secorvo
security consulting

Secorvo Security News

Januar 2008

Editorial: Abgeschöpft

Skimming („Abschöpfen") heißt die neue Kampfansage an bargeldlose Zahlungsmittel, nachdem es zumindest in Deutschland schwieriger geworden ist, mit Phishing reich zu werden. Zwar ist das Abgreifen der PIN am Geldautomaten keine ganz frische Idee: Erste Betrugsfälle, bei denen mittels präparierter Tastatur (Pulver o.ä.) die PIN-Ziffern am Geldautomaten ausgespäht und anschließend die EC-Karte entwendet wurde, gab es schon vor über 15 Jahren.

Die Entwicklung kleinster digitaler Kameras und Kartenleser ermöglicht heute jedoch „Massenattacken" durch die Konstruktion täuschend echter Attrappen für Kartenleser und Tastatur. Dabei werden die Daten der eingeschobenen EC-Karte vom aufgesetzten Lesegerät kopiert und die PIN-Eingabe mit einem Tastaturaufsatz oder mittels winziger verborgener Video-Kameras aufgezeichnet. Anschließend übermittelt die Attrappe die Daten per Funk oder speichert sie auf einem Flash-Chip. Die damit geklonten EC-Karten funktionieren zwar nur im Ausland – dafür kann das Tageslimit meist mehrmals abgeschöpft werden, bevor das Konto gesperrt wird.

2007 wurden in Deutschland 10.400 Skimming-Fälle mit insgesamt 41.000 betrügerischen Abhebungen gezählt – fast doppelt so viele wie 2006. Einige der Täter ließen sich bei der Montage der Attrappen sogar fotografieren und filmen. Und es dürfte noch schlimmer kommen: Denn nicht nur 53.000 Geldautomaten sondern auch die rund 600.000 Point-of-Sales-Terminals sind ein attraktives Ziel – erste manipulierte Geräte, die PIN und Daten per SMS verschicken, wurden bereits entdeckt. Und die PIN-Zahlungen im EC-Cash-Verfahren steigen seit Jahren. Quelle des Übels ist die Speicherung der Kartendaten auf Magnetstreifen statt auf zugriffsgeschützten Chips, einer seit über 15 Jahren verfügbaren Technik. Bis zur Nachrüstung hilft manchmal das Abdecken der PIN-Eingabe mit der freien Hand. Vom Rütteln am Automaten hingegen wird abgeraten – ein Zerstören der Attrappe könnte den Zorn in der Nähe wartender Täter erregen.

Inhalt

secorvo
security consulting

Security News

Router ohne Hosen

Von Tomaz Bratusa wurde am 07.01.2008 eine Session-Riding-Schwachstelle in der Router-Serie Linksys WRT54GL veröffentlicht. Ist ein Benutzer per Browser auf dem Router angemeldet, kann die Firewall des Routers durch einfaches Klicken auf einen präparierten Link deaktiviert werden. Die Routereinstellungen werden gemäß den in der URL übergebenen Parametern ohne weitere Bestätigung verändert, wenn ein Browser-Cookie der authentifizierten Sitzung hinterlegt ist.

Da bei Heimarbeitsplätzen die Firewall des Routers oft die einzige Schutzbarriere zum Internet darstellt und nicht immer zusätzlich eine Personal Firewall eingesetzt wird, besteht eine direkte Gefährdung für die dem Router nachgelagerten Endsysteme. Daher wird dringend empfohlen, administrative Tätigkeiten am Router und Surfen – auch das Recherchieren von Routerkonfigurationen – nicht zeitgleich oder zumindest nicht mit demselben Browser durchzuführen.

Grundsätzlich ist es ohnehin empfehlenswert, die Standardeinstellungen des Routers (wie Kennworte und voreingestellte IP-Netzbereiche) vor Inbetriebnahme zu ändern.

Kompass IT-Sicherheitsstandards

Der in Zusammenarbeit zwischen dem NIA und dem Bitkom erarbeitete Kompass der IT-Sicherheitsstandards wurde am 03.12.2007 in einer neuen Version 3.0 vorgestellt. Der Kompass gibt eine aktuelle Übersicht und Bewertung aller verfügbaren nationalen und internationalen Standards mit Bezug zur IT-Sicherheit. Den Autoren ist es gelungen, eine knappe und sehr hilfreiche Handreichung zu erstellen, die sowohl für IT-Sicherheitsverantwortliche als auch für Geschäftsführer und IT-Führungskräfte ein Leitfaden bei der Planung und Umsetzung von IT-Sicherheitskonzepten sein kann.

Im Rahmen des Sicherheitsmanagements spielen qualifizierte Audits eine immer wichtigere Rolle, daher haben wir den Standard ISO 19011:2002 „Guidelines for quality and/or environmental management systems auditing" vermisst. Auch auf die aktuelle Weiterentwicklung der ISO Standards 27xxx wird nicht eingegangen: So fehlt der Ausblick auf die Standards zu Benchmarking (ISO 27004), Management von Informationssicherheits-Risiken (ISO 27005) und Disaster Recovery Services (ISO 27006). Dies trübt den ansonsten sehr positiven Gesamteindruck allerdings nur minimal.

OpenSource Grundschutztool

Die SerNet GmbH publizierte am 21.01.2008 das OpenSource Grundschutztool Verinice in der Version 0.6. Es unterstützt das Sicherheitsmanagement und die Durchführung von Audits auf der Basis von IT-Grundschutz und ist – im Unterschied zu den etablierten Grundschutztools – kostenfrei erhältlich, sowohl für Windows, als auch für Linux und MacOS. Alle Versionen des Tools sind als Download verfügbar.

Unsere ersten Testeindrücke waren sehr positiv. Das Werkzeug zeichnet sich durch eine intuitive Bedienbarkeit, ein erweiterbares Objektmodell und die Möglichkeit zur Anbindung an verschiedene Datenbanken aus.

Infra-Root

Am 11.01.2008 berichtete die Online-Ausgabe der britischen „Telegraph", dass es einem Jugendlichen gelungen sei, mittels einer TV-Fernbedienung Wiechen der U-Bahn in Lodz umzustellen und so mindestens eine Entgleisung zu verursachen. Die technischen Details bleiben in dem Bericht im Dunkeln – zweifellos aber war die fehlende gegenseitige Authentisierung der beteiligten Geräte wieder einmal (vgl. SSN 04/2007) Hauptursache für das Problem. Statt eines Challenge-Response-Verfahrens wird bei Infrarot-Steuerungen bestenfalls ein Authentisierungscode übermittelt, der grundsätzlich (mit mehr oder weniger hohem Aufwand) kopiert und erneut „eingespielt" werden kann. Bei einfachen Systemen werden moderne programmierbare Fernbedienungen sowie viele PDAs bzw. Mobiltelefone so im virtuellen Handumdrehen über ihre Infrarot-Schnittstelle zum Angriffswerkzeug.

Die meisten Automobilhersteller haben bei ihren Zentralverriegelungen inzwischen professionellere Lösungen implementiert, die von einer einfachen Fernbedienung nicht „erlernt" werden können. Man sollte also erwarten können, dass Systeme mit einem höheren Gefährdungspotential mit mindestens der gleichen Sorgfalt konzipiert werden. Dennoch hat es in der Vergangenheit weitere und ähnliche Vorfälle gegeben. Unsere Empfehlung für's neue Jahr: Hausaufgaben nachholen!

Mit Spammern Geld verdienen

Nicht immer enthalten Spam-E-Mails URLs, auf die man klicken soll, oder Bilder von beworbenen Produkten. Seit einiger Zeit werden reine Text-E-Mails verschickt, die den Kauf bestimmter Aktien bewerben – so genannter „Stock Spam".

Wer sich immer schon gefragt hat, wie und warum derartige Aktionen erfolgreich sein können, dem sei die 39-seitige Anklageschrift zu Alan Ralsky als Lektüre empfohlen: Ralsky gilt seit vielen Jahren als einer der internationalen Top-Spammer, konnte aber nie verhaftet werden. Am 03.01.2008 nun wurden er sowie zehn weitere Personen weltweit angeklagt. Ihnen wird vorgeworfen, über einen Zeitraum von mindestens 21 Monaten durch das Versenden von bis zu mehreren Millionen Spam-E-Mails pro Tag einen Gewinn von geschätzten 2,6 Millionen US-Dollar eingestrichen zu haben.

Dazu kauften sie zunächst gezielt die (niedrig-preisigen) Aktien chinesischer Unternehmen und bewarben diese anschließend via Spam. Etliche Käufer trieben dann den Wert der Aktien in die Höhe, so dass die Spammer ihre Aktienpakete teuer verkaufen konnten. Die gesamte „Aktion" umfasste die Manipulation von Aktienpaketen, Registrierung gefälschter Domains, Bestechung von E-Mail-Server-Administratoren sowie das Mieten von Botnetzen (vgl. SSN 05/2005).

15 Jahre und kein bisschen leise...

Kaum eine andere Security-Veranstaltung zieht seit so vielen Jahren so viele Sicherheitsexperten an: Der DFN Workshop „Sicherheit in vernetzten Systemen" findet in diesem Jahr schon zum 15. Mal statt. Wieder einmal verspricht das Programm, an dessen Erstellung Stefan Kelm als Mitglied des Programmkomitees mitgewirkt hat, sowie die schon legendäre Abendveranstaltung Highlights zu aktuellen Themen der IT-Sicherheit. Auch Secorvo ist – wie in jedem Jahr – an dem Workshop beteiligt: Dirk Fox wird über Realisierung, Grenzen und Risiken der 'Online-Durchsuchung' vortragen.

Kreditscoring im Fokus

Für viele Datenschützer ist der Einsatz von Scoring-Verfahren, mit denen Banken die Bonität ihrer Kunden analysieren, ein rotes Tuch. Denn dabei wird bei Privatkunden oft erheblich in der Persönlichkeitssphäre „gewühlt" – und die unterliegt dem Schutz des Bundesdatenschutzgesetzes (BDSG).

Zahlreiche Kreditinstitute nehmen es jedoch offenbar mit dem BDSG nicht so genau, wie eine am 23.01.2008 vom Bundesverband der Verbraucherzentralen vorgelegte Studie zur Kreditscoring-Praxis in Deutschland zeigt. In über 90% der Stichproben wurden Testpersonen nicht über den Scoring-Wert informiert, in 30% der Fälle wurde nicht einmal eine Einwilligung zur Schufa-Anfrage eingeholt. Schließlich wurden z.T. äußerst fragwürdige Angaben wie „Wohndauer", „Arbeitgeber", „berufliche Stellung" und „Umzugshäufigkeit" erhoben.

Hackers Challenge

Die US-amerikanische Firma Digital Armaments Inc. hat am 04.01.2008 eine Hacker Challenge gestartet, die jede bis zum 29.02.2008 eingereichte neue Schwachstelle mit funktionsfähigem Exploit-Code mit 20.000 US$ prämiert. Das Geschäftsmodell des 2003 gegründeten Unternehmens ist interessant: Es versucht, Hacker zur Zusammenarbeit zu gewinnen und schreibt seit April 2006 immer wieder thematische Hacker Challenges aus. Geld verdient das Unternehmen mit dem Verkauf exklusiver Reports über die eingereichten (und möglicherweise auch selbst gefundenen) Schwachstellen.

Genau so müsste es das organisierte Verbrechen wohl machen, um günstig an unveröffentlichte Exploits zu kommen. Oder BND, BKA und Verfassungsschutz – für die Online-Durchsuchung.

Sicherheitsstudie 2008

Seit vielen Jahren sind die Ergebnisse der IT-Sicherheitsstudie der Zeitschrift KES, die alle zwei Jahre erstellt wird, für viele Sicherheitsbeauftragte eine große Hilfe – denn „belastbare" Zahlen, mit denen sich eigene Risikoeinschätzungen und Investitionsentscheidungen stützen lassen, gibt es viel zu wenig.

Den pdf-Fragebogen für die Sicherheitsstudie 2008 gibt es online unter www.kes.info/studie2008. Die Auswertung erfolgt anonym. Alle Teilnehmer erhalten exklusiven Zugriff auf die tabellarische Auswertung sowie ein Präsent. Einsendeschluss für den ausgefüllten Fragebogen ist der 01.03.2008.

Secorvo News

Secorvo College aktuell

Im vergangenen Jahr hat sich die Zahl der TISP-Absolventen auf mehr als 200 verdoppelt – und die Nachfrage reißt nicht ab. Damit ist der TISP auf dem Weg zum führenden beruflichen Weiterbildungszertifikat im Gebiet IT-Sicherheit. Vom **25.–29.02.2008** bietet Secorvo College mit der fünftägigen T.I.S.P.-Schulung die nächste Gelegenheit, ein TISP-Zertifikat zu erwerben.

Anfang März (**11.–14.03.2008**) bietet das Seminar PKI - Grundlagen, Vertiefung, Realisierung genau das Wissen und die Erfahrung, die für die zielorientierte Entwicklung und den effizienten Betrieb einer PKI unabdingbar sind.

Das gesamte Seminarangebot 2008 sowie ein Online-Anmeldeformular finden Sie unter http://www.secorvo.de/college.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Februar 2008	
05.-06.02.	18. SmartCard Workshop (Fraunhofer, Darmstadt)
10.-13.02.	Fast Software Encryption Workshop (FSE 08) (IACR, Lausanne/CH)
13.-14.02.	15. DFN CERT & PCA Workshop - Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
25.-29.02.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
März 2008	
09.-12.03.	11. International Workshop on Practice and Theory in Public Key Cryptography (IACR, Barcelona/ES)
11.-14.03.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo College, Karlsruhe)
19.-21.03.	5. Theory of Cryptography Conference (TCC 2008) (IACR, New York/US)
April 2008	
01.-03.04.	Forensik - Verfahren, Tools, Praxiserfahrung (Secorvo College, Karlsruhe)
14.-17.04.	Eurocrypt 2008 (IACR, Istanbul/TR)
15.-18.04.	Information Security Management - von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
15.04.	First USENIX Workshop on Large-scale Exploits and Emergent Threats (Usenix, San Francisco/US)
22.-23.04.	Identity Management Symposium 2008 (Secorvo, Karlsruhe-Ettlingen)

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de