Secorvo Security News
Januar 2005

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

Nr. 1, 4. Jhrg. 2005
Stand 28. Januar 2005

ISSN 1613-4311

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

Inhalt

Editorial:
Von Hasen und Igeln

1 Security News

1.1 Aktualisiertes IT-Grundschutzhandbuch des BSI

1.2 Anti-Spyware Tool

1.3 Anfänger für Office...

1.4 DoS gegen VoIP bei IOS

1.5 Microsoft lässt Patches intensiver testen

1.6 Apple Security Update

1.7 Einheitliche Sperrung

1.8 Anti-Phishing

1.9 12. DFN-CERT Workshop

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Forensik Symposium

2.3 DuD 2005

2.4 Teamverstärkung

3 Veranstaltungshinweise

Impressum

Editorial: Von Hasen und Igeln

Sie erinnern sich? Es war einmal an einem Sonntagmorgen im Herbst... ein Märchen der Gebrüder Grimm, erzählt an Ihrem Kinderbett, oder dem Ihrer Kinder.

Haben Sie nicht auch geschmunzelt über die List des Igels, der den Wettlauf gegen den körperlich weit überlegenen Hasen gewinnt, indem er sich in die Ackerfurche duckt und abwechselnd mit seiner Frau „Ich bin schon da!“ ruft, sobald der Hase das Ziel vermeintlich als Erster erreicht?

Zu denken hat mir damals gegeben, dass mein Großvater zu sagen pflegte: "Wahr muss die Geschichte sein, mein Sohn, sonst könnte man sie ja nicht erzählen.“

Und tatsächlich, da stellt sich, Jahrzehnte später, mit Blick auf das wirkliche Leben ein Déjà-vu ein. Der IT-Nutzer ruft: „Ich brauche einen sicheren Internetzugang“ – und Sie starten, installieren Firewall, Virenscanner und Spamfilter. Sie sind noch nicht fertig, da ruft er schon: „Ich brauche einen sicheren Laptop“ – und Sie sorgen für einen VPN-Tunnel, Personal Firewall und Festplattenverschlüsselung. Es ist noch nicht alles lauffähig, da ruft er bereits: „Meine E-Mails will ich auf meinem BlackBerry lesen“ – verschlüsselt natürlich. Und Sie rennen los und...

Eigentümlich nur, dass mir dabei meine kindliche Sympathie für den ob seiner krummen Beine verhöhnten und sich listig rächenden Igel ein wenig abhanden gekommen ist. Spielt nicht der Hase fair, indem er sich an die Regeln hält und alles gibt? Und ist nicht in Wahrheit der Igel grausam, nicht der erst hochnäsige Hase?

Auch aus diesem Märchen lässt sich also etwas fürs Leben lernen:

Erstens: Wenn die Igel nicht gestorben sind, leben sie noch heute. Zweitens: Eine höhere Geschwindigkeit löst nicht das Problem, sondern verkürzt die Lebenserwartung des Hasen.

Und drittens: Wer nicht auf dem Feld verenden möchte, sollte sich gelegentlich auch einmal in die Ackerfurche ducken.

1 Security News

1.1 Aktualisiertes IT-Grundschutzhandbuch des BSI

Am 10.01.2005 wurde eine aktualisierte Version des Grundschutzhandbuchs auf den Webseiten des BSI im PDF-Format zum Download bereit gestellt. Die HTML-Version soll in Kürze folgen. Neu hinzu gekommen sind die Bausteine „Router und Switches“, „S/390 und zSeries“ sowie „PDA“; der Baustein Sicherheitsgateway (Firewall) wurde überarbeitet. Das Grundschutzhandbuch deckt damit weitere wichtige Systeme ab – wird damit aber zugleich immer umfangreicher und komplexer. Daher wird über eine Ersetzung der inzwischen eher untertriebenen Bezeichnung „Grund“-Schutz diskutiert.

Fakt ist: Wer nach IT-Grundschutz zertifiziert ist, hat in der Regel ein hohes IT-Sicherheitsniveau erreicht. Kombiniert mit adäquatem Sicherheitsmanagement und ergänzenden Maßnahmen für besonders gefährdete Systeme sorgt Grundschutz für einen umfassenden Schutz der Unternehmens-IT.

1.2 Anti-Spyware Tool

Unter den am 11.01.2005 von Microsoft veröffentlichten Sicherheitspatches für XP findet sich die Beta-Version eines Anti-Spyware-Tools (MAS). Es erlaubt sowohl eine kontinuierliche als auch eine Anlass bezogene Untersuchung des PC auf verdächtige Programme.

Durch den Kauf der Firma Giant Ende 2004 verfügt Microsoft nun nicht nur über spezielles Spyware-Know-How, sondern auch über ein Programm, das grundsätzlich als umfassende Schädlingserkennungs-Engine ausgelegt ist: Es untersucht Registry und Systembibliotheken auf bekannte Spyware, prüft ausgewählte Konfigurationseinstellungen und arbeitet mit einer aktualisierbaren Signaturdatenbank – das Grundgerüst eines jeden Virenschutzprogramms.

Daher sprießen bereits die Gerüchte, Microsoft wolle doch noch in den Virenschutz-Markt einsteigen. Genährt wird dieser Verdacht dadurch, dass die genannten Sicherheitspatches – etwas versteckt – ein zweites Tool enthalten: ein „Malicious Software Removal Tool“, das nicht allein die in der Vergangenheit für ausgewählte Viren bereit gestellten Deinstallationstools zusammenfasst, sondern zusätzlich im Hintergrund versucht, ein erneutes Auftauchen dieser Viren zu erkennen.

1.3 Anfänger für Office...

...statt Office für Anfänger: In einem am 10.01.2005 bei der International Association for Cryptologic Research eingereichten Papier enthüllt ein Forscher aus Singapur, dass Microsoft bei der Verschlüsselung von Dokumenten in Office dieselbe Schlüsselfolge mehrfach verwendet. Dies gilt unter Kryptologen als typischer Anfängerfehler und sorgt dafür, dass Dokumente trotz starker 128-Bit RC4-Verschlüsselung unter Umständen leicht entschlüsselt werden können.

Bei Motoren gilt die alte Weisheit „Hubraum ist durch nichts zu ersetzen, außer durch mehr Hubraum!“. Bei Entwurf und Review eines Sicherheitskonzepts gilt dies analog – für langjährige Erfahrung.

1.4 DoS gegen VoIP bei IOS

Wie nicht anders zu erwarten, weisen auch moderne Voice-over-IP Systeme Schwachstellen auf. Da es sich dabei „nur“ um IT-Systeme handelt, trifft man auch hier auf bekannte Lücken durch fehlerhafte Implementierungen und Protokollschwächen. Jüngstes Beispiel ist ein von Cisco am 19.01.2005 veröffentlichtes Security Advisory: Bei Telephony Service (ITS), Call-Manager Express (CME) und Survivable Remote Site Telephony (SRST) bestimmter IOS-Versionen kann mit präparierten Nachrichten ein Reboot des Systems ausgelöst werden. Per „Dauerbeschuss“ lässt sich so ein ausgewachsener Denial-of-Service-Angriff durchführen. Es wird empfohlen, die aktuellen Updates baldigst einzuspielen.

1.5 Microsoft lässt Patches intensiver testen

Wie die Zeitschrift eWeek am 12.01.2005 berichtete, startet Microsoft ein „Security Update Validation Program“: Zukünftig sollen Sicherheitspatches nicht nur von Microsoft selbst und wenigen Großkunden getestet, sondern an weitere externe Beta-Tester verteilt werden. Hierdurch sollen in der Vergangenheit aufgetretene Problemfälle vermieden und die Qualität der Patches – und damit auch die Sicherheit – gesteigert werden. Das Programm verdient weitere Beobachtung; der Erfolg wird sich an den bei künftigen Patches auftretenden Problemen erweisen müssen.

1.6 Apple Security Update

Nicht nur Windows braucht Patch Management: Am 25.01.2005 veröffentlichte Apple das erste Security Update des Jahres für das hauseigene Betriebssystem Mac OS X.

Dabei wurde zugleich die vorher Datumsbasierte Bezeichnung der Security Updates auf eine laufende Nummer (2005-001) umgestellt – eine ebenso einfache wie wirkungsvolle Maßnahme, um Anwendern die Prüfung zu erleichtern, ob alle Updates bereits eingespielt wurden.

1.7 Einheitliche Sperrung

Die Regulierungsbehörde für Telekommunikation und Post (RegTP) hat am 21.12.2004 dem Sperr e. V. – Verein zur Förderung der Sicherheit in der Informationsgesellschaft – die bundeseinheitliche Telefonnummer 116 116 für die Sperrung von EC-, Kredit- Handy-, Krankenkassen- und Kundenkarten zugeteilt. Die Rufnummer muss 180 Tage ab Zuteilung, also ab Anfang Juli 2005 (im Inland entgeltfrei) erreichbar sein.

1.8 Anti-Phishing

Am 20.01.2005 veröffentlichte die Anti-Phishing Workung Group einen Report über die erkannten Phishing-Aktivitäten im Dezember 2004. Demnach werden die meisten der gefälschten Server zum ab„phish“en von Passwörtern nicht, wie man vielleicht erwarten könnte, in Osteuropa, Fernost oder Offshore-Steuerparadiesen installiert, sondern in den USA.

Diese Server waren durchschnittlich nur 5,9 Tage am Netz – daher ist bei Phishing-Attacken vor allem die erste Woche nach deren Auftreten kritisch. Daraus erklärt sich auch, dass einschlägige E-Mails oft an überdeutlichen Hinweisen auf ihre vorgeblich besondere Dringlichkeit zu erkennen sind.

Einen anderen Weg der Phishing-Detektion gehen, wie am 21.01.2005 gemeldet wurde, die Entwickler des Mozilla Mail-Clients Thunderbird: Sie wollen den Anwender warnen, wenn er eine in der Mail enthaltene URL anklickt, bei der z. B. anstelle des im Text angezeigten Hostnamens eine IP-Adresse hinterlegt ist. Umstritten ist jedoch, wie diese Warnung einem Endanwender verständlich vermittelt werden kann...

1.9 12. DFN-CERT Workshop

Die wichtigste deutsche Security-Konferenz wirft wieder einmal ihre langen Schatten voraus: Bereits zum zwölften Mal wird am 2. und 3. März im Kongresszentrum (CCH) in Hamburg der zweitägige DFN-CERT/ PCA-Workshop stattfinden. Das auch diesmal sehr viel versprechende Programm dürfte auch 2005 wieder deutlich mehr als 300 interessierte Teilnehmer aus Forschung, Unternehmen und Behörden anlocken und zum Diskutieren anregen.

Als eingeladener Sprecher konnte Lance Spitzner gewonnen werden, der vor allem für das Projekt „Honeynet“ verantwortlich zeichnet. Auch die anderen Vorträge versprechen interessante Themen auf hohem Niveau.

2 Secorvo News

2.1 Secorvo College aktuell

Secorvo College startet in das Jahr 2005 nicht nur mit einem um vier neue Seminare

erweiterten Angebot, sondern auch mit verkürzten Reisezeiten für Sie: Das neue Domizil von Secorvo liegt in Fußweite vom Karlsruher Hauptbahnhof (300 m) und fünf Autominuten von der A5.

Die Seminare im Februar geben einen Überblick über die IT-Sicherheit heute und vertiefen das zunehmend wichtige Thema Information Security Management (Anmeldung).

http://www.secorvo.de/college

2.2 Forensik Symposium

Secorvo veranstaltet im Rahmen der Karlsruher IT-Sicherheitsinitiative und in Kooperation mit Viccon am 01.-02.03.2005 das Computer Forensik Symposium 2005. Die systematische „virtuelle Spurensicherung" hat in den beiden vergangenen Jahren mit der Zunahme erfolgreicher Angriffe auf die IT-Infrastrukturen von Unternehmen spürbar an Bedeutung gewonnen. Das Programm des Symposiums beleuchtet das Thema erstmals von allen Seiten – aus der Perspektive der Strafverfolgung, der Unternehmenspraxis, der Technik und der „best practices".

2.3 DuD 2005

Inzwischen steht das Programm der diesjährigen siebten Konferenz „Datenschutz und Datensicherheit – DuD 2005", konzipiert und geleitet von den Herausgebern der Fachzeitschrift DuD. Sie findet am 18.-19.04.2005 in alter Tradition im Berliner Dorint-Hotel Schweizerhof statt; eine rechtzeitige Anmeldung wird empfohlen (die Teilnehmerzahl ist auf 100 begrenzt).

2.4 Teamverstärkung

Seit Mitte Januar ergänzt Ralph Wiedemann das Secorvo-Team: Er bringt mehrjährige Berufserfahrung als IT-Sicherheitsverantwortlicher, Berater und Projektleiter für IT-Security mit und verstärkt unser Know-How rund um Firewalls, PKI-basierte VPNs, Security-Audits, Intrusion Detection und Security Policies.

3 Veranstaltungshinweise

Februar 2005	
15.-17.02.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
21.-22.02.	IT-Security Management (Secorvo College, Karlsruhe)
21.-25.02.	Information Security Management (Secorvo College, Karlsruhe)
März 2005	
01.-02.03.	Computer Forensik Symposium 2005 (KA-IT-Si, Karlsruhe)
02.03.	Datenschutz kompakt (Secorvo College, Karlsruhe)
02.-03.03.	DFN-CERT Workshop (DFN-CERT, Hamburg)
15.-16.03.	D-A-CH Security 2005 (GI/OCG/ BITKOM/SI/TTT, TU Darmstadt)
April 2005	
05.-07.04.	Sichere E-Mail-Kommunikation (Secorvo College, Karlsruhe)
05.-08.04.	Sicherheit 2005 (GI, Regensburg)
12.-13.04.	Lotus Notes Security (Secorvo College, Karlsruhe)
14.04.	Lotus Notes Security advanced (Secorvo College, Karlsruhe)
18.-19.04.	Datenschutz und Datensicherheit – DuD 2005 (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
Ettlinger Straße 12-14
D-76137 Karlsruhe
Tel. +49 721 225 171-0
Fax +49 721 225 171-100

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

Secorvo Security News
Februar 2005

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

Nr. 2, 4. Jhrg. 2005
Stand 24. Februar 2005

ISSN 1613-4311

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

Inhalt

Editorial: Wer dreimal lügt...

1 Security News

1.1 SHA-1 – Gebrochen?

1.2 SigG-Algorithmen

1.3 Riskmanagement-Studie

1.4 Neue Schläuche bei RFID

1.5 Netfilter IP-Tables 1.3

1.6 Nessus übernommen

1.7 Suse mit EAL 4-Zertifikat

1.8 VoIP Security

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Forensik kompakt

2.3 DuD – das Programm

3 Veranstaltungshinweise

Impressum

Editorial: Wer dreimal lügt...

Wieder einmal wird eine (Krypto-)Sau durchs Dorf getrieben. Diesmal haben die Hashfunktionen Jagdsaison. Zum zweiten Mal steht der „Secure Hash Standard“ (SHA) des NIST auf der Abschussliste: Schon 2004 geisterten Gerüchte durch die Gazetten, SHA sei gebrochen. Tatsächlich waren Schwachstellen der ursprünglichen, vom NIST bereits 1995 ersetzten Version SHA-0 gefunden worden. „Hilfe, der Wolf kommt!“ – der erste Fehlalarm.

Jetzt hat es jedoch den SHA-1 erwischt. Bruce Schneier löste am 15.02.2005 mit einem Eintrag in seinem Blog („SHA-1 has been broken“) die zweite Welle der „Hilfe, der Wolf kommt!“-Alarme aus. Vier chinesische Forscher hatten ein kryptographisch bemerkenswertes Ergebnis angekündigt: Mit einem Aufwand von 2^{69} sei es möglich, SHA-1-Kollisionen zu finden. Dies ist allerdings ein Aufwand, der deutlich jenseits eines praktikablen Angriffs liegt – und nur zwei beliebige, keineswegs sinnvolle Zeichenfolgen liefert, die denselben Hash-Wert besitzen. Zweiter Fehlalarm.

Die Erfahrung der vergangenen Jahre hat jedoch gezeigt, dass ein solcherart angeschossener Algorithmus schon bald tatsächlich erlegt sein kann. Fatal wäre allerdings, wenn der SHA das Schicksal des Hashalgorithmus MD5 teilen würde: Auch beim MD5 gab es zwei Fehlalarme; der dritte Alarm Mitte 2004, nach dem Kollisionen mit einem Workstation-Cluster in weniger als einer Stunde konstruiert werden können, wurde überhört: Noch immer verwenden zahlreiche kryptographische Anwendungen und Produkte den MD5 als Hash-Algorithmus.

Sollte ein dritter, berechtigter „Hilfe, der Wolf kommt!“-Alarm beim SHA-1 ungehört verhallen, droht allerdings ein GAU – denn zum SHA-1 gibt es derzeit fast keine standardisierte und vor allem in Anwendungsstandards wie z. B. S/MIME berücksichtigte Alternative.

Der einzige Unterschied zwischen dieser Geschichte und dem Gleichnis mit dem Wolf: Die „Hilfe“-Rufer würden überleben.

1 Security News

1.1 SHA-1 – Gebrochen?

Ausgelöst durch einen Weblog-Eintrag des Krypto-Experten Bruce Schneier verbreitete sich am 15.02.2005 wie ein Lauffeuer die Nachricht, dass es einem renommierten chinesischen Forscherteam um Xiaoyun Wang gelungen ist, die Krypto-Hashfunktion SHA-1 zu brechen. Die Aufregung ist verständlich, wenn man bedenkt, dass SHA-1 ein zentraler Baustein für PKI-Zertifikate und -Anwendungen wie z.B. digitale Signaturen, SSL oder S/MIME ist.

Das Papier von Wang und Kollegen ist noch nicht öffentlich verfügbar. Soweit die Fakten mittlerweile bekannt sind, bedeutet „gebrochen", dass ein theoretischer Durchbruch gelungen ist: Der Aufwand zum Finden zweier verschiedener Klartexte, die denselben 160-Bit SHA-1-Hashwert besitzen, konnte von 2^{80} für eine Brute-Force-Attacke auf 2^{69} Schritte verringert werden. Letzteres erscheint z.B. im Vergleich mit dem mehr als vier Jahre dauernden „Brute-Forcing" von 2^{64} RC-5 Schlüsseln deutlich jenseits des heute praktisch Machbaren.

Zweifel an der Sicherheit des SHA-1 waren bereits aufgekommen, als auf der Expertenkonferenz Crypto 2004 mehrere Forschergruppen neue Angriffe auf Hashfunktionen vorstellten. Als Reaktion hierauf kündigte das NIST, Urheber des SHA-1, bereits am 25.08.2004 an, spätestens 2010 den SHA-1 zugunsten der designierten Nachfolger SHA-224 bis SHA-512 (jüngster SHA-Standard vom 01.08.2002) auslaufen zu lassen.

Das Dilemma für den Anwender ist, dass derzeit praktisch keine Alternativen zur Verfügung stehen: MD4 und MD5 wurden effektiv gebrochen (siehe auch SSN 12-04), RIPEMD-160 ist kaum verbreitet und nach ähnlichen Prinzipien aufgebaut wie SHA-1 (also eventuell auch ähnlich anfällig), und die jüngeren Algorithmen SHA-224/256/384/512 (auch als „SHA-2" bezeichnet) wurden bislang erst in wenige Produkte integriert.

Handlungsbedarf besteht also, aber Panik ist nicht angezeigt. Selbst wenn die Attacke in Einzelfällen praktisch umsetzbar wäre, erlaubt sie es nicht, einen zweiten Klartext zu finden, der zu einem vorgegebenen Hashwert – z.B. aus einem existierenden CA-Zertifikat – passt, sondern erzeugt „nur" zwei zunächst zufällige Zeichenfolgen so, dass deren Hashwerte (und damit auch die Signaturen) übereinstimmen. Somit sind bereits geleistete Signaturen ohnehin nicht gefährdet.

Am dringlichsten sind die Hersteller von Signaturanwendungen gefordert, alternative Hash-Algorithmen in ihre Produkte aufzunehmen. Als einer der ersten Hersteller hat PGP am 18.02.2005 die Gelegenheit ergriffen, ein Update anzukündigen.

1.2 SigG-Algorithmen

Noch ohne Kenntnis der neuesten Ergebnisse zum SHA-1 gab die RegTP am 02.01.2005 die Übersicht über geeignete Algorithmen nach dem Signaturgesetz bekannt. Wie auch durch das NIST wird darin dem SHA-1 eine (nun möglicherweise zu überdenkende) Lebenszeit bis 2010 gegeben. Zulässige Alternativen als Hashfunktion sind RIPEMD-160 und SHA-2.

1.3 Riskmanagement-Studie

Das Institut für Wirtschafts- und Verwaltungsinformatik von Prof. Dr. Hampe an der Universität Koblenz führt ab dem 24.02. 2005 eine Delphi-Studie zum IT Riskmanagement durch. Ziel dieser Studie ist es, Trends und Entwicklungen im Bereich des IT Risk Managements zu ermitteln. Die Studie richtet sich ausschließlich an Fachexperten, daher ist eine Teilnahme nur mit den folgenden Login-Daten möglich: Kennung: itrm, Passwort: mrti. Für weitere Informationen steht die Projektleiterin, Frau Meletiadou (0261/287-2535) zur Verfügung.

1.4 Neue Schläuche bei RFID

Am 28.01.2005 veröffentlichte ein Forscherteam der Johns Hopkins University

und der RSA Laboratories die – auch praktisch umgesetzte – Analyse eines RFID-Chips von Texas Instruments, der u.a. in Wegfahrsperren häufig eingesetzt wird.

Angesichts der Verwendung eines 40-Bit-Schlüssels, der eine Brute-Force-Suche ermöglicht, ließe sich dies als alter Wein (oder eher Essig) in neuen RFID-Schläuchen abtun. Bemerkenswert daran sind jedoch mehrere Punkte: Die Bereitschaft zur Kooperation des Herstellers (anstelle eines leider häufigen peinlichen Schweigens oder Abstreitens), die von den Autoren beschriebene Black-Box Rekonstruktion des im Chip verwendeten Algorithmus und die Überlegungen, wie man sich als Träger eines RFID-Chips vor unbeabsichtigtem Auslesen der darauf gespeicherten Daten schützen kann. Letzteres könnte eine neue Klasse von Produkten oder Werbe-Giveaways hervorbringen: einfach zu handhabende Faradaysche-RFID-Hüllen – womit sich der Kreis zu den Schläuchen schließt.

1.5 Netfilter IP-Tables 1.3

Das Netfilter-Team um Harald Welte hat am 12.02.2005 die Version 1.3 von iptables freigegeben. Die im Linux Kernel integrierten Funktionen ermöglichen eine stateful Paketfilterung und eine Reihe weiterer (Firewall)-Funktionen. In Version 1.3 wurden Bugs beseitigt und die Performance nochmals verbessert.

1.6 Nessus übernommen

Der verbreitete OpenSource-Scanner Nessus wurde unter die Hoheit von Tenable Network Security als offiziellem Sponsor gestellt. Tenable ist der Hersteller der kostenpflichtigen Windows32-Variante des Security Scanners (NeWT Pro), die kostenfreie Variante NeWT ist auf das lokale Subnetz beschränkt.

Nach einer Benutzerregistrierung kann Nessus weiterhin kostenfrei unter Linux und anderen Unix-Plattformen eingesetzt werden. Allerdings werden aktuelle Plugins von Tenable erst nach einer Wartezeit von sieben Tagen zur Verfügung gestellt. Wer die Plugins sofort einsetzen möchte, muss den „Direct Feed Update Service“ zum Preis von 1.200 $ pro Jahr buchen. Die unter der Gnu Public Licence (GPL) von der Community erstellten Plugins sind auch weiterhin ohne Verzögerung und kostenfrei erhältlich.

1.7 Suse mit EAL 4-Zertifikat

Am 15.02.2005 teilte die atsec information security GmbH mit, dass sie für Suse's Linux Enterprise Server 9 (SLES 9) den Prozess der Evaluierung nach Common Criteria (CC) EAL 4+ abgeschlossen habe und ein entsprechendes Zertifikat folgen werde.

EAL 4+ ist ein hohes Evaluationslevel; diese Stufe wird auch für Chipkarten nach dem Signaturgesetz (SigG) verlangt. Eine fundierte Beurteilung einer CC-Evaluierung ist jedoch nur unter Berücksichtigung des der Prüfung zu Grunde liegende Kriterienkatalogs („Protection Profile“) möglich, in dem die Prüfanforderungen definiert sind.

SLES 9 wurde in diesem Fall gegen das Schutzprofil „Controlled Access Protection Profile (CAPP)“ geprüft, welches insbesondere Anforderungen an die Zugriffskontrolle definiert. Auch Windows 2000 wurde bereits gegen CAPP EAL 4 evaluiert – genau diese Evaluierung führte jedoch vor einigen Jahren zu massiver Kritik an dem Schutzprofil: Bei genauerer Betrachtung gilt es nämlich nicht in üblichen Netzwerk-Umgebungen wie dem Internet („*The profile is not intended to be applicable to circumstances in which protection is required against determined attempts by hostile and well funded attackers...*“).

1.8 VoIP Security

Am 07.02.2005 wurde unter der Federführung von Tippingpoint die Voice Over IP Security Alliance (VOIPSA) ins Leben gerufen. Die Gruppe hat sich zum Ziel gesetzt, das Thema Security im Bereich VoIP vorwärts zu bringen.

Vom National Institute of Standards and Technology (NIST) ist seit dem 03.01.2005

ein Whitepaper zum Thema "Security Considerations in Voice over IP Systems" verfügbar. Neben technischen Grundlagen werden insbesondere die Sicherheitsfunktionen der Protokolle und auch die Integration mit weiteren Schutzmechanismen wie Firewalls und VPN dargestellt.

2 Secorvo News

2.1 Secorvo College aktuell

Im April stehen zahlreiche Seminarangebote auf der Agenda von Secorvo College:

- drei aktuelle Seminare zur Systemsicherheit: Sichere E-Mail-Kommunikation (05.-07.04.) Lotus Notes Security (12.-13./14.04.) und Inside Windows Security (19.-20.04.2005), sowie
- eine in Zusammenarbeit mit dem Unternehmen Compass Security Network Computing AG (Schweiz) entwickelte „Hands on" Seminarreihe: Live Hacking Lab (26.-28./29.04.2005) und Web-Application Security (02.-04.05. 2005).

Veranstaltungsprogramme, das vollständige Seminarangebot mit weiteren Terminen und ein Anmeldeformular finden Sie auf den Webseiten von Secorvo College.

2.2 Forensik kompakt

In der kommenden Woche findet das erste Computer Forensik Symposium der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) bei Secorvo in Karlsruhe statt (01.-02.03. 2005). Themen sind die Sichtweisen und Erfahrungen von Staatsanwaltschaft, BKA und betroffenen Unternehmen sowie die Vorstellung von Forensik Tools und deren praktischem Einsatz. Die zahlreichen Anmeldungen versprechen spannende Diskussionen. Für Kurzentschlossene gibt es noch einige wenige freie Plätze.

2.3 DuD – das Programm

Das Programm der Fachkonferenz „Datenschutz und Datensicherheit" (DuD, 18.-19. 04.2005) ist jetzt verfügbar.

3 Veranstaltungshinweise

März 2005	
01.-02.03.	Computer Forensik Symposium 2005 (KA-IT-Si, Karlsruhe)
02.-03.03.	DFN-CERT Workshop (DFN-CERT, Hamburg)
15.-16.03.	D-A-CH Security 2005 (GI/OCG/ BITKOM/SI/TTT, TU Darmstadt)
April 2005	
05.-07.04.	Sichere E-Mail-Kommunikation (Secorvo College, Karlsruhe)
05.-08.04.	Sicherheit 2005 (GI, Uni Regensburg)
12.-13.04.	Lotus Notes Security (Secorvo College, Karlsruhe)
14.04.	Lotus Notes Security advanced (Secorvo College, Karlsruhe)
18.-19.04.	Datenschutz und Datensicherheit – DuD 2005 (COMPUTAS, Berlin)
19.-20.04.	Inside Windows Security (Secorvo College, Karlsruhe)
26.-28.04.	Live Hacking Lab (Secorvo College, Karlsruhe)
29.04.	Live Hacking Spezial (Secorvo College, Karlsruhe)
Mai 2005	
02.-04.05.	Web-Application Security (Secorvo College, Karlsruhe)

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
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

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

Secorvo Security News
März 2005

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

Nr. 3, 4. Jhrg. 2005
Stand 29. März 2005

ISSN 1613-4311

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

Inhalt

Editorial:
Vom Suchen und vom Finden

1 Security News

1.1 Kollidierende Zertifikate

1.2 Haftungsrisiken

1.3 NIST SP 800-53

1.4 Microsoft im Fadenkreuz

1.5 Kompass der IT-Sicherheitsstandards

1.6 Knack' den Knacker

1.7 Data-Mining the NSA

2 Secorvo New

2.1 Secorvo College aktuell

2.2 security-finder.de

3 Veranstaltungshinweise

Impressum

Editorial:
Vom Suchen und vom Finden

Nicht erst seit der Proklamation des „lebenslangen Lernens" wissen wir: Die Halbwertzeit unserer Kenntnisse ist oft überraschend kurz. Erst recht im Gebiet IT-Sicherheit müssen wir immer wieder feststellen, dass manch mühsam erworbene und lieb gewonnene Erkenntnis durch neue Entwicklungen Makulatur wird. Nicht nur Hashfunktionen, Verschlüsselungsverfahren und kryptoanalytische Erkenntnisse jagen einander, auch neue Technologien halten uns in Atem – und die Security-Ticker in Bewegung. Da bleibt wenig Anderes, als mit der Entwicklung zu gehen, denn Stagnation in Sicherheitsfragen kann schwer wiegende Folgen haben.

Wie aber bleibt man „auf dem Laufenden"? Unter den Bedingungen knapper Zeitressourcen helfen allein aktuelle, konzentrierte, verständliche und fundierte Informationsmaterialien. Nur: Wo findet man die?

Meist geht inzwischen der Griff zur Tastatur statt zum Buch. Das zeigt eine aktuelle Befragung von 400 DAX-30-Managern: Für 94% ist das Internet die wichtigste Informationsquelle, 84% verbringen eine bis vier Stunden wöchentlich mit der Informationsrecherche (imc, 2005).

Zwar gilt auch für das Internet das Bibelwort: *„... wer da suchet, der findet"* (Matthäus, 7. Kapitel, Vers 8). Nur findet er nicht unbedingt auch das Gesuchte. Denn eines verrät keine Suchmaschine: Ob ein gefundenes Dokument informativ, verständlich und fachlich fundiert ist. Diesem Mangel kann man nur mit viel Leseaufwand begegnen.

Auch wir mussten uns dieser Herausforderung stellen. So ist bei Secorvo ein Informationspool aus vielen hundert ausgewählten Dokumenten entstanden. Den Zugriff auf diese „virtuelle Bibliothek" ermöglichen wir nun unter http://www.security-finder.de/ – den Lesern der Security News bis zum 10. April 2005 unentgeltlich (Login: „SSN-01", Passwort: „security-finder"). Wir freuen uns auf Ihre Rückmeldungen.

1 Security News

1.1 Kollidierende Zertifikate

Für viel Wirbel hat am 01.03.2005 die Publikation eines Forscherteams gesorgt, dem es gelungen ist, zwei unterschiedliche X.509-Zertifikate zu erzeugen, die denselben MD5-Hashwert liefern. Obwohl die Existenz von MD5-Kollisionen schon seit geraumer Zeit bekannt ist, waren praktische Angriffe selten – bis jetzt: Lenstra, Wang und de Weger präsentierten zwei Beispielzertifikate mit unterschiedlichem Public Key aber demselben MD5-Hashwert.

Die praktischen Auswirkungen dieses Angriffs sind dennoch gering: Ein Angreifer müsste eine vertrauenswürdige Zertifizierungsinstanz (CA) dazu bringen, das vorbereitete Zertifikat zu signieren, ohne eine Änderung daran vorzunehmen. Jede „vernünftig“ arbeitende CA wird jedoch vor allem kritische Felder wie die Seriennummer und das Gültigkeitsdatum des Zertifikats selbst ausfüllen.

Weiter erlaubt das Verfahren nicht die Konstruktion einer Kollision zu einem bereits vorliegenden Zertifikat. Damit sind insbesondere bereits ausgestellte Zertifikate nicht auf diese Weise angreifbar. Schließlich müssen die Zertifikatsparameter eine Bitlänge besitzen, die ein ganzzahliges Vielfaches von 512 ist.

Aber vor allem: Welchen Nutzen hätte ein Angreifer von zwei Zertifikaten zu von ihm selbst konstruierten Public Keys? Schlimm wäre, wenn er Zertifikatsparameter ändern könnte, um z.B. den Public Key einer zweiten Identität zuzuordnen oder aus einem End-User- ein CA-Zertifikat zu machen – dies ermöglicht das Konstruktionsverfahren jedoch nicht.

Nach eigenen Aussagen versucht das Forscherteam jetzt, vergleichbare Zertifikate auf SHA-1-Basis zu finden. Doch obwohl SHA-1 stark „angekratzt“ ist, scheint dies deutlich aufwändiger zu sein. Wer allerdings noch immer MD5 einsetzt, ist nicht nur nicht sicher, sondern selbst Schuld.

1.2 Haftungsrisiken

Vom Bitkom ist am 10.03.2005 ein Leitfaden zum Thema Haftungsrisiken erschienen. Das Dokument stellt recht übersichtlich die wichtigsten rechtlichen Anforderungen zusammen und unterscheidet insbesondere nach strategischen, konzeptionellen und operativen Aufgaben. Für verschiedene Zielgruppen wie Geschäftsführung/-Vorstand und IT-Leitung/-Sicherheitsbeauftragte werden in einer Matrix die jeweiligen Pflichten und der Bedarf den Rechtsgrundlagen, potentiellen Schäden und Ansprüchen Dritter gegenüber gestellt. Der Leitfaden bietet einen guten Einstieg in das Thema und zeichnet sich durch klare Strukturierung und übersichtliche Darstellung aus.

1.3 NIST SP 800-53

Am 07.03.2005 wurde die NIST Special Publication 800-53 „Recommended Security Controls for Federal Information Systems“ veröffentlicht. Sie stellt in guter, sehr detaillierter und umfassender Form die möglichen Ausprägungen von Sicherheitsmaßnahmen dar, die im Rahmen der Sicherheitsarchitektur einer Organisation notwendig sind. NIST SP 800-53 korrespondiert dabei mit dem im Dezember 2003 publizierten Standard FIPS-199 „Standards for Security Categorization of Federal Information and Information Systems“.

Das 121 Seiten starke Dokument differenziert Maßnahmen in den drei Kategorien Management, Organisation/Betrieb sowie Technik mit insgesamt 17 Teilbereichen. Passend dazu gibt es drei Ergänzungsdokumente, in denen die Sicherheitsmaßnahmen für drei unterschiedliche Grundsicherheitsniveaus (low/moderate/high) zusammen gestellt werden. Es ist zu erwarten, dass diese in den USA zukünftig verstärkt zur Bewertung des erreichten Sicherheitsniveaus heran gezogen werden.

Für Ende 2005 ist der Standard FIPS-200 "Minimum Security Controls for Federal Information Systems" angekündigt, der die Empfehlungen der SP 800-53 für US-amerikanische Organisationen ablösen soll.

1.4 Microsoft im Fadenkreuz

Wie bereits am 09.02.2005 vom Antivirus-Hersteller Sophos gemeldet versucht der Trojaner Bankash.A neben seiner eigentlichen „Tätigkeit", Zugangskennungen zum Online-Banking auszukundschaften, auch die am 20.01.2005 erschienene Beta-Version des Windows AntiSpyware Tools von Microsoft zu deaktivieren.

Dies könnte ein erstes Indiz sein, dass sich bei Sicherheits-Software das fortsetzt, was bei Betriebssystemen gang und gäbe ist: Andere Lösungen sind vielleicht nicht viel sicherer als Microsofts (apropos: am 12.03.2005 erschien das erste Sicherheits-update zu Firefox 1.0, am 23.03.2005 schon das zweite), aber allein auf Grund ihrer Verbreitung stehen Microsoft-Produkte im Fadenkreuz der Hacker und werden häufiger und schneller angegriffen.

1.5 Kompass der IT-Sicherheitsstandards

Auch am 10.03.2005 wurde vom Bitkom ein Leitfaden für mittelständische Unternehmen mit dem Titel „Kompass der IT-Sicherheitsstandards" veröffentlicht. Das Dokument bietet einen gelungenen Überblick wichtiger Standards wie ISO 17799, BS 7799-2, IT-Grundschutz, Cobit, ITIL sowie weiterer für spezifischere Sicherheitsaspekte. Durch ein Klassifizierungsschema ist je nach Art des Unternehmens und der IT-Relevanz sehr übersichtlich dargestellt, welche Felder der jeweilige Standard abdeckt und für welche Personen und Rollen er angewendet werden kann.

1.6 Knack' den Knacker

Das Passwort Recovery Tool Cain&Abel ist wegen seines mächtigen Funktionsumfangs und der eingängigen Bedienoberfläche bei Penetrations-Testern und IT-Forensikern vermutlich ebenso beliebt wie bei Hackern jeglicher Couleur. Ironie des Schicksals: Am 18.03.2005 wurde bekannt, dass Cain&Abel bis Version 2.65 anfällig für einen Buffer-Overflow ist, wenn es beim Abhören eines VPN-Verbindungsaufbaus auf manipulierte IKE-Pakete stößt.

Nimmt man einmal an, dass viele Angreifer es mit dem Patch-Level ihrer Werkzeuge nicht anders halten als die meisten ihrer Opfer, könnte man vor diesem Hintergrund auf die Idee verfallen, präventiv „vergiftete" Pakete im eigenen Netz auszustreuen...

1.7 Data-Mining the NSA

Dem österreichischen Verein Quintessenz ist es nach eigenen Angaben aufgrund eines Konfigurationsfehlers gelungen, ein vollständiges Archiv der „Biometrics Consortium List" zur erlangen, welches ca. 60 MB Text sowie 2 GB an Fachdokumenten und Präsentationen enthält. Insgesamt haben 2.500 Personen bzw. Organisationen an der Mailingliste mitgewirkt.

Unter dem Aufmacher „Datamining the NSA – Part I" wird derzeit mit Hilfe von Werkzeugen des Data-Minings höchst aufschlussreich und sehr detailliert nachgewiesen, in welchem Ausmaß über die letzten zehn Jahre hinweg mit dieser Mailingliste von US-amerikanischen Organisationen versucht wurde, den Biometriebereich systematisch zu beeinflussen. Die Diagnose: Ziel war ein patentfreier, universaler Standard, der eine technologische Unabhängigkeit der USA von nicht-amerikanischen Patentgebern sicherstellt.

Laut Quintessenz ist die Auswertung bisher erst bis zum Jahre 1996 erfolgt; daher kann noch nicht beurteilt werden, inwieweit die Entwicklung biometrischer Technologien und der Einsatz in Deutschland und Europa in den letzten Jahren „Impulse" durch diese Mailingliste erfahren haben.

2 Secorvo New

2.1 Secorvo College aktuell

Zusammen mit dem Schweizer Spezialisten Compass Security – Gewinner des 24-Stunden-Hacker-Contest 2004 des Schweizer Fernsehens – bieten wir Ihnen im April und Mai in vier technisch aufwändigen

Labor-Schulungen einen vertieften Einblick in die wichtigsten aktuellen Angriffsmethoden auf IT-Systeme – live und unter Ihrer aktiven Beteiligung vorgestellt. In den vier Labor-Seminaren wechselt die Arbeit im Übungslabor mit Referatsblöcken, in denen die wesentlichen theoretischen Hintergründe und Schutzmethoden vermittelt werden:

- Live-Hacking Lab (**26.-28.04.**)
- Live-Hacking Spezial (**29.04.**)
- Web Application Security (**02.-04.05.**)
- Spurensuche im Web (**23.-25.05.**).

2.2 security-finder.de

Seit Mitte März 2005 bietet Secorvo einen neuen Service: Den Zugang zur über mehr als zehn Jahre gewachsenen Secorvo-eigenen Know-How-Datenbank mit vielen Hundert ausgesuchten Dokumenten zu Fragestellungen der Datensicherheit und des Datenschutzes. Getreu dem Anspruch der Security News, eine „Schneise in die Informationsflut“ zu schlagen, bietet der Security-Finder den Zugang zu nach Wichtigkeit und Aktualität ausgewählten Dokumenten – jeweils mit Kategorisierung, inhaltlicher Zusammenfassung und Bewertung.

„Finden statt suchen“: Statt mühsamen Durchforschens von Suchmaschinenergebnissen führt der Security-Finder strukturiert direkt zum passenden Dokument. Besonders wertvolle Funde können per Mausklick in die private Bibliothek übernommen werden, und regelmäßig wird per E-Mail über Neuzugänge informiert.

Der Preis für den Zugang zum Security-Finder orientiert sich am Modell einer Loseblattsammlung: Der Zugang zum „Grundwerk“ kostet einmalig 299 €, das Jahresabonnement 149 €. Bis zum 30.06.2005 kostet der Zugang nur 249 € (Grundwerk) und das Jahresabonnement 124 €. (Preise für Unternehmenszugänge auf Anfrage).

Leser der Security News erhalten bis zum 10.04.2005 freien Zugang unter der ID „SSN-01“ (Passwort: „security-finder“).

3 Veranstaltungshinweise

April 2005	
05.-08.04.	Sicherheit 2005 (GI, Uni Regensburg)
12.-13.04.	Lotus Notes Security (Secorvo College, Karlsruhe)
14.04.	Lotus Notes Security advanced (Secorvo College, Karlsruhe)
18.-19.04.	Datenschutz und Datensicherheit – DuD 2005 (COMPUTAS, Berlin)
19.-20.04.	Inside Windows Security (Secorvo College, Karlsruhe)
26.-28.04.	Live Hacking Lab (Secorvo College, Karlsruhe)
29.04.	Live Hacking Spezial (Secorvo College, Karlsruhe)
Mai 2005	
02.-04.05.	Web-Application Security (Secorvo College, Karlsruhe)
10.-11.05.	Datenschutzkongress 2005 (Euroforum, München)
10.-12.05.	IT-Sicherheitskongress 2005 (BSI, Bonn)
22.-26.05.	Eurocrypt 2005 (IACR, Aarhus/DK)
23.-25.05.	Spurensuche im Web (Secorvo College, Karlsruhe)

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
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

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

Secorvo Security News
April 2005

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

Nr. 4, 4. Jhrg. 2005
Stand 25. April 2005

ISSN 1613-4311

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

Inhalt

Editorial: Verschwörung!

1 Security News

1.1 Datenschutz: Toll Collect

1.2 Hacken mit Google

1.3 MS Windows 2003 SP 1

1.4 Immer wieder: DNS-Gift

1.5 Un-Sicherheitsfeature

1.6 Wegmarke bei ISIS-MTT

1.7 WinZIP-Verschlüsselung

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Security Awareness Symposium 2005

3 Veranstaltungshinweise

Impressum

Editorial: Verschwörung!

Die Geschichte ist schnell erzählt: Für einen großen Kongress eines Sicherheits-Bundesamtes wird ein für kritische Kommentare bekannter Informatik-Professor um einen Vortrag über biometrische Sicherheitssysteme gebeten. Der Text ist geliefert, das Programm gedruckt – da kommt die Ausladung durch den Präsidenten, begründet mit „neuen Entwicklungen“. Der Brüskierte wendet sich an die Presse.

Zunächst nur ein Vorgang grober Unhöflichkeit unter Beamten. Aber: Der Beirat des Kongresses erfährt von der Ausladung aus der Zeitung, weiß nichts von „neuen Entwicklungen“, die im Programm unterzubringen sind. Ein Schelm, wer Arges dabei denkt: Fiebert doch der Innenminister bekanntlich nach biometrischen Merkmalen im Ausweis. Sollte da auf Veranlassung von oben ein Kritiker mundtot gemacht werden? „Zensur“, schreien die Kritiker. „Zu kurz gedacht“, erwidern Besonnene: Es sei doch dumm, Kritik und Professor medial so aufzuwerten. War es dann ein schwacher Moment des Präsidenten, der Versuch, in voraus eilendem Gehorsam befürchteten Minister-Groll abzuwenden? Nein, zu billig.

Dahinter steckt mehr. Schließlich war der Vortrag perfekt platziert: Um 9 Uhr am Morgen nach dem intensiv besuchten Empfang des ersten Kongressabends – nur Unverdrossene hätten die Reihen gefüllt. Da drängt sich eine andere Erklärung auf: Der Präsident, im Herzen Biometrie-Verächter, wollte der Kritik eine größere Bühne geben, sich selbst aber aus der ministeriellen Schusslinie halten. Jedoch: Auch dieser Verdacht hinkt. Die Kritik des Kritikers ist dünn, knapp (fünf Seiten) und akademisch, keine Bedrohung für den neuen Personalausweis. Versuchte der Präsident also, die Biometriekritik durch öffentliche Aufwertung magerer Argumente zu schwächen? Ist der Kritiker gar Agent der Biometrie-Industrie?

Tatsächlich diente die Farce ganz anderen Zwecken: Sie lenkte ab vom aufkeimenden Verschwörungsverdacht zur Rolle der NSA beim SHA-1-Design! (Warum bloß ist der SHA-1 nun Thema des Ersatzvortrags ...?)

1 Security News

1.1 Datenschutz: Toll Collect

Am 19.04.2005 hat Peter Schaar, der Bundesdatenschutzbeauftragte (BfD) den 20. Tätigkeitsbericht für die Jahre 2002-2004 vorgelegt. Darin äußert er sich unter anderem ausführlich zur Umsetzung des Datenschutzes im LKW-Mautsystem Toll Collect.

Dieses von der Toll Collect GmbH im Auftrag des Bundes nach dem Autobahnmautgesetz (ABMG) errichtete und seit Januar 2005 störungsfrei betriebene Mautsystem unterliegt strengen Datenschutzanforderungen. So dürfen beispielsweise von den ca. 300 Autobahn-Mautbrücken ausschließlich mautpflichtige Fahrzeuge erfasst werden; Fotos und Kennzeichen von PKW sind sofort zu löschen. Denn das ABMG berechtigt Toll Collect nur zur Nutzung von Daten, die für die Mauterhebung erforderlich sind. Die Erfassung von Daten, mit denen sich beispielsweise Bewegungsprofile erstellen oder Fahrzeuge von Straftätern verfolgen ließen, ist nicht erlaubt. Das Gesetz lässt daran keinen Zweifel: „Eine Übermittlung, Nutzung oder Beschlagnahme dieser Daten nach anderen Rechtsvorschriften ist unzulässig“ (§§ 4 Abs. 2, 7 Abs. 2 ABMG).

Um diese datenschutzrechtlichen Anforderungen in dem hoch komplexen Mautsystem umzusetzen, das täglich durchschnittlich 700.000 mautpflichtige LKW erfasst und kontrolliert, wurden zahlreiche Löschfunktionen für nicht erforderliche oder nicht mehr benötigte Fahrzeugdaten implementiert. An der Konzeption, Umsetzung und Kontrolle dieser Datenschutzmechanismen war Secorvo maßgeblich beteiligt.

Der BfD kommentiert das Ergebnis seiner Überprüfung des Datenschutzes bei Toll Collect in seinem Tätigkeitsbericht abschließend wie folgt: „Ich habe mich davon überzeugt, dass die Grundlagen für eine Umsetzung der datenschutzrechtlichen Anforderungen des Gesetzes in den Funktionalitäten des Systems auch geschaffen wurden.“ (S. 181). Wie sagt der Schwabe: „Ned gschumpfe isch gnug globd.“

1.2 Hacken mit Google

Bereits in den späten 1980er-Jahren diskutierten Sicherheitsexperten, dass damals aktuelle Suchmaschinen wie Gopher oder FTPsearch auch von Angreifern zur Recherche sensitiver Informationen – beispielsweise Passwortdateien – missbraucht werden könnten. Obwohl heutige Suchmaschinen wie Google ungleich mächtiger sind als ihre virtuellen Vorfahren, wurde diese Gefahr lange nicht untersucht.

Inzwischen betreibt der Sicherheitsexperte Johnny Long seit einiger Zeit eine viel beachtete Webseite, auf der Hunderte von Beispielen dafür zu finden sind, wie Google zum Suchen und Finden von z.B. Passwortdateien, versteckten Verzeichnissen, Logdateien, Software- und Betriebssystem-Schwachstellen, Login-Portalen, Datenbanken, Kreditkarteninformationen, oder Netzwerkdruckern, teilweise sogar automatisiert eingesetzt werden kann. In einem White Paper beschreibt Long die wichtigsten Beispiele und effektive Gegenmaßnahmen. Weiter geht sein soeben erschienenes Buch „Google Hacking for Penetration Testers“, das in keiner Bibliothek fehlen sollte.

1.3 MS Windows 2003 SP 1

Der am 30.03.2005 von Microsoft veröffentlichte Service Pack 1 (SP1) für Windows 2003 Server integriert alle sicherheitsrelevanten Patches der Jahre 2003-2005 bis einschließlich MS05-015. Darunter finden sich der Security Configuration Wizard (SCW) für eine vereinheitlichte und prozessorientierte Sicherheitsadministration, die Post-Setup Security Updates (PSSU) zur Blockade von Netzwerkverkehr bei einer Erstinstallation (schützt bis zur Patcheinspielung), die Windows Firewall (WF), die für jedes Interface über Group Policies administrierbar ist und die Data Execution Prevention (DEP) zum Schutz vor Speicherüberläufen.

Des weiteren wurden die Standard-Sicherheitseinstellungen restriktiver vordefiniert; damit sind Windows Server zukünftig hoffentlich auch sicherer konfiguriert.

1.4 Immer wieder: DNS-Gift

Seit dem 03.03.2005 gingen beim SANS-Institut zahlreiche Berichte über erfolgreiche „Cache Poisoning"-Angriffe auf diverse DNS-Server ein. Wieder hatten Angreifer die schon auf der USENIX 1995 publizierte DNS-Schwachstelle ausgenutzt. Neu war indes die Art der Angriffe: Gezielt wurden bekannte Lücken verschiedener Anwendungen genutzt: Zunächst wurden anfälligen DNS-Servern unter Windows NT4 bzw. 2000 sowie Gateways von Symantec gefälschte DNS-Einträge (Zuordnung von Hostnamen zu IP-Adressen) „untergejubelt". Anschließend wurden für bestimmte Hostnamen die IP-Adressen von Webservern geliefert, die dann über Schwachstellen des Internet Explorer versuchten, Spyware zu installieren. Vom SANS existiert eine detaillierte Analyse (deutsche Fassung), die auch Gegenmaßnahmen für Betroffene beschreibt.

Dieser Angriff zeigt nicht nur, dass unzureichendes Patch-Management immer wieder die Ausnutzung lange bekannter Schwachstellen ermöglicht. Sondern er lässt auch die Rufe nach DNSSEC wieder lauter werden. Mehrere Studien, u.a. von Secorvo und vom BSI, beschäftigten sich in den vergangenen Jahren mit der globalen Einführung von DNSSEC, rieten aber aus organisatorischen und technischen Gründen zur Zurückhaltung. Einige der identifizierten Mängel wurden jüngst in aktuellen RFCs korrigiert – mittelfristig führt sicherlich kein Weg an DNSSEC vorbei.

1.5 Un-Sicherheitsfeature

Ein am 01.04.2005 online veröffentlichter (und ernst gemeinter) Beitrag in der Zeitschrift c't ruft in Erinnerung, dass Zugriffsschutz und Denial-of-Service zwei Seiten einer Medaille sein können. So unterstützen viele Festplatten die im ATA-Standard vorgesehene Möglichkeit, den Zugriff auf die gespeicherten Daten durch ein Passwort in der Firmware des Laufwerks zu sperren. Dieses Passwort soll automatisch vom BIOS des Rechners, in dem die Festplatte eingebaut ist, gesetzt und verwendet werden. Weil jedoch viele BIOS-Hersteller das ATA-Passwort nicht unterstützen, wird nicht nur der mögliche Schutzeffekt nicht erzielt, sondern Trojanern & Co. die Möglichkeit gegeben, die Festplatte durch den Eintrag eines eigenen Passworts nahezu irreversibel zu sperren. So gesehen ist es ein Pluspunkt, dass der Schutz durch das ATA-Passwort nicht unüberwindbar ist...

Hersteller sollten daraus lernen, Anwendern konfigurierbare Sicherheitsfunktionen nur zugänglich zu machen, wenn diese bekannt und einfach konfigurierbar sind – sonst droht Missbrauch durch Angreifer.

1.6 Wegmarke bei ISIS-MTT

Am 14.04.2005 wurde im Rahmen einer Präsentation beim Bundeswirtschaftsministerium (BMWA) das im Jahr 2001 als „Public-Private-Partnership" gestartete Projekt ISIS-MTT in die „Obhut" der Wirtschaft übergeben.

Das mit einem Auftrag des BMWA an TeleTrusT e.V. in Kooperation mit T7 e.V. im Jahr 2001 gestartete Projekt zielte auf eine bessere Interoperabilität von PKI-Anwendungen. Seitdem wurden – unter Mitwirkung von Secorvo – die ISIS-MTT-Spezifikation weiter entwickelt, ein Testbed auf Open-Source-Basis konzipiert und realisiert sowie für inzwischen sechs Produkte ISIS-MTT Siegel vergeben, deren Standard-Konformität vom anerkannten ISIS-MTT-Prüflabor bei Secorvo bestätigt wurde.

1.7 WinZIP-Verschlüsselung

Immer wieder wird die im Kompressionsprogramm WinZIP integrierte Verschlüsselungsfunktion als Alternative zu einem Dateiverschlüsselungsprogramm eingesetzt. Früher war das riskant: Der PKZIP-kompatible Verschlüsselungsalgorithmus war 1994 von Biham und Kocher, 2001 mit einem verbesserten Verfahren von Stay erfolgreich attackiert worden.

Mit der Anfang 2004 publizierten Version 9 wurde die Verschlüsselung auf AES umgestellt (128 bzw. 256 bit Schlüssellänge) und HMAC-SHA-1 zur Integritätssicherung eingeführt. Seither gilt die Verschlüsselung als

kryptographisch stark. Dennoch ist Vorsicht geboten, wie Tadayoshi Kohno in einer Analyse vom 08.05.2004 zeigt: Er identifizierte zahlreiche Sicherheitsmängel der Implementierung (unverschlüsselte Dateiinformationen, Mischung verschlüsselter und offener Dateien, fehlerhafte Ableitung des AES-Keys von der Passphrase), die spezielle Angriffe ermöglichen.

2 Secorvo News

2.1 Secorvo College aktuell

Speziell für Administratoren haben wir zwei neue Seminare entwickelt, die sich dem Thema „Sichere IT-Administration“ widmen. Im Wechsel von Theorie, Workshop und Übung werden technische Anleitungen zur sicheren IT-Administration gegeben:

IT-Sicherheit für Admins (Windows) am **07.-08.06.2005**

IT-Sicherheit für Admins (Unix) am **09.-10.06.2005**

http://www.secorvo.de/college

2.2 Security Awareness Symposium 2005

Zum dritten Mal veranstaltet Secorvo am **21. und 22.06.2005** das “Security Awareness Symposium”. Es hat sich in den vergangenen Jahren zur Plattform für den Erfahrungsaustausch entwickelt. Security-Awareness-Aktivitäten leben von guten Ideen – und damit auch von einem aktiven Ideenaustausch. An den Symposien 2003 und 2004 wirkten u.a. BMW, die Münchener Rück, SAP, RWE Systems, Finanz-IT, die schweizerische Armee, BASF und T-Systems mit Erfahrungsberichten mit. Auch in diesem Jahr werden wieder mehrere deutsche Unternehmen mit einem Erfahrungsbericht vertreten sein; das Programm ist derzeit in Abstimmung. Das vorläufige Programm und ein Anmeldeformular finden Sie unter

http://www.security-awareness-symposium.de

3 Veranstaltungshinweise

April 2005	
26.-28.04.	Live Hacking Lab (Secorvo College, Karlsruhe)
29.04.	Live Hacking Spezial (Secorvo College, Karlsruhe)
Mai 2005	
10.-11.05.	Datenschutzkongress 2005 (Euroforum, München)
10.-12.05.	IT-Sicherheitskongress 2005 (BSI, Bonn)
22.-26.05.	Eurocrypt 2005 (IACR, Aarhus/DK)
23.-25.05.	Spurensuche im Web (Secorvo College, Karlsruhe)
31.05. -02.06.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
Juni 2005	
01.-02.06.	Einführung in die Praxis des DSB (Euroforum, Wiesbaden)
06.-07.06.	IT-Risk Management 2005 (COMPUTAS, Karlsruhe)
13.- 14./17.06.	Information Security Management (Secorvo College, Karlsruhe)
21.-22.06.	Security Awareness Symposium (Secorvo, Karlsruhe)

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
Ettlinger Straße 12-14
D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

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

Secorvo Security News
Mai 2005

Dirk Fox, Stefan Gora, Stefan Kelm, Jochen Schlichting
Secorvo Security Consulting GmbH

Nr. 5, 4. Jhrg. 2005
Stand 25. Mai 2005

ISSN 1613-4311

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

Inhalt

Editorial:
Spieglein, Spieglein ...

1 Security News

1.1 RSA-200 faktorisiert

1.2 Cross-Zertifikats-Report

1.3 BSI-Antispam-Leitfaden

1.4 Phishing exposed

1.5 Hash-Workshop

1.6 PIV-Standards

1.7 LAND unter

1.8 „Roo“ v1.0 erschienen

1.9 Firefox strikes back

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Toll Collect auf Midvision

2.3 Security Awareness Symposium 2005

3 Veranstaltungshinweise

Impressum

Editorial: Spieglein, Spieglein ...

Der Traum von biometrischen Identifikationssystemen, die uns von der Not befreien, unser Gedächtnis mit Myriaden ständig wechselnder User-IDs, Passwörter und PINs zu quälen, ist viel älter, als so manche Science Fiction-Verfilmung uns glauben machen will. Schon unter den von den Gebrüdern Grimm tradierten klassischen Märchen findet sie sich: „Schneewittchen und die sieben Zwerge“ kommt zwar ohne Elektrizität und fließendes Wasser aus, wäre aber ohne Biometrie nicht denkbar.

In der Gestalt des Spiegels der Königin erwacht sie zum vollen Leistungsumfang. Nicht nur erkennt der seine Herrin eindeutig an Stimme und Gesicht, sondern er gibt auch bereitwillig Auskunft über biometrische Merkmale Dritter – wie der Schönheit Schneewittchens. Mehr noch: Selbst den Aufenthaltsort Schneewittchens kennt er (dank RFID?) und gibt ihn Preis, er weiß sogar um ihren aktuellen Gesundheitszustand. Ganz zu schweigen von der fortschrittlichen natürlichsprachlichen Benutzerschnittstelle...

Vielleicht ist es Zeit, Schneewittchen neu zu interpretieren. Denn das Märchen zeigt in drastischer Klarheit, was durch die Vernetzung biometrischer und personenbezogener Daten möglich ist. Der Zauberspiegel, der zweifellos eine sehr effektive Durchführung von Schönheitswettbewerben ermöglichen würde, wird in der Hand der Königin zum Mordwerkzeug. Wir erinnern uns: Jede Technik öffnet auch dem Missbrauch Tür und Tor – nicht nur in Herrscherhand.

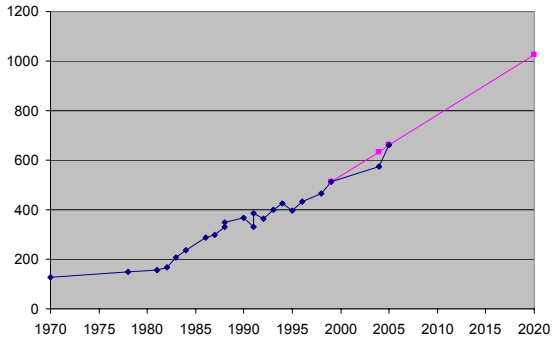
Dabei lassen sich biometrische und andere Identifikationssysteme auch so gestalten, dass eine Erfassung und Auswertung biometrischer Daten sowie der Aufenthaltsinformation nicht oder nur in kontrolliertem Umfang möglich ist. Dazu gehören die Einhaltung von Löschfristen, eine bedachte Technikgestaltung – vor allem aber der politische Wille, die Freiheit nicht um ihrer selbst Willen abzuschaffen.

„Spieglein, Spieglein an der Wand, wie lebenswert ist die Zukunft in diesem Land?“

1 Security News

1.1 RSA-200 faktorisiert

Am 09.05.2005 meldete die Bonner Forschungsgruppe von Prof. Jens Franke die erfolgreiche Faktorisierung der RSA-Challenge „RSA-200“ (Modullänge: 663 bit). Knapp 17 Monate hatte die Faktorisierung durch die Gruppe um Bahr, Böhm, Franke, Kleinjung, Montgomery und te Riele gedauert; der Rechenaufwand lag bei umgerechnet etwa 120.000 MIPS-Jahren. Für die Faktorisierung der Challenge „RSA-576“ Ende 2003, die auch auf das Konto dieser Forschergruppe ging, hatte sie „nur“ ca. 13.200 MIPS-Jahre benötigt (SSN 5/2004).



Grafik: Faktorisierungsprognose [BoFT 02]

Diese jüngste Faktorisierung entspricht fast exakt der Secorvo-Vorhersage aus dem Jahr 2001 – damals haben wir für 2005 die Faktorisierung eines 660 bit langen Moduls prognostiziert. Hält die Prognose, dann ist die Faktorisierung eines RSA-Moduls der Länge 1.024 bit in 15 Jahren zu erwarten.

1.2 Cross-Zertifikats-Report

Die Verknüpfung von Public-Key-Infrastrukturen (PKI) über Cross-Zertifikate oder Bridge-CAs ist in der Praxis noch immer nicht zufrieden stellend gelöst. Insbesondere Standard-Anwendungen wie Browser und E-Mail-Clients zeigen beim Umgang mit den entsprechenden Zertifikaten auch heute noch ein eher „holpriges“ Verhalten.

Diesem Problem sind die DFN-CERT Services GmbH und SURFnet in der Studie “PKI-Linking-Report: Connecting Public-Key-Infrastructures” nachgegangen, die am 26.04.2005 veröffentlicht wurde. Darin ist dokumentiert, wie unterschiedliche PKI-Anwendungen mit Cross-Zertifikaten etc. in der Praxis umgehen – und wo sie scheitern. Untersucht wurden Outlook Express, Outlook, Mozilla, Thunderbird, KMail, Internet Explorer, Mozilla, Firefox, Opera und Konqueror.

1.3 BSI-Antispam-Leitfaden

Spam ist schon lange nicht mehr nur eine Belästigung: Durch den Missbrauch zur Verbreitung von Phishing-Mails und Schadprogrammen ist Spam auch ein Sicherheitsproblem. Am 12.05.2005 stellte das BSI eine „Antispam-Strategien – Unerwünschte E-Mails erkennen und abwehren“ betitelte Studie zu diesem Thema vor. Die Untersuchung widmet sich dem Thema in großer Ausführlichkeit: Neben technischen Problemen und Lösungsvorschlägen werden auch die (vor allem finanziellen) Hintergründe organisierter Spammer diskutiert.

1.4 Phishing exposed

Phishing-Angriffe, in denen über Massen-E-Mails, die vorgeblich z. B. von Ebay oder einer Bank stammen, versucht wird, die Empfänger auf eine gefälschte Webseite zu locken und zur Eingabe vertraulicher Daten wie Passwörter, PINs oder TANs zu verleiten, nehmen nicht nur bedenklich zu, sondern werden auch immer perfider.

Dem Honeynet-Projekt ist es jetzt gelungen, hinter die virtuellen Kulissen einiger Phishing-Angriffe zu schauen. So konnten „Phisher“ dazu gebracht werden, Köder-Rechner (Honeypots) zu hacken und von dort ihre Angriffe (Aufsetzen gefälschter Webseiten, Verschicken von Massen-E-Mails, etc.) durchzuführen. Die Phisher wurden dabei mehrere Monate lang beobachtet. Dabei konnten drei generelle Angriffsmuster identifiziert werden. Ein am 16.05.2005 veröffentlichtes White Paper beschreibt die Details dieser Live-Analyse: Vieles weist darauf hin, dass zunächst automatisierte Angriffs-Tools verwendet

werden, um Hintertüren in einem System zu installieren. Über diese werden anschließend die Phishing-Attacken initiiert. Offenbar sind die Angreifer dabei sehr gut organisiert: So wurden Phishing-Archive mit gefälschten Webseiten vieler großer Online-Anbieter entdeckt. Erschreckend ist die Beobachtung, dass sehr viele Privatnutzer den Phishern auf den Leim gehen und auf deren gefälschte Webseiten zugreifen.

1.5 Hash-Workshop

Als Reaktion auf die jüngsten kryptoanalytischen Erfolge beim SHA-1 (SSN 02/2005) hat die Computer Security Division des NIST am 28.04.2005 einen Workshop zu kryptographischen Hashfunktionen ausgeschrieben (31.10.-01.11.2005). Interessierte sind aufgefordert, bis zum 15.07.2005 Vorschläge für Präsentationen einzureichen. Nähere Informationen finden sich auf der Workshop-Webseite.

1.6 PIV-Standards

Zur Umsetzung der Homeland Security Presidential Directive 12 vom 27.08.2004 wurde am 25.02.2005 vom NIST mit FIPS 201 ein Standard für eine einheitliche Personal Identity Verification (PIV) von Federal Employees und Contractors verabschiedet. Darin sind sowohl die grundsätzlichen Anforderungen an Identity-Cards als auch – sehr detailliert – die physisch-technischen Merkmale festgelegt, darunter die Abmessungen, Mechanismen (Foto, Barcode, Chip, Unterschriftsfeld, Magnetstreifen, Bedruckung) und Daten (z. B. biometrische Merkmale).

Der am 25.04.2005 publizierte NIST Special Report SP 800-78 enthält die Spezifikation der für PIV-Karten gemäß FIPS 201 zugelassenen kryptographischen Algorithmen und Schlüssellängen, vergleichbar der Algorithmenempfehlung des BSI für qualifizierte digitale Signaturen. Empfohlen werden darin bis Ende 2008/2010 RSA (ab 1024 bit), ECDSA (Kurven nach FIPS 186-3, ab 224 bit), TripleDES und AES (ab 128 bit) und als Hashfunktion SHA-1, SHA-224 oder SHA-256.

1.7 LAND unter

Am 17.05.2005 wurde auf der Bugtraq-Mailingliste die Anfälligkeit aktueller Windows-Systeme für LAND-Attacken gemeldet. Dieser Denial-of-Service Angriff wurde 1997 erstmalig veröffentlicht und eine entsprechende Schwachstelle bei Windows 95 geschlossen. Anfang 2005 wurde bei aktuellen Windows-Systemen erneut eine LAND-Anfälligkeit festgestellt. Die von Microsoft veröffentlichten Sicherheitspatches vom April sollten sie beheben; offenbar wirkt der Patch aber nicht bei Einsatz von IPv6. Wenn aber selbst die Patches vor Verbreitung nicht besser getestet werden als die Originalsoftware – was bleibt dann noch?

1.8 „Roo“ v1.0 erschienen

Am 17.05.2005 veröffentlichte das Honeynet-Projekt die Version 1.0 der kostenlosen Software „Honeywall CDROM Roo“. Dabei handelt es sich um eine auf Fedora basierende, sehr mächtige Tool-Sammlung, die es erlaubt, ein Honeynet der neuesten Generation sehr leicht aufzusetzen und zu administrieren, sowie potentielle Angriffsversuche auf das Honeynet effizient zu analysieren.

Stefan Kelm von Secorvo war während der mehrwöchigen Beta-Testphase intensiv an der Honeywall-Entwicklung beteiligt: Eine entsprechende Testumgebung wurde mehrere Wochen betrieben und Angriffe beobachtet. Die Ergebnisse dieser Testphase werden in Bälde als Secorvo White Paper veröffentlicht.

1.9 Firefox strikes back

Brian Livingston berichtet in seinem Newsletter vom 12.05.2005 von einem neuen Sicherheitsvergleich zwischen Internet Explorer und Firefox. Darin wurde nicht einfach die Anzahl der schwer wiegenden Schwachstellen verglichen, sondern die Zahl der Tage im Jahr 2004, an denen ein Browser mindestens eine ungepatchte, schwere Schwachstelle aufwies. Danach besaß die jeweils aktuelle Version des IE im Jahr 2004 an nur sieben Tagen keine

bekannten Schwachstellen. An 200 Tagen kursierten bereits Exploits (Angriffscode), ohne dass ein geeigneter Patch für den IE verfügbar war – bei Firefox kam dies nicht ein einziges Mal vor. Damit hat die Open-Source Community eindrucksvoll ihre hohe Reaktionsgeschwindigkeit bewiesen.

2 Secorvo News

2.1 Secorvo College aktuell

Wie sorge ich systematisch für Informationssicherheit im Unternehmen? Welche „Best Practices" gibt es, und was fordern die wichtigsten Standards? Antworten auf diese Schlüsselfragen gibt das zwei- bis fünftägige Seminar „Information Security Management von A(udit) bis Z(ertifizierung)" am **13.-14./17.06.2005**.

2.2 Toll Collect auf Midvision

Anlässlich der IT-Mittelstandsmesse „Midvision 2005" (Neue Messe Karlsruhe, 08.-09.06.2005) wird die Karlsruher IT-Sicherheitsinitiative am Abend des **08.06.2005** gemeinsam mit CAS und Cyberforum ein besonderes Event gestalten, in dessen Rahmen der Datenschutzbeauftragte von Toll Collect, Herr Reinhard Fraenkel, über Entwicklung und Umsetzung des Datenschutzkonzepts bei Toll Collect berichten wird. Programm und Anmeldung zu diesem Event mit anschließendem Buffet finden Sie auf der Webseite der KA-IT-Si.

2.3 Security Awareness Symposium 2005

Auf dem diesjährigen dritten „Security Awareness Symposium" am **21.-22.06.2005** in Karlsruhe, das sich in den beiden vergangenen Jahren als Plattform für den Erfahrungsaustausch über Sensibilisierungsmaßnahmen etabliert hat, werden unter anderem die Kampagnen von Bosch, DAK, Novartis und SAP präsentiert. Das aktuelle Programm und ein Anmeldeformular finden sich unter http://www.security-awareness-symposium.de/.

3 Veranstaltungshinweise

Mai 2005	
31.05. -02.06.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
Juni 2005	
01.-02.06.	Einführung in die Praxis des DSB (Euroforum, Wiesbaden)
06.-07.06.	IT-Risk Management 2005 (COMPUTAS, Karlsruhe)
08.06.	Datenschutz bei Toll Collect (KA-IT-SI/Midvision, Karlsruhe)
13.-14.06.	IT-Security Management (Secorvo College, Karlsruhe)
13.-17.06.	Information Security Management (Secorvo College, Karlsruhe)
14.-15.06.	Einführung in die Praxis des DSB (Euroforum, Berlin)
21.-22.06.	Security Awareness Symposium (Secorvo, Karlsruhe)
26.06.- 01.07.	17th Annual Computer Security Incident Handling Conference (FIRST, Singapore)
Juli 2005	
05.-07.07	Western European Workshop on Research in Cryptography (WEWoRC, Leuven-Heverlee)
27.-28.07.	Black Hat Briefings (Black Hat USA, Las Vegas)
29.-31.07.	Defcon 13 (Defcon, Las Vegas)

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

Abonnement des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
Juni 2005

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

Nr. 6, 4. Jhrg. 2005
Stand 27. Juni 2005

ISSN 1613-4311

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

Inhalt

Editorial: Es wird ernst

1 Security News

1.1 Malcode Analysetools

1.2 Remote Desktop Attacke

1.3 VoIP-Scanning

1.4 Bluetooth-Angriff

1.5 Phisher-Test

1.6 SHA-Angriff publiziert

1.7 Win Security Monitoring

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Suchen in Security News

2.3 Thitz gestaltet Plakat

2.4 Security Awareness 2005

2.5 Forensische Analysen

3 Veranstaltungshinweise

Impressum

Editorial: Es wird ernst

Seit Jahren registrieren wir steigende Vorfallszahlen – jährlich eine Verdreifachung der Anzahl neuer Viren, Würmer und Trojaner, eine Verdoppelung der vom CERT registrierten Angriffsarten und einen rapiden Anstieg der in verbreiteter Software gefundenen kritischen Sicherheitslücken.

Allerdings: Der Anstieg der veröffentlichten – und nach unserer Beobachtung auch der der tatsächlichen – Schadensfälle entwickelte sich bislang moderat. Als Ursache dafür werden häufig wachsende Sensibilität der Verantwortlichen und die Etablierung wirksamer Schutzmaßnahmen vermutet.

Eine genaue Analyse der Angriffe und Schadensfälle zeigt jedoch, dass dies nicht die Hauptursache ist. Denn das vergleichsweise geringe Schadensniveau verdanken wir im Kern der Harmlosigkeit der Attacken:

- Die Entwickler von Viren und Würmern konzentrierten sich bisher auf Verbreitungs- und Tarnfunktionen; die Schadensroutinen waren oft primitiv und meist wirkungslos.
- Die Verbreitungsmechanismen waren ungezielt und nur auf große öffentliche Sichtbarkeit ausgelegt.
- Schäden wurden meist durch Programmierfehler verursacht; finanziell profitierten die Angreifer nicht.

Das ändert sich jedoch derzeit. Vermehrt lassen sich gezielte Angriffe beobachten, hinter denen wirtschaftlich interessante Geschäftsmodelle erkennbar werden: Im Auftrag entwickelte Trojaner, die Unternehmen aushorchen, ausgeklügelte Phishing-Attacken und Verschlüsselungs-Trojaner, die erst nach Lösegeldzahlung das Passwort preisgeben.

Daher wird es dringlich, die unseren Schutzmaßnahmen zu Grunde liegenden Annahmen zu überprüfen – denn gezielt geplante und professionell umgesetzte kriminelle Angriffe schaffen eine grundsätzlich neue Situation.

Die „Zeit der Spiele“ ist vorbei – es wird ernst.

1 Security News

1.1 Malcode Analysetools

David Zimmer vom Sicherheitsdienstleister iDefense hat am 07.06.2005 unter dem Namen Malcode Analyst Pack sieben Tools zur Analyse von Windows-Schadsoftware veröffentlicht. Darunter findet sich auch ein kleiner DNS-Server, der alle Anfragen an die IP-Adresse eines Forensikers lenkt. Die ebenfalls enthaltene Shell Extension zur Anzeige von Datei-Hashsummen im Explorer verwendet zwar noch den MD5 als Hashfunktion; da die Sammlung unter GPL Lizenz veröffentlicht wurde, steht einer Ersetzung durch den SHA nichts im Wege.

Dem wollte das BSI offenbar nicht nachstehen: Es veröffentlichte am 17.06.05 unter dem Namen BOSS (BSI OSS Security Suite) eine Knoppix CD mit Open Source Security Tools, darunter einer grafisch bedienbaren Version des Nessus Scanners. Dem beliebten Security Scanner wurde eine deutsche Oberfläche verpasst, die für versierte Nessus-User allerdings etwas gewöhnungsbedürftig ist. Da die Ergebnisse weiterhin in Englisch dargestellt werden und eine Übersetzung der inzwischen über 7.000 Nessus-Plugins recht aufwändig sein dürfte, sind Zweifel am Sinn dieser Eindeutschung angebracht. Auch wenn einige weitere Tools wie beispielsweise NMap mitgeliefert werden, besitzen spezialisierte Knoppix-Versionen wie Knoppix-STD deutlich umfangreichere Möglichkeiten.

Schließlich erschien am 22.06.2005 eine aktualisierte Fassung der Auditor Security Collection CD, eine der mächtigsten Sammlungen aktueller Versionen wichtiger Tools zur Durchführung von Sicherheitsanalysen.

1.2 Remote Desktop Attacke

Mit der am 10.06.05 erschienenen Version 2.7.3 des Auditwerkzeugs Cain&Abel ist es möglich – einen geeigneten Netzzugang vorausgesetzt – die Schutzmechanismen einer Remote Desktop Protocol Sitzung im Rahmen einer Man-in-the-Middle Attacke zu unterlaufen und die Tastatureingaben aufzuzeichnen. Betroffen von dieser Möglichkeit sind alle aktuellen Windows Releases (WXP SP2 / W2K3 SP1), auf denen die Terminal Services eingesetzt werden. Der Angriff funktioniert dank der integrierten ARP Poison Routing-Technolgie auch in geswitchten Netzwerkinfrastrukturen.

Ermöglicht wird dieser Angriff durch ein grob fehlerhaftes Design der initialen Public-Key Authentifikation bei Microsoft: Der generierte Public-Key des Terminal Servers, der bei der Initialisierung der Terminal-Session verwendet wird, wird mit einem Private Key signiert, der fest kodiert im Betriebssystem vorhanden und damit für jedermann auslesbar ist (mstlsapi.dll).

Zum Schutz vor diesem Angriff bleibt für eine sichere Remote Administration von Windows Systemen (XP/2003) auf Basis von RDP nur der konsequente Einsatz der Virtual Private Network Funktionalität.

1.3 VoIP-Scanning

Viele Hacker- und Analyse-Tools werden in den aktuellen Versionen mit Funktionen zum Mitschneiden von VoIP-Datenströmen ausgeliefert, mit denen Telefonate als wav-Datei gespeichert werden können.

Mit diesen Analysetools lassen sich sehr eindrucksvolle Demonstrationen gestalten – z. B. durch die Aufnahme eines via ARP-Poisoning umgelenkten Telefonats im internen Netz. Aber Vorsicht: Das Belauschen und Mitschneiden eines Telefongesprächs, selbst die „näheren Umstände“ (Zeitpunkt, Teilnehmer) auch eines erfolglosen Verbindungsversuchs ohne Wissen der Kommunikationspartner ist ein strafbewehrter Verstoß gegen § 88 TKG, der das in Artikel 10 Grundgesetz garantierte Fernmeldegeheimnis schützt – unabhängig vom Motiv des Abhörvorgangs und unabhängig davon, ob der Betreiber der Anlage geeignete Schutzmaßnahmen getroffen hat.

Für WLAN-Verbindungen gelten verschärfte Bedingungen: § 89 TKG enthält ein explizites Abhörverbot für Funkanlagen, das nicht nur Telefonverbindungen umfasst,

sondern alle Nachrichten, die für die Funkanlage nicht bestimmt sind. Erfolgt ein unbeabsichtigter Empfang, unterliegen die Daten der Geheimhaltung und dürfen nicht an Dritte weitergegeben werden.

1.4 Bluetooth-Angriff

Zwei israelische Forscher präsentierten am 06.06.05 einen Bericht, in welchem sie den erfolgreichen Angriff auf einen zentralen Sicherheitsmechanismus von Bluetooth – die PIN beim Pairing von Geräten – darstellen. Durch ein Belauschen des Pairing-Prozesses kann eine kurze PIN (4 Zeichen) selbst auf veralteten PCs (Pentium III, 450 MHz) in weniger als einer Sekunde (0,3 sec) bestimmt werden.

Zusätzliche Relevanz erlangt der Angriff dadurch, dass die Autoren auch beschreiben, wie ein Angreifer per Funk zwei bereits „gepaarte" Bluetooth-Geräte zum erneuten Pairing veranlassen kann – um auch deren PIN zu gewinnen.

1.5 Phisher-Test

Phishing-Angriffe nehmen nicht nur in ihrer Anzahl stetig zu – die verschickten E-Mails sind auch immer schwieriger von „echten" E-Mails zu unterscheiden. Wer mag, kann sein diesbezügliches Urteilsvermögen beim (zweiten) „Phishing IQ Test" der Firma MailFrontier auf die Probe stellen: Für zehn Beispiele (eBay, Amazon, Bank of America etc.) ist zu entscheiden, ob es sich um eine Phishing-Mail handelt.

Der Test schärft nicht nur die eigene Urteilsfähigkeit, sondern bietet dank ausführlicher Erläuterungen auch eine gute Hilfestellung bei der Gestaltung eigener Online-Dienstleistungen. Am ersten Test haben sich angeblich mehr als 225.000 Personen beteiligt.

1.6 SHA-Angriff publiziert

Für Kryptologen interessant: Die Autoren des SHA-Angriffs (siehe SSN 02/2005), die Forschungsgruppe um Wang, haben am 17.06.2005 ihre für die Crypto 2005 eingereichte Forschungsarbeit zu SHA-0 und SHA-1 öffentlich zugänglich gemacht.

1.7 Win Security Monitoring

Microsoft hat am 06.06.2005 einen Security Monitoring and Attack Detection Planning Guide veröffentlicht, der Hilfestellung bei der Konfiguration und Nutzung der Microsoft Windowxs Security Event Logs für ein wirksames Security Monitoring leistet. Im Anhang des 53seitigen Dokuments finden sich außerdem Empfehlungen für die Konfiguration der Audit Policy in den Group Policy Settings.

2 Secorvo News

2.1 Secorvo College aktuell

Nach einer Sommerpause in den Monaten Juli und August startet das College-Programm des zweiten Halbjahrs 2005 im September mit Seminaren zu Public Key Infrastrukturen (20.-21./22.09.2005) und Web-Application Security (27.-29.09.2005). Wir freuen uns, wenn wir Sie im Herbst auf einem unserer Seminare begrüßen dürfen.

http://www.secorvo.de/college

2.2 Suchen in Security News

Viele Leser schätzen die seit Juli 2002 monatlich erscheinenden Secorvo Security News wegen der zahlreichen Links auf wertvolle Originaldokumente. Bisher war die Suche nach älteren Links jedoch mühsam: Es gelang bestenfalls mit einer Volltextsuche in den pdf-Dateien des Jahrgangsarchivs, und gelegentlich hatte sich die gesuchte URL inzwischen verändert.

Daher finden sich inzwischen alle in den Secorvo Security News zitierten Dokumente vollständig im Security Finder und ermöglichen so eine thematische Recherche und eine regelmäßige Aktualisierung der Links. Mit dem Erscheinen der vorliegenden Juni-Ausgabe der SSN können jetzt auch SSN-Jahrgänge komplett im Security Finder durchsucht werden.

Zur Erinnerung: Bis 30.06.2005 gibt es den Security Finder noch zum Einstiegspreis.

2.3 Thitz gestaltet Plakat

Der Secorvo-Künstler Thitz hat für SWR3 das Plakat des diesjährigen New Pop Festival gestaltet – und folgt damit James Rizzie und Chales Kaufman, die 2003 und 2004 die Plakate entwarfen. Ein weiterer Meilenstein auf dem Weg zum Weltruhm – erst Ende 2004 hielt er mit einer Tüte zur Gründung Einzug in die „Sammlung Frieder Burda“ in Baden-Baden.

2.4 Security Awareness 2005

Die Materialien des diesjährigen dritten Security Awareness Symposium am 21. und 22.06.2005 sind jetzt – wie auch die der Vorjahresveranstaltungen – auf CD erhältlich – darunter die Präsentationen der Security Awareness Kampagnen von Bosch, Novartis und SAP, eine Vorstellung der Initiative „Deutschland sicher im Netz“ und ein Vortrag von Herrn Prof. Dr. Zerr zur Evaluation und Erfolgskontrolle von Awareness-Maßnahmen. Die CDs der beiden Vorjahresveranstaltungen enthalten Darstellungen der Kampagnen von BASF, BMW, Fiducia, Münchener Rück, RWE, der Schweizerischen Armee und T-Systems sowie weiterführende Materialien und eine Fotodokumentation der Ausstellung auf dem Symposium 2003.

2.5 Forensische Analysen

Die zunehmende Anzahl und „Qualität“ interner und externer Angriffe führt immer häufiger zu größeren Schadensfällen. In der Praxis treten damit verstärkt Fragestellungen nach dem Schadensumfang, der Zielsetzung des Angreifers und hinterlassenen Spuren für eine mögliche Strafverfolgung auf. Antworten auf diese und ähnliche Fragen kann eine Forensische Analyse liefern. Secorvo bietet diese Dienstleistung bereits seit einiger Zeit an – die wachsende Nachfrage hat uns nun dazu veranlasst, das entsprechende Leistungsangebot deutlich zu überarbeiten und zu konkretisieren.

3 Veranstaltungshinweise

Juli 2005	
05.-07.07	Western European Workshop on Research in Cryptography (WEWoRC, Leuven-Heverlee)
27.-28.07.	Black Hat Briefings (Black Hat USA, Las Vegas)
29.-31.07.	Defcon 13 (Defcon, Las Vegas)
August 2005	
01.-05.08.	14th USENIX Security Symposium (Usenix, Baltimore/US)
14.-18.08.	Crypto 2005 (IACR, Santa Barbara/US)
September 2005	
20.-21.09.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
22.09.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
27.-29.09.	Web-Application Security (Secorvo College, Karlsruhe)
Oktober 2005	
04.10.	Datenschutz kompakt (Secorvo College, Karlsruhe)
05.-06.10.	Inside Windows Security (Secorvo College, Karlsruhe)
11.-13.10.	IT-Sicherheit heute (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

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

Secorvo Security News
Juli 2005

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

Nr. 7, 4. Jhrg. 2005
Stand 29. Juli 2005

ISSN 1613-4311

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

Inhalt

Editorial: Wilder Westen

1 Security News

1.1 MBSA 2.0 verfügbar

1.2 Anwendungs-Bugs

1.3 Exploits mit Trojaner

1.4 CSI/FBI-Studie 2005

1.5 Vorsorgeüberwachung

1.6 Security-Checklisten

1.7 Postraub anno 2005

1.8 PKI-Token-Evaluierung

2 Secorvo News

2.1 Secorvo College aktuell

2.2 eco-AK “Sicherheit”

3 Veranstaltungshinweise

Impressum

Editorial: Wilder Westen

Als ich nach Bloody Corner kam, sah ich von weitem her:
Die Summe unter meinem Namen hatte zwei Stellen mehr.
Ein Prämienjäger sagte: Pfeifer, ich wart' schon auf dich!
Ich fuhr herum, pfiff einen Ton –
dann sprach mein Colt für mich.

Bald zwei Jahre ist es her: Am 05.11.2003 setzte Microsoft im Rahmen des Antivirus Reward Program Kopfgelder in Höhe von insgesamt 5 Mio. US$ für Hinweise aus, die zur Identifikation und Ergreifung der Entwickler von Blaster, Sobig, MyDoom et. al. führen (SSN 11/2003). Mit der Verurteilung des Deutschen Sven Jaschan, Autor des Sasser-Wurms, am 08.07.2005 zu 21 Monaten Haft auf Bewährung kommt nun das erste Kopfgeld zur Auszahlung: Die beiden Whistleblower aus der „Szene“, die die entscheidenden Hinweise auf Jaschan gaben, erhalten 250.000 US$.

Zweifellos schreien die ausufernde Verbreitung von Viren und Würmern und die irrsinnigen Schadenssummen geradezu nach unkonventionellen Maßnahmen, um einer Entwicklung Einhalt zu gebieten, die die Informationstechnik als Ganzes existentiell zu bedrohen beginnt.

Dennoch drängt sich die Frage auf, ob diese medienwirksam in Szene gesetzten Kopfgelder noch angemessen sind. Der Maßnahme haftet nicht nur ein Hauch Selbstjustiz an, sondern sie verzerrt auch die Verhältnisse: Die Belohnungen deutscher Behörden für Hinweise auf Geiselnehmer, Mörder und Raubmörder bewegen sich zwischen 1.000 und 5.000 €. Ist daraus nun zu schließen, dass die Ergreifung eines Virenprogrammierers so begrüßenswert ist wie die Verhaftung von 50 bis 250 Kapitalverbrechern?

Bleibt zu hoffen, dass diese auf die Verursacher nahezu spurenloser Straftaten ausgesetzten monströsen Kopfgelder wenigstens zur Selbstanzeige motivieren...

Jetzt sitz’ ich hinter Gittern, von Zweifeln angenagt.
Vielleicht war doch des Denkers Plan
so gut nicht wie er sagt.
Er sagte: Es bringt Dir 10.000 Dollar, wenn Du's wagst
zum Sheriff ins Büro zu geh'n,
Dich vorstellst und ihm sagst:
Grüß Gott, ich bin der Pfeifer, ich komm' selber wie ihr seht,
um die Belohnung zu kassier'n, die auf meinen Kopf steht!
Reinhard Mey, Die Ballade vom Pfeifer

1 Security News

1.1 MBSA 2.0 verfügbar

Seit dem 01.07.2005 ist der Microsoft Baseline Security Analyser (MBSA) in der Version 2.0 verfügbar – ein seit Dezember 2002 angebotenes Tool (SSN 1/2003), das die Duchführung lokaler und Remote-Scans von Windows-Systemen auf Sicherheitsschwächen ermöglicht und detaillierte Vorschläge für Abhilfemaßnahmen liefert. Neu hinzugekommen sind neben einer verbesserten Bewertung der festgestellten Schwachstellen und fehlenden Patches umfangreiche Hilfefunktionen sowie die Unterstützung von Office XP und 64 bit Windows-Versionen. MBSA 2.0 ist kostenfrei und zu Microsofts Windows Server Update Services kompatibel.

1.2 Anwendungs-Bugs

Beim Thema Patch Management darf man die Anwendungen nicht vernachlässigen – auch diese können Schwachstellen aufweisen, die eine Übernahme des Systems mit dem Rechteprofil des Benutzers erlauben.

Das beweist eine am 05.07.2005 veröffentlichte Schwachstelle in Adobes Acrobat Reader 5.0.9 und 5.0.10 unter UNIX und Linux, die es einem Angreifer ermöglichen kann, durch Zusendung eines geeignet konstruierten PDF-Dokuments beliebigen Code auf dem Empfängersystem auszuführen. Ein Update auf die aktuelle Version des Readers wird empfohlen.

Eine ähnliche Schwachstelle wurde am 12.07.2005 in Microsoft Word 2000 und Word 2002 entdeckt: Ein Buffer Overflow erlaubt die Ausführung von Angriffscode über ein Word-Dokument. Passende Updates sind inzwischen verfügbar.

1.3 Exploits mit Trojaner

So genannte Exploits, das sind über das Internet verbreitete Quellcode-„Häppchen“, die neue sicherheitsrelevante Lücken in Betriebssystemen oder Anwendungen vorführen, verwenden häufig einen Codeabschnitt, der bei Ausführung des Programmcodes eine Kommandozeilen-Shell auf dem befallenen System startet.

Am 26.07.2005 wurde bekannt, dass zahlreiche der im Internet kursierenden Exploits versteckte Trojaner, Rootkits oder Schadensroutinen enthalten – dort wurde jeweils der Shellcode ersetzt. Jeder, der diesen manipulierten Code ausprobiert oder ihn sogar unverändert in ein Analysetool integriert, installiert beim ersten Starten einen Trojaner oder ein Rootkit auf seinem System – oder wird von einer rekursiven Löschfunktion („`rm -rf /*`“) überrascht.

1.4 CSI/FBI-Studie 2005

Seit dem 18.07.2005 ist der zehnte jährlich von CSI und FBI publizierte Computer Crime and Security Survey 2005 verfügbar, der aufgrund der regelmäßigen Durchführung und der rund 700 Befragten ein sehr repräsentatives Bild der Entwicklung der IT-Security in den USA zeichnet (siehe auch Studien-Überblick in SSN 4/2002).

Die Ergebnisse sind immer wieder erhellend: So liegen die durchschnlittlichen jährlichen Ausgaben für IT-Sicherheit bei 200-300 US$ je Mitarbeiter, hat der Missbrauch von WLANs erheblich zugenommen und verschlüsseln schon 68% der Unternehmen ihre Daten während der Übertragung.

1.5 Vorsorgeüberwachung

Mit seiner Entscheidung vom 27.07.2005 (1 BvR 668/04) hat das Bundesverfassungsgericht die Regelung des niedersächsischen „Gesetzes über die öffentliche Sicherheit und Ordnung“ (SOG) über die Zulässigkeit einer Telefonüberwachung zur „Vorsorge für die Verfolgung oder die Verhütung dieser Straftaten“ (§ 33a) als mit dem Grundgesetz nicht vereinbar und daher nichtig erklärt.

Ein wichtiges Urteil, denn es setzt erstmals seit den New Yorker Terroranschlägen vom 11.09.2001 den ausufernden Begehrlichkeiten und Kompetenzerweiterungen deutscher Strafverfolgungs- und Sicherheitsbe-

hörden eine verfassungsrechtliche Grenze. Bleibt zu hoffen, dass auch der Bundesinnenminister die Begründung liest.

1.6 Security-Checklisten

Mit dem Cyber Security Research and Development Act des Jahres 2002 wurde das amerikanische NIST verpflichtet, Checklisten zu entwickeln, die es erlauben, das für Hard- und Software bestehende und mit deren Nutzung einher gehende Risiko in US-Bundesbehörden zu minimieren. Das NIST startete daraufhin das „Security Configuration Checklists Program for IT Products“ und veröffentlichte am 26.05.2005 die gleichnamige NIST Special Publication SP 800-70 und das NIST Beta Checklists Repository.

Die Checklisten im Repository sind derzeit nach elf Kategorien sortiert, die mit sicherheitsrelevanten Checklisten anderer Regierungsorganisationen (u.a. NSA, DISA, CIS) und von Herstellern befüllt werden. Inzwischen finden sich darin insgesamt schon mehr als 50. Ziel ist, auf der Basis standardisierter Checklisten und des Austauschs von Erfahrungen die Voraussetzungen für ein vereinheitlichtes „Basis-Sicherheitsniveau“ zu entwickeln. Die eingereichten Checklisten werden daher vom NIST mit 32 formalen Rahmenparametern charakterisiert.

Das NIST plant, für Checklisten, die von Herstellern eingereicht werden, ein SP 800-70-Konformitätssiegel zu vergeben. Im Fall eines Siegelerhalts verpflichten sich die teilnehmenden Hersteller, die Garantie der Herstellerserviceverträge auf die Anwendung dieser Checklisten auszudehnen. Noch gibt es weder eine einheitliche Struktur noch das geplante Siegel, daher wurde das Repository auch als „Beta“ eingestuft. Einen Vorgeschmack auf mögliche zukünftige standardisierte Checklisten gibt die Spezifikation des Extensible Configuration Checklist Description Format (XCCDF). Allerdings warten auch die NIST-eigenen Dokumente noch auf die Umsetzung in XCCDF.

1.7 Postraub anno 2005

Am 07.06.2005 musste die Citybank öffentlich den Verlust eines Backup-Bands mit ca. 4 Mio. Kundendatensätzen während eines Transports durch United Parcel Service (UPS) einräumen. Die vermissten Datensätze enthalten u.a. auch die Social Security Numbers – und bilden damit die Grundlage für zukünftige Identitätsdiebstähle. Kein Einzelfall: Ameritrade vermisst seit Jahresanfang ein Band mit 200.000 Kundendaten, Time Warner verlor ein Tape mit Daten von 600.000 Kunden, und der Bank of America fehlen seit Mai 2005 100.000 Kundendatensätze.

Die Sicherheitslücke scheint systematisch zu sein: Offenbar umfass(t)en die Sicherheitskonzepte zwar die Erstellung von Backups, nicht aber den Umgang mit dieser höchst sensiblen Konzentration kritischer Daten. So waren die Daten auf den Bändern weder verschlüsselt, noch erfolgte der Versand unter besonderen Sicherheitsauflagen, wie z.B. dem Rückgriff auf einen besonders vertrauenswürdigen und sicherheitsüberprüften Kurier.

1.8 PKI-Token-Evaluierung

Immer häufiger kommen – nicht nur in PKI-Umgebungen – Hardware-Token wie USB-Sticks oder Smartcards zum Einsatz, um vor allem kryptographisches Schlüsselmaterial geeignet vor Missbrauch zu schützen. Jedoch funktionieren diese Token nicht immer mit der gewünschten Anwendung, bzw. bestimmte Anforderungen an die Sicherheit werden entgegen den Herstellerangaben nicht erfüllt.

Die DFN-CERT Services GmbH hat daher gemeinsam mit SURFnet mehrere dieser Hardware-Tokens intensiven Tests unterzogen. Die Autoren des Reports prüften die Verwendbarkeit von USB-Token zur PKI-Unterstützung in verschiedenen Standard-Anwendungen (u.a. Internet Explorer, Outlook, Mozilla, Acrobat) unter Windows und Linux. Mangels Teststellungen durch die Hersteller konnten von ursprünglich 20 ausgewählten nur acht Token getestet werden, von denen nur sechs aktiv Private-

Key Operationen im Token durchführen. Von diesen wiederum ist nur ein einziges in der Lage, Operationen mit asymmetrischen Schlüsseln durchzuführen, die länger sind als 1024 bit.

Das Ergebnis der Untersuchung ist wenig überraschend: Microsoft-Anwendungen und aktuelle Windows-Versionen werden allgemein gut unterstützt, auch wenn dem Benutzer einiges Mitdenken abgefordert wird. Bei Windows-Anwendungen, die über die PKCS#11-Schnittstelle bedient werden, traten bei verschiedenen Token Fehler auf. Auch decken sich Herstellerangaben nicht immer mit der Realität. Die Unterstützung für Linux bleibt vergleichsweise rudimentär.

2 Secorvo News

2.1 Secorvo College aktuell

Am 20.09.2005 startet das Programm des zweiten Halbjahrs 2005. In den bis dahin verbleibenden beiden Monaten werden alle Seminare einem gründlichen „Lifting“ und alle Vorträge – wie in jeder Seminarpause – einer systematischen Aktualisierung und Überarbeitung unterzogen.

Mehr noch: Unser Seminarangebot 2006 wird um neue Seminare zu aktuellen und spannenden Themen der IT-Sicherheit erweitert – mehr dazu im September. Auf ein Wiedersehen in Karlsruhe!

http://www.secorvo.de/college

2.2 eco-AK “Sicherheit”

Nach dem großen Zuspruch, den die Sitzung des von Dirk Fox geleiteten Arbeitskreises „Sicherheit“ des eco e.V. zum Thema „Zertifizierte Sicherheit“ am 08.04.2005 fand, wird die nächste Sitzung des Arbeitskreises am 16.09.2005 das Thema „Forensik“ vertiefen – wieder in den Räumen der Karlsruher Secorvo Security Consulting GmbH. Programm und Anmeldung sind in Bälde auf der Webseite des eco-Arbeitskreises verfügbar. Interessierte können sich in den E-Mail-Verteiler des Arbeitskreises aufnehmen lassen.

3 Veranstaltungshinweise

Juli 2005	
29.-31.07.	Defcon 13 (Defcon, Las Vegas)
August 2005	
01.-05.08.	14th USENIX Security Symposium (Usenix, Baltimore/US)
14.-18.08.	Crypto 2005 (IACR, Santa Barbara/US)
September 2005	
05.-09.09.	Computer Network Forensics Workshop 2005 (IEEE/Create-Net, Athen/GR)
16.09.	Forensik (AK „Sicherheit“ des eco e.V.)
20.-21.09.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
22.09.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
27.-29.09.	Web-Application Security (Secorvo College, Karlsruhe)
Oktober 2005	
04.10.	Datenschutz kompakt (Secorvo College, Karlsruhe)
05.-06.10.	Inside Windows Security (Secorvo College, Karlsruhe)
11.-13.10.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
25.-27.10.	Spurensuche im Web (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

Secorvo Security News
August 2005

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

Nr. 8, 4. Jhrg. 2005
Stand 24. August 2005

ISSN 1613-4311

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

Inhalt

Editorial: Der Phisher und die 7 Geißlein

1 Security News

1.1 Web Password Hashing

1.2 iTAN

1.3 XP-Client-Honeypots

1.4 Anonym ins Web

1.5 Lage der IT-Sicherheit

1.6 Bluetooth-Kfz-Attacken

1.7 Infosec Dictionary

1.8 Wettlauf mit der Zeit

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Mehr Datenschutz

2.3 IT-Forensik

2.4 Neues Video verfügbar

3 Veranstaltungshinweise

Impressum

Editorial: Der Phisher und die 7 Geißlein

„Liebe Kinder, sperrt die Türe gut zu und nehmt euch in acht vor dem Wolf! (...) Der Bösewicht verstellt sich oft, aber an seiner rauen Stimme und an seinen schwarzen Füßen werdet ihr ihn gleich erkennen.“
Gebrüder Grimm, Der Wolf und die sieben Geißlein

Fast gleichlautend lesen sich die Mahnungen der deutschen Banken. Letztere leiden unter der zunehmenden Flut von Phishing-Angriffen: Im Mai 2005 zählte Messagelabs über 9 Mio. Phishing-E-Mails, ein trauriger Rekord. Die Anti-Phishing Working Group erhielt im Juli 2005 über 14.000 Phishing-Reports, im Juli 2004 waren es erst 2.000.

Bisher ließen sich deutsche Phishing-E-Mails leicht an der „rauen Stimme“ erkennen: Das Deutsch war holprig, die Geschichte unglaubwürdig. Aber der Wolf hat Kreide gefressen – neue Phishing-E-Mails sind sprachlich einwandfrei und klingen plausibel. Und auch die Pfote ist nicht mehr verräterisch schwarz – die gefälschten Webseiten der Phisher sind perfekt nachgebildet, verwenden originale Frames, Grafiken, Schriften und Texte.

Einige Banken unterstützen die Phisher, indem sie E-Mails an ihre Kunden senden, oft im HTML-Format, manchmal sogar mit verborgenen Links. Häufig werden zudem Domains für das Online-Banking verwendet, die auch einem Phisher gehören könnten, oder SSL-Zertifikate, die nicht zweifelsfrei die Bank als Anbieter erkennen lassen.

Wenn zugleich E-Commerce-Anbieter aus falscher Sparsamkeit selbst signierte SSL-Zertifikate nutzen, der Support bei abgelaufenem Zertifikat empfiehlt, die Sicherheitseinstellungen des Browsers herab zu setzen oder die Warnung vor einer unverschlüsselten Passwortübertragung zu deaktivieren, muss man sich nicht wundern, wenn die Geißlein keine Chance haben.

Irgendwann passt auch das Märchen nicht mehr. Zumal es bei grenzüberschreitendem Phishing ohnehin schwierig ist, dem Wolf den Bauch aufzuschneiden und die Geißlein lebendig herauszuholen. Passender wird dann vom „Tapferen Phisherlein“ zu berichten sein: Sieben auf einen Streich.

1 Security News

1.1 Web Password Hashing

Von einem Forschungsteam der Stanford University wurde auf dem USENIX Security Symposium Anfang August ein interessantes Verfahren zur Individualisierung von Internet-Passworten vorgestellt. Das Tool und Verfahren Pwd-Hash erfordert keine Änderungen an den Systemen und ist für die Benutzer weitgehend transparent.

Die – oft identischen – Passworte der Benutzer werden mit einem Browser-Plugin (derzeit verfügbar für Mozilla und Internet Explorer) durch ein für jede Zieldomäne individuelles Passwort ersetzt. Hierbei dienen die Ziel-Website, das ursprüngliche Passwort und bei Bedarf ein „salt“ auf dem Clientsystem als Eingangsgrößen. Eine Pseudozufallsfunktion berechnet daraus dann ein neues Passwort. Fällt einem Angreifer auf einem schlecht geschützten System eine Passwortdatei in die Hände, kann er nicht mehr einfach mit derselben User-/Passwortkombination auf weitere sensiblere Systeme zugreifen.

Hierdurch wird implizit in vielen Fällen auch ein Schutz vor Phishing-Angriffen geboten, da die Plugins gefälschte Zielsysteme anhand des Domänennamens vom Originalsystem unterscheiden können.

1.2 iTAN

Auf Phishing-Angriffe reagieren jetzt auch die deutschen Banken mit zusätzlichen Sicherheitsmerkmalen. Die Postbank meldete am 07.08.2005, dass sie ihr PIN-TAN-Verfahren um ein iTAN genanntes Merkmal ergänzt: Zukünftig sind die TAN auf der Liste indexiert. Bei jeder Transaktion schickt der Bankserver den Index, und nur die passende TAN ist gültig. Dieser einfache Challenge-Response-Mechanismus entwertet abge-„phishte“ TAN, denn die Wahrscheinlichkeit, dass eine solche passt, sinkt auf 1/(Anzahl TAN je Bogen). Die iTAN schützt nicht vor allen Angriffen, erhöht aber die Sicherheit des Online-Bankings deutlich.

1.3 XP-Client-Honeypots

Honeypots werden immer beliebter (SSN 5/2005). Während diese jedoch üblicherweise als Server implementiert werden, der darauf wartet, von Angreifern oder Würmern kompromittiert zu werden, verfolgen Forscher von Microsoft Research einen anderen interessanten Ansatz: Im Rahmen des Projekts „Strider HoneyMonkey“ surfen Windows-XP-Clients ständig durch das World Wide Web und identifizieren dabei Webseiten, die insbesondere auf Grund von Schwachstellen im Internet Explorer geeignet sind, einen XP-Rechner zu kompromittieren. Die Rechner verwenden dabei unterschiedliche Patch-Stände – von einem völlig ungepatchten XP-System bis hin zu einem mit den aktuellen Updates ausgestatteten Rechner. Da die Clients innerhalb von virtuellen Maschinen laufen, können sie nach „erfolgreicher“ Kompromittierung sofort und automatisiert in den Ursprungszustand gebracht werden.

Auf dem am 05.08.2005 in Baltimore zu Ende gegangenen USENIX Security Symposium stellte Microsoft im Rahmen eines Kurzvortrags erste Zwischenergebnisse vor. So gelang es den Forschern beispielsweise, innerhalb weniger Wochen 752 URLs zu identifizieren, nach deren Besuch ein ungepatchtes XP-System kompromittiert würde. Interessant ist ferner die Tatsache, dass viele dieser URLs von denselben Betreibern gehostet werden und zudem untereinander stark verlinkt sind.

Ob Microsoft die Informationen der HoneyMonkeys zu Gunsten von besser gepatchten eigenen Produkten nutzen wird, ist fraglich: Der Report enthält im Ausblick lediglich Statistiken und „legal actions“ gegen die Betreiber solcher Webseiten.

1.4 Anonym ins Web

Das Projekt AN.ON (TU Dresden) hat am 14.08.2005 eine neue Version des kostenlosen Anonymisierungsproxies zum Download bereit gestellt. Wie die vorhergehenden Versionen macht die Version 0.05.022 einen stabilen Eindruck – auch wenn sie offiziell als Testversion bezeichnet wird.

Durch JAP erfolgt der Zugriff beim Surfen verschlüsselt über einen extern gehosteten Proxy, der das MIX-Protokoll zur Anonymisierung verwendet. Da dieser in der Regel von mehreren Tausend Benutzern verwendet wird, kann eine Verbindung keinem bestimmten User zugeordnet werden. Wenn man die Protokollierungsfunktionen des Servers nicht berücksichtigt, ist so eine anonyme Internetnutzung möglich. Das einfache Updateverfahren, die umfangreiche Auswahl an Servern inklusive Aktualisierungsmöglichkeit und die Beschränkung der netzseitigen Zugriffsmöglichkeit auf die lokale Clientkomponente machen einen sehr guten Eindruck.

Allerdings werden hierdurch Content-Filter-Mechanismen von Unternehmensnetzen ausgehebelt, sofern ein Zugriff auf die Anonymisierungsdienste über HTTPS zugelassen ist. Auch Angriffe auf HTTP-Ebene können über den Proxy ausgeführt und somit nicht zurückverfolgt werden. Aus Sicherheitssicht ein Nachteil, aus Datenschutzsicht ein Gewinn.

1.5 Lage der IT-Sicherheit

Vom BSI wurde am 19.08.2005 ein Lagebericht zur IT-Sicherheit in Deutschland veröffentlicht – zur aktuellen Situation, Bedrohungen und Trends. Die Ergebnisse überraschen nicht: Der Stellenwert von IT-Sicherheit wird insbesondere angesichts der gewachsenen Abhängigkeit von einer funktionierenden IT nach wie vor unterschätzt. Auch wenn das Bewusstsein um die Bedrohungslage zugenommen hat, stellen nur 39% der Unternehmen ein höheres Budget zur Verfügung. Auch im öffentlichen Bereich fehlen finanzielle Mittel. Recht gut werden neuere Bedrohungen wie Phishing und Bot-Netze zusammengefasst.

1.6 Bluetooth-Kfz-Attacken

In den SSN 11/2003 und 8/2004 berichteten wir von Angriffsmöglichkeiten über Bluetooth. Die Wirklichkeit hat uns inzwischen eingeholt: Eine der Methoden, bei denen ein Angreifer Audiodaten in die integrierte Freisprechanlage eines Fahrzeugs einspielt, wird seit dem 02.08.2005 als Tool im Internet verbreitet. Opfer des Angriffs sind Bluetooth-Geräte mit fest voreingestellter zu einfacher PIN (z.B. 0000, 1234).

Mit dem Tool kann ein Angreifer nicht nur Musik wiedergeben, sondern auch ein lautstarkes „Bremsen!“ über die Lautsprecher erklingen lassen – kein Spaß bei hoher Geschwindigkeit. Liebe (Bluetooth-) Hersteller: Es gibt bessere Verfahren als feste PINs. Riskiert nicht die Gesundheit Eurer Kunden zu Gunsten eines vermeintlichen Bequemlichkeitsgewinns.

1.7 Infosec Dictionary

In der August-Ausgabe des CSO-Magazins erschien The Devil's Infosec Dictionary – ein unterhaltsames, leider z.T. sehr wahres Glossar zentraler Begriffe der Informationssicherheit.

1.8 Wettlauf mit der Zeit

Das Zeitfenster zwischen Fehlerentdeckung und Ausnutzung durch ein Angriffsprogramm schrumpft: Am 17.08.2005 meldete das Online-Magazin WindowsITpro, dass derzeit mindestens sieben Internet-Würmer (u.a. Zotop und RBOT) Systeme befallen, die den erst am 09.08.2005 veröffentlichten Microsoft-Patch MS05-39 nicht installiert haben. Betroffen sind Windows 2000, Windows XP und auch Windows 2003. Ein Testen und Einspielen der Patches wird dringend empfohlen.

2 Secorvo News

2.1 Secorvo College aktuell

Angesichts der wachsenden Herausforderungen, vor die sich Sicherheitsbeauftragte durch neue Kommunikationstechniken gestellt sehen, haben wir diesem Thema ein eigenes, neues Seminar gewidmet. Im Zentrum der dreitätigen Veranstaltung stehen sowohl die Bedrohungen und Risiken von E-Mail, WLANs, Bluetooth, Laptops, PDAs und Voice over IP als auch konkrete Schutzmöglichkeiten, von Verschlüsselung

über die SPAM-Abwehr bis zur Content-Filterung. Dabei stellen sich nicht nur technische Fragen; auch zahlreiche rechtliche Anforderungen sind bei der Umsetzung zu berücksichtigen. Das Seminar wird erstmals am **08.-10.11.2005** durchgeführt.

Alle Termine und Seminarangebote des zweiten Halbjahrs 2005 finden Sie unter

http://www.secorvo.de/college

2.2 Mehr Datenschutz

Seit dem 15.08.2005 gehört Karin Schuler zum Secorvo Team. Sie bringt mehr als 15 Jahre Erfahrung in IT-Sicherheit und Datenschutz mit und verstärkt vor allem unsere Expertise in Datenschutzfragen.

2.3 IT-Forensik

Forensische Fragestellungen treten immer öfter auf. Eine vertiefte Einführung bietet Secorvo College mit dem Seminar Spurensuche im Web (**25.-27.10.2005**). Auch die nächste Sitzung des eco-Arbeitskreises Sicherheit am **16.09.2005** ist dem Thema Forensik gewidmet.

2.4 Neues Video verfügbar

Zum Ende des vergangenen Jahres hatten wir es angekündigt – jetzt ist es endlich verfügbar: unser neues Lehrvideo „Passwort-Sicherheit“ zur Sensibilisierung von Mitarbeitern und Kollegen.

Das ca. zehnminütige Flash-Video nimmt sich dieses schon seit Jahren diskutierten Themas an und zeigt, was ein gutes Passwort ausmacht, wie leistungsfähig heutzutage die Tools und Methoden potenzieller Angreifer sind und was im Umgang mit Passworten beachtet werden sollte, um Angreifer auf Distanz zu halten. Einen kurzen Ausschnitt aus dem Video finden Sie in Kürze als Demo auf unseren Webseiten.

Das Video ist in deutscher Sprache als Einzel- und Intranet-Lizenz verfügbar, als Intranet-Lizenz auch in englischer Sprache. Weitere Sprachversionen erstellen wir auf Anfrage; nehmen Sie diesbezüglich gerne Kontakt mit uns auf.

3 Veranstaltungshinweise

September 2005	
05.-09.09.	Computer Network Forensics Workshop 2005 (IEEE/Create-Net, Athen/GR)
16.09.	Forensik (AK „Sicherheit“ des eco e.V.)
20.-21.09.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
21.09.	1. IT-Grundschutz Tag 2005 (BSI, Bonn)
22.09.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
27.-29.09.	ISSE 2005 (Teletrust, Budapest/H)
27.-29.09.	Web-Application Security (Secorvo College, Karlsruhe)
Oktober 2005	
04.10.	Datenschutz kompakt (Secorvo College, Karlsruhe)
05.-06.10.	Inside Windows Security (Secorvo College, Karlsruhe)
11.-13.10.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
14.-15.10.	hack.lu 2005 (CSRRT-LU, Kirchberg/L)
19.10.	2. IT-Grundschutztag 2005 (BSI,Fraunhofer SIT, St. Augustin)
25.-27.10.	Spurensuche im Web (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

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

1 Security News

1.1 To Patch Or Not To Patch

1.2 BDSG-Korrektur?

1.3 Multi-Plattform-Virus

1.4 DropMySecurity

1.5 Es geht auch „ohne“ (II)

1.6 Big Brother Awards

2 Secorvo News

2.1 Secorvo College aktuell

2.2 PhonoNet zertifiziert

2.3 Sicher ist nicht genug

2.4 IsSec/ZertiFA 2005

2.5 Team-Verstärkung

3 Veranstaltungshinweise

Impressum

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

Secorvo Security News
Oktober 2005

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

Nr. 10, 4. Jhrg. 2005
Stand 28. Oktober 2005

ISSN 1613-4311

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

Inhalt

Editorial:
Das Enigma-Trauma

1 Security News

1.1 Open Source und zurück

1.2 ISO 27001 + Grundschutz

1.3 No-NX

1.4 Pünktchen und Xerox

1.5 Where Do You Want to Surf Today?

1.6 Langzeitarchivierung

1.7 Überlistete Scanner

2 Secorvo News

2.1 Secorvo College aktuell

2.2 IsSec/ZertiFA 2005

2.3 Secorvo White Paper ISM

3 Veranstaltungshinweise

Impressum

Editorial: Das Enigma-Trauma

Mit der Veröffentlichung in der Wirtschaftswoche platzte am 05.10.2005 die Bombe: In einer internen Studie vom 20.09.2005 bescheinigt das BSI dem auch liebevoll Tamagotchi für Manager genannten Blackberry des kanadischen Herstellers RIM, er sei „auf Grund der unsicheren Architektur (...) für den Einsatz in der öffentlichen Verwaltung und spionagegefährdeten Unternehmen nicht geeignet“ – ein Verdikt, dass die Wogen hoch schlagen ließ. Die Angst: Der britische Geheimdienst könnte trotz Verschlüsselung über das in Egham bei London gelegene RIM-Rechenzentrum auf Verbindungs- und Inhaltsdaten zugreifen.

Ob hier ein Enigma-Trauma nachwirkt? Lange glaubte man bei den Nachrichtendiensten, auch dem BSI-Vorläufer ZfCh, an die Sicherheit der von der Wehrmacht eingesetzten Verschlüsselungsmaschine, bis Ende der 60er Jahre bekannt wurde, dass der britische Geheimdienst seit Anfang der 40er Jahre in Bletchley Park deutsche Funksprüche entschlüsselte.

Damit sich die Geschichte nicht wiederhole, informierte Lutz Diwell, Staatssekretär im BMI, bereits am 16.09.2005 alle Bundesministerien und bat „nachdrücklich, keine weiteren Investitionen in Blackberry-Geräte zu tätigen“. Statt dessen empfahl er, sich an einer in den Informationsverbund Berlin-Bonn (IVBB) integrierten Alternativlösung zu beteiligen, die „aufgrund der hohen Bedarfslage in der Bundesverwaltung“ von BMI, BMF und BSI „mit Hochdruck“ entwickelt werde und sich bereits im Pilotbetrieb befinde.

Nach RIM-Managerin Eggberry beruhen die BSI-Schlussfolgerungen „auf einem kompletten Mangel an Kenntnis von RIMs Sicherheitsarchitektur und –infrastruktur“. Für RIM und die Mobilfunkbetreiber steht viel auf dem Spiel: Schon über 3,65 Millionen Manager lassen sich ihre E-Mails direkt auf Blackberry oder Handy liefern.

Zur Versachlichung der Diskussion plant Secorvo für den 30.11.2005 eine Veranstaltung mit einem Vertreter von RIM und dem BSI in Karlsruhe – Näheres in Kürze.

1 Security News

1.1 Open Source und zurück

Kürzlich wurde das Unternehmen Sourcefire, maßgeblich an der Entwicklung des Open Source IDS-Systems snort beteiligt, durch Checkpoint übernommenen. Nun soll auch die nächste Nessus Version 3 zwar kostenfrei bleiben, aber vom maßgeblich am Nessus-Projekt beteiligten Unternehmen Tenable (siehe SSN 2/2005) als closed source weiterentwickelt werden.

Die Begründung des Tenable-Geschäftsführers Ron Gula, dieser Schritt sei auf zunehmende Kundenanfragen zurück zu führen, die OpenSource nicht einsetzen möchten oder können, klingt vorgeschoben. Auch anderen scheint es so zu gehen: So wurden bereits Nessus-Ableger wie die Projekte Porz-Wahn und GNessUs gegründet, die Nessus als Open Source unter GPL weiterentwickeln möchten.

1.2 ISO 27001 + Grundschutz

Seit dem 14.10.2005 ist die ISO 27001 nun offiziell publiziert und kann für 124 CHF unter http://www.iso.ch bezogen werden.

Mit der ISO 27001 wurde der britische Standard BS7799-2:2002 in einen internationalen Standard überführt. Die Änderungen zu BS7799-2:2002 sind eher gering. Es gibt einige wenige zusätzliche Detailanforderungen, eine leichte Umstrukturierung der Gliederung (das Kapitel 6.4 "Internal ISMS audits" aus BS7799 ist nun als eigenes Kapitel 6 geführt) und der normative Annex A (control objectives and controls) verweist jetzt auf die ISO/IEC 17799:2005 statt der 2000er Version.

Bestehende bzw. laufende Zertifizierungen nach BS7799-2:2002 sollten eigentlich nach ISO 27001 überführt werden können. Die für Deutschland zuständige Akkreditierungsstelle (Trägergemeinschaft für Akkreditierung GmbH) müsste hierzu ein entsprechendes „certification transition statement“ veröffentlichen; bislang scheint es ein solches aber nicht zu geben.

Das BSI hat das Sicherheitsmanagement beim IT-Grundschutz maßgeblich an den neuen ISO-Standard 27001 angepasst. Der BS 7799-2 Nachfolger ist ab 2006 auch Bestandteil der Zertifizierung nach IT-Grundschutz. Daher wurde zum 01.10.2005 auch das Lizenzierungsschema für IT-Grundschutzauditoren geändert: Die Anforderungen der internationalen Norm EA 07/03 müssen zukünftig erfüllt werden. Für bereits lizenzierte Auditoren werden entsprechende Kompaktkurse angeboten.

1.3 No-NX

Seit 2004 verfügen moderne x86-Prozessoren über ein „No Execute“ (NX) genanntes Sicherheits-Feature. Dieses Feature realisiert die schon seit vielen Jahren (zumindest in der Theorie) bekannte strikte Trennung zwischen Daten- und Codesegmenten, die vor allem dem Missbrauch der weit verbreiteten Buffer Overflow Bugs ein Ende setzen sollen. AMD bezeichnet diese neue Funktionalität gar als „Enhanced Virus Protection“; führt sie doch dazu, dass nicht mehr beliebiger Code im Stack oder Heap des Prozessors ausgeführt werden kann.

Noch bevor dieses Feature von allen Betriebssystemen unterstützt wird, gibt es bereits erste erfolgreiche Angriffe dagegen: am 04.10.2005 veröffentlichte Suse-Mitarbeiter Sebastian Krahmer einen technischen Artikel, in dem er zeigt, wie entsprechende Prozessorregister trotz gesetztem NX-Bit mit beliebigen Werten vorbelegt werden können. Dabei handelt es sich nicht um ausführbaren Code, sondern um beliebige Einsprungadressen, an denen Angreifer dann z. B. eigenen Code platzieren könnten. Und obwohl dieser Angriff nicht trivial ist, veröffentlichte der Autor zeitgleich einen unter Linux laufenden Proof-of-concept.

Fazit: Leider ein weiteres Beispiel für „gut gedacht, schlecht gemacht“...

1.4 Pünktchen und Xerox

Schon länger wird gemunkelt, dass hochwertige Farblaserdrucker und –kopierer auf jedem Ausdruck für das bloße Auge

unsichtbare Markierungen anbringen. Hauptziel solcher individueller Wasserzeichen ist es, leichter die Herkunft gefälschter Banknoten oder anderer „Wert"-Papiere aufspüren zu können.

Missbrauchsmöglichkeiten dieses Überwachungsmechanismus liegen aber genau so auf der Hand. Daher hatte die Electronic Frontier Foundation (EFF) dazu aufgerufen, Testseiten möglichst vieler verschiedener Druckertypen für Vergleichstests einzuschicken. Am 13.10.2005 wurde nun als Ergebnis dieser Bemühungen die Analyse des von Xerox verwendeten Markierungscodes aus winzigen gelben Punkten veröffentlicht.

Ein grundsätzliches Problem von derlei Wasserzeichen ist es, korrekt auseinander zu halten, wenn mehrere davon nacheinander angebracht wurden. Es ist daher wohl nur eine Frage der Zeit, bis die erste Software bereit steht, die es erlaubt, beim Ausdruck einer Seite „eigene" Xerox-Pünktchen anzubringen – unabhängig vom Hersteller des Druckers.

1.5 Where Do You Want to Surf Today?

Gleich auf mehreren Wegen versucht man im Moment, der Phishing-Plage Herr zu werden. So hat der Gouvernator von Kalifornien am 30.09.2005 einen Anti-Phishing Act of 2005 in Kraft gesetzt, der bei Strafandrohung von mindestens US$ 2.500 pro Fall (zuzüglich US-üblich hohen Schadensersatzforderungen) Phishing verbietet. Ob dieses Gesetz mehr Wirkung zeigt als Verbote anderer Straftaten, bleibt abzuwarten.

Technisch statt legislativ versucht es Microsoft: Bereits am 29.08.2005 wurde unter dem sperrigen Namen Microsoft® Phishing Filter Add-in for MSN® Search Toolbar (Beta) ein Zusatzmodul für den Internet Explorer 6 veröffentlicht, das eine Funktion der Version 7 vorweg nimmt. URLs bzw. Webserver, die nicht in einer lokalen Whitelist aufgeführt sind, werden von einem zentralen, von Microsoft betriebenen Server geprüft. Ist einer davon als Phishing-Server bekannt, wird der Anwender gewarnt.

Gegen Pharming, bei dem eine gültige URL mit DNS-Tricks auf den falschen Server „verbogen" wird, hilft dieser Ansatz alleine jedoch nicht viel. Und ob der erzielbare Sicherheitsgewinn gegen Phisher es aufwiegt, Microsoft direkt über (fast) alle aufgerufenen URLs zu informieren, darf auch bezweifelt werden.

1.6 Langzeitarchivierung

Die Universität Kassel führt im Auftrag des Bundesministeriums für Wirtschaft und Arbeit (BMWA) eine Studie über Anforderungen und Trends zur Langzeitaufbewahrung elektronisch signierter Dokumente unter der Leitung von Prof. Dr. Roßnagel durch. Dazu sollen Anwender aus Verwaltung und Wirtschaft sowie Hersteller von Aufbewahrungssystemen befragt werden.

Auf der Webseite des Projekts können der Fragebogen und weitere Informationen zur Studie abgerufen werden. Die Universität Kassel freut sich über eine rege Beteiligung bis zum 11.11.2005. Die Ergebnisse der Studie werden Mitte Dezember publiziert.

1.7 Überlistete Scanner

Zentrale oder dezentrale Virenscanner gehören schon seit vielen Jahren zu den Standard-Anwendungen jeder IT-Infrastruktur: Immer mehr verlässt man sich auf hohe Erkennungsraten sowie einwandfreie Funktionalität zum Schutz lokaler Netze.

Um so schlimmer, wenn systematische Schwachstellen in diesen Scannern gefunden werden, wie im Oktober gleich doppelt geschehen: Am 05.10.2005 veröffentlichten Mitarbeiter der SecuBox Labs ein Advisory, in dem sie beschreiben, wie bestimmte Archive so manipuliert werden können, dass Virenscanner nicht mehr in der Lage sind, diese auszupacken und nach Viren zu suchen. Und am 25.10.2005 beschrieb Andrey Bayora in einem weiteren Advisory, dass viele Scanner beim Erkennen von Dateitypen überlistet werden können, in dem wenige Bytes einer Datei verändert

werden, die jedoch weiterhin ausführbar bleibt – interessanterweise ist auf ein ähnliches Problem bereits im Jahr 2000 hingewiesen worden.

Von beiden Schwachstellen sind nahezu alle gängigen Produkte betroffen; viele Hersteller haben jedoch kurzfristig mit entsprechenden Patches ihrer Scanner reagiert. Fazit: nicht nur die Viren-Datenbanken müssen oft und regelmäßig aktualisiert werden, auch die Programme selbst bedürfen ständiger Updates.

2 Secorvo News

2.1 Secorvo College aktuell

Angesichts der aktuellen Entwicklungen beim IT-Grundschutz und dem ISO-Standard 27001 (siehe oben) haben wir unser Seminar „Information Security Management“ entsprechend aktualisiert. Am 14.-16.11. bzw. 14.-18.11.2005 erhalten Sie einen aktuellen Einblick in Best Practices, Standards und Zertifizierungserfahrungen.

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

2.2 IsSec/ZertiFA 2005

Am 05.-06.12.2005 lädt COMPUTAS nach Berlin zu der von Dirk Fox und Stefan Kelm inhaltlich mitgestalteten Doppelkonferenz IsSec/ZertiFA 2005. Das Programm lässt eine spannende Tagung erwarten.

2.3 Secorvo White Paper ISM

Das von Jörg Völker im November 2003 veröffentlichte Secorvo White Paper zum Sicherheitsmanagement nach BS 7799 hat sich mit seitdem mehr als 25.000 Downloads zum meistgelesenen White Paper von Secorvo entwickelt.

Inzwischen hat die Veröffentlichung des ISO 17799:2005 eine Überarbeitung erforderlich gemacht. Die Neufassung des White Papers steht inzwischen auf den Secorvo-Webseiten zum Download bereit.

3 Veranstaltungshinweise

November 2005	
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)
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)
27.-30.12.	22nd Chaos Communication Congress (CCC, Berlin)
Januar 2006	
24.-26.01.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
30.-31.01.	Net-ID 2006 (COMPUTAS, Berlin)

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

Secorvo Security News
November 2005

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

Nr. 11, 4. Jhrg. 2005
Stand 30. November 2005

ISSN 1613-4311

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

Inhalt

Editorial: Getrübter Blick

1 Security News

1.1 Codebreaker im Plan

1.2 BlackBerry Symposium

1.3 High-speed spoofing

1.4 Literaturpreis für Sober

1.5 Standards-Workshop

1.6 (w)Or(m)acle

1.7 Dunkle Seite der Macht

1.8 Neue Top 20-Liste

2 Secorvo News

2.1 Secorvo College aktuell

2.2 White Paper: BlackBerry

2.3 DuD 2006 – 27.-28. März

3 Veranstaltungshinweise

Impressum

Editorial: Getrübter Blick

Stellen wir uns vor, wir seien Politiker. Einflussreich, gerne gesehener Gast im Fernsehen und bei öffentlichen Veranstaltungen. Jovial, eloquent, erfolgreich. Und täglich Seite an Seite mit unserem Bodyguard unterwegs. Gepanzerter Dienstwagen, Fahrer mit wachsamem Auge und Fluchttraining. Schusssicheres Glas in Büro und Wohnzimmer, Personenkontrollen für jeden, der sich auf Wurfweite nähert, überwachter Schulweg für unsere Kinder. Aus einer solchen Perspektive nimmt sich Freiheit anders aus. Ertrüge man diese Randbedingungen über Jahre, erscheint es unvorstellbar, dass sie unser Urteil unbeeinflusst ließen – vor allem bei Fragen der inneren Sicherheit.

Das war schon so in den Hochzeiten des Terrorismus in Deutschland. Obwohl sich die Zahl der Opfer der menschenverachtenden Ideologie der RAF zum Glück zahlenmäßig in Grenzen hielt, wurde ihr eine polizeiliche Aufmerksamkeit zu Teil, die kein anderer Mörder je fürchten müsste – dabei war die Identität der Täter bekannt. Die Folgen des Perspektivwechsels ließen sich bei niemandem so ausgeprägt beobachten wie bei Bundesinnenminister Schily, der als ehemaliger RAF-Anwalt nach den Attentaten des 11.09.2001 die Befugnisse der Strafverfolgung fast geräuschlos ausweitete wie kein Minister zuvor.

Kaum hat die Große Koalition mit der Opposition im Bundesrat die letzte Bastion des Widerstandes geschliffen, wachsen die Begehrlichkeiten weiter: Die Vorratsdatenspeicherung von Telekommunikationsdaten und die Umwandlung des LKW-Maut-Systems in ein PKW-Verfolgungs-System stehen jetzt auf der Tagesordnung. Dabei bleiben die Strafverfolgungsbehörden bis heute den Nachweis schuldig, dass Großer Lauschangriff, Telefonüberwachung oder Rasterfahndung auch nur einen einzigen Täter überführt oder wenigstens abgeschreckt hätten. Aus der Perspektive des Kaninchens, das auf den Fuchs starrt, ist der mit wachsender Überwachung einher gehende Verlust an Lebensqualität jedoch offenbar kein gewichtiges Argument.

1 Security News

1.1 Codebreaker im Plan

Am 02.11.2005 konnte die auf dem Gebiet der angewandten Faktorisierung führende Arbeitsgruppe der Universität Bonn die beiden Primfaktoren der Zahl RSA-640 benennen und den von RSA Security Inc. ausgelobten Preis von $ 20.000 einstreichen.

Kein Grund zur Panik für Anwender des RSA-Verfahrens – es liegt alles im Plan: Weder ist dies ein neuer Weltrekord (bereits am 09.05.2005 hatte die selbe Gruppe die 663-Bit-Zahl RSA-200 gebrochen, siehe SSN 05/05), noch wurde ein radikal neuer Algorithmus angewandt. Das Resultat bestätigt lediglich die in den Jahren 2001 (Lenstra) und 2002 (Secorvo) aufgestellten Prognosen über den Fortschritt der Faktorisierung unter Berücksichtigung der Entwicklung der Rechenleistung.

Vielleicht gelingt der nächste große Durchbruch ja den Nachwuchs-Codebreakern, die die NSA derzeit mit ihrer CryptoKids™ Kampagne sucht.

1.2 BlackBerry Symposium

Die Diskussion um die bislang unveröffentlichte BSI-Studie vom 20.09.2005, die dem Push-Mail-System „BlackBerry“ der Firma RIM die Eignung für sicherheitskritische Bereiche abspricht, dauert an. Zum Glück hat sie wieder die Sachebene erreicht.

Zwei Veranstaltungen sind in den kommenden Tagen dieser Fragestellung gewidmet: Das von Secorvo veranstaltete „BlackBerry Security Symposium“ am 30.11.2005 in Karlsruhe und das Simedia-Tagesseminar „Sicherheit von E-Mail-Push-Diensten“ am 08.12.2005 in Bonn. Wer am 30.11.2005 verhindert ist, kann die Teilnehmerunterlagen auf CD online ordern.[1]

[1] Security Finder-Abonnenten finden Materialien zum Thema unter *Mobile Security*. Eine Darstellung des BlackBerry-Sicherheitskonzepts erschien in der DuD 11/05.

1.3 High-speed spoofing

Dass IP- sowie MAC-Adressen leicht gefälscht werden können, ist seit langem bekannt. Inzwischen existieren zahlreiche frei verfügbare Tools, mit denen ein Angreifer – ohne eigenes Know-how zu besitzen – derartige Spoofing-Angriffe durchführen kann. Dennoch wird vor allem die Kombination aus IP- und MAC-Adresse noch immer in vielen Netzbereichen zur Authentisierung verwendet.

Am 03.11.2005 nun veröffentlichte Paweł Pokrywka ein im Rahmen seines Master of Science-Studiengangs erstelltes Angriffsprogramm namens multispoof. Dieses Tool unterscheidet sich in zwei wesentlichen Punkten von bisher verfügbaren Spoofing-Programmen: zum einen kann es mehrere IP-/MAC-Adresskombinationen gleichzeitig fälschen (was den Datendurchsatz deutlich erhöhen kann), zum anderen fälscht multispoof nur inaktive Adressen, so dass es nicht zu Konflikten mit legitimen Benutzern kommt – was das Entdecken solcher Angriffe erheblich erschwert.

Will man diese Funktionalität nutzen, wird multispoof zunächst in einer Art „Lernmodus“ betrieben: Das Tool protokolliert dazu über einen bestimmten Zeitraum alle gültigen Adressen eines Netzes in einer eigenen Datenbank; anschließend nutzt es diese Informationen, um inaktive Adressen zu missbrauchen.

Wer noch immer auf IP- und MAC-Adressen als Authentisierungsmechanismus vertraut, den wird ein Probelauf von multispoof eines Besseren belehren...

1.4 Literaturpreis für Sober

Seit dem 19.11.2005 grassiert eine neue Variante des altbekannten E-Mail-Wurms Sober, die mancherorts sogar das Aufkommen an Spam-Mails in den Schatten stellt. Die hohe Verbreitung verursacht nicht etwa eine neue Verbreitungstechnik – sie ist einzig auf die bessere „literarische Qualität“ der Social-Egineering Komponente, vulgo E-Mail-Betreff und -Text, zurück zu führen: Unzählige Empfänger starten das komprimierte anhängende Schadprogramm.

Bleibt nur zu hoffen, dass die Versender von Phishing-Mails und Anwerbeversuchen für Geldwäscher noch eine Weile brauchen, bis sie mit ihren bislang meist sehr holprigen Texten diese Verführungsqualität erreichen.

1.5 Standards-Workshop

Für den 05.12.2005 lädt der ISO/IEC SC27 „Security Techniques" des DIN zu einem eintägigen internationalen Workshop nach Berlin. Das Programm der Veranstaltung ist viel versprechend; eine Anmeldung zu dieser unentgeltlichen Veranstaltung ist auch online möglich.

1.6 (w)Or(m)acle

Der Ablauf war schulbuchartig: Erst sprach man darüber (2002), dann wurde fachlich präzisiert (Q3/2005) – die praktische Umsetzung stellte sich dann von selbst ein. Am 31.10.2005 wurde der „Voyager Beta Worm" für Oracle anonym auf der Mailingliste Full-Disclosure veröffentlicht. Am 05. 11.2005 folgte eine Warnung von Oracle an alle Kunden.

Käme nun noch eine erfolgreiche Freisetzung des „Proof of Concept", müsste sich der Hersteller Oracle mit seinen 22 Sicherheitszertifizierungen wohl zu den Themen Compliance, SOX, Haftungs- und Schadensersatzansprüche neu positionieren. Die Checkliste anlässlich des aktuellen Vorfalls könnte sich dafür als unzureichend erweisen.

1.7 Dunkle Seite der Macht

Das durch das vielfältige Medienecho seit der ersten Meldung am 31.10.2005 zur Affäre gewordene Kopierschutz-„Rootkit" auf CDs von Sony BMG hat eine Welle der Empörung ausgelöst. Es lehrt zweierlei:

- Erstens sollte insbesondere derjenige, der bestrebt ist, sein eigenes geistiges Eigentum zu schützen, dasjenige von anderen peinlich genau beachten.

Denn sollte die eingesetzte Kopierschutz-Software tatsächlich die Open-Source Lizenzen GPL und LGPL verletzen, dann muss dies Konsequenzen für den Lieferanten der Software haben.

- Zweitens ist die Grenze zwischen unerwünschter Malicious Software und nützlichen System-Tools mindestens so durchlässig wie die zwischen den beiden Seiten der StarWars Macht.

Denn die Eigenschaften „gut" und „böse" lassen sich nicht aus technischer Funktionalität ableiten, sondern einzig aus der jeweiligen Nutzung. Und die ist oft nicht eindeutig, wie die Wandlung von NetBus vom Saulus (Trojaner) zum Paulus (Administrations-Tool) eindrucksvoll demonstriert.

Auch für Sony BMGs Kopierschutz, der in der öffentlichen Wahrnehmung ein Schritt auf die „dunkle Seite" war, haben findige Online-Spieler schon eine neue Anwendung ausgemacht: Sie verstecken damit ihre kleinen „Schummel"-Programme.

1.8 Neue Top 20-Liste

Zum fünften Mal veröffentlichte SANS am 20.11.2005 seine Liste der 20 kritischsten IT-Sicherheitslücken. Teilten sich diese bis 2004 nur zwei Klassen, nämlich Windows und Unix, wurde die Liste 2005 deutlich erweitert: Neben den Betriebssystemen Windows und Unix werden Sicherheitslücken in systemübergreifenden Programmen (wie Backup, DNS, PHP und Datenbanken) und in Netzkomponenten (wie Cisco) unterschieden.

Auch hat sich das Gewicht verschoben: Nur noch sieben der 20 Sicherheitslücken betreffen Microsoft (5) oder Unix (2). Die Liste ist auch nicht mehr „kumulativ", d.h. Sicherheitslücken, die 2005 in der Top 20-Liste vermerkt waren, werden 2006 nicht mehr aufgenommen.

Die in der – als Hilfestellung für Unternehmen gedachten – Aufstellung gelisteten Top-Sicherheitsmängel sollten schnellstmöglich durch das Einspielen der entsprechenden Patches beseitigt werden.

2 Secorvo News

2.1 Secorvo College aktuell

Das Seminarangebot von Secorvo College wartet im Jahr 2006 mit zahlreichen neuen Themen auf, darunter die sichere Gestaltung von IT-Outsourcing, die Praxis von IT-Sicherheitsaudits und das kürzlich erstmalig durchgeführte Seminar Kommunikationsschutz und Datensicherheit, das eine besonders gute Seminarbewertung erhielt.

Auf vielfachen Wunsch hat endlich auch der E-Commerce bei College Einzug gehalten: Mit dem Programm 2006 ist nun auch eine Online-Seminaranmeldung möglich – natürlich SSL-gesichert.

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

2.2 White Paper: BlackBerry

Die Sicherheit des BlackBerry-Push-Mail-Systems ist seit Bekanntwerden der internen BSI-Studie Gegenstand zahlreicher Diskussionen. Das am 23.11.2005 publizierte 12. Secorvo White Paper „BlackBerry Security“ stellt das Sicherheitskonzept des Push-Dienstes vor und bewertet die von RIM verwendeten Schutzmechanismen.

2.3 DuD 2006 – 27.-28. März

Das Programm der achten jährlichen Fachkonferenz „Datenschutz und Datensicherheit – DuD 2006“ am 27.-28.03.2006, seit 1999 von COMPUTAS in Zusammenarbeit mit den Herausgebern der Zeitschrift DuD konzipiert und durchgeführt, wird in Kürze verfügbar sein.

Das etablierte Treffen führender Datenschützer und IT-Sicherheitsverantwortlicher in Deutschland wird sich aktuellen Themen wie Phishing, Spam, Pharming, BlackBerry Security, Kundenkarten, Scoring und Honeynets widmen. Schon jetzt ist eine Voranmeldung möglich.

3 Veranstaltungshinweise

November 2005	
30.11.	BlackBerry Security Symposium (Secorvo, Karlsruhe)
Dezember 2005	
01.-02.12.	Der bDSB in der Praxis (Euroforum, Düsseldorf)
05.-06.12.	IsSec/Zertifa 2005 (COMPUTAS, Berlin)
06.-07.12.	Prüfung zum Certified IT Security Professional (CISP) (Secorvo College, Karlsruhe)
08.12.	Sicherheit von E-Mail-Push-Diensten (Simedia, Bonn)
27.-30.12.	22nd Chaos Communication Congress (CCC, Berlin)
Januar 2006	
24.-26.01.	IT-Sicherheit heute – Angriffe, Konzepte, Lösungen (Secorvo College, Karlsruhe)
30.-31.01.	Net-ID 2006 - Identity, Trust, Privacy & Security (COMPUTAS, Berlin)
Februar 2006	
07.-10.02.	PKI (Secorvo College, Karlsruhe)
14.-15.02.	Inside Windows Security (Secorvo College, Karlsruhe)
März 2006	
27.-28.03.	DuD 2006 (COMPUTAS, Berlin)

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

Secorvo Security News
Dezember 2005

Dirk Fox, Stefan Gora, Stefan Kelm,
Hans-Joachim Knobloch, Kai Jendrian

Secorvo Security Consulting GmbH

Nr. 12, 4. Jhrg. 2005
Stand 22. Dezember 2005

ISSN 1613-4311

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

Inhalt

Editorial:
War es Prometheus?

1 Security News

1.1 ETSI on the Road

1.2 Schwachstellenauktion

1.3 Generationenproblem?

1.4 OpenCA goes OpenXPKI

1.5 Happy New Year, Sober!

1.6 W2K3 SP1 CC EAL4+

1.7 Softies und Saboteure

1.8 Sandkastensicherheit

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Externer DSB

3 Veranstaltungshinweise

Impressum

Editorial: War es Prometheus?

Genug, ich traue den Geschenken nicht,
Die mir von solchen Freunden kommen!
Auf ein Kamin zu stellen, nun, dazu
Ist diese Büchse schön genug; gib immer her!
Christoph Martin Wieland, „Pandora“ (1779)

Vor über 200 Jahren geschrieben, und doch merkwürdig aktuell: Dies könnte das einleitende Zitat in der umstrittenen BlackBerry-Studie des BSI sein. Pandoras Büchse als Symbol für das unbekannte Gerät, die „Closed Source“-Software, die, einmal geöffnet, Übles über die Welt bringt.

Tatsächlich lässt sich das Bild auf praktisch jedes IT-System anwenden, das wir heute einsetzen. Kennen wir die Software? Wissen wir wirklich, was Prozessor und Hardwarekomponenten tun? Schließlich gibt es zahlreiche Möglichkeiten, ein Sicherheitssystem unbemerkt zu penetrieren: Manipulation der Schlüsselgenerierung, Erweiterungen des Kommunikationsprotokolls, oder, ganz perfide, verdeckte Informationskanäle wie vermeintliches „Padding“ zum Auffüllen der Datenpakete in Normlänge.

Erwiesenermaßen lässt sich nicht beweisen, dass ein IT-System nicht mehr als das Gewünschte leistet. Wir sind daher angewiesen auf Audits, im besten Fall eine Zertifizierung nach international anerkannten Standards wie den Common Criteria. Nur: Auch eine solche Zertifizierung zeigt lediglich, dass es in einer konkreten Version keine Hintertür gab – mit jedem Versionswechsel, ja mit jeder Neuübersetzung des Codes kann sich das ändern, bei Vorsatz ohnehin. Lernen wir also von Hesiod:

Erstens: Es ist gar nicht ausgemacht, dass Pandora die Büchse geöffnet hat – womöglich war es ihr Schwager Prometheus oder Epimetheus, ihr Gatte. Mit Verdächtigungen sollte man also vorsichtig sein.

Zweitens: Inzwischen gilt als erwiesen, dass es gar keine Büchse war, sondern ein Krug – ein Übersetzungsfehler. Dem geschriebenen Wort sollte man demnach lieber nicht automatisch trauen.

Und drittens: Dem Krug ist auch *Ελπίς*, die Hoffnung, entwichen. Immerhin bleibt uns die.

1 Security News

1.1 ETSI on the Road

Vom 16.01. bis 19.01.2006 macht das European Telecommunications Standards Institute (ETSI) im Rahmen einer ICT-Roadshow durch mehrere europäische Länder in Deutschland Station und bietet vier Informationsveranstaltungen zu seinen Standardisierungsaktivitäten im Bereich Informations- und Kommunikationstechnik an.

Hochrangige deutsche ETSI-Vertreter werden über die Gremienarbeit referieren und die Vorteile von Standards für beteiligte Unternehmen beleuchten. Ziel der Roadshow ist es – neben der Präsentation aktueller Entwicklungen – vor allem, neue Mitglieder und aktive Teilnehmer für die ETSI-Gremien zu gewinnen – also eine gute Gelegenheit zur Kontaktaufnahme für alle, die ETSI-Standards nutzen, z. B. im Mobilfunk oder bei elektronischen Signaturen.

1.2 Schwachstellenauktion

Anfang Dezember versuchte ein Anbieter Informationen zu einer noch nicht veröffentlichten Excel-Schwachstelle via eBay zu versteigern. Die Auktion wurde angeblich auf Betreiben von Microsoft vorzeitig abgebrochen. Offensichtlich wollte der Anbieter die teilweise langwierige Behebung von Schwachstellen bei Microsoft kritisieren. Microsoft-Mitarbeitern wollte er bei Nennung des Rabatt-Codes „LINUXRULZ“ Vergünstigungen einräumen...

Tatsächlich hätte uns diese Auktion eine Vorstellung vom (Markt-) Wert einer Sicherheitslücke in einer verbreiteten Software liefern können – nicht uninteressant.

Dennoch: Schwachstellen sollten immer unmittelbar und zuerst, vor allem auch bedingungslos dem betroffenen Hersteller zur Verfügung gestellt werden. Über Probleme hierbei berichteten wir allerdings bereits in den SSN 9/2004.

1.3 Generationenproblem?

Am 08.11.2005 veröffentlichte eine Gruppe um den u.a. durch seine Angriffe auf den Clipper-Abhörchip bekannten Sicherheitsexperten Matt Blaze eine Sicherheitsanalyse von in den USA verwendeten Abhörgeräten für analoge Telefongespräche. Grundlage der Analyse waren ausschließlich öffentlich zugängliche Informationen und auf dem freien Markt erworbene Geräte.

Ergebnis: Verdächtige, die befürchten, abgehört zu werden, können durch das Senden von Signalisierungstönen die Aufzeichnungen über von ihnen geführte Telefongespräche manipulieren, teilweise sogar die Aufzeichnung vorzeitig abschalten. Das alles erinnert fatal an das Blue-Boxing, mit dem Captain Crunch vor mehr als 30 Jahren die Abrechnung von Gesprächen über AT&T deaktivieren konnte.

Die Frage drängt sich auf: Wie kann man heutigen Systemdesignern genug über Angriffe und Konzepte der Vergangenheit beibringen, damit sie nicht ständig altbekannte Schwachstellen in neuer Form wiederbeleben?

1.4 OpenCA goes OpenXPKI

Viele Jahre gab es bei der Frage nach geeigneter Software für den Betrieb einer eigenen PKI nur die Auswahl zwischen sehr teuren kommerziellen Produkten, der ins Microsoft Betriebssystem integrierten, teilweise rudimentären PKI und sehr aufwändigen „Bastellösungen“, bestehend aus frei verfügbaren OpenSource-Paketen und selbst entwickelten Skripten. Bereits 1998 versuchte deshalb das OpenCA-Projekt durch den Aufbau einer OpenSource-Toolbox samt graphischer Oberfläche dieses Problem zu adressieren. Mangels Ressourcen konnte sich OpenCA dennoch nie zu einer produktionsreifen Lösung entwickeln.

In den vergangenen beiden Jahren jedoch wurde OpenCA an vielen Stellen erheblich weiterentwickelt. Seit dem 09.12.2005 wird die Toolbox nun unter dem Namen OpenXPKI neu entworfen und fortgeführt. Open-

XPKI ist – vor allem im universitären Umfeld – bereits in vielen Organisationen im Einsatz: Beispielweise basieren auch die neuen Dienste der DFN-PKI auf OpenXPKI, wie am 18.10.2005 vorgestellt.

Fazit: Wieder einmal schafft es die „Open-Source-Szene“, eine ernst zu nehmende Alternative zu kommerziellen Produkten zu entwickeln.

1.5 Happy New Year, Sober!

Es gibt wenig, worauf man sich heutzutage noch verlassen kann. Aber ein Bekannter bleibt uns zumindest auch noch im neuen Jahr erhalten: der Sober-Wurm. Mitarbeitern des Herstellers F-Secure ist es gelungen, den Update-Mechanismus des Wurms zu entschlüsseln. Dabei entdeckten sie, dass ab 05.01.2006 mit einer neuen Sober-Angriffswelle zu rechnen ist.

1.6 W2K3 SP1 CC EAL4+

Was in der Überschrift aussieht wie ein Geekcode, bedeutet: Am 14.12.2005 gab Microsoft bekannt, dass Windows 2003 und XP in verschiedenen Versionen – jeweils mit Service Pack 1 bzw. 2 und ganz bestimmten Kombinationen von Hotfixes – sowie die Certificate Services von Windows 2003 nach Common Criteria (CC) mit Evaluation Assurance Level (EAL) 4+ zertifiziert wurden.

Neben der Angabe der Prüftiefe mit dem Marketing-wirksamen EAL-Wert ist bei einer CC-Evaluierung stets zu beachten, welcher Funktionsumfang denn geprüft wurde (siehe SSN 2/2005). Und hier steckt – wie bei vergleichbaren Evaluierungen anderer Betriebssysteme (u.a. Solaris, SuSE Linux, AIX) auch – der Pferdefuß: Einmal mehr wurde das Controlled Access Protection Profile (CAPP) angewandt, das keine besonderen Anforderungen an die Netzwerksicherheit stellt. Wörtlich heißt es da: „Any other systems [...] are assumed to be under the same management control”. Mit anderen Worten: Schon ein Internet-Anschluss verstößt gegen die der Zertifizierung zu Grunde liegenden Annahmen.

An zwei Stellen geht Microsoft löblicherweise über CAPP/EAL4 hinaus: Zum einen wurde neben den Grundanforderungen der CC auch der Umgang mit Schwachstellen (Flaw Remediation) mit geprüft. Zum anderen wurden die Certificate Services nach dem vom NIST speziell für PKI entwickelten Protection Profile CIMC evaluiert.

1.7 Softies und Saboteure

Eine am 21.12.2005 auf Deutsch veröffentlichte Studie wertet in sechs verschiedenen europäischen Ländern erstellte Umfragen zur Gefährdung der IT-Sicherheit durch interne Mitarbeiter aus. Die Studie wurde im Auftrag von McAfee erstellt, was angesichts eines Produktportfolios, das sich besonders dem Schutz gegen „Gefahren von innen“ widmet, wenig verwundert.

Die Zahlen werden aber auch all denen eine Hilfe sein, die Maßnahmen in den Bereichen Security Awareness oder interne Sicherheit begründen müssen und sich dabei nicht auf hinter vorgehaltener Hand gemunkelte Beispiele und Mutmaßungen verlassen wollen.

Bei der Klassifikation der internen Gefahren waren die Autoren humorvoll-kreativ: es wird nach fahrlässigen „Sicherheits-Softies“, verspielten „Gadget-Freaks“, Umnutzung durch „Illegale“ (im englischen Original der Studie: „Squatter“ – Systembesetzer) und vorsätzlichen „Saboteuren“ unterschieden.

1.8 Sandkastensicherheit

Auch in einem Sandkasten kann hin und wieder etwas passieren, was von den Erbauern so nicht vorhergesehen wurde. Das ist mit Kindern auf dem Spielplatz im realen Leben ähnlich wie bei Software in einer virtuellen Maschine.

Am 21.12.2005 wurde auf [Full-Disclosure] von Tim Shelton auf eine Schwachstelle in den meisten VMWare-Versionen (außer ESX-Server) hingewiesen. Durch einen Fehler in der NAT Implementierung wird ein Nutzer des Gastsystems in die Lage

versetzt, Kommandos auf dem Wirtssystem auszuführen.

Das Konzept der virtuellen Maschinen ist nicht nur aus Verfügbarkeitsgründen ein wertvoller Schritt in Richtung erhöhter Sicherheit. Auch wenn dies der erste nachgewiesene Einbruch in das Hostsystem ist, darf man sich allerdings nicht in der trügerischen Sicherheit wähnen, dass diese Maschinen in allen Fällen wasserdicht sind. Sehr kritische Systeme sind daher nach wie vor auf einer eigenen (Hardware-) Plattform besser aufgehoben. Bei der Mehrzahl der Systeme dürften die Vorteile der Virtualisierung die Risiken aber überwiegen.

2 Secorvo News

2.1 Secorvo College aktuell

Für den „Jahrgang 2006“ wurde das bewährte Seminar Public Key Infrastrukturen um einen (optional buchbaren) vierten Tag erweitert, an dem die an den vorangegangenen Tagen vermittelten Grundlagen und Erfahrungen aus zahlreichen PKI-Projekten in Workshop-Form in die Praxis umgesetzt werden können. Es findet erstmals vom 07.-10.02.2006 statt.

Der Workshop-Tag kann auch separat oder zusammen mit dem dritten Seminartag, der fortgeschrittene PKI-Fragestellungen adressiert, gebucht werden.

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

2.2 Externer DSB

Für mehrere Unternehmen hat Secorvo bereits die Funktion des externen Datenschutzbeauftragten übernommen. Mit Karin Schuler, Volker Hammer und Dirk Fox stehen jetzt drei erfahrene Datenschutzexperten für diese Aufgabenstellung zur Verfügung. Eine detaillierte Leistungsbeschreibung kann unter info@secorvo.de angefordert werden.

3 Veranstaltungshinweise

Dezember 2005	
24.12.	Heiligabend
Januar 2006	
16.-19.01.	ETSI ICT Roadshow (Vier Veranstaltungen in Bonn, Mainz, Ulm, München)
24.-26.01.	IT-Sicherheit heute – Angriffe, Konzepte, Lösungen (Secorvo College, Karlsruhe)
30.-31.01.	Net-ID 2006 – Identity, Trust, Privacy & Security (COMPUTAS, Berlin)
Februar 2006	
07.-10.02.	PKI (Secorvo College, Karlsruhe)
14.-15.02.	Inside Windows Security (Secorvo College, Karlsruhe)
20.-21.02.	IT-Governance (COMPUTAS, Berlin)
20.-23.02.	Sicherheit 2006 (Gesellschaft für Informatik, Magdeburg)
28.02.-03.03.	Black Hat Europe 2006 (Black Hat, Amsterdam)
März 2006	
01.-02.03.	DFN-CERT-Workshop (DFN-CERT, Hamburg)
27.-28.03.	DuD 2006 (COMPUTAS, Berlin)
28.-29.03.	D-A-CH Security 2006 (Universität Klagenfurt)

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