secorvo
security consulting

Secorvo Security News

August 2007

Editorial: Digitaler Blockwart

Irren ist menschlich. Aber wenn man richtig Mist bauen will, braucht man einen Computer.
Dan Rather

Seit dem 11.07.2007 liegt der offizielle Abschlussbericht des BKA-Feldversuchs zur Foto-Fahndung vor. Von Oktober 2006 bis Januar 2007 war im Hauptbahnhof Mainz die automatische Gesichtserkennung als Fahndungshilfsmittel mit 200 Freiwilligen untersucht worden. Die Ergebnisse sind in verschiedener Hinsicht ernüchternd. Statt der erhofften 80% lag die Erkennungsrate der drei evaluierten Systeme zwischen 17% und 29%, bei im Schnitt mehr als 22.000 Passanten täglich und einer False-Acceptance-Rate (FAR) von 0,1% (23 Personen/Tag). Bei guten Lichtverhältnissen stieg die Erkennungsrate auf bis zu 60%, nachts lag sie unter 20%. Damit sind die Systeme nach Überzeugung des BKA-Präsidenten Jörg Ziercke für den polizeilichen Einsatz untauglich.

Nun übertrifft aber schon ein System, das in Stoßzeiten aus 50-100 Personen pro Minute bei Tageslicht mehr als die Hälfte von 200 Gesuchten herausfiltert, bei weitem die Erkennungsleistung menschlicher Beobachter. Und zweifellos wird die Systemleistung in den kommenden Jahren steigen: Höher auflösende Bilder, verbesserte dreidimensionale Erkennungsalgorithmen und schnellere Prozessoren werden ihren Teil dazu beitragen. Auch durch einfache Maßnahmen wie eine Aufmerksamkeit heischende Laufschrift in Kameranähe lässt sich die Erkennungsrate deutlich verbessern.

Sobald öffentliche Räume hierzulande ähnlich umfassend mit Videokameras ausgeleuchtet sind wie in London ist es nicht mehr weit bis zur „Knopfdruckfahndung“: Bilddaten eingespeist, und kurz darauf laufen die Treffer ein. Der Preis, den wir für die automatisierte Verbrecherjagd zahlen werden, wird hoch sein. Denn selbst bei einer FAR von 0,001% (im Bereich der natürlichen Ähnlichkeiten) müssten wir allein in Ballungszentren jährlich mit über 100.000 Fehlidentifikationen rechen.

Deutschland, Land der Verdächtigen.

Inhalt

secorvo
security consulting

Security News

CrypTool 1.4.10 erschienen

Das von der Deutschen Bank und der TH Darmstadt entwickelte freie E-Learning-Programm „Cryptool“ erschien am 30.07.2007 in Version 1.4.10. Neu enthalten sind u. a. eine über 100seitige Präsentation, eine erheblich erweiterte und verbesserte Online-Hilfe, hybride Verschlüsselungsverfahren auf der Basis Elliptischer Kurven, Flash-Animationen für Enigma und AES sowie ein Dialog zur Bestimmung der Qualität eines Passworts. Das inzwischen 230seitige CrypTool-Skript wurde um aktuelle Erkenntnisse der Kryptographie ergänzt und glänzt mit verständlichen Beispielen. Die inhaltliche Dichte macht es vor allem für Leser mit Grundkenntnissen der Kryptographie zu einer Goldgrube.

Der König ist tot ...

... es lebe der König: Am 01.07.2007 wurde durch das Technical Committee JTC 1/SC 27 der ISO der ISMS-Standard ISO/IEC 17799:2005 in ISO/IEC 27002:2005 „Information technology – Security techniques – Code of practice for information security management“ umbenannt. Inhaltlich blieb er dabei unverändert.

Mit der Umbenennung hat die ISO einen wichtigen Beitrag zur Bereinigung der babylonischen Namensverwirrung im Bereich der sicherheitsrelevanten Standards geleistet – nach den Standards ISO/IEC 27001:2005 und ISO/IEC 27006:2007 existiert jetzt der dritte Standard im Nummernkreis 270xx. Die Numerierung verdeutlicht die „Verwandtschaft“ zu ISO 9001 (Qualitätsmanagement) und ISO 14001 (Umweltmanagement).

Sicherer Fensterln

Fast 20 Monate – genauer seit dem 27.12.2005 – im Netz, aber bisher ohne Erwähnung in den Security News: das lesenswerte und hilfreiche Microsoft TechNet-Handbuch „Bedrohungen und Gegenmaßnahmen“. Es fasst in 12 Kapiteln alle wesentlichen Sicherheitseinstellungen für Windows Server 2003 und Windows XP zusammen, verlinkt auf alle in diesem Kontext wichtigen Microsoft-Dokumente und ergänzt so die beiden Sicherheitshandbücher für Windows XP und Windows 2003 Server. Die Struktur wurde an den Aufbau der Benutzeroberfläche des Gruppenrichtlinien-Editors angelehnt. Nur das englische Original ist als zusammenhängende PDF-Datei verfügbar; die deutsche Fassung ist ein 14teiliges Online-Dokument.

Virtual Honeypots

Dass das Thema Honeypots immer wichtiger wird, verdeutlichen nicht nur zahlreiche Tools (SSN 08/2005, 12/2006). Auch Veröffentlichungen auf Konferenzen und White Paper nehmen zu. Dies hat zwei deutsche Autoren zu dem im Juli 2007 erschienenen Fachbuch „Virtual Honeypots – From Botnet Tracking to Intrusion Detection“ motiviert: Niels Provos und Thorsten Holz prägen seit vielen Jahren die „Honeypot-Szene“ und haben nun ihre Erfahrungen dokumentiert. Heraus gekommen ist eine Publikation, die das Zeug zum Standardwerk hat: Alle aktuellen Themen rund um Honeypots/ Honeynets werden detailliert beschrieben. Dabei kommt die Praxis nicht zu kurz – die Autoren geben Installationshinweise für eine Reihe unterschiedlicher Tools und runden das Thema durch mehrere Fallstudien ab. Lance Spitzner – Gründer des Honeynet-Projekts – hält das Buch für „the best reference for honeypots today“. Kaufempfehlung.

Neugefasster Leitfaden

Am 20.06.2007 wurde der Bitkom-Leitfaden zur Nutzung von E-Mail und Internet im Unternehmen in einer überarbeiteten Version 1.4 veröffentlicht. Darin werden alle im Zusammenhang mit der dienstlichen und privaten Nutzung relevanten und bei Regelungen zu berücksichtigenden gesetzlichen Bestimmungen aus dem Steuer-, Telekommunikations-, Datenschutz-, Mitbestimmungs- und Strafrecht zusammengefasst. Die neue Version berücksichtigt aktuelle Entwicklungen in der Rechtsprechung sowie die Bestimmungen des am 01.03.2007 in Kraft getretenen Telemediengesetzes (TMG), das das Teledienstegesetz (TDG), das Teledienstedatenschutzgesetz (TDDSG) sowie weitgehend auch den Mediendienste-Staatsvertrag (MdStV) abgelöst hat. Für Datenschutzbeauftragte und Betriebsräte ist die Lektüre dieses 50seitigen Leitfadens ein absolutes "Muss".

Botnetz-Bedrohung

Das seit Jahresanfang vom „Storm Worm“ aufgebaute Botnetz, dessen Schädling sich zunächst als Anhang vermeintlicher Gruß-E-Mails verbreitete, ist nach Einschätzung von Joe Stewart von SecureWorks inzwischen auf 1,7 Mio. infizierte Rechner (Zombies) angewachsen. Damit wäre es das bisher größte bekannte Botnetz – konzentriert auf eine einzelne Domäne wäre gegen die Gewalt eines konzertierten Denial of Service-Angriffs (DoS) wenig auszurichten.

Mikko Hyppönen, Chefanalyst von F-Secure, hält die Meldung jedoch für Hysterie: Seiner Einschätzung nach seien bis Mitte August keine 100.000 Rechner infiziert worden, und auch ein DoS-Angriff sei nicht zu befürchten – Botnetze dieser Größe ließen sich durch Vermietung viel attraktiver vermarkten. Mit

dieser Einschätzung liegt er jedoch falsch: Etliche Wissenschaftler, die „Storm Worm" untersuchten, berichten von Denial of Service-Attacken gegen ihre Systeme.

Außerdem zeichnen sich die „Storm Worm"-Betreiber durch eine gefährliche Kreativität aus. Die jüngste Variante des Wurms tauscht den Treiber tcpip.sys gegen eine Version, die den eigentlichen Schadcode nachlädt – und ist damit nach einem Eintrag in McAfees Labs Blog offenbar sehr erfolgreich. Ferner ändern die „Betreiber" solcher Botnetze über so genannte „Fast Flux" die DNS-Einträge sehr oft – teilweise im Minutentakt – so dass die Verursacher schwerer zu finden sind. Dass ein großes Botnetz eine erhebliche Bedrohung darstellt, steht außer Frage: Nicht nur als Spam-Quelle, sondern auch für Erpresserdrohungen z. B. gegen Sportwettenanbieter wurden Botnetze in der Vergangenheit „erfolgreich" eingesetzt.

RFIDIOt live

Auf der diesjährigen Blackhat führte Adam Laurie am 02.08.2007 auf recht unterhaltsame Weise das RFID-Tool RFIDIOt vor. Mit Hilfe des Tools können Daten von RFID-Chips ausgelesen und auf neue RFID-Chips übertragen werden („rfid cloning"). Damit können Zugangskontrollsysteme auf Basis einfacher RFID-Techniken kompromittiert werden.

Auch europäische Reisepässe lassen sich, wie wir feststellen mussten, mit RFIDIOt und einem handelsüblichen RFID-Lesegerät problemlos inklusive der gespeicherten Bilder auslesen – trotz Verschlüsselung, da die verwendeten Schlüssel aus dem maschinenlesbaren Bereich des Passes entnommen werden können. Zum Schutz vor Fälschung sind die RFID-Daten digital signiert; eine Veränderung der Informationen kann also prinzipiell erkannt werden. Da aber nicht alle Länder die Zertifikate überprüfen, werden selbstsignierte Informationen nicht überall als Fälschung erkannt. Wie sagte Manfred Rommel so treffend: „Halb richtig ist meistens ganz falsch."

Secorvo News

Secorvo College aktuell

Das zweite Halbjahr beginnt für Secorvo College am 18.09.2007 mit dem Klassiker „IT-Sicherheit heute" (nur noch wenige Plätze frei). Im Oktober folgen die Seminare „Public-Key-Infrastrukturen" (09.-12.10.2007) und „Information Security Management" (16.-19.10.2007). Anfang November bietet sich die nächste Gelegenheit zur T.I.S.P.-Zertifizierung (05.-10.11.2007); es folgt das Seminar „Sichere Softwareentwicklung" (13.-15.11.2007).

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

Forensische Checkliste

Die ersten Schritte nach einem Sicherheitsvorfall sind oft die entscheidenden, insbesondere dann, wenn das Ereignis im Rahmen einer forensischen Analyse im Detail untersucht werden soll. Viele Fehler werden in den ersten Minuten danach gemacht – etliche wichtige Informationen gehen unwiederbringlich verloren oder werden nicht ausreichend dokumentiert.

Um diese Informationserhebung zu erleichtern, hat Secorvo eine forensische Checkliste entwickelt, die die zu Beginn einer Analyse wichtigsten Fragen beinhaltet. Diese Checkliste hilft bei jedem wichtigen Sicherheitsvorfall – unabhängig davon, ob die anschließende Untersuchung selbst oder mit externer Unterstützung durchgeführt werden soll.

Bericht aus der Schlangengrube

Es war einmal – vor 20 Jahren: Der erste PC-Virus erblickt das Licht der Welt; er verbreitet sich über Disketten (wissen Sie noch, was das ist?). Vor 10 Jahren: Macro-Viren kommen auf, die sich in Word-Dokumenten via E-Mail verbreiten; 3-5 neue Varianten am Tag. Paradiesische Zustände. Denn 2007 sind es 16.000 neue Schädlinge pro Jahr, durchschnittlich 45 an jedem Kalendertag, weltweit verbreitet innerhalb von Sekunden über Botnetze.

Wie werden sie gefunden? Wie identifiziert? Was bedeutet diese Entwicklung für den Alltag im Viren-Labor? Und was droht für die kommenden 10 Jahre? Ein Live-Bericht über das Leben in der Schlangengrube von Angel Jodra, Virenanalyst bei Kaspersky Labs, auf dem kommenden Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am 27.09.2007, 18 Uhr (Schlosshotel Karlsruhe). Online-Anmeldung erforderlich.

Preiswürdig

Am 14.09.2007 wird der in diesem Jahr erstmals ausgelobte „Sicherheitspreis Baden-Württemberg 2007" im Rahmen der Fachmesse SafeKon von Innenminister Heribert Rech verliehen. Prämiert werden „herausragende Projekte der betrieblichen Sicherheit mit Zielsetzung Know-how-Schutz" und „mustergültige Projekte zur praxisgerechten Konzeption, Realisierung und Kontrolle unternehmensinterner Sicherheitsmaßnahmen".

So viel dürfen wir bereits verraten: Zu den vier Projekten, die diese in Deutschland einmalige Auszeichnung erhalten, zählt die von Secorvo unterstützte Security-Awareness-Kampagne der T-Systems Enterprise Services GmbH. Mehr in den September-News...

Veranstaltungshinweise

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

September 2007	
10.-13.09.	CHES 2007 (IACR, Wien/AT)
11.-13.09.	3rd International Conference on IT-Incident Management & IT-Forensics (GI, Stuttgart)
18.-20.09.	IT-Sicherheit heute (Secorvo, Karlsruhe)
24.-26.09.	ESORICS 2007 (TU Dresden, Dresden)
27.09.	Leben in der Schlangengrube (KA-IT-Si, Karlsruhe)
Oktober 2007	
09.-12.10.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
16.-19.10.	Information Security Management - von A(udit) bis Z(ertifizierung) (Secorvo, Karlsruhe)
November 2007	
05.-09.11.	T.I.S.P. Schulung (Secorvo, Karlsruhe)
13.-15.11.	Sichere Software-Entwicklung (Secorvo, Karlsruhe)

Fundsache

Auszug aus www.security-finder.de

Das lesenswerte White-Paper „Exploiting SAP Internals – a Security Analysis of the RFC Interface Implementation“ von Mariano Nunez Di Croce vom 08.03.2007 beschreibt zahlreiche Sicherheitslücken der RFC (Remote Function Call) Schnittstelle innerhalb von SAP und zeigt Gegenmaßnahmen auf. Die Ergebnisse wurden auch auf der Black Hat Europe 2007 präsentiert (siehe auch SSN 05/2007).

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

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