secorvo
security consulting

Secorvo Security News

Februar 2011

Falsche Freunde

Im Englischen nennt man sie „false friends“. Wörter einer Fremdsprache, die einem Wort der Muttersprache phonetisch oder orthografisch ähneln, aber eine gänzlich andere Bedeutung besitzen, und so zu falschen Übersetzungen verleiten. So z. B. *become* (nicht bekommen, sondern werden), *sensible* (nicht sensibel, sondern fühlbar) oder *pathetic* (nicht pathetisch, sondern erbärmlich).

Ein ähnliches Phänomen lässt sich in der Informationssicherheit beobachten. Damit sind weniger die verbreiteten begrifflichen Unschärfen („persönliche Daten“) oder unterschiedlichen Definitionen von Sicherheit (*safety* versus *security*) gemeint, die gelegentlich zu Missverständnissen führen. Weit schlimmer sind Schutzmaßnahmen, die manchmal sogar Profis ein „Sicherheitsgefühl“ vermitteln – aber im Kern teure potemkinsche Dörfer sind.

So ist es heute in größeren Unternehmen üblich, den Gebäudezugang durch Betriebsausweise mit Foto zu kontrollieren. Tatsächlich werden die Fotos jedoch selten aktualisiert und oft sogar bei der Neuausgabe von Ausweisen wieder verwendet. Konsequenterweise überprüft das Sicherheitspersonal Ausweisfotos gar nicht erst auf Übereinstimmung mit dem Gesicht des Trägers. Zumeist genügt daher ein selbst gebastelter Pappausweis mit beliebigem Passfoto, um Zugang zu erhalten. Verhindert eine elektronische Schranke den unberechtigten Zugang, hilft ein großer Trolley (oder Rollstuhl), damit der „barrierefreie Zugang“ bereitwillig entriegelt wird.

Am Rechnerarbeitsplatz finden sich dann weitere Angriffserleichterungen: Die (ohnehin oft mickrige) Passwortlänge wird durch die Erzwingung regelmäßiger Wechsel effektiv weiter verringert – schließlich werden die letzten Stellen als Folgezähler benötigt (was den Zweck des Passwortwechsels konterkariert). Nicht selten gelingt eine Passwortrücksetzung durch Anruf beim Helpdesk – häufig wird dies durch keine wirksame Anruferauthentisierung verhindert.

Es wäre nicht nur billiger, auf derartigen Schein-Schutz zu verzichten. Denn die Illusion von Sicherheit reduziert die Wachsamkeit.

Inhalt

Security News

Vorgedacht

Im vergangenen Jahr war es der Datenschutz, der Bewegung in das Thema Smart Metering brachte - nun rückt auch die Datensicherheit in den Fokus. Am 28.01.2011 stellte das BSI einen ersten Entwurf eines Schutzprofils für die Kommunikationseinheit des Messsystems vor, das auch auf dem Smart Grid Symposium in Ettlingen diskutiert wurde. Die Planung sieht vor, das Schutzprofil noch im Jahr 2011 fertig zu stellen.

Da Smart Grids in den USA vor allem eine höhere Robustheit und Netzverfügbarkeit bewirken sollen, genießen Sicherheitsfragen in der amerikanischen Diskussion einen sehr hohen Stellenwert. So hat das NIST bereits im September 2010 600seitige „Guidelines for Smart Grid Cyber Security" (aktuelle Fassung vom 25.10.2010) veröffentlicht. Es wäre zu begrüßen, wenn sich die darin enthaltenen Überlegungen und Erkenntnisse auch im deutschen Schutzprofil wiederfänden.

Nachgedacht

Der Bundesgerichtshof hat am 13.01.2011 über die derzeitige Praxis der Access-Provider zur ca. einwöchigen benutzerbezogenen Speicherung der IP-Adresszuordnung (Urteilsbegründung vom 08.02.2011) entschieden. Nach dem Telekommunikationsgesetz (TKG) bestehen zwei Rechtfertigungsmöglichkeiten: die Speicherung zu Abrechnungszwecken (§ 97 Abs. 1 S. 1, Abs. 2 Nr. 1 TKG) und die Speicherung zur Störungsanalyse und -beseitigung (§ 100 Abs. 1 TKG). Der BGH hat nun deutlich gemacht, dass die Geeignetheit und Erforderlichkeit der Speicherung zu beiden Zwecken detailliert unter Beweis zu stellen ist. Die Instanzgerichte hatten die Erforderlichkeit und mögliche Alternativen gar nicht erst geprüft und eine diesbezügliche Beweislast des beklagten Telekommunikationsunternehmens verneint.

Tatsächlich bestehen begründete Zweifel, denn auch einzeln abzurechnende Dienste innerhalb einer Flatrate rechtfertigen keine generelle Speicherung zu Abrechnungszwecken. Die Begründungen für eine Speicherung zur Störungsbeseitigung beziehen sich bislang überwiegend auf die Störerermittlung bei SPAM- oder DoS-Attacken – dabei ist eine Speicherung jedoch nur für eine anschließende Rechtsverfolgung erforderlich. Ob diese von § 100 Abs. 1 TKG erfasst wird, ist äußerst fraglich. Nun ist das OLG Frankfurt am Zug. Die Prüfanforderungen zur Begründung von IP-Adressspeicherungen sind mit dem Urteil jedoch deutlich schärfer geworden.

Zu kurz gedacht

Die am 26.01.2011 von Alex Rice im Facebook-Blog vorgestellte Reaktion auf Session-Hijacking-Angriffe, die mit Tools wie Firesheep (SSN 10/2010) einfach durchzuführen sind, erweitert das Benutzerprofil um die Option „Facebook mit einer sicheren Verbindung (https) durchstöbern, wenn möglich". Nach Aktivierung werden dann nicht nur die Login-Daten mit SSL geschützt an Facebook übertragen, sondern alle Daten, inklusive des Session-Cookie.

So weit, so gut. Was is aber mit „wenn möglich" gemeint? Da nicht alle Facebook-Apps den Umgang mit gesicherten Verbindungen beherrschen, erhält ein Benutzer beim Zugriff auf eine solche App den Warnhinweis: „Es tut uns leid, aber wir können diese Inhalte nicht anzeigen, während du Facebook über eine sichere Verbindung (https) benutzt. Um diese Anwendung nutzen zu können, musst du zu einer regulären Verbindung (http) wechseln." Das wäre verschmerzbar – wenn das Wechseln auf eine ungeschützte Verbindung temporär erfolgen würde. Tatsächlich schaltet Facebook in diesem Fall die Option zum sicheren Surfen dauerhaft ab.

Umgedacht

Mit der verantwortungsvollen Veröffentlichung von Schwachstellen (Stichwort „responsible disclosure") beschäftigt sich die vom Intrusion Detection Hersteller Tipping Point (HP) betriebene Zero Day Initiative (ZDI) seit ihrer Gründung. Die Kernidee ist, dass festgestellte Schwachstellen zuerst dem Hersteller gemeldet werden, um diesem Zeit zu geben, Gegenmaßnahmen zu ergreifen oder einen Patch bereit zu stellen. Danach erst wird die Schwachstelle öffentlich gemacht. Vorausgesetzt wird dabei, dass die betroffenen Hersteller ein Interesse daran haben, gefundene Schwachstellen umgehend zu beheben. Dass dies nicht immer der Fall ist, zeigt eine am 06.02.2011 von Sami Koivu veröffentlichte Schwachstelle, die er bereits 2008 an Sun gemeldet hatte – und die bis heute nicht behoben wurde.

Die Zero Day Initiative verfolgt daher nun ein „responsible disclosure mit Ultimatum": Festgestellte Schwachstellen werden nach 180 Tagen veröffentlicht, unabhängig davon, ob ein Patch verfügbar ist – zum einen, um betroffene Nutzer möglichst frühzeitig über vorhandene Schwachstellen zu informieren, und zum anderen, um den Druck auf die Hersteller zu erhöhen. Von den aktuellen Veröffentlichungen sind unter anderem Adobe (Acrobat Reader, Flashplayer), Microsoft (Visio, Powerpoint, Excel), EMC, CA, Hewlett-Packard und IBM (Lotus Notes) betroffen. Betroffenen Nutzern empfehlen wir bis zur Bereitstellung von Updates temporär zusätzliche Schutzmaßnahmen.

Kompliziert gedacht

Die SHA-2 Familie bekommt Zuwachs: Neben den beiden unterschiedlichen Algorithmen SHA-256 und SHA-512 definiert FIPS 180-3 vom 17.10.2008 (SSN 10/2008) den SHA-224 als SHA-256 mit unterschiedlichem Initialwert, dessen Ausgabe auf 224 bit gestutzt wird, und SHA-384 als auf 384 Ausgabebits zurechtgestutzten SHA-512, auch diesen mit abweichendem Initialwert.

Der am 11.02.2011 vom NIST veröffentlichte Draft FIPS 180-4 ergänzt nun entsprechend zurechtgestutzte Versionen des SHA-512 als SHA-512/224 und SHA-512/256. Interessanterweise wird als Begründung für die neuen Familienmitglieder nicht die höhere Sicherheit angeführt, sondern die Tatsache, dass SHA-512 mit 80 Runden auf 64-Bit-Prozessoren schneller ist als der für 32-Bit-Architekturen entworfene SHA-256 mit 64 Runden. Einfach ist anders.

Neu gedacht

Dass Linux-Systeme nicht „per se" sicherer sind als Windows-Systeme zeigen die inzwischen zahlreichen Sicherheitswarnungen und Patches zu den verschiedenen Distributionen. Allerdings hält sich hartnäckig die Überzeugung, dass Windows-Systeme der Ergonomie Vorzug vor der Sicherheit geben und daher – wie bei der Autorun-Funktion von DVD und USB-Sticks – mehr Einfallstore bieten. Tatsächlich wurden solche Einfallswege durch Softwareupdates inzwischen weitgehend dicht gemacht.

Für Linux-Systeme gilt das offenbar nicht, wie Jon Larimer auf der Shmoocon am 30.01.2011 nachwies. Das Einstecken eines USB-Sticks genügt, um beispielsweise über Schwachstellen im Dateisystemtreiber oder (wie im konkreten Fall) des GNOME Filemanagers „Nautilus" Schaden zu stiften – sogar bei aktivierter Bildschirmsperre. Dagegen hilft nur, das automatische Mounten von Wechseldatenträgern manuell zu deaktivieren.

Speziell gedacht

Am 14.02.2011 erschienen gleich drei neue (Web)-Application-Firewalls: OpenWAF, IronBee und Oracle Database Firewall. Bei OpenWAF und IronBee handelt es sich um Open-Source-Lösungen von Herstellern mit Erfahrung – OpenWAF ist aus dem kommerziellen Hyperguard entstanden, IronBee entstammt der Feder von Ivan Ristic, dem Autor von mod_security. Oracles Lösung soll SQL-Datenbanken aller Art vor Angriffen schützen.

So schön die Verfügbarkeit dieser Schutzlösungen ist, drängt sich die Frage auf, wie viele Produkte eigentlich noch hintereinander geschaltet werden müssen, um einen ausreichenden Schutz von Anwendungen zu erreichen? Viel wichtiger wäre es wohl, Hersteller und Entwickler in die Lage zu versetzen, sichere Anwendungen auszuliefern, die nicht auf zusätzlichen Schutz angewiesen sind.

Zu Ende gedacht

Aufgrund der positiven Erfahrungen beim Betrieb des DNSSEC Testbeds (SSN 01/2010) kündigte DENIC am 08.02.2011 an, dass ab dem 31.05.2011 auch für die produktive .de-Zone DNSSEC eingeführt werden wird. Passend dazu gaben bei einer am 18.02.2011 präsentierten Studie von eco e.V. und VeriSign 61 % der befragten deutschen Domain-Anbieter an, DNSSEC bereits anzubieten oder innerhalb der kommenden zwölf Monaten anbieten zu wollen.

Viele Domaininhaber dürften in Bälde zur sichereren Version von DNS übergehen. Unternehmen und Organisationen können also demnächst ihre DNS-Resolver am Übergang zum Internet DNSSEC-Signaturen prüfen lassen.

Secorvo News

Grundlagenseminare …

Am 22.03.2011 startet die zweiteilige Seminarreihe „Grundlagen" mit dem dreitägigen Seminar Sicherheitsmanagement heute, einer Einführung in alle wesentlichen Bereiche des Informationssicherheitsmanagements. Mitte Mai folgt Teil zwei mit dem ebenfalls dreitägigen Seminar IT-Sicherheit heute.

… und der T.I.S.P.

Experten in Sachen Informationssicherheit bietet das einwöchige T.I.S.P.-Seminar ab 28.03.2011 mit einer Kombination aus Schulung und zertifizierter TÜV-Prüfung einen aussagekräftigen und weithin anerkannten Kompetenznachweis.

Die Programme aller Seminare und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

Sicherheit von IPv6

Anlässlich der bevorstehenden Ausschöpfung des Adressraums von IPv4 haben sich Dr. Safuat Hamdy und Hans-Joachim Knobloch mit den Herausforderungen und Sicherheitsrisiken von IPv6 auseinander gesetzt. Die Ergebnisse ihrer Überlegungen sind nachzulesen in der aktuellen Ausgabe der Zeitschrift <kes> (Seiten 11-16).

Veranstaltungshinweise

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

März 2011	
01.-05.03.	CeBIT (Deutsche Messe, Hannover)
22.-24.03.	Sicherheitsmanagement heute (Secorvo College)
28.03.-01.04.	T.I.S.P.-Schulung (Secorvo College)
April 2011	
04.-06.04.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
07.-08.04.	Datenschutzaudit: Best Practice (Secorvo College)
12.-13.04.	Verlässliche Web-Anwendungs-Sicherheit (Secorvo College)
Mai 2011	
10.-13.05.	Public Key Infrastrukturen (PKI) (Secorvo College)
10.-12.05.	12. Deutscher IT-Sicherheitskongress (BSI, Bonn)
17.-20.05.	12. Datenschutzkongress (Euroforum, Berlin)
24.-27.05.	ISSECO Certified Professional for Secure Software Engineering - CPSSE (Secorvo College)

Fundsache

Die internationale SAFECode-Initiative, die sich der Erhöhung der Vertrauenswürdigkeit informationstechnischer Systeme durch die Verbesserung und Verbreitung von Methoden sicherer Sofware-Entwicklung verschrieben hat, und in der sich neben EMC, Juniper und Microsoft insbesondere die SAP AG stark engagiert, veröffentlichte am 08.02.2011 die zweite Auflage der Fundamental Practices for Secure Software Development. Das 56 Seiten starke Dokument enthält praxiserprobte Prinzipien und Empfehlungen für Design, Programmierung und Tests.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Klaus J. Müller

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