internet Crime Complaint Center	4
Situation in Europa	5
Formen des Betrugs	6
Identitätsdiebstahl in großem und kleinem Stil	7
Karten- und Datenspionage	8
Phishing und Pharming	8
Crimeware	9
Geldwäsche	10
Kuriere	10
Virtuelle Casinos	11
Pump-and-Dump-Betrug	12
Nigeria-Vorschussbetrug (419-Scam)	13
Auktionen	14
Online-Shopping	16
Anonyme Zahlungsmethoden	17
Schutzmaßnahmen	18
Bewertung	18
EMV-Standard (Europay, MasterCard und Visa)	18
PCI DSS	19
Protokolle SSL (Secure Sockets Layer) und TLS (Transport Layer Security)	19
Erweiterte SSL-Überprüfung	20
3-D Secure	21
Starke Authentifizierung und Geräte für einmalig verwendbare Kennwörter	22
Wissensbasierte Authentifizierung	23
E-Mail-Authentifizierung	23
Fazit	24
Über McAfee, Inc.	26

Finanzbetrug hat viele Gesichter. Dazu können Täuschung oder Kreditkartenbetrug, Immobilienbetrug, Drogenhandel, Identitätsdiebstahl, betrügerisches Telefonmarketing oder Geldwäsche gehören. Das Ziel ist immer dasselbe: Die Cyber-Kriminellen wollen innerhalb kürzester Zeit und unauffällig so viel Geld wie möglich einnehmen.

In diesem Whitepaper werden verschiedene Bedrohungen für Banken und ihre Kunden vorgestellt. Dazu gehören einige Statistiken und Beschreibungen zu Lösungen, mit denen Leser einen Überblick über die aktuelle Situation erhalten – unabhängig davon, ob sie sich mit der Sicherheit in einem Finanzinstitut befassen oder ein Kunde sind.

Einige Daten für die USA

Statistik der US-amerikanischen Bundeshandelskommission

In den USA haben viele Beobachter schon seit Jahren nach Beweisen dafür gesucht, ob sich Finanzbetrug stabilisiert oder zurückgeht. Die US-amerikanische Bundeshandelskommission (Federal Trade Commission, FTC) ist für den Schutz der Kunden und die Überwachung des Wettbewerbs zuständig. Die Jahresberichte verdeutlichen, dass die Anzahl der Anzeigen von 2004 bis 2006 sank.¹ Im Jahr 2007 lagen die Zahlen jedoch ein wenig höher.² Seitdem steigen alle drei FTC-Indikatoren.

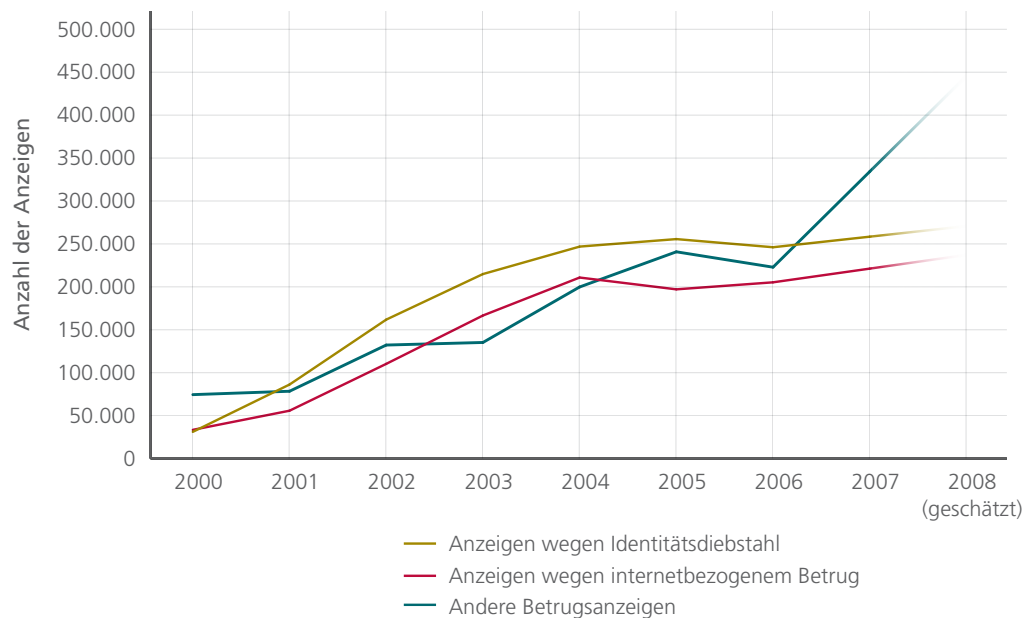


Abbildung 1: Jahresstatistik der US-amerikanischen Bundeshandelskommission für Verbraucher (Quelle: FTC)

Im Jahr 2008 wurden die internetbezogenen Betrugsanzeigen nicht mehr getrennt von der Gesamtanzahl erfasst.³ In Abbildung 2 wird die neue Aufteilung gezeigt. Im Jahr 2008 wurde nur bei 58 Prozent aller Betrugsanzeigen angegeben, wie der Erstkontakt hergestellt wurde, und bei diesen Anzeigen gaben 52 Prozent E-Mails und weitere 11 Prozent eine Internet-Webseite an. Nur 7 Prozent der Verbraucher gaben an, dass der Erstkontakt über das Telefon hergestellt wurde.

1. Daten zu Anzeigen wegen Kundenbetrug und Identitätsdiebstahl:
Jahr 2004: <http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2004.pdf>
Jahr 2005: <http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2005.pdf>
Jahr 2006: <http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2006.pdf>

2. Jahr 2007: <http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2007.pdf>

3. Daten zu Anzeigen wegen Kundenbetrug und Identitätsdiebstahl: Jahr 2008.
<http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf>

Methode der Kontaktherstellung	KJ 2006		KJ 2007		KJ 2008	
	Anzeigen	Anteil*	Anzeigen	Anteil*	Anzeigen	Anteil*
Internet – E-Mail	138.195	45 %	152.131	50 %	193.817	52 %
Post	50.317	16 %	42.330	14 %	51.837	14 %
Internet – Webseite/Sonstiges	46.687	15 %	45.447	15 %	40.596	11 %
Telefon	39.365	13 %	33.733	11 %	26.067	7 %
Sonstiges	31.722	10 %	33.481	11 %	57.695	16 %
Gesamtanzahl der gemeldeten Kontaktmethoden	306.286		307.122		370.012	

* Der Anteil basiert auf der Gesamtanzahl der CSN-Betrugsanzeigen pro Kalenderjahr, bei denen die Verbraucherangaben, über welche Methode der Erstkontakt erfolgte: KJ 2006 = 306.286, KJ 2007 = 307.122 und KJ 2008 = 370.012. 58 Prozent der Verbraucher gaben im KJ 2008 die Erstkontaktmethode an, 71 Prozent im KJ 2006 und 53 Prozent im KJ 2007.

Abbildung 2: Betrugsanzeigen beim Consumer Sentinel Network nach Kontaktmethode (Quelle: CSN)

CyberSource

Betrug als Anteil der Online-Einnahmen (in den USA und Kanada kombiniert) hat in den letzten Jahren nachgelassen. Der Wert hat sich laut CyberSource, einem Anbieter für elektronische Zahlung und Sicherheit, vor drei Jahren auf 1,4 Prozent stabilisiert.

Die Einnahmenverluste sind dennoch erheblich gestiegen. Das Wachstum der Online-Verkäufe hat im Jahr 2008 nachgelassen, und die gemeldeten Verluste werden allein für den US-Markt auf etwa 4 Mrd. US-Dollar geschätzt. Dies bedeutet eine Zunahme von 11 Prozent, nachdem der Wert im vorherigen Jahr um 20 Prozent gestiegen war.⁴

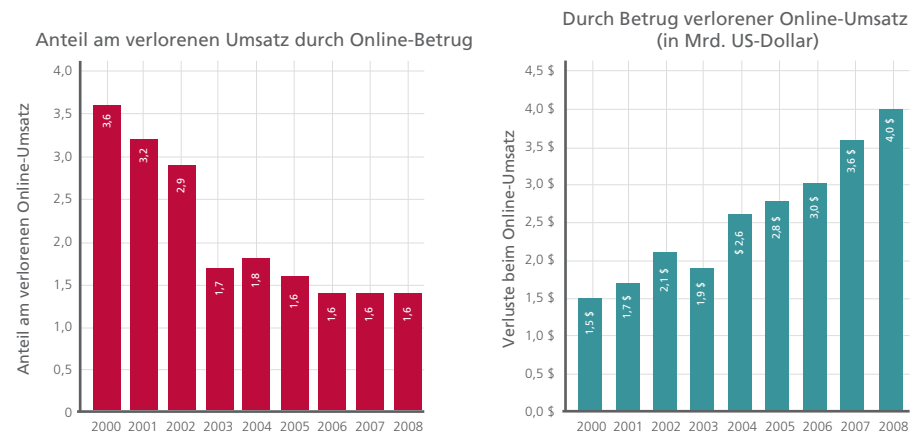


Abbildung 3: Statistik zum Zahlungsbetrug für den US-Markt. Obwohl der Anteil der Umsatzverluste durch Online-Zahlungsbetrug im Jahr 2008 nicht anstieg, ist der Gesamtverlust durch Betrug aufgrund der Zunahme der Online-Verkäufe gestiegen. (Quelle: 10. jährlicher Bericht zu Online-Betrug von CyberSource)

Internet Crime Complaint Center

Das Internet Crime Complaint Center (IC3)⁵ arbeitet mit der US-Behörde Federal Bureau of Investigation (FBI) und dem National White Collar Crime Center (eine gemeinnützige US-Organisation, die US-Strafverfolgungsbehörden darin schult, gegen Wirtschafts- und Cyber-Verbrechen vorzugehen) und erfasst ebenfalls Daten. Im Jahr 2008 wurden im Vergleich zu 2007 von US-Amerikanern 33,1 Prozent mehr Fälle zur Anzeige gebracht. Der Gesamtwert des bei Online-Betrugsfällen gestohlenen Geldes erreichte dabei einen historischen Höchstwert. Beim IC3 wurden fast 275.000 Anzeigen registriert. Der Gesamtwert der Anzeigen bedeutet einen Verlust von 265 Millionen US-Dollar, das sind 10,6 Prozent mehr als im Jahr 2007.

4. CyberSource. 10. Jahresbericht, Edition 2009, „Online Fraud Report“ (Bericht zu Online-Betrug). <http://forms.cybersource.com/forms/FraudReport2009NACYBSwww020309>

5. Internet Crime Complaint Center: „2008 Internet Crime Report“ (Bericht über Internet-Kriminalität 2008). http://www.nw3c.org/downloads/2008_IC3_Annual%20Report_3_27_09_small.pdf

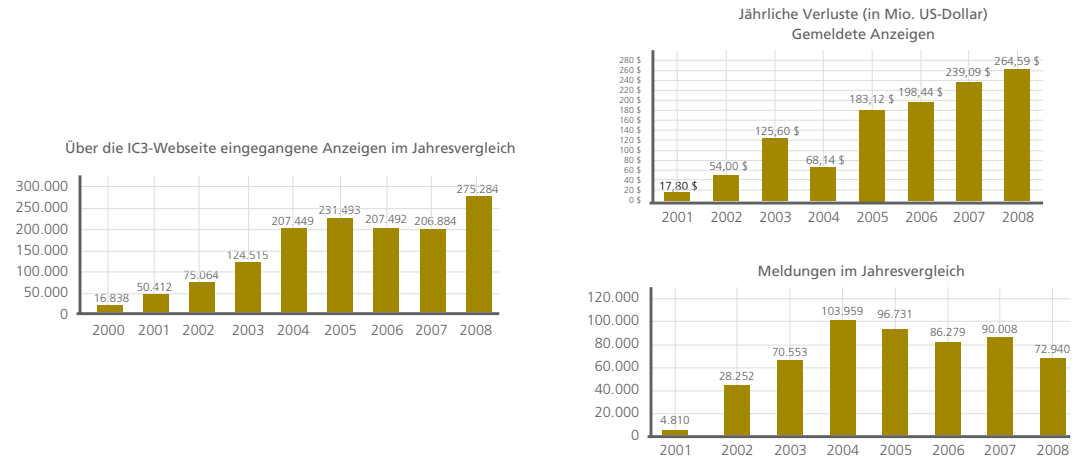


Abbildung 4: Statistik des Internet Crime Complaint Center für die USA (Quelle: Bericht des IC3 über Internet-Kriminalität 2008)

Bei der Hälfte der Fälle betrug der finanzielle Verlust weniger als 1.000 US-Dollar. Bei einem Drittel (33,7 Prozent) der eingereichten Anzeigen betrug der Verlust zwischen 1.000 und 5.000 US-Dollar. Nur bei 15 Prozent betrug der Verlust mehr als 5.000 US-Dollar.

Art des Betrugs	Anteil der gemeldeten Gesamtverluste	Durchschnittlicher Verlust pro Anzeige, bei der ein Verlust gemeldet wurde
Scheckbetrug	7,8	3.000 \$
Vertrauensbetrug	14,4	2.000 \$
Betrug über Nigeria-Scam	5,2	1.650 \$
Computerbetrug	3,8	1.000 \$
Nichtlieferung (Waren und Zahlung)	28,6	800 \$
Auktionsbetrug	16,3	610 \$
Kreditkartenbetrug	4,7	223 \$

Abbildung 5: Verluste durch Betrug, nach Art des Betrugs, für US-Einwohner, die einen Verlust gemeldet haben (Quelle: Bericht des IC3 über Internet-Kriminalität 2008)

Die meisten Anzeigen bezogen sich auf Auktionsbetrug und Nichtlieferung bezahlter Waren. Andere Anzeigen bezogen sich auf Kreditkartenbetrug oder Vorkassebetrug (Scam). Die Betrüger nutzten hauptsächlich E-Mails und Webseiten für die Kontaktaufnahme mit den Opfern. In vielen Fällen bezog sich der Betrug auf den Kauf oder Verkauf von Haustieren.

Die Mehrzahl der Anzeigen wurde von Männern erstattet. Fast die Hälfte der Männer sind 30 bis 50 Jahre alt, und ein Drittel von ihnen leben in den US-Bundesstaaten mit den meisten Einwohnern: Kalifornien, Florida, Texas und New York.

Situation in Europa

Die Statistik der britischen Organisation für Fragen des Zahlungsverkehrs (Association for Payment Clearing Services, APACS) zeigt im gleichen Zeitraum (2004 bis 2007) einen Rückgang der Fälle von Online-Banking-Betrug und entspricht damit den Statistiken für Nordamerika. In Großbritannien setzte sich der starke Anstieg von 2006 im darauf folgenden Jahr nicht fort, stattdessen lagen die Zahlen von 2007 sogar noch niedriger als die von 2005. Dies ist leider kein Grund für Optimismus, da die Daten für die erste Hälfte des Jahres 2008 einen 185-prozentigen Anstieg im Vergleich zum Vorjahr zeigen.⁶

6. APACS: „APACS announces latest fraud figures“ (APACS gibt neuste Betrugszahlen bekannt). <http://www.apacs.org.uk/APACSannounceslatestfraudfigures.htm>

	Januar – Juni 2004	Januar – Juni 2005	Januar – Juni 2006	Januar – Juni 2007	Januar – Juni 2008	Zunahme 2007 – 2008
Verluste durch Online-Banking- Betrug (in Mio.)	4 £	14,5 £	22,4 £	7,5 £	21,4 £	185 %
Phishing- Zwischenfälle	126	312	5.087	7.224	20.682	186 %
Angebote als „Kurier“	–	196	468	655	873	33 %

Abbildung 6: Online-Banking-Betrug, Phishing und Angebote für Geldwäsche-„Kuriere“ in Großbritannien (Quelle: APACS, die britische Organisation für Fragen des Zahlungsverkehrs)

In Frankreich gilt den Risiken durch Remote-Online-Zahlungen eine besondere Sorge. Laut dem Bericht des Observatoire de la sécurité des cartes de paiement⁷ (einem französischen Forum, das sich mit Zahlkartensystemen befasst) von 2007 sind diese Transaktionen für 44 Prozent aller Betrugsfälle verantwortlich (im Vergleich zu 32 Prozent im Jahr 2006), obwohl sie nur fünf Prozent der „papierlosen“ Transaktionen (z. B. Überweisungen, Lastschriften und Kartenzahlungen) ausmachen.

Die Verluste durch Cyber-Betrug bei Inlandstransaktionen stiegen in Frankreich um 97 Prozent auf 26,4 Mio. EUR.

Bei internationalen Transaktionen stellt das Forum nur Daten zu solchen Transaktionen zur Verfügung, die mit französischen Karten im Ausland getätigt wurden. Auch hier ist der Anteil der Betrugsfälle mit Remote-Zahlungen bei Internet-Zahlungen höher als bei anderen Arten von Remote-Transaktionen.

		Betrugssumme (in Mio. EUR)	
Remote-Zahlungsbetrug		2006	2007
Inlandstransaktionen	Per Post oder Telefon	19,8 €	23,8 €
	Online	13,4 €	26,4 €
Französischer Zahler, Empfänger im Ausland	Per Post oder Telefon	5,7 €	7,6 €
	Online	20,3 €	27,4 €

Abbildung 7: Betrugsverteilung nach Art der Transaktion in Frankreich (Quelle: Observatoire de la sécurité des cartes de paiement)

Die französische Überwachungsorganisation O.C.L.C.T.I.C. (Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication) gibt an, dass 80 Prozent der im Jahr 2007 erhaltenen Anrufe mit Internet-Scam zusammenhängen.

Formen des Betrugs

Der PC ist ein begehrtes Ziel für Cyber-Kriminelle, da er häufig nicht gut geschützt ist. Benutzer lassen sich oft durch Lockangebote oder Warnungen verführen, die sie dem Anschein nach von ihrer Bank erhalten.

Hinter diesen Angriffen verbergen sich Phishing-Webseiten oder Webseiten, auf denen Malware gehostet ist. Laut der Anti-Phishing Working Group (Anti-Phishing-Arbeitsgruppe) führen die USA, Russland, China, Kanada, Frankreich und die Republik Korea die Liste der Länder an, in denen Malware gehostet wird.⁸ Sicherheitsfirmen wie RSA setzen zudem häufig Deutschland und neuerdings auch Luxemburg auf diese Liste.⁹

7. Observatoire de la sécurité des cartes de paiement: „Rapport annuel 2007“ (Jahresbericht 2007)
http://www.banque-france.fr/observatoire/telecharlr/ap_an_2007.pdf

8. APWG: „Phishing Activity Trends Report, Q1/2008“ (Bericht zu den Trends bei Phishing-Aktivitäten, 1. Quartal 2008).
http://www.antiphishing.org/reports/apwg_report_Q1_2008.pdf

9. RSA: „RSA Online Fraud Report“ (RSA-Bericht zu Online-Betrug), Juli 2008.
http://www.rsa.com/solutions/consumer_authentication/intelreport/FRARPT_DS_0708.pdf

Wenn es um die Intelligenz der Angriffe geht, werden häufig die früheren Blockstaaten der Sowjetunion hervorgehoben. Es existieren sogar Gerüchte, die besagen, dass die führenden Mitglieder des mächtigen russischen Internetdiensteanbieters Russian Business Network (RBN) enge Verbindungen zur Regierung haben.¹⁰ Bis November 2007 machte es der „kugelsichere“ Hostingservice von RBN zahlreichen seiner Verbündeten möglich, alle Arten von illegalen Aktivitäten durchzuführen. Für etwa 600 US-Dollar pro Client und Monat gab die Organisation vor, an sie gerichtete Beschwerden zu bearbeiten. Tatsächlich aber ermöglichte sie ihren Schutzbefohlenen die Weiterarbeit an ihren kriminellen Machenschaften. Das Geschäft war mit einer Million Webseiten, mehreren Millionen verfügbaren IP-Adressen und vier Millionen Besuchern pro Monat einträglich.¹¹ Diverse in Frankreich und in den USA durchgeführte Ermittlungen haben diesem Geschäft ein Ende gesetzt. Mit dem Verschwinden von RBN konzentrierte sich der Verdacht rasch auf den türkischen Internetdiensteanbieter Abdallah Internet Hizmetleri (AIH)^{12,13} und die beiden US-amerikanischen Anbieter Atrivo und EstDomains.^{14,15}

Heutzutage fragen sich die Experten, ob sie es mit einer sukzessiven Abwanderung von RBN-Kunden zu anderen Datenoasen zu tun haben oder ob die russische Organisation in aller Ruhe Untergrundnetzwerke von Allianzen und Mafia-ähnlichen Strukturen aufgebaut hat, um einen Großteil derjenigen, die in den Online-Finanzbetrug verwickelt waren, weiter zu unterstützen.

Identitätsdiebstahl in großem und kleinem Stil

Die Identität einer Person bildet die Grundlage für ihre Rechtspersönlichkeit. Im tatsächlichen Leben definiert sich diese Identität durch den Personenstand, diese wird zudem durch das Gesetz geschützt. In der virtuellen Welt reicht die Identität einer Person viel weiter und ist weniger klar umrissen. Einige digitale Daten, die die Identität einer Person betreffen (z. B. Kontodaten, Benutzernamen und Kennwörter) ermöglichen den Zugang zu privaten Daten. All diese digitalen Identifizierungsmerkmale, die nicht als Elemente der Rechtspersönlichkeit einer Person betrachtet werden, werden immer begehrt.

Die Client-Workstation ist das Hauptziel von Cyber-Kriminellen. Viele Fälle von verlorenen Datensicherungen oder Entdeckungen von kompromittierten Geschäfts- oder Banknetzwerken zeigen jedoch, dass Identitätsdiebstahl auch in großem Stil betrieben wird.¹⁶

Betroffene Daten	Dauer	Meldedatum	Organisationen	Herkunft
94.000.000	Juli 2005 – Dezember 2006	17. Januar 07	TJX-Unternehmen	Mängel im Drahtlosnetzwerk ermöglichten den Datendiebstahl
40.000.000	September 2004 – Mai 2005	19. Juni 2005	CardSystems, Visa, MasterCard, American Express	Böswilliger Code, der über eine Webanwendung eingebracht wurde
30.000.000	April 2003 – April 2004	24. Juni 2004	America Online	Daten wurden von Mitarbeitern gestohlen und an Spammer verkauft
26.500.000	3. Mai 2006	22. Mai 2006	Kriegsveteranenministerium der USA	Persönliche Daten auf einem Laptop, die bei einem Einbruch gestohlen wurden
25.000.000	Oktober 2007	20. November 2007	HM Revenue and Customs (Großbritannien), TNT	Verlust von zwei CDs
17.000.000	2006 – 2008	6. Oktober 2008	T-Mobile, Deutsche Telekom	Daten gestohlen und online zum Verkauf angeboten
12.500.000	27. Februar 2008	7. Mai 2008	Archive Systems, Bank of New York Mellon	Verlust von unverschlüsselten Bandlaufwerken
11.000.000	Juli – August 2008	6. September 2008	GS Caltex	Mitarbeiter erstellten Kopien von persönlichen Daten zum Zwecke des Verkaufs
8.637.405	Mai 2001 – März 2006	12. März 2007	Dai Nippon Printing Company	Daten wurden von einem früheren Vertragsarbeiter gestohlen und an eine kriminelle Vereinigung verkauft
8.500.000	2002 – Juni 2007	3. Juli 2007	Certegy Check Services, Fidelity National Information Services	Daten wurden von einem Mitarbeiter gestohlen und für Werbezwecke an einen Dritten verkauft

Abbildung 8: Vorfälle mit den größten Datenverlusten (Quelle: McAfee Avert Labs)

10. VeriSign iDefense: „Global Threat Research Report: Russia“ (Forschungsbericht zu globalen Bedrohungen: Russland), Seite 23. <http://www.verisign.com/istatic/042139.pdf>

11. VeriSign: „Uncovering Online Fraud Rings: The Russian Business Network“ (Aufdecken von Online-Betrugsringen: Das russische Geschäftsnetzwerk) (Webcast-Aufzeichnung). <http://www.verisign.com/>

12. David Bizeul: „Russian Business Network study“ (Studie zum russischen Geschäftsnetzwerk). http://bizeul.org/files/RBN_study.pdf

13. The Shadowserver Foundation: „RBN ‘Rizing’: Abdallah Internet Hizmetleri (AIH)“ (RBN kommt wieder: AIH). http://digitalninjitsu.com/downloads/RBN_Rizing.pdf

14. Armin, Jart, u. a.: „Atrivo – Cyber Crime USA“ (Atrivo – Cyber-Kriminalität in den USA). <http://hostexploit.com/downloads/Atrivo%20white%20paper%20090308ad.pdf>

15. Washington Post: „EstDomains: A Sordid History and a Storied CEO“ (EstDomains: Eine schäbige Geschichte und ein dubioser CEO) http://voices.washingtonpost.com/securityfix/2008/09/estdomains_a_sordid_history_an.html

16. Open Security Foundation: „DataLossDB“. <http://datalossdb.org/>

Auch wenn die Anzahl der Vorfälle mit mehreren Millionen oder mehr betroffenen Daten weiter ansteigt, bleibt der Fall von TJX in den Köpfen der Menschen doch der herausragende. Seit März 2007 wurden mehrere Wiederverkäufer und Benutzer dieser Daten festgenommen und im Zusammenhang mit diesem Fall verurteilt.¹⁷ Einer von ihnen, bekannt unter dem Namen „Lord Kaisersose“, wurde im Juni 2007 in Frankreich verhaftet.¹⁸

Karten- und Datenspionage

Kriminelle suchen häufig Kartenwebseiten auf, die sie problemlos im Internet finden. Dort kaufen oder verkaufen sie Bankkontozugänge, gestohlene Kartennummern, Kopien von Magnetstreifen und komplette Personenprofile.

Am 2. Mai 2008 haben wir mehrere Bankkonten gefunden, die zum Verkauf angeboten wurden. Das teuerste war auch das kapitalkräftigste: Ein Konto bei der europäischen Bank BNP Paribas mit einem Kontostand von 30.792 EUR, das online gerade mal für 2.200 EUR zum Verkauf angeboten wurde. Zusätzlich zu diesem Spottpreis bot der Verkäufer eine 24-Stundengarantie: Wenn der Käufer sich nicht innerhalb dieses Zeitraums anmelden könne oder das Geld nicht mehr auf dem Konto vorhanden sei, würde ein Ersatzkonto gestellt.

Name der Bank	Land	Kontostand	Preis
Bank of America	USA	...	Verkauft
Asmouth Bank	USA	16.040 \$	700 €
Washington Mutual Bank	USA	14.400 \$	600 €
Washington Mutual Bank	USA	7.950 \$ + 2.612 £	500 €
Washington Mutual Bank	USA	...	Verkauft
MBNA America Bank	USA	22.003 \$	1.500 €
Banco Bradesco S.A.	Brasilien	13.451 \$	650 €
Citibank	Großbritannien	10.044 £	850 €
NatWest	Großbritannien	12.000 £	1.000 €
BNP Paribas	Frankreich	30.792 €	2.200 €
Caja de Ahorros de Galicia	Spanien	23.200 €	1.200 €
Caja de Ahorros de Galicia	Spanien	7.846 €	500 €
Banc Sabadell	Spanien	25.663 €	1.450 €

Abbildung 9: Zum Verkauf stehende Daten über Bankkonten (von einer Webseite mit gestohlenen Kreditkartendaten)

Phishing und Pharming

Phishing ist eine bekannte Technik zum Abgreifen vertraulicher Daten eines Benutzers durch Vortäuschen einer vertrauenswürdigen Identität. In den meisten Fällen leitet der Angreifer sein Opfer mithilfe einer Täuschungs-E-Mail an eine Mirror-Webseite um.

Mithilfe eines Trojaners ist es außerdem möglich, die Verbindung zwischen der IP-Adresse und dem zugehörigen Servernamen zu infiltrieren. Dieser Vorgang wird als Pharming bezeichnet.

In beiden Fällen glauben die Opfer, dass sie seriöse Webseiten aufsuchen. Viele Benutzer sind sich nicht darüber im Klaren, dass 80 Prozent aller Bank-E-Mails betrügerisch sind,¹⁹ und geben ohne zu zögern persönliche Informationen preis. Laut der Monatsstatistik des Anti-Phishing-Projekts PhishTank ist PayPal das beliebteste Ziel.²⁰ Die Ergebnisse zeigen, dass PayPal mit großem Abstand an erster Stelle steht, andere beliebte Unternehmen haben jeden Monat leicht wechselnde Positionen. eBay, das 2007 dicht hinter PayPal lag, findet sich häufig auf dem zweiten Platz.

17. US-Justizministerium: „Retail Hacking Ring Charged for Stealing and Distributing Credit and Debit Card Numbers from Major U.S. Retailers“ (Einzelhandel-Hacker-Ring wegen Diebstahl und Verbreitung von Kreditkartennummern großer US-Händler angeklagt). <http://www.usdoj.gov/criminal/cybercrime/gonzalezIndict.pdf>

18. US-Bezirksgericht Columbia: „Affidavit in Support of Complaint for Forfeiture“ (Eidesstattliche Erklärung zur Unterstützung einer Anzeige wegen Einziehung). <http://docs.justia.com/cases/federal/district-courts/district-of-columbia/dcdce/1:2007cv01346/126695/1/1.pdf>

19. „Leading Companies & Non-Profits Realize the Benefits of Brand and Consumer Protection Through Email Authentication“ (Führende Unternehmen und gemeinnützige Organisationen erkennen Vorteile von Marken- und Kundenschutz durch E-Mail-Authentifizierung). <http://www.reuters.com/article/pressRelease/idUS191046+31-Jan-2008+MW20080131>

20. Statistiken, April 2009. <http://www.phishtank.com/stats/2009/04/>

Ziele	Erfolgreiche Phishing-Angriffe im Jahr 2009			
	Januar	Februar	März	April
PayPal	9.575	6.245	9.605	7.575
Internal Revenue Service	469	326	96	426
eBay	720	292	459	356
Google	336	203	169	330
Bank of America Corp.	231	204	429	290
HSBC Group	272	97	265	228

Abbildung 10: Beliebteste Ziele beim Phishing (Quelle: PhishTank)

Auch wenn die Zahlen voneinander abweichen, so handelt es sich gemäß den zuständigen Stellen bei den angegriffenen Unternehmen hauptsächlich um amerikanische und britische Banken. Laut RSA richten sich 72 Prozent der Angriffe gegen amerikanische Banken, während die Anti-Phishing Working Group (eine amerikanische Organisation, die sich die Eliminierung von betrügerischen Handlungen im Internet zur Aufgabe gemacht hat) berichtet, dass die Hälfte davon auf europäische Organisationen gerichtet ist. Gartner schätzt, dass der Durchschnittsverlust pro Opfer in den USA bei 886 US-Dollar liegt.²¹

Crimeware

Unter Kriminellen sind – neben Phishing – Trojaner ein beliebtes Mittel der Wahl. Diese Form der Crimeware umfasst Kennwortdiebstahlprogramme und Keylogger, die Tastatureingaben protokollieren, Screenshots aufzeichnen und alle Daten an Sammlungswebseiten schicken. Die Menge der Crimeware nimmt zu, und sie ist wirkungsvoller denn je. Crimeware ist häufig mit Rootkits verknüpft. Das sind Diebstahlprogramme, die die Crimeware für viele Sicherheitstools unkenntlich oder komplett unsichtbar machen.

Crimeware wird jetzt außerdem häufiger in gezielten Angriffen eingesetzt. Sie kann unbemerkt durch die Erkennung rutschen, wenn die Tools sie nicht mit Standardmethoden oder über eine Verhaltensanalyse identifizieren können.

Crimeware konzentriert sich häufig auf virtuelle Welten und Online-Spiele: Etwa 30 oder 40 Prozent der Hunderttausenden von Kennwortdieben, die von McAfee VirusScan® erkannt werden, haben es auf diese Ziele abgesehen. Crimeware wird häufig mithilfe von Standardmethoden erkannt, bei einigen großen Familien ist die Klassifikation jedoch detaillierter.

- *PWS-Banker* – Bankverbindungen
- *PWS-MMORPG* – Diverse Online-Spiele mit mehreren Spielern
- *PWS-LDPinch* – Sammelt Daten zum Hostsystem, sucht nach auf der Festplatte gespeicherten Kennwörtern (ICQ, TheBat, DFÜ-Verbindung)
- *PWS-Legmir* – „Legend of Mir“-Spiele
- *Keylog-Ardamax* – Erfasst Tastatureingaben
- *PWS-Lineage* – „Lineage“-Spiele
- *PWS-Online-Spiele* – Diverse Online-Spiele mit mehreren Spielern

21. 257 US-Dollar im Jahr 2005 und 1.244 US-Dollar im Jahr 2006. Laut der Gartner-Umfrage verloren US-amerikanische Internet-Benutzer im Jahr 2007 durch Phishing 3,2 Mrd. US-Dollar (2,2 Mrd. EUR), 64 Prozent der Opfer erhielten Entschädigungen.
<http://www.gartner.com/it/page.jsp?id=565125>

Dies sind die derzeit wichtigsten Programme zum Diebstahl von Kennwörtern. Im unten stehenden Diagramm wird ihre Häufigkeit in den letzten beiden Jahren gezeigt.

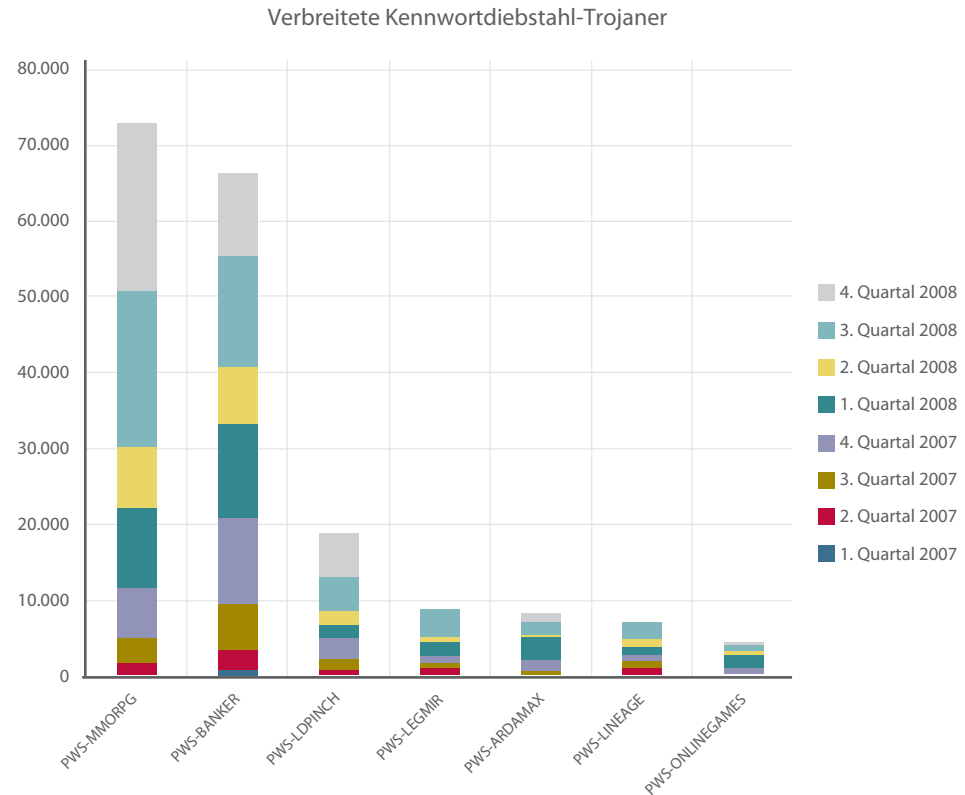


Abbildung 11: Varianten von Kennwortdiebstahl-Malware (Quelle: McAfee Avert Labs)

Geldwäsche

Für nahezu jede kriminelle Aktivität muss Geld gewaschen werden. Zusätzlich zu zahlreichen herkömmlichen Methoden (einschließlich elektronischem Zahlungsverkehr, fiktiven Unternehmen mit ausländischen Banken, Bargeldschmuggel, Bankbetrug und informelle Geldwechsler) haben sich andere moderne Verfahren, wie „Kuriere“ und virtuelle Casinos, im Internet entwickelt.

Kuriere

Diese Methode wurde nach den Schmugglern benannt, die illegale Waren transportieren. Heute beschreibt der Begriff Personen, die über das Internet rekrutiert werden und als Zwischenhändler für die Wiederbeschaffung von Bargeld für Mittel fungieren, die illegal über Phishing, Keylogging und andere betrügerische Handlungen erlangt wurden. Für jede Transaktion zieht der Kurier zwischen fünf und zehn Prozent des vorhandenen Betrags ab und leitet den Differenzbetrag über einen anonymen Geldtransferdienst wie WebMoney, e-gold oder Western Union weiter.

Häufig stellt man sich unter Kurieren leichtgläubige Personen vor, die durch ein professionell aussehendes Angebot (über Spam oder bestimmte Webseiten) ausgetrickst werden. Tatsächlich sind Kuriere in den seltensten Fällen unschuldige Opfer. Viele Menschen, die sich oft über das Gesetz hinwegsetzen und das schnelle Geld suchen, bieten sich hier gerne als Freiwillige an. Heutzutage wird die Tätigkeit des Kuriers immer mehr zur Profession. Dies zeigen auch jüngste Verhaftungen in Frankreich und anderen Ländern. Vier Kuriere wurden im Zusammenhang mit einem Fall im Mai 2008 offiziell verhört und unter gerichtlich verfügte Beobachtung gestellt.²² Sie befanden sich im Zentrum von betrügerischen Machenschaften, die PayPal und

eBay als Ziele hatten, und sie wurden wegen „organisiertem Betrug“ und „organisierter Verschleierung von Betrug“ angeklagt. Ein Komplize, ein 17-jähriger Hacker, soll sich derzeit Tunesien aufhalten. Zusammen sollen die Kuriere 19 französische Internetbenutzer um insgesamt etwa 20.000 EUR betrogen haben. Untersuchungen zeigen, dass es mindestens 10.000 weitere mögliche Opfer gibt.

Um zu erfahren, wie diese Angebote funktionieren, habe ich im September 2007 auf eine Anzeige im Internet für einen Telearbeitsplatz geantwortet. Ich erhielt eine Zusammenfassung der häufigsten Fragen zu diesem Geschäft.

Häufige Fragen und Antworten zur Telearbeit:

Frage 1: Was ist meine Aufgabe?

Antwort: Zu Ihren Aufgaben gehören die Kontrolle des Geldflusses und die Ausführung eines Teils der Transaktionen. Zu einem für Sie günstigen Zeitpunkt erhalten Sie Zahlungen von unseren großen Kunden auf Ihr Bankkonto. Anschließend überweisen Sie das Geld an uns. Die Provision für jede Transaktion beträgt 7 Prozent. Sie müssen KEINE eigenen Investitionen tätigen.

Frage 2: Warum bezahlen Ihre Kunden nicht direkt an Sie?

Antwort: Die Kunden überweisen das Geld nicht direkt an uns, da wir in Europa außerhalb von Großbritannien keine Niederlassungen haben. Wir senken also die Produktionskosten, und Sie verdienen 7 Prozent. Auf diese Weise ist das Geschäft für beide Seiten profitabel.

Frage 3: Nennen Sie mir bitte ein Beispiel für den Arbeitsablauf.

Antwort: 1. Der Kunde/Die Kundin überweist das Geld von seinem/ihrer Bankkonto und informiert uns.*

2. Wir informieren Sie per Telefon und E-Mail darüber, dass das Geld überwiesen wurde. Anschließend erhalten Sie eine E-Mail (Beispiel): „Das Geld wurde auf Ihr Bankkonto überwiesen. Die Summe beträgt 5.000 EUR, der Name unseres Kunden lautet Peter Tischler, und er kommt aus Berlin, Deutschland. Überprüfen Sie bitte morgen Ihren Kontostand, heben Sie das Geld ab, und senden Sie es über Western Union oder MoneyGram an Kate Lewis, London, Großbritannien.“

3. Gehen Sie zu Ihrer Bank, und heben Sie das Geld ab.

4. Behalten Sie 7 Prozent vom Betrag, und gehen Sie mit dem verbleibenden Geld zu Western Union oder MoneyGram, und überweisen Sie es an Kate Lewis, London, Großbritannien.

5. Sie senden uns die Daten zur Überweisung über Western Union oder MoneyGram und eine eingescannte Kopie der Überweisungsbestätigung per E-Mail.

* Unser Manager ruft Sie vor der Banküberweisung an. Wenn Sie den Betrag nicht empfangen können, wird die Überweisung zu einem anderen Zeitpunkt getätigt. Auf diese Weise können Sie die Arbeit mit Ihrem eigenen Tagesablauf kombinieren.

Abbildung 12: Die häufigsten Fragen auf einer Webseite zur Rekrutierung von Kurieren

Nach einem Erstkontakt über E-Mail erhielt ich einen Arbeitsvertrag. Angesichts der augenscheinlichen Professionalität meiner Kontaktperson und der Qualität der Dokumente, die ich zu Gesicht bekam, konnte ein nicht informierter Bewerber ohne weiteres auf diese Masche hereinfallen. Computersicherheitsfirmen, Banken und die Polizei reden immer häufiger über diese Bedrohungen, doch einige meiner jüngsten Kontakte mit der Öffentlichkeit zeigen, dass immer noch hoher Aufklärungsbedarf besteht.

Virtuelle Casinos

Im Jahr 2006 gab es etwa 15.000 aktive Webseiten für Online-Glücksspiel.²³ Es ist unwahrscheinlich, dass diese Zahl seither nach unten gegangen ist. Da derzeit nur 1.766 Webseiten für Online-Glücksspiel mit einer Lizenz betrieben werden,²⁴ stellen heimliche Aktivitäten (Webseiten, die ohne Lizenz operieren) mehr als 87 Prozent des verfügbaren Gesamtangebots im Internet dar.

Durch das Fehlen einer Gesetzesstruktur kann sich jede beliebige Person für eine Internetseite registrieren lassen und die Kunden über ein anonymes Offshore-Bankkonto oder ein virtuelles Geldsystem belasten. Die meisten Gruppen der russischen Cyber-Kriminellen, die heute aktiv sind (einschließlich Ex-Mitarbeiter von RBN und Yambo Financial), haben ihre kriminelle Karriere über Kinderpornografie und Online-Casinos begonnen.

23. CERT-LEXSI: „Cybercriminalité des Jeux en Ligne“ (Cyber-Kriminalität bei Online-Glücksspielen), Juli 2006.
http://www.lexsi.com/telecharger/gambling_cybercrime_2006.pdf

24. Casino City: „Online Gaming Jurisdictions“ (Rechtssprechung bei Online-Glücksspielen).
<http://online.casinocity.com/jurisdictions/index.cfm?sorttab=n/a&sortlist=sites&filterlist=&numero=25&searchall=1>

Pump-and-Dump-Betrug

Social-Engineering-Tricks wie die Verbreitung falscher Nachrichten in Internetforen werden bereits seit langem verwendet, um den Aktienmarkt zu manipulieren. Im Jahr 2006 gab es einen Anstieg bei einer beliebten Abwandlung dieser Technik: Pump-and-Dump-Aktien, bei denen Niedrigkursaktien (Billigaktien) von normalerweise unattraktiven Unternehmen manipuliert werden.

Nach dem Kauf einer großen Menge der Aktien zum niedrigen Kurs verwendet der manipulierende Käufer Spam-Techniken, um positive Nachrichten zu versenden und den Aktienpreis künstlich in die Höhe zu treiben. Ein oder zwei Tage später, nach einem Kursanstieg, verkauft der Spammer zu dem künstlich in die Höhe getriebenen Kurs und nimmt den Gewinn mit.

Eine an der Purdue University in Indiana (USA) und an der Oxford University in Großbritannien durchgeführte Studie zeigt einen signifikanten Anstieg sowohl im Kurs als auch im Umfang von Aktien, die als Spam-Aktien gehandelt werden, vom Tag vor dem Werbungsbeginn bis zum Tag nach den heftigsten Spam-Aktivitäten.²⁵ Laura Frieder, Coautorin dieser Studie, erläutert, wer neben den Spammern selbst an diesem Handel beteiligt war. „Zuerst gibt es die naiven Anleger, die gierig und möglicherweise nicht besonders intelligent sind, ähnlich den Menschen, die hohe Summen nach Nigeria schicken oder Kettenbriefe weiterleiten“, so Frieder. „Wenn sie auch nur die kleinste Möglichkeit sehen, dass sie hiermit Geld verdienen können, meinen sie, es sei einen Versuch wert.“²⁶

Es gibt Menschen, die wissen, dass diese Informationen wertlos sind, aber sie denken, dass es hier die Möglichkeit zum Geldverdienen gibt, weil andere Menschen dies eben nicht wissen. „Wenn ich denke, dass andere Menschen kaufen und den Kurs nach oben treiben werden, werde ich möglicherweise auch kaufen, wenn ich denke, dass ich frühzeitig genug ins Geschäft einsteige, ein paar Gewinne mitnehme und dann aussteige“, sagte sie.

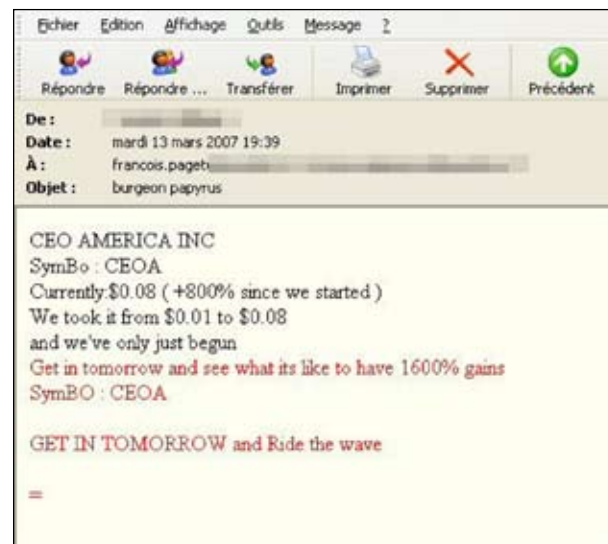


Abbildung 13: Pump-and-Dump-E-Mails

Das allgemeine Misstrauen von Kleinaktionären, die dürftigen Gewinnmitnahmen und die Tatsache, dass sich gelegentlich unerwünschte Personen an der Aktienmanipulation versucht haben, mögen dazu geführt haben, dass die Wirksamkeit dieser Betrugsform und das Interesse daran nachgelassen haben. Da Pump-and-Dump-Betrug nicht die Erwartungen seiner Erfinder erfüllt hat, tritt er seltener auf.

25. Laura Frieder und Jonathan Zittrain: „Spam Works: Evidence from Stock Touts and Corresponding Market Activity“ (Spam: Beweise für Verbindung zwischen Aktien-Spam und entsprechender Marktaktivität).

<http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Spam%20Works.pdf>

26. CBC: „Stock Spam: The New Boiler Room“ (Aktien-Spam: Das neue Pulverfass).

<http://www.cbc.ca/news/background/personalfinance/stock-spam.html>

Nigeria-Vorschussbetrug (419-Scam)

Der 419-Scam ist extrem beliebt und lukrativ und nach dem Abschnitt des nigerianischen Gesetzes benannt, das diesen Betrug abdeckt. Der Hoax wird häufig in Form einer E-Mail von einem Familienmitglied eines (normalerweise afrikanischen) Würdenträgers verbreitet. Der Absender erklärt, dass nach dem Tod eines einflussreichen Mitglieds seiner Familie irgendwo auf einem Bankkonto eine große Menge Geld blockiert ist. Der Absender behauptet, dass es mit der Hilfe des Empfängers und aufgrund der finanziellen Sicherheiten des Opfers für den Geldtransfer möglich sei, das Geld auszulösen. Demjenigen, der sich darauf einlässt, winkt eine beträchtliche Vergütung.

Sobald der Kontakt hergestellt ist, verlangen die Gauner einen Vorschuss. Das kann die Eröffnung eines Bankkontos oder die Bezahlung von Gebühren umfassen. Daraufhin folgen eine Reihe von Ausgaben und Problemen, die manchmal auch zu tatsächlichen Bedrohungen führen. Und selbstverständlich existiert das blockierte Geld tatsächlich gar nicht.

In Frankreich führen Fehler in der Grammatik oder Rechtschreibung in den E-Mails anscheinend sogar dazu, das Vertrauen bei arglosen Menschen zu erhöhen, statt sie misstrauisch zu machen. Dasselbe gilt für das äußerst professionelle Aussehen der offiziellen Dokumente, die dann folgen.


 BANQUE ATLANTIQUE COTE D'IVOIRE LA BANQUE DE L'AFRIQUE DE L'OUEST SIEGE / AGENCE AVENUE DU GENERAL DEGAULLE 04 BP 1036 ABIDJAN 04 - COTE D'IVOIRE							
N° : BACI 882013							
RECU OFFICIEL DE DEPOT DE FONDS							
RECEIVED FROM RECU DE	MR. KONAN JOSEPH						
DENOMINATION	<input type="checkbox"/> US\$ 100 <input checked="" type="checkbox"/> US\$ 100 5.300.000 US\$ <input type="checkbox"/> US\$ 50 <input type="checkbox"/> US\$ 20 <input type="checkbox"/> US\$ 10 <input type="checkbox"/> US\$ 10						
CURRENCY DEVISE	<table border="1"> <tr> <td>CFA</td> <td>€</td> <td>\$</td> </tr> <tr> <td></td> <td></td> <td><input checked="" type="checkbox"/></td> </tr> </table>	CFA	€	\$			<input checked="" type="checkbox"/>
CFA	€	\$					
		<input checked="" type="checkbox"/>					
MONTANT TOTAL TOTAL SUM	CINQ MILLIONS TROIS CENT MILLE DE DOLLARS AMERICAIN (5.300.000 US\$)						
BUT DU DEPOSIT PURPOSE	PROJET D'INVESTISSEMENT						
BENEFICIAIRE NEXT OF KIN	Mme ESTELLE KONAN						
ADRESSE ADDRESS	05 BP 292 ABIDJAN 05						
DEPOSITAIRE DEPOSITOR	MR. JOSEPH KONAN						
ADRESSE BANCAIRE BANK ADDRESS	BANQUE ATLANTIQUE CI 04 BP 1036 ABIDJAN 04 COTE D'IVOIRE						
CAISSIER RECEIVER'S CASHIER	A/C N° COMPTE BLOQUE 596103487921 Mme ELISABETH PETE						
DATE	14 Février 2003						
INSPECTE PAR INSPECTED BY	MR. KASSI EUGENE						
POSITION	DIRECTEUR DES OPERATIONS BANCAIRES						

Abbildung 14: Ein Vertrag für den Vorschussbetrug

Laut den Statistiken zu Vorschussbetrug erreichten die Verluste im Jahr 2007 4,3 Mrd. US-Dollar.²⁷

Land	Verluste (in Millionen US-Dollar)
USA	830
Großbritannien	580
Spanien	355
Deutschland	280
Japan	270
Frankreich	235
China	205
Australien	166
Italien	159
Kanada	158

Abbildung 15: Verluste aus dem Vorschussbetrug im Jahr 2007 von Unternehmen und Einzelpersonen (Quelle: Ultrascan Research Services)

In Frankreich verlor ein sehr naives Opfer vor einiger Zeit 1 Million EUR!

Zur selben Kategorie gehören Lotterie-E-Mails, die ankündigen, dass Ihre E-Mail-Adresse in einer Millionenziehung ausgewählt wurde. Das Ziel liegt darin, die Opfer zu ermutigen, eine geringe Summe Geld auszugeben und sie in dem Glauben zu wiegen, dass dieser Einsatz sich hundertfach bezahlt macht.

Auktionen

Auktionsbetrug ist eine der größten Sorgen der Behörden. Eine im Mai 2008 von ConsumerWebWatch durchgeführte Umfrage ergab, dass mehr als einer von vier Anwohnern im US-Bundesstaat New York, die an einer Online-Auktion teilgenommen haben (meist eBay, Amazon.com und Overstock.com), mit Scam oder Täuschungspraktiken konfrontiert wurden.²⁸ In den meisten Fällen (11 Prozent) gaben die Benutzer an, dass sie die ersteigerten Waren nie erhalten hatten. Zusätzlich gaben sieben Prozent der Umfrageteilnehmer an, dass die erhaltenen Waren nicht zu verwenden waren. In anderen Fällen fehlten wichtige Details zum ersteigerten Artikel im Angebot (sieben Prozent) oder der gesendete Artikel war von geringerem Wert als angegeben (sieben Prozent).

Mehr als die Hälfte der Personen in den meisten Altersgruppen gab an, dass sie im Falle einer betrügerischen Absicht versucht hätten, das Problem direkt mit dem Verkäufer zu lösen. Etwa 40 Prozent der Opfer erklärten, dass sie eine offizielle Beschwerde bei PayPal, dem Online-Zahlungsdienst von eBay, eingereicht hätten. Mehr als 25 Prozent gaben dem Verkäufer eine negative Bewertung. Insgesamt haben vergleichsweise wenige Umfrageteilnehmer rechtliche Schritte eingeleitet, z. B. einen Rechtsanwalt oder die Federal Trade Commission eingeschaltet.

Überweisungsanforderungen über einen alternativen und anonymen Geldtransferdienst sowie falsche Zahlungen sind weitere Probleme, die sowohl Käufer als auch Verkäufer betreffen können. Werden falsche Zahlungen an einen Verkäufer getätigt, gibt der Kriminelle (der Käufer) an, dass er im Ausland lebt und fordert einen BIC-Code oder eine IBAN-Nummer vom Verkäufer an. Davon sind in vielen Fällen Kfz-Verkäufe betroffen, bei denen das Auto von einem Mittelsmann abgeholt wird. Der Zahlungsbetrag wird auf dem Konto des Verkäufers gutgeschrieben, und das Auto wird sehr schnell abgeholt. Etwas später wird die Zahlung storniert, da die Überweisung keine echte Überweisung war, sondern aufgrund des BIC-Codes nur eine einfache Scheckeinreichung. Da der Scheck nicht ausreichend gedeckt, gestohlen oder gefälscht ist, wird die Transaktion storniert. Der Mittelsmann ist oftmals ein Kurier.

27. Ultrascan Research Services: „419 AFF and the media“ (419 AFF und die Medien). http://www.ultrascan.nl/html/_the_media.html

28. Umfrage von Consumer Reports WebWatch: „More than 25 Percent of New Yorkers Stung in Online Auction Site Scams“ (Mehr als 25 Prozent der New Yorker von Online-Auktions-Scam betroffen). <http://www.consumerwebwatch.org/pdfs/survey/pressrelease.pdf>

Ein anderes Anzeichen für einen Betrug besteht darin, dass eine Person aufgefordert wird, telegrafisch Geld an Western Union oder MoneyGram zu überweisen. Hier ein Beispiel:



Abbildung 16: Gefälschtes Angebot einer Kfz-Auktion

Ein Käufer, der bei einem zu 7.400 EUR angebotenen VW einen Betrug vermutet, wendet sich an den Verkäufer, um dessen Vertrauenswürdigkeit zu testen. Hier die Antwort des Verkäufers:

„Hallo,

vielen Dank für Ihre Nachricht.

Das Fahrzeug hat einen Dieselmotor mit 1900 cm³. Dieser Motor ist sehr leistungsstark und liefert zu diesem Preis eine wirklich sehr gute Leistung.

Dieses Fahrzeug ist in sehr gutem Zustand. Es ist ein Nichtraucherfahrzeug, kein Unfallwagen, hat keine Beulen und Kratzer. Außerdem handelt es sich um einen Garagenwagen. Es ist scheckheftgepflegt, alle Kundendienste wurden von Volkswagen-Händlern durchgeführt. Es hatte keine weiteren Vorbesitzer, alle Papiere sind vorhanden: Scheckheft, Kfz-Zulassung, eidesstattliche Versicherung, usw. Der Verkauf ist unproblematisch, da der Wagen in Frankreich gekauft und zugelassen wurde.

Derzeit lebe ich in Großbritannien, wo ich geheiratet und eine Familie gegründet habe. Ich verkaufe das Fahrzeug, um den Transfer (von Frankreich nach Großbritannien) zu vermeiden. Weil ich außerdem über einen Firmenwagen verfüge, möchte ich das Fahrzeug schnell verkaufen. Mein Wagen befindet sich in der Garage meines alten Wohnhauses in Frankreich (75003 Paris), das ich vor kurzem verkauft habe. In drei Wochen zieht der neue Besitzer ein, daher möchte ich das Auto so schnell wie möglich verkaufen.

Der Preis liegt deutlich unter dem Marktpreis.

Wenn Sie das Auto kaufen möchten, das fast einem Neuwagen entspricht, benötige ich Ihre Daten (kompletter Name und Adresse), um sie an eBay weiterzuleiten. Von eBay erhalten Sie alle weiteren Informationen, die für die rasche und sichere Abwicklung dieser Transaktion erforderlich sind.

Ich hoffe, ich habe mich verständlich ausgedrückt. Bitte senden Sie mir Ihre Kontaktdaten, damit ich Sie als Käufer bestätigen kann.

Ich würde mich freuen, von Ihnen zu hören!“

Nach weiteren Kontakten, in denen der Verkäufer auf Fragen zu seiner Identität und auf den Wunsch des Käufers, das Auto zu sehen, nicht eingeht, erhält der Käufer eine gefälschte E-Mail von eBay, in der eine Überweisung von 3.000 EUR über Western Union angefordert wird. (Dieses Mal wurde der Käufer nicht ausgetrickst. Er wusste vielmehr, dass eBay die Verwendung von sofortigen Geldtransferdiensten verbietet.)²⁹



Abbildung 17: Logo von eBay (Quelle: eBay France)

Online-Shopping

Auch der Vorgang des direkten Online-Kaufs (ohne vorherige Angebotsabgabe) ist das Ziel vieler Angriffe. Webseiten, die keine sicheren Zahlungen anbieten, sollten Sie von vorneherein meiden. Häufig wird Spam verwendet, um leichtgläubige Käufer anzulocken. Wenn die Produkte überhaupt existieren, handelt es sich sehr oft um Fälschungen oder Placebos. Im Sicherheitsbericht von 2007 deckte IronPort³⁰, ein Anbieter von Sicherheitslösungen in Kalifornien (USA), einen Angriff auf, der mehr Ähnlichkeit mit dem organisierten Verbrechen als mit dem Onlinehandel aufweist.

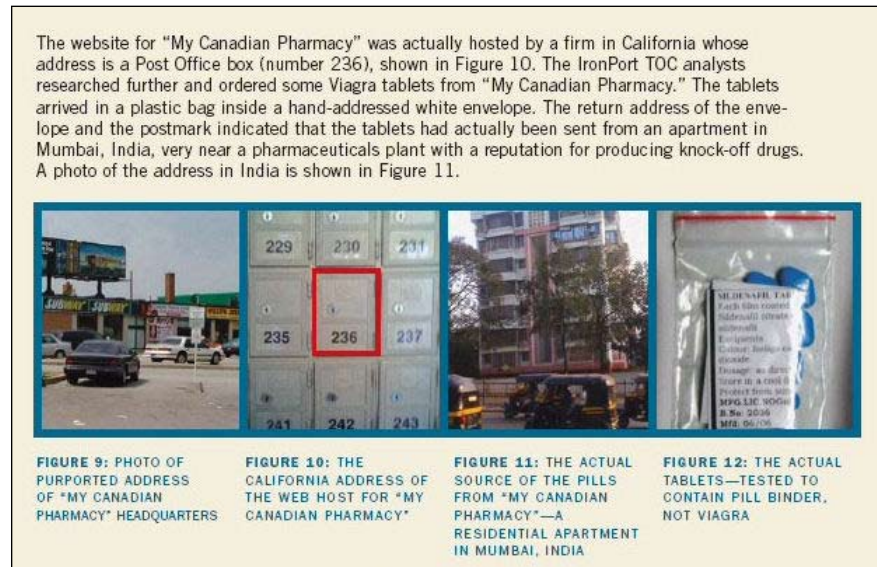



Abbildung 18: Auszug aus dem Betrug des dubiosen Medikamentenanbieters „Canadian Pharmacy“ (Quelle: IronPort-Bericht 2007 für Trends bei der Internetsicherheit)

Eine weitere Art des Käuferbetrugs besteht darin, in Suchmaschinen an hervorstechender Position aufzutreten. Der Kunde wird dann direkt an eine Shopping-Webseite weitergeleitet, auf der alle Arten von Medikamenten, Fälschungen oder Software zu einem Zehntel des Normalpreises angeboten werden. Zum Beispiel ist es wesentlich einfacher, gefälschte Vertu-Telefone aus der Luxusabteilung von Nokia für den Verkauf zu finden als die Originale.

Originals VERTU phones:	VERTU Replica phones:
Are manufactured at one of NOKIA's factories	Are manufactured at one of NOKIA's factories in Hong Kong
Range between 5000 and 68,000 Euros in price	Cost between 550 and 1500 Euros
Are made of amorphous 'Liquidmetal'	Are made of top-quality steel and titanium
Contain gold and platinum	Are covered by real gold and silver using hi-tech IPG methods
Are laced with diamonds and rubies	Are laced with semi-precious stones from Swarovsky
Have sapphire glass	Have a durable plastic anti-gleam screen
Are covered with top-quality leather from Northern Europe	Are covered with top-quality natural leather, which is no worse than that from Northern Europe


NEW PRODUCTS:



VERTU SIGNATURE GOLD HALF PAVE DIAMONDS
An exclusive VERTU Signature replica with Diamond Crystals and...

\$999.00
Original Price: \$68,500.00

[Details](#)
[Add to Cart](#)



VERTU SIGNATURE GOLD POLISHED
Simply a CLASSIC! The VERTU Signature Gold Polished Replica phone is ceramic...

\$859.00
Original Price: \$13,000.00

[Details](#)
[Add to Cart](#)

Abbildung 19: Webseite mit Fälschungen

Anonyme Zahlungsmethoden

Kriminelle ziehen Zahlungen über Dienste wie e-gold und WebMoney vor. Heutzutage gibt es weltweit etwa zwanzig solcher Dienste. Sie sind anonym und bequem.

In Frankreich müssen Online-Zahlungsdienste (anders als von der Bankenbehörde zugelassene Notare und Banken) keine Verdachtserklärung bei TRACFIN (Dienst des französischen Finanzministeriums zur Aufdeckung heimlicher Finanznetzwerke) abgeben, wenn verdächtige Aktivitäten auftreten oder ein bestimmter Betrag überschritten wird.

In den USA ist das Financial Crimes Enforcement Network³¹ (ein US-amerikanisches Netzwerk zur Bekämpfung von Geldwäsche) für das Sammeln und Analysieren von Kontoauszügen zuständig. Bei Bedarf werden die Ermittlungsdienste im Bezug auf Geldwäsche aktiv beraten. Dieser Verwaltungsdienst wurde in das US-Finanzministerium integriert.

Zu den führenden Geldtransferdiensten gehören:

- *e-gold* – Gegründet 1996, mit Firmensitz in Florida, USA. Die Behörden haben dieses Unternehmen bereits seit langem im Verdacht, an illegalen Aktivitäten beteiligt zu sein. Gegen die Gründer und einige der Partner wird derzeit ermittelt.
- *Western Union* – US-amerikanisches Unternehmen mit Niederlassungen in mehr als 200 Ländern. Der Dienst, der nur für Geldüberweisungen an Familienmitglieder genutzt werden sollte, wird oftmals missbraucht.
- *WebMoney* – Dieses russische Unternehmen führt täglich Transaktionen im Wert von 7 Mio. US-Dollar aus. Es verfügt über vier Millionen Kunden, von denen nicht alle rechtschaffen sind.

Auch andere Dienste (einschließlich MoneyGram, Money Express, Ria, Flouss und DabaDaba) werden bei verdächtigen Geldüberweisungen eingesetzt, die mit kriminellen Machenschaften in Verbindung gebracht werden.



Abbildung 20: Eine russische Webseite, die einen Dienst für DDoS-Angriffe (Distributed Denial of Service) anbietet

Schutzmaßnahmen

Finanzbetrug beginnt häufig damit, dass eine fremde Person über den Hausmüll, einen Papierkorb, ein Telefongespräch oder einen unzureichend geschützten Computer Zugriff auf persönliche Daten erhält.

Auch Unternehmen sind durch gestohlene Laptops und Datenkompromittierungen verwundbar, was zu lang anhaltenden Image-Schäden und schweren finanziellen Verlusten für das Unternehmen oder dessen Kunden führen kann. In dieser Hinsicht stehen Banken an vorderster Front.

Obwohl es unmöglich ist, die Gefahr von Identitätsdiebstahl völlig auszuschließen, können Sie das Risiko mithilfe der folgenden einfachen Empfehlungen erheblich reduzieren. (Viele dieser Empfehlungen wurden bereits im McAfee Avert Labs-Whitepaper über Identitätsdiebstahl³² beschrieben.) Im Folgenden werden einige Schutzmaßnahmen beschrieben, die sich direkt auf Bankgeschäfte beziehen.

Bewertung

Mit „Bewertung“ wird eine Methode zur Risikoanalyse bezeichnet, bei der die Wahrscheinlichkeit des erfolgreichen Abschlusses einer Transaktion (d. h. ohne Betrug) berechnet wird. Hierbei werden die verschiedenen Informationen, die zu einem Kauf und dessen Käufer gehören (z. B. E-Mail-Adresse, Kontaktinformationen, Ursprung der IP-Adresse, Umfang der Bestellung) gewichtet. Je nach erzieltm Wahrscheinlichkeitswert wird die Transaktion autorisiert – oder auch nicht.

EMV-Standard (Europay, MasterCard und Visa)

EMV ist der Standard für Zahlungskarten und gilt nur für Karten, die mit einem Prozessorchip ausgestattet sind. Karten, die nur über einen Magnetstreifen verfügen, unterliegen nicht diesem Standard. Die Bank für Internationalen Zahlungsausgleich hat es sich zum Ziel gesetzt, den neuen internationalen EMV-Standard zunächst in ganz Europa und anschließend weltweit als Standard zu etablieren. Im Jahr 2010 werden voraussichtlich mehr als 800 Millionen Zahlungskarten mit diesem Prozessorchip im Umlauf sein.³³

32. http://www.mcafee.com/us/local_content/white_papers/wp_id_theft_en.pdf

33. CARTES 2007: „CARTES & IDentification 2007 fait le point sur le SEPA“ (CARTES & IDentification 2007 bewerten die SEPA-Situation). http://fr.cartes.com/ExposiumCms/cms_sites/SITE_319050/ressources319050/lcp_sepa-fr.pdf

PCI DSS

Zum Schutz vor den Entwicklungen im Bereich der Cyber-Kriminalität haben die Visa- und MasterCard-Netzwerke einen Standard entwickelt, mit dem die Karteninhaber bei Online-Käufen geschützt werden. Der Datenschutzstandard für Kreditkartenunternehmen PCI DSS (Payment Card Industry Data Security Standard) ermöglicht die Verbesserung der Transaktionssicherheit und der Bankdatenspeicherung. Dieser internationale Standard wird auch von anderen Kartennetzwerken wie American Express, JCB und Diners Club unterstützt.

Unternehmen, die Zahlungskartentransaktionen akzeptieren, sind verpflichtet, diesen Standard einzuhalten. Andernfalls kann ihnen untersagt werden, die Daten der Karteninhaber zu ändern. Bei Datenverlust oder -diebstahl drohen außerdem bis zu 500.000 US-Dollar Strafe.

PCI DSS beinhaltet 12 Sicherheitsvorschriften, das von Visa als „Digitales Dutzend“ bezeichnet wird. Diese Anforderungen sind in sechs Kategorien gegliedert:³⁴

- Einrichtung und Verwaltung eines sicheren Netzwerks
 - » Installation und Verwaltung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten
 - » Keine Verwendung der Standardwerte des Herstellers für Systemkennwörter und andere Sicherheitsparameter
- Schutz gespeicherter Karteninhaberdaten
 - » Schutz gespeicherter Daten
 - » Verschlüsselung der Übertragung von Karteninhaberdaten und anderer sensibler Daten über öffentliche Netzwerke
- Verwendung eines Programms zur Schwachstellenverwaltung
 - » Verwendung und regelmäßige Aktualisierung der verwendeten Antivirus-Programme und der Software
 - » Entwicklung und Verwaltung sicherer Systeme und Anwendungen
- Implementierung strenger Maßnahmen zur Zugriffsteuerung
 - » Beschränkung des Zugriffs auf die geschäftlich erforderlichen Karteninhaberdaten
 - » Zuweisung einer eindeutigen ID für jede Person mit Zugriff auf den Computer
 - » Beschränkung des physischen Zugriffs auf Karteninhaberdaten
- Regelmäßige Tests und Überwachung des Netzwerks
 - » Verfolgung und Überwachung sämtlicher Zugriffe auf Netzwerkressourcen und Karteninhaberdaten
 - » Regelmäßiger Test der Sicherheitsprozesse und -systeme
- Verwendung einer Richtlinie zur Informationssicherheit
 - » Verwendung einer Richtlinie zur Informationssicherheit für Angestellte und Auftragnehmer

Protokolle SSL (Secure Sockets Layer) und TLS (Transport Layer Security)

Mit SSL und dessen Version 3.1, genannt TLS, kann eine über das Internet durchgeführte Transaktion gesichert werden. Diese Protokolle wurden von Netscape in Zusammenarbeit mit MasterCard, Bank of America, MCI und Silicon Graphics entwickelt.

Zur Gewährleistung der Sicherheit bei der Datenübertragung setzen SSL und TLS eine Verschlüsselung mit öffentlichem Schlüssel ein. Bei dieser Methode wird nach der Authentifizierung ein sicherer (verschlüsselter) Kommunikationskanal zwischen zwei Geräten (einem Client und einem Server) hergestellt. Dazu gehören die folgenden Funktionen:³⁵

- *Authentifizierung* – Der Client muss die Identität des Servers überprüfen können. Ab SSL 3.0 (der derzeit am häufigsten eingesetzten Version) kann der Server auch den Client auffordern, sich selbst zu authentifizieren. Diese Funktion wird mithilfe von Zertifikaten umgesetzt.
- *Vertraulichkeit* – Es muss gewährleistet werden, dass die Kommunikation zwischen Client und Server nicht von Dritten abgehört werden kann. Diese Funktion wird mithilfe eines Verschlüsselungsalgorithmus umgesetzt.

34. GFI Software: „Le standard PCI DSS simplifié“ (Der vereinfachte PCI DSS-Standard).
<http://www.gfsfrance.com/fr/whitepapers/pci-dss-made-easy.pdf>

35. Vincent Limorte, François Verry und Sébastien Fontaine: „SSL et TLS“ (SSL und TLS). <http://www.authsecu.com/ssl-tls/ssl-tls.php>

- *Identifizierung und Integrität* – Es muss sichergestellt werden, dass die übertragenen Meldungen weder abgeschnitten noch geändert wurden (d. h. die Integrität gewahrt wurde) und vom erwarteten Absender stammen. Diese Funktionen werden mithilfe der Datensignatur umgesetzt.

Funktionsweise von SSL

Mit diesen Schritten authentifiziert ein SSL-Server einen Benutzer.

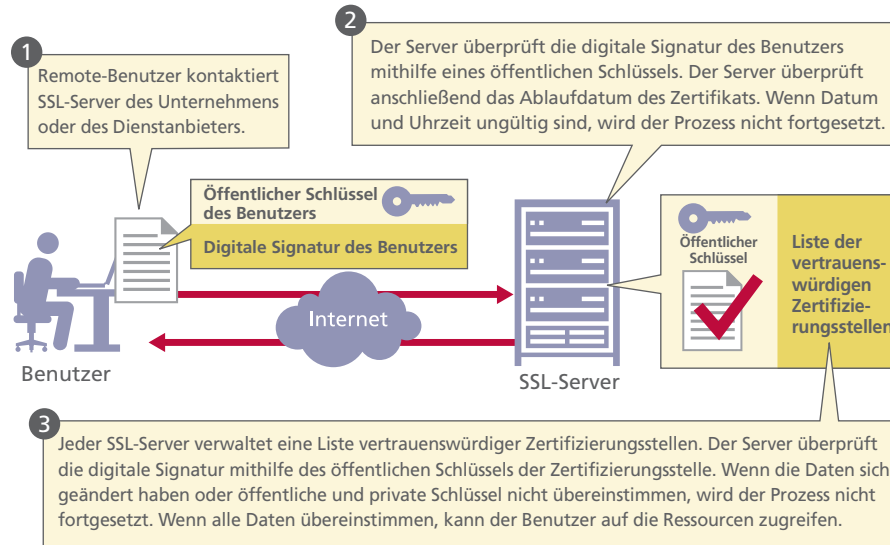


Abbildung 21: Eine Analyse des SSL-Protokolls (Quelle: Netscape)

Da SSL 2.0 zu schwach und angreifbar wurde, ist für eine effektive Verschlüsselung SSL 3.0 oder TLS 1.0 erforderlich.

Es gibt auch andere Protokolle, die die Netzwerksicherheit gewährleisten können. Obwohl sie Funktionen enthalten, die es mit SSL und TLS aufnehmen können, gelten sie dennoch hauptsächlich als ergänzende Protokolle. Bei diesen Protokollen handelt es sich um Secure Shell (SSH) und Internet Protocol Security (IPSec).

- SSH ist ein Protokoll auf Anwendungsebene mit einer sicheren Alternative zu den klassischen Hilfsprogrammen (z. B. rlogin, rsh und telnet), die keine Vertraulichkeit gewährleisten können.
- IPSec stellt eine Sicherheitsmethode auf Netzwerkebene (IP) zur Verfügung und wird vor allem für die Implementierung virtueller privater Netzwerke verwendet.

Im Browser wird bei Verwendung einer SSL-Sitzung ein geschlossenes Schloss angezeigt (Beispiele siehe Abbildung unten).

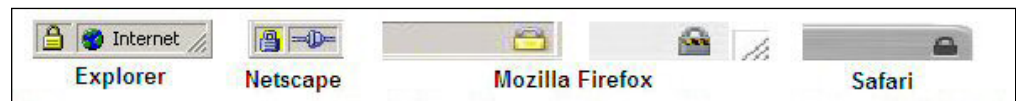


Abbildung 22: Einige Schloss-Symbole für eine aktive SSL-Sitzung (Quelle: McAfee Avert Labs)

Erweiterte SSL-Überprüfung

Wenn Internet Explorer 7 unter Windows Vista oder Windows XP ausgeführt wird, werden Webseiten, die als sicher eingestuft werden und über ein erweitertes SSL-Überprüfungszertifikat verfügen, grün gekennzeichnet. Das Vorhandensein dieses Zertifikats garantiert, dass die Kommunikation sicher ist. Außerdem wird dem Benutzer damit die Identität des Webseiteneigentümers in der Adresszeile angezeigt. Firefox Version 3 und Opera Version 9.5 werden dieses Zertifikat ebenfalls unterstützen.

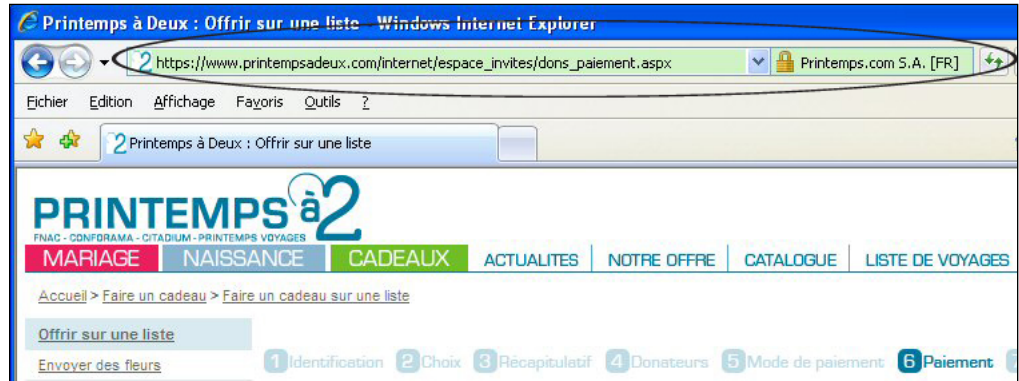


Abbildung 23: Eine Sitzung mit erweiterter SSL-Überprüfung (Quelle: McAfee Avert Labs)

3-D Secure

Die Online-Zahlungsarchitektur 3-D Secure (für „Sicherheit mithilfe von 3 Domänen“) wurde 2001 von Visa und MasterCard ins Leben gerufen. Sie basiert auf SSL und TLS, wobei die Authentifizierung von einer dritten Seite (Domäne) überprüft wird. Bei 3-D Secure müssen sich Kunden, die über das Internet bezahlen möchten, registrieren. Bei der Kaufabwicklung überprüft der Händler bei jeder Remote-Online-Transaktion, ob die Kunden tatsächlich registriert sind.

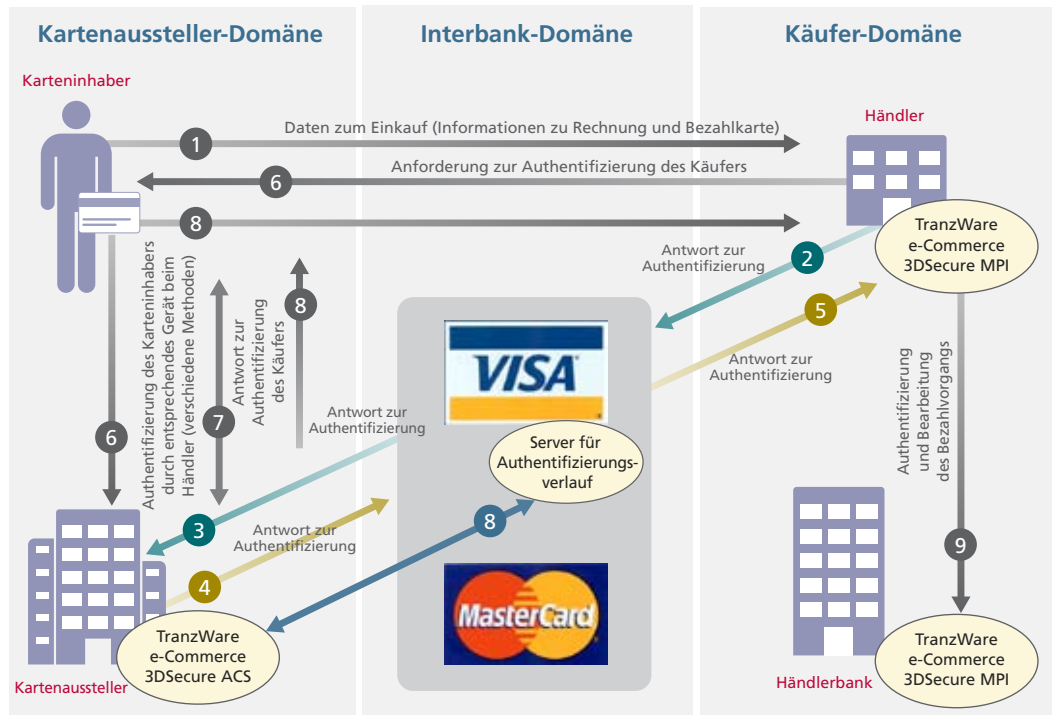


Abbildung 24: Das 3-D Secure-Modell (Quelle: Compass Plus³⁶)

Jede der drei Domänen entspricht einem Benutzertyp:

- Kartenaussteller-Domäne (schließt eine Funktion zur Authentifizierung des Karteninhabers ein)
- Interbank-Domäne (ermöglicht die Kommunikation zwischen den anderen beiden Domänen über das Internet)
- Käufer-Domäne

3-D Secure beschreibt den Ablauf der Informationen zwischen den drei Domänen, die die Kartenzahlung durchführen, und verteilt die Verantwortlichkeiten gleichmäßig:

- Die Bank des Karteninhabers authentifiziert ihren Kunden.
- Die Bank des Händlers authentifiziert ihren Händler.
- Die Interbank-Domäne erlaubt, dass der Händler den Käufer auf dieselbe Art und Weise authentifizieren darf – unabhängig davon, welche Methode vom Käufer verwendet wird.

Starke Authentifizierung und Geräte für einmalig verwendbare Kennwörter

Die Grenzen der traditionellen Authentifizierung mithilfe von Benutzername und Kennwort sind seit langem bekannt (z. B. einfache, auf einem Zettel neben dem Computer notierte oder als Klartext über das Internet gesendete Kennwörter sowie Crimeware). Aufgrund dieser Grenzen besteht ein Bedarf nach starker Authentifizierung mithilfe von drei Elementen:

- Was der Benutzer kennt: Kennwort, PIN, geheime Frage
- Was der Benutzer hat: Karten, Authentifikatoren, Zertifikate
- Was der Benutzer ist: ein biometrisches Element

Eine starke Authentifizierung verwendet mindestens zwei dieser Faktoren.

Ein einmal verwendbares Kennwort (engl.: one-time password, OTP) ist sehr flexibel. Wie der Name impliziert, ist es dazu gedacht, nur einmal gültig zu sein. Durch die Verwendung eines OTP-Geräts wird ein zweiter Authentifizierungsfaktor hinzugefügt:

- Der erste betrifft etwas, das der Benutzer hat, z. B. eine Kreditkarte, die OTP unterstützt.
- Der zweite betrifft etwas, das der Benutzer kennt, z. B. ein Kennwort oder eine PIN. Dieses Element wird dazu verwendet, das OTP unterstützende Objekt zu entsperren.



Abbildung 25: Ein Gerät zur Generierung eines einmalig verwendbaren Kennworts (Fotoquelle: www.reseaux-telecoms.net)³⁷

Ein OTP kann auf verschiedene Weise generiert werden:

- Ein „Token“ oder Rechner – Kompakte Geräte, die das OTP anzeigen und aktualisieren.
- Eine SmartCard – Sie wird mit einem Laptop oder Desktop-Computer verbunden und kann zum Generieren eines Kennworts verwendet werden.
- Ein Mobiltelefon, PDA oder Computer – Diese Geräte verfügen manchmal über spezielle Software zum Generieren von Kennwörtern.

Ein Beispiel ist das PayPal-Plug-In,³⁸ das von PayPal in Zusammenarbeit mit MasterCard angeboten wird. Bei jeder Transaktion generiert das Plug-In eine MasterCard-Kontonummer. Zum Bezahlen mithilfe von PayPal müssen Sie auf einer Webseite, der Sie nicht vertrauen, nicht mehr Ihre PayPal-Kontonummer eingeben. Die Anwendung funktioniert auf jeder Webseite, die MasterCard-Zahlungen akzeptiert.

In Frankreich ist das Konzept der virtuellen Bankkarten nicht neu. Seit 2002 bietet GIE Carte Bleue mit Visa einen Dienst an, der der e-Carte Bleue von Visa entspricht. Heute finden Kunden diese Dienste bei mehreren Banken: LCL, Société Générale, Banque Populaire, La Banque Postale und Caisse d'Épargne. Dennoch ist diese Einkaufsmethode noch nicht weit verbreitet.

Auch sichere Karten sind nicht neu. Bank of America, Citibank und Discover bieten solche Karten an. Sie ermöglichen den Kunden den Einsatz ihrer Karten im Internet, ohne dass diese den Anbietern die tatsächlichen Kartendaten mitteilen müssen. Der Unterschied dieser Karten zu PayPal besteht darin, dass die Käufer fast überall eine sichere Karte verwenden können, ohne tatsächliche eine Kreditkarte zu besitzen (sofern sie die Zahlung mit ihren Bankkonten verknüpfen). Alternativ können sie auch eine beliebige Karte als sichere Karte für Käufe einsetzen, sodass sie sich nicht auf die sicheren Zahlungstools von Bank of America, Citibank oder Discover verlassen müssen.

Im Februar 2008 gaben vier große britische Banken die Bereitstellung von OTP-Geräten bekannt, die mit ihren Bankkarten funktionieren. Statt der Eingabe eines geheimen Codes im Tastenfeld stellt das OTP-Gerät ein Kennwort zur Verfügung, das nur einmal eingesetzt werden kann.

Wissensbasierte Authentifizierung

Die wissensbasierte Authentifizierung wird in den USA häufig eingesetzt. Die traditionelle Variante beinhaltet Fragen wie „Wie lautet der Mädchenname Ihrer Mutter?“ oder „In welcher Stadt wurden Sie geboren?“ In vielen Fällen ist es jedoch für Angreifer einfach, die entsprechenden Antworten zu finden. Der kürzliche Hacker-Angriff auf das E-Mail-Postfach von Sarah Palin ist nur ein Beispiel dafür.³⁹

Diese Methode wird durch die Verwendung dynamisch generierter geheimer Fragen verbessert. In diesem Fall wird vom System während der Laufzeit eine Frage erstellt, deren Antwort Sie kennen müssten, z. B. den Betrag einer Ihrer Zahlungen, den Kaufbetrag eines kürzlichen Einkaufs oder Ihre Adresse im vergangenen Jahr. Die Frage wird dynamisch erstellt und die Antwort nicht für die spätere Verwendung gespeichert. Während der Kunde voraussichtlich recht schnell auf diese Fragen antworten kann, fällt die Antwort Kriminellen wahrscheinlich schwer. Dieses System wird nur selten eingesetzt. Sein Anbieter Verid wurde jedoch im Juni 2007 von EMC gekauft.⁴⁰

E-Mail-Authentifizierung

Zusätzlich zu Methoden für sichere Zahlungen gibt es weitere Authentifizierungsmethoden, die Phishing verhindern helfen:

- Sender Policy Framework ist ein Standard, der die Fälschung von Adressen verhindert. Er basiert auf DNS-Servern, die eine Liste autorisierter IP-Adressen erstellen, über die E-Mails von einer bestimmten Domäne gesendet werden.
- Das von Microsoft herausgegebene Absender-ID-Protokoll unterstützt das Sender Policy Framework.
- Mithilfe von per DomainKeys identifizierten Mails lässt sich die Identität überprüfen, die einer Nachricht während der Übertragung über das Internet zugeordnet wird. Diese Identität gilt dann als für die Nachricht verantwortlich.

38. Bank Systems & Technology: „PayPal's Plug-in Provides Payment Parity“ (Das PayPal-Plug-In ermöglicht Zahlungsparität). http://www.banktech.com/blog/archives/2008/03/paypals_plugin.html

39. Malkin, Michelle: „The Story Behind the Palin Email Hacking“ (Die Geschichte hinter dem E-Mail-Hacker-Angriff auf Palin). <http://michellemalkin.com/2008/09/17/the-story-behind-the-palin-e-mail-hacking/>

40. VNUnet: „EMC rachète Verid, spécialiste de l'authentification basée sur la connaissance“ (EMC kauft Verid, einen Spezialisten für wissensbasierte Authentifizierung). <http://www.vnunet.fr/news/groupe-emc-rach-te-verid-sp-2018533>

Fazit

Auch neun Jahre nach dem Erscheinen des „I love you“-Virus sind viele Internet-Benutzer angreifbar. Optimisten sagen, dass Benutzer heute nicht mehr so unbekümmert auf einen E-Mail-Anhang doppelklicken und dass sie bei ungewöhnlichen Anfragen wie bei einer Mirror-Webseite langsam wachsender werden. Selbst wenn dies der Fall ist: Neue Internet-Abonnenten bilden einen unerschöpflichen Nachschub an naiven Benutzern.

Um sowohl die leichtgläubigen als auch die erfahrenen Benutzer zu erreichen, entwickeln die Cyber-Kriminellen immer wieder neue Methoden und Fallen. Ein Beispiel hierfür ist das Clickjacking, bei dem Schwächen in der Webseitenstruktur ausgenutzt werden: Bei entsprechenden böswilligen Webseiten, die aus zwei Ebenen bestehen, denken Benutzer, dass sie Aktionen auf der sichtbaren Ebene ausführen. Stattdessen führen sie jedoch Aktionen auf einer durchsichtigen Ebene aus, die sich über der sichtbaren Ebene befindet. Der Angriff erfolgt in zwei Schritten – zuerst wird der Mausclick „abgefangen“ und anschließend das Ziel umgeleitet. Nach dem Abfangen des Mausclicks kann der Benutzer zu fast jeder Aktion verleitet werden, ohne dass dieser etwas davon merkt, zum Beispiel Käufe tätigen, Geld transferieren oder einen vertrauenswürdigen Kontakt hinzufügen. Um dieser Schwachstelle entgegen zu treten, werden Browsern zunehmend Sicherheitsfunktionen hinzugefügt, mit denen das Klicken auf „versteckte“ Elemente verhindert wird.

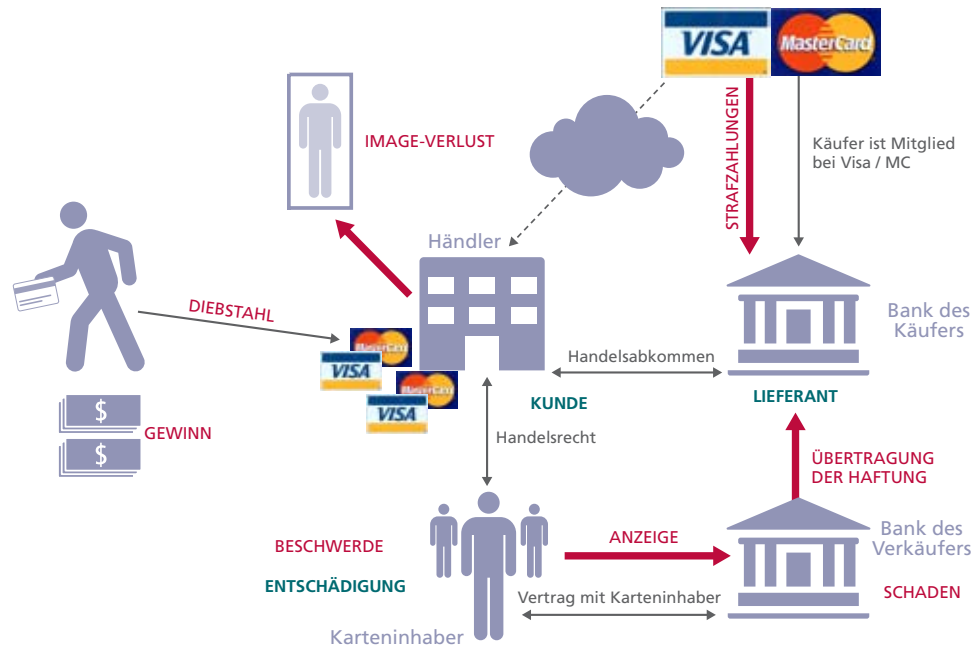
In Anbetracht der Finanzkrise setzen Cyber-Kriminelle auf zahlreiche gefälschte Bank-Webseiten.



Abbildung 26: Gefälschte Bank-Webseiten (Screenshots von McAfee Avert Labs erstellt)

Dabei handelt es sich nicht um Mirror-Webseiten – stattdessen wurden diese Webseiten völlig neu erstellt, um angreifbare Personen anzulocken, deren echte Bank möglicherweise einen Kredit abgelehnt hat. Das Missbrauchen von Menschen, die ohnehin bereits finanzielle Probleme haben, ist skandalös. Wenn noch irgendein Zweifel darin bestand, ob die heutigen Kriminellen Skrupel haben, die Schwächsten unter uns auszunutzen, ist dies der Beweis.

In den vergangenen Jahren stieg der Umfang der Online-Transaktionen im gleichen Maße wie die Betrugsfälle. Die Risiken werden dadurch vergrößert, dass Konten online verwaltet werden können, kein Kontakt zwischen den Parteien (Käufer und Verkäufer sowie zwischen naivem Internet-Benutzer und skrupellosem Kriminellen) besteht, die Kommunikation direkt zwischen zwei Computern erfolgt und für den Abschluss eines Kaufvertrags eine Kreditkartennummer eingegeben werden muss.

Abbildung 27: Die Probleme der Parteien bei einem Online-Kauf (Quelle: CLUSIF⁴¹)

Die Zahlung mithilfe von Bankkarten gilt immer noch als eine der besten Methoden für Käufe, die über das Internet getätigt werden. Als die Anzahl der Transaktionen noch gering war, galt das darin liegende Risiko für beide Seiten als „annehmbar“. Doch in Anbetracht der heutigen großen Transaktionsvolumen verschlechtert sich das Image einiger Händler. Die Kunden sind verärgert und beschweren sich, und die Banken erleiden Verluste, die sie lieber vermeiden würden.

Aufgrund der immer professioneller werdenden Straftaten stärken Banken und große Online-Händler ihre Infrastrukturen, um sich besser vor Betrugsfällen zu schützen. Kleine und mittelständische Unternehmen, für die eCommerce der Schlüssel zu florierenden Geschäften darstellt, haben ihrerseits einen dringenden Bedarf nach Sicherheitslösungen, mit denen sie das Vertrauen der Kunden erlangen und erhalten können. Aufgrund fehlender Schulungen oder purer Nachlässigkeiten stehen diese Unternehmen Angriffen manchmal hilflos gegenüber – und diese Angriffe werden immer raffinierter und hinterhältiger.

Mithilfe von Sicherheitslösungen von anerkannten Anbietern, die Tools und Software für die Verwaltung von Datensätzen und Schwachstellen implementieren, können Unternehmen Compliance mit Sicherheitsstandards erreichen. Letzten Endes stellen zunehmendes Risikobewusstsein der Benutzer und die Verfügbarkeit intuitiver und transparenter Sicherheitstools für Computer die wichtigsten Entwicklungsbereiche für die Zukunft dar.



François Paget ist Senior Malware Research Engineer bei McAfee Avert Labs in Frankreich. Er beschäftigt sich seit 1990 mit Malware-Forschung und gehörte 1995 zu den Gründern von Avert Labs. Paget ist regelmäßig Referent bei französischen und internationalen Konferenzen zu Sicherheitsfragen, Autor zahlreicher Artikel und eines Buches und außerdem Generalsekretär des French Information Security Club (CLUSIF, Französischer Club für Sicherheitsinformationen).

Über McAfee, Inc.

McAfee (NYSE: MFE) ist der weltweit größte dedizierte Spezialist für IT-Sicherheit. Das Unternehmen mit Hauptsitz im kalifornischen Santa Clara hat sich der Beantwortung anspruchsvollster Sicherheits-herausforderungen verschrieben. Seinen Kunden liefert McAfee präventive, praxiserprobte Lösungen und Dienstleistungen, die Computer und ITK-Netze auf der ganzen Welt vor Angriffen schützen und es den Anwendern ermöglichen, gefahrlos Verbindung mit dem Internet aufzunehmen und sich im World Wide Web zu bewegen. Unterstützt von einer preisgekrönten Forschungsabteilung, entwickelt McAfee innovative Produkte, die Privatnutzern, Firmen und Behörden helfen, ihre Daten zu schützen, einschlägige Gesetze einzuhalten, Störungen zu verhindern, Schwachstellen zu ermitteln und die Sicherheit ihrer Systeme laufend zu überwachen und zu verbessern. Weitere Informationen über McAfee finden Sie unter <http://www.mcafee.com/de>.

