secorvo
security consulting

Secorvo Security News

Oktober 2006

Editorial: Verboten

Je mehr Verbote, desto ärmer das Volk.
Laotse, Dao-de-dsching

Verbote besitzen einen unbestreitbaren Vorteil: Mit ihnen wird zielgerichtetes Handeln des Gesetzgebers demonstriert – und diese Klarheit kommt an beim Publikum. Die Wirklichkeit dagegen besitzt einen hässlichen Nachteil: Sie ist komplex – und das häufig in größerem Maße, als es der Mensch mit seiner zur Vereinfachung neigenden Wahrnehmung zu erfassen vermag. Das dürfte die tiefere Ursache dafür sein, dass klare Verbote einerseits so beliebt sind – und mit ihnen andererseits oft nicht nur nicht das angestrebte Ziel, sondern sogar dessen Gegenteil erreicht wird.

Beispielhaft lässt sich dies bei der geplanten Änderung des Strafgesetzbuches beobachten. Mit dem neuen § 202c sollen Vorbereitungshandlungen des Ausspähens und Zugänglichmachens von Daten unter Strafe gestellt werden – darunter auch die Herstellung, Verschaffung und Verbreitung von Computerprogrammen, „deren Zweck die Begehung einer solchen Tat ist". An wenigstens drei grundsätzlichen Fehlverständnissen krankt dieses Vorhaben:

1. *Ein Hacker-Tool ist von einem Sicherheits-Tool oft nicht unterscheidbar*. So wird der ehemalige Trojaner Netbus heute als Tool für die Remote-Wartung vertrieben, und Cain & Abel wird zur Wiedergewinnung verlorener Passwörter empfohlen. Eine „objektive Zweckbestimmung" ist da schwer auszumachen.
2. *Die öffentliche Verbreitung von Angriffs-Tools ist ein Sicherheitsgarant*. Nur wenn Hacker nicht im Verborgenen wirken, wissen wir, was sie wirklich können. Dies ist wesentliche Vorbedingung für das Ergreifen angemessener Sicherheitsmaßnahmen.
3. *Die Nutzung von Hacker-Tools steigert die Sicherheit von IT-Infrastrukturen* – das fordert auch das BSI und verbreitet Nessus seit dem 17.06.2005 (SSN 06/2005) über ihre BOSS-CD. Vielleicht hört die Justizministerin wenigstens auf das Bundesamt?

Inhalt

secorvo
security consulting

Security News

Schach den Wahlmaschinen

Seit einigen Jahren werden zur Vereinfachung des Auszählungsverfahrens bei Wahlen Maschinen der niederländischen Firma Nedap für die Stimmabgabe eingesetzt. Das Modell ESD1 besitzt eine Zulassung des Bundesinnenministeriums; mehr als 15 Mio. Stimmabgaben erfolgten bisher bei Kommunal-, Landtags- und Bundestagswahlen auf solchen Geräten. Geschäftsführer Jan Groenendaal preist seine Geräte als „Dedicated Special Purpose" Maschinen: „Dass man mit unserer Wahlmaschine auch Schach spielen kann, würde ich gerne vorgeführt bekommen."

Der Spott dürfte ihm am 04.10.2006 im Halse stecken geblieben sein: In einem Bericht des niederländischen Fernsehens demonstrierte eine Aktivistengruppe ihren „Nedap Schachcomputer" – der Austausch des EPROMs beim (in 90 % der Wahllokale in den Niederlanden eingesetzten und mit ESD1 weitgehend baugleichen) Wahlcomputer ES3B dauerte keine fünf Minuten, die Anbringung des Schachbretts auf der schrägen Bedienfläche war etwas aufwändiger.

Am 05.10.2006 publizierte die Gruppe eine umfangreiche Sicherheitsanalyse und schob am 10.10.2006 auf YouTube ein Video nach, das zeigt, dass die Stimmabgabe noch aus 25 m Entfernung abgehört werden kann. Tatsächlich lassen sich Manipulationen an Wahlmaschinen nur durch Geräteprüfungen verbunden mit signiertem Programmcode und versiegelten Maschinen nachweisen – eine sehr aufwändige Prozedur, die allerdings nicht vor Manipulationscode im Original-EPROM schützt.

Internet Security Threat Report

Am 25.10.2006 veröffentlichte Symantec ihren 10. Internet Security Threat Report. Darin werden auf gut 100 Seiten die von Symantec im Zeitraum vom 01.01. bis 30.06.2006 mit über 40.000 Sensoren weltweit beobachteten Bedrohungen zusammengefasst. Gegenüber früheren Reports ist bei Angriffen eine Verlagerung der Ziele von der Infrastruktur hin zu Endbenutzer-PCs und Web-Applikationen zu beobachten. Ursächlich dürfte dies auf eine Verschiebung der Interessen von Angreifern zurück zu führen sein – weg von „traditionellen" Motiven wie Geltungssucht hin zu kriminellen Interessen.

Etwa 69 % aller gefundenen Schwachstellen betreffen Web-Applikationen. Hier besteht seitens der Software-Entwickler erheblicher Handlungsbedarf – vor allem, weil diese Schwachstellen 78 % aller leicht nutzbaren ausmachen. Meist handelt es sich um längst bekannte Probleme wie SQL-Injection und Cross-Site-Skripting. Ebenfalls bemerkenswert ist der starke Anstieg von Phishing-Attacken, die im Beobachtungszeitraum um 81 % auf über 157.000 unterschiedliche Nachrichten anstiegen. Als Top-Herausforderungen sieht der Report die Entwicklungen um Web 2.0 (AJAX) und Windows Vista.

iPod spielt „Trojanisches Pferd"

Am 18.10.2006 gab Apple bekannt, dass Video-iPods mit dem Windows RavMonE.exe-Virus ausgeliefert worden waren. Erst am 13.10.2006 hatte die japanische McDonalds-Zentrale vor 10.000 im Rahmen eines Gewinnspiels verteilten, mit dem Trojaner QQPass verseuchten MP3-Playern gewarnt. Zwei Beispiele für Bedrohungen, die in Geräten aus vermeintlich vertrauenswürdiger Quelle lauern können – Trojanische Pferde im ursprünglichen Sinn.

USB Dumper

Dass *mit* USB-Sticks Viren übertragen oder unerlaubt Daten ausgetauscht werden können, ist bekannt. Die Bedrohung *von* USB-Sticks wird jedoch meist nicht gesehen: Steckt man den eigenen USB-Stick in ein fremdes System, auf dem ein Tool wie „USB-Dumper" installiert ist, so werden unbemerkt sämtliche Inhalte des Sticks auf das System kopiert. Ebenso ist es möglich, ein komplettes Image des USB-Sticks zu erstellen, mit dem selbst gelöschte Dateien wieder hergestellt werden können.

Daher ist grundsätzlich der Einsatz von Verschlüsselungslösungen für sensible Daten auf USB-Sticks, mindestens aber eines Tools zum sicheren Löschen (wie beispielsweise „Eraser") zu empfehlen.

Panzerung publik

Am 10.10.2006 berichtete die Financial Times Deutschland über einen bereits am 21.09.2006 erfolgten Diebstahl von Laptops und Flachbildschirmen aus einem VW- und Audi-Vertriebszentrum in Teltow. Das ermittelnde LKA hat den Fall als brisant eingestuft, da auf den entwendeten Systemen auch Informationen über die Sicherheitseigenschaften und -ausstattungen sowie den Aufbau der Dienstfahrzeuge hochrangiger Spitzenpolitiker gespeichert sein sollen. Die Meldung gelangte trotz Nachrichtensperre während der noch andauernden Ermittlungen in die Öffentlichkeit.

Bleibt zu hoffen, dass der Vorfall nicht nur den betroffenen Unternehmen zu denken gibt, sondern allen, die noch immer über keinen durchgängigen Schutz sensibler Daten insbesondere auf mobilen Systemen verfügen – selbst wenn es sich herausstellen sollte, dass es sich in diesem Fall um keinen gezielten Informationsdiebstahl gehandelt hat.

Überblick SAP-Ports

SAP veröffentlichte am 13.10.2006 im NetWeaver Security Knowledge Center eine Neufassung der praktischen und umfassenden Übersicht der von den unterschiedlichen SAP-Anwendungen genutzten TCP- und UDP-Ports. Allein die Zahl der Kommunikationsmöglichkeiten verdeutlicht, wie wichtig es ist, beim Einsatz von SAP-Anwendungen ein ausgereiftes Netzsicherheitskonzept umzusetzen – mit jeder Schwachstelle in der Software droht sonst ein Einfallstor.

Begrüßenswert wäre es allerdings, wenn SAP sich hinsichtlich der genutzten und publizierten Ports mit den Protocol Number Assignment Services der global anerkannten Portliste von IANA abstimmen würde.

Manipulation des Vista Kernel

Einen perfiden Angriff auf den Vista Kernel demonstrierte Joanna Rutkowska auf der diesjährigen Blackhat: Es gelang ihr, durch direkte Zugriffe auf die Festplatte das Swapfile so zu manipulieren, dass dem Vista Kernel unsignierter Code untergeschoben wurde – was die Architektur des Kernels eigentlich durch die Verwendung von Codesignaturen verhindern sollte.

Abhilfe könnte eine Verschlüsselung des Swapfiles schaffen; damit wäre der für diesen Angriff erforderliche direkte Plattenzugriff nicht mehr möglich. Alternativ könnte man auch – ausreichend physikalischen Speicher vorausgesetzt – das Swapfile komplett deaktivieren. Denn das Konzept der „Auslagerung von RAM auf Festplatte" stammt aus Zeiten, in denen Speicherbausteine noch sehr teuer waren.

Security Awareness Monitor

Das Steinbeis-Beratungszentrum Karlsruhe hat auf der Grundlage wissenschaftlicher Methoden der Marktforschung ein Tool entwickelt, mit dem die Sensibilität (Awareness) der Mitarbeiter für Belange der IT-Sicherheit gemessen werden kann – den Security Awareness Monitor (SAM). Der Monitor wurde bereits erfolgreich zur Erfolgsmessung in einer Awareness-Kampagne der T-Systems eingesetzt. Die Ergebnisse dieser Messungen hatte Professor Dr. Konrad Zerr, Leiter des Beratungszentrums, auf dem diesjährigen Karlsruher Security Awareness Symposium vorgestellt.

Secorvo News

Secorvo College aktuell

Neben der Zertifizierung zum T.I.S.P. vom **20. bis 25.11.2006** (siehe unten) gibt es in diesem Jahr noch zwei weitere Gelegenheiten, vom Wissenstransfer eines Secorvo College-Seminars zu profitieren:

- Vom **14. bis 16.11.2006** vermittelt das Seminar „IT-Sicherheitsaudits in der Praxis" unsere Best Practices aus acht Jahren Sicherheitsaudits.
- Vom **28. bis 30.11.2006** folgt ein echter Klassiker: die aktuelle Fassung eines des erfolgreichsten College-Seminare: Kommunikationsschutz und Datensicherheit – intern, extern, mobil.

Programm, Preise und Online-Anmeldung unter

http://www.secorvo.de/college

T.I.S.P. @ Secorvo College

In fünf Tagen zum zertifizierten Information Security Professional: Mit mehr als 100 Absolventen hat sich der „TeleTrusT Information Security Professional" (T.I.S.P.) in weniger als drei Jahren zu einem der verbreitetsten Security-Zertifikate „gemausert".

Dieser Entwicklung trägt Secorvo College durch das Angebot eines T.I.S.P.-„Steilkurses" Rechnung – erstmalig vom **20. bis 25.11.2006** inklusive zugehöriger Prüfung. Für diese Erstveranstaltung zahlen alle Teilnehmer den Frühbucherpreis.

Erfolgreiches KA-IT-Si-Jubiläum

Am 18.10. feierte die auf Initiative von Secorvo und den Karlsruher Versicherungen Anfang 2001 gegründete Karlsruher IT-Sicherheitsinitiative (kurz: KA-IT-Si) ihr fünfjähriges Bestehen – mit weit über 100 Teilnehmern, einer Key Note des Präsidenten des Bundesamtes für Sicherheit in der Informationstechnik, BSI (vertreten durch den Abteilungspräsidenten Bernd Kowalski) und Vorträge und Demonstrationen rund um ein ganzheitliches Verständnis der IT-Sicherheit.

Pünktlich zum Geburtstag stießen zwei neue Partner zur Initiative: die Karlsruher ptv AG und die CONNECT Karlsruhe Computer und Netzwerktechnik GmbH.

Die Unterlagen der Veranstaltung können von der Webseite der Sicherheitsinitiative heruntergeladen werden.

Veranstaltungshinweise

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

Oktober 2006	
23.-27.10.	Systems 2006 (Messe München, München)
November 2006	
07.11.	IT Risk Management 2006 (COMPUTAS, Berlin)
14.-16.11.	IT-Sicherheitsaudits in der Praxis (Secorvo College, Karlsruhe)
20.-24.11.	TISP-Schulung (Secorvo College, Karlsruhe)
25.11.	TISP-Prüfung (Secorvo College, Karlsruhe)
28.-30.11.	Kommunikationsschutz und Datensicherheit (Secorvo College, Karlsruhe)
Dezember 2006	
04.-05.12.	IsSec / ZertiFA 2006 (COMPUTAS, Berlin)
27.-30.12.	23. Chaos Communication Congress (CCC, Berlin)

Fundsachen

Auszug aus www.security-finder.de

Security Engineering –
A Guide to Building Dependable Distributed Systems
Das wegweisende Standardwerk von Ross Anderson ist nun auch online verfügbar. Obwohl fünf Jahre auf dem Markt, hat es nichts an Aktualität eingebüßt, sondern thematisiert alle für die Entwicklung von IT-Systemen relevanten Sicherheitsaspekte, von Passwörtern über Protokolle, Tamper Resistance und Telekommunikationssicherheit bis Monitoring und Management. Ein Muss für alle, die mit Design, Entwicklung oder Implementierung sicherer Systeme befasst sind.

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