secorvo
security consulting

Secorvo Security News

August 2012

Sprachmartialisierung

Erst verwirren sich die Worte.
Dann verwirren sich die Begriffe.
Und schließlich verwirren sich die Sachen.

Konfuzius (551-479 v.Chr.)

Schon immer ist der Fachjargon der IT-Sicherheit mit sprachlichen Anleihen aus dem Militärischen gespickt. Ein Einbruchsversuch in ein IT-System ist ein „Angriff", extern erreichbare Rechner isolieren wir in „demilitarisierten Zonen" (DMZ) und mögliche Bedrohungen beschreiben wir als „Angriffsvektoren". Das mag historische Gründe haben – inzwischen haben wir uns daran gewöhnt. Hilfreich war das allerdings nie. So ist es schwierig, Laien für Schutzmaßnahmen zu gewinnen, wenn man von drohenden „Angriffen" schwadroniert – das klingt maßlos überzogen. Überzeugender ist der Hinweis auf mögliche „Eindringlinge", die „Daten entwenden" – digitale Einbruchsszenarien liegen eher im Bereich des Vorstellbaren.

Sprache ist aber, wie wir nicht erst seit Orwells „Neusprech" wissen, nicht nur Ausdruck unserer Weltsicht. Sie beeinflusst auch unsere Wahrnehmung, mittelfristig unser Denken und langfristig unser Verhalten. Wie wirksam ein konsequentes Sprachuniversum sogar offensichtliche Unmenschlichkeit rechtfertigen kann, ließ sich in Deutschland wiederholt (zuletzt bei der RAF) beobachten.

Inzwischen hat die militärische Diktion auch die Politik erreicht. Ob sich Politiker die martialischen Bezeichnungen wegen ihrer Medienwirksamkeit zu Eigen gemacht haben oder das mediale Dauerfeuer die Ursache ist: Seit 2011 haben wir ein „Nationales Cyber-Abwehrzentrum". Wenn ein Staat eine solche Institution benötigt, rechnet er offenbar mit drohenden Cyber-Schlachten – auf gut Deutsch: dem Cyberkrieg, einem „organisierten und unter Einsatz erheblicher Mittel mit Waffen und Gewalt ausgetragenen Konflikt, dessen Handlungen auf die Verletzung und Tötung des Gegners zielen". Bei allem Respekt vor den Möglichkeiten digitaler Spionage und Sabotage – ist es wirklich „Krieg", was wir realistischer Weise befürchten müssen? Und wann fühlt sich da jemand zum „Erstschlag" genötigt?

Inhalt

secorvo
security consulting

Security News

Web-App-Krümel

Nur 3 % der Entwickler seien an Sicherheit von Software interessiert – zu diesem Schluss kommt SANS-Autor Frank Kim in seinem Blog-Eintrag vom 23.07.2012 nach Zählung der Security-Vorträge auf Entwicklerkonferenzen. Dem widersprechen die Ergebnisse der (inzwischen zwölften) WhiteHat-Studie zu sicherheitsrelevanten Schwachstellen in Webanwendungen vom 17.07.2012: Danach hat die Zahl schwerer Schwachstellen pro Anwendung in den vergangenen Jahren signifikant abgenommen. Allerdings werden im Schnitt noch immer zu viele Schwachstellen gefunden.

Zahlreiche neue Tools unterstützen die Entwicklung sicherer Software. Zur Integration von Sicherheit in die agile Software-Entwicklung hat SAFECode am 16.07.2012 das lesenswerte White-Paper „Practical Security Stories and Security Tasks for Agile Development Environments" veröffentlicht. Bezüglich der Überprüfung der Sicherheit von Software bietet die aktuelle Übersicht über 62 freie und kommerzielle Webanwendungsscanner aus dem Juli 2012 mit Benchmarks nach verschiedenen Kriterien eine Entscheidungshilfe. Für das virtuelle Patchen ist in vielen Apache-Webservern heute mod_security im Einsatz. Seit dem 26.07.2012 ist mod_security auch für die Webserver IIS und ngnix verfügbar.

Eingebettet in ein Gesamtkonzept eines erweiterten Software Development Life Cycle aus Entwicklerschulung und -sensibilisierung, Sicherheitsaudits, Monitoring und Blocking tragen solche Tools auch zu einer Reduktion von Sicherheits-Schwachstellen bei. Security-Vorträge auf Entwicklerkonferenzen könnten dann irgendwann obsolet werden.

Ende der Übergangsregelung

Am 31.08.2012 läuft die letzte Übergangsfrist der BDSG-Novelle von 2009 ab. Verschiedene Newsletter und Seiten aus dem Datenschutz- und E-Commerce-Spektrum fordern daher zum Durchforsten der zur Werbung genutzten Adressdatenbanken auf; viele Anbieter bitten ihre Mailing-Empfänger bereits um neue Einwilligungen.

Tatsächlich führt der Fristablauf nicht zu größeren Änderungen. Von § 47 Nr. 2 BDSG sind nur vor dem 01.09.2009 zum Zweck der Werbung (§ 28 Abs. 3-5 BDSG) erhobene Daten betroffen. Die Voraussetzungen für die Zulässigkeit der Versendung von E-Mail-Newslettern sind im Wesentlichen durch § 7 Abs. 2 und 3 UWG und die elektronische Einwilligung durch §§ 6 Abs. 2 und 13 Abs. 2 TMG geregelt.

Die Versendung von E-Mail-Werbung an Bestandskunden steht – vorbehaltlich eines Kundenwiderspruchs – auch zukünftig nicht unter einem Einwilligungsvorbehalt und darf auch weiterhin über einen „Opt-Out"-Mechanismus realisiert werden.

Die BDSG-Novelle von 2009 hat lediglich eine Angleichung an diese schon seit 2001 bzw. 2004 geltenden Vorschriften vorgenommen. Die vor 2009 bestehenden Erlaubnistatbestände sind zwar teils eingeschränkt, teils erweitert (und in der Verständlichkeit reduziert) worden; sie gelten jedoch im Wesentlichen fort. Eine neue Einwilligung ist nur erforderlich, wenn keiner der Erlaubnistatbestände ohne Betroffenenbeteiligung greift und keine dokumentierte Einwilligung vorliegt.

Wer bislang Datenschutzvorgaben eingehalten hat, muss nicht befürchten, dass er mit Ablauf der Übergangsfrist seine Kunden nicht mehr anschreiben darf.

Wer die Vergangenheit kontrolliert...

...kontrolliert die Zukunft, sagt die Ingsoc-Partei in George Orwells 1984. Für elektronische Geldgeschäfte gilt sinngemäß: Wer die Benutzerschnittstelle kontrolliert, kontrolliert den Benutzer. Beim Online-Banking manifestiert sich das Problem unter dem Schlagwort Man-in-the-Browser. Dass ca. 60% der Varianten des Zeus-Trojaners selbst von aktueller Antivirus-Software nicht erkannt werden, veranlasste die ENISA in einer Pressemeldung vom 05.07.2012 zur Warnung an die Banken, doch besser davon auszugehen, dass alle Kunden-PCs infiziert sind, so dass deren Browser-Anzeige und -Transaktionen von Angreifern beeinflusst werden können. Die ENISA empfiehlt daher, zur Prüfung durch den Benutzer Transaktionsdaten auf einem zweiten, vertrauenswürdigen Gerät anzuzeigen. Online-Banking mit TAN-Listen sollte man tunlichst nur noch auf frisch gebooteten, sauberen Systemen nutzen, wie z. B. Bankix.

Auch am Point-of-Sale muss man inzwischen mit solchen Angriffen rechnen – und dort helfen weder TAN-Generator noch Bankix: Am 12.07.2012 demonstrierten Forscher von SRLabs in einem ARD-Beitrag, wie sich die Firmware von weit verbreiteten POS-Terminals manipulieren lässt. Mehrere von SRLabs entdeckte Schwachstellen erlauben, über Netzwerk oder lokale Schnittstellen einen „Man-in-the-POS" einzuschleusen. Keine der Schwachstellen erlaubt es, das zertifizierte Sicherheitsmodul des Geräts zu manipulieren – aber das ist auch gar nicht nötig, da das Modul nur die Protokollschritte des Zahlungsverfahrens kontrolliert und nicht das Display und PIN-Pad. So können Angreifer direkt an der Quelle phishen – denn wer die Benutzerschnittstelle kontrolliert...

Datenschutz in der Cloud

Die Art. 29 Datenschutzgruppe hat am 01.07.2012 eine Stellungnahme zum Datenschutz bei Cloud Computing veröffentlicht. Neben einer Zusammenfassung der typischen Datenschutzrisiken und Empfehlungen zur Herstellung von Datenschutzkonformität hebt sie die Durchführung einer umfassenden Risikoanalyse durch den Cloud-Nutzer hervor. Bezüglich der meist komplexen Unterauftragnehmerstrukturen wird in Anlehnung an die Europäischen Standardvertragsklauseln empfohlen, eine Haftung des Cloud-Anbieters für Unterauftragnehmer, das Einholen des Einverständnisses des Auftraggebers zu Unterauftragnehmern und die obligatorische Weitergabe der Vertragspflichten an diese vertraglich zu verankern.

Darüber hinaus listet die Stellungnahme zu berücksichtigende Vertragsinhalte bei der Cloud-Beauftragung auf, die über die Liste in § 11 Abs. 2 BDSG zur Auftragsdatenverarbeitung hinausgehen, darunter bspw. eine Standortliste der Verarbeitungsorte. Ebenso findet sich eine Liste der Kategorien von zu verlangenden technisch-organisatorischen Maßnahmen. Es wird mehrfach hervorgehoben, dass ein starkes Verhandlungsungleichgewicht zwischen Nutzer und Anwender keine Rechtfertigung für den Verzicht auf Datenschutzanforderungen darstellt.

Interessant ist die Einschätzung der Safe Harbor Relevanz: Daneben wird in jedem Fall eine vertragliche Vereinbarung gefordert, die Datenschutzanforderungen konkretisiert. Außerdem sollen vom Dienstleister zusätzlich zur Selbstzertifizierung Nachweise über die Erfüllung der Datenschutzanforderungen erbracht werden. Damit enthält die Stellungnahme wichtige Hinweise und Mindestanforderungen an die Vertragsgestaltung.

Awareness wirkt

Im Juli berichtete The Register, dass bei der niederländischen Chemiefirma DSM die Aufmerksamkeit einiger Angestellten verhinderte, dass Schadsoftware in das Intranet des Unternehmens eingeschleust wurde. Die Mitarbeiter übergaben der IT-Abteilung auf dem Firmenparkplatz entdeckte USB-Sticks – auf denen sich, wie eine Analyse ergab, Malware befand, die zu einer Infektion geführt hätte.

Fokussierte Angriffe dieser Art sind inzwischen keine Seltenheit mehr. Nur Unternehmen, die es nicht dem Zufall überlassen, wie kompetent Mitarbeiter auf Gefährdungen und Eindringversuche reagieren, haben gegen solche Attacken eine realistische Chance.

Am **11.–12.09.2012** treffen sich Verantwortliche aus zahlreichen Unternehmen in der Buhlschen Mühle in Ettlingen auf dem von Secorvo organisierten "8. Security Awareness Symposium", um über erfolgreiche Sensibilisierungsmaßnahmen und ihre Erfahrungen aus eigenen Awareness-Kampagnen zu diskutieren.

Secorvo News

Vertieftes Know-How

Festigen Sie vorhandenes Wissen, schließen Sie Lücken, ergänzen Sie Ihre Erfahrungen und Kenntnisse um aktuelle Erkenntnisse der Informationssicherheit mit einer Schulung zum T.I.S.P. Lassen Sie sich von den Autoren des T.I.S.P.-Buchs vom **17.–21.09.** oder **12.–16.11.2012** auf die anschließende Zertifikatsprüfung vorbereiten.

Wie sich Sicherheit von Beginn an in den Softwareentwicklungsprozess integrieren lässt, erfahren Sie in der Zertifikatsschulung "Certified Professional for Secure Software Engineering (CPSSE)" am **24.–27.09.2012** in Karlsruhe.

Alles, was Sie für die Konzeption und den Betrieb einer Unternehmens-PKI wissen müssen, vermitteln wir Ihnen auf unserer PKI-Schulung am **23.–26.10.2012.**

Alle Seminarangebote und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college

Teamverstärkung

Seit dem 01.08.2012 verstärkt Sven Köhler das Secorvo-Consulting-Team. Die Schwerpunkte des erfahrenen Sicherheitsspezialisten liegen im Risiko- und Notfallmanagement, bei Sicherheitsaudits sowie der Zertifizierung nach IT-Grundschutz und dem IDW Prüfungsstandard 980 für die Prüfung von Compliance Management Systemen.

Trutzburg für jeden

Mit steigendem Leistungsbedarf nehmen die Herausforderungen zu, die bei der Planung und Gestaltung eines sicheren Serverraums oder Rechenzentrums auch von kleinen und mittleren Unternehmen zu bewältigen sind.

Markus Schäfer (proRZ Rechenzentrumsbau GmbH) gibt mit seinem Vortrag auf dem kommenden KA-IT-Si Event am **13.09.2012** einen Überblick über die Anforderungen an eine moderne zentrale IT und stellt Best-Practice-Maßnahmen zu deren sicherer Realisierung vor. Beginn ist um 18 Uhr im Schlosshotel Karlsruhe. Wir freuen uns auf Ihre Teilnahme!

Veranstaltungshinweise

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

September 2012	
11.-12.09.	8. Security Awareness Symposium (Secorvo, KA-Ettlingen)
13.09.	Trutzburg für jeden (KA-IT-Si, Kalrsuruhe)
17.-21.09.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
18.09.	Anwendertag IT-Forensik 2012 (Fraunhofer SIT, Darmstadt)
24.-27.09.	CPSSE-Schulung (Secorvo College, Karlsruhe)
25.-26.09.	D·A·CH Security (GI/OCG/BITKOM/SI/TeleTrusT, Konstanz)
Oktober 2012	
09.-11.10.	Sicherheitsmanagement heute (Secorvo College, Karlsruhe)
12.10.	1. Freiburger Datenschutztag (vivaSoft/Datenschutz individuell, Freiburg)
15.-17.10.	IDACON 2012, (WEKA-Akademie, Würzburg)
16.-18.10.	it-sa 2012, (SecuMedia Verlag, Nürnberg)
22.-26.10.	OWASP AppSec USA 2012, (OWASP Foundation, Austin/US)
23.-24.10.	ISSE 2012, (TeleTrusT/eema, Brüssel)
23.-26.10.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College, Karlsruhe)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp.

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