Secorvo Security News
September 2004

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

Nr. 9, 3. Jhrg. 2004
Stand 28. September 2004

ISSN 1613-4311

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

Inhalt

Editorial: Schicksal Patchen

Vor gut sieben Jahren erheiterte die angeblich von Bill Gates provozierte Pressemitteilung von General Motors, die in 13 Punkten beschrieb, was wäre, wenn Autos mit einer Technologie wie der von Microsoft gebaut würden. Drei Kostproben: „Wenn man bestimmte Manöver ausführt, z. B. eine Linkskurve, stellt sich das Auto ab und weigert sich, neu zu starten. Man muss dann den Motor neu installieren.“ Oder: „Das Airbag-System würde bei jedem Unfall fragen: ‚Sind Sie sicher?’ bevor es auslöst.“ Und: „Man muss den <Start>-Knopf drücken, um den Motor auszuschalten.“

Tatsächlich: Zwischen der Qualität eines Autos und der von Software lagen Welten. Ein Daimler mit Bluescreen? Ein Porsche, der selbstständig bootet? Ein BMW, der ‚Die Anwendung reagiert nicht’ meldet? Undenkbar. Warum aber war und ist Software nicht so fehlerarm wie ein Auto?

Der Grund ist einfach: Die präzise Produktion von Achsen, Kolben und Getrieben hat im Maschinenbau eine weit über 100jährige Tradition. Anders als die Softwaretechnik – sie existiert noch keine 20 Jahre. Denn allen theoretischen Ansätzen zum Trotz gebiert noch immer Erfahrung den größten Fortschritt. So versagten Fahrzeuge vor 80 Jahren – bei niedrigerer Geschwindigkeit und Belastung – weit häufiger als heute.

Vermutlich wäre GM heute zurückhaltender mit ihrer Replik. Denn in modernen Fahrzeugen werkeln inzwischen bis zu 50 vernetzte Kleinstrechner, um Antrieb, Beleuchtung Sicherheitseinrichtungen und Steuerung zu koordinieren und an die Umgebungsbedingungen anzupassen. Der Preis: 2003 war die Fahrzeugelektronik Pannenursache Nr. 1. Wir werden also weiterhin damit leben müssen, dass Software Fehler enthält – im Schnitt 20 je 1.000 Programmzeilen, darunter auch Sicherheitslücken. Damit bleibt bis auf Weiteres das „Flicken“ (Patchen) eine wichtige Security-Disziplin. Allerdings unter verschärften Randbedingungen: Exploits sind inzwischen im Schnitt nach 5,8 Tagen verfügbar.

1 Security News

1.1 Erfahrungen mit XP SP 2

Im Schnitt treten bei 10 % aller Systeme nach der Installation des Service Pack 2 für Windows XP Probleme auf – das jedenfalls behauptet eine am 31.08.2004 veröffentlichte Studie des Asset Management Providers AssetMetrix auf der Basis von 340 befragten Unternehmen mit insgesamt 44.000 PCs. Dabei fanden sich signifikante Unterschiede zwischen kleineren und großen Netzen: Bei weniger als 100 Arbeitsstationen gab es bei gut 12 % der Systeme Probleme, während in grösseren Netzen nur etwa 6 % betroffen waren.

SANS führt derzeit ebenfalls eine (Online-) Umfrage zu Erfahrungen mit SP 2 durch. Zwischenstand: 42 % der knapp 2.100 Befragten hatten keine Schwierigkeiten, dafür aber 10 % große, nicht lösbare Probleme – und 12 % mussten ihre Systeme komplett neu aufsetzen. Trotz des nicht vernachlässigbaren Anteils negativer Erfahrungen raten wir aus Sicherheitsgründen weiterhin zur SP 2-Installation – jedoch erst nach intensiven Tests.

1.2 Abenteuer E-Banking

Das Erkennen von Phishing-E-Mails ist für viele Online-Banking-Anwender eine Herausforderung, nicht zuletzt wegen der perfide verfeinerten Tarntechniken der Absender. Wiederholt wurde von Fällen berichtet, in denen Kunden bereitwillig PIN und TANs preisgaben – und die Transfers der Täter erst in letzter Sekunde von der Bank rückgängig gemacht werden konnten. SANS publizierte am 10.09.2004 sechs Empfehlungen für Webseitenanbieter zur Erkennung von Phishing-Angriffen. Ein absolutes Muss für Entwickler ist Gunter Ollmanns 42seitiger Phishing Guide vom 23.09.2004.

Weit dramatischer jedoch ist die Wirkung des am 07.09.2004 erstmalig dokumentierten Trojaners Bizex-E, der eine knapp drei Wochen alte Schwachstelle des Internet Explorers ausnutzt – und systematisch PIN- und TAN-Eingaben abfängt. Für je einen Kunden der Dresdner Bank und der Postbank ist belegt, dass auf diesem Weg die PIN und eine gültige TAN entwendet und damit je ein vierstelliger €-Betrag auf ein Konto in Lettland überwiesen wurden. Beide Überweisungen konnten von den Banken noch gestoppt werden. Weitere vielleicht „erfolgreiche“ Fälle sind, auch bei anderen Banken, höchst wahrscheinlich.

Gegen Angriffe dieser Art hilft vor allem die Verwendung eines möglichst Fehler freien und restriktiv konfigurierten Browsers. Dafür ist seit Jahren (bekanntermaßen) der Internet Explorer nicht erste Wahl. Diese Überzeugung vertritt nun auch das BSI – zumindest kann man das Interview mit Sprecher Michael Dickopf zu diesem Anlass (Berliner Zeitung vom 10.09.2004) so lesen. Das Portal www.bsi-fuer-buerger.de empfiehlt unverblümter: „Um auf Nummer sicher zu gehen: Wechseln Sie den Browser“.

1.3 Es geht auch ohne...

Eine wichtige Ursache zahlreicher erfolgreicher Viren-, Wurm- und Trojaner-Attacken sind die administrativen Berechtigungen vieler Windows-PC-Nutzer. Erst diese hohe Berechtigungsstufe erlaubt die Installation und Deinstallation beliebiger Software. Daher wird schon lange empfohlen, Anwender nur mit eingeschränkten Rechten auszustatten. Neben dem Widerstand der Nutzer gegen den Rechteentzug sind Probleme mit Anwendungen, die Daten in Systemverzeichnisse schreiben oder auf geschützte Bereiche der Registry zugreifen, häufigstes Umsetzungshindernis.

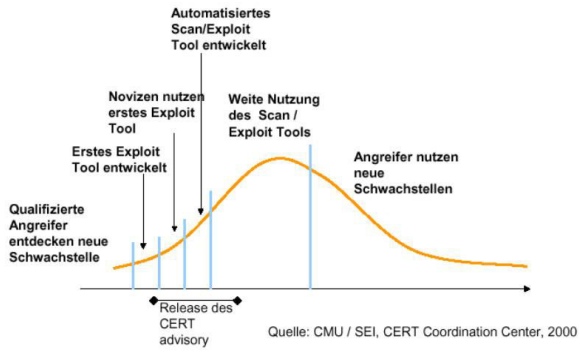
Oft gibt es jedoch eine (undokumentierte) Möglichkeit, die betroffene Anwendung auch ohne Administrationsrechte zu betreiben. Angeregt durch einen Beitrag in c’t 15/2004 wurde solchen Problemlösungen die Webseite www.noadmin.de gewidmet. Zur Zeit können dort in einem Forum Tipps ausgetauscht werden; der Aufbau einer umfassenden Datenbank ist geplant.

1.4 Hacme Bank v1.0

Von Foundstone wurde am 08.09.2004 das kostenfreie Tool Hacme Bank veröffentlicht, eine Webapplikation, in die typische Schwachstellen integriert wurden. Gedacht ist es zur Schulung von Systemverantwortlichen und Entwicklern: Sie sollen die Schwachstellen mit geeigneten Analysetools entdecken. Solchermaßen sensibilisiert werden sie anschließend Schwachstellen in eigenen Applikationen hoffentlich selbst erkennen bzw. schon in der Entwicklungsphase vermeiden.

1.5 Laws of Vulnerabilities

Unter dem Titel "Laws of Vulnerabilities" publizierte Gerhard Eschelbeck, CTO von Qualsys, auf den diesjährigen Black Hat Briefings am 28.07.2004 in Las Vegas die Ergebnisse einer Auswertung von 6,5 Mio. Device Scans. Danach benötigen Unternehmen ab dem Bekanntwerden schwer wiegender Schwachstellen derzeit im Schnitt 62 Tage, um die Hälfte ihrer internen Systeme zu patchen, und 21 Tage für die Hälfte der direkt vom Internet aus erreichbaren Systeme.



Da die Zeitspanne zwischen Bekanntwerden einer Schwachstelle und der Verfügbarkeit eines Exploits oder der Ausnutzung durch einen Wurm immer kürzer wird – nach Symantecs aktuellem Security Thread Report vom 22.09.2004 schrumpfte sie in der ersten Jahreshälfte 2004 auf sechs (!) Tage – sollte ein wirksames Patch-Management derzeit ganz oben auf der Agenda des Security-Managements geführt werden.

1.6 Frechheit siegt...

Die marktführende Online-Handelsplattform Ebay wurde Ende August für einige Stunden außer Betrieb gesetzt – allerdings nicht durch eine Distributed Denial of Service Attacke, wie man vermuten könnte. Eine Privatperson hatte ganz dreist beim Provider intergenia die Domänen ebay.de und amazon.de bestellt. Der automatisierte KK-Antrag zur Übertragung der Domäne wurde von Amazon abgelehnt. Von Ebay kam jedoch keine Reaktion, und so wurde der korrekte DNS-Eintrag durch den der Webseite der Privatperson ersetzt.

Merke: Nicht nur in komplexen Anwendungen, sondern auch in einfachsten Prozessen kann der Wurm drin sein – und nicht unerhebliche Umsatzausfälle verursachen.

1.7 Gefahr durch VxWorks?

Frank Denis publizierte am 04.09.2004 auf der Mailing-Liste full disclosure eine kritische Schwachstelle von Storage Devices, die einen Controller von Engenio (ehemals LSI Logic) verwenden. Diese Devices werden u.a. in Fibre-Channel Switches von Brocade und in Storage-Systemen der Hersteller Storagetek (D series) und IBM (DS4xxx series, ehemals FAStT) sowie weiteren, wie SGI und Teradata eingesetzt.

Durch den Fehler kann das Device mit Hilfe spezieller IP-Pakete zum Absturz gebracht werden; in bestimmten Fällen ist ein Datenverlust möglich. Je nach Einsatzumfeld können die Auswirkungen eines solchen Angriffs erheblich sein. Vor diesem Hintergrund stimmen die Reaktionen der betroffenen Hersteller sehr nachdenklich: Nicht genug damit, dass die schon Mitte Juni durch Frank Denis informierten Hersteller trotz mitgesandtem funktionierenden Exploit, sofern überhaupt, erst nach mehreren Wochen reagierten. Sollte der Fehler, wie Storagetek behauptet, dem verwendeten Betriebssystem VxWorks zuzuordnen sein, dann könnten zahlreiche weitere Systeme betroffen sein. Der Hersteller Windriver war jedoch angeblich nicht bereit, sich des Falls ohne Lizenznachweis anzunehmen.

2 Secorvo News

2.1 Secorvo College aktuell

Die “Herbstsaison” hat begonnen. Mit dem gefragten „Live Hacking Lab“, das wir gemeinsam mit der Schweizer Compass Security und einem umfangreichen Laboraufbau durchführen, lassen wir Sie zwei Tage lang, vom **12.-13.10.2004**, einen Blick in die Hexenküche aktueller Angriffsmethoden werfen – von Spoofing und Sniffing über inside-out-Attacken bis hin zu SQL-Injektion und Cross-Site-Scripting.

Daran schließt sich am **14.10.2004** ein eintägiger Aufbauworkshop an, der Internet-Angriffe, LAN-Attacken und Penetrationstests vertieft.

http://www.secorvo.de/college

2.2 Und da waren es sechs...

Am 01.09.2004 konnte Secorvo auf sechs erfolgreiche Unternehmensjahre zurückblicken. Über 200 erfolgreiche Projekte, mehr als 650 zufriedene Teilnehmer aus über 220 namhaften Unternehmen, die an Seminaren von Secorvo College teilgenommen hatten, über 150 Fachpublikationen und mehr als 160 Fachvorträge sowie 1,5 Mio. Webseitenzugriffe auf Artikel, White Paper und 25 Security News dokumentieren unsere Entwicklung – auf die wir auch ein wenig stolz sind.

2.3 Secorvo wächst

Aufgrund der in den vergangenen Monaten erheblich gestiegenen Zahl von Projektanfragen erweitern wir unser Team. Ab dem 01.10.2004 wird Petra Barzin uns verstärken. Sie bringt neun Jahre Berufserfahrung in der IT-Sicherheit mit und hat sich u.a. als Autorin der Signatur-Interoperabilitätsspezifikation und der RFC 3039 (Qualified Certificates) sowie als Mitentwicklerin der SecuDE-Bibliothek einen Namen gemacht.

3 Veranstaltungshinweise

September 2004	
28.-30.09.	ISSE 2004 (EEMA/TeleTrusT, Berlin)
Oktober 2004	
12.-13.10.	Live Hacking Lab (Secorvo College, Karlsruhe)
14.10.	Live Hacking Lab – Aufbauworkshop (Secorvo College)
26.-27.10.	Inside Windows Security (Secorvo College, Karlsruhe)
November 2004	
02.-04.11.	Sichere E-Mail-Kommunikation (Secorvo College, Karlsruhe)
09.-10.11.	Computer Forensic Symposium (Secorvo/VICCON, Karlsruhe)
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)
November 2004	
06.-07.12.	IsSec/ZertiFA 2004 (COMPUTAS, Berlin)

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