secorvo
security consulting

Secorvo Security News

März 2017

Sündenfall

In der Genesis beendet der Biss in die verbotene Frucht vom Baum der Erkenntnis, zu dem sich Adam und Eva verführen lassen, ihr Leben im Paradies. Wie auch immer man diese Szene interpretieren mag – die Strafe folgt dem Verstoß gegen das Verbot auf dem Fuße.

Selbst aus dieser existentiellen Erfahrung hat der Mensch offenbar nichts gelernt, und wird bis heute selten aus Erfahrung klüger. Denn auch die Informatik hat ihren Sündenfall, den sie bis heute nicht korrigiert hat. Die von *John von Neumann* (1903-1957) im Jahr 1945 veröffentlichte Referenzarchitektur für Computer, die auf Ideen *Konrad Zuses* (1910-1995) basierte, gehorchte ebenso wie die konkurrierende Harward-Architektur einem zentralen Grundprinzip: der strikten Trennung von Daten und Programm. Bis heute folgen Prozessorarchitekturen diesem Grundsatz: Befehle stehen in Befehls-, Daten in Datenregistern.

Bei den Betriebssystemen und Anwendungen nahmen es die Entwickler mit dem Prinzip schon bald nicht mehr so genau. Schließlich bereicherte die Makro-Programmiersprache Visual Basic for Applications Microsofts Office-Programme – der Biss in den Apfel: Wer seitdem ein Word-Dokument oder ein Excel-Sheet öffnet, startet zugleich etwaige darin enthaltene Programme oder Skripte.

Anfang der 90er Jahre folge die Strafe: Eine Welle von Makro-Viren verseuchte großflächig ganze PC-Netze. Gelernt haben wir fast nichts daraus: Seit fast 30 Jahren versuchen (nicht nur) Microsoft-Programmierer eifrig, jedes nur denkbare Skript in einem Office-Dokument auszuführen. Damit später niemand mit dem Finger auf sie zeigt, schalten sie Makros standardmäßig ab; klickt der Benutzer auf die Warnung („Inhalt aktivieren“ – klar, will ich doch das Dokument lesen), liegt die Verantwortung bei ihm, wenn anschließend unerwünschte Dinge passieren. Fallen die besonders hässlich aus, runzelt Microsofts Security Officer darob überrascht die Stirn.

Inhalt

secorvo
security consulting

Security News

oldClouds

Am 16.03.2017 warnte das BSI, dass über 20.000 der in Deutschland betriebenen ownCloud- (bzw. Nextcloud-) Instanzen verwundbare Softwareversionen einsetzen, die kritische Sicherheitslücken enthalten. ownCloud wird oft als Alternative zu Dropbox oder ähnlichen Diensten für den vertraulichen Austausch großer Dateien empfohlen. Der Eigenbetrieb birgt allerdings die Herausforderung, die eigene Instanz sicher zu betreiben.

Auch andere Web-Anwendungen (wie Online-Shops oder CMS) werden oft nicht ausreichend gewartet und auf dem aktuellen Stand gehalten. Eine Hilfe dabei sind kostenfreie Dienste zur Prüfung von ownCloud (bzw. Nextcloud) auf bekannte Schwachstellen. Die automatische Installation von Sicherheitsupdates steht jedoch oft im Konflikt mit Schutzmaßnahmen wie dem Entzug von Schreibrechten auf den Verzeichnissen des Webservers. Daher sollte man einen zuverlässigen Dienstleister, der die Anwendung professionell wartet, einem halbherzigen Eigenbetrieb immer vorziehen.

Nicht gehackt = sicher?

Am 26.01.2017 spendierte Mozilla seinem Browser Firefox in Version 51 ein neues Feature: Der Browser warnt nun vor Passwortfeldern, die über eine unsichere HTTP-Verbindung übertragen werden. Der Betreiber einer Nachrichtenseite über die Öl- und Gasindustrie nahm diese Neuerung zum Anlass, am 20.03.2017 einen Fehlerbericht bei Mozilla einzureichen, da die Warnung die Nutzer seiner Seite verunsichere. Er betreibe ein selbstentwickeltes Sicherheitssystem, das in 15 Betriebsjahren kein einziges Mal geknackt worden sei. Diese Aussage nahmen einige Internet-Nutzer zum Anlass, die Seite einmal auf Herz und Nieren zu prüfen. Kurze Zeit später war ein Login nicht mehr möglich – die Benutzerdatenbank war gelöscht worden. Mittlerweile ist die Webseite nicht mehr erreichbar.

Leider ist der Glaube an die eigene Unfehlbarkeit bei der Entwicklung „unknackbarer" Sicherheitssysteme noch immer verbreitet. Oder, um es mit Bruce Schneier zu sagen: Jeder kann ein Sicherheitsystem erfinden, dass so sicher ist, dass er es selbst nicht knacken kann. Unknackbar ist es deshalb noch lange nicht...

Datenschutz an der Grenze

Die Electronic Frontier Foundation veröffentlichte am 07.03.2017 ein Whitepaper zum Datenschutz bei der Einreise in die USA. Laut Regierungsinformationen hat sich die Zahl der Durchsuchungen von Smartphones oder Notebooks 2016 auf knapp 24.000 verfünffacht. Für Berufsgeheimnisträger, aber auch für Reisende mit umfangreichen privaten oder geschäftlichen Daten auf ihren Geräten können solche Kontrollbefugnisse zum Problem werden. Das Papier empfiehlt daher vor Reiseantritt eine Risikoabschätzung, zu der zu beachtende Kriterien vorgeschlagen werden.

Der Rechtsteil erläutert u. a. die zugrunde liegende Ausnahme für Grenzkontrollen von dem vierten Verfassungszusatz, der gegen unverhältnismäßige Durchsuchungen oder Beschlagnahmen schützt. Durch die Ausnahme werden Durchsuchungen ohne richterlichen Beschluss an der Grenze möglich. Das Herausverlangen von Passwörtern wird am fünften Verfassungszusatz gemessen, nach dem niemand gezwungen werden darf sich selbst zu beschuldigen, und die unterschiedlich interpretierte Befugnislage thematisiert. Gewarnt wird vor einer unbeabsichtigten oder voreiligen Einwilligung in die Durchsuchung, da diese die Betroffenen weitgehend schutzlos stellt.

Die Maßnahmenvorschläge beginnen mit dem Löschen vor Reiseantritt und der Warnung vor der Wiederherstellbarkeit. Umfangreich diskutiert wird die verschlüsselte Speicherung über Cloud-Dienste. Eine empfehlenswerte Lektüre für USA-Reisende.

Zertifikatsdesaster

Am 23.03.2017 publizierte der Chrome-Entwickler Ryan Sleevi die Entscheidung des Chrome-Teams, von Symantec ausgestellten Zertifikaten das Vertrauen zu entziehen. In mehreren Fällen hätten die Entwickler seit Mitte Januar insgesamt über 30.000 Zertifikate identifiziert, bei denen Symantec sich bei der Ausstellung nicht an die Grundprinzipien eines seriösen Zertifikatsausstellungsprozesses gehalten habe. Sleevi kündigte an, in Chrome – gestuft nach Browser-Versionen – Symantecs Root-Zertifikate auf „ungültig" zusetzen und damit geschützte Webseiten als „unsicher" zu qualifizieren, beginnend mit Version 64 in neun Monaten.

Die relativ lange Übergangszeit für offensichtlich nicht vertrauenswürdige Zertifikate ist der Tatsache geschuldet, dass (Statistiken von Mozilla zu Folge) etwa 42 % aller Zertifikatsprüfungen Symantec-Zertifikaten zuzuordnen sind, da Symantec inzwischen zahlreiche CAs der ersten Stunde übernommen hat. Derzeit „verhandelt" Symantec noch mit Google. Bleibt es bei der Entscheidung und ziehen die anderen Browseranbieter nach, könnte das erhebliche Erschütterungen auslösen – beim Vertrauen der Nutzer in HTTPS ebenso wie bei den Unternehmen, die dann kurzfristig ihre Zertifikate ersetzen müssen.

Google Analytics

Der Hamburgische Datenschutzbeauftragte hat seine Handreichung zum Einsatz von Google Analytics am 21.02.2017 aktualisiert. Anlass war zum einen die EU-US-Privacy Shield Zertifizierung von Google, zum anderen das Schrems-Urteil des EuGH zur Safe Harbor Entscheidung. Die Handreichung hält nach wie vor einen datenschutzkonformen Betrieb von Google Analytics für möglich, nun gestützt auf die Angemessenheitsentscheidung über den Privacy Shield.

Als Voraussetzungen werden weiterhin die Beschränkung auf pseudonyme Profile, der Hinweis auf das Widerspruchsrecht und dessen technische Umsetzung sowie der Abschluss des von Google zur Verfügung gestellten Auftragsdatenverarbeitungsvertrages genannt. Bei letzterem ist die Nichtigkeit des Verweises auf Safe Harbor zu beachten. Weiter sind die Nutzer durch Verlinkung auf den von Google formulierten Datenschutzhinweis aufzuklären. Besondere Pflichten ergeben sich, wenn Webangebote durch Browser genutzt werden, die den Widerspruch nicht unterstützen. Auch hierfür wird von Google eine Lösung bereitgestellt. Außerdem ist weiter der Programmcode zur Kürzung der IP-Adressen durch Google zu verwenden. Bis Mai 2018 ist damit die Nutzung von Google Analytics rechtssicher möglich. Welche Konsequenzen sich aus der Datenschutzgrundverordnung ergeben lässt die Handreichung leider offen.

Secorvo News

Seminare

Wer beim PKI-Aufbau und –Betrieb nicht in dieselben oder ähnliche Fallen tappen will wie Symantec (siehe oben), dem sei das Seminar „PKI – Grundlagen, Vertiefung, Realisierung“ vom **25. bis 28.04. 2017** ans Herz gelegt. 20 Jahre Erfahrung mit der Konzeption und dem Aufbau von PKIs verstecken sich hinter der ständig aktualisierten Konzeption. Sie werden in Theorie und praktische Umsetzung eingeführt und dürfen selbst „Hand anlegen“. Es gibt nur noch wenige freie Plätze.

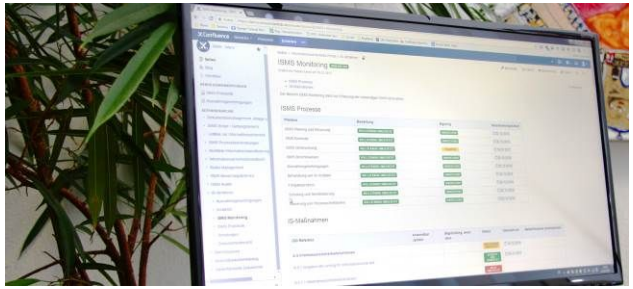
Im Juni bietet sich Ihnen vom **19.–23.06.2017** die nächste Möglichkeit, Ihre Kenntnisse und Erfahrungen in der Informationssicherheit mit dem T.I.S.P.-Zertifikat zu krönen. Ihre Referenten sind die Autoren des Begleitbuchs zum T.I.S.P., das sie vorab zur Vorbereitung erhalten.

Programm und Online-Anmeldung unter
https://www.secorvo.de/seminare

ISMS – Ready2Go

Aufbau und Betrieb eines Informationssicherheits-Managementsystems (ISMS) gemäß DIN ISO/IEC 27001:2015 erfordern in der Regel erhebliche Aufwände: ISMS-Prozesse müssen gestaltet und gelebt, die erforderliche Dokumentation erstellt und gepflegt, die Umsetzung von Vorgaben muss überwacht und kontrolliert werden. Nicht zuletzt müssen belastbare Umsetzungsnachweise erbracht werden. Die Erfüllung all dieser Anforderungen stellt insbesondere kleinere und mittlere Unternehmen vor besondere Herausforderungen.

Mit ISMS ready2go bietet Secorvo nun eine Lösung: Anstatt das Rad ständig wieder neu zu erfinden, hat Secorvo Best-Practice-Vorgaben aus über 15 Jahren Erfahrung mit Aufbau und Zertifizierung von ISMS in ein Produkt einfließen lassen, das es Unternehmen erlaubt, mit überschaubarem Aufwand und geringen Anpassungen in sehr kurzer Zeit die Anforderungen und Vorgaben der DIN ISO/IEC 27001 zu erfüllen und eine Zertifizierung effizient vorzubereiten. In Kürze steht die Zertifizierung der beiden ersten Kunden bevor.



Sollten Sie ebenfalls den Aufbau eines ISMS planen, setzen Sie sich gerne mit uns in Verbindung. Und melden Sie sich für die diesjährige SECORVENTION 2017 am **30.+31.05.2017** an.

Software ist sicher.
Und die Erde eine Scheibe.

Das nächste KA-IT-Si-Event am **18.05.2017** nimmt das Thema „Sichere Softwareentwicklung“ in den Fokus: Matthias Honka (asknet AG) wird die wichtigsten Prinzipien für die Softwareentwicklung und das technische Design sicherer Software-Systeme vorstellen.

Wenige einfache Regeln reichen dafür aus – und erschließen sich dem gesunden Menschenverstand. Oft genug jedoch werden sie missachtet, und Produktmanager, Entwickler und Administratoren reißen dadurch Sicherheitslücken.

Im Anschluss an den Vortrag haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking" (zur Anmeldung).

Veranstaltungshinweise

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

April 2017	
24.-25.04.	a-i3/BSI-Symposium 2017 (Arbeitsgruppe Identitätsschutz im Internet, Bochum)
25.-26.04.	Datenschutztage 2017 (Forum für Datenschutz, Mainz)
25.-28.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
26.-28.04.	2nd IEEE European Symposium on Security and Privacy (IEEE Computer Society, Paris/FRA)
30.04.-04.05.	Eurocrypt 2017 (IACR, Paris/FRA)
Mai 2017	
03.-04.05.	OWASP Middle East Cyber Security Conference 2017 (OWASP Foundation, Dubai/AE)
08.-12.05.	OWASP AppSec EU 2017 (OWASP Foundation, Belfast/NIR)
09.-12.05.	European Identity & Cloud Conference 2017 (KuppingerCole Ltd., München)
16.-18.05.	15. Deutscher IT-Sicherheitskongress (BSI, Bonn)
17.-18.05.	18. Datenschutzkongress (EUROFORUM Deutschland SE, Berlin)
22.-24.05.	Entwicklertag 2017 (VKSI, GI, ObjektForum, Karlsruhe)
30.-31.05.	SECORVENTION (Secorvo, Ettlingen)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Fabian Ebner, Stefan Gora, Kai Jendrian, 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