Secorvo Security News
August 2005

Dirk Fox, Stefan Gora, Stefan Kelm, Hans-Joachim Knobloch
Secorvo Security Consulting GmbH

Nr. 8, 4. Jhrg. 2005
Stand 24. August 2005

ISSN 1613-4311

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

Inhalt

Editorial: Der Phisher und die 7 Geißlein

„Liebe Kinder, sperrt die Türe gut zu und nehmt euch in acht vor dem Wolf! (...) Der Bösewicht verstellt sich oft, aber an seiner rauen Stimme und an seinen schwarzen Füßen werdet ihr ihn gleich erkennen.“
Gebrüder Grimm, Der Wolf und die sieben Geißlein

Fast gleichlautend lesen sich die Mahnungen der deutschen Banken. Letztere leiden unter der zunehmenden Flut von Phishing-Angriffen: Im Mai 2005 zählte Messagelabs über 9 Mio. Phishing-E-Mails, ein trauriger Rekord. Die Anti-Phishing Working Group erhielt im Juli 2005 über 14.000 Phishing-Reports, im Juli 2004 waren es erst 2.000.

Bisher ließen sich deutsche Phishing-E-Mails leicht an der „rauen Stimme“ erkennen: Das Deutsch war holprig, die Geschichte unglaubwürdig. Aber der Wolf hat Kreide gefressen – neue Phishing-E-Mails sind sprachlich einwandfrei und klingen plausibel. Und auch die Pfote ist nicht mehr verräterisch schwarz – die gefälschten Webseiten der Phisher sind perfekt nachgebildet, verwenden originale Frames, Grafiken, Schriften und Texte.

Einige Banken unterstützen die Phisher, indem sie E-Mails an ihre Kunden senden, oft im HTML-Format, manchmal sogar mit verborgenen Links. Häufig werden zudem Domains für das Online-Banking verwendet, die auch einem Phisher gehören könnten, oder SSL-Zertifikate, die nicht zweifelsfrei die Bank als Anbieter erkennen lassen.

Wenn zugleich E-Commerce-Anbieter aus falscher Sparsamkeit selbst signierte SSL-Zertifikate nutzen, der Support bei abgelaufenem Zertifikat empfiehlt, die Sicherheitseinstellungen des Browsers herab zu setzen oder die Warnung vor einer unverschlüsselten Passwortübertragung zu deaktivieren, muss man sich nicht wundern, wenn die Geißlein keine Chance haben.

Irgendwann passt auch das Märchen nicht mehr. Zumal es bei grenzüberschreitendem Phishing ohnehin schwierig ist, dem Wolf den Bauch aufzuschneiden und die Geißlein lebendig herauszuholen. Passender wird dann vom „Tapferen Phisherlein“ zu berichten sein: Sieben auf einen Streich.

1 Security News

1.1 Web Password Hashing

Von einem Forschungsteam der Stanford University wurde auf dem USENIX Security Symposium Anfang August ein interessantes Verfahren zur Individualisierung von Internet-Passworten vorgestellt. Das Tool und Verfahren Pwd-Hash erfordert keine Änderungen an den Systemen und ist für die Benutzer weitgehend transparent.

Die – oft identischen – Passworte der Benutzer werden mit einem Browser-Plugin (derzeit verfügbar für Mozilla und Internet Explorer) durch ein für jede Zieldomäne individuelles Passwort ersetzt. Hierbei dienen die Ziel-Website, das ursprüngliche Passwort und bei Bedarf ein „salt“ auf dem Clientsystem als Eingangsgrößen. Eine Pseudozufallsfunktion berechnet daraus dann ein neues Passwort. Fällt einem Angreifer auf einem schlecht geschützten System eine Passwortdatei in die Hände, kann er nicht mehr einfach mit derselben User-/Passwortkombination auf weitere sensiblere Systeme zugreifen.

Hierdurch wird implizit in vielen Fällen auch ein Schutz vor Phishing-Angriffen geboten, da die Plugins gefälschte Zielsysteme anhand des Domänennamens vom Originalsystem unterscheiden können.

1.2 iTAN

Auf Phishing-Angriffe reagieren jetzt auch die deutschen Banken mit zusätzlichen Sicherheitsmerkmalen. Die Postbank meldete am 07.08.2005, dass sie ihr PIN-TAN-Verfahren um ein iTAN genanntes Merkmal ergänzt: Zukünftig sind die TAN auf der Liste indexiert. Bei jeder Transaktion schickt der Bankserver den Index, und nur die passende TAN ist gültig. Dieser einfache Challenge-Response-Mechanismus entwertet abge-„phishte“ TAN, denn die Wahrscheinlichkeit, dass eine solche passt, sinkt auf 1/(Anzahl TAN je Bogen). Die iTAN schützt nicht vor allen Angriffen, erhöht aber die Sicherheit des Online-Bankings deutlich.

1.3 XP-Client-Honeypots

Honeypots werden immer beliebter (SSN 5/2005). Während diese jedoch üblicherweise als Server implementiert werden, der darauf wartet, von Angreifern oder Würmern kompromittiert zu werden, verfolgen Forscher von Microsoft Research einen anderen interessanten Ansatz: Im Rahmen des Projekts „Strider HoneyMonkey“ surfen Windows-XP-Clients ständig durch das World Wide Web und identifizieren dabei Webseiten, die insbesondere auf Grund von Schwachstellen im Internet Explorer geeignet sind, einen XP-Rechner zu kompromittieren. Die Rechner verwenden dabei unterschiedliche Patch-Stände – von einem völlig ungepatchten XP-System bis hin zu einem mit den aktuellen Updates ausgestatteten Rechner. Da die Clients innerhalb von virtuellen Maschinen laufen, können sie nach „erfolgreicher“ Kompromittierung sofort und automatisiert in den Ursprungszustand gebracht werden.

Auf dem am 05.08.2005 in Baltimore zu Ende gegangenen USENIX Security Symposium stellte Microsoft im Rahmen eines Kurzvortrags erste Zwischenergebnisse vor. So gelang es den Forschern beispielsweise, innerhalb weniger Wochen 752 URLs zu identifizieren, nach deren Besuch ein ungepatchtes XP-System kompromittiert würde. Interessant ist ferner die Tatsache, dass viele dieser URLs von denselben Betreibern gehostet werden und zudem untereinander stark verlinkt sind.

Ob Microsoft die Informationen der HoneyMonkeys zu Gunsten von besser gepatchten eigenen Produkten nutzen wird, ist fraglich: Der Report enthält im Ausblick lediglich Statistiken und „legal actions“ gegen die Betreiber solcher Webseiten.

1.4 Anonym ins Web

Das Projekt AN.ON (TU Dresden) hat am 14.08.2005 eine neue Version des kostenlosen Anonymisierungsproxies zum Download bereit gestellt. Wie die vorhergehenden Versionen macht die Version 0.05.022 einen stabilen Eindruck – auch wenn sie offiziell als Testversion bezeichnet wird.

Durch JAP erfolgt der Zugriff beim Surfen verschlüsselt über einen extern gehosteten Proxy, der das MIX-Protokoll zur Anonymisierung verwendet. Da dieser in der Regel von mehreren Tausend Benutzern verwendet wird, kann eine Verbindung keinem bestimmten User zugeordnet werden. Wenn man die Protokollierungsfunktionen des Servers nicht berücksichtigt, ist so eine anonyme Internetnutzung möglich. Das einfache Updateverfahren, die umfangreiche Auswahl an Servern inklusive Aktualisierungsmöglichkeit und die Beschränkung der netzseitigen Zugriffsmöglichkeit auf die lokale Clientkomponente machen einen sehr guten Eindruck.

Allerdings werden hierdurch Content-Filter-Mechanismen von Unternehmensnetzen ausgehebelt, sofern ein Zugriff auf die Anonymisierungsdienste über HTTPS zugelassen ist. Auch Angriffe auf HTTP-Ebene können über den Proxy ausgeführt und somit nicht zurückverfolgt werden. Aus Sicherheitssicht ein Nachteil, aus Datenschutzsicht ein Gewinn.

1.5 Lage der IT-Sicherheit

Vom BSI wurde am 19.08.2005 ein Lagebericht zur IT-Sicherheit in Deutschland veröffentlicht – zur aktuellen Situation, Bedrohungen und Trends. Die Ergebnisse überraschen nicht: Der Stellenwert von IT-Sicherheit wird insbesondere angesichts der gewachsenen Abhängigkeit von einer funktionierenden IT nach wie vor unterschätzt. Auch wenn das Bewusstsein um die Bedrohungslage zugenommen hat, stellen nur 39% der Unternehmen ein höheres Budget zur Verfügung. Auch im öffentlichen Bereich fehlen finanzielle Mittel. Recht gut werden neuere Bedrohungen wie Phishing und Bot-Netze zusammengefasst.

1.6 Bluetooth-Kfz-Attacken

In den SSN 11/2003 und 8/2004 berichteten wir von Angriffsmöglichkeiten über Bluetooth. Die Wirklichkeit hat uns inzwischen eingeholt: Eine der Methoden, bei denen ein Angreifer Audiodaten in die integrierte Freisprechanlage eines Fahrzeugs einspielt, wird seit dem 02.08.2005 als Tool im Internet verbreitet. Opfer des Angriffs sind Bluetooth-Geräte mit fest voreingestellter zu einfacher PIN (z.B. 0000, 1234).

Mit dem Tool kann ein Angreifer nicht nur Musik wiedergeben, sondern auch ein lautstarkes „Bremsen!“ über die Lautsprecher erklingen lassen – kein Spaß bei hoher Geschwindigkeit. Liebe (Bluetooth-) Hersteller: Es gibt bessere Verfahren als feste PINs. Riskiert nicht die Gesundheit Eurer Kunden zu Gunsten eines vermeintlichen Bequemlichkeitsgewinns.

1.7 Infosec Dictionary

In der August-Ausgabe des CSO-Magazins erschien The Devil's Infosec Dictionary – ein unterhaltsames, leider z.T. sehr wahres Glossar zentraler Begriffe der Informationssicherheit.

1.8 Wettlauf mit der Zeit

Das Zeitfenster zwischen Fehlerentdeckung und Ausnutzung durch ein Angriffsprogramm schrumpft: Am 17.08.2005 meldete das Online-Magazin WindowsITpro, dass derzeit mindestens sieben Internet-Würmer (u.a. Zotop und RBOT) Systeme befallen, die den erst am 09.08.2005 veröffentlichten Microsoft-Patch MS05-39 nicht installiert haben. Betroffen sind Windows 2000, Windows XP und auch Windows 2003. Ein Testen und Einspielen der Patches wird dringend empfohlen.

2 Secorvo News

2.1 Secorvo College aktuell

Angesichts der wachsenden Herausforderungen, vor die sich Sicherheitsbeauftragte durch neue Kommunikationstechniken gestellt sehen, haben wir diesem Thema ein eigenes, neues Seminar gewidmet. Im Zentrum der dreitätigen Veranstaltung stehen sowohl die Bedrohungen und Risiken von E-Mail, WLANs, Bluetooth, Laptops, PDAs und Voice over IP als auch konkrete Schutzmöglichkeiten, von Verschlüsselung

über die SPAM-Abwehr bis zur Content-Filterung. Dabei stellen sich nicht nur technische Fragen; auch zahlreiche rechtliche Anforderungen sind bei der Umsetzung zu berücksichtigen. Das Seminar wird erstmals am **08.-10.11.2005** durchgeführt.

Alle Termine und Seminarangebote des zweiten Halbjahrs 2005 finden Sie unter

http://www.secorvo.de/college

2.2 Mehr Datenschutz

Seit dem 15.08.2005 gehört Karin Schuler zum Secorvo Team. Sie bringt mehr als 15 Jahre Erfahrung in IT-Sicherheit und Datenschutz mit und verstärkt vor allem unsere Expertise in Datenschutzfragen.

2.3 IT-Forensik

Forensische Fragestellungen treten immer öfter auf. Eine vertiefte Einführung bietet Secorvo College mit dem Seminar Spurensuche im Web (**25.-27.10.2005**). Auch die nächste Sitzung des eco-Arbeitskreises Sicherheit am **16.09.2005** ist dem Thema Forensik gewidmet.

2.4 Neues Video verfügbar

Zum Ende des vergangenen Jahres hatten wir es angekündigt – jetzt ist es endlich verfügbar: unser neues Lehrvideo „Passwort-Sicherheit“ zur Sensibilisierung von Mitarbeitern und Kollegen.

Das ca. zehnminütige Flash-Video nimmt sich dieses schon seit Jahren diskutierten Themas an und zeigt, was ein gutes Passwort ausmacht, wie leistungsfähig heutzutage die Tools und Methoden potenzieller Angreifer sind und was im Umgang mit Passworten beachtet werden sollte, um Angreifer auf Distanz zu halten. Einen kurzen Ausschnitt aus dem Video finden Sie in Kürze als Demo auf unseren Webseiten.

Das Video ist in deutscher Sprache als Einzel- und Intranet-Lizenz verfügbar, als Intranet-Lizenz auch in englischer Sprache. Weitere Sprachversionen erstellen wir auf Anfrage; nehmen Sie diesbezüglich gerne Kontakt mit uns auf.

3 Veranstaltungshinweise

September 2005	
05.-09.09.	Computer Network Forensics Workshop 2005 (IEEE/Create-Net, Athen/GR)
16.09.	Forensik (AK „Sicherheit“ des eco e.V.)
20.-21.09.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
21.09.	1. IT-Grundschutz Tag 2005 (BSI, Bonn)
22.09.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
27.-29.09.	ISSE 2005 (Teletrust, Budapest/H)
27.-29.09.	Web-Application Security (Secorvo College, Karlsruhe)
Oktober 2005	
04.10.	Datenschutz kompakt (Secorvo College, Karlsruhe)
05.-06.10.	Inside Windows Security (Secorvo College, Karlsruhe)
11.-13.10.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
14.-15.10.	hack.lu 2005 (CSRRT-LU, Kirchberg/L)
19.10.	2. IT-Grundschutztag 2005 (BSI,Fraunhofer SIT, St. Augustin)
25.-27.10.	Spurensuche im Web (Secorvo College, Karlsruhe)

Aktuelle Veranstaltungsübersicht:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

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

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