secorvo
security consulting

Secorvo Security News

Januar 2009

Editorial: Sammler

Die Begehrlichkeit kennt keine Schranken, nur Steigerung.
Lucius Annaeus Seneca (ca. 1-65 n. Chr.)

Wer die Datenschutzpraxis nicht nur aus den Gazetten kennt, den wundert eher Seltenheit als Ausmaß der aktuellen Datenschutzvorfälle. Technikentwicklung und explodierende Speicherkapazitäten lassen den Umfang personenbezogener Datensammlungen ständig anschwellen – deutlich schneller als die Sensibilität der für die Datenverarbeitung Verantwortlichen, und wohl auch die der Betroffenen.

Natürlich erfolgt die Verarbeitung immer zu deren eigenem Wohle: Schließlich geht es um zielgenauere Angebote, bedienungsfreundlichere Webseiten und Fehlerbeseitigung. Sobald ein „Mehrwert" winkt, sind die Betroffenen selbst nur zu gerne bereit, die Sammlungen um sensibelste Daten zu ergänzen.

Nirgendwo wird das deutlicher als am Beispiel von Google. Erst am 27.01.2009 hat das Unternehmen lautlos seine Datenschutzerklärung geändert: Neben den üblichen Web-Log-Daten (deren Zulässigkeit in Deutschland umstritten ist) und Cookies, die den Surfer eindeutig identifizieren, speichert Google nun auch Daten über die Nutzung der Google-Dienste. Chrome transferiert außerdem alle URLs, die der Nutzer besucht, direkt an Google. Und wer auf Seiten surft, die Google Analytics verwenden (99 % der Webseitenbetreiber ignorieren Googles Kennzeichnungspflicht), liefert Google sein komplettes Bewegungsprofil im Cyberspace. Schließlich sind da noch Google Mail und das Handybetriebssystem Android, bei denen Mail-Verzeichnisse, Adressbücher und Terminkalender nicht direkt mit dem lokalen PC, sondern über Googles Server abgeglichen werden.

Eine mächtige Datensammlung in den Händen eines einzelnen Unternehmens. Selbstverständlich werden diese Daten zu keinen anderen Zwecken genutzt als zu den in der Datenschutzerklärung angegebenen. Zumindest bisher. Wenigstens angeblich. Und gelöscht wird nach neun Monaten. Frühestens. Sagt Google.

Inhalt

Security News

PKI-Praxisprobleme

Eine möglichst weitgehende Kompatibilität mit unterschiedlichen, besonders auch älteren Datenformaten ist in den meisten Fällen ein erwünschtes Merkmal von IT-Systemen – für die Sicherheit ist sie es häufig jedoch nicht. Ein Beispiel aus der PKI-Welt: Während Kryptologen wegen der Schwachstellen im Hashalgorithmus SHA-1 bereits einen SHA-3 suchen (SSN 10/2008), akzeptieren gängige Systeme immer noch klaglos dessen mittlerweile gebrochenen Urgroßvater MD5 (SSN 3/2005).

Am 30.12.2008 präsentierte Alexander Sotirov beim 25C3 Kongress, wie er zusammen mit Kollegen amerikanischer und europäischer Forschungseinrichtungen ein Sub-CA Zertifikat erzeugen konnte, das denselben MD5-Hashwert hat wie ein SSL-Zertifikat, das die Forscher von einem öffentlichen Trustcenter signieren ließen. Über den heimlichen Zwilling des regulär bezogenen Serverzertifikats wurden die Forscher quasi zum ebenso unautorisierten wie unkontrollierten Unterverkäufer des betroffenen Anbieters – da es um eine Demonstration ging, rückwirkend nur bis Ende 2004. Während der Nutzen von SSL ohnehin umstritten ist, löste der Beitrag bei Trustcentern natürlich umgehend Aktivitäten und Klarstellungen aus.

Aber das Problem ist nicht auf SSL beschränkt: Am 17.01.2009 veröffentlichte Didier Stevens ein per Authenticode signiertes „Hello, World!"-Programm, dessen böser MD5-Zwilling, der damit ebenso gültig signiert ist, glücklicherweise nur so tut, als ob er die Festplatte löscht. Obwohl für den offiziellen Zeitstempel SHA-1 verwendet wird, gilt dieser ebenso für beide Programme, da in Authenticode-Zeitstempel nur die angebrachte Code-Signatur, nicht aber der eigentliche Programmcode eingeht. Die Software von Peter Selinger zum Erstellen von Programm-Zwillingen ist ebenfalls im Netz verfügbar.

Nicht den MD5, sondern die in der Praxis eher ungebräuchlichen Signaturalgorithmen DSA und ECDSA betrifft ein Security Advisory des OpenSSL Projekts vom 07.01.2009. Die OpenSSL-Implementierung derartiger Signaturen liefert bei der Prüfung u. U. andere Fehlercodes als beim verbreiteten RSA-Verfahren. OpenSSL selbst und weitere betroffene Systeme lassen auch „rechnerisch falsche" Signaturen als gültig durchgehen, weil sie diese speziellen Fehlercodes nicht richtig auswerten.

Allen drei Fällen ist gemeinsam, dass ihnen am einfachsten beizukommen wäre, wenn es die PKI-Software erlaubte, die für Zertifikats- bzw. Signaturprüfung akzeptablen Algorithmen auf diejenigen zu beschränken, die als sicher gelten und auch tatsächlich gebraucht werden. Die Herausforderung für die Hersteller wäre dabei nicht, diese Funktionalität einzubauen, sondern sie so umzusetzen, dass Anwender sie einfach und effektiv nutzen können.

No Risk – No Web

Die detaillierte Analyse „Bootkits – die Herausforderung des Jahres 2008" von Kaspersky Lab, publiziert am 18.12.2008, führt erneut eindrucksvoll vor Augen, welchen Bedrohungen alle Nutzer beim Surfen im Web ausgesetzt sind. Die Erkenntnisse sind keine bahnbrechenden Neuigkeiten. Ein Google-Whitepaper vom 04.04.2007 mit dem Titel „The Ghost In The Browser" enthält umfangreiche Analysen ähnlicher Bedrohungen beim Surfen im Web. Allerdings wird in der Bootkits-Analyse verdeutlicht, wie verschiedene Eigenschaften und architekturbedingte Schwachstellen oder Mängel des Internets clever ausgenutzt werden, um zufällige Opfer mit Schadsoftware zu infiltrieren.

Zur Zeit gibt es keine umfassenden Schutzmechanismen gegen entsprechende Attacken durch Drive-by-Downloads. Die meisten Ansätze erfordern entweder hohe Anpassungs- und Wartungsaufwände oder werden als Einschränkung des „Surfgenusses" empfunden; beides ist mit geringer Akzeptanz verbunden. Trotzdem sind aktuelle Virenscannersuites, spezielle Surftools (z. B. NoScript, RequestPolicy und zukünftig auch Application Boundaries Enforcer) sowie eine gehörige Portion Vorsicht angeraten, um wenigstens gegen die häufigsten Angriffe gewappnet zu sein. Unter Umständen kann ein Werkzeug wie Bothunter helfen, Fälle aufzuspüren, bei denen das Kind schon in den Brunnen gefallen ist. Leider ist das in der Regel nicht leicht zu erkennen.

Passwörter in Browsern

Am 12.12.2008 veröffentlichte Robert Chapin die Ergebnisse eines umfangreichen Tests der Passwortmanager aktueller Versionen der Windows-Browser Firefox, Chrome, Opera, Safari und Internet Explorer. Die Ergebnisse sind ernüchternd: Von 21 Tests bestanden Firefox und Opera ganze sieben – und schnitten damit am besten ab. Chrome und Safari erfüllten nur zwei Sicherheitsanforderungen.

Besonders ernüchternd: Allein Firefox und Opera überprüfen, ob das automatisiert eingetragene Passwort auch von derselben Internet-Adresse stammt, für die es gespeichert wurde, und ob das Protokoll (bspw. http vs. https) übereinstimmt. Und lediglich Firefox erwartet – als einziger der getesteten Browser – die Zustimmung des Nutzers, wenn Herkunftsadresse oder das Übermittlungsprotokoll im entsprechenden Eintrag des Passwortmanagers überschrieben werden soll.

Zwar sollte man zumindest auf mobilen Geräten ohnehin von der Nutzung eines Browser-Passwortmanagers absehen, sofern das System nicht vollständig verschlüsselt ist. Denn der verschlüsselte Passwort-Speicher könnte auf einem verlorenen System einer Brute Force-Attacke zum Opfer fallen. Dennoch ist eine Browser-Attacke für einen Angreifer sehr viel attraktiver: Mühe- und spurenlos lassen sich bei entsprechender Verbreitung der Schadsoftware in kürzester Zeit Millionen Passwort-Datensätze einsammeln – und sogar automatisiert missbrauchen. Ein Browser mit fehlerhaftem Passwortmanager ist ein Blankoscheck für „Drive-by"-Angreifer.

Wer sicher gehen will, dass der Passwortmanager seiner Browser-Version zumindest den wichtigsten Anforderungen genügt, sollte sie der von Chapin entwickelten Online-Überprüfung unterziehen.

Gelöscht ist gelöscht

Bekanntlich führt das Löschen einer Datei in modernen Betriebssystemen nicht zur Beseitigung der Daten vom Speichermedium. Zur großen Freude von Forensikern lassen sich daher oft alle Dateien rekonstruieren, die jemals auf einer Festplatte gespeichert wurden. In der Maßnahmenempfehlung M 2.167 der IT-Grundschutz-Kataloge des BSI wird für das sichere Löschen von Dateien folgerichtig ein zwei- bis dreimaliges Überschreiben empfohlen.

Datenschützer gehen noch weiter: Im IT-Grundschutz-Baustein B 1.5 „Datenschutz" vom 04.07. 2007 werden für das datenschutzgerechte Löschen von personenbezogenen Daten mindestens sieben, bei Daten hoher Schutzstufe sogar 33 Überschreibzyklen gefordert. Diese Forderung dürfte auf eine (missverstandene) Veröffentlichung von Peter Gutmann („Secure Deletion of Data from Magnetic and Solid-State Memory") vom 22.07.1996 zurück gehen – die sich auf inzwischen veraltete Festplattentechnologie bezog. Daher sorgte der Beitrag „Overwriting Hard Drive Data: The Great Wiping Controversy" von Craig Wright, Dave Kleiman und Shyaam Sundhar auf der ICISS 2008 (16.-20.12.2008) für Wirbel: Abgesehen von ein paar technischen Fehlern (siehe „Further Epilogue" in Gutmanns Papier) stellen die Autoren überzeugend klar, dass die Rekonstruktion eines einzigen, einmal überschriebenen Bits immer nur mit einer gewissen Wahrscheinlichkeit gelingt. Selbst wenn die Erfolgsaussicht 99,9 % erreicht, liegt die Wahrscheinlichkeit, eine nur 2 kB große Datei zu rekonstruieren, bei 0,000076 % (so viel wie ein 6er im Lotto). Merke: Ein einfaches, einmaliges und vollständiges Überschreiben genügt für ein sicheres Löschen.

Common PKI 2.0 erschienen

Am 20.01.2009 wurde Version 2.0 der Common PKI-Spezifikation (ehemals ISIS-MTT) vom T7 e. V., dem Verband der Trustcenter-Betreiber, und dem TeleTrusT e. V. veröffentlicht. Die neue Version wurde – unter Mitwirkung von Secorvo – dem aktuellen Stand der in der Common PKI zusammengestellten und profilierten internationalen Standards angepasst und trägt so der Entwicklung auf dem Gebiet der PKI-Standardisierung seit der Publikation von ISIS-MTT 1.1 (am 16.03.2004) Rechnung.

Eine wesentliche Neuerung von Common PKI 2.0 stellt die Signatur-API dar, die das PKCS#11-Profil von ISIS-MTT 1.1 ersetzt. Sie basiert auf der eCard-API-Spezifikation des Bundes, ist aber deutlich kompakter, da sie sich auf die Funktionen beschränkt, die zur Anwendung der in Common PKI definierten Datenformate für Signatur und Verschlüsselung benötigt werden.

Secorvo News

Secorvo College aktuell

Seit 2004 haben mehr als 250 Sicherheitsexperten das T.I.S.P.-Zertifikat erworben. Im März steht das erste T.I.S.P.-Seminar bei Secorvo College auf dem Programm. Frühbucher sollten sich bis zum 09.02.2009 die letzten vergünstigten Plätze sichern.

Damit Softwareentwicklung in Zukunft sicherer wird, hat ISSECO einen international Zertifizierungsstandard für Software-Engineers entwickelt. Eine Schulung mit Prüfung zum CPSSE (Certified Professional for Secure Software Engineering) bietet Secorvo erstmals im Februar und September an.

Neben Klassikern wie IT-Sicherheit heute und PKI hält Secorvo College spannende neue Themen aus allen Bereichen der IT-Sicherheit für Sie bereit. Termine und Seminar-Details finden Sie im Seminarkalender und den ausführlichen Seminarprogrammen.

Trau keiner Wahl ...

... die du nicht selbst gefälscht hast: Auf dem ersten Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) im neuen Jahr wird Dr. Jörn Müller-Quade das mit dem Deutschen IT-Sicherheitspreis 2008 ausgezeichnete "Bingo Voting" vorstellen – ein Verfahren, bei dem der Wähler einen Beleg erhält, der es ihm ermöglicht, die korrekte Zählung der eigenen Stimme zu überprüfen. Dr. Müller-Quade war einer der Gutachter vor dem Bundesverfassungsgericht zu elektronischen Wahlmaschinen und leitet das Europäische Institut für Systemsicherheit (E.I.S.S.). Der Vortrag findet statt am 19.02.2009 im Schlosshotel Karlsruhe, Beginn: 18 Uhr. Im Anschluss gibt es – wie gewohnt – Gelegenheit zum "Buffet-Net(t)working". Um Anmeldung wird gebeten.

Veranstaltungshinweise

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

Februar 2009	
03.-04.02.	19. SmartCard-Workshop (Fraunhofer, Darmstadt)
19.02.	Trau keiner Wahl, die du nicht selbst gefälscht hast (KA-IT-Si, Karlsruhe)
22.-25.02.	16th Int. Workshop on Fast Software Encryption (IACR, Leuven/BE)
März 2009	
09.-13.03.	T.I.S.P.-Schulung (Secorvo College)
15.-17.03.	Sixth IACR Theory of Cryptography Conference (IACR, San Francisco, US)
16.-19.03.	Third International Workshop on Secure Software Engineering (SINTEF, Fukuoka/JP)
17.-18.03.	16. DFN Workshop – Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
17.-19.03.	IT-Sicherheitsaudits (Secorvo College)
24.-25.03.	Security Awareness (Secorvo College)
31.03.-03.04.	Forensik - Verfahren, Tools, Praxiserfahrung (Secorvo College)

Fundsache

Einer der häufigsten Fehler in Datenbank basierten Web-Anwendungen ist die Anfälligkeit für SQL-Injection (Platz zwei der OWASP Top 10). Am 05.12.2008 haben die Oracle-Mitarbeiter Mark Fallon, Bryn Llewellyn und Howard Smith ein 67seitiges White Paper („How to write SQL injection proof PL/SQL“) mit wertvollen Hinweisen veröffentlicht, wie sich sichere SQL-Abfragen entwickeln lassen.

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Hans-Joachim Knobloch, Jochen Schlichting

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

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

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

secorvo
security consulting

Secorvo Security News

Februar 2009

Editorial: Double Cross

NSA offering ‚billions' for Skype eavesdrop solution. The register, 12.02.2009

Der Psychologe und Kommunikationswissenschaftler Paul Watzlawick wäre begeistert gewesen. In „Wie wirklich ist die Wirklichkeit" erläuterte er 1976 anschaulich das Phänomen der Interdependenz, illustriert am Beispiel geheimdienstlicher Desinformation („XX"). Hier finden wir nun ein Exempel in Reinkultur. Was lässt sich aus dem angeblichen Angebot der NSA lernen? Dass sie Skype tatsächlich nicht abhören kann? Oder dass sie den Eindruck erwecken möchte, dass sie es kann, damit Nutzer sich auf die Vertraulichkeit verlassen – und hemmungslos offen kommunizieren?

Tatsächlich lässt sich die Aussage systematisch analysieren. Angenommen, das Gerücht ist wahr. Wann würde die NSA davon profitieren? Fall 1: Sie kann Skype bisher nicht entschlüsseln und findet jemanden, der Skype bricht. Dann kann sie es – und gewinnt, selbst wenn es bekannt wird (denn erstens wird das mglw. für eine Desinformation gehalten, und zweitens gibt es bisher keine gute Alternative). Allerdings kostet sie das einen Milliardenbetrag. Fall 2: Findet sie niemanden, bleibt die Situation, wie sie ist – die Nutzer wissen nicht, dass sie niemanden gefunden hat und nicht abhören kann. Fall 3: Sie kann Skype bereits entschlüsseln und findet niemanden, der es schafft. Auch dann gewinnt sie – denn das stärkt das Vertrauen der Nutzer in Skype. Kritisch ist allein Fall 4: Sie kann Skype entschlüsseln, und jemand bricht Skype. Dann kann sie verlieren – nicht nur einen Milliardenbetrag für etwas, das sie nicht braucht, sondern auch die Nutzer, die bisher darauf vertrauten, dass die NSA nicht mithören kann. Daraus lernen wir: Die NSA ist sich sicher, dass das Brechen von Skype schwierig ist – es ist ihr entweder sehr viel Geld wert, oder sie ist überzeugt, dass es niemandem gelingen wird.

Übrigens: Man munkelt, Secorvo habe Skype gebrochen, wolle das Wissen aber nicht an die NSA verkaufen.

Jetzt sind Sie dran.

Inhalt

secorvo
security consulting

Security News

Wurm drin

Nun gibt es sicherlich zahlreiche Gründe, sich für einen Computer des Herstellers Apple zu entscheiden. Ein Grund hat allerdings inzwischen nur noch wenig Überzeugungskraft: Das Betriebssystem OS X sei erheblich sicherer als Windows. Am 13.02.2009 veröffentlichte Apple das Sicherheitsupdate 2009-001 für Mac OS X 10.4 und 10.5. Damit stopft Apple insgesamt 48 Sicherheitslücken in über 20 Betriebssystemkomponenten, darunter ein kritischer Zero-Day-Bug im Safari-Browser. Wer – ungeachtet des schlechten Abschneidens beim Umgang mit Passworten (siehe SSN 01/2009) – die Windows-Version von Safari nutzt, sollte umgehend auf Version 3.2.2 wechseln.

Spätestens jetzt wird es Zeit, auch unter OS X die Software-Update-Funktion zu aktivieren. Denn nun ist auch für Apple-Nutzer das Paradies zu Ende. (Vielleicht hätten sie besser nicht hineingebissen.)

Druckerpatch

Es ist so weit: Die Sicherheitsdisziplin des Patchens hat nicht nur Apple, sondern auch die Peripheriegeräte erreicht. Am 04.02.2009 veröffentlichte HP einen Security Patch für seine Laser- und Farbdrucker, der eine kritische Sicherheitslücke schließt. Geschickt ausgenutzt kann sie Unberechtigten den Zugriff auf Druckdateien ermöglichen.

Angesichts immer leistungsfähigerer „Embedded Systems“ und der zunehmenden Vernetzung von Kleinstgeräten wird es nun nicht mehr lange dauern, bis Security Patches auch beim digitalen Bilderrahmen, dem MP3-Player und dem E-Book-Reader zur Gewohnheit werden – sofern die Hersteller nicht endlich beginnen, ihre Entwickler in sicherer Softwareentwicklung zu trainieren. Dann könnte es bald Zeit werden, vom PC zur Schreibmaschine „upzugraden“.

Schwächelnde Profis

Nachdem der Hashalgorithmus MD5 gebrochen und der Secure Hash Standard (SHA) von 1993 erst 2002 und erneut im Oktober 2008 wegen neuerer Angriffe aktualisiert werden musste, schrieb das US-amerikanische NIST am 02.11.2007 ähnlich wie 10 Jahre zuvor beim AES eine „Cryptographic Hash Algorithm Competition“ aus. Bis zum 31.10.2008 konnten Kandidaten für einen Nachfolger des SHA-2 (Arbeitstitel: SHA-3) gemeldet werden.

Zwei Tage vor Beginn der ersten Hash Function Candidate Conference an der Universität Leuven veröffentlichte Fortify am 20.02.2009 die Ergebnisse einer Analyse der Referenzimplementierungen von 42 der vom NIST für Runde 1 akzeptierten und noch nicht gebrochenen Kandidateneinreichungen.

Ergebnis: Bei sechs Kandidaten fand Fortify mit seinem Source Code Analyser sicherheitskritische Bugs. Besonders peinlich: Die Implementierung des MD6 von Ron Rivest enthielt allein drei (!) Buffer Overflows – und das, nachdem ein Buffer Overflow in der RSA-Referenzimplementierung erst 1999 fast alle SSL- und SSH-Implementierungen kaltgestellt hatte. Merke: Trau' keiner Referenzimplementierung, die Du nicht selbst geprüft hast. Erst recht, wenn sie von einem Kryptologen stammt.

Web Apps – kritisch betrachtet

Mit der am 18.12.2008 erstmalig auf der OWASP-Webseite erwähnten Neuauflage des „OWASP Testing Guide“ wurde ein bewährtes Standardwerk zur Analyse von Web-Applikationen aktuellen Anforderungen angepasst und noch einmal erweitert. Die aktuelle Version v3 erleichtert durch die Einführung von Referenznummern für Testfälle die Kommunikation über Applikationstests gegenüber der Vorgängerversion v2 erheblich.

Inhaltlich wurden die meisten technischen Tests aktualisiert. Einige Testfälle wurden neu sortiert, so dass der neue Guide sich deutlich flüssiger liest, obwohl er um knapp 80 Seiten gewachsen ist. Bei den Tests stechen folgende Änderungen ins Auge: die ausführliche Erweiterung um den Bereich „Configuration Management Testing“, die Ergänzung um Aspekte von „Authorization Testing“ und weitere Änderungen beim „Data Validation Testing“.

Der Ansatz einer ganzheitlichen Betrachtung der Sicherheit von Applikationen über deren gesamten Lebenszyklus steht auch weiterhin im Vordergrund des Guides.

Ergänzend zu dem OWASP-Guide, der eine analytische Sicht der Sicherheit bietet, beleuchtet ein Positionspapier der ENISA zu „Web 2.0 Security and Privacy“ aus dem Dezember 2008 Sicherheits- und Datenschutzrisiken bei aktuellen Trends im World Wide Web. Die Kombination aus motivierendem Überblick und technischem Handwerkszeug gibt Verantwortlichen ausgiebiges Know-How zur Verbesserung der Sicherheit im WWW an die Hand.

Sametime – Same Password

Am 31.01.2009 veröffentlichte Carl Tyler in seinem Blog ein aus Sicherheitssicht kritisches Feature von Lotus Sametime: Ab Version 7.5 kann durch ein Plugin auf die gespeicherten Kennwörter im Klartext zugegriffen werden. Diese Funktion unter-

stützt die Realisierung von Single-Sing-On, könnte aber in verschiedenen Angriffsszenarien ausgenutzt werden: Meldet sich ein Benutzer in einer anderen Community an, die die Installation von Plugins zulässt, können dort ein Plugin installiert und die Sametime-Kennwörter ausgespäht werden. Auch könnte sich über diese Funktion ein Sametime/ Notes-Administrator Zugang zu den Kennwörtern verschaffen. Beide Szenarien sind besonders kritisch, wenn die Sametime-Kennwörter (benutzerfreundlich per Passwortsynchronisation) auch für weitere Anwendungen verwendet werden und somit ein unbefugter Zugriff auf weitere Daten möglich ist.

Sofern nur die im Notes Client integrierte Version von Sametime verwendet oder Samtetime über IBMs LTPA-Token authentifiziert wird, kann die Funktion nicht genutzt werden. In der Stellungnahme des Herstellers IBM vom 06.02.2009 wird darauf hingewiesen, dass derartige Funktionen beabsichtigt sind – und auch bei anderen Produkten wie Browsern verwendet werden, um beispielsweise ein Single-Sign-On zu ermöglichen. Um den eigenen Sicherheitsansprüchen gerecht zu werden, ist vorgesehen, in einer Technote auf die potentiellen Sicherheitsprobleme hinzuweisen und zu definieren, wie ein Schutz – beispielsweise durch eine digitale Signatur und Autorisierung für Plugins – erreicht werden kann. Betroffene Unternehmen sollten diese Diskussion verfolgen.

Helix ist tot, es lebe Helix

Nessus hat es vorgemacht (vgl. SSN 06/2008) – nun hat auch e-fense als Entwickler des äußerst populären Forensik-Werkzeugkastens Helix sein Lizenzmodell geändert. Seit dem 23.01.2009 ist Helix weder Open Source noch frei verfügbar. Wer künftig „Helix Pro“ einsetzen möchte, muss sich für ca. 15 Dollar pro Monat beim Hersteller registrieren lassen – was freilich noch immer deutlich preisgünstiger ist als die meisten anderen kommerziellen Forensik-Tools. Glücklich schätzen können sich diejenigen, die vor wenigen Monaten die letzte freie Version heruntergeladen haben (vgl. SSN 10/2008).

Fast zeitgleich mit der Kommerzialisierung von Helix ist übrigens am 11.02.2009 eine Beta-Version von Backtrack erschienen – eine Live-Distribution, die zumindest rudimentäre Forensik-Funktionen enthält.

Online Games – Serious Business

Am 28.01.2009 wurde im Presseportal der Polizei Nordrhein-Westfalen über eine kuriose Diebstahlanzeige berichtet: Ein Spieler eines Online-Rollenspiels war seiner virtuellen, mit viel zeitlichem und finanziellem Aufwand erworbenen Ausrüstungsgegenstände beraubt worden.

Die Anzeige wirft zahlreiche technische und rechtliche Fragen auf. Interessant ist allerdings, dass die Fragestellung deutlich präsenter ist, als vielleicht angenommen. Schon im November 2008 beleuchteten 18 Autoren in einem ENISA-Bericht „Virtual Worlds, Real Money“ auf 80 Seiten Sicherheitsrisiken und Empfehlungen für „Massively-Multiplayer Online Games and Social and Corporate Virtual World“. Ereignisse in zahlreichen „virtuellen Welten“ – nicht nur in Second Life – dürften in den kommenden Jahren in wachsendem Maße Auswirkungen in der „realen Welt“ haben. Der kurzweilig geschriebene Bericht gibt davon einen ersten Eindruck.

TCG-versiegelt

Die Trusted Computing Group (TCG), der u. a. Hersteller wie HP, IBM, Lenovo und Sun Microsystems angehören, hat am 27.01.2009 zwei richtungsweisende Standards zur Verschlüsselung von Speichersystemen sowohl für Desktops und Laptops als auch für Enterprise Lösungen veröffentlicht.

Angesichts der schwer verdaulichen 80 bzw. 130seitigen Standards gerät leicht aus dem Blick, dass die TCG damit die Grundlage für eine einheitliche und von den Chips der PC-Hardware-Hersteller unterstützte Verschlüsselung von Speichermedien gelegt hat. Sollte sich der Ansatz durchsetzen, könnten verschlüsselte Festplatten in wenigen Jahren der „Hardware-Standard“ sein – und die heutigen Spezialanbieter einschlägiger Softwarelösungen sich auf die allein schon herausfordernde Aufgabe des Schlüsselmanagements konzentrieren.

Secorvo News

Secorvo College aktuell

Nur noch wenige Seminarplätze sind im März für Sie frei: Vom 09.-14.03.2009 können Sie Ihr Wissen mit dem begehrten T.I.S.P.-Zertifikat besiegeln. Wertvolle Tipps für die erfolgreiche Umsetzung von Sicherheitsmaßnahmen zur Schließung von Sicherheitslücken bekommen Sie im Seminar "IT-Sicherheitsaudits in der Praxis" - nutzen Sie Ihre Chance, bevor auch dieses Seminar vom 17.-19. 03.2009 ausgebucht ist.

Im April halten wir einen Klassiker zu Grundlagenthemen für Sie bereit: "IT-Sicherheit heute" vom 21.-24.04.2009. Buchen Sie Ihren Platz noch bis zum 16.03.2009 mit Frühbucherrabatt. Alle weiteren Termine und Infos finden Sie auch in unserem Seminarkalender 2009.

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

Veranstaltungshinweise

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

März 2009	
09.-13.03.	T.I.S.P.-Schulung (Secorvo College)
15.-17.03.	Sixth IACR Theory of Cryptography Conference (IACR, San Francisco, US)
16.-19.03.	Third International Workshop on Secure Software Engineering (SINTEF, Fukuoka/JP)
17.-18.03.	16. DFN Workshop – Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
17.-19.03.	IT-Sicherheitsaudits (Secorvo College)
24.-25.03.	Security Awareness (Secorvo College)
31.03.-03.04.	Forensik - Verfahren, Tools, Praxiserfahrung (Secorvo College)
April 2009	
21.04.	2nd USENIX Workshop on Large-Scale Exploits and Emergent Threats (Usenix, Boston/US)
21.-24.04.	IT-Sicherheit heute (Secorvo College)
26.-30.04.	Eurocrypt 2009 (IACR, Köln)

Fundsache

Bereits am 10.12.2008 hat Google sein "Browser Security Handbook" unter Google Code veröffentlicht, um die Entwicklung sicherer Web 2.0-Anwendungen zu fördern. Seitdem haben die Autoren um Michal Zalewski die Gegenüberstellung der Sicherheitsfeatures aktueller Browser-Versionen aufgrund jüngster Tests mehrfach aktualisiert. Die Übersicht gibt wertvolle Hinweise zur Sicherheit aktueller Browser und geht damit über die Untersuchung von Robert Chapin (SSN 01/2009) hinaus.

Impressum

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

ISSN 1613-4311

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

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

secorvo
security consulting

Secorvo Security News

März 2009

Editorial: Zwangsbeglückung

Vor 22 Jahren erblickte der erste E-Mail-Sicherheitsstandard das Licht der Welt: In RFC 989 spezifizierte John Linn im Februar 1987 „Privacy Enhancement for Internet Electronic Mail“, einen frühen Vorläufer von S/MIME. Obwohl zahlreiche E-Mail-Clients, darunter Thunderbird, Notes und Outlook, heute S/MIME-basierte E-Mail-Verschlüsselung standardmäßig unterstützen und OpenPGP-Verschlüsselung sogar über die freie GnuPG-Programmfamilie komfortabel genutzt werden kann, sind E-Mails nach wie vor zumeist elektronische Postkarten.

Eine willkommene Gelegenheit, behütend einzugreifen: „*Der moderne Staat steht deshalb vor der Aufgabe, im elektronischen Kommunikationsraum für eine Grundversorgung an Verbindlichkeit und Vertraulichkeit zu sorgen*“, so das BSI im BSI-Forum der Fachzeitschrift <KES> (1/2008). „De-Mail“ soll der Dienst heißen, der ab 2010 mit Hilfe privatwirtschaftlicher „Bürgerportale“ einen Schlussstrich unter die chaotische Internet-Kommunikation ziehen soll.

Bei genauer Betrachtung entpuppt sich De-Mail als missratener Versuch, der digitalen Signatur nach 12 Jahren Misserfolgsgeschichte doch noch in den Sattel zu helfen. Das Konzept krankt an denselben Designfehlern: Wer De-Mail nutzt, schickt eine nicht abstreitbare Nachricht. Der Empfänger wiederum ist verantwortlich für das fristgerechte Abholen elektronischer Zustellurkunden. Eine Verschlüsselung erfolgt hingegen nur zwischen Nutzern und Bürgerportalen.

Am 23.03.2009 erlitt der Gesetzentwurf zur Regelung der Bürgerportale vom 04.02.2009 eine empfindliche Schlappe: Die Empfehlung der Ausschüsse des Bundesrats ist ebenso klarsichtig wie vernichtend: So seien die „konkreten Sicherheitsanforderungen an mehreren Stellen unklar“ und die Pflicht des Empfängers zur regelmäßigen Leerung des Postfaches ein unzumutbarer Grundrechtseingriff. Offenbar gibt es noch Volksvertreter, die nicht vergessen haben, dass der Idealtypus des „modernen Staates“ kein Leviathan, sondern eine freiheitliche Ordnung ist.

Inhalt

secorvo
security consulting

Security News

Klare Absage

So deutlich hat das Bundesverfassungsgericht weder bei der Online-Durchsuchung noch bei der Vorratsdatenspeicherung geurteilt: Am 03.03.2009 erklärte es den Einsatz von Nedap-Wahlcomputern und die Bundeswahlgeräteverordnung (BWahlGV) vom 20.04.1999 für verfassungswidrig, da „sie keine dem verfassungsrechtlichen Grundsatz der Öffentlichkeit der Wahl entsprechende Kontrolle sicherstellt". Denn es gilt: „Beim Einsatz von elektronischen Wahlgeräten müssen die wesentlichen Schritte von Wahlhandlung und Ergebnisermittlung [vom Wähler] zuverlässig und ohne besondere Sachkenntnis überprüft werden können." Ein klares Votum für die Souveränität des Souveräns (siehe SSN 10/2008) – und das an der Universität Karlsruhe entwickelte und mit dem IT-Sicherheitspreis 2008 ausgezeichnete „Bingo Voting" (Kurzbeschreibung).

Keine drei Wochen nach dem Urteil berichtete Matt Blaze, Mitautor einer Studie über Sicherheitsmängel einer in den USA verbreiteten elektronischen Wahlmaschine, am 23.03.2009 über die Aufdeckung systematischer Wahlfälschungen in Kentucky: Sechs Wahlhelfer hatten eine Schwäche in der Benutzerschnittstelle der Wahlmaschine zur Veränderung von Stimmabgaben genutzt.

SSL-Authentifikation für alle

SSL – seit zehn Jahren unter dem Namen Transport Layer Security (TLS) genormt – ist ein bekanntes, bewährtes und deshalb von seinem ursprünglichen Zweck, der Absicherung von Webzugriffen, auch auf andere Bereiche wie z. B. VPN oder WLAN übertragenes Sicherheitsprotokoll. Sollte man meinen. Auch sollte sich im Jahr 20 nach der Erstveröffentlichung des X.509 Standards herumgesprochen haben, dass Zertifikate naturgemäß öffentliche Daten sind und für sicherheitsrelevante Operationen das private Gegenstück des per Zertifikat bestätigten öffentlichen Schlüssels benötigt wird.

Umso größer die Verwunderung, als Microsoft am 10.03.2009 im Security Bulletin MS09-007 einräumte, dass die SSL-Komponente in Windows – vom Veteranen Windows 2000 bis zum neuesten 64-Bit-System – bei der Client-Authentifikation jahrelang patzte: Zwar wurde die Gültigkeit des vorgelegten Zertifikats geprüft; der im Standard vorgeschriebene Schritt, per Signatur der ausgetauschten Protokollnachrichten zu verifizieren, dass der Client auch den passenden privaten Schlüssel verwendet, wurde jedoch eingespart. Tatsächlich akzeptierte der Server also jeden Client mit irgend einem gültigen Zertifikat - ob nun dem eigenen oder einem fremden.

Durch das weite Einsatzspektrum von SSL/TLS sind wahrscheinlich nicht nur IIS-basierte Webanwendungen von diesem Bug betroffen, sondern jede zertifikatsbasierte VPN-, WLAN- und NAC-Anmeldung, sofern dabei der Microsoft-eigene RADIUS-Dienst IAS zum Einsatz kommt.

Vielleicht haben sich die Microsoft-Entwickler bei der Implementierung auf das SSL-Diagramm in Wikipedia verlassen – das den wichtigen Verifikationsschritt ebenfalls fehlerhaft darstellt. Manchmal geht Studieren doch über Probieren.

„Man in the Middle" is back

Nachdem in der jüngeren Vergangenheit andere Themen öffentlich diskutiert wurden, ist kürzlich die Bedrohung durch "Man in the Middle"-Attacken wieder ins Zentrum der Aufmerksamkeit gerückt, insbesondere dank der Veröffentlichung des White Papers "Active Man in the Middle Attacks – A Security Advisory" von Roi Saltzman und Adi Sharabani aus der IBM Rational Application Security Group am 27.02.2009.

In der Präsentation und dem White Paper werden Szenarien vorgestellt, bei denen ein Angreifer als "Man in the Middle" nicht durch Mitlesen auf zufällig übertragene Credentials (Cookies) wartet, sondern Server-Antworten so manipuliert, dass der Client seine Credentials ohne Wissen des Benutzers an ausgesuchte Webseiten überträgt. Dabei wird kein Implementierungsfehler, sondern ein Design-Problem von HTTP ausgenutzt.

Erst wenige Tage zuvor war das Thema „Man in the Middle" (MitM) am 18.02.2009 auf der Blackhat 2009 von Moxie Marlinspike in seinem Vortrag "New Tricks For Defeating SSL In Practice" aus einem anderen Blickwinkel beleuchtet worden. Darin wurden MitM-Angriffe betrachtet, die mit Manipulationen an SSL-Zertifikaten arbeiten. Als „Proof of Concept" wurde das Tool sslstrip vorgestellt.

Die Präsentationen beider Autoren auf der OWASP AU 2009 wurden am 04.03.2009 von Robert Hansem („RSnake") auf ha.ckers.org kommentiert. Wir können uns seinem Fazit anschließen: Das Thema ist keineswegs neu, aber inzwischen stehen so mächtige Angriffswerkzeuge zur Verfügung, dass zu erwarten ist, dass diese in Zukunft verstärkt von Amateur-Hackern genutzt werden.

Aktuelle Fehlerübersicht

Am 10.03.2009 wurde Version 1.3 des von 50 führenden amerikanischen IT-Unternehmen und Organisationen getragenen Projekts Common Weakness Enumeration (CWE) vorgestellt. In dieser Liste

werden die aktuell wichtigsten und schwerwiegendsten Sicherheitsprobleme bei der Softwareentwicklung identifiziert. Dazu werden sicherheitsrelevante Fehlerquellen bei der Erstellung von Software systematisch erfasst und detailliert ausgewertet.

Entsprechend wurden die 2009 CWE/SANS Top 25 Most Dangerous Programming Errors an die Resultate der aktuellen Erhebung angepasst. Sie sollten an dem Arbeitsplatz eines jeden Softwareentwicklers hängen – gleich neben den OWASP Top 10.

Umstrittenes BDSG

In seiner Sitzung am 23.03.2009 befasste sich der Innenausschuss des Deutschen Bundestages mit den geplanten Änderungen im Bundesdatenschutzgesetz und dem Entwurf eines Datenschutzauditgesetzes (DSAG). Die Bundesregierung hatte hierzu im Dezember neue Texte vorgelegt, nachdem die Erstentwürfe vom Spätsommer in der Fachwelt insgesamt auf große Kritik gestoßen waren.

Leider folgt der aktuelle Entwurf des DSAG weiterhin einem einstufigen Verfahren, bei dem die Gutachter (Kontrollstellen) gleichzeitig die zertifizierende Stelle sein sollen. Es ist schlichtweg unerklärlich, warum die Bundesregierung hinter international übliche Standards zurückfallen will: Schließlich ist die Trennung von Begutachtung und Zertifizierung in einem zweistufigen Verfahren Voraussetzung für die Minimierung von Interessenskonflikten – und damit Garant für die Seriosität eines Zertifikats. Erwartungsgemäß erntete gerade diese Grundkonzeption allgemeines Kopfschütteln in der Expertenrunde.

Heftige Kontroversen wurden unter den Sachverständigen über die vorgesehenen Regelungen zum Listenprivileg ausgetragen. Sogar einige Abgeordnete ließen sich angesichts der teils recht emotional vorgetragenen Stellungnahmen zu flammenden Reden während der Anhörung hinreißen, die sonst der parlamentarischen Debatte vorbehalten sind.

Die auf dem Datenschutzgipfel im Herbst beschlossene Abkehr vom Opt-Out-Verfahren im Bereich der Werbung, Markt- und Meinungsforschung und des Adresshandels steht wieder zur Debatte. So sehr fühlen sich Versandhandel, Adresshändler und Verlage durch die Pflicht zur Einwilligungserteilung eingeschränkt, dass sie das Schreckgespenst tausender bedrohter Arbeitsplätze an die Wand malen. In wirtschaftlich problematischen Zeiten offenbar ein wirksames Argument, um das informationelle Selbstbestimmungsrecht wieder einmal hintenan zu stellen. Nun wird die Stellungnahme des Innenausschusses gespannt erwartet.

AutoRun Revisited

Schon am 08.11.2007 hatte Scott Dunn darauf hingewiesen – und war am 20.03.2008 vom US-Cert bestätigt worden: Die von Microsoft beschriebenen Maßnahmen zur Deaktivierung der AutoRun-Funktion funktionierten nicht korrekt (SSN 12/2008). Der von Microsoft am 08.07.2008 veröffentlichte Patch zur Behebung dieser Schwachstellen war allerdings zunächst nur für Windows Vista und Windows Server 2008 verfügbar – nicht für die weit verbreiteten Systeme unter Windows XP.

Wohl angesichts der Conficker-Wurm-Infektionen über USB-Sticks und eines neuen US-CERT Advisorys vom 20.01.2009 hat Microsoft endlich reagiert und am 24.02.2009 ein Security Advisory sowie Patches für Windows 2000, XP und Server 2003 zur Verfügung gestellt, die diese Gefährdung beseitigen.

Unsere Empfehlung: Wer zur Deaktivierung von AutoRun den neuen Patch installiert, sollte sicherheitshalber auch die Wirksamkeit überprüfen.

Secorvo News

Secorvo College aktuell

Nach der Zertifizierung ist vor der Zertifizierung: Vom **22. bis 26.06.2009** findet das zweite diesjährige T.I.S.P.-Seminar mit anschließender Zertifikatsprüfung statt. Vorher bietet Secorvo College mit dem „aktuellen Klassiker“ IT-Sicherheit heute vom **21. bis 24.04.2009** einen Überblick der zentralen Themen der IT-Sicherheit und vom **05. bis 08.05.2009** einen umfassenden Einblick in die Welt der Public Key Infrastrukturen, praktische Übungen inklusive.

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

Das Original ist die beste Kopie

Auf dem kommenden Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am **07.05.2009** wird Rüdiger Kügler von WIBU SYSTEMS – einem der Pioniere auf dem Markt für Softwarelizenzmanagement – Hintergründe und aktuelle Herausforderungen des Schutzes digitaler Güter vor Plagiaten (vulgo Raubkopien) beleuchten und heutige "best practices" zur Realisierung des Lizenzhandlings vorstellen. Im Anschluss gibt es wie gewohnt Gelegenheit zum „Buffet-Networking“. Um Anmeldung wird gebeten.

Das darauffolgende KA-IT-Si-Event am **25.06.2009** – Vertrauen ist gut – Zertifizierung ist besser – ist einem Erfahrungsbereicht zur Zertifizierung nach dem Sicherheitsstandard ISO 27001 gewidmet.

Veranstaltungshinweise

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

April 2009	
21.04.	2nd USENIX Workshop on Large-Scale Exploits and Emergent Threats (Usenix, Boston/US)
21.-24.04.	IT-Sicherheit heute (Secorvo College)
26.-30.04.	Eurocrypt 2009 (IACR, Köln)
Mai 2009	
05.-07.05.	10. Datenschutzkongress 2009 (EUROFORUM, Berlin)
05.-08.05.	PKI (Secorvo College)
07.05.	Das Original ist die beste Kopie (KA-IT-Si, Karlsruhe)
18.-20.05.	IFIP SEC 2009 (IFIP, Zypern/CY)
20.-22.05.	2009 ADFSL Conference on Digital Forensics, Security and Law (ADFSL, Burlington/US)
Juni 2009	
08.-09.06.	DuD 2009 (Computas, Berlin)
22.-26.06.	T.I.S.P. Schulung (Secorvo College)

Fundsache

Am 25.03.2009 wurde Version 1.0 von OpenSAMM (Software Assurance Maturity Model) des Open Web Application Security Projects (OWASP) veröffentlicht. Das Modell beschäftigt sich mit der Bewertung der Sicherheit im Softwareentwicklungsprozesse. Dabei werden alle Aspekte von der Steuerung über die Entwicklung, die Tests bis hin zur Verteilung betrachtet. Auf 96 Seiten werden nicht nur abstrakte Anforderungen gestellt, sondern auch praktische Hinweise zum Einsatz verschiedener Maßnahmen zur Verbesserung der Softwareentwicklung gegeben.

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Karin Schuler

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

secorvo
security consulting

Secorvo Security News

April 2009

Editorial: Kuckucks-Eier

Abgesehen von gesetzlichen Pflichten ist die Reduktion operationeller Risiken die einzige vertretbare Begründung für Investitionen in den Schutz sensibler Daten und Information.

Als Existenznachweis für solche Risiken erfreuen sich die Ergebnisse von Studien und Befragungen großer Beliebtheit – besonders, wenn Teilergebnisse die eigenen Argumente untermauern. Tatsächlich aber besitzen veröffentlichte Studien fast ausnahmslos dieselben Schwächen: die Zahl der Befragten ist gering, die Fragen unscharf und interpretationsbedürftig, was wiederum die Aussagekraft der Antworten schwächt, und die Auswertung ist oberflächlich bis tendenziös. Nicht zuletzt mündet die Auswahl der Befragten (überwiegend selbst IT-Sicherheitsbeauftragte) oft in der gegenseitigen Bestätigung gemeinsam geteilter Vorurteile.

Eindrucksvoll belegt dies der am 14.04.2009 publizierte 2009 Data Breach Investigations Report von Verizon, für den 90 Sicherheitsvorfälle systematisch analysiert wurden. Dabei zeigte sich: Die meisten Vorfälle hatten mehrere Ursachen und ließen sich nicht in die beliebten simplen Verursacherkategorien „Insider“ oder „Externer“ einordnen. Zahlreiche Hacking-Attacken wären ohne die Ahnungslosigkeit oder den Leichtsinn von Mitarbeitern nicht erfolgreich. Und: Die absolute Zahl bestimmter Angriffe und auch deren prozentualer Anteil sagt wenig über das tatsächliche Risiko, denn das wird wesentlich von dem durch den Angriff verursachten Schaden bestimmt.

Wer bei der Steuerung seiner Investitionen in die Informationssicherheit auf zweifelhafte Studienergebnisse setzt, lässt sich fremde Eier ins Nest legen. Belastbare Hinweise auf das tatsächliche eigene Risiko ergeben sich nur bei vorurteilsfreier und differenzierter Analyse und Bewertung der eigenen Schwachstellen.

Wer dennoch aus Scheu vor dem Ruf des „Propheten im eigenen Lande“ zu Studien greifen möchte, sollte es wenigstens mit Sir Winston Churchill halten: „Ich glaube nur der Statistik, die ich selbst gefälscht habe.“ Sofern das Zitat ihm nicht untergeschoben wurde.

Inhalt

secorvo
security consulting

Security News

Signatur-Ei

Die Prüfung elektronischer Signaturen ist ein typisches Henne-Ei-Problem: Um eine Signatur zu prüfen, muss man auch das Zertifikat des Signierenden prüfen, das die Signatur einer ausstellenden Certification Authority (CA) trägt, die es wiederum zu prüfen gilt. Das Ganze muss man so lange fortsetzen, bis man am Ende der Kette bei einer vertrauenswürdigen, bekannten Henne (sprich: Root CA) bzw. deren Ei (sprich: Stammzertifikat) angekommen ist.

Doch damit nicht genug: Für jedes dieser Zertifikate im Eierkorb will auch noch validiert sein, ob es nicht bereits vor Erreichen seines aufgedruckten Haltbarkeitsendes als verdorben erkannt wurde. Dazu wird eine Sperrliste oder Online-Statusauskunft zu Rate gezogen, die – der Leser ahnt es sicher schon – ihrerseits signiert ist und über eine Kette von Zertifikaten geprüft werden muss, für die auch jeweils der Sperrstatus zu validieren ist – und so weiter und so fort …

Und wie man beim Eierkauf schaut, ob die Eier auch keinen Knacks in der Schale haben, so ist zu prüfen, ob alle Signaturen mit sicheren Algorithmen und Schlüssellängen erstellt wurden. Weil aber bei letzteren nur besonders feine Nasen erkennen, wann sie faulig zu duften beginnen, veröffentlicht die Bundesnetzagentur (BNetzA) jährlich im Bundesanzeiger eine aktuelle Liste aller Algorithmen der Hkl. A (zuletzt am 27.01.2009).

Am 06.03.2009 nun wies die BNetzA darauf hin, dass einer vermeintlich qualifizierten Signatur ein gegenüber § 371a ZPO verminderter Beweiswert zukommt, wenn bei der Prüfung des ganzen Hühnerstalls voller Hennen und Eier ein fauler Algorithmus entdeckt wird, der nicht rechtzeitig durch eine neue Eierschale (sprich: Übersignatur) gekittet wurde. Damit ergibt sich als siebte Klasse elektronischer Signaturen (vgl. SSN 02/2003) die „qualifizierte Signatur Hkl. B“ – mit abgelaufener Mindesthaltbarkeit. Vielleicht sollten potenzielle Anwender schon einmal beim Eierkauf üben und die Augen für das Kleingedruckte offen halten.

Konjunktur-Ei

Die Bundesregierung verteilt gerade Ostergeschenke in Gestalt von Konjunkturpaketen. Darunter finden sich 30 Millionen Eier, die gemäß der Antwort auf eine Kleine Anfrage der FDP-Bundestagsfraktion vom 25.03.2009 zur Steigerung der IT-Sicherheit verwendet werden sollen.

So ist geplant, von Anfang 2010 an über eine Million „IT-Sicherheitskits“ in Form von Kartenlesern und Software zur Nutzung der optionalen Authentifikations- und Signaturfunktionen der elektronischen Gesundheitskarte und des künftigen elektronischen Personalausweises zu verschenken – bevorzugt an die Teilnehmer des geplanten Anwendungstests (vgl. SSN 12/2008). Wie praktisch: Ein Softwarepaket zur Installation auf Privatrechnern – „from the people who brought you the Bundestrojaner“. Wer wird sich wohl so ein Ei ins eigene Nest legen?

RZ-Ei

Die gleichzeitige Gewährleistung von Vertraulichkeit und Verfügbarkeit gespeicherter Daten ist oft ähnlich schwierig, wie ein Omelette zuzubereiten, ohne dabei die Eier zu zerschlagen – „wasch' mich, aber mach' mich nicht nass“. Ein besonders hübsches Beispiel für diese Quadratur des Eis ist die von der israelischen Firma Axxana vermarktete Daten-Black-Box (am 30.03.3009 von Gartner in den Rang eines „Cool Vendor in Storage Technology and Systems“ erhoben). Darin sollen die Daten eines Rechenzentrums ähnlich geschützt sein wie ein rohes Ei in der richtigen Verpackung.

Damit man dieses „Daten-Ei“ selbst in einem eingestürzten Gebäude schnell finden kann, hat es einen eingebauten Peilsender. Und will man auf die wertvollen Daten nicht warten, bis alle Trümmer beiseite geräumt sind, lässt sich über eine Fernbedienung das drahtlose Netzwerk der Box aktivieren. Fragt sich nur, woran die Box erkennen kann, dass sie unter Trümmern begraben liegt – und nicht die Aufmerksamkeit eines nicht-autorisierten Eiersuchers auf sich gezogen hat.

Entwickler-Ei

„Easter Eggs“ werden verborgene Funktionen in Programmen genannt, mit denen sich die Entwickler ein „Denkmal“ gesetzt haben. Alte Bekannte sind der Flugsimulator in Microsoft Excel oder Space Invadors in Word. Aber auch in zahlreichen aktuellen Programmversionen lassen sich „Easter Eggs“ finden. Oft sind sie im Umfeld der Versions- und Copyright-Angaben verborgen, und meist muss man Insider-Kenntnisse haben, um sie zu finden – wie die „about:robots“-Seite in Firefox. Eine der bekanntesten Sammlungen solcher Easter Eggs findet sich auf eeggs.com.

Derartige Eier sollten allerdings auch daran erinnern, dass sich in jedem Programm unbekannte Funktionen verbergen können – auch solche, die nicht einmal vom Programmierer intendiert waren. Und unter diesen Eiern kann das eine oder andere faul sein. Merke: Die Axt im Haus erspart den Zimmermann – und die Backdoor im Programm einen mühsamen Hackerangriff.

Backbone-Ei

Auch im Backbone-Bereich wurden erst kürzlich einige Eier gefunden, u. a. von Enno Rey und Daniel Mende, die diese am 16.04.2009 auf der Blackhat Europe vorstellten. In ihrer Präsentation zeigten sie, wie man die durch MD5 gesicherten Signaturen von BGP (Border Gateway Protocol) kompromittieren kann, zum Beispiel mit dem von ihnen entwickelten Tool bgp_md5crack. Außerdem stellten die Autoren fest, dass man die Vertrauensanker von MPLS-VPNs kritisch prüfen sollte.

Auch wenn die Angriffsmöglichkeiten durch Tools wie mpls_redirect entsprechende Zugangsmöglichkeiten im Core-Bereich voraussetzen, weist der Vortrag nach, dass der Zugang alleine ausreichen kann, um den Verkehr umzuleiten. Die unterhaltsamen Folien können von der Webseite der Autoren herunter geladen werden.

Ankündigungs-Ei

Am 20.03.2009 veröffentlichte das US Department of Homeland Security einen Bericht über eine Überprüfung der Sicherheitssysteme an verschiedenen amerikanischen Flughäfen, die im Vorfeld bei der TSA intern per E-Mail angekündigt worden war. Die Darlegung von Details der geplanten Tests in dieser E-Mail musste zwangsläufig zur Nutzlosigkeit der verdeckt geplanten Überprüfung führen.

Als Aprilscherz wäre der Bericht vielleicht lustig zu lesen; tatsächlich muss er als Lehrstück verstanden werden, wie Tests und Audits gerade nicht durchgeführt werden sollten.

Datenbank-Ei

Einen ganzen Korb fauler Eier präsentierte Oracle am 14.04.2009 in seinem vierteljährlichen Critical Patch Update Advisory (letzte Aktualisierung vom 22.04.2009): Insgesamt 43 kritische Sicherheitslücken stopfen die Patches. Darunter finden sich zwei, die durch Fernzugriff auf eine Oracle-Datenbank ohne Authentisierung ausgenutzt werden können, und zwei weitere, die auf dieselbe Weise Peoplesoft Enterprise betreffen – in vielen Unternehmen mit amerikanischen Müttern das führende HR-System.

Betroffene Unternehmen sollten umgehend patchen – und die Datenschutzbeauftragten kritisch nachfragen.

Wurm-Ei

Am 22.04.2009 entdeckte Manh Dzung, Senior Malware Analyst beim vietnamesischen Unternehmen Bach Khoa Internetwork Security in Hanoi, einen Wurm, der Captchas von Google Mail löst – und so in der Lage ist, anonym eine beliebige Anzahl von E-Mail-Konten anzulegen. Die Analyse der Captchas übernimmt ein auf einem kanadischen Server beheimateter Dienst, an den der Wurm die Captcha-Grafik per E-Mail sendet.

Den erhofften Schutz vor automatisierten Angriffen bieten Captchas (vgl. SSN 2/2008) nicht mehr – die Tricks von Würmern und Trojanern kombiniert mit der Leistungsfähigkeit heutiger Analyse-Algorithmen macht eine verlässliche Unterscheidung von Mensch und Maschine praktisch unmöglich.

Secorvo News

Secorvo College aktuell

Den Sommer beginnen wir mit der nächsten Gelegenheit zur Zertifizierung Ihrer persönlichen Qualifikation: Das zweite T.I.S.P.-Seminar dieses Jahres findet vom 22. bis 27.06.2009 statt – Zertifikatsprüfung inklusive.

Vom 20.06. bis 03.07.2009 erfahren Sie bei unserer einzigen diesjährigen Veranstaltung zum Thema Information Security Management alles über Konzepte, Praxiserfolge und konkrete Umsetzung.

Stichwort Umsetzung: Erfolgreiche Forensik benötigt komplexe organisatorische und technische Vorgehensweisen. Bei uns lernen Sie diese kennen und können sie aktiv einüben – vom 07. bis 10.07.2009.

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

Nächste KA-IT-Si-Events

Die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) stellt seit ihrer Gründung im Januar 2001 auf fünf bis sechs Abendveranstaltungen pro Jahr aktuelle Themen der IT-Sicherheit in den Fokus. Am 07.05.2009 widmet sich Rüdiger Kügler von WIBU SYSTEMS – einem der Pioniere auf dem Markt für Softwarelizenzmanagement – in seinem Fachvortrag dem Schutz digitaler Güter vor Plagiaten. Im Anschluss werden die Diskussionen beim "Buffet-Networking" wie gewohnt vertieft.

Am 25.06.2009 wird Peter Zimmer von der prego services GmbH einen Erfahrungsbericht zur Zertifizierung nach dem Sicherheitsstandard ISO 27001 vorstellen. Für beide Events bitten wir um rechtzeitige Anmeldung unter www.ka-it-si.de.

Veranstaltungshinweise

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

Mai 2009	
05.-07.05.	10. Datenschutzkongress 2009 (EUROFORUM, Berlin)
07.05.	Das Original ist die beste Kopie (KA-IT-Si, Karlsruhe)
18.-20.05.	IFIP SEC 2009 (IFIP, Zypern/CY)
20.-22.05.	2009 ADFSL Conference on Digital Forensics, Security and Law (ADFSL, Burlington/US)
Juni 2009	
02.-05.06.	ACNS '09: International Conference on Applied Cryptography and Network Security (INRIA, Paris/FR)
03.-04.06.	ASIA '09: 4th Annual Symposium on Information Assurance (University at Albany, Albany/US)
08.-09.06.	DuD 2009 (Computas, Berlin)
21.-25.06.	Africacrypt 2009 (IACR, Gammarth/TN)
22.-26.06.	T.I.S.P. Schulung (Secorvo College)
30.06.-03.07.	Information Security Management (Secorvo College)

Fundsache

Die Mustervertragsanlage des Bitkom zur Auftragsdatenverarbeitung liegt nun in einer um eine englische Übersetzungshilfe erweiterten Fassung 2.1 vor. Die auf das Wesentliche beschränkte (und als Word-Formular verfügbare) Vertragsvorlage zur Umsetzung der Anforderungen aus § 11 BDSG an die Verarbeitung personenbezogener Daten im Auftrag liefert eine wertvolle Grundlage für die Erstellung angepasster Vertragsentwürfe – und wird insbesondere mittelständischen Unternehmen ans Herz gelegt.

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch

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

secorvo
security consulting

Secorvo Security News

Mai 2009

Der Feind in meinem PDA

„Es ist also die Geschichte der Natur wie der menschlichen Gesellschaft, aus der die Gesetze der Dialektik abstrahiert werden. (...) Und zwar reduzieren sie sich der Hauptsache nach auf drei: das Gesetz des Umschlagens von Quantität in Qualität und umgekehrt, (...)“
Friedrich Engels, Dialektik der Natur

Es gibt gute Gründe, der Neudefinition der Hegelschen Dialektik durch Marx und Engels mit Skepsis zu begegnen. Die rasante Entwicklung der Informationstechnik liefert jedoch zahlreiche Belege für die Plausibilität von Engels erstem dialektischen Gesetz: Immer wieder ist es deren Verbreitung, die zu qualitativ neuen Sichtweisen zwingt. Das gilt besonders für die IT-Sicherheit: Erst die Allgegenwart von PCs machte sie als Angriffsziel interessant, Client-Server-Architekturen erhöhten den Schutzbedarf, und deren universelle Vernetzung führte zu gänzlich neuen Schutzkonzepten.

Nun ist es wieder so weit: Der Siegeszug moderner Personal Digital Assistants (PDAs) fordert Sicherheitsarchitekturen heraus. Vor wenigen Jahren noch waren PDAs bestenfalls persönliche Kalender mit Adressbuch auf proprietären Spezialsystemen. Schadsoftware hatte Seltenheitswert, da Inkompatibilität und rudimentäre Kommunikationsschnittstellen eine nennenswerte Verbreitung verhinderte.

Das hat sich geändert. PDAs sind dabei, Laptops zu verdrängen. Die Beliebtheit von Blackberry und iPhone haben ebenso dazu beigetragen wie der Preisverfall bei Mobilfunk-Flatrates und die gestiegene Leistungsfähigkeit. Unternehmen reagieren auf diese Entwicklung, indem sie über Hersteller-APIs den PDA-Zugriff auf Unternehmenssoftware freigeben. Damit stellt ein PDA heute aus der Perspektive des Informationsschutzes dasselbe Risiko dar wie ein Laptop.

Allerdings: PDAs gehen häufiger verloren, sind ständig „online“ (oft ohne Passwortsperre), werden selten „sauber“ entsorgt und verfügen fast nie über eine Vollverschlüsselung. Und sind das perfekte Tool für Industriespione: Mit Kamera, Mikrofon, Online-Verbindung, GPS-Empfänger und Zugriffsrechten – und einem Nutzer, der jeden Hinweis auf eine „hippe“ neue Applikation sofort dankbar umsetzt.

Inhalt

secorvo
security consulting

Security News

Websecurity-Statistik

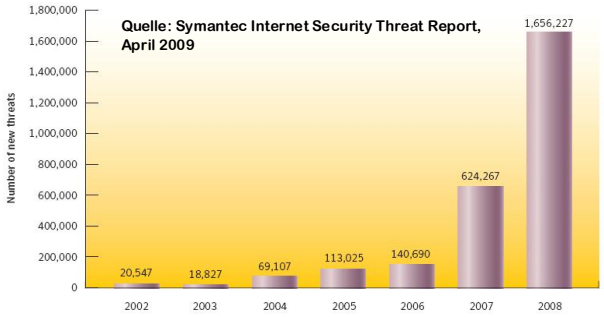
Zwar sollte man Statistiken grundsätzlich mit einer kritischen Distanz begegnen. Dennoch soll an dieser Stelle auf den Web Site Security Statistics Report der amerikanischen Firma WhiteHat Security, der am 18.05.2009 vorgestellt wurde, hingewiesen werden: Hinter diesem Bericht steckt unter anderem der Firmengründer und in Web-App-Security-Kreisen sehr geschätzte Jeremiah Grossman. Erschreckend ist, dass von den im ersten Quartal 2009 untersuchten Websites 82 % eine Schwachstelle aufwiesen, die von WhiteHat mit HIGH, CRITICAL oder URGENT bewertet wurde. Bei 63 % der Sites waren die Schwachstellen zum Veröffentlichungszeitpunkt noch nicht beseitigt.

Der Bericht stellt interessante aktuelle Entwicklungen vor und belegt viel diskutierte Sicherheitsprobleme von Webanwendungen mit konkreten Zahlen. Er kann auf der Webseite von WhiteHat zum Download angefordert werden.

Malware explodiert

Am 14.04.2009 hat Symantec den Internet Security Thread Report für 2008 veröffentlicht. Er dokumentiert die Fortsetzung einer beängstigenden Entwicklung: Die Zahl neuer Schadsoftware, die bereits 2007 auf mehr als das Vierfache angestiegen war, hat sich 2008 erneut vervielfacht – auf 1,65 Mio. Anders ausgedrückt: An jedem Kalendertag wurden 2008 im Schnitt über 4.500 neue Schadprogramme in die Welt entlassen.

Im vergangenen Jahr hatte die Zahl im Mittel noch bei etwa 1.700 gelegen. Eine solche Flutwelle lässt sich nur noch mit Heuristiken bewältigen: Virenscanner können neuartige Schadsoftware, die auf einen Schlag via Botnetz verteilt wird, nicht mehr an einer bekannten Signatur, sondern nur noch an „auffälligen" Eigenschaften erkennen. Daher steigt die Bedeutung einer alten Empfehlung wieder: Durch den Einsatz unterschiedlicher Scanner auf zentralen und lokalen Systemen und möglichst kurze Aktualisierungszyklen sollte die Qualität der Analyse optimiert werden. Und eine regelmäßige Komplettprüfung (vor allem mobiler) Endsysteme sollte ebenfalls etablierte „Best Practice" sein.



„GSG Botnetz"

Forschern der University of California ist es Anfang 2009 gelungen, das „Torping"-Botnetz zu übernehmen. In einem am 29.04.2009 veröffentlichten Forschungsbericht „Your Botnet is My Botnet" wird im Detail beschrieben, wie die dynamisch wechselnden Zieldomänen für die Command-und-Control-Server vorab bestimmt und reserviert werden konnten. Auf diese Weise konnten die Forscher – aus Sicht des Botnetz-Betreibers „feindliche" – C&C-Server aufbauen und darüber das Botnetz kontrollieren. Ein neues Binary des Botnetz-Betreibers, das an die infizierten Systeme verteilt wurde, unterband die Kontrolle nach zehn Tagen wieder.

Dennoch konnten in dieser Zeit über 70 Gigabyte an Botnetz-Daten, darunter zahlreiche Kennwörter gesammelt werden:

Data Type	Data Items (#)
Mailbox account	54,090
Email	1,258,862
Form data	11,966,532
HTTP account	411,039
FTP account	12,307
POP account	415,206
SMTP account	100,472
Windows password	1,235,122

Neben Details zur Funktionsweise stellten die Forscher fest, dass die Größe von Botnetzen vielfach überschätzt wird: Eine Unterscheidung zwischen infizierten Systemen und festgestellten IP-Adressen zeigt, dass aufgrund wechselnder IP-Adressen die reale Anzahl von „Zombies" erheblich kleiner ist als vermutet. Dennoch belegt das Beispiel eindrucksvoll die tatsächliche Gefährdung und verdeutlicht das Erfordernis, Systeme aktuell zu halten und Sicherheitssoftware wie Virenschutz und Personal Firewalls einzusetzen.

News from OWASP

Bei OWASP hat sich auch im Mai 2009 viel getan. Vom 13.-14.05.2009 fand in Warschau die OWASP AppSec Europe 2009 statt. Für Interessierte sind die Präsentationen von Tag 1 und Tag 2 inzwischen online verfügbar. Auf der Konferenz wurden in drei parallelen Tracks spannende Themen zur Sicherheit von Web-Anwendungen behandelt, darunter Vorträge zu den Themen „Threat Modeling", „The Bank in the Browser – Defending web infrastructures from banking malware", „CSRF: the nightmare becomes reality?" und „Factoring malware and

organized crime in to Web application security".

Im Schatten der OWASP-Konferenz wurde im Mai das OWASP PCI Project etabliert. Im Verlauf des Projekts sollen vereinheitlichte Anforderungen an Web-Anwendungen formuliert werden, die den Erfordernissen der Payment Card Industry Data Security Standards (PCI-DSS) der Kreditkartenorganisationen genügen.

Offene Gesellschaften

Bereits am 21.01.2009 veröffentlichte der ZEW-Forscher Dr. Wolfgang Sofka das Ergebnis einer in Zusammenarbeit mit Edlira Shehu von der Universität Hamburg durchgeführten Untersuchung über die Maßnahmen multinationaler Unternehmen zum Schutz vor unerwünschtem Informationsabfluss (Host Country Contingencies on Knowledge Protection Strategies of Multinational Firms).

Die zentrale Erkenntnis der Studie, gestützt durch eine Stichproben-Befragung von 1.500 deutschen Unternehmen, dürfte überraschen: Die ergriffenen Schutzmaßnahmen zur Verhinderung von Know-How-Diebstahl orientieren sich keineswegs an „Best Practices" oder etablierten Standards, sondern folgen überwiegend einem ökonomischen Kalkül: Hat ein ausländischer Standort den Status eines „Technologieführers", verlegen sich Unternehmen auf das Patentrecht und möglichst enge Kooperationen – mit dem Ziel eines für sie profitablen gegenseitigen Wissenstransfers. Umgekehrt steigt die Bedeutung von Abschottungsmaßnahmen, wenn ein Standort als technologisch rückständig gilt.

Selbstverständlich muss eine angemessene Klassifikation sensibler Daten in der Praxis einer realistischen Risikobewertung folgen. Zu kurz gesprungen erscheint allerdings die offensichtliche Zurückhaltung von Unternehmen in technologisch führenden Standorten – denn Wirtschaftsspionage ist schon lange kein nationales Problem mehr. So werden Patentschriften nicht nur im Inland gelesen, und die Spionageaktivitäten von Ländern mit technologischem Nachholbedarf konzentriert sich schon seit Jahren auf die „offenen" Gesellschaften des Westens, in denen das benötigte Wissen, wie die Studie belegt, oft viel leichter zugänglich ist.

Secorvo News

Secorvo College aktuell

In guten wie in schlechten Zeiten bleiben die Weiterentwicklung der persönlichen Qualifikation und deren Nachweis der Schlüssel für Ihre berufliche Entwicklung. Mit dem TISP bieten wir Ihnen die Möglichkeit, Ihre Kenntnisse auf hohem Niveau zu erweitern und mit einem anerkannten Zertifikat zu belegen. Acht Referenten bündeln ihr Wissen, ihre Expertise und ihre langjährige Berufserfahrung, um Ihnen in fünf Tagen die essentiellen Inhalte der Informationssicherheit zu präsentieren. Die nächsten TISP-Seminare finden statt am **22.–27.06.** und **07.–12.09.2009** (jeweils einschließlich Prüfung).

Vom **30.06.–03.07.2009** erfahren Sie bei unserer einzigen diesjährigen Veranstaltung zum Thema Information Security Management alles über Konzepte, Praxiserfolge und konkrete Umsetzung.

Detaillierte Programme, College-Jahreskalender und Online-Anmeldung unter http://www.secorvo.de/college.

… Zertifizierung ist besser

Am **25.06.2009** dreht sich bei der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) alles um das Thema ISO 27001: Im Rahmen des Events „Vertrauen ist gut – Zertifizierung ist besser" gibt Peter Zimmer von der prego services GmbH in Ludwigshafen mit einem Erfahrungsbericht Einblick in die notwendigen Vorbereitungen zur Erlangung der Zertifizierungsreife sowie die Wirkung des ISO-Standards im Geschäftsalltag. Um Anmeldung wird gebeten.

Tag der IT-Sicherheit

Gemeinsam mit dem Cyberforum und der IHK-Karlsruhe veranstaltet die KA-IT-Si am **16.07.2009** den ersten Karlsruher „Tag der IT-Sicherheit" im Saal Baden der IHK (Beginn: 14 Uhr, Teilnahmebeitrag 75 Euro). Neben Fragen der Haftung („Wer hastet, der haftet!") und einer aktuellen Einschätzung der Bedrohungen werden Unternehmen der TechnologieRegion in Erfahrungsberichten ihre „Best Practices" vorstellen: die Telemaxx Kommunikation GmbH, die Fiducia IT AG und die Edelstahl Rosswag GmbH – ausgezeichnet mit dem IT-Sicherheitspreis Baden-Württemberg 2007 bzw. 2009. Die Veranstaltung klingt ab ca. 18 Uhr mit einem KA-IT-Si-typischen „Buffet-Networking" aus.

Anmeldung bitte bis 09.07.2009 an Frau Helen Armbruster (IHK Karlsruhe), Tel.: 0721/174-190, helen.armbruster@karlsruhe.ihk.de.

Anschließend beginnt für die KA-IT-Si die Sommerpause – bevor es am **24.09.2009** mit dem Event „Pacta sunt servanda" zum Thema „Softwaresicherheit – Design by Contract" weitergeht.

Veranstaltungshinweise

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

Juni 2009	
02.-05.06.	ACNS '09: International Conference on Applied Cryptography and Network Security (INRIA, Paris/FR)
03.-04.06.	ASIA '09: 4th Annual Symposium on Information Assurance (University at Albany, Albany/US)
08.-09.06.	DuD 2009 (Computas, Berlin)
21.-25.06.	Africacrypt 2009 (IACR, Gammarth/TN)
22.-26.06.	T.I.S.P.-Schulung (Secorvo College)
25.06.	„Vertrauen ist gut – Zertifizierung ist besser“ (KA-IT-Si, Karlsruhe)
30.06.-03.07.	Information Security Management (Secorvo College)
Juli 2009	
06.-07.07.	SANS WhatWorks Summit in Forensics and Incident Response (SANS, Washington/US)
07.-10.07.	Forensik – Verfahren, Tools, Praxiserfahrung (Secorvo College)

Fundsache

Ende August 2008 veröffentlichte Thomas Noon, inzwischen vereidigter Sachverständiger für IT-Systeme, seine Masterarbeit über „Geldspielgeräte und die SpielV“. Das Dokument ist ein weiteres erschütterndes Beispiel für die Risiken inkompetenter Digitalisierung ursprünglich analoger Geräte, wie erst unlängst bei Wahlmaschinen (SSN 10/2008) zu beobachten. Angesichts von Milliardenumsätzen geht es hier jedoch um Lizenzen zum Gelddrucken. Und wieder hat die PTB ihre Hand im Spiel ...

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian

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

secorvo
security consulting

Secorvo Security News

Juni 2009

Riskante Mythen

Mythen erfreuen sich unausrottbarer Beliebtheit. Wie gerne glauben wir an einfache Erklärungen – besonders, wenn sie ein wohlfeiles Argument für vage Überzeugungen liefern, an unterschwellige Wünsche appellieren oder lieb gewonnene Vorurteile bestätigen.

1890 bestimmte der Physiologe Gustav von Bunge den Eisengehalt von 100 Gramm Spinat mit 35 Milligramm – von getrocknetem allerdings, dessen Eisengehalt zehnmal größer ist als der frischen Spinats. Das im Spinat enthaltene Eisen kann die menschliche Verdauung nicht einmal verwerten; dennoch glauben wir an dessen entwicklungsfördernde Kraft. Unzählige weitere Mythen bestimmen unsere Weltsicht: dass Lesen bei schlechtem Licht die Augen verdirbt oder wir nur einen Bruchteil der Kapazität unseres Gehirns nutzen. Alles Unsinn. Im Wochenmagazin DIE ZEIT geht Christoph Drösser seit 1997 in der Kolumne „Stimmt's?" verbreiteten Alltagsüberzeugungen auf den Grund und konnte viele als überlieferten Irrglauben entlarven.

Offenbar hat auch das Fachgebiet IT-Sicherheit ein Alter erreicht, in dem sich Glaubenssätze einnisten, die ohne weitere Prüfung übernommen und weitergegeben werden. Selbst die IT-Grundschutz-Kataloge sind davor nicht gefeit, wie sich am Beispiel der Passwort-Empfehlungen (M 2.11) zeigen lässt. Dort wird eine Sperrung des Zugangs nach drei Fehleingaben empfohlen – eine Maßnahme, die keinerlei Sicherheitsgewinn bewirkt, jedoch kostspielige Kennwortrücksetzungen nach Urlauben und erzwungenen Passwortwechseln. Schlimmer noch: Sie ermöglicht simple Denial-of-Service-Angriffe – durch absichtliche Fehleingaben bei fremden Accounts. Ähnlich die Forderung nach Passworten mit mindestens einem nicht-alphabetischen Zeichen: Da die meisten Benutzer Ziffer oder Sonderzeichen anhängen, verkleinert sich dadurch der Suchraum. Viel wirksamer wäre eine um ein Zeichen erhöhte Mindestlänge.

Auch diese Mythen werden, so ist zu befürchten, weiterleben: „Es ist schwieriger, eine vorgefasste Meinung zu zertrümmern, als ein Atom", wusste schon Albert Einstein.

Inhalt

secorvo
security consulting

Security News

Windows 7 Security

Windows 7 soll im Oktober 2009 auf den Markt kommen und gegenüber Windows Vista verbesserte und neue Sicherheitsfunktionen enthalten. Eine Einführung in diese Funktionen bietet Chris Corio in einem Technet-Artikel vom 24.04.2009.

Neben der verbesserten Integration biometrischer Authentifzierungsverfahren und Verfeinerungen bei Bitlocker zur Festplattenverschlüsselung ist vor allem die neue Funktion „Applocker" viel versprechend. Durch eine zentrale Steuerung der Anwendungen, die durch einen Benutzer ausgeführt werden können, kann die Sicherheit maßgeblich gesteigert werden. Im Vergleich zu den bereits in XP und Vista vorhandenen „Software Restriction Policies" wurden das Management verbessert und weitere Funktionen etabliert, die es beispielsweise ermöglichen, die Auswirkungen von Policies vorab zu testen und den Umgang mit aktualisierten Programmversionen und Updates erheblich zu vereinfachen.

Sofern im Unternehmen Prozesse zur Freigabe von Software für die Benutzer etabliert sind, können diese durch diese neuen Funktionen technisch durchgesetzt werden – ein Gewinn vor allem für Unternehmen, die bisher über keine Kontrollmöglichkeit des Softwareeinsatzes verfügen.

SHA-1 auf Kollisionskurs

Die Krypto-Hashfunktion SHA-1 steht bekanntlich schon seit längerem unter Beschuss, und der Nach-Nachfolger SHA-3 macht sich bereit, in die Startblöcke zu steigen (siehe SSN 10/2008). In der Rump-Session der Eurocrypt 2009 kündigten drei australische Forscher am 28.04.2009 in Köln den bisher besten Angriff auf SHA-1 an, den sie am 02.06.2009 veröffentlichten. Er soll den Aufwand zum Finden einer Kollision auf 2^{52} Operationen reduzieren. Auch wenn bezweifelt wird, dass alle Annahmen der Autoren haltbar sind, und der Aufwand realistisch auf 2^{57} Operationen geschätzt wird, sinkt die Sicherheit des SHA-1 damit auf die des überholten DES (2^{56}).

Allerdings spielen Kollisionsattacken in der Praxis erst dann eine Rolle, wenn der Angreifer die beiden zur Kollision führenden Texte bzw. Dateien selbst konstruieren kann. Die Kunst besteht dann darin, ein „Zwillingspärchen" aus einem unverfänglichen Datum (z. B. einem Webserver-Zertifikat oder einem einfachen „Hello World"-Programm, SSN 01/2009), das man legal signieren lässt, und einem bösartigen Alter Ego (z. B. einem Zertifizierungsstellen-Zertifikat oder einem Programm mit Schadcode) zu wählen, das denselben Hashwert und damit dieselbe Signatur besitzt. Eine Signaturprüfung wird sowohl Jekyll als auch Hyde als gültig (und vertrauenswürdig) akzeptieren.

Eine solche Kollisionskonstruktion gelingt mit dem vorgestellten Angriff nur, wenn es gelingt, zu einer mehr oder weniger sinnlosen Zeichenfolge eine legale Signatur zu erschleichen. Und auch der Einsatz von SHA-1 zum Integritätsschutz per HMAC ist glücklicherweise nicht betroffen.

Opera Unite(d)

Am 16.06.2009 wurde die Opera-Browser-Nachfolger Unite (V10b1) verfügbar gemacht; eine portable Version soll folgen. Als Update ist er vollständig im Benutzerkontext installier- und nutzbar. Neu in Opera Unite sind „Social Network"-Server-Komponenten („Services"), durch die innerhalb von Minuten nach Beantragung eines (auch pseudonymen) Accounts bei Opera auf dem lokalen Clientsystem u. a. Filesharing und ein Webserver gestartet werden. Der Webserver ist direkt von Extern über einen Fully Qualified Domain Name (FQDN) erreichbar, sobald der Einstiegspunkt in die Dateiverzeichnisstruktur gesetzt wurde. Unter Windows sind auch Server-Shares in Gestalt zugewiesener Laufwerksbuchstaben möglich. Mit einer einfachen Google-Suche werden die Shares sichtbar.

Das verwendete Proxykonzept tunnelt dazu bestehende Firewallstrukturen, sofern ein Zugriff auf den Unite Proxy bei Opera auf Port 16680/tcp zugelassen ist. Ist der Unite Proxy nicht erreichbar und die UPnP-Option in Opera Unite aktiviert, wird ein Multicast auf Netz 239/8 nach RFC 3171 durchgeführt. Immerhin: Port Punching-Techniken à la Skype werden bisher nicht unterstützt – allerdings befindet sich die Software auch erst im Beta-Stadium.

Opera's Zielsetzung, mit diesem Konzept Daten in Social Networks wieder unter die Kontrolle der Besitzer zu stellen, in Ehren – ein Blick in Kapitel 7 der EULA („Use of Service") zeigt jedoch, dass es wohl eher auf eine Wahl zwischen Teufel und Beelzebub hinausläuft.

Security-Check für Anwendungen

Am 03.06.2009 wurde die erste Version des Application Security Verification Standard (ASVS) des Open Web Application Security Projekts (OWASP) veröffentlicht. Der Standard enthält eine Vorgehensweise zur einheitlichen Durchführung von Sicherheitstests von (Web-) Anwendungen und will damit vergleichbare Aussagen über das Sicherheitsniveau erreichen. Eine Überprüfung kann dabei auf einem von vier Ebenen erfolgen: Automatisierte Prüfung (L1), manuelle Prüfung (L2), Design-Prüfung (L3) oder interne Prüfung (L4).

Zu begrüßen ist, dass der Schwerpunkt des Standards auf der Überprüfung des Vorhandenseins effektiver Sicherheitsmechanismen liegt. Auf 42 Seiten werden neben der generellen Vorgehensweise der vier Überprüfungs-Level auch detaillierte Prüfvorgaben für jedes Level vorgegeben. Diese unterfallen in 14 Themengebiete, darunter Security Architecture, Authentication, Session Management und Access Control, und neben weiteren auch Input Validation, Cryptography und HTTP Security. Schließlich legt der ASVS Anforderungen an die zu erstellenden Sicherheitsberichte fest.

Damit steht Entwicklern, Betreibern und Nutzern eine unabhängige Grundlage zur Überprüfung der Sicherheit von (Web-) Anwendungen zur Verfügung. Der Standard wird sich im Zusammenspiel mit weiteren OWASP-Projekten durchsetzen, die sich in der Praxis bewährt haben (wie z. B. dem Testing Guide oder Development Guide). Aber Vorsicht: Auch hier darf der Blick auf das Zertifikat nicht die Beschäftigung mit dem Testbericht ersetzen.

Regenbogenbrecher

Eine Passwort-Mindestlänge von acht Zeichen gilt selbst bei alphanumerischen Passwörtern noch immer als solide Empfehlung, auch in den IT-Grundschutz-Maßnahmenkatalogen des BSI.

Dabei werden die Entwicklung der Rechenleistung aktueller PCs, die Nutzung von Grafikkarten durch moderne Cracking-Tools sowie die Auswirkungen der von Philippe Oechslin (EPFL) bereits auf der Crypto 2003 publizierten Optimierungen für Rainbow Tables offenbar erheblich unterschätzt.

Ein schneller PC berechnet heute 800 Mio. NTLM-Hashwerte pro Sekunde – und hat in knapp 80 Stunden alle möglichen achtstelligen alphanumerischen Passwörter durchprobiert. Mit einer schnellen Grafikkarte (2 Mrd. Hashes/sec.) genügen 30 Stunden – und unter Verwendung von Oechslins Rainbow-Tables vom 12.02.2009 (74 Mrd. Hashes/sec.) sogar 50 Minuten. Wenn sie einem Cracking-Angriff auf die SAM-Datei zumindest einige Tage widerstehen sollen, müssen alphanumerische Passwörter heute eine Mindestlänge von 10 Zeichen aufweisen.

Phishing still alive

Am 12.05.2009 belegte die Anti-Phishing Working Group (APWG) mit Veröffentlichung ihres „Global Phishing Survey", dass Phishing noch lange nicht tot ist. Der 26 Seiten starke Bericht über die Trends im zweiten Halbjahr 2008 dokumentiert knapp 57.000 Phishing-Attacken unter Benutzung von 30.500 Domain-Namen – aus 170 Top Level Domains (TLDs). 81 % der Angriffe wurden von kompromittierten Webservern ausgeführt. Phishing ist weiterhin ein attraktiver Markt – und die Phisher passen sich aktuellen Verteidigungstrends an.

Erfreulich: Die APWG bietet eine Hilfestellung für den Fall, dass eine Webseite einem Hacking-Angriff durch Phisher zum Opfer gefallen ist. Und auch für den Endverbraucher werden gute Ratschläge erteilt – wenn auch nur in Englisch.

Folgt man einem Positionspapier von Microsoft Research vom 01.09.2008, ist Phishing ein „Profitless Endeavour": Danach weisen die hohen Aktivitätszahlen darauf hin, dass – größtenteils erfolglose – Kriminelle verzweifelt versuchen, sich doch noch ein Stück vom vermeintlich großen Kuchen der aus Online-Konten zu phishenden Beträge abzuschneiden. Allerdings geht das Papier nur von „einfachen" Phishing-Mails aus, die Anwender dazu auffordern, ihre Passwörter auf einer betrügerischen Webseite einzugeben. Das mag in den USA ausreichen, um ein Online-Konto zu plündern – in Deutschland gehört die iTAN mittlerweile zum Mindeststandard.

Allerdings ist auch die iTAN für Täter dank Trojanern und Man-in-the-Middle Attacken nicht unüberwindlich, wie ein Beitrag des BKA auf dem BSI Sicherheitskongress am 18.05.2009 belegt. Ob die Microsoft-Autoren bedacht haben, dass vermeintlich leergefegte Phishgründe wieder ergiebig werden, wenn man statt einer Angelrute einen Trawler mit Echolot benutzt?

Secorvo News

Sicherheitsregion Karlsruhe

Das Hightech.Unternehmer.Netzwerk CyberForum, die IHK Karlsruhe und die KA-IT-Si laden zum ersten Karlsruher „Tag der IT-Sicherheit" am **16.07.2009** ein. Im Saal Baden der IHK werden ausgewiesene Experten aus der „Sicherheitsregion Karlsruhe" ab 14 Uhr mit spannenden Vorträgen („Die sieben Todsünden der IT-Sicherheit") und preisgekrönten Beispielen aus der Praxis, u. a. von der Edelstahl Rosswag GmbH und der Fiducia IT AG, Einblicke in ihre Erfahrungen und Anregungen zur Diskussion geben. Beim anschließenden Buffet-Networking ab 18 Uhr bietet sich die Gelegenheit, Fragen zu Haftung, Datenschutz und IT-Sicherheit mit Referenten und Gästen zu vertiefen.

Nähere Informationen und Anmeldung unter www.ka-it-si.de. Teilnahmegebühr: 75 Euro.

Veranstaltungshinweise

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

Juli 2009	
06.-07.07.	SANS WhatWorks Summit in Forensics and Incident Response (SANS, Washington/US)
16.07.	Tag der IT-Sicherheit (IHK Karlsruhe/CyberForum e.V./KA-IT-Si, Karlsruhe)
August 2009	
12.-14.08.	USENIX Security '09 (Usenix, Montreal/CA)
16.-20.08.	Crypto 2009 (IACR, Santa Barbara/US)
17.-18.08.	Digital Forensic Research Workshop (DFRWS, Montreal/CA)
31.08.-04.09.	TRUSTBUS 09: 6th International Conference on Trust, Privacy & Security in Digital Business (University of the Aegean, Linz/AT)
September 2009	
07.-11.09.	TISP-Schulung (Secorvo College)
21.-23.09.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
24.09.	Pacta sunt servanda (KA-IT-Si, Karlsruhe)
29.09.-02.10.	ISSECO Certified Professional for Secure Software Engineering - CPSSE (Secorvo College)

Fundsache

Dass die Entwicklung einer modernen Passwort-Policy komplexer ist, als es auf den ersten Blick scheinen mag, belegt der am 21.04.2009 als Draft erschienene „Guide to Enterprise Password Management“ des NIST (Special Publication 800-118).

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Jochen Schlichting

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

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

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

secorvo
security consulting

Secorvo Security News

Juli 2009

Zenon und die Verfüglichkeit

Die Beispiele sind zahlreich und reichen von der RZ-Blackbox, die im Notfall die gespeicherten Daten via WLAN preisgibt, bis zum Verlust der PKI-Root-Keys bei der gematik: Immer wieder verursacht der Konflikt zwischen den Sicherheitszielen Vertraulichkeit und Verfügbarkeit Sicherheitsvorfälle oder zumindest – wie beim Thema Schlüsselhinterlegung (Key Escrow) – heftige Auseinandersetzungen.

Tatsächlich geraten diese beiden Sicherheitsziele bei fast jeder Sicherheitslösung aneinander. Wer Backups erstellt, um eine hohe Datenverfügbarkeit zu erreichen, schafft unvermeidlich einen neuen Angriffspunkt auf deren Vertraulichkeit. Wer Daten verschlüsselt abspeichert, riskiert mit dem Verlust des Schlüssels auch den der Daten. Und ein Passwortrücksetzungsverfahren kann die Vertraulichkeit bedrohen, wenn Unberechtigte es auslösen können.

Das Spannungsverhältnis ist beiden Zielen immanent – warum aber werden in der Praxis allzu häufig Maßnahmen für das eine Ziel auf Kosten des anderen umgesetzt? Zu vermuten ist, dass bei vielen Konzepten übersehen wird, dass jede Maßnahme zur Erreichung eines der Sicherheitsziele das Schutzobjekt des anderen Ziels verändert: Auch Backups sind bei Vertraulichkeitsmaßnahmen zu berücksichtigen, und für Passworte und Schlüssel müssen Verfügbarkeitsmaßnahmen getroffen werden.

Das klingt verdächtig nach Zenon von Eleas Paradoxie von Achilles und der Schildkröte, deren Vorsprung er trotz höherer Geschwindigkeit nicht einholen kann: Sobald er die Stelle erreicht, auf der die Schildkröte eben noch stand, ist diese bereits weitergekrochen.

Ein Trugschluss – denn auch eine unendliche Reihe (wie die schrumpfenden Abstände zwischen Achilles und der Schildkröte) kann eine endliche Summe besitzen. So müssen auch Vertraulichkeit und Verfügbarkeit nicht ad infinitum konkurrieren – geeignete Schutzkonzepte müssen jedoch immer beide angemessen berücksichtigen.

Inhalt

secorvo
security consulting

Security News

Sicher ist sicher – oder?

„Sicherheitsmechanismen bei Root-Zertifikaten wirksam“ meldete am 15.07.2009 die gematik, als Projektgesellschaft zuständig für die elektronische Gesundheitskarte (eGK) und die Heilberufsausweise (HBA) für medizinisches Personal. Anfang Juli hatte D-TRUST, Betreiber des Trustcenters für eGK und HBA, ein neues Root-Zertifikat erstellen müssen – übrigens nicht nach X.509, sondern im „card verifiable“ Zertifikatformat gemäß ISO-7816, das u. a. auch beim digitalen Tachographen verwendet wird: Das für den Schutz der Schlüssel eingesetzte Hardware Security Modul (HSM) hatte Probleme in der Stromversorgung als Angriff gewertet und folgerichtig – alle Schlüssel gelöscht.

Nun müssen etliche Hundert „Musterkarten“ ausgetauscht werden. Zwar hätte man für Tests mit fiktiven Daten besser auf die hohe Sicherheit durch HSMs verzichtet und eine Root-CA in Software eingesetzt, oder die geplante Produktivumgebung inklusive Backup und Restore des Root-Schlüssels nachgebildet. Der Entscheidung für ein HSM ohne Backup verdankt die Welt jedoch zwei wichtige Ergebnisse: Erstens einen seltenen, realitätsnahen Test des Worst-Case Szenarios, und zweitens ein geschärftes Bewusstsein dafür, dass Sicherheit nicht nur bedeutet, dass Daten nicht in die falschen Hände fallen, sondern auch, dass sie in den richtigen verbleiben.

Veteranen der PKI-Szene mag bei der Meldung ein Deja-vu-Gefühl beschlichen haben: Vor knapp zehn Jahren verlor eine weltweite Banken-PKI kurz nach Betriebsbeginn auf dieselbe Weise die Root-Schlüssel. Ob es ein schlechtes Omen für die eGK ist, dass besagte Banken-PKI inzwischen als Beispiel für einen überkomplexen, grandiosen Fehlschlag gilt?

BDSG novelliert

In der letzten regulären Sitzung dieser Legislaturperiode hat der Deutsche Bundestag am 03.07.2009 den „Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften“ der Bundesregierung vom 18.02.2009 (BT-Drs. 16/12011) entsprechend den Beschlussempfehlungen des Innenausschusses vom 01.07.2009 (BT-Drs. 16/13657) verabschiedet. Im Hau-Ruck-Verfahren wurde damit in letzter Minute auf die teilweise vernichtende Kritik selbst engagierter Verfechter eines gesetzlich geregelten Datenschutzaudits reagiert und das Datenschutzauditgesetz, seit 2001 in § 9a BDSG angekündigt, erneut vertagt. Das Resultat wäre anderenfalls ein mit heißer Nadel gestricktes Gesetz voller handwerklicher Mängel im Detail gewesen – ohne Aussicht, den Datenschutz wirksam zu verbessern.

Nach der nun beschlossenen „Novelle II“, die am 01.09.2009 in Kraft tritt, ist der betriebliche Datenschutzbeauftragte zukünftig nur noch „aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist“ kündbar, und die verantwortliche Stelle verpflichtet, die Teilnahme an Fort- und Weiterbildungsmaßnahmen zu ermöglichen und zu finanzieren. Die Zulässigkeit der Nutzung listenmäßig zusammengefasster Daten für Zwecke des Adresshandels bleibt erhalten. Konsequenter geregelt wurde die Auftragsdatenverarbeitung in § 11 BDSG – eine Überprüfung der Verarbeitung beim Auftragnehmer hat nun vor Beginn der Verarbeitung und regelmäßig während dessen Verlaufs zu erfolgen; die Ergebnisse sind zu dokumentieren. Als neuer § 32 wurde eine Regelung zum Arbeitnehmerdatenschutz ergänzt – gut gemeint, aber inhaltlich nicht mehr als ohnehin bereits geltendes Recht. Schließlich wurden die Geldbußen auf bis zu 300.000 Euro angehoben und damit unmissverständlich klar gestellt: Die Zeit, in der Datenschutzverstöße als Kavaliersdelikt durchgehen, ist endgültig vorbei.

Bedrohungsanalysetools

Wieder war es ein Softwarefehler in BIND 9 des ISC, der ziemlich genau ein Jahr nach der letzten großen Attacke (SSN 07/2008) am 28.07.2009 das weit verbreitete Softwarepaket BIND 9 erneut in die Knie zwang. Diesmal reichte ein einzelnes „dynamic update message“-Paket, um Master-DNS-Server zum Absturz zu bringen – ein weiterer Beleg für die Dringlichkeit sichererer Softwareentwicklung.

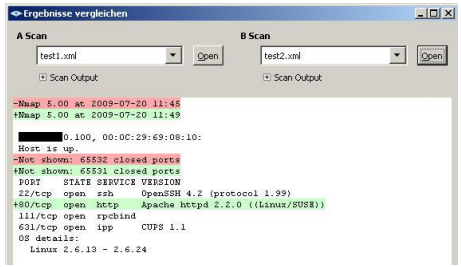
Einen großen Komfortsprung bei der Erstellung von Bedrohungsanalysen für Applikationen verspricht nun Version 3.0 von Microsofts TAM (Threat Analysis and Modelling). An der am 23.07.2009 erschienenen ersten Beta-Version lassen sich, wie erste Tests zeigen, signifikante Fortschritte bei der Bedienbarkeit des Werkzeugs feststellen. Getrübt wird der Eindruck durch Instabilitäten in der Testumgebung: So ließen sich manche Funktionen noch nicht richtig oder gar nicht ausführen. Die Verbesserungen der Visualisierungsmöglichkeiten sind vielversprechend. Bei verbesserter Stabilität wird TAM 3.0 eine sinnvolle Ergänzung des Werkzeugkastens zur sicheren Softwareentwicklung darstellen.

Einen anderen Ansatz verfolgt IBM mit seiner auf die Sicherheit von Web Applikationen zielende Rational AppScan Suite, die in der Enterprise Edition neben dem Application Scanner ein Dashboard mit Reports über die Entwicklung der Zahl und Art der gefundenen Schwachstellen enthält. Dazu erschien am 29.05.2009 in der Serie Redguides das 38seitige

Whitepaper „Improving Your Web Application Software Development Life Cycle's Security Posture“, das auf den ersten 20 Seiten eine sehr anschauliche Einführung in die aktuelle Bedrohungslage und Best Practices zur Entwicklung sicherer Web-Applikationen bietet.

Nmap/Zenmap v5.0

Am 16.07.2009 wurde Version 5.0 des wohl bekanntesten Netzwerk-Portscanners Nmap veröffentlicht. Sie ist sowohl für Linux als auch für Windows verfügbar und bietet über die eigentlichen Scan-Funktionen hinaus die Möglichkeit, grafische Netzwerkübersichten zu erstellen und Scan-Ergebnisse mit früheren Resultaten zu vergleichen.



Auch die Verwaltung der Scan-Profile wurde verbessert, und für alle, die keine Kommandozeilen-Gurus sind, wurde die grafische Oberfläche „Zenmap“ intuitiver und übersichtlicher gestaltet. Schon deswegen lohnt der Wechsel auf die neue Version.

Rechtssicherheit beim § 202c

Mit dem Nichtannahmebeschluss vom 18.05.2009 über drei Verfassungsbeschwerden im Zusammenhang mit dem „Hackerparagraphen“ § 202c StGB hat das Bundesverfassungsgericht Rechtssicherheit geschaffen und klargestellt, dass Programme, die lediglich für Hacking-Angriffe geeignet, nicht aber genau dafür entwickelt wurden (so genannte „Dual Use“-Software) nicht unter die Strafvorschrift fallen. Zur Durchführung von Penetrationstests ist auch die Nutzung von Hacking- und Analyse-Tools wie Nmap zulässig – sollte allerdings nachvollziehbar dokumentiert werden.

Urlaubsrätsel

Wer auch im Urlaub Security-Themen nicht missen und auch am Strand nicht von der Websicherheit lassen will, dem sei das OWASP-Kreuzworträtsel empfohlen. Es gibt auch was zu gewinnen – aber Beeilung, das Rätsel ist seit dem 21.07.2009 online.

Secorvo News

Secorvo College aktuell

Direkt nach der Sommerpause haben Sie wieder Gelegenheit, Ihre Information-Security Kenntnisse zertifizieren zu lassen: Am 07.09.2009 startet die fünftägige TISP-Schulung mit anschließender Prüfung. Auch bei allen weiteren Seminaren, die wir im Herbst anbieten, präsentieren Ihnen unsere Experten gebündeltes Wissen und Expertise aus langjähriger Berufserfahrung und Beratungspraxis. Sichern Sie sich einen der wenigen noch freien Plätze für „IT-Sicherheitsaudits in der Praxis“ vom 21. bis 23.09.2009 oder für „PKI“ vom 03. bis 06.11.2009.

Den „Schwarzen Gürtel“ in sicherer Softwareentwicklung können Sie vom 29.09. bis 02.10.2009 in Gestalt des CPSSE-Zertifikats (Certified Professional for Secure Software Engineering) erwerben oder Ihre IT-Security Grundlagenkenntnisse mit dem Seminar „IT-Sicherheit heute“ vom 13. bis 16.10.2009 auffrischen. Programme und Online-Anmeldung unter www.secorvo.de/college.

Security News Symposium

Mit den Secorvo Security News unterstützen wir Sie seit Juli 2002 Monat für Monat dabei, in der Informationsflut der IT-Sicherheit die wichtigsten Entwicklungen nicht aus den Augen zu verlieren, und lassen Sie an unseren Einschätzungen teilhaben. Aber nicht alle wichtigen Entwicklungen der Informations- und IT-Sicherheit lassen sich in einem wenige Zeilen umfassenden Beitrag angemessen beleuchten. Daher greifen wir in diesem Jahr mit dem ersten „Security News Symposium 2009“ am **06.-07.10.2009** in Ettlingen ausgewählte Themen auf und möchten sie in Vorträgen und Diskussionen mit Ihnen vertiefen. Zusammen mit ausgewählten weiteren Fachexperten bieten wir Ihnen ein spannendes und hoch aktuelles Programm in einem inspirierenden Ambiente – und freuen uns auf den Austausch mit Ihnen (Anmeldung).

Vertrag ist Vertrag

Auf dem Event „Pacta sunt servanda“ weiht Sie die KA-IT-Si am 24.09.2009 in „Design by contract – die hohe Schule der sicheren Softwareentwicklung“ ein. Hagen Buchwald, Vorstandsvorsitzender des Cyber-Forum e.V., gibt Einblick in den Prozess, der Softwareentwicklern helfen soll, das reibungslose und Sicherheitslücken freie Zusammenspiel einzelner Programmmodule von Anfang an zu gewährleisten. Im Anschluss gibt es wie immer die Möglichkeit zum Buffet Networking. Das Event beginnt um 18 Uhr im Schlosshotel Karlsruhe (Anmeldung).

Veranstaltungshinweise

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

August 2009	
12.-14.08.	USENIX Security '09 (Usenix, Montreal/CA)
16.-20.08.	Crypto 2009 (IACR, Santa Barbara/US)
17.-18.08.	Digital Forensic Research Workshop (DFRWS, Montreal/CA)
September 2009	
06.-09.09.	CHES: Workshop on Cryptographic Hardware and Embedded Systems (IACR, Lausanne/CH)
07.-11.09.	TISP-Schulung (Secorvo College)
15.-17.09.	IMF 2009: 5th International Conference on IT Security Incident Management & IT Forensics (GI, Stuttgart)
17.09.	RZ-Compliance (Lampertz/Secorvo/Kroll Ontrack, Friedrichshafen)
21.-23.09.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
24.09.	Pacta sunt servanda (KA-IT-Si, Karlsruhe)
29.09.-02.10.	ISSECO Certified Professional for Secure Software Engineering – CPSSE (Secorvo College)

Fundsache

Seth Misenar systematisiert in seinem am 13.06.2009 bei SANS publizierten Aufsatz „A Virtually Secure Browser" die aktuellen Bedrohungen beim Surfen im Internet. Als wirksame Schutzmaßnahme empfiehlt er insbesondere den Einsatz einer lokalen Sandbox: Damit lässt sich die Sicherheit beim Surfen ohne signifikanten Komfortverlust erheblich steigern. Ein Ansatz, den auch Microsoft im Projekt Office 2010 verfolgt.

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch und Jochen Schlichting.

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

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

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

secorvo
security consulting

Secorvo Security News

August 2009

Gefährliche Gewissheiten

In seinem kürzlich erschienenen lesenswerten Thriller „Der Täuscher“ (2009) schildert Jeffery Deaver, wie leicht überzeugende Tatbeweise konstruiert und so Straftaten Unschuldigen „untergeschoben“ werden können.

Nicht ahnen konnte er beim Verfassen seines Romans (Originaltitel: „The Broken Window“), dass es noch schlimmer kommen würde. Inzwischen wissen wir, dass selbst DNA-Spuren ein zweifelhaftes Beweismittel sind. Nicht nur, dass DNA auch bei der Spurensuche am Tatort und durch Verunreinigung hinterlassen werden kann, wie die monatelange peinliche Suche nach dem „Phantom“ eindrucksvoll bewies. Nun wiesen vier israelische Forscher in dem am 17.07.2009 im Fachorgan der International Society for Forensic Genetics erschienenen Beitrag „Authentication of forensic DNA samples“ nach, dass jeder Biologiestudent im 3. Semester DNA-Spuren fälschen kann.

Auch IT-forensische Beweismittel wackeln. Nach einem Bericht des Daily Telegraph vom 25.08.2009 belegt eine interne Studie der britischen Polizei die geringe Wirkung der aufwändigen Videoüberwachung: Auf je 1.000 Kameras käme gerade eine aufgeklärte Straftat – pro Jahr. Eine Erkenntnis, die sich mit den Ergebnissen einer Studie der Berliner Verkehrsbetriebe aus dem Jahr 2006 deckt: Das Bildmaterial erlaubte selten eine Täteridentifikation, und eine Abschreckungswirkung war nicht nachweisbar. Ein ähnliches Schicksal droht der Vorratsdatenspeicherung, sofern sie kommt: Darf man aus der IP-Adresse eines DSL-Anschlusses tatsächlich auf einen Täter schließen? Was, wenn sich dahinter ein schlecht oder gar nicht geschütztes WLAN verbirgt? Dasselbe gilt für forensische Analysen beschlagnahmter PCs. Was beweist die Entdeckung kinderpornographischer Bilder, wenn das Passwort schlecht gewählt oder bekannt ist?

Rechtfertigt mit dem zweifelhaften Argument gesteigerter innerer Sicherheit dulden wir die Entstehung unkontrolliert wachsender Datensammlungen – mit der voraussehbar fatalen Folge einer kontinuierlichen Verkleinerung des privaten Rückzugsraums.

Inhalt

Security News

iSpion

Die kontrollierte Verbreitung mobiler Applikationen, wie von Apple für das iPhone und von Nokia für SymbianOS praktiziert, bietet in der Praxis nur einen unzureichenden Schutz, wie ein Blogeintrag am 31.07.2009 enthüllte: Auf zahlreiche Benutzerdaten, von der ID-Nummer des Geräts über das Geburtsdatum (falls Facebook genutzt wird) bis zum aktuellen Standort als Geokoordinate, greifen beliebige iPhone-Apps zu – um die gesammelten Daten an die Firma Pinchmedia weiter zu leiten, die daraus Statistiken z. B. zur Nutzungshäufigkeit und -dauer erstellt. Um Zustimmung zu dieser Übermittlung werden Nutzer von den wenigsten Apps gebeten – nach Ansicht von Pinchmedia genügt dazu die allgemeine Nutzervereinbarung von Apple.

Um so erfreulicher der Ansatz, den Rich Cannings vom – nicht gerade für Datensparsamkeit bekannten – Konzern Google am 12.08.2009 auf der diesjährigen Usenix in Montreal vorstellte: In das auf Linux und OpenSource basierende Handy-Betriebssystem Android werden Mechanismen integriert, die den Benutzer entscheiden lassen, ob er z. B. einem Spiel den Zugriff auf seinen Adressbestand gestatten möchte. Auch wenn die Gefahr besteht, dass wenig versierte Benutzer einfach „permit all“ wählen, erscheint der Ansatz geeignet, das zu Grunde liegende Privacy-Problem durch Transparenz und Benutzerkontrolle zu lösen.

RainbowCrack 1.4

Am 17.08.2009 gab das Projekt RainbowCrack (siehe SSN 6/2009) eine erneut deutlich verbesserte Version 1.4 ihres Passwort-Crackers frei: Auf einem mit der Grafikkarte NVIDIA GForce 9800 GTX+ ausgestatteten PC prüft sie knapp 104 Milliarden NTLM-Hashwerte pro Sekunde – eine 40-prozentige Steigerung. Alpha-numerische 10-Zeichen-Passwörter sind damit nach spätestens 1,5 Monaten gefunden.

Blitzkekse

Am 10.08.2009 veröffentlichten fünf amerikanische Forscher eine Studie über Sicherheits- und Datenschutzimplikationen von Flash-Cookies („Flash Cookies and Privacy“). Dabei handelt es sich wie bei HTTP-Cookies um Mechanismen zur Speicherung von Statusinformationen zwischen Aufrufen von Webseiten.

Die Studie gibt einen guten Überblick über die Technik der immer populäreren Flash-Cookies. So kann ein Flash-Cookie 100 KB an Informationen speichern – gegenüber maximal 4 KB bei traditionellen HTTP-Cookies. Flash-Cookies können browserübergreifend ausgelesen werden, und werden von den Privacy-Mechanismen in aktuellen Browsern nicht erfasst.

Komfortable Werkzeuge zur Benutzerkontrolle von Flash-Cookies sind Mangelware. Adobe bietet zur Steuerung der lokalen Einstellungen den „Settings Manager“ als Flash-Applikation an, der – wenn auch unkomfortabel – eine gewisse Kontrolle von Flash-Cookies ermöglicht. Seit Version 2.19.889 (Mai 2009) unterstützt das freie Tool CCleaner die Löschung von Flash-Cookies. Nutzern von Firefox immerhin bietet das Add-on BetterPrivacy eine Flash-Cookie-Kontrolle.

Fortschritte bei AES-Analyse

So sicher wie der Tag der Nacht folgt verbessern sich auch Analysen kryptographischer Verfahren. So hat ein Team um Biryukov und Khovratovich zum zweiten Mal in diesem Jahr einen Angriff auf AES vorgestellt. Dessen Grundlage ist eine Schwäche im Key-Scheduling, das die Rundenschlüssel aus dem eigentlichen Schlüssel ableitet.

Der gegen AES-192 und AES-256 mit reduzierter Rundenzahl gerichtete Angriff ist eine Related-Key-Attacke, d. h. der Angreifer benötigt nicht beliebige Klartext-Schlüsseltext-Paare, sondern solche, die *verschiedene* Schlüssel in einer *dem Angreifer bekannten* Beziehung verwenden. Der Angriff ist wirkungslos, wenn für jede Verschlüsselung ein zufällig gewählter Schlüssel verwendet wird, und betrifft keine AES-Variante mit voller Rundenzahl.

Dennoch ist der Angriff etwas befremdlich: Obgleich man eine stetige Verbesserung der Angriffe erwarten kann, ist der sprunghafte Fortschritt überraschend. AES-256 hat 14 Runden, davon sind bereits 10 mit einem praktikablen Angriff überwunden. Und ausgerechnet AES-256, das mutmaßlich stärkste Mitglied der AES-Familie, weist hier die größten Schwächen auf, während AES-128 praktisch unbehelligt bleibt. Man hüte sich jedoch vor falschen Schlüssen: AES-256 ist nach wie vor erheblich schwerer zu brechen als AES-128, denn für beide Verfahren ist bei voller Rundenzahl weiterhin Brute-Force der beste bekannte Angriff.

Wird den AES nun dasselbe Schicksal ereilen wie den SHA-1, dessen Sicherheit schneller als erwartet erodiert ist (siehe SSN 6/2009)? Die Autoren halten den Angriff für bedenklich, gleichwohl sind sie weit davon entfernt, AES als unsicher zu deklarieren. Auch David Wagner, Koautor von Twofish, meldet sich in Bruce Schneier's Blog in diesem Sinne zu Wort: Der AES ist, spezifikationsgemäß eingesetzt, sicher. Kein Grund zur Panik also.

Exploits kein Kinderspiel

Alexander Sotirov präsentierte am 12.08.2009 auf der Usenix einen historischen Abriss der letzten 10 Jahre Exploit-Entwicklung. Danach schien 2004 die Welt aus Entwicklersicht noch in Ordnung: War eine Schwachstelle entdeckt, ließ sich ein Exploit innerhalb kurzer Zeit entwickeln. Während Schwachstellen seitdem immer leichter zu finden sind, wird die Entwicklung von Exploits hingegen durch neue Sicherheitsmechanismen in Betriebssystemen erschwert. Zwar ist ein Denial-of-Service-Angriff über einen Buffer Overflow immer noch eine vergleichsweise einfache Sache – die Ausführung von eigenem Code wird hingegen schwieriger. Nach Sotirov kann die Entwicklung eines zuverlässigen Exploits heute mehrere Monate erfordern.

Damit verschiebt sich im Wettrennen zwischen Exploits und Patches das Gleichgewicht zu Ungunsten der Angreifer, sofern die Schwachstelle bekannt ist – vorausgesetzt, die Sicherheitsfunktionen des Betriebssystems werden ausreichend genutzt.

Fast alles über Chipkarten

Die fünfte Auflage des „Handbuchs der Chipkarten“ von Wolfgang Rankl und Wolfgang Effing erschien nach zweijähriger Überarbeitung im August 2008. Angesichts von über 1100 Seiten braucht man eine kräftige Hand, um das Buch zu halten. Da ist es einfacher zu sagen, was nicht darin enthalten ist: Kryptologische Grundlagen werden nur so weit behandelt, wie dies für Anwendungen in Chipkarten relevant ist, und auch zur Einbindung in PC-Betriebssysteme finden sich eher überblicksartige Informationen – Details zu Themen wie Windows Smart Card Logon, .NET-Karten oder Kartenmanagement-Systeme sucht man vergeblich.

Aber alles, was an Chipkarten-Basistechnik dazwischen liegt, ist ausführlich beschreiben. Die Liste der Angriffe auf Chipkarten reicht vom Abgreifen der Kommunikation an den Kontakten bis zu den Mifare-Attacken vom vergangenen Jahr. Eine der wichtigsten Überarbeitungen ist die Darstellung kontaktloser Karten. Speziell die ISO 14443 „Proximity“-Kommunikation wird dank Near Field Communication in Handys und dem elektronischen Personalausweis immer wichtiger.

Auch mit dieser Auflage ist die Geschichte der Chipkarten sicher noch nicht zu Ende: Die Kapitel zu elektronischen Gesundheitskarten und Chipkarten als Ausweisdokumenten warten darauf, fortgeschrieben zu werden. Dennoch gehört das aktualisierte Standardwerk in den Bücherschrank.

Sommerrätsel

Amateur- und Profi-Kryptologen, die ein wenig Denksport an heißen Tagen mögen, mögen sich an dem folgenden Kryptogramm versuchen:

```
signaturif+kaoti+aun+lzqimiuaia+sig
eebu+signaturiz+m0+g9
```

Unter allen richtigen Lösungen, die die Redaktion unter redaktion-security-news@secorvo.de bis zum 30.09.2009 erreichen, verlosen wir unter Ausschluss des Rechtswegs drei Exemplare des „Handbuchs der Chipkarten“.

Secorvo News

Secorvo College aktuell

Unsere Herbstseminare erfreuen sich erheblicher Nachfrage – daher sichern Sie sich bei Interesse möglichst bald einen der wenigen noch freien Plätze des Seminars „IT-Sicherheitsaudits in der Praxis“ (21.-23.09.2009) bzw. „PKI“ (03.-06.11.2009).

Vom 29.09. bis 02.10.2009 gibt es den „Schwarzen Gürtel“ in sicherer Softwareentwicklung – in Gestalt des CPSSE-Zertifikats. Eine Auffrischung Ihrer IT-Security Grundlagenkenntnisse bietet das Seminar „IT-Sicherheit heute“ (13.-16.10.2009).

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

Erstes Security News Symposium

Die Themengebiete IT-Sicherheit und Datenschutz unterliegen ständiger Weiterentwicklung – das merken wir nicht zuletzt Monat für Monat bei der Zusammenstellung unserer Security News. Aber nicht alle wichtigen Entwicklungen lassen sich in einem kurzen Textbeitrag angemessen beleuchten.

Daher bieten wir Ihnen in diesem Jahr erstmalig mit dem „Security News Symposium 2009“ am 06.-07.10.2009 in Ettlingen die Gelegenheit, ausgewählte Themen – darunter der Umgang mit USB-Sticks, Aktuelles zur Passwortsicherheit und zur Zukunft des Mifare-Chips – in Vorträgen, Demonstrationen und Diskussionen mit uns und weiteren Fachexperten zu vertiefen.

Die Vorträge und Referenten, das können wir versprechen, werden vom Feinsten sein – ein fachliches „Best of“ in einem inspirierenden Ambiente. Wir freuen uns auf Ihr Kommen und den Austausch mit Ihnen (Anmeldung).

Veranstaltungshinweise

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

September 2009	
06.-09.09.	CHES: Workshop on Cryptographic Hardware and Embedded Systems (IACR, Lausanne/CH)
15.-17.09.	IMF 2009: 5th International Conference on IT Security Incident Management & IT Forensics (GI, Stuttgart)
17.09.	RZ-Compliance (Lampertz, Friedrichshafen)
21.-23.09.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
24.09.	Pacta sunt servanda (KA-IT-Si, Karlsruhe)
29.09.-02.10.	ISSECO Certified Professional for Secure Software Engineering – CPSSE (Secorvo College)
Oktober 2009	
06.-07.10.	Security News Symposium 2009 (Secorvo, Ettlingen)
13.-16.10.	IT-Sicherheit heute (Secorvo College)
November 2009	
03.-06.11.	PKI (Secorvo College)
23.-27.11.	TISP-Schulung (Secorvo College)

Fundsache

Am 16.08.2009 veröffentlichte John Gerber in seinem Blog eine hilfreiche Zusammenstellung von 30 „Cheat Sheets“ zu diversen Security Themen, darunter auch ausgefallenere wie „Reverse-Engineering Malware Cheat Sheet“ und „Troubleshooting Human Communications“. Ergänzend verweist er auf weitere „Cheat Sheets“ zu Tools, Netzwerktechniken und weiteren Sammlungen.

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch

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

secorvo
security consulting

Secorvo Security News

September 2009

Profilvertrieb

Die hohe Kunst des Vertriebs beginnt lange vor der Kontaktaufnahme mit potentiellen Kunden. Ein gutes Produkt, gute Argumente und ein überzeugungsstarker Vertrieb allein garantieren keinen Verkaufserfolg: Entscheidend sind die „Streuverluste" bei der Auswahl der Kontakte. Daher ist das Bemühen verständlich, die Selektion durch das Sammeln von Informationen zu schärfen. Besonders viel versprechend sind echte Interessenten – Menschen mit Bedarf, die sich bereits über das Angebot informiert haben.

Da bietet der eigene Internetauftritt gänzlich neue Möglichkeiten. Webseiten-Optimierungstools wie Google Analytics haben den Appetit geweckt: Welche Seiten hat ein Nutzer besucht? Hat er eine Demo-Software, ein Datenblatt oder eine Leistungsbeschreibung heruntergeladen? Wie viel Zeit hat er auf der Seite verbracht?

Wie schön wäre es, aus der IP-Adresse auf die Identität des Besuchers schließen und ihn unmittelbar kontaktieren zu können! Oft ist das nicht schwierig: Hat er einmal ein Kontaktformular ausgefüllt, können Name und Anschrift im CRM mit der IP-Adresse verknüpft werden – und jeder weitere Besuch lässt sich zuordnen. Kostenlose Angebote wie utrace oder infosniper liefern auf Knopfdruck Provider und Domaininhaber, kommerzielle Anbieter ordnen IP-Adressen recherchierte Namen zu. Und wäre es vor einem Anruf nicht gut zu wissen, bei welchem Wettbewerber der Besucher sich vorher informiert hat und welches Bildungsniveau und Interessenprofil aus dem Surfverhalten abgeleitet werden können?

Tatsächlich ist die Erstellung von Surf-Profilen ohne Einwilligung des Betroffenen verboten (§ 12 Telemediengesetz). Ein Passus in der Datenschutzerklärung, der eine implizite Einwilligung bei Nutzung annimmt, genügt § 13 (2) TMG nicht. Verstöße sind jedoch verbreitet, wie das Xamit-Datenschutzbarometer vom 30.06.2009 belegt. Wer sicher gehen will, prüft eine Webseite vorher – vielleicht auch einmal die des eigenen Arbeitgebers...

Inhalt

secorvo
security consulting

Security News

Playstation-Cracker

Am 08.07.2009 gelang es der Forschungsgruppe um Arjen Lenstra an der École Polytechnique Fédérale de Lausanne, nach knapp sechs Monaten einen diskreten Logarithmus auf einer elliptischen Kurve über einem endlichen Primkörper von 112 bit zu lösen – mit anderen Worten: den privaten Schlüssel eines asymmetrischen Kryptosystems auf einer elliptischen Kurve der Moduluslänge 112 bit zu bestimmen. Ein neuer Rekord. Zuletzt war im Oktober 2002 die Berechnung eines diskreten Logarithmus auf einer elliptischen Kurve über einem 109 bit großen endlichen Körper gelungen (SSN 1/2003).

Nicht nur die verwendeten „Rechenknechte" sind ungewöhnlich – Lenstra parallelisierte die Berechnung in einem Cluster von über 200 Playstations. Auch die Implikationen sind erheblich, wie Lenstra gemeinsam mit Peter Montgomery, einem weiteren Schwergewicht der Faktorisierungsforschung, in einer IACR-Online-Veröffentlichung vom 01.09.2009 darlegt: Anders als in der berühmten Schlüssellängen-Prognose, die Lenstra 1999 mit Verheul publizierte, kommen die Autoren zu dem Schluss, dass mit der Faktorisierung einer 1024 bit langen Zahl kaum vor 2020 zu rechnen sei; die erste Faktorisierung eines 768 bit langen RSA-Modulus erwarten sie für das kommende Jahr. Diese Einschätzung deckt sich mit einer Prognose von Secorvo aus dem Jahr 2001 (SSN 5/2004).

Durchbruch: 15 = 3*5

Bereits im Jahr 1994 entdeckte Peter Shor einen Algorithmus, der es erlaubt, das RSA-Kryptoverfahren in polynomialer Zeit zu brechen, also ebenso schnell, wie man damit verschlüsseln oder signieren kann. Ein Krypto-GAU. Zum Glück läuft sein Algorithmus nur auf einem hypothetischen Quantencomputer.

Am 03.09.2009 wurde bekannt, dass es Physikern der Universität Bristol gelungen ist, einen rudimentären Quantencomputer zu bauen. Damit gelang es, mit Shors Algorithmus die Zahl 15 in die Primfaktoren 3 und 5 zu zerlegen. Das gleiche Kunststück gelang Forschern von IBM schon im Jahr 2001; die Gruppe aus Bristol verkleinerte jedoch den Experimentalaufbau deutlich. Die Kontrolle von mehr Quanten-Bits zur Faktorisierung größerer Zahlen ist allerdings auch ihnen nicht gelungen.

Beruhigend für RSA-Anwender: In der Welt herkömmlicher Computer stockt die Entwicklung besserer Faktorisierungsalgorithmen, in der Welt der Quanten die von größeren Computern.

Soziale Sicherheitsbugs

Nachdem im von Aviv Raff zum „Month of Twitter Bugs" erklärten Juli 2009 insgesamt 31 Schwachstellen in Third-Party-Diensten rund um Twitter veröffentlicht wurden, stand im September das nächste Soziale Netzwerk im Brennpunkt. Pünktlich zum Bergfest des „Month of Facebook Bugs" am 15.09.2009 wurde im „Halfway Report" ein Zwischenstand veröffentlicht. Danach wurde auch diesmal jeden Tag ein „FAXX Hack" (= Facebook Application XSS/XSRF) veröffentlicht.

Wie einige Social Networks haben Facebook und Twitter einen rasanten Aufstieg hinter sich. Der Erfolg bringt aber offensichtlich zahlreiche Sicherheitslücken mit sich. Beide „MoB"s haben zu einer Erhöhung der Sicherheit der Plattformen beigetragen – wohl auch, weil sich die Betreiber und Entwickler bei der Behebung der Schwachstellen sehr kooperativ zeigten. Hoffentlich nehmen sich weitere Social Networks daran ein Beispiel.

WLAN-Sicherheit

Würden Sie mit einem Flugzeug fliegen, das, sagen wir mal, von Straßenbauingenieuren konstruiert wurde? Wohl kaum. In der digitalen Welt passieren Dinge dieser Art jedoch andauernd. Das WEP-Protokoll zur kryptografischen Sicherung von WLAN-Datenübertragungen gehört zu der Sorte von ad-hoc-Kryptografie, die von Laien entworfen wurde. Es überraschte daher nicht, als WEP im Jahr 2001 gebrochen wurde (SSN 3/2002).

Ein zentraler Punkt der Angriffsstrategie war dabei eine Methode mit dem Namen chopchop. Beim Entwurf des WEP-Nachfolgers WPA verfiel man daher auf die Idee, dieser Strategie mit einer anti-chopchop-Funktion zu begegnen - dazu wurde TKIP erfunden. Anstatt einen fundierten Protokollentwurf vorzulegen, wurde mehr oder weniger lediglich der spezielle Angriff abgewehrt, dem WEP zum Opfer gefallen war.

Im November 2008 wurde eine Schwäche von TKIP bekannt, durch die ein chopchop-Angriff auf WPA möglich wurde (SSN 11/2008). Der Angriff dauert strategiebedingt etwa eine Viertelstunde und ermöglicht lediglich das Erreichen von Teilzielen; ein Angreifer kann das WLAN also (noch) nicht übernehmen. Am 15.07.2009 veröffentlichten japanische Forscher einen praktikablen physischen Man-in-the-Middle-Angriff, der den Angriff verbessert und auf unter eine Minute beschleunigt. Auch wenn dieser nur relativ „kleine" Angriffsziele erreicht, zeigt sich einmal mehr: Hat man erst einmal einen guten Ansatzpunkt für das Brecheisen gefunden, ist die Kiste bald offen.

Was sollte man daraus lernen? Erstens, dass der Umstieg auf WPA2 mit AES-CCMP spätestens jetzt fällig ist, und zweitens, dass beweisbare Sicherheit gelegentlich ein sehr praktisches Fundament für langfristige Sicherheit bildet.

Top Cyber Security Risks

Die von SANS im September 2009 veröffentlichten „Top Cyber Security Risks" bestätigen Trends, die uns schon länger am Herzen liegen. Danach sind die beiden Top Sicherheitsthemen ungepatchte Client-Software, über die Schadcode eingeschleust werden kann, sowie Schwachstellen in Web-Applikationen.

Diese Beobachtung deckt sich mit unseren eigenen Erfahrungen, dass einerseits Netzwerk- und Perimetersicherheit in Firmen immer besser werden, es andererseits aber immer schwieriger wird, die eingelassenen Daten zu kontrollieren. Die Stadtmauern sind errichtet – an den Torkontrollen muss jedoch noch gearbeitet werden.

Open Source Security

Am 21.09.2009 hat der Toolhersteller Coverity den „Scan Open Source Report 2009" veröffentlicht. Für den zum ersten Mal 2006 auf Initiative des Department of Homeland Security (DHS) veröffentlichten Bericht wurden 280 auf C/C++ basierende Open Source Projekte mit statischer Code-Analyse auf Schwachstellen untersucht und vergleichend bewertet. Die Ergebnisse, Metriken und Benchmarks präsentiert der Bericht ausführlich auf 35 Seiten.

In erster Linie ist der Bericht eine Hilfestellung für Entscheider, die Sicherheitsaspekte bei der Auswahl von Open-Source-Lösungen berücksichtigen wollen. Aber auch die teilnehmenden Projekte selbst profitierten von der Untersuchung. Die Verbesserung der Qualität und Sicherheit einzelner Projekte wird von Coverity in der „Scan Ladder" gewürdigt. 127 Projekte erklommen die Stufe 1, 36 inzwischen sogar die Stufe 2 – darunter honorige Vertreter wie OpenVPN, OpenLDAP, Perl und Postfix.

Mobilfunk-Knacken für alle

Die Rechenleistung moderner Grafikprozessoren zieht immer mehr Codebreaker an: Bei der Konferenz Hacking at Random präsentierte Karsten Nohl (bekannt durch seine Analyse der Mifare-Chips) am 15.08.2009 ein Projekt zur weltweit verteilten Vorberechnung der Schlüsselsuche für die GSM-Mobilfunk-Chiffre A5.1, die schon lange „angezählt" ist (SSN 9/2003 und SSN 11/2007).

Nach Abschluss dieser Vorberechnung könnten abgehörte GSM-Gespräche unter Rückgriff auf die dabei erzeugte riesige Tabelle in kurzer Zeit entschlüsselt werden. Falls sie überhaupt verschlüsselt waren: Denn ob die Verschlüsselung ein- oder ausgeschaltet wird, entscheidet das GSM-Mobilfunknetz, und macht damit das Abhören via IMSI-Catcher erst möglich – unsichtbar für den Benutzer, denn fast kein Handy zeigt seinem Besitzer an, in welchem Modus es gerade arbeitet.

Secorvo News

Secorvo College aktuell

Zwei Gelegenheiten zur Aktualisierung, Erweiterung und Zertifizierung Ihres Fachwissens bietet Ihnen Secorvo-College noch in diesem Jahr:

Das viertägige Seminar „PKI – Grundlagen, Vertiefung, Realisierung" am **03.–06.11.2009** lässt keine Ihrer Fragen zu Konzeption, Implementierung und Nutzung von PKIs unbeantwortet.

Und vom **23.–27.11.2009** (mit direkt anschließender Prüfung am 28.11.2009) haben Sie Gelegenheit, Ihre Fachkenntnisse mit dem TISP-Zertifikat zu krönen – das inzwischen schon die Visitenkarten von mehr als 300 Absolventen ziert.

Neben detaillierten Seminarprogrammen mit Online-Anmeldung finden Sie auf unseren Webseiten den druckfrischen Seminarkalender 2010 zur Planung Ihrer Seminarbesuche im kommenden Jahr.

Lesefutter

Immer wieder beschäftigt uns die Frage nach der Angemessenheit diverser Anforderungen an eine Passwort-Policy. Das Ergebnis unserer Überlegungen und vieler Diskussionen haben wir nun publiziert – und räumen darin mit einigen liebgewonnenen, aber irreführenden Überzeugungen auf. Wer noch nicht vollständig auf Token-basierte Zwei-Faktor-Authentisierung umgestellt hat, findet in dem Aufsatz „Passwörter – fünf Mythen und fünf Versäumnisse" (Dirk Fox, Frank Schaefer; DuD 7/2009, S. 425-429) möglicherweise den einen oder anderen wertvollen Hinweis.

Auch zum Löschen von Daten kursieren zahlreiche nicht mehr zeitgemäße Vorstellungen (SSN 1/2009), die zu aufwändigen Verfahren führen. Unser schon im Februar erschienene Aufsatz „Sicheres Löschen von Daten auf Festplatten" (DuD 2/2009, S. 110-113) gibt aktuelle Empfehlungen und stellt geeignete Tools vor.

Security News Symposium 2010

Schon jetzt steht er fest – der Termin unseres „Security News Symposiums 2010". Wer das Event am **20.–21.04.2010** nicht verpassen will, kann sich bereits heute online anmelden.

Veranstaltungshinweise

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

Oktober 2009	
03.-04.10.	Datenspuren 2009 (CCC, Dresden)
06.-08.10.	ISSE 2009 (eema & enisa, The Hague/NL)
28.-30.10.	Hack.LU (CSRRT-LU, Luxembourg)
November 2009	
03.-06.11.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College)
17.-20.11.	In-Depth Security Conference 2009 (DeepSec, Wien/AU)
19.-20.11.	33. Dafta (GDD, Köln)
23.-27.11.	TISP-Schulung (Secorvo College)
Dezember 2009	
27.-30.12.	26th Chaos Communication Congress (CCC, Berlin)
Januar 2010	
19.-21.01.	Omnicard 2010 (inTIME, Berlin)

Fundsache

Derzeit erfreuen sich pointierte Historiendarstellungen großer Beliebtheit. So die Geschichte und Funktionsweise des AES – erzählt von Jeff Moser in knapp 70 Strichmännchen-Bildern. Ebenfalls amüsant ist die knappe History of Hacking. Gleichfalls fokussiert und sehr informativ kommt die mit Unterstützung von Jean-Jacques Quisquater entwickelte interaktive Darstellung der Cryptographic Key Length Recommendations von BlueKrypt daher, zuletzt aktualisiert am 28.09.2009.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch

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

secorvo
security consulting

Secorvo Security News

Oktober 2009

EgPh>10S-uks0Mm*

Trotz aller Ermahnungen, Drohungen, Anleitungen und Best-Practice-Tipps zum sicheren Gebrauch von Passwörtern besteht bis heute ein erhebliches Defizit auf diesem Gebiet. Warum ist das so? Nüchtern betrachtet kann man nur eine Antwort darauf geben: Passwörter sind ungeeignet. Denn es liegt nicht in der Natur des Menschen, sich kontextfreie Zeichenfolgen mit hoher Entropie zu merken.

Zwar gibt es Best-Practice-Regeln zur Ableitung von Passwörtern z. B. aus ganzen Sätzen. Daher werden schlechte Passwörter gerne mit falschen Gewohnheiten begründet, in der tröstlichen Hoffnung, dass für die nächste Generation die Wahl guter Passwörter genauso selbstverständlich sein werde wie andere Dinge des täglichen Lebens. Das greift jedoch zu kurz, denn es geht ja nicht um ein oder zwei Passwörter, sondern zumeist um mehr als ein Dutzend, die unterschiedlich sein und regelmäßig gewechselt werden sollen. Nur wenige Menschen sind dazu in der Lage, und noch weniger sind hierzu gewillt – alle anderen stehen Schlange beim Helpdesk. Das ist wenig überraschend, denn die meisten Menschen wollen einfach nur unbehindert ihren Aufgaben nachgehen, und das Ausdenken und Merken kryptischer Passwörter gehört selten dazu. Das Langzeit-Experiment an Millionen IT-Nutzern lässt nur einen Schluss zu: Für durchschnittliche Menschen sind Passwörter ein völlig ungeeigneter Authentifizierungsmechanismus, und keine noch so guten Tipps (die ja auch erst mal gelesen sein wollen) werden daran etwas ändern.

Der entscheidende Grund für die weite Verbreitung von Passwörtern ist, dass sie so billig sind: ihr sicherer Gebrauch kann auf die Benutzer abgewälzt werden. Passwort-Manager und -Diversifizierer können das Leiden mildern, aber lösen das eigentliche Problem nicht. Wenn Authentifizierung wirklich so kritisch für eine Organisation ist, dann sind Passwörter schlicht und einfach nicht die richtige Wahl.

Dr. Safuat Hamdy

* *„Ein gutes Passwort hat mehr als 10 Stellen – und kann sich kein Mensch merken."*

Inhalt

secorvo
security consulting

Security News

Koalitionspläne

Am 26.10.2009 wurde der zwischen CDU, FDP und CSU ausgehandelte Koalitionsvertrag unterzeichnet. Immerhin knapp 10 der 124 Seiten des Werks beschäftigen sich mit Themen der Inneren Sicherheit, zwei Seiten darunter mit dem Datenschutz.

So sollen zahlreiche Gesetze der Inneren Sicherheit, von der Telekommunikationsüberwachung bis zum BKA-Gesetz, im Hinblick auf die Zielerreichung und den „Schutz des Kernbereichs privater Lebensgestaltung" evaluiert werden – die Ergebnisse früherer Evaluierungen staatlicher Eingriffsbefugnisse geben jedoch wenig Anlass zur Hoffnung auf substanzielle Korrekturen. Der Zugriff der Bundesbehörden auf die Daten der Vorratsdatenspeicherung wird bis zur Entscheidung des Bundesverfassungsgericht ausgesetzt – eine wirksame Stärkung der „Grundsätze der Verhältnismäßigkeit, der (...) Datensparsamkeit, der Zweckbindung" sieht allerdings anders aus.

Die Bürger sollen durch „Aufklärung und Sensibilisierung der Öffentlichkeit zu mehr Selbstschutz und der Nutzung sicherer IT-Produkte" motiviert und es soll eine „Stiftung Datenschutz" errichtet werden, „die den Auftrag hat, Produkte und Dienstleistungen auf Datenschutzfreundlichkeit zu prüfen (...) und ein Datenschutzaudit zu entwickeln". So weit sind wir also schon gekommen: Weil eigene ordnungspolitische Vorstellungen fehlen, wird das Primat der Politik an eine Stiftung delegiert.

Das Bundesdatenschutzgesetz soll dafür „lesbarer und verständlicher" gestaltet und der „Arbeitnehmerdatenschutz in einem eigenen Kapitel (...) ausgestaltet" werden. Auch das De-Mail-Gesetz bleibt auf der Tagesordnung: um „Unternehmen die Möglichkeit (zu) geben, Geschäftsprozesse elektronisch abzuwickeln". Na endlich – darauf haben die deutschen Unternehmen nur gewartet.

Wie von einem unter Zeitdruck und zwischen erfahrenen und unerfahrenen Partnern ausgehandelten Text kaum anders zu erwarten, ist der Koalitionsvertrag eine Mischung aus nebulösen Absichtserklärungen, wenigen konkreten Vereinbarungen und einigen skurrilen Ideen – ein großer Wurf ist er jedenfalls nicht. Immerhin: Die Regierung will zukünftig „die Lebenswirklichkeit der Mehrheit der Menschen in Deutschland (...) berücksichtigen". Offenbar war das bisher nicht üblich.

Schutz vor Querverweisen

Dass Firefox-Anwender mit dem Add-On NoScript die Ausführung von Skripten und anderen potentiell gefährlichen Webseiteninhalten an ihr Einverständnis binden können, hat sich mittlerweile herumgesprochen (siehe auch SSN 10/2008).

Aber auch NoScript stopft nicht alle Bedrohungen auf Webseiten. So ermöglicht es keine Kontrolle von Flash-Cookies (vgl. SSN 08/2009), und bei Cross-Site-Requests – das sind in eine Suite eingebettete Inhalte, die von anderen Websites bezogen werden und oft zur Verfolgung von Benutzer-Aktivitäten dienen – kann NoScript nur die Ausführung von Skripten in diesen Inhalten verhindern, nicht aber den Aufruf selbst. Zumeist hat der Anwender damit schon seine Daten beim Tracking-Server abgeliefert – dazu genügt ein eingebettetes „Null-Pixel"-Bild.

Gegen Flash-Cookies hilft BetterPrivacy und gegen Cross-Site-Requests das zuletzt am 28.07.2009 aktualisierte Add-On RequestPolicy, das ähnlich wie NoScript die komfortable Pflege zulässiger Ausnahmen erlaubt, für unbekannte Websites aber die betreffende Lücke versperrt. Wer darüber hinaus zulässige und verbotene Cookies komfortabler kontrollieren will, als mit Firefox möglich, sollte zu einem Cookie-Manager wie Firecookie greifen.

Benchmarking Software Security

Building Security In Maturity Model (BSIMM) ist eine Sammlung von Best Practices zur sicheren Software-Entwicklung, vergleichbar den Best Practices zur Information Security im Standard ISO/IEC 27002:2005. Das darin beschriebene Software Security Framework (SSF) ist in zwölf Bereiche mit insgesamt 110 empfohlenen Maßnahmen unterteilt. Software-Entwickler können anhand des Abdeckungsgrades der Maßnahmen den Reifegrad der Software-Sicherheit in ihrer eigenen Organisation überprüfen.

Seit dem 24.09.2009 läuft eine von Gary McGraw initiierte Web-Studie, bei der der Umsetzungsgrad eines eingeschränkten Umfangs von Maßnahmen als BSIMM Beginn durch eine Umfrage erfasst wird. Die Ergebnisse dieser Studie sollen den Einstieg in einen geregelten Security-Prozess bei der Softwareentwicklung erleichtern und grundlegende Daten für erste Benchmarks liefern. Die Teilnahme an der Studie ist für alle Interessierten offen und jedem zu empfehlen, der die Qualität dieses Benchmark-Ansatzes zu verbessern helfen möchte.

Schwarzer-Peter-Spiele

Kurz bevor Microsoft am 13.10.2009 – sicher nicht ohne Stolz – auf sechs Jahre Patch Tuesday zurück blicken konnte, erklärte Steve Ballmer am 05.10. 2009 in einem Interview den mangelnden wirtschaftlichen Erfolg von Windows Vista mit den verbesserten Sicherheitsfunktionen: Sie seien für

dessen schlechten Ruf verantwortlich. In diese Perspektive passen die häufigen Sicherheitswarnungen und Rückfragen des Vista-Systems, die bestimmt eben so häufig mit routiniertem Klick auf den „Ist mir doch egal!"-Button ignoriert werden.

In die Diskussion, die das Ballmer-Interview losgetreten hatte, mischte sich am 21.10.2009 Bruce Schneier mit einem bemerkenswerten Argument: Für ihn sind viele Sicherheitswarnungen Ausdruck der Ratlosigkeit von Entwicklern, die die Verantwortung für sicherheitsrelevante Entscheidungen, zu denen sie selbst keine vernünftige Antwort wissen, auf diese Weise als Schwarzen Peter an den überforderten Anwender weitergeben.

Merke: Die Vereinbarkeit von Sicherheit und Bedienbarkeit ist ein zentraler Aspekt der sicheren Softwareentwicklung, der im Kampf gegen Buffer Overflows, Cross Site Scripting & Co. oft vergessen wird. „Security and Usability" ist dementsprechend auch eines der vier Schwerpunkt-Themen der Psychology and Security Resource Page, die Ross Anderson vom Computer Laboratory der Universität Cambridge am 23.10.2009 ins Netz gestellt hat.

Passwörter im Web

Das Bekanntwerden eines umfangreichen und erfolgreichen Phishing-Angriffs auf E-Mail-Accounts von Hotmail und anderen Providern am 01.10.2009 hat erneute Diskussionen über Passwörter als Schutzmechanismus ausgelöst. Dass die Wahl und Nutzung von Passwörtern auch heute immer noch weit entfernt von Best-Practice-Ansätzen ist, belegt eine Analyse der veröffentlichten Passwörter des Tool-Herstellers Acunetix vom 06.10.2009.

Hierdurch inspiriert hat Jeremiah Grossman am 07.10.2009 auf seinem Blog den Eintrag "All about Website Password Policies" veröffentlicht. Darin beleuchtet er verschiedene Aspekte der Passwort-Sicherheit (insbesondere) im Web, wie z. B. Längenbetrachtungen, Zeichenauswahl, Komplexität, Speicherung beim Anbieter, Schutz vor Brute-Force-Angriffen und Gültigkeitsfristen.

Viele Überlegungen zur Passwort-Sicherheit konzentrieren sich auf die Auswahl eines guten Passworts. Die aktuellen Attacken zeigen aber, dass Aufbewahrung und Nutzung eine ebenso wichtige Rolle für die Sicherheit von Passwörtern spielen, da bei den Angriffen auf u. a. Hotmail keine Sicherheitslücken ausgenutzt, sondern die Passwörter den betroffenen Opfern entlockt wurden.

Eine Hilfe bietet das Open-Source-Tool pwdHash vom Stanford Security Lab. Es erzeugt für jede Webseite einen individuellen Schlüssel, den es aus einem Master-Passwort und der URL der Webseite ableitet. Dadurch führt ein kompromittiertes Passwort nicht gleich zur Preisgabe aller eigenen Web-Accounts. Außerdem wird im Falle eines Phishing-Angriffs dem Angreifer ein falsches Passwort übermittelt, da für die Erzeugung die URL der Phishing-Seite einfließt. Das Tool steht in aktuellen Versionen für verschiedene Browser auf der Projektseite zum Download zur Verfügung.

Secorvo News

Secorvo College aktuell

Bevor Secorvo College mit neuen Seminaren in das Jahr 2010 startet, haben Sie noch in diesem Jahr Gelegenheit, Ihr Wissen mit dem TISP-Zertifikat zu besiegeln. Sichern Sie sich einen Platz auf der TISP-Schulung vom 23. bis 27.11.2009 mit direkt anschließender Prüfung am 28.11.2009. So starten Sie mit einem Know-How-Update ins neue Jahr. Detaillierte Seminarbeschreibungen des Schulungsangebots für 2010 finden Sie auf unseren Webseiten, darunter die neuen Seminare Datenschutzaudit und Sicherheitsmanagement. Eine Planungserleichterung bietet Ihnen die praktische Jahresübersicht 2010. Wir freuen uns auf Ihre Anmeldung.

Passwort- und Schlüssellängen

Nicht nur Rechenleistung und Speicherkapazität (Verdoppelung alle 1,5 Jahre gemäß Moore's Law), sondern auch Angriffsalgorithmen wie RainbowCrack (siehe SSN 08/2009) entwickeln sich weiter. Daher müssen kryptographische Schlüssel und Passwort-Mindestlängen von Zeit zu Zeit an die technische Entwicklung angepasst werden. Der Frage, welche Längen heute und für die kommenden Jahre zu empfehlen sind, geht der Beitrag „Mindestlängen von Passwörtern und kryptographischen Schlüsseln" von Dirk Fox nach, erschienen in Datenschutz und Datensicherheit (DuD), Heft 10/2009.

Abrakadabra

Das letzte KA-IT-Si-Event in diesem Jahr dreht sich rund um die Datenrettung. In einem Expertenbericht zeigt Margret Horn von Kroll Ontrack, was zu tun ist, wenn eine Datei versehentlich gelöscht wird oder eine Platte plötzlich defekt ist. Was lässt sich überhaupt retten? Wann ist eine Datei unwiederbringlich gelöscht? Was sollte man bei einer unbeabsichtigten Löschung tun, um eine Datenrettung zu erleichtern – ohne noch mehr Schaden anzurichten? Am 26.11.2009 erfahren Sie es – ab 18 Uhr im Schlosshotel Karlsruhe. Im Anschluss gibt es wie immer die Möglichkeit zum Buffet Networking. Um Anmeldung wird gebeten.

Veranstaltungshinweise

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

November 2009	
03.-06.11.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College)
17.-20.11.	In-Depth Security Conference 2009 (DeepSec, Wien/AU)
19.-20.11.	33. Dafta (GDD, Köln)
23.-27.11.	TISP-Schulung (Secorvo College)
Dezember 2009	
27.-30.12.	26th Chaos Communication Congress (CCC, Berlin)
Januar 2010	
19.-21.01.	Omnicard 2010 (inTIME, Berlin)
Februar 2010	
02.-03.02.	20. SIT-SmartCard-Workshop (Fraunhofer-Institut SIT, Darmstadt)
05.-07.02.	ShmooCon 2010 (Shmoo Group, Washington/USA)
09.-10.02.	17. DFN Workshop – Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)

Fundsache

Am 24.08.2009 ging die Webseite „verbraucher-sicher-online.de“ an den Start. Das vom Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz geförderte und der TU Berlin umgesetzte Projekt bietet eine Sammlung von Hilfestellungen für den Schutz von Rechnern und Daten. Die Hinweise richten sich an Privatnutzer, dürften aber auch in Awareness-Kampagnen hilfreich sein.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch

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

secorvo
security consulting

Secorvo Security News

November 2009

Social Engineering 2.0

Für viele Jugendliche ist der eigene Auftritt in SchülerVZ, Wer-kennt-wen oder Facebook inzwischen ein soziales Muss, wie die Nutzerzahlen von Sozialen Netzwerken belegen. Und immer mehr Berufstätige pflegen ihre Kontakte über Business-Netzwerke wie Xing oder publizieren ihre Ein- und Ansichten in Twitter. Diese Entwicklung ist schon allein aus Datenschutzperspektive bedenklich: Neben den gespeicherten Personendaten kennt der Netzwerk-Betreiber alle Kontaktbeziehungen, das Nutzungsverhalten und die Suchanfragen.

Für einen Social Engineer ist ein mächtigeres Auskunftssystem hingegen kaum vorstellbar. Jeder registrierte Nutzer kann die öffentlichen Teile aller Personenprofile einsehen und nach Unternehmen und Personen, in deren persönlichen Daten, Interessen und Kontakten recherchieren – ideales Informationsfutter für einen gezielten Social Engineering Angriff. Da die Identität bei der Registrierung nicht überprüft wird, fällt es leicht, sich mit falschem Namen und CV anzumelden, um sich anschließend in das Kontaktnetz anderer Nutzer hineinzumogeln. Dann sind deren Kontakte, Telefondurchwahl und Mobilfunknummer, Interessen, E-Mail-Adresse und jede Änderung im Kontakt-Netzwerk sichtbar. Und Auswertungstools wie Twitnest liefern die wichtigsten Kontaktknoten frei Haus.

Zum Schutz vor raffinierten Social Engineers hilft da nur ein striktes Nutzungsverbot – oder die Aufklärung über „Dos and Don'ts".

Abb. 1: Twitnest-Grafik

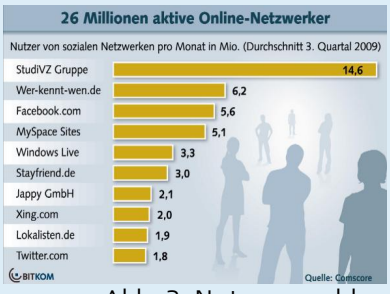


Abb. 2: Nutzungszahlen

Inhalt

secorvo
security consulting

Security News

Angriff auf SSL/TLS

Marsh Ray und Steve Dispensa deckten am 04.11.2009 eine bislang unbekannte, gravierende Schwäche des SSL- und TLS-Protokolls – seit Januar 1999 IETF-Standard – auf. Sie erlaubt einem Angreifer, beliebigen Text in die Kommunikation zwischen Client und Server einzuschleusen. Im Fall von HTTPS kann das z. B. dazu führen, dass ein Client ein vom Angreifer bestimmtes Formular im Kontext einer neuen Sitzung angezeigt bekommt.

Die Schwäche betrifft das Protokoll zur Neuaushandlung von Sitzungsschlüsseln. Zwar bleibt die Vertraulichkeit gewahrt, aber bei der Aushandlung entsteht eine „Authentizitäts-Lücke", durch die nicht nur der Client oder Server, sondern auch ein Angreifer die (üblicherweise gar nicht benötigte) Neuaushandlung veranlassen kann. Der Angriff wurde zunächst für Client-Zertifikate demonstriert, funktioniert jedoch auch allein mit Server-Zertifikat. Betroffen sind alle Anwendungsprotokolle vom Online-Banking bis POP3S, die SSL/TLS nutzen.

Als schnelle Abhilfe gibt es zumindest für OpenSSL einen Patch, der die Neuaushandlung von Schlüsseln einfach abschaltet.

Ein so wirksamer Angriff auf ein so gut untersuchtes und etabliertes Protokoll wie SSL/TLS kommt sehr überraschend. Er zeigt aber einmal mehr, dass Schwachstellen oft an den „Nähten" auftreten (hier der Kontextwechsel zwischen zwei Sitzungen), und dass daher selten genutzte Features in einem Sicherheitsprotokoll entweder weggelassen oder mindestens ebenso genau analysiert werden sollten wie das Kernprotokoll.

(Alp)Traum iPhone

Dem seit dem 19.06.2009 in Deutschland verfügbaren iPhone 3GS hat Apple neben einer neuen Betriebssystemversion auch eine hardware-basierende Verschlüsselung gegönnt. Dank dieser und weiterer Sicherheitsfunktionen wie IPSec VPN, WPA2 Enterprise Wi-Fi und SSL/TLS erfreut sich das iPhone 3GS auch in Unternehmen wachsender Beliebtheit. Um letzte Zweifler von der Sicherheit des iPhone zu überzeugen, bietet Apple mit dem Dienst „Mobile Me" für 79 €/Jahr die Services „Mein iPhone suchen" und „Remote Wipe" an. Damit sollen sich ein vermisstes iPhone lokalisieren und alle Benutzerdaten aus der Ferne löschen lassen.

Der Sicherheitsgewinn ist jedoch begrenzt, denn zur Deaktivierung beider Dienste genügt es, die SIM-Karte zu wechseln. Auch die Datenverschlüsselung lässt sich umgehen, selbst wenn das iPhone durch einen Passcode gesperrt ist, wie Jonathan Zdziarski am 23.07.2009 in einem Interview mit dem Magazin Wired beschrieben und in einem tags darauf auf Youtube veröffentlichten Video demonstriert hat. Denn wie beim iPhone 2G/3G ist eine „Sicherung" der Benutzerdaten auch beim iPhone 3GS ohne Aufspielen einer modifizierten Firmware und ohne Brechen der Verschlüsselung möglich. Dazu wird das iPhone von einer RAM-Disk gebootet und dann die Partition mit den Benutzerdaten als Raw-Disk-Image gesichert – für die Entschlüsselung der Daten sorgt das iPhone dabei automatisch. Anschließend lässt sich das Raw-Image unter Mac OS mounten oder mit gängigen Forensik-Tools analysieren.

Das Glück des Forensikers ist in diesem Fall zugleich der Alptraum des Sicherheitsverantwortlichen, der seinem Management darlegen muss, warum der sichere Einsatz des iPhones im Unternehmen tatsächlich nicht so einfach ist, wie Apple verspricht.

Windows 7 Sicherheitsprofile

Mit dem am 28.10.2009 von Microsoft veröffentlichten Security Compliance Management Toolkit stehen nun neben einer detaillierten Dokumentation der Sicherheitseinstellungen von Windows 7 auch zwei direkt nutzbare Grundtypen von Sicherheitsprofilen zur Verfügung: Die Profile EC (Enterprise Client) und SSLF (Specialized Security – Limited Functionality), beide schon von ihrer Einführung für Windows XP, Server 2003, Vista und Server 2008 im Februar 2009 bekannt.

SSLF folgt dem Prinzip, Sicherheitseinschränkungen vor Funktionalität zu stellen, und legt damit eine gute Grundlage für die Härtung kritischer Systeme. Spezialisten sei als weiterführende Lektüre das Windows 7 and Windows Server 2008 R2 Application Quality Cookbook empfohlen.

Schade nur, dass der Fehler von vergangenen Windows-Härtungen konsequent fortgesetzt wurde: auch diesmal werden die Sicherheitseinstellungen der Zugriffskontrolllisten (DACL) für u. a Dateisystem, Registrierung und Dienste (Services) sowie die dazugehörigen Auditfunktionen (SACL) nicht weiter gewürdigt. Mit Windows NT4 (SP6a) war Microsoft da schon einmal weiter.

OWASP Top 10 runderneuert

Im Rahmen der OWASP Appsec 2009 in Washington stellte Dave Wichers am 13.11.2009 die Überarbeitung der bekannten OWASP Top 10 vor. Zeitgleich wurde der Release Candidate 1 der Top 10 zum Download veröffentlicht.

Bei der neuen Version handelt es sich um die inzwischen dritte Überarbeitung. Die Änderungen liegen etwas im Verborgenen, prägen aber den Charakter der neuen Top 10 grundlegend. Listeten

die Vorgängerversionen die am meisten auftretenden Schwachstellen bei Web-Anwendungen auf, orientieren sich die Top 10 nun an Risiken, die nach vorgegebenen Kriterien bewertet wurden. Dabei wurden Angreifer, Ausnutzbarkeit der Schwachstelle und mögliche Auswirkungen berücksichtigt.

Auch die Darstellung der Top 10 hat sich verändert. Zielte das Dokument bisher hauptsächlich darauf, die Awareness von Entwicklern für Schwachstellen zu verbessern, wurde die Zielgruppe jetzt auf Entscheider, Tester und Sicherheitsexperten erweitert. Jeder Eintrag besteht aus einer Bewertung des Risikos, der Vorstellung von Schutzmaßnahmen, Beispielen und Referenzen. Die meisten der enthaltenen Verweise zeigen auf hilfreiche OWASP-eigene Dokumente.

In den neuen Top 10 haben die beiden Spitzenreiter der Vorversion „Injection" und „XSS" die Plätze getauscht. Auf Platz 6 und 8 finden sich als Neueinsteiger „Security Misconfiguration" und „Unvalidated Redirects and Forwards". Zur Zeit befinden sich die Top 10 noch in der Review-Phase. Kommentare und Verbesserungsvorschläge an den Autor sind herzlich willkommen.

Vorsicht Falle!

Für einen am 04.09.2009 veröffentlichten Technical Report hat sich Frank Stajano von der Universität Cambridge mit Paul Wilson, einem der Autoren der BBC-Serie „The Real Hustle" (einer Art Mischung aus „Vorsicht Falle!" und „Vorsicht Kamera!") zusammen getan – nicht, um Prinzipien der Informationssicherheit anschaulich zu illustrieren, sondern um die „menschlichen Faktoren" zu verstehen, die Trickbetrüger regelmäßig ausnutzen.

Der Report stellt zunächst zahlreiche typische, in der Sendung gezeigte Betrugsfälle vor. Daraus leiten die Autoren dann sieben Verhaltensprinzipien von Ablenkung über Herdentrieb bis zum gefühlten Zeitdruck ab, die Betrüger ausnutzen – und die es im Umkehrschluss beim Design von sicher nutzbaren Systemen zu vermeiden gilt.

Das Dokument liefert viele lebendige Beispiele zur Illustration von Security-Themen – und könnte als Lehrmaterial für Entwickler von Security-relevanten Benutzerschnittstellen effektiver sein als manches Theorie lastige „Securitiy & Usability"-Papier. Unterhaltsamer ist es allemal.

Secorvo News

Secorvo College aktuell

Der TISP ist etabliert: Seit der Einführung im Jahr 2004 haben 350 Teilnehmer das Zertifikat erworben – Tendenz steigend. Gehören auch Sie zu den ersten 500 und buchen Sie Ihren Platz in einer der TISP Schulungen 2010 bei Secorvo College – zum Beispiel vom 22. bis 26.02.2010. Auch in der Softwareentwicklung beginnt sich erfreulicherweise Sicherheit als Qualifikation durchzusetzen. Das zeigt unter anderem das Interesse am CPSSE, dem ersten Qualifikationszertifikat für sichere Softwareentwicklung. Nächster Termin: 16. bis 19.03.2010.

Details zu allen Seminaren finden Sie auf unseren Webseiten; die Jahresübersicht 2010 erleichtert die Planung. Wir freuen uns auf Ihre Anmeldung.

Wunsch und Wirklichkeit

Gelegentlich werden auch in der IT-Sicherheit Wünsche wahr. Das zeigt die Awareness-Kampagne „SecurityCup 2009", in der es die FIDUCIA zusammen mit der Agentur DauthKaun geschafft hat, ihre Mitarbeiter wirksam zum Schutz von Informationen, Daten und Know-How zu sensibilisieren. Am 18.02.2010 stellen Sven Kaun (DauthKaun) und Lutz Bleyer (FIDUCIA) die Kampagne auf der ersten Veranstaltung der KA-IT-Si im neuen Jahr vor – wir freuen uns auf Ihre Teilnahme (Beginn wie immer um 18 Uhr im Schlosshotel Karlsruhe, mit anschließendem Buffet-Networking).

Übrigens: Die Unterlagen des letzten diesjährigen KA-IT-Si-Events vom 26.11.2009 zum Thema Datenrettung finden Sie zum Download auf den KA-IT-Si-Seiten.

Feiertagslektüre

Seit Online-Banking in den Fokus von Internet-Angriffen gerückt ist und sowohl Phishing-E-Mails als auch spezialisierte Banking-Trojaner die Vermögen deutscher Bankkunden bedrohen, haben Banken neue Protokollvarianten eingeführt – von iTAN über mTAN bis zum TAN-Generator. Nun hat Hans-Joachim Knobloch zwei grundlegende Verfahren einer Sicherheitsanalyse mittels BAN-Logik unterzogen und die Ergebnisse in Ausgabe 12/2009 der Fachzeitschrift „Datenschutz und Datensicherheit (DuD)" veröffentlicht.

Ebenfalls in der DuD erscheint im Januar 2010 in der Rubrik „Best Practice" eine Empfehlung von Kai Jendrian zur Erweiterung des Web-Browsers Firefox um Add-ons, die die Sicherheit und den Schutz der persönlichen Daten beim Surfen signifikant erhöhen. Da ist möglicherweise der eine oder andere wertvolle Tipp dabei, um an den Feiertagen den Schutz des neuen PCs wirksam zu verbessern.

Weitere Publikationen von Secorvo finden Sie in der Übersicht auf unserer Webseite.

Veranstaltungshinweise

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

Dezember 2009	
06.-10.12.	15th ASIACRYPT 2009 (IACR, Tokio/JP)
27.-30.12.	26th Chaos Communication Congress (CCC, Berlin)
Januar 2010	
19.-21.01.	Omnicard 2010 (inTIME, Berlin)
Februar 2010	
02.-03.02.	20. SIT-SmartCard-Workshop (Fraunhofer-Institut SIT, Darmstadt)
03.-04.02.	ESSoS (DistriNet Research Group, Pisa/I)
05.-07.02.	ShmooCon 2010 (Shmoo Group, Washington/USA)
09.-10.02.	17. DFN Workshop – Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
22.-26.02.	TISP-Schulung (Secorvo College)
März 2010	
16.-19.03.	ISSECO Certified Professional for Secure Software Engineering - CPSSE (Secorvo College)
23.-25.03.	Sicherheitsmanagement heute (Secorvo College)

Fundsache

In einem 123seitigen Report vom 20.11.2009 hat die European Network and Information Security Agency (ENISA) die Nutzung von Cloud-Computing einer Risiko-Analyse unterzogen. Acht von 35 betrachteten Risiken ordnet sie dabei der Risikoklasse „High“ zu. Daraus leitet sie zahlreiche Empfehlungen für die Nutzung von Cloud-Computing ab.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch, Jochen Schlichting, Jörg Völker

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

secorvo
security consulting

Secorvo Security News

Dezember 2009

Endogene Bedarfsexpansion

Wenn Sie Kinder haben, kennen Sie das Phänomen. Besonders gut ist es jährlich vor dem Weihnachtsbaum zu beobachten: Ganz gleich, wie viele Pakete Ihre Kinder ausgepackt haben – nach dem letzten schweifen die Blicke sehnsüchtig suchend bis zur enttäuschenden Einsicht durch den Raum, dass es tatsächlich das letzte war.

Vielleicht ist diese „Gier nach mehr" ja nicht nur die natürliche Erklärung für die Faszination des österlichen Eiersuchens, sondern der wahre Antrieb hinter dem Streben nach immer mehr Kontrolldaten – wie die Ausweitung der Videoüberwachung im öffentlichen Personenverkehr (Verkehrsministerkonferenz vom 04.12.2009) oder die anlassunabhängige des Individualverkehrs, die erst das Bundesverfassungsgericht stoppen konnte (Beschluss vom 11.08.2009). Auch die Zahl der Telefonüberwachungen, bereits 2007 weltweit auf historisch einmalig hohem Niveau, stieg 2008 erneut – um 11% auf 16.463 Maßnahmen. Dass daher die Vorratsdatenspeicherung von Telekommunikationsdaten, die am 15.12.2009 vom Bundesverfassungsgericht verhandelt wurde, keine gute Idee ist, zeigen auch die Versuche der Strafverfolgungsbehörden, trotz expliziten Verbots im § 7 Autobahnbaumtgesetz („Eine Übermittlung, Nutzung oder Beschlagnahme dieser Daten nach anderen Rechtsvorschriften ist unzulässig") auf die vom Betreiber Toll Collect an Maut-Kontrollbrücken erhobenen Daten zuzugreifen, Stellungnahmen wie die der Musikindustrie und die Feststellungen des Bundesdatenschutzbeauftragten, dass TK-Unternehmen weit mehr speichern als erlaubt: Einst auf schwere Straftaten beschränkt, droht der Eingriff ins Fernmeldegeheimnis zum Standard-Ermittlungsinstrument zu werden. Fehlen noch die Pflicht zu „intelligenten Stromzählern" und die Abschaffung des Bargelds: Präziser lassen sich Lebensgewohnheiten kaum bestimmen.

„Die Freiheit stirbt scheibchenweise": Worte des Jahres 2001 in „Die ZEIT", von Sabine Leutheusser-Schnarrenberger. Seit dem 28.10. 2009 ist sie Bundesjustizministerin. Die Hoffnung stirbt zuletzt.

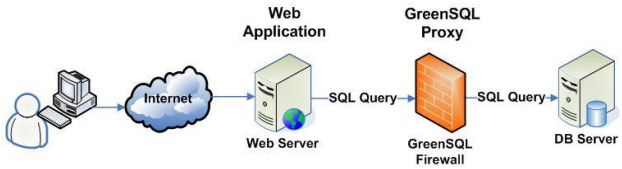
Inhalt

secorvo
security consulting

Security News

SQL-Firewall

Am 02.12.2009 wurde Version 1.2 der OpenSource SQL-Firewall GreenSQL freigegeben. Die Idee hinter diesem speziellen Application Level Gateway ist, Zugriffe von (Web-) Applikationen auf dahinter liegende Datenbanken zentral und unabhängig von der Anwendung filtern zu können.



(Quelle: greensql.net)

Audits von Web-Applikationen zeigen, dass sehr viele Web-Anwendungen keine ausreichende Eingabevalidierung vornehmen und so anfällig für SQL-Injection sind. Zudem besteht immer das Risiko, dass ein Webserver über Schwachstellen der Plattform, des Webservers selbst oder der Anwendung (PHP, .net, J2EE, Ruby etc.) kompromittiert wird. In diesen Fällen kann auf die dahinter liegende Datenbank, selbst wenn sie in einer separaten Netzwerkzone betrieben wird, unberechtigt zugegriffen werden.

Bei einer Kontrolle der Zugriffe mittels GreenSQL ist es beispielsweise möglich zu definieren, auf welche Tabellen und Datenbestände zugegriffen werden darf, oder ob Daten nur gelesen, aber nicht geschrieben werden dürfen. Einen ersten Eindruck zu den Konfigurationsmöglichkeiten kann man sich in einer Live-Demo verschaffen. Derzeit werden MySQL und PostgreSQL unterstützt.

Nichts gelernt ...

... aus den Datenschutzskandalen der jüngsten Zeit hatten offenbar die Verantwortlichen des Sozialen Schülernetzwerks haefft.de. Am 04.12.2009 deckte der Chaos Computer Club (CCC) Scheunentor große Sicherheitslöcher bei dem Portal auf. Erschreckend in diesem konkreten Fall: die schlechten Implementierungen von Sicherheitsmaßnahmen zum Schutz intimer personenbezogener Daten von Kindern.

Nachdem in einer inzwischen gelöschten Pressemitteilung der Fall von den Verantwortlichen herunter gespielt worden war, eskalierte der Vorgang. Nun ist das Portal offline – der Betreiber entschuldigt sich in einer neuen Stellungnahme für die Fehler und erläutert das nun geplante Vorgehen.

Der Vorfall ruft drei Grundregeln ins Gedächtnis:

1. Sorgen Sie *als Entwickler* von Web-Anwendungen, die personenbezogene Daten speichern und verarbeiten, für korrekte Implementierung, sicheren Betrieb und wirksame Schutzmaßahmen.

2. Achten Sie *als Betreiber* bei Sicherheitsvorfällen auf eine angemessene Krisenkommunikation.

3. Bedenken Sie *als Betroffener* genau, welche Daten Sie über sich wo preisgeben – und sprechen Sie mit Ihren Kindern über das Thema.

Forensik-Folklore

Zu dem bereits am 15.04.2009 veröffentlichten 2009 Data Breach Investigations Report des Sicherheitsdienstleisters Verizon Business (vgl. SSN 04/2009) erschien am 09.12.2009 – als Nachschlag – ein Supplemental Report, der die Bedrohung durch die 15 häufigsten Angriffsarten, von Keyloggern über Social Engineering bis hin zum Durchforsten des RAM-Speichers in Kassensystemen und zum „*ishing“, ausführlicher analysiert und jeweils ein anonymisiertes Fallbeispiel schildert.

Bei einigen dieser anekdotischen Schwachstellenbeschreibungen lässt sich ein Schmunzeln kaum unterdrücken (wie beim manuellen Ersetzen von „validUser=0“ durch „...=1“ in einer Web-Anwendung, um die Anmeldung einzusparen), bei anderen beschleicht einen das ungute Gefühl, möglicherweise selbst nicht ausreichend gegen ähnliche Angriffe gefeit zu sein.

Schöner neuer Personalausweis

Nachdem am 10.11.2009 bekannt geworden war, dass das BMI ein Konsortium unter Siemens-Führung mit der Bereitstellung der Middleware für den neuen elektronischen Personalausweis, den „Bürger-Client“ beauftragt hatte, meldete die mtG media transfer AG am 30.11.2009, dass sie den Zuschlag für den Aufbau der Root CAs für die Nutzung und den Zugriff auf die Daten des künftigen Personalausweises erhalten habe.

Bemerkenswert: Diese Root CAs werden beim BSI in Anlehnung an die bestehende Verwaltungs-PKI (die im gleichen Zuge runderneuert wird) aufgebaut. Hingegen bleiben die Zertifizierungsdiensteanbeiter für die elektronische Signatur und deren bei der BNetzA betriebene Root CA ein optionales Anhängsel der Ausweiskarte. Darf das als späte Einsicht in die Erfolglosigkeit überregulierter Signatur-Infrastrukturen gewertet werden?

ISO 2700x mit x=4

Mit Veröffentlichungsdatum vom 15.12.2009 ist ein neuer Standard in der ISO-27000er-Reihe zur Messung der Informationssicherheit erhältlich – ISO/IEC 27004:2009 „Information technology – Security

techniques – Information security management – Measurement".

Darin wird endlich verbindlich geregelt, was unter Messungen und Bewertungen im Rahmen eines Informationssicherheitsmanagements nach ISO 27001 zu verstehen ist. Neben den Erklärungen zu einem sinnvollen Vorgehen bei der Entwicklung von Messungen finden sich auch Hinweise zur Verantwortung des Managements sowie zu Durchführung und Dokumentation von Messungen.

Einen großen Teil der über 50 Seiten des Standards füllen praktische Beispiele und eine Dokumentationsvorlage im Anhang. Damit wird dem Praktiker eine nützliche Arbeitshilfe zur Verfügung gestellt. Der neue Standard ergänzt das Dokument „BIP 0074 – Measuring the effectiveness of your ISMS implementations" nun verbindlich.

Übrigens: Seit etwa sechs Monaten ist das Rahmenwerk – der Standard ISO 27000 – auch Lizenzkosten frei verfügbar.

Feiertagslektüre

Wer schon immer wissen wollte, wie es wäre, wenn Stanley Kubrick eine Anfängervorlesung in IT-Sicherheit gegeben hätte, wird wohl mit Vergnügen den am 15.12.2009 erschienenen Bericht von Matt Blaze über seinen Besuch in einem zum Museum umgewandelten Interkontinentalraketen-Silo lesen. Darin analysiert der bekannte Kryptologe und Autor des Cryptographic Filesystem CFS die Sicherheitsmaßnahmen, mit denen im Kalten Krieg die ins Extrem getriebenen, einander widerstrebenden Anforderungen nach Hochverfügbarkeit bei gleichzeitiger strikter Zugriffskontrolle realisiert wurden, wie Vier-Augen-Prinzip, Physische Zutrittskontrollen oder „Separation of Duties".

Secorvo News

Secorvo College aktuell

Auch im neuen Jahr bieten wir Ihnen im Secorvo College wieder zahlreiche Gelegenheiten, Ihr Wissen zu zertifizieren. Neben der etablierten TISP-Schulung, unter anderem vom 22. bis 26.02.2010, können Sie sich mit dem CPSSE als Experte im Bereich der sicheren Softwareentwicklung zertifizieren. Die erste Schulung im neuen Jahr findet vom 16. bis 18.03.2010 statt. Hintergründe zur Zielsetzung und Entstehung des Zertifikats liefern zwei kürzlich erschienene Aufsätze von Petra Barzin, einer der Initiatorinnen des CPSSE: „A New Qualification to Guarantee Secure Software Engineering Skills" (in: ENISA Quarterly Review, Vol. 5 No. 3, September 2009, S. 18) und „International Secure Software Engineering Council (ISSECO)" (in: SecurityActs No. 1, Oktober 2009, S. 14 f.).

Unsere Grundlagenseminare zu den Themen Sicherheitsmanagement, PKI und IT-Sicherheitsaudit finden Sie ebenfalls im Programm 2010, nicht zuletzt dank der durchweg positiven Rückmeldungen der Teilnehmer. Eine aktuelle Übersicht finden Sie in unserem Seminarkalender 2010. Melden Sie sich an, wir freuen uns auf Sie!

Wege zum Ruhm

Die KA-IT-Si verabschiedet sich nach sechs Events zu spannenden Themen der IT-Sicherheit aus dem Jahr 2009 in eine kurze Verschnaufpause. Am 18.02.2010 stellen Sven Kaun und Lutz Bleyer die Awareness-Kampagne „Security Cup 2009" der FIDUCIA IT AG vor – und sich beim anschließenden Buffet-Net(t)working der Diskussion. Um Anmeldung wird gebeten.

A propos Awareness: Die KA-IT-Si freut sich über jeden weiteren Partner, der die Arbeit der Initiative unterstützt – den Wissenstransfer zur IT-Sicherheit auf den Fachevents, den regen Erfahrungsaustausch unter IT-Sicherheitsverantwortlichen und die Sensibilisierung insbesondere mittelständischer Unternehmen für die Bedeutung der Informationssicherheit. Nähere Informationen zur KA-IT-Si-Partnerschaft finden Sie auf der KA-IT-Si-Webseite.

Teamverstärkung

Seit dem 01.08.2009 verstärkt Dr. Safuat Hamdy das Secorvo-Team – den regelmäßigen und aufmerksamen Lesern bereits vom Editorial der SSN 10/2009 bekannt.

Im kommenden Jahr soll unser Team weiter wachsen: Wir suchen mehrere Beraterinnen oder Berater im Gebiet Datenschutz und IT-Sicherheit mit Berufserfahrung für zahlreiche herausfordernde Projekte – und freuen uns über Empfehlungen und Bewerbungen an personal@secorvo.de.

Veranstaltungshinweise

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

Dezember 2009	
27.-30.12.	26th Chaos Communication Congress (CCC, Berlin)
Januar 2010	
19.-21.01.	Omnicard 2010 (inTIME, Berlin)
Februar 2010	
02.-03.02.	20. SIT-SmartCard-Workshop (Fraunhofer-Institut SIT, Darmstadt)
03.-04.02.	ESSoS (DistriNet Research Group, Pisa/I)
05.-07.02.	ShmooCon 2010 (Shmoo Group, Washington/USA)
09.-10.02.	17. DFN Workshop – Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
15.-18.02.	SecSE 2010: Fourth International Workshop on Secure Software Engineering (SINTEF, Krakau/PL)
22.-26.02.	TISP-Schulung (Secorvo College)
März 2010	
16.-19.03.	ISSECO Certified Professional for Secure Software Engineering – CPSSE (Secorvo College)
23.-25.03.	Sicherheitsmanagement heute (Secorvo College)

Fundsache

Wer noch ein Weihnachtsgeschenk oder Lesestoff für die Feiertage sucht, dem sei ein Blick in die Bücherliste von Tobias Schrödel empfohlen. Fast 500 Werke rund um das Thema Kryptographie hat er zusammengetragen. Allerdings sind einige nicht mehr käuflich zu erwerben, so wie Giovanni Battista Bellasos „Novi et singolari modi di cifrare“ (1555).

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch

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