secorvo
security consulting

Secorvo Security News

August 2010

Editorial: Todesmut

Urlaube überraschen gelegentlich mit neuen Erfahrungen. So fand ich mich kürzlich unversehens auf einem Baum wieder: unter mir zwölf Meter gähnendes Nichts, vor mir zwei nicht einmal fingerdicke, zehn Meter lange Drahtschnürchen zum nächsten Stamm, und dort, auf einer weniger als 1 qm großen hölzernen Plattform, meine feixenden Söhne. Vor meinem inneren Auge spulten sich, von inbrünstiger Reue begleitet, zwar nicht mein bisheriges Leben, aber doch die Ereignisse des vergangenen Abends ab: In geradezu jugendlichem Leichtsinn hatte ich meinen Söhnen zugesagt, mit ihnen einen nahen Hochseilgarten zu besuchen. Nun ja, welcher Vater mag sich schon von seinen Halbwüchsigen als Hasenfuß verlachen lassen... Jetzt aber gab es kein zurück mehr, und mit zittrigen Fingern klinkte ich meine beiden Karabiner ins Seil.

Als ich nach langen 60 Minuten endlich wieder festen Boden unter den Füßen hatte und mein Hirn wieder an etwas anderes als „Todesmut" denken konnte, machte ich eine überraschende Beobachtung: Kein einziger Besucher rutschte von einem der an Seilen baumelnden Balken, federnden Feuerwehrschläuche oder schaukelnden Saftkisten, über die man sich von Baum zu Baum hangeln musste. Und schon beim zweiten Parcours, auf den mich meine Söhne zwangen, wuchs meine Zuversicht, die andere Seite wohlbehalten zu erreichen, und gewann schließlich sogar die Oberhand.

Bei nüchterner Betrachtung war das kein Wunder, denn die soliden Sicherungen begrenzen das tatsächliche Risiko auf eine Falltiefe von 20 cm (und lachende Söhne).

Kaum zurück aus dem Urlaub konfrontierte mich das echte Leben mit einem völligen Kontrasterlebnis: ein CIO, der die Risiken unverschlüsselter mobiler Geräte mit einem „Bei uns ist noch nie etwas passiert" beiseite wischte. Da beschlich mich die ketzerische Idee, ihn in den Hochseilgarten einzuladen. Ob er sich dort oben wohl auch ausklinken würde?

Inhalt

secorvo
security consulting

Security News

Rechtswidrige Webseitenanalyse

Die Aufsichtsbehörde Baden-Württembergs für den Datenschutz im nicht-öffentlichen Bereich hat auf der Grundlage des Entschlusses des Düsseldorfer Kreises vom 26./27.11.2009 am 01.07.2010 eigene Hinweise zum Einsatz von Web-Analysediensten veröffentlicht. Insbesondere der Einsatz von Google Analytics wird als rechtswidrig eingestuft.

Die Datenschutzaufsichtbehörden betrachten IP-Adressen als grundsätzlich personenbezogene Daten. Daher erfordert ihre Erhebung und Verarbeitung zu Analysezwecken gemäß §§ 12, 15 TMG eine (praktisch nicht realisierbare) Einwilligung des Website-Nutzers. Weitere Gründe für die Einstufung liegen in der Datenübertragung in das außereuropäische Ausland, den Nutzungsbedingungen, in denen sich Google die Verarbeitung der Daten auch zu eigenen Zwecken vorbehält, die unzureichende Widerspruchsmöglichkeit und die ungewisse Löschsituation bei Vertragsende.

Fehl geht das Innenministerium allerdings, wenn es eine Auftragsdatenverarbeitung annimmt: Hierzu fehlen Kontrollmöglichkeiten und Weisungsrechte der Verwender sowie ein entsprechender Vertrag nach § 11 BDSG. Vor allem aber beschränkt sich Google nicht auf ein auftragsgebundenes Verarbeiten, sondern handelt eigenständig.

Damit riskieren die Nutzer von Google Analytics, die sich über Webseiten wie OnTraxx leicht identifizieren lassen, Bußgelder nach § 16 TMG. Zwar bietet Google in Reaktion auf den Düsseldorfer Kreis bereits Zusatzcode zur Verkürzung von IP-Adressen. Aber auch damit werden die Probleme des Widerspruchs gegen eine Profilbildung und der Auslandsübertragung nicht gelöst. Die Widerspruchslösung von Google – Sperrung von Cockies – ist unzureichend. In Baden-Württemberg sind nun verstärkte Kontrollen angekündigt; weitere Bundesländer dürften dem Beispiel folgen.

iPhone Jailbreak via Safari

Seit längerem ist bekannt, dass auch für das iPhone 4 und iOS 4.0.1 sowohl ein Jailbreak als auch ein Unlock möglich sein sollen (siehe SSN 11/2009). Dennoch war die Überraschung groß, als am 02.08.2010 das Dev Team den Jailbreak für das iPhone 4 veröffentlichte. So stand der Jailbreak nun nicht nur für alle iOS-Geräte von Apple (iPod, iPad, iPhone) und alle iOS-Versionen zur Verfügung, sondern nutzte eine Lücke im PDF-Reader des mobilen Safari-Browsers aus, der es PDF-Dateien erlaubt, unsignierten Code auf dem iPhone auszuführen.

Diese Lücke kann natürlich auch durch andere Angreifer ausgenutzt werden, um beliebige Anwendungen auf dem Gerät zu installieren. Einen wirksamen Schutz gegen diese Schwachstelle bietet derzeit nur das Update für iOS 4.0.2 vom 11.08.2010. Auf Geräten, die bereits einen Jailbreak durchgeführt haben, lässt sich ein Tool installieren, dass vor dem Öffnen von PDFs warnt. Ansonsten bleibt nur die Empfehlung, auf dem iPhone vorläufig lieber keine PDF-Dateien unbekannter oder zweifelhafter Herkunft zu öffnen.

RainbowCrack 1.5

Fast exakt ein Jahr nach Veröffentlichung der Version 1.4 (siehe SSN 08/2009) stellte das Projekt RainbowCrack am 26.08.2010 mit Version 1.5 eine für 64bit-Betriebssysteme optimierte Fassung ihres Passwort-Crackers zum Download bereit. Mit über 320 Milliarden (MD5-) Hashwerten pro Sekunde erreicht diese Version auf der Referenzhardware mehr als die vierfache Geschwindigkeit der Vorversion – selbst alpha-numerische 10-Zeichen-Passwörter lassen sich damit auf einem Standard-PC mit schneller Grafikkarte in wenigen Tagen finden.

I Can Stalk You...

Erst Mitte Februar hatte der Dienst „PleaseRobMe“ für Aufregung gesorgt, der aktuelle Twitter-Nachrichten anzeigte, in denen die Autoren ihren Aufenthaltsort fern von zu Hause preisgaben (siehe SSN 02/2010). Offenbar genügte das nicht, um Millionen naiver Tweeter die Gefährlichkeit ihrer öffentlichen Mitteilungsfreude vor Augen zu führen. Daher startete Myhemic Labs mit „ICanStalkU“ am 05.05.2010 eine Webseite, die den aktuellen Aufenthaltsort aus den Metadaten von auf Twitter veröffentlichten SmartPhone-Fotos gewinnt – die inzwischen häufig Geodaten enthalten.

Dabei ist Abhilfe simpel: Wie man iPhone, Android und Blackberry dazu überredet, keine Geodaten zu speichern, erläutern die Autoren bereitwillig. Wer eine solche Vorsicht pathologisch (oder zumindest übertrieben) findet, dem sei der Aufsatz von Blumberg und Eckersley über Locational Privacy vom August 2009 dringend zur Lektüre empfohlen.

Cryptool 1.4.30

Am 04.08.2010 wurde Version 1.4.30 der Lernsoftware Cryptool veröffentlicht. Wir haben dies zum Anlass genommen, die Software unter didaktischen Gesichtspunkten unter die Lupe zu nehmen. Nach der Installation stellt die Anwendung ein Hauptfenster zur Verfügung, innerhalb dessen allerlei Experimente angestellt werden können, d. h. der Anwender kann eine große Vielfalt von kryptografischen Verfahren auf beliebige Textdateien anwen-

den lassen, etwa zur Verschlüsselung oder zur Signaturerzeugung. Der Punkt, der Cryptool dabei so interessant macht, ist die Visualisierung der Verfahren. Die ist allerdings unterschiedlich gelungen ausgefallen; bei manchen Verfahren werden nur Zwischenergebnisse angezeigt, bei anderen wird der Anwender im Detail durch den Algorithmus geführt. Andere Experimentierfelder ergeben sich bei der Analyse klassischer Kryptoverfahren oder bei der Durchführung zahlentheoretischer Experimente.

Da es viele Mitwirkende an dem Projekt gibt, ist das Erscheinungsbild der Software insgesamt recht inhomogen. Das ist kein Schaden; etwas störend fielen aber unterschiedliche didaktische Herangehensweisen auf. So kommt die Zahlentheorie mit dem Charme einer Vorlesung daher, während etwa die Demonstration des AES-Verfahrens sehr lebendig und greifbar wirkt. Für zukünftige Versionen wäre es schön, wenn der didaktische Ansatz sowie die Visualisierung an verschiedenen Stellen poliert und vereinheitlicht würde. Auch wenn Cryptool aus einem Anwender keinen Kryptologen macht, hat es zweifellos einen hohen Lernwert – mit Spaßfaktor.

EU-Verfahrensverzeichnis

Die EU-Kommission hat am 26.07.2010 einen „Überblick über das Informationsmanagement im Bereich Freiheit, Sicherheit und Recht“ veröffentlicht. Das Papier soll den EU-Bürgern Transparenz darüber verschaffen, wer auf europäischer Ebene welche Daten zu welchem Zweck speichert und welche Stellen Zugriff erhalten. Erläutert werden 18 bestehende, in Umsetzung befindliche oder geplante Datensammlungen vom Schengener Informationssystem (SIS) über die Vorratsdatenspeicherungsrichtlinie bis zu dem geplanten Passenger Name Records (PNR) System für Europa.

Im Stil eines Verfahrensverzeichnisses werden zu jedem Instrument Hintergrund, Zweck, zentraler oder dezentraler Aufbau, die Art der gespeicherten personenbezogenen Daten, die Zugriffsberechtigungen, Regelungen zum Datenschutz, Speicherdauer, Umsetzungsstand und Überprüfungsverfahren angegeben. Zu einigen Datensammlungen, darunter zur Vorratsdatenspeicherungsrichtlinie, zur schwedischen Initiative zum Austausch von Ermittlungsdaten und zum Prüm-Beschluss (grenzüberschreitender DNA-Abgleich) werden Beispiele erfolgreicher Straftataufklärungen oder Statistiken angeführt. Zur Vorratsdatenspeicherung fehlt eine Erfolgsstatistik; es werden lediglich zwei Beispiele aufgeklärter Tötungsdelikte, eine Einbruchsserie und eine bandenmäßige Raubserie benannt.

Die Mitteilung ist gerade auch im Zusammenhang der Rechtsprechung des Bundesverfassungsgerichts zur TK-Vorratsdatenspeicherung zu begrüßen, die angesichts der sehr umfassenden Speicherung in diesem Bereich zur Zurückhaltung in weiteren Bereichen mahnt. Sie könnte Ausgangspunkt für die überfällige Diskussion sein, wie viel Kontrolle wir uns angesichts der tatsächlichen Aufklärungserfolge leisten wollen.

Secorvo News

Secorvo College aktuell

Sichern Sie sich einen Platz auf einem unserer Herbst-Seminare. Los geht es im September mit der Möglichkeit, Ihr Fachwissen durch das anerkannte T.I.S.P.-Zertifikat belegen zu lassen: Vom 20. bis 24.09.2010 findet die nächste T.I.S.P.-Schulung mit anschließender Zertifikatsprüfung statt. Für den „Doppelpack Grundlagen“ empfehlen wir eine baldige Anmeldung: Sicherheitsmanagement heute – Prozesse, Steuerung, Organisation vom 05. bis 07.10.2010 und der „Klassiker“ IT-Sicherheit heute vom 26. bis 28.10.2010 beleuchten neben den aktuellen Standards die wichtigsten Trends im IT-Sicherheitsbereich.

Xdr3$gFa*9z

Eine zentrale Verschlüsselungslösung für die größte Bank im Südwesten Deutschlands – diese Aufgabe haben die IT-Security-Experten Joachim Seeger und Volker Kölz von der Landesbank Baden-Württemberg (LBBW) gemeistert. Die Anforderungen umfassten nicht nur technische Herausforderungen: So sollte die Lösung für den Anwender so unauffällig wie möglich sein, weitestgehend automatisiert laufen und keinen Einfluss auf die Betriebsführung haben. Schließlich mussten die Daten bei einer Störung einfach wiederherstellbar sein. Wie die Experten der LBBW die Datei- und Ordnerverschlüsselung und die Verschlüsselung der Endgeräte heute organisieren, verraten sie am **23.09.2010** bei der nächsten Veranstaltung der KA-IT-Si im Schlosshotel Karlsruhe (Anmeldung).

Security Awareness 7.0

Auf dem siebten „Security Awareness Symposium“ am **28.–29.09.2010** in Ettlingen, das Secorvo zusammen mit dem Berliner eLearning-Spezialisten digital spirit und der Karlsruher Agentur DauthKaun initiierte, erwarten Sie wieder spannende Erfahrungsberichte von Projektleitern zahlreicher Awareness-Kampagnen, die ihre Ideen, Erfolge und „Lessons Learned“ präsentieren – ein Treffen, das Sie sich nicht entgehen lassen sollten, wenn die Sensibilisierung Ihrer Kollegen für IT-Sicherheit oder Datenschutz auf Ihrer Agenda steht (Anmeldung).

Veranstaltungshinweise

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

September 2010	
07.-10.09.	OWASP AppSec US (Irvine/US)
20.-24.09.	TISP-Schulung (Secorvo College)
21.-22.09.	D·A·CH Security (GI/OCG/BITKOM/SI/TeleTrusT, Wien)
28.-29.09.	7. Security Awareness Symposium (Secorvo, Ettlingen)
28.-30.09.	Forensik – Verfahren, Tools, Praxiserfahrung (Secorvo College)
Oktober 2010	
04.-07.10.	ISSE 2010 (Teletrust, Berlin)
04.-07.10.	Sicherheitsmanagement heute (Secorvo College)
19.-21.10.	ISSECO Certified Professional for Secure Software Engineering (Secorvo College)
19.-21.10.	it-sa (SecuMedia Verlag, Nürnberg)
21.10.	it-sa Datenschutztag 2010 (Computas, Nürnberg)
November 2010	
18.-19.11.	34. DAFTA (GDD e.V., Köln)

Fundsache

Der jüngste IBM X-Force-Halbjahresbericht vom 24.08.2010 belegt einige beunruhigende Tendenzen: Ein deutlicher Anstieg von pdf-Angriffen, die Zunahme von mit Schadsoftware „versetzten" Webseiten und die meisten innerhalb von sechs Monaten gezählten Sicherheitsschwachstellen. Für Interessierte bietet der 112seitige Bericht zahlreiche wertvolle Detailanalysen aktueller Bedrohungen.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Michael Knopp, 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