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