Secorvo Security News
September 2005

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

Nr. 9, 4. Jhrg. 2005
Stand 28. September 2005

ISSN 1613-4311

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

Inhalt

Editorial: Das Gegenteil von gut ist ... gut gemeint

Die Komplexität von Software wächst ungebremst: Kam Windows 3.1 (1990) mit 2,5 Mio. Programmzeilen aus, benötigte XP (2002) schon 40 Mio. – vier Mal so viel wie die Software des Space Shuttle. Zugleich wächst die Programmvielfalt und mit beidem die Zahl sicherheitskritischer Fehler. Deren schiere Menge relativiert bisher jede Qualitätsverbesserung im Softwareentwicklungsprozess. Das zeigt nicht zuletzt der exponentielle Anstieg der gefundenen Bugs: Von 171, die das CERT/CC 1995 zählte, auf mehr als 2.800 allein im ersten Halbjahr 2005.

Immerhin werden zunehmend Sicherheitsmechanismen in Softwareprodukte integriert. Das ist grundsätzlich eine begrüßenswerte Entwicklung. Problematisch sind jedoch die handwerklichen und konzeptionellen Fehler, die sich dabei immer wieder beobachten lassen. Das beginnt mit Offensichtlichem wie der Klartextübermittlung von Passwörtern beim Login, geht weiter mit fehlerhaften Authentifikationsprotokollen, bei denen sich nicht der Client gegenüber dem Server sondern umgekehrt der Server gegenüber dem Client authentifiziert, über die „versteckte“ Klartext-Übermittlung eines Verschlüsselungsschlüssels oder die Ableitung eines 256-bit-Schlüssels aus einer sechsstelligen numerischen PIN (Schlüsselraum: 2^{20} bit) bis hin zur „raffinierten“ Beschleunigung des Verschlüsselungsalgorithmus durch das Weglassen einer rechenintensiven Operation.

Diese Fehler zeugen von mangelhaftem Verständnis der, zugegeben oft komplexen, relevanten Zusammenhänge – und haben zudem die fatale Folge, dass der Nutzer der Anwendung sich auch noch bestens geschützt wähnt. Damit gewinnt „Security Engineering“ an Bedeutung, erstmals systematisch behandelt von Ross Anderson in seinem einschlägigen Kompendium. Jüngst trugen SAP und Microsoft dieser Entwicklung mit der Veröffentlichung einer Fibel Sicheres Programmieren Rechnung – vielleicht wichtigstes Ergebnis der Initiative „Deutschland sicher im Netz“.

1 Security News

1.1 To Patch Or Not To Patch

Jeder, der für das Patch-Management verantwortlich ist – und das sollten in der Regel nicht dieselben Mitarbeiter sein, die das Patch-Management ausführen – kennt das Dilemma: Aus Sicherheitssicht sollte ein Patch installiert, zur Gewährleistung der Produktivität laufender Systeme jedoch möglichst nicht verändert werden.

Daher sind – auch in den Fachabteilungen – Ressourcen zum Testen und zusätzliche „Wartungsfenster" zur Durchführung der Updates erforderlich. Doch was tun im Fall der Fälle? Wie reagiert man beispielsweise als Dienstleister, wenn für die betriebenen Webserver Updates gegen vermutete Schwachstellen verfügbar, sie in der jeweiligen Distribution aber noch nicht als „stabil" gekennzeichnet sind?

Dieses Dilemma wird zunehmend durch die normative Kraft des Faktischen entschieden: Die schnelle Verbreitung von Exploits verkürzt die verfügbare Reaktionszeit inzwischen so stark, dass beispielsweise seit 09.09.2005 von Debian auch für die Testing-Version Patches bereit gestellt werden.

1.2 BDSG-Korrektur?

Der Bundesrat hat in seiner 814. Sitzung am 23.09.2005 auf Antrag der Länder Hessen und Niedersachsen einen Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes (BDSG) beschlossen: Danach soll das Quorum, ab dem die Bestellung eines betrieblichen Datenschutzbeauftragten und die Meldung automatisierter Verarbeitungen für nicht-öffentliche Stellen verpflichtend sind, von derzeit fünf auf 20 Mitarbeiter, die mit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten beschäftigt sind, angehoben werden.

Mit dem derzeit innenpolitisch zugkräftigen Argument der Entbürokratisierung und Entlastung kleiner Unternehmen würden damit, falls der Bundestag dem Entwurf zustimmt, mehr als 95% aller Unternehmen von der Pflicht zur Bestellung eines Datenschutzbeauftragten befreit. Zwar würde so zweifellos zunächst ein faktisches Vollzugsdefizit des BDSG legalisiert – angesichts der zunehmenden automatisierten Verarbeitung personenbezogener Daten jedoch ein Pyrrhussieg. Denn betriebliche Datenschutzbeauftragte sind nicht zuletzt in kleinen Unternehmen die wesentliche Triebfeder bei der Umsetzung des datenschutzrechtlichen Persönlichkeitsschutzes.

1.3 Multi-Plattform-Virus

Viren und Würmer, die sich plattformunabhängig verbreiten und Schaden stiften können, sind nicht neu: Bereits der allererste, von Robert Morris Jr. programmierte Internet-Wurm sprang am 02.11.1988 von DEC- auf SUN-3-Systeme über und umgekehrt. Allerdings sind heutige Plattformen zugegebenermaßen ein wenig komplexer.

Laut Trendmicro wurde am 21.09.2005 erstmals ein plattformunabhängiger Handy-Virus gesichtet. Cardtrp.A setzt hinterlistige Methoden ein – hat er ein mit SymbianOS Series 60 betriebenes SmartPhone infiziert, nutzt er die Routinen von Cabir.A zur Weiterverbreitung via Bluetooth. Zusätzlich kopiert er Windows-Schadsoftware auf die Speicherkarte des Handys. Wird die infizierte Speicherkarte in einen PC-Kartenleser eingelegt, droht dort eine Infektion mit der Backdoor Berbew.A und dem Wurm Wukill.B.

1.4 DropMySecurity

Microsoft bietet seit dem 15.11.2004 mit dem auch als Source-Code verfügbaren Tool DropMyRights von Michael Howard ein Hilfsmittel, um Anwendungen aus dem Administratorkontext heraus mit eingeschränkten Berechtigungen zu starten.

Dass Microsoft damit den Spagat versucht, die potenziellen Schadensauswirkungen bekannter „Sicherheitsproblem-Magneten" trotz schlecht programmierte Anwendungen, die Administrator-Rechte erfordern, zu begrenzen, ist zunächst löblich. Dennoch setzt der Ansatz die falschen Zeichen: Anstatt das Übel an der Wurzel zu bekäm-

pfen und die Ursachen der Sicherheitsprobleme zu eliminieren, wird an den Symptomen herumgedoktert: Benutzern wird ermöglicht, weiterhin mit administrativen Berechtigungen zu arbeiten, und nur für bestimmte, besonders risikobehaftete Anwendungen wie E-Mail und Browser werden reduzierte Rechte gewährt.

Zudem kann es gefährlich sein, sich auf Tools wie DropMyRights zu verlassen: Am 01.09.2005 wurden Schwachstellen publiziert, über die sich die vollen Rechte wieder herstellen lassen.

Die Verantwortung ist allerdings auch auf Seiten der Anwender zu suchen, die auch heute noch Anwendungen einsetzen, die einfachste Sicherheitsmechanismen missachten. Bei der Beschaffung von Softwarelösungen sollten Sicherheitsanforderungen nie im Kriterienkatalog fehlen.

1.5 Es geht auch „ohne“ (II)

Dass man es auch besser machen kann als mit DropMyRights zeigt Microsoft in einer Sonderbeilage zum Thema Sicherheit, unter anderem in der aktuellen Ausgabe der c’t. Neben strategischen Themen wie dem Risikomanagement werden auch technische Architekturen wie Trustworthy Computing vorgestellt.

Eines der wichtigsten Themen (siehe SSN 9/2004) wird unter dem Titel „Least Privileges! Es geht auch ohne Administratorrechte!“ behandelt. Darin werden Lösungswege für die tägliche Praxis aufgezeigt: Wie findet man heraus, warum eine Anwendung Administratorrechte benötigt, und wie kann man das System so umkonfigurieren, dass der Benutzer die Anwendung auch „ohne“ nutzen kann? Dazu werden hilfreiche Tools wie der Application Verifier und das Application Compatibility Toolkit vorgestellt.

Aus technischer Sicht kann der Artikel sehr empfohlen werden, ein „Danke“ für die gute Hilfestellung seitens der Redaktion. Nur auf einen wichtigen Punkt weist der Text lediglich am Rande hin: die Aufwände zum Recherchieren der Problemursachen und zum Testen geeigneter Lösungen und Einstellungen binden wertvolle Ressourcen.

Ein weiterer Beitrag beschäftigt sich mit der Entwicklung sicherer Software. Zum selben wichtigen Thema arbeitet Microsoft mit SAP in der Initiative Deutschland sicher im Netz zusammen. In diesem Rahmen präsentieren die beiden Unternehmen ihre Erfahrungen und Richtlinien für die Berücksichtigung von Sicherheitsaspekten bei der Softwareentwicklung: Im Rahmen von drei offenen Veranstaltungen an Universitäten zwischen dem 16.09. und 13.10.2005 und in Gestalt einer von SAP entwickelten 74-seitigen Fibel Sicheres Programmieren, die nicht nur für Programmierer, sondern für alle am Entwicklungszyklus Beteiligten einen Blick wert ist – auch wenn bei der Schlussredaktion der eine oder andere kleine Fehler durchgerutscht ist.

1.6 Big Brother Awards

Die diesjährige Verleihung der deutschen Big Brother Awards, die seit dem Jahr 2000 von FoeBuD e.V. organisiert wird, findet am Freitag, 28.10.2005 im historischen Saal der Ravensberger Spinnerei in Bielefeld statt. Der Preis wird jährlich in mehreren Kategorien für besondere Verdienste um die Überwachung in Deutschland vergeben. Die Auszeichnungen der vergangenen Jahre finden sich inklusive Laudatio auf der Webseite des FoeBuD e.V.

2 Secorvo News

2.1 Secorvo College aktuell

Die Seminare von Secorvo College in Oktober und November spiegeln die vielen Facetten der IT-Sicherheit: IT-Sicherheit heute (11.-13.10.) liefert die Grundlagen und einen aktuellen Überblick über das ständig wachsende Gebiet, Spurensuche im Web (25.-27.10.) erläutert die Möglichkeiten der Forensik mit zahlreichen Beispielen und vielen erkenntnisreichen praktischen Übungen, und schließlich vertieft das Seminar Kommunikationsschutz und Datensicherheit (08.-10.11.) Risiken und Sicherheitsmechanismen der unterschiedlichen elektronischen Kommunikationsmedien und -techniken.

Weitere Seminarangebote und Termine von Secorvo College finden Sie unter http://www.secorvo.de/college

2.2 PhonoNet zertifiziert

Jörg Völker, Autor des mit über 25.000 Downloads derzeit meist gelesenen Secorvo-Whitepapers „BS 7799 – Von Best Practice zum Standard" und seit November 2004 lizensierter BS 7799-Lead Auditor, hat die BS 7799-Zertifizierung der PhonoNet GmbH erfolgreich begleitet: Am 16.09. 2005 wurde das Zertifikat auf der PopKomm 2005 in Berlin offiziell überreicht.

2.3 Sicher ist nicht genug

Auf dem kommenden Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am 20.10. 2005 (18 Uhr) wird Herr Christoph Machner (WebQuake) von seinen Erfahrungen mit dem Aufbau eines Hochsicherheitsrechenzentrums in einem ehemaligen Stollen in Österreich berichten. Anschließend: Net(t)working. Anmeldung und weitere Informationen unter http://www.ka-it-si.de/.

2.4 IsSec/ZertiFA 2005

Das Programm der diesjährigen Computas-„Doppelkonferenz" IsSec und ZertiFA am 05.-06.12.2005 steht. Unter anderem stehen die Sicherheitsaspekte von VoIP, Outsourcing, ITIL, Phishing und Identity-Management sowie Erfahrungsberichte über Datenschutz-Standardisierung, Videoüberwachung und BS 7799-Zertifizierung auf der Agenda, die wie immer mit kompetenten Referenten glänzt.

2.5 Team-Verstärkung

Am 01.10.2005 erhält das Secorvo-Team erneut Verstärkung: Zum Beratungsteam stößt Kai Jendrian hinzu. Er bringt mehrjährige Erfahrung aus der Umsetzung von IT-Sicherheitslösungen in mittelständischen Unternehmen und als IT-Leiter mit. Besonders in den Bereichen Sicherheit von Datenbanken und Web-Applikationen wird er unser Leistungsangebot ergänzen.

3 Veranstaltungshinweise

Oktober 2005	
11.-13.10.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
20.10.	Sicher ist nicht genug (KA-IT-Si, Karlsruhe)
25.-27.10.	Spurensuche im Web (Secorvo College, Karlsruhe)
November 2005	
02.-04.11.	Lotus Notes Security (Secorvo College, Karlsruhe)
08.-11.11.	Kommunikationsschutz und Datensicherheit (Secorvo College, Karlsruhe)
14.-18.11.	Information Security Management (Secorvo College, Karlsruhe)
15.-16.11.	Einführung in die Praxis des DSB (Euroforum, Berlin)
22.-25.11.	Live Hacking Lab (Secorvo College, Karlsruhe)
29.-30.11.	IT-Sicherheit für Windows-Admins (Secorvo College, Karlsruhe)
Dezember 2005	
01.-02.12.	Einführung in die Praxis des DSB (Euroforum, Düsseldorf)
05.-06.12.	IsSec/Zertifa 2005 (COMPUTAS, Berlin)
06.-07.12.	Prüfung zum Certified IT Security Professional (CISP) (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