Secorvo Security News
Mai 2004

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

Nr. 5, 3. Jhrg. 2004
Stand 28. Mai 2004

ISSN 1613-4311

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

Inhalt

Editorial: Vom Wichtigen

1 Security News

1.1 RSA-576 faktorisiert

1.2 TCP-Schwachstelle

1.3 Kommt DNSSEC?

1.4 T-Online-Authentifikation

1.5 Sicherheitsloch Schutzsoftware

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Security Awareness Symposium 2004

3 Veranstaltungshinweise

Impressum

Editorial: Vom Wichtigen

Das Wichtigste im Leben ist, zu wissen,
was das Wichtigste ist.

Otto Milo (Aphoristiker, 1902-1980)

Es ist wie im „wirklichen Leben“: Entscheidungen über Maßnahmen der IT-Sicherheit sind eine tägliche Herausforderung. Denn natürlich sind Zeit und Mittel begrenzt und damit Prioritätensetzungen unvermeidlich.

Begrenzt ist aber auch die Perspektive der beiden wichtigsten Entscheider – die des Verantwortlichen für IT-Sicherheit und die der Budget-verantwortlichen Geschäftsleitung. Schlimmer: Beide haben eine unterschiedliche Perspektive – und das liegt auch noch in der Natur der Sache.

Ein typischer Fall: Der IT-Leiter wählt für eine kritische Netz-Komponente ein Produkt mit Austausch-Garantie innerhalb weniger Stunden. Als die Geschäftsleitung das erfährt, wird sie blass: Die betroffene geschäftskritische Anwendung verträgt eine Ausfallzeit von nur wenigen Minuten.

Kern des Problems: Die Geschäftsleitung interessiert nur das Risiko, der IT-Sicherheitsverantwortliche kümmert sich um das Sicherheitsniveau. Das ist nicht dasselbe: Die Risikoperspektive zielt auf eine fallbezogene Kosten-Nutzen-Entscheidung, ob ein Risiko in Kauf genommen, transferiert (Versicherung, Outsourcing) oder durch Vorbeugung reduziert wird, nicht aber auf eine Verbesserung des Sicherheitsniveaus.

Denn das geschäftliche Risiko leitet sich nicht (allein) aus realen Bedrohungen ab, sondern muss die Kritikalität der betroffenen Anwendung für das Kerngeschäft berücksichtigen. Sicherheitsbeauftragte kennen aber häufig die maximalen Ausfallzeiten nicht, die sie für ein IT-System garantieren müssen, und der Geschäftsleitung sind die konkreten Bedrohungen der genutzten Systeme und Daten oft unbekannt.

Risiko-adäquate Prioritätensetzung in der IT-Sicherheit gelingt daher nur mit Kenntnis des „Business Impact“ betroffener IT-Systeme und Daten einerseits und deren realer Bedrohungen andererseits.

1 Security News

1.1 RSA-576 faktorisiert

Am 27.04.2004 ging die Nachricht durch die Ticker, dass die 576-bit-Challenge der Firma RSA gelöst sei. Tatsächlich wurde die 174 Dezimalstellen lange Zahl bereits am 03.12.2003 zerlegt. Die Faktorisierung gelang einem Team der Universität Bonn um Professor Franke mit Unterstützung durch das Institut für Experimentelle Mathematik in Essen und das BSI. Die verteilte Berechung erfolge auf einem Linux-Cluster mit 144 PCs (400 MHz, Pentium II) und verwendete den General Number Field Sieve-Algorithmus – mit einem Aufwand von umgerechnet 13.200 MIPS-Jahren.

Interessant dabei: Dieser Faktorisierungserfolg bestätigt die Prognose, die Secorvo vor drei Jahren auf der Basis der Faktorisierungserfolge der vergangenen 30 Jahre gestellt hat (siehe Bild), und die weit weniger dramatisch ausfiel als viele Expertenwarnungen und die Erwartung des BSI. Danach wäre 2004 erstmals die Faktorisierung einer 630 bit langen Zahl zu erwarten gewesen – was nun eher unwahrscheinlich erscheint. Selbst die frühestens für das Jahr 2020 vorausgesagte Faktorisierung eines 1024 bit langen RSA-Schlüssels könnte sich daher noch als zu pessimistische Befürchtung erweisen – allen Warnern zum Trotz, die seit Jahren Schlüssellängen von 2048 bit und mehr empfehlen oder gar das baldige Ende von RSA prophezeihen.

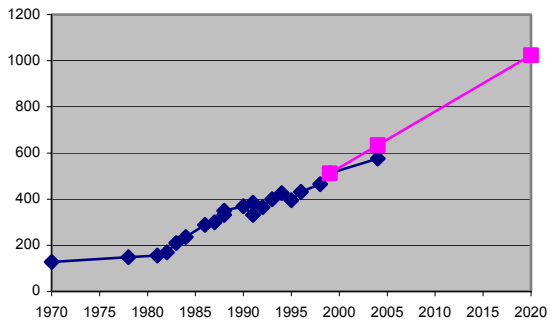

Bild: Secorvo-Prognose 2001 [BoFT_02]

1.2 TCP-Schwachstelle

Das im September 1981 in RFC 793 spezifizierte TCP (Transmission Control Protocol) ist heute das zentrale Protokoll des Internet. Da überrascht es, dass erst im Jahr 2004 eine inhärente Schwachstelle dieses Protokolls aufgedeckt wird: Der Standard erlaubt – aus guten Gründen – bestehende TCP-Verbindungen durch ein Reset-Paket (RST) abzubrechen. Diese Eigenschaft wird zur Schwachstelle, wenn das RST-Paket nicht vom einem der beiden Verbindungspartner gesendet wird, sondern von einem Dritten. Besonders kritisch ist, wenn so Verbindungen gekappt werden, über die Backbone-Router im Internet ihre Routing-Informationen austauschen. Der Angreifer muss allerdings die 32 bit lange, zum Schutz gegen dererlei Attacken zufällig gewählte so genannte Sequence-Number kennen – und dazu entweder die Verbindung belauschen oder sie erraten.

Am 20.04.2004 schlug nun das US-CERT aufgrund einer am gleichen Tag veröffentlichten Studie von Paul Watson Alarm: Häufig akzeptieren TCP-Implementierungen jede Sequence-Number in einem Fenster von 64 kB Größe. Hierdurch wird der effektiv zu durchsuchende Schlüsselraum für den Angreifer von 2^{32} auf 2^{16} Möglichkeiten reduziert. Er muss also maximal 65.536 Pakete schicken – anders als 1981 ist das heute eine Angelegenheit von nur wenigen Minuten.

Fast zeitgleich wurde von der IETF am 19.04.2004 ein Internet-Draft veröffentlicht, der diese Schwachstelle beheben soll. Pikanterweise hat Cisco ein Patent auf das dort beschriebene Verfahren eingereicht. Dieses Vorgehen wurde prompt von Open-Source-Vertretern kritisiert. In OpenBSD findet sich ein anderer Ansatz zur Behebung der Schachstelle: Dort wird die ebenfalls vom Angreifer zu ratende Quell-Portnummer nicht fortlaufend, sondern ebenfalls zufällig gewählt. So gewinnt man die fehlenden 16 bit des effektiven Schlüsselraums wieder zurück.

1.3 Kommt DNSSEC?

Eines der wichtigsten Kommunikationsprotokolle im Internet ist das Domain Name System (DNS), welches für die Zuordnung von IP-Adressen und Hostnamen verantwortlich ist. Dass DNS – genau wie alle anderen verbreiteten Protokolle, die sich des DNS bedienen – über keinerlei Sicherheitsmechanismen verfügt, ist seit Jahren bekannt; bereits Mitte der 90er Jahre wurde daher die IETF-Arbeitsgruppe DNSSEC gegründet, um das Protokoll abzusichern.

Erste technische Drafts zu DNSSEC wurden bald veröffentlicht; ebenso schnell kam man jedoch zu der Einsicht, dass zur Einführung von DNS – insbesondere auf Ebene der Root-Nameserver – vor allem organisatorische Probleme zu überwinden sind. Im Jahr 2000 untersuchte die DENIC eG mit Untersützung von Secorvo die flächendeckende Einführung von DNSSEC innerhalb der Top Level Domain .de. Die Studie kam zu dem Ergebnis, dass DNSSEC im großen Stil noch nicht einsetzbar war. Jüngst legte auch das BSI eine Studie vor, die zu vergleichbaren Resultaten kommt.

Immerhin: Der erste Schritt auf Anwendungsseite ist getan. Die neueste Version 9.3 des im Internet am häufigsten eingesetzten Nameservers BIND unterstützt die DNSSEC-Protokolle. Auch liefen erste erfolgreiche Pilotprojekte. Nun bleibt abzuwarten, ob einerseits andere Hersteller nachziehen und andererseits die wichtigen Betriebsprozesse zur Einführung von DNSSEC so etabliert werden können, dass auch Top Level Domains und die Root-Nameserver DNSSEC anbieten können. Dann erst entfalten Security-Protokolle wie SSL ihre volle Wirkung.

1.4 T-Online-Authentifikation

Die Authentifikation beim Zugriff auf E-Mail-Postfächer erfolgt bei T-Online implizit über das Einwahl-Login. Ein zusätzliches Passwort wird daher beim Zugriff auf die Mailbox nicht mehr benötigt.

Das verursacht bei T-DSL-Router-Zugängen, die von mehreren Personen genutzt werden, ein Problem: Beim Zugriff auf die T-Online-Mailbox werden automatisch die E-Mails des T-DSL-Inhabers abgerufen. Schlimmer: Gelingt es einem Nachbarn (oder „war driver“), sich in ein via T-DSL mit dem Internet verbundenes WLAN einzuklinken, hat er unmittelbaren Zugriff auf den Mail-Account des WLAN-Betreibers.

Seit Kurzem bietet T-Online daher die Möglichkeit, für den E-Mail-Account einen POP3-Passwortschutz einzurichten.

1.5 Sicherheitsloch Schutzsoftware

In den vergangenen Wochen waren wieder mehrere Sicherheitsprodukte Thema von Security Advisories. Am 13.05.2004 wurden schwer wiegende Schwachstellen der verbreiteten Norton Personal Firewall und von Norton Internet Security (Symantec) in verschiedenen Versionen aufgedeckt. Manipulierte DNS- und NetBIOS-Pakete können Heap oder Buffer Overflows und damit die Ausführung beliebigen Codes verursachen. Das Einspielen von Updates oder die Aktivierung der LiveUpdate-Funktion ist daher dringend angeraten. Nachdem am 24.05.2004 auch ein fehlerhaftes ActiveX-Control in Norton Antivirus bekannt wurde, das die Ausführung beliebigen Codes erlaubt, folgte am 26.04.2004 der Virenscanner von F-Secure: Er erkennt die aktuelle Sobig.G-Variante nicht in LHA-komprimierten Dateien – und kann über manipulierte LHA-Anhänge zum Absturz gebracht werden. Zum Schutz vor diesen Angriffen sollten die vom Hersteller für die Client- und die Serverkomponenten bereit gestellten Patches installiert werden.

Schließlich wurde am 15.05.2004 der aktuelle Source Code von Ciscos Router- und Switch-Betriebssystem IOS v12.3 im Internet publiziert. Zwar ist der Code inzwischen nicht mehr auf den Seiten von Securitylab verfügbar; mit gezielten Angriffen auf neue Schwachstellen sollte in den kommenden Wochen jedoch gerechnet werden.

2 Secorvo News

2.1 Secorvo College aktuell

Gerne hätten wir unser Ausbildungsangebot zur IT-Sicherheit schon 1999 vom Start weg mit einem international anerkannten Abschluss vervollständigt. Weil jedoch alle international verbreiteten Zertifikate sich inhaltlich entweder an der eingeschränkten Perspektive der Revision bzw. an spezifisch amerikanischen, insbesondere rechtlichen Rahmenbedingungen orientieren oder auf eine Multiple-Choice-Prüfung beschränken, bieten wir nun einen eigenen Ausbildungsgang zum „IT Security Professional“ an.

Der Ausbildungsgang orientiert sich an der an Hochschulen bewährten Kombination aus Pflicht- und Wahlveranstaltungen: Die Teilnahme an fünf Seminaren von Secorvo College, darunter „IT-Sicherheit heute“ und je ein Seminar aus den Bereichen „Grundlagen“, „Lösungen“ und „Systeme“ qualifiziert zum „IT Security Professional“.

Mit einer theoretischen und praktischen Prüfung, die ab 2005 mindestens zweimal jährlich angeboten wird, können Sie das Zertifikat zum „Certified IT Security Professional“ erwerben.

http://www.secorvo.de/college

2.2 Security Awareness Symposium 2004

Inzwischen steht das Programm des diesjährigen zweiten Security Awareness-Symposium am 29.-30.06.2004. Nach Fiducia, Münchener Rück, RWE, SAP und der Schweizerischen Armee (2003) werden in diesem Jahr BASF, BMW, FinanzIT und T-Systems über ihre Awareness-Aktivitäten berichten. Weiter steht die Frage der Nachhaltigkeit der Sensibilisierung im Mittelpunkt der Veranstaltung, zu der sich schon jetzt Sicherheitsverantwortliche zahlreicher Unternehmen angemeldet haben. Die Teilnahmegebühr liegt bei 390 € (zzgl. MwSt.).

3 Veranstaltungshinweise

Juni 2004	
07.-08.06.	IT Risk Management 2004 (COMPUAS, Köln)
13.-18.06.	16th Computer Security Incident Handling Conference, Budapest (FIRST, Budapest)
14.-15.06.	IT-Security Management (Secorvo College, Karlsruhe)
14.-18.06.	Information Security Management (Secorvo College, Karlsruhe)
22.-23.06.	Live Hacking Lab (Secorvo College, Karlsruhe)
29.-30.06.	Security Awareness Symposium 2004 (Secorvo, Karlsruhe)
August 2004	
09.-13.08.	USENIX Security Symposium (San Diego)
September 2004	
21.-22.09.	Lotus Notes Security (Secorvo College, Karlsruhe)
28.-29.09.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
28.-30.09.	ISSE 2004 (EEMA/TeleTrusT, 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