secorvo
security consulting

Secorvo Security News

April 2017

Moving Targets

Es ist die Königsdisziplin des Jägers: das Erlegen bewegten Wildes, „Bewegungsschießen“ genannt. Kein Auflegen der Waffe, kein ruhiges Zielen auf ein stehendes Tier – sondern Zielen und Schießen direkt aus der Bewegung.

Dabei dürfte sich der Jäger fühlen wie ein CISO: ständig neue, plötzlich auftauchende Ziele (≈ Bedrohungen) und wechselnde Bewegungsmuster (≈ Angriffstechniken) bei durch Bäume verstellter Sicht (≈ unvollständigen Spuren).

Dennoch hat der Jäger dem CISO etwas voraus: Er kann die Bewegungsabläufe am Schießstand üben. Der CISO hingegen ist dem Haken schlagenden Angreifer ausgeliefert: Während dieser seinen Angriff planen und strukturieren kann, ist jener zum Reagieren verdammt. Kein Wunder, dass sich da häufig das Bild eines „Katz‘ und Maus“-Spiels aufdrängt – bei dem der CISO nicht die Katze ist.

Aber stimmt das Bild tatsächlich? Die zahlreichen Berichte über erfolgreiche Angriffe täuschen leicht darüber hinweg, dass die weit überwiegende Mehrzahl der Angriffsversuche gerade nicht erfolgreich ist. Denn oft ist auch für einen Angreifer das Ziel ein *Moving Target*: Ständige Software-Patches und Betriebssystem-Upgrades, Änderungen an der Infrastruktur oder Wechsel des Schutzmechanismus‘ lassen wochenlange Recherchen und Vorbereitungen schnell Makulatur werden. Und auch der Angreifer hat keinen Schießstand – viele IT-Infrastrukturen sind so individuell, dass kein „Standardvorgehen“ zum gewünschten Ziel führt.

Warum machen wir daraus nicht eine Tugend? „Hase und Igel“ statt „Katz‘ und Maus“? Updates und Patches sollten ohnehin selbstverständlich sein – warum also das Ziel nicht auch durch Weiterentwicklungen der Schutzmechanismen „in Bewegung“ halten? Wer genug schnelle Haken schlägt, wird auch den Jäger ermüden. Bis dieser sich auf seinen Hochsitz zurückzieht und sich wieder dem äsenden Schwarzwild zuwendet.

Inhalt

Moving Targets

Security News

Versteckte Open-Source-Software

Anti-Virus Assisted Attacks

DSAnpUG-EU

Volatility automatisiert

Vorbeigefahren

Secorvo News

Secorvo Seminare

SECORVENTION 2017

9. Tag der IT-Sicherheit

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Versteckte Open-Source-Software

Am 19.04.2017 veröffentlichte die Firma Black Duck die Open Source Security and Risk Analysis (SSRA) 2017. Der Bericht basiert auf der Analyse von über 1.000 kommerziellen Anwendungen auf die Verwendung quelloffener Software. Bei 96% der untersuchten Anwendungen wurden die Autoren fündig. Dabei interpretiert ein Großteil der Hersteller die Lizenzbedingungen der quelloffenen Komponenten offenbar recht freizügig.

Aus Sicherheitssicht bedenklich ist allerdings, dass in 67% der Anwendungen verwundbare quelloffene Komponenten enthalten sind. Typische Kandidaten sind OpenSSL, jQuery oder Apache Tomcat. Ähnliches gilt für die am 20.04.2017 veröffentlichte Schwachstelle im NVIDIA-Grafikkartentreiber: Die proprietäre Software enthält einen NodeJS-Server, den Angreifer zum Umgehen von Sicherheitsmechanismen nutzen könnten. Das eigentliche Sicherheitsrisiko ist dabei nicht die Open-Source-Software an sich, sondern das unzureichende Schwachstellenmanagement der Softwarehersteller.

Um den Überblick zu behalten, sollten Abhängigkeiten wie Frameworks und Bibliotheken inklusive eingesetzter Versionsstände inventarisiert werden. Da sind die Entwickler in der Pflicht: Unter Rückgriff auf Schwachstellen-Datenbanken könnten sie so rechtzeitig Software-Updates bereitstellen.

Anti-Virus Assisted Attacks

Auf der diesjährigen ASIACCS am 05.04.2017 stellten Forscher der TU Braunschweig und der Universität Göttingen „Anti-Virus Assisted Attacks“ vor. Dabei werden keine Implementierungsfehler in der Antivirensoftware ausgenutzt, sondern die prinzipielle Funktionsweise signaturbasierter Erkennungsverfahren als Angriffsmittel missbraucht. Auf raffinierte Weise gelang es Wressnegger, Freeman, Yamaguchi und Rieck Bytefolgen herauszufinden, auf welche die untersuchten Virenscanner anschlagen. Diese Bytefolgen sind ein Erkennungsmerkmal („Marker“) infizierter Dateien.

Gelingt es nun, diese Bytefolgen in Dateien einzuschleusen, können erhebliche Störungen ausgelöst werden. Werden die Marker beispielsweise als Teil eines Textes oder Headers per E-Mail übermittelt, schlägt ein Virenscanner in der Regel nicht an, da er nur Anhänge prüft. Wird diese E-Mail von einem E-Mail-Client wie Thunderbird in einer Inbox-Datei gespeichert, kann ein lokaler Virenscanner die Inbox-Datei als „infiziert“ klassifizieren und entweder löschen oder in Quarantäne nehmen.

Kennt man den verwendeten Virenscanner, kann die Marker-Wahl auf ein bestimmtes Zielsystem abgestimmt werden. Zwar sind solche gezielten Angriffe mit einem gewissen Aufwand verbunden; auch hilft es, die „Inbox“ des E-Mail-Systems vom Virenscan auszunehmen. Dennoch ist dies ein weiterer überraschender Ansatz, um eine Schutzsoftware für Angriffe zu missbrauchen. Der erwartete Nutzen von Sicherheitslösungen sollte daher immer möglichen neuen Gefährdungen durch die Lösung selbst gegenübergestellt werden.

DSAnpUG-EU

Das Datenschutz-Anpassungs- und Umsetzungsgesetz (DSAnpUG-EU) wurde am 27.04.2017 vom Bundestag verabschiedet, knapp drei Monate nach Beschluss des Kabinettentwurfs und ein halbes Jahr nach Bekanntwerden des stark kritisierten ersten Entwurfs.

Von den Änderungsvorschlägen des Bundesrats und der Kritik aus der Sachverständigenanhörung aus dem Innenausschuss wurde nur wenig berücksichtigt. Den Bedenken gegenüber den zusätzlichen Ausnahmeregelungen zu den Transparenzpflichten und Betroffenenrechten wurde lediglich durch kleinere Korrekturen Rechnung getragen. Die Einschränkung des Rechts auf Löschung beispielsweise wurde zwar auf analoge Daten beschränkt, ergeht aber immer noch ohne Öffnungsklausel in Art. 17 der DS-GVO.

Immerhin ist das One-Stop-Prinzip der Aufsicht von der europäischen Ebene auf die nationale übertragen worden: auch bei den Landesaufsichtsbehörden bestimmt jetzt die Hauptniederlassung des für die Verarbeitung Verantwortlichen die Zuständigkeit (§ 40 Abs. 2). Ansonsten behält das Gesetz die bisherigen Regelungen zum Beschäftigtendatenschutz, zum Datenschutzbeauftragten oder zum Scoring mit geringen Abweichungen bei.

In einigen für die Praxis und die Umsetzung der DS-GVO wichtigen Punkten herrscht nun Klarheit, etwa bei der Aufsichtsstruktur oder den Datenschutzbeauftragten. Das „neue BDSG“ ist allerdings erkennbar von dem Gedanken getragen, die DS-GVO entgegen den Betroffeneninteressen zu entschärfen. Letztere könnten der rekordverdächtigen Verabschiedungsgeschwindigkeit zum Opfer gefallen sein.

Volatility automatisiert

Volatility, das bewährte Werkzeug der Speicherforensik, lässt nur sehr wenige Wünsche offen. Einer davon ist mit dem am 06.04.2017 veröffent-

lichten robusten Volatize-Script in Erfüllung gegangen. Die kommandozeilenbasierte Ergänzung erlaubt es, mit automatischer Windows-Profilerkennung die wichtigen Aspekte der Bereiche Dump, Plugins, Strings, Timeline, VAD und Yarascan ohne weitere Interaktion für ein Hauptspeicherabbild abzuarbeiten.

Sehr hilfreich ist die automatische Erstellung der zentralen .volatilityrc-Konfigurationsdatei, die zeitsparende Umgebungsvariablen z. B. bei den Plugin-Aufrufen bereitstellt, und die dann von Volatility via Volatize für Performancesteigerungen von 30%-40% genutzt werden kann. Erzeugt man z. B. für eine große Zahl an Hauptspeicherabbildern vorab alle .volatilityrc-Konfigurationsdateien und skriptet den Volatize-Aufruf, kann man über den Playbook-Modus spezifische Datendumps direkt an die Virustotal-API übergeben.

Da Volatize quellcodeoffen ist, lassen sich damit auch Playbooks für spezifische Incident-Szenarien erstellen. In Kombination mit der yarascan-Option kann über eine große Anzahl von konvertierten hiberfil.sys-Hauptspeicherauslagerungsdateien mit der Signaturregel zur Equation Group vom 20.04. 2017 die Historie analysiert werden. Welches Unternehmen wüsste nicht gerne, ob es schon einmal Opfer eines erfolgreichen Angriffs war?

Vorbeigefahren

Bereits am 30.03.2017 hat der Bundestag das Gesetz zur Änderung des Straßenverkehrsgesetzes beschlossen. Ziel des Gesetzes ist es, einen gesetzlichen Rahmen für den Einsatz automatisierter Systeme in Fahrzeugen zu schaffen. Das Gesetz konzentriert sich zunächst auf die Regelung der Verantwortung, Sanktionen und Pflichten der Fahrzeugführer.

Bereits der Bundesrat hatte darauf hingewiesen, dass Verbraucherinteressen nicht ausreichend berücksichtigt, die Zulassungsvoraussetzungen für die Systeme nicht konkretisiert und dass vor allem Sicherheitsanforderungen bezüglich möglicher Angriffe von außen nicht geregelt würden.

Geregelt wurden dagegen Datenschutzfragen der Aufzeichnungen im Fahrzeug. Zwar wurde die Löschfrist von drei Jahren auf ein halbes Jahr verkürzt; dennoch blieben umfangreiche Zugriffsbefugnisse der Verkehrsbehörden bestehen. Der Schutz der Daten vor unbefugtem Zugriff, die diesbezügliche Verantwortung, eine ausreichende grundsätzliche Zweckbeschränkung und der erlaubte Umfang der Datenerhebung wurden dagegen nicht geregelt.

Insgesamt verfehlt das Gesetz das Ziel, einen verlässlichen Rahmen zu schaffen, da es letztlich nur einen Teil des Regelungsbedarfs aufgreift. Daher würde es nicht überraschen, wenn der Bundesrat nun den Vermittlungsausschuss anriefe.

Secorvo News

Secorvo Seminare

Vom **19. bis 23.06.2017** bieten wir Ihnen die nächste Möglichkeit, Ihre Kenntnisse und Erfahrungen in der Informations- und IT-Sicherheit mit einem T.I.S.P.-Zertifikat zu krönen. Zur Vorbereitung auf das einwöchige Intensivseminar mit anschließender Zertifizierung erhalten Sie vorab das Begleitbuch „Zentrale Bausteine der Informationssicherheit“. Sollte Ihnen eine Teilnahme an diesem Termin nicht möglich sein, bieten sich Ihnen am **25.** bis **29.09.2017** und am **27.11.** bis **01.12.2017** zwei weitere Gelegenheiten.

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

SECORVENTION 2017

Was bedeutet eine ISO-27001-Zertifizierung in der Praxis? Welcher Aufwand ist damit verbunden - und lohnt sich dieser? Was lässt sich aus den Erfahrungen zertifizierter Unternehmen lernen?

Antworten auf diese und ähnliche Fragen gibt es auf der SECORVENTION am **30.** und **31.05.2017** in der Buhlschen Mühle in Ettlingen. Das vollständige Programm finden Sie auf unserer Webseite www.secorvention.de.

9. Tag der IT-Sicherheit

Der „Karlsruher Tag der IT-Sicherheit“, eine Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative mit der IHK Karlsruhe und dem Cyber-Forum e.V., beschäftigt sich in diesem Jahr zum neunten Mal mit aktuellen Herausforderungen der IT-Sicherheit für Unternehmen. Als Keynote-Speaker konnten wir Herrn Dr. Stefan Brink, den frisch gekürten Landesbeauftragten für den Datenschutz in Baden-Württemberg gewinnen. Fachvorträge behandeln die Themen Risikomanagement, Aufbau eines DIN ISO 27001 orientierten ISMS und Social Engineering. Schließlich zeichnet das BSI ein aktuelles Lagebild der Cybersicherheit.

Gelegenheit zum fachlichen Erfahrungsaustausch mit Referenten, Teilnehmern und Ausstellern gibt es am Buffet. Die Veranstaltung findet statt am **28.06.2017** im Saal Baden der IHK Karlsruhe. Das Programm sowie die Möglichkeit zur Anmeldung finden Sie auf unserer Webseite www.tag-der-it-sicherheit.de.

Veranstaltungshinweise

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

Mai 2017	
03.-04.05.	OWASP Middle East Cyber Security Conference 2017 (OWASP, Dubai/AE)
04.05.	BvD Verbandstag 2017 (BvD, Berlin)
08.-12.05.	OWASP AppSec EU 2017 (OWASP, 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, Berlin)
22.-24.05.	Entwicklertag 2017 (VKSI, GI, ObjektForum, Karlsruhe)
30.-31.05.	SECORVENTION (Secorvo, Ettlingen)
Juni 2017	
07.-08.06.	Annual Privacy Forum 2017 (ENISA, EC DG Connect, Universität Wien, Wien/AT)
19.-23.06.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
28.06.	9. Tag der IT-Sicherheit (IHK, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)

Fundsache

Am 26.04.2017 veröffentlichte das SEI CERT (Software Engineering Institute der Carnegie Mellon University) eine sehr umfassende Liste von C++ Secure Coding Standards.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Stefan Gora, Michael Knopp, Jochen Schlichting

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