Secorvo Security News
Oktober 2004

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

Nr. 10, 3. Jhrg. 2004
Stand 29. Oktober 2004

ISSN 1613-4311

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

Inhalt

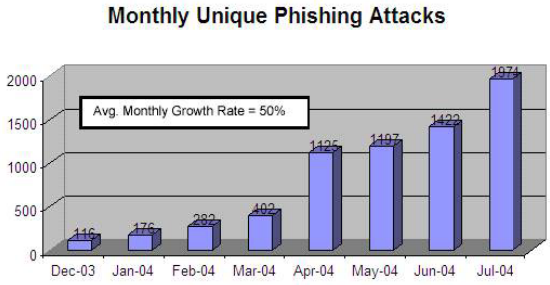
Editorial: Auf Phishfang

Erhoffe das Beste und sei gefasst auf das Schlimmste. (Anonymus)

Seit einem Jahr ist das gezielte Abgreifen von persönlichen Authentifikationsdaten in Mode. Im Hacker-Jargon wird das Ergattern von „hacked accounts“, so genannten „phishes“, seit 1996 als „phishing“ bezeichnet. Damals waren AOL-Accounts das Ziel; Phishes galten in Hackerkreisen als digitale Währung.

Mit dem Aufkommen von Spam haben sich Vorgehensweise und Angriffsziel geändert: In vermeintlich von einer Bank stammenden E-Mails, die das Corporate Design des Geldinstituts täuschend echt nachbilden, werden die Empfänger aufgefordert, eine verlinkte Webseite zu besuchen und dort ihre Authentifikationsdaten einzugeben, wie User-ID, PIN und TANs. Perfider noch ist verstecktes Phishing via Cross Site Scripting, mit Hidden Frames oder URL Obfuscation.

Bislang sind vor allem amerikanische Banken und Privatnutzer von diesen Angriffen betroffen. In Deutschland sind nur wenige Fast-Schadensfälle bekannt – die Überweisungen konnten noch rechtzeitig gestoppt werden. Das muss aber nicht so bleiben: Der Phishing Attack Trend Report der Anti-Phishing Working Group vom 30.08.2004 weist für den Zeitraum von Dezember 2003 bis Juli 2004 einen monatlichen Anstieg der Phishing-Angriffe um im Mittel 50 % aus.



Außer Aufklärung ist bisher kein Kraut dagegen gewachsen. Nur ein Positives lässt sich der neuen Plage abgewinnen: Vielleicht steigt durch Phishing die Sensibilität der Nutzer – auch in den Unternehmen.

1 Security News

1.1 Neue SANS Top 20

Am 08.10.2004 erschien Version 5.0 der SANS Top 20: Einer Liste der 20 kritischsten Internetschwachstellen, je zehn für Windows- und für Unix-Systeme, inklusive einer Auflistung der wichtigsten Patches. Sie wird jährlich aus den Einschätzungen zahlreicher internationaler Sicherheitsexperten zusammen gestellt. Diesmal auf Platz eins: die Standard-Installation von HTTP-Servern und die BIND-Implementierung des DNS. Auch eine deutsche Version der Top 20 ist verfügbar.

1.2 Scanner ausgetrickst

Jeder Virenscanner beherrscht heute die Analyse von .zip-Dateien. Am 18.10.2004 veröffentlichte iDefense jedoch eine perfide Methode, mit der sich diese Funktion bei vielen gängigen Virenscannern austricksen lässt: Setzt man im Header der .zip-Datei die Größenangabe der Originaldatei auf Null, überspringen diese Scanner das Archiv – die Dekompression beim Empfänger funktioniert jedoch weiterhin. Ein Update der Virenscanner-Software ist sehr zu empfehlen.

1.3 Linux strikes back

Nachdem Microsoft in Anzeigen und mit Veröffentlichungen zu belegen versucht, dass Linux das unsicherere Betriebssystem ist, hat sich nun Nicholas Petreley, ehemals Redakteur der Zeitschrift LinuxWorld, an einen Sicherheitsvergleich gewagt – sicherlich auch als Replik auf die umstrittene Studie von Forrester Research vom 19.03.2004 (siehe SSN 04/2004). Das Ergebnis der von Petreley am 25.10.2004 publizierten Studie, in der er 40 aktuelle Schwachstellen von Windows Server 2003 und Red Hat Enterprise Linux Advanced Server v3 verglich: Unter Anlegung gleicher Maßstäbe waren nur 10 % der Red Hat Bugs als schwer wiegend einzustufen, jedoch 50 % der Windows-Bugs.

Aus diesem Ergebnis ist nicht – und schon gar nicht generell – abzuleiten, dass Linux sicherer ist als Windows, wohl aber, dass in der Momentaufnahme von Petreley deutlich mehr der veröffentlichten Microsoft-Schwachstellen schwerwiegend waren. Über die nicht veröffentlichten und die unentdeckten Schwachstellen lässt sich nur spekulieren.

1.4 JPEG-of-Death

Bilder können nicht nur verbotenen und jugendgefährdenden Inhalts sein, sondern auch ein Trojanisches Pferd enthalten – das belegt Microsofts Warnmeldung vom 14.09.2004 (aktualisiert am 12.10.2004). Durch einen kritischen Fehler, der alle Betriebssystem- und Anwendungsprogrammversionen von Microsoft betrifft, kann das Öffnen von manipulierten (JPEG-) Bildern einem Angreifer die Ausführung beliebigen Programmcodes ermöglichen.

Seit dem 29.09.2004 sind solche Bilder unter der martialischen Bezeichnung „JPEG-of-Death“ in Umlauf, die den JPEG-of-Death-Exploit enthalten. Sie schieben dem System durch einen Buffer-Overflow einen kleinen Trojaner unter. Der Angreifer erhält über das Netzwerk Zugriff auf die Kommandozeile des angegriffenen Systems und kann es so kontrollieren. Um den Trojaner zu aktivieren genügt das bloße Ansehen eines manipulierten Bildes – auf einer Webseite, als Anhang oder sogar innerhalb einer E-Mail. Die Schwachstelle betrifft auch das weniger gebräuchliche Windows Metafile-Format (.emf/.wmf), wie ein weiteres Exploit von K-OTIK belegt.

Als Gegenmaßnahme sollten umgehend die Microsoft-Patches MS04-28 und MS04-32 installiert werden, da inzwischen schon „Baukästen“ zur Herstellung derartiger Bilder über das Internet verbreitet werden. Auch ein Update des Virenscanners kann helfen: Zahlreiche Hersteller haben ihre Signaturen angepasst und erkennen jetzt auch manipulierte Bilder.

1.5 Erfolgreiche Bug Bounty

Das Konzept des Bug Bounty Programms der Mozilla-Gemeinde vom 05.08.2004, für die Entdeckung jeder relevanten Schwachstelle eine Belohnung von 500 $ in bar auszuloben, scheint aufzugehen. Die ersten Prämien wurden am 14.09.2004 ausgezahlt – und die festgestellten Schwachstellen umgehend behoben. Ein Update auf die jeweils aktuellen Versionen von Mozilla, Thunderbird und Firefox wird empfohlen.

1.6 Samba Bug

Noch immer wirkt er weiter: Der am 30.09.2003 erstmals veröffentlichte Fehler im ASN.1-Parser von OpenSSL (SSN 10/2003), der in vielen Implementierungen eingesetzt wird – und von zahlreichen vergleichbaren Fehlern anderen in verbreiteten Produkten begleitet wurde (siehe SSN 11/2003, 1/2004, 2/2004, 8/2004). Am 13.09.2004 wurde ein solcher Bug in smbd festgestellt: Durch entsprechend präparierte Pakete können sowohl der Dämon als auch das Serversystem über das Netzwerk „abgeschossen“ werden. Die Installation des zur Verfügung gestellten Patches oder ein Update auf die aktuelle Version 3.0.7 wird dringend empfohlen.

1.7 Pufferüberlauf dank XML

Als Sprache für die Kodierung komplexer Datenelemente hat XML mittlerweile ASN.1 und proprietäre Formate in vielen Bereichen verdrängt. Dies ist sicherlich auch der Erwartung zu verdanken, dass XML-Datenstrukturen einfacher zu handhaben sein sollten als solche in ASN.1.

Zumindest aus dem Blickwinkel der Sicherheit müssen an dieser Erwartung mittlerweile Abstriche gemacht werden: Am 12.10.2004 veröffentlichte Microsoft den Patch für eine Sicherheitslücke bei der XML-Verarbeitung durch das hauseigene WebDAV-Modul, und am 26.10.2004 meldete ein Security-Alert, dass sich in aktuellen Versionen der weit verbreiteten XML-Bibliothek libxml2 des Gnome-Projekts ein halbes Dutzend Pufferüberläufe finden lassen. Tags darauf wurde Version 2.6.15 von libxml2 veröffentlicht, die diese Lücken stopfen soll.

Möglicherweise ist dies der Anfang einer zweiten Folgefehler-Geschichte, wie wir sie im ASN.1-Bereich erleben mussten (s.o.) – dann wäre zu befürchten, dass ähnliche Fehler in einer Implementierung nach der anderen entdeckt werden.

1.8 Vorsicht bei Browser-Eingaben

Dass JavaScript und andere aktive Inhalte sicherheitskritisch sein können, ist bekannt. Am 20.10.2004 wurden jetzt zwei weitere Probleme veröffentlicht, diesmal im Zusammenhang mit dem so genannten „tabbed browsing“, einer Funktionalität vieler Browser, mehrere Webseiten innerhalb eines Browserfensters darzustellen.

Tabbed Browsing kann immer dann problematisch sein, wenn JavaScript aktiviert ist: Die Eingaben, die ein Benutzer scheinbar auf der Webseite z.B. seiner Online-Bank tätigt, können durch geeignet manipulierte Skripte auf anderen Servern landen, wenn entsprechende Webseiten gleichzeitig (innerhalb eines anderen „Tabs“) im Browser angezeigt werden. Betroffen sind alle gängigen Browser in den aktuellen Versionen (siehe auch SSN 7/2004).

Solange keine Patches der Hersteller verfügbar sind, schützen nur die bekannten Verhaltenstipps: JavaScript nach Möglichkeit deaktivieren, URLs immer direkt aufrufen (nicht über Links) sowie andere Seiten (Tabs) schließen, bevor vertrauliche Daten wie Passwörter, PIN oder TAN in ein HTML-Formular eingegeben werden.

Ähnliche Probleme sind seit Jahren im Zusammenhang mit Java-Applets bekannt: Falls Java aktiviert ist, hat der Benutzer keine Kontrolle darüber, wann ein Java-Applet im Browser abläuft. Es kann auch erst dann gestartet werden, wenn der Benutzer längst auf anderen Webseiten „unterwegs“ ist.

2 Secorvo News

2.1 Secorvo College aktuell

Dreimal haben Sie in diesem Jahr noch Gelegenheit, von unseren Erfahrungen zu profitieren – auf dem Grundlagenseminar "IT-Sicherheit heute" vom **09.-11.11.2004**, der Einführung in das "IT-Security Management" vom **22.-23.11.2004** und dem einwöchigen Intensivseminar "Information Security Management" vom **22.-26.11.2004**. Auf Grund der großen Nachfrage empfehlen wir Ihnen bei Interesse eine baldige Anmeldung unter

http://www.secorvo.de/college

2.2 Neues Video in Arbeit

Nach dem großen Erfolg unserer Flash-Videos „Trojanisches Pferd" und „E-Mail-Sicherheit" zur Sensibilisierung der Mitarbeiter haben wir auf Kundenwunsch mit der Entwicklung eines neuen Videos zum Thema „Passwortsicherheit" begonnen. Das zehnminütige Video zeigt die Leistungsfähigkeit heutiger Passwort-Cracker, motiviert für die Verwendung hinreichend sicherer Passworte und zeigt, wie sich gute Passworte bilden und merken lassen.

Die Fertigstellung des Videos ist für Mitte Januar geplant; gerne können Sie ein Exemplar vormerken lassen.

2.3 IsSec und ZertiFA 2004

Anfang Dezember (**06.-07.12.2004**) finden die traditionellen COMPUTAS-Fachkonferenzen IsSec und ZertiFA im Herzen Berlins statt – in diesem Jahr als gemeinsame Veranstaltung unter dem Vorsitz von Stefan Kelm, Johann Bizer und Dirk Fox.

2.4 DuD 2005

Für Ihren Kalender: Die Konferenz DuD 2005 – Datenschutz und Datensicherheit findet vom **18.-19.04.2005** in Berlin statt.

3 Veranstaltungshinweise

November 2004	
09.-11.11.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
22.-23.11.	IT-Security Management (Secorvo College, Karlsruhe)
22.-26.11.	Information Security Management (Secorvo College, Karlsruhe)
23.-24.11.	Einführung in die Praxis des DSB (Euroforum, Wiesbaden)
Dezember 2004	
05.-09.12.	Asiacrypt 2004 (IACR, Jeju Island/Korea)
06.-07.12.	IsSec/ZertiFA 2004 (COMPUTAS, Berlin)
09.-10.12.	Einführung in die Praxis des DSB (Euroforum, Düsseldorf)
16.12.	Nächstes KA-IT-Si-Event (KA-IT-Si, Karlsruhe)
Januar 2005	
25.-26.01.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
27.01.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Die Zusendung des Inhaltsverzeichnisses können Sie per E-Mail anfordern:
security-news@secorvo.de
(Subject: „subscribe security news")

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