secorvo
security consulting

Secorvo Security News

April 2007

Editorial: 1 x 1 > 2

Seit dem zweifelhaften „Siegeszug“ des Phishing ist die „Zwei-Faktor-Authentisierung“ als Ersatz für PINs, TANs und Passworte in aller Munde. Ein sicherheitstechnisches „Ei des Kolumbus“ ist der Ansatz allerdings nicht: Ein höheres Schutzniveau ist damit nicht automatisch verbunden. Wie so oft liegt der Teufel im Detail.

So gibt es zwei notwendige Eigenschaften, die ein „zweiter Faktor“ bei der Authentisierung erfüllen muss: er muss ein zusätzliches, vom ersten unabhängiges Merkmal sein (keine zweite PIN), und seine Gewinnung muss für einen Angreifer eine zusätzliche Hürde darstellen, sodass er beide Faktoren nicht „in einem Streich“ gewinnen kann. Beispielsweise erfordert ein Authentisierungstoken das physische Entwenden, das im Unterschied zu einer PIN bemerkt werden kann; gute biometrische Verfahren erfordern die körperliche Mitwirkung des „Opfers“. Häufig wird daher die Kombination von „Haben“ und „Wissen“ (z. B. eine Smartcard mit einer PIN), bei sehr hohen Sicherheitsanforderungen die von „Wissen“ und „Sein“ empfohlen (z. B. ein Fingerabdruck-Sensor mit einem Passwort).

Das allein aber genügt nicht, um einen Zugriffsschutz wirksam zu verbessern. Denn einen tatsächlichen Sicherheitsgewinn leistet eine solche Kombination nur, wenn beide Faktoren technisch gekoppelt sind: Nur eine Smartcard mit PIN-Schutz und Fehlbedienungszähler bietet ein höheres Schutzniveau, nicht aber eine Kartenprüfung mit unabhängiger PIN-Abfrage durch das System.

Schließlich muss die Authentisierung immer gegenüber dem Endsystem erfolgen – gibt es ein unsicheres „Zwischensystem“, so kann ein Angreifer den Mechanismus dort aushebeln. Daher sind Zwei-Faktor-Authentisierungen bei Client-Server-Anwendungen (wie Online-Banking) nur sicher, wenn die Authentisierung nicht am Client-PC endet, sondern das Authentisierungsprotokoll zwischen Token und Server abläuft – und der PC nur als „Übermittler“ auftritt. An einem Token mit eigener Recheneinheit führt da kein Weg vorbei.

Inhalt

secorvo
security consulting

Security News

Sargnagel für WEP

Wer noch immer hofft, sein Wireless LAN per WEP absichern zu können, muss sich endgültig eines Besseren belehren lassen. Drei Forscher der TU Darmstadt präsentieren in einem am 03.04.2007 veröffentlichten Papier ihre neuesten Ergebnisse zum Brechen von WEP in der Praxis. Durch Kombination von neuen theoretischen Optimierungen beim Angriff auf den RC4-Algorithmus mit bekannten Techniken zum Erlangen von Klartext/Chiffrat-Paaren wie z. B. ARP-Re-Injection ist es möglich, in Minutenschnelle auch 104 Bit WEP-Schlüssel (aus Marketing-Gründen gerne als „128 Bit WEP" bezeichnet) zu ermitteln. Eine Implementierung ihres Angriffs liefern die Forscher gleich mit. Die Attacke ist zwar probabilistischer Natur – allerdings lassen sich mit nur 85.000 Paketen, die innerhalb von etwa zwei Minuten aus dem Netz gefischt werden können, ganze 95% der Schlüssel knacken.

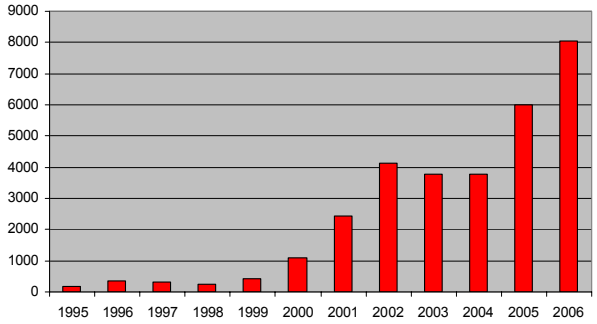
DNS Weakness

Die am 12.04.2007 publizierte Schwachstelle in Microsofts DNS-Dienst ist eine eigene Meldung wert. Nicht, weil sie eine Übernahme des Systems ermöglicht, Exploits zur Ausnutzung der Schwachstelle existieren und es noch keinen Patch gibt: Schwerer wiegt, dass auf ein wichtiges Betriebsrisiko nicht hingewiesen wird und die vorgeschlagenen Workarounds zumindest diskussionswürdig sind. So wird der DNS-Dienst oft auf Domänencontrollern betrieben; damit sind bei einer Übernahme das gesamte System und auch komplette Domänen kompromittiert – dadurch verschärft sich die Bedrohung in der Praxis.

Doch was tun ohne Patch? Einige der in Microsofts TechNet vorgeschlagenen Workarounds deaktivieren Funktionen wie das Remote Management des DNS-Dienstes. Andere wirken etwas hilflos, wie die vorgeschlagene Portfilterung der RPC-Verbindungen über eine Firewall – die sollten bei über das Internet erreichbaren Systemen ohnehin blockiert sein. Ein Seiteneffekt des Workarounds „Blocking port 445" verhindert SMB Connects – und wirkt wohl eher als Denial-of-Service. Besser wäre gewesen, auf Empfehlungen dieser Art zu verzichten – und die Energie in eine zügige Patch-Entwicklung zu stecken.

Vulnerabilities Reports

Jahr für Jahr veröffentlicht das Coordination Center des CERT an der Carnegie Mellon University eine Übersicht der von den weltweit verteilten CERTs berichteten sicherheitskritischen Software-Fehlern in verbreiteten Applikationen. Nach kurzer Stagnation (2002 bis 2004) steigt die Gesamtzahl der gefundenen kritischen Bugs seit zwei Jahren wieder kräftig an: Allein in 2006 wurden über 26 % aller seit 1995 entdeckten Bugs gefunden.



Grafik: CERT/CC-Statistik (Stand: 16.01.2007)

Auch wenn diese Entwicklung einem Gutteil der verbesserten und intensivierten Suche nach Sicherheitsfehlern zuzuschreiben sein könnte, ist diese Tendenz dennoch sehr beunruhigend – belegen die Zahlen doch, dass 2006 durchschnittlich 22 neue Sicherheitslücken täglich zu bewältigen waren, Wochenenden und Feiertage inklusive.

Vista Security Guide

Am 25.01.2007 hat Microsoft Version 1.2 des 107-seitigen Windows Vista Security Guide veröffentlicht. Der auf dem Windows XP Security Guide v2.2 vom 10.04.2006 basierende Leitfaden wurde in einer ersten Fassung schon am 08.11.2006 publiziert und anschließend mehrmals aktualisiert.

Der Guide beschreibt, mit welchen Einstellungen ein Grundschutz-Niveau („Basis-Sicherheit") auf einem Vista-Client erreicht werden kann, sowie die Konfiguration eines Hochsicherheits-Clients unter Inkaufnahme von Funktionseinschränkungen. Mitgeliefert wird ein Excel-Sheet mit Dutzenden von Group Policy Settings sowie dem Group Policy Objects (GPO) Accelerator Tool, das die Umsetzung der Sicherheitskonfiguration über vorgefertigte Templates erheblich erleichtert. Besonders hilfreich: Der tabellarische Vergleich der Default- mit der empfohlenen Grundschutz-Konfiguration von Vista.

Friendly Fire

Ein am 07.03.2007 vom Center for Strategic & International Studies (CSIS) veröffentlichter Bericht über „Foreign Influence on Software" beleuchtet Risiken, die sich aus der Verlagerung der Entwicklung von Software – besonders in kritischen Bereichen – ins Ausland ergeben. Bereits im Oktober 2005 wurde eine Task-Force des amerikanischen Verteidigungsministeriums mit der Erstellung einer

Studie zum „Mission Impact of Foreign Influence on DoD Software“ beauftragt. Der CSIS-Bericht kommt zu dem Schluss, dass die Entwicklungs- und Abnahmeprozesse für Software im Hinblick auf Sicherheit deutlich verbessert werden müssen, unabhängig davon, ob Software im Ausland oder Inland erstellt wird. Die Verurteilung eines Vertragspartners der U.S. Navy in Norfolk am 05.04.2007, der U-Boot-Computer sabotierte, unterstützt die These, dass nicht nur von unkontrolliertem Off-Shoring Gefahren ausgehen.

Department of DNS Security?

Auf einer Sitzung der Internet Corporation for Assigned Names and Numbers (ICANN) in Lissabon am 27.03.2007 berichtete der Chef der kanadischen Internet Registration Authority (CIRA), Bernard Turcotte, von einem internen Papier der US-Regierung, welches offenbar an einige Domainregistrare verteilt wurde: Das U.S. Department of Homeland Security (DHS) soll darin gefordert haben, die Kontrolle über den zur DNSSEC-Signierung der Root-Zone (.) notwendigen Root-Schlüssel zu erhalten. Sieht man einmal davon ab, dass DNSSEC (schon seit zu vielen Jahren) erst vor der Einführung steht (SSN 05/2004, 04/2006) und dieser Schlüssel daher noch gar nicht existiert, stellt sich doch die Frage, welchen Zweck das DHS mit dieser Forderung verfolgt. Denn weder könnte mit diesem Schlüssel etwas ver- oder entschlüsselt werden, noch würde er sich zum Spoofing von IP- oder DNS-Informationen eignen.

Theoretisch würde die Kontrolle des Root-Schlüssels erlauben, durch Fälschung von DNSSEC-Schlüsseln bestimmte (z. B. „unerwünschte“) Domains zu übernehmen. Die Domain boese-terroristen.org könnte dann bspw. vom DHS mit eigenen Inhalten betrieben werden. Dies würde jedoch relativ schnell bemerkt – vorausgesetzt, DNSSEC würde auch tatsächlich flächendeckend verwendet. Da drängt sich der Eindruck auf, dass die eigentliche Funktion der DNSSEC-Schlüssel vom DHS schlichtweg nicht verstanden wurde…

TrueCrypt für Vista

Am 19.03.2007 erschien Version 4.3 der freien Open Source-Implementierung TrueCrypt zur Verschlüsselung von Dateien und Festplattenpartitionen – jetzt auch für Windows Vista. TrueCrypt unterstützt mehrere Sprachen, zahlreiche Verschlüsselungsverfahren, ist leicht zu bedienen – und schnell.

„Two Factor“ – redefined

Zuerst verwirren sich die Worte, dann verwirren sich die Begriffe, und schließlich verwirren sich die Sachen (Konfuzius, 551-479 v. Chr.).

Am 11.04.2007 wurde in einer Pressemitteilung zu einem Sicherheitsvorfall bei der New Horizons Community Credit Union berichtet: „The computer was protected by two layers of security, a unique user-identifier and a multiple-character, alpha-numeric password.“ Vermutlich war die Erklärung irrtümlich zehn Tage zu spät veröffentlicht worden.

Secorvo News

Secorvo College aktuell

Lassen Sie sich Ihre Qualifikation zertifizieren: Die nächste Schulung und Prüfung zum Teletrust Information Security Professional (T.I.S.P.) findet am **25.-30.06.2007** statt. Programm und Online-Anmeldung unter http://www.secorvo.de/college

Tütenwelten

Was hat die Karlsruher IT-Sicherheitsinitiative mit Kunst zu tun? Das Geheimnis dieses Zusammenhangs wird von dem international renommierten Künstler Thitz auf der Vernissage der Neue Kunst Gallery (Karlsruhe) am 11.05.2007 ab 19 Uhr gelüftet. Wie immer mit Net(t)working und Erfahrungsaustausch. Eintritt frei, Anmeldung bis 10.05.2007.

Online-Datensicherung

Am 03.05.2007 lädt der von Dirk Fox geleitete Arbeitskreis Sicherheit des eco (Verband der deutschen Internetwirtschaft e. V.) zu einer halbtägigen Veranstaltung zum Thema Online-Datensicherung nach Frankfurt. Die Teilnahme ist unentgeltlich, eine Anmeldung ist bis 30.04.3007 erforderlich.

Security Awareness Symposium

Auf dem diesjährigen fünften „Security Awareness Symposium“ vom **12. bis 13.06.2007** werden u. a. das BSI, Carl Zeiss, e.on Ruhrgas, European Investment Bank, Fiducia und M. Dumont Schauberg ihre Konzepte und „Lessons Learned“ präsentieren – nach Kampagnenberichten von BASF, BMW, Bosch, DAK, FinanzIT, Münchener Rück, Novartis, RWE, SAP, Swiss Re und T-Systems in den Vorjahren.

Der jährliche Erfahrungsaustausch über wirksame Maßnahmen und Kampagnenideen zur Sensibilisierung der Mitarbeiter für Informationssicherheit findet wegen der wachsenden Teilnehmerzahlen in diesem Jahr in den stilvollen Räumlichkeiten der Buhlschen Mühle in Ettlingen statt (ca. 10 min. Fahrt vom Karlsruher Hauptbahnhof). Teilnahmegebühr: 490 Euro (zzgl. MwSt.). Programm, Online-Anmeldung und Anfahrtskizze:
http://www.security-awareness-symposium.de

Veranstaltungshinweise

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

Mai 2007	
03.05.	Online-Datensicherung (eco AK Sicherheit, Frankfurt)
07.-08.05.	Datenschutzkongress (Euroforum, Berlin)
07.-10.05.	ITSF 2007 (ComConsult, Königswinter)
11.05.	Tütenwelten (KA-IT-Si, Karlsruhe)
15.-17.05.	6th OWASP Appsec Conference (Mailand)
20.-23.05.	2007 IEEE Symp. on Security and Privacy (Oakland)
20.-24.05.	Eurocrypt 2007 (IACR, Barcelona)
22.-24.05.	10. Deutscher IT-Sicherheitskongress (BSI, Bonn)
Juni 2007	
12.-13.06.	Security Awareness Symposium 2007 (Secorvo, Karlsruhe-Ettlingen)
25.-29.06.	T.I.S.P. Schulung (Secorvo, Karlsruhe)
30.06.	T.I.S.P. Zertifikatsprüfung (Secorvo, Karlsruhe)

Fundsachen

Auszug aus www.security-finder.de

Um ein Datenschutz-Zertifikat zur Bestätigung eines hohen Datenschutz-Niveaus erfolgreich zu etablieren, müssen die Rahmenbedingungen stimmen. Ausgehend vom Informationsbedarf möglicher Zielgruppen an ein solches Zertifikat begründet der Beitrag Cui bono? - Ziele und Inhalte eines Datenschutz-Zertifikats die Datenschutzorganisation als Prüfgegenstand und stellt die nach Ansicht der Autoren wichtigsten Inhalte der Prüfung vor.

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Hans-Joachim-Knobloch, 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