secorvo
security consulting

SSecorvo Security News

Juni 2008

Editorial: Reden ist Silber

Schweiger erfreuen sich in westlichen Gesellschaften eines guten Rufs. Wer wenig redet, den umgibt der Nimbus des Vergeistigten – denn „Stille Wasser sind tief", wie der Volksmund weiß. Oder er gilt gar als weise: Von Ernest Hemingway (1899-1961) ist der Ausspruch überliefert, man brauche „zwei Jahre, um sprechen zu lernen, und fünfzig, um schweigen zu lernen". Zumeist gilt Schweigen als ein Indiz für Nachdenken – wenigstens bis zum Beweis des Gegenteils: „Wo Männer schweigen, reden die Gedanken" (Carl Spitteler, 1845-1924).

Nicht immer aber stimmt das Klischee. Denn Schweigen kann auch mehr Schein als Sein verbergen. Das wird oft erst deutlich, wenn sich ein stilles Wasser als seichte Pfütze outet. Ein fast 1.500 Jahre altes Bonmot belegt die lange Tradition des Schweigens als potemkinsches Dorf: „Si tacuisses, philosophus mansisses" reimte der Philosoph Boethius (ca. 475–525 n. Chr.) – „Hättest Du geschwiegen, wärst Du Philosoph geblieben." Die Motivation des taktischen Schweigens hat der französische Schriftsteller François Duc de La Rochefoucauld (1613-1680) auf den Punkt gebracht: „Schweigen ist der beste Ausweg für den, der seiner Sache nicht sicher ist." Bei hartnäckigem Schweigen ist daher Vorsicht angeraten.

Die Geschichte der Kryptographie kennt unzählige Beispiele für dünne Bretter, die allein durch Schweigen hielten: Crypto-1 (Mifare) und KeeLoq sind zwei der jüngsten. Auch wenn es immer wieder behauptet wird: Die Sicherheit eines (Krypto-)Verfahrens steigt nicht durch Geheimhaltung. Im Gegenteil: „Security by Obscurity" erhöht das Risiko eines schlagartigen Sicherheitsverlustes, falls das Verfahren bekannt wird. Immer wieder bestätigt sich der von Auguste Kerckhoffs vor 125 Jahren in „La Cryptographie Mililtaire" formulierte Fundamentalsatz der modernen Kryptographie: Die Sicherheit eines kryptographischen Mechanismus' darf nur von der Geheimhaltung des Schlüssels abhängen. Oder kurz: Reden ist Silber. Schweigen ist ... Mist. Zumindest in der Kryptographie.

Inhalt

secorvo
security consulting

Security News

OpenSSL Nachwehen

Die meisten Probleme des am 13.05.2008 bekannt gewordenen Sicherheits-Desasters von OpenSSL in Debian-basierten Linux-Distributionen sind umfänglich beschrieben und diskutiert worden (siehe auch SSN 05/2008). Möglicherweise betroffene Server-Schlüssel können seit dem 09.06.2008 mit dem SSL-Online-Check des Heise-Verlags überprüft werden.

Auf ein etwas vernachlässigtes Risiko wollen wir jedoch hinweisen: Auch Schlüssel, die auf Systemen erzeugt wurden, die von der OpenSSL-Problematik nicht betroffen waren, müssen als kompromittiert gelten, wenn sie auf einem betroffenen System zur Public-Key-Authentifizierung mit DSA, wie z. B. bei SSH, eingesetzt wurden. DSA benötigt zum Signieren eine vom Client-System erzeugte Zufallszahl, die geheim bleiben muss. Mit Kenntnis dieser Zufallszahl kann mit einfacher Mathematik in wenigen Schritten der private Schlüssel aus einer veröffentlichten DSA-Signatur herausgerechnet werden. Noch einfacher ist es bei einem Diffie-Hellman-Schlüsselaustausch: Die kleine Menge möglicher Zufallszahlen auf einem betroffenen Client erlaubt es einem Angreifer, mit begrenztem Aufwand den Session-Key aus mitgeschnittenen SSH-Sessions zu gewinnen.

ISO-Risikomanagement

Mit dem am 04.06.2008 veröffentlichten Standard ISO/IEC 27005:2008 "Information technology – Security techniques – Information security risk management" hat die ISO die Normenreihe ISO/IEC 2700x um einen wichtigen Baustein ergänzt. Neben einer verallgemeinerten Herangehensweise an das Thema Risikomanagement werden darin wesentliche Prozessschritte wie beispielsweise die Risiko-Identifikation, -Bewertung und -Akzeptanz beschrieben und konkrete Hilfestellung zur Anwendung gegeben. Der neue Standard konkretisiert damit die Anforderungen an das Risikomanagement aus ISO/IEC 27001:2005.

Cisco Rootkits

Am 22.05.2008 stellte Sebastian Muniz auf der EuSecWest in London ein funktionsfähiges Rootkit für Cisco IOS vor. Dessen Wirksamkeit wurde inzwischen durch eine offizielle Stellungnahme des Herstellers bestätigt. Einen Tag zuvor hatte Cisco drei außerplanmäßige Patches veröffentlicht, die mit der IOS-Rootkit-Thematik zusammenhängen dürften. Insbesondere der Cisco IOS SSHService Denial of Service-Fehler wird als reengineer-bar eingestuft, daher sollte mit Angriffen auf diese Schwachstelle gerechnet werden. Wir empfehlen, betroffene Systeme umgehend zu patchen.

Automatische Exploits

David Brumley, Pongsin Poosankam, Dawn Song, und Jiang Zheng veröffentlichten am 18.04.2008 einen Ansatz zur automatischen Erzeugung von Exploits aus Patches. Die Kernidee: Sie vergleichen das gepatchte mit dem ursprünglichen Programm. Identifizieren sie dabei beispielsweise eine Input-Validierung, so erzeugen sie daraus Angriffscode, der gegen genau diese Validierung verstößt – und können nun jedes ungepatchte System attackieren. Zwar lassen sich mit diesem Ansatz (noch) nicht alle Exploits zu jedem Patch finden; für ausgewählte Microsoft-Patches konnten sie jedoch in weniger als 30 Sekunden funktionsfähige Exploits gewinnen. Sollte dieser Ansatz weiter entwickelt werden, könnten Hersteller und Anwender in Zugzwang geraten und müssten sich um geeignete Gegenmaßnahmen und zügigeres Patchen bemühen.

PTK Forensics

Seit dem 30.05.2008 läuft der öffentliche Beta-Test für PTK – eine neue, völlig überarbeitete graphische Benutzeroberfläche für das altehrwürdige Forensik-Tool The Sleuthkit (TSK). Dabei handelt es sich nicht bloß um eine aktuellere Version der bereits etwas in die Tage gekommenen Sleuthkit-Benutzeroberfläche Autopsy. Die Entwickler der italienischen DF LABS srl wollten vielmehr komplett neue Funktionen zur Verfügung stellen.

Wir haben das Tool einem ausgiebigen Test unterzogen. Vor der eigentlichen Analyse extrahiert die neue "Indexing Engine" Textpassagen, sucht nach bekannten Dateitypen, führt File-Carving durch, berechnet bei Bedarf kryptographische Prüfsummen und legt die Ergebnisse in einer SQL-Datenbank ab. Anschließend kann der Forensiker über eine Ajax-basierte Web-Schnittstelle auf zahlreiche Funktionen zugreifen. Dabei überzeugen Features wie die "Gallery", die eine Vorschau auf gefundene Bilder erlaubt, oder eine nützliche "Bookmark"-Funktion zur Hervorhebung wichtiger Suchtreffer.

Der Beta-Test läuft bis September 2008. Da es gelegentlich zu Fehlermeldungen kommt und noch nicht alle Funktionen aus TSK und Autopsy implementiert sind, stellt PTK zur Zeit noch keinen vollwertigen Ersatz dar.

Exponierte Leittechnik

Nun ist es ja nicht so, dass analoge Leittechnik unangreifbar wäre: Ein durchgetrenntes Kabel kann die Verfügbarkeit von Anlagen gefährden, und das

Drehen an einem Potentiometer könnte Signale verfälschen. Allein der Umstand, dass man hierzu einen physikalischen Zugriff vor Ort benötigt, erschwert derartige Angriffe erheblich. Anders sieht es dagegen bei der digitalen Leittechnik aus: Durch TCP/IP verbundende Systeme können über hunderte von Kilometern hinweg beeinflusst werden.

Schutz bieten hier durchdachte Netzwerk-Zonenkonzepte und entsprechend restriktiv konfigurierte Firewalls. Dass es daran gelegentlich mangelt, zeigen die Feststellungen der US-amerikanischen Überwachungsbehörde Government Accountability Office (GOA) bei einem der größten Energieversorger, der Tennessee Valley Authority (TVA); nachlesbar in einem Prüfbericht vom 21.05.2008. Darin werden unter anderem Verbindungen zwischen Anlagennetzen und Office-Netzsegmenten und zu offen konfigurierte Firewallsysteme bemängelt. Kein Wunder, dass in den USA die Angst vor einem Hacker-Angriff auf die Energieversorgung umgeht.

Reaktorabschaltung per Patch

Am 05.06.2008 wurde ein peinlicher Zwischenfall in einem amerikanischen Atomkraftwerk bekannt: Ein Service-Techniker hatte im Kraftwerk Hatch auf einem PC im Office-Netzsegment ein Update installiert, das durch eine fehlerhafte Synchronisierung Daten auf einem Kontrollsystem im Anlagennetz löschte. Die fehlenden Daten wurden von den Schutzsystemen des Reaktors als zu niedriger Kühlwasserstand interpretiert – und daher eine Notabschaltung ausgelöst, so die Darstellung im NRC-Bericht (Nuclear Regulatory Commission).

Zwar ist zu hoffen, dass ein solcher Vorfall in einem deutschen Kraftwerk nicht möglich wäre. Aber beunruhigend ist auch schon die Vorstellung, dass ein einfaches Systemupdate solche Aktionen auslösen kann – selbst bei einem 7.400 km entfernten Kernkraftwerk.

Nessus-Lizenz

Der Security-Scanners Nessus, einstmals Open Source, seit 2005 als Closed Source weiterentwickelt (vgl. SSN 02/2005), erfreut sich auch in Unternehmen großer Beliebtheit. Mit dem bisherigen Nutzungsmodell, nach dem Updates und Plugins mit etwas Verzögerung kostenfrei zum Download bereitgestellt wurden, ist es für den kommerziellen Einsatz am 31.07.2008 vorbei: In einem Schreiben informierte der Hersteller Tenable registrierte Nutzer am 14.05.2008 über die bevorstehenden Änderungen der Lizenzbedingungen.

Ab dem 01.08.2008 ist nur noch die private Nutzung kostenfrei. Auf die Reaktion der Nessus-Fangemeinde darf man gespannt sein. Vielleicht hätte Tenable lieber die Reaktion des Marktes auf die am 06.06.2008 angekündigte 33%ige Preiserhöhung des Kultgetränks Bionade (um sich so „von seinen Nachahmern abzusetzen“) abgewartet – schließlich lernt man immer am billigsten aus den Fehlern anderer. Die Kommerzialisierung von Nessus dürfte dem vom BSI unterstützen und am 21.05.2008 auf dem LinuxTag 2008 vorgestellten Projekt OpenVAS Vortrieb leisten: einem auf Basis der letzten frei verfügbaren Quellen von Nessus entwickelten kostenfreien Security-Scanner.

Secorvo News

Secorvo College aktuell

Vom **01.–03.07.2008** entführen Stefan Kelm, Stefan Gora und Jochen Schlichting in die Tiefen der Forensik – inklusive praktischer Übungen an elementaren Tools und einer Einführung in den rechtlichen Kontext. Der Termin ist seit einigen Wochen ausgebucht – die nächste Gelegenheit zur Teilnahme bietet sich am **11.–13.11.2008**. Interessierten empfehlen wir eine frühzeitige Anmeldung.

Das Programm des zweiten Halbjahrs beginnt nach der Sommerpause mit einer T.I.S.P.-Schulung vom **08.–12.09.2008** mit anschließender Zertifizierung. Die große Nachfrage nach dem T.I.S.P.-Zertifikat lässt erwarten, dass sich die Zahl der Absolventen in 2008 erneut verdoppelt.

Programm und Online-Anmeldung unter
http://www.secorvo.de/college

Team(ver)stärkung

Das Secorvo-Team ist zum 01.06.2008 weiter gewachsen: Alexander Göbel – T.I.S.P., CISM, CISO und BSI-zertifizierter Audit-Teamleiter für ISO 27001-Audits auf der Basis von IT-Grundschutz – bringt vieljährige Erfahrung aus dem IT-Risk-Management eines DAX-Unternehmens und der Zertifizierung eines Rechenzentrums nach ISO 27001 auf der Basis von IT-Grundschutz mit. Neben allen Facetten des Sicherheitsmanagements ist der betriebliche Datenschutz eines seiner Schwerpunktthemen.

Ebenfalls gewachsen ist die inzwischen lange Liste der Zertifizierungen der Secorvo-Consultants: Petra Barzin erhielt die Zertifizierung als CISSP, und Jochen Schlichting darf neben seinen Zertifizierungen als CISA und CISSP nun auch das CISM-Zertifikat (Certified Information Security Manager) der ISACA führen.

Veranstaltungshinweise

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

Juli 2008	
01.-03.07.	Forensik (Secorvo College)
10.07.	Die Mifare-Attacke und andere Krypto-Desaster (KA-IT-Si, Karlsruhe)
10.-11.07.	DIMVA 2008 (GI, Paris)
28.07.-01.08.	17th USENIX Security Symposium 2008 (Usenix, San José/US)
August 2008	
17.-21.08.	Crypto 2008 (IACR, Santa Barbara/US)
September 2008	
07.-10.09.	OSSCoNF 08 (IFIP, Mailand)
08.-12.09.	T.I.S.P.-Schulung (Secorvo College)
23.-25.09.	IMF 2008 (GI, Mannheim)
23.-26.09.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College)
Oktober 2008	
07.-10.10.	IT-Sicherheit heute (Secorvo College)

Fundsache

Am 09.05.2008 veröffentlichte die schweizerische Melde- und Analyse-stelle Informationssicherung (Melani) den Halbjahresbericht 2007/2, der die Entwicklung der Gefährdungslage in der Schweiz und international beleuchtet. Als Beispiel wird ein sehr professioneller Phising-Angriff auf Systeme der Schweizer Bundesverwaltung detailreich dargestellt – der die Wirkungslosigkeit des etablierten Virenschutzes aufzeigte.

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