secorvo
security consulting

Secorvo Security News

Mai 2017

Fragile IT-Sicherheit

Am 13.05.2017 wirbelte der Kryptotrojaner ‚WannaCry' die IT weltweit durcheinander. Von oft reißerischen Presseberichten getrieben beschäftigte der Vorfall Security-Verantwortliche auf der ganzen Welt. Mit etwas Abstand können wir heute den Fall genauer unter die Lupe nehmen: Was können wir daraus lernen?

WannaCry war weder ein besonders neuartiger noch ein besonders gut gemachter Angriff – im Gegenteil: Die Autoren machten Fehler, die frühere Kryptotrojaner schon nicht mehr enthielten. Eine Neuerung war die Verwendung eines der von der NSA gesammelten Exploits, die im April von Hackern veröffentlicht worden waren. So verbreitete sich der Trojaner sowohl via E-Mail (und die Schwachstelle Mensch) als auch über eine Wurmkomponente, die alle erreichbaren Rechner attackierte, die die vom Exploit ausgenutzte Windows-Schwachstelle aufwiesen. Wie andere Kryptotrojaner verschlüsselte er alle Dateien, auf die der betroffene Nutzer oder Rechner Zugriff hatte.

Vor derartiger Schadsoftware schützen nur aufeinander abgestimmte präventive und Schaden begrenzende Maßnahmen wirkungsvoll. Der Virenschutz hilft, bekannte Schädlinge aus dem Netz und vom Rechner fernhalten – gegen neue Schadsoftware hilft er selten. Daher gilt es, Benutzer zu sensibilisieren – und für den Fall der Fälle den Schaden einzudämmen und die Verbreitung zu begrenzen. Eine restriktive Berechtigungsvergabe und systematische Netzwerksegmentierung tragen ebenso dazu bei wie ein funktionierendes Backup- und Recovery-Konzept, ein sorgfältiges Patch-Management und der professionelle Umgang mit Vorfällen.

Das Zauberwort zur sinnvollen Abstimmung von Schutzmaßnahmen heißt übrigens Informationssicherheitsmanagement. Kombinierte Angriffe wie WannaCry werden zukünftig der Standard sein. Daher sollte man WannaCry als Weckruf verstehen, das eigene ISMS einmal auf den Prüfstand zu stellen.

Inhalt

secorvo
security consulting

Security News

Virus per Virenscanner

Im Schatten der allgemeinen Aufregung über die Schadsoftware WannaCry wurde im Mai eine kritische Schwachstelle in Microsofts Defender entdeckt: Am 05.05.2017 publizierte Travis Ormandy via Tweet die Entdeckung der gefährlichsten Windows-Schwachstelle seit langem. Sie steckte in der NScript-Komponente des Windows Defender, die mit erhöhten Rechten und ohne Sandbox-Mechanismen dynamische Analysen von JavaScript-Code durchführt, und lässt sich mit wenigen Zeilen JavaScript-Code beispielsweise in einer Website, E-Mail oder Datei platzieren. Der Angreifer kann darüber das komplette System übernehmen. Betroffen sind die meisten Windows-Versionen, allerdings ist die Ausnutzung bei neueren Versionen (Windows 10 und 8.1) durch zusätzliche Schutzmechanismen erschwert. Microsoft reagierte schnell und lieferte am 08.05.2017 ein Update aus, das die Schwachstelle behebt. Keine acht Tage später fanden Google-Forscher am 16.05.2017 via Fuzzing die nächste kritische Schwachstelle im Defender – für die Microsoft am 25.05.2017 einen Bugfix außerhalb des Update-Zyklus' lieferte.

Da signaturbasierte Ansätze heute praktisch wirkungslos sind, setzen Virenscanner verstärkt auf die dynamische Analyse von Inhalten. Dabei werden die Daten interpretiert oder ausgeführt. Solche Analysen sind riskant, denn wie bei jeder anderen Software muss man auch hier mit Schwachstellen rechnen – dank erhöhter Rechte und fehlendem Sandboxing eine heikle Angelegenheit. Daher ist die Frage berechtigt, ob Virenscanner inzwischen nicht mehr schaden als nützen.

Sichere Passwörter revisited

Am 02.05.2017 beendete das National Institute of Standards and Technology (NIST) die Diskussion des Entwurfs der Richtlinie für Digitale Identitäten. (NIST Special Publication 800-63B). Bemerkenswert sind der Wegfall der Empfehlung von Komplexitätsvorgaben und die Verankerung der Sicherheit von Passwörtern vor allem an deren Länge.

Die Begründung des Standards deckt sich mit unseren Erfahrungen – schon seit 2009 weisen wir auf Fehlsteuerungen durch die gängigen Hinweise zur Gestaltung von Passwörtern hin.

Anfängerfehler

Intels Active Management Technology ist ein Fernwartungsverfahren mit Webinterface. Mitte Februar 2017 wurde darin eine Sicherheitslücke entdeckt, die es einem Angreifer ermöglicht, damit ausgestattete Geräte fernzusteuern. Die besondere Brisanz dieser Schwachstelle liegt in der Möglichkeit, die Authentifizierung als Administrator zu umgehen.

Am 05.05.2017 wurden weitere Details öffentlich. Ursache war ein Fehler, dem ein Ehrenplatz in Lehrbüchern für Softwaresicherheit gebührt: Für den Vergleich zweier MD5-Hashwerte verwendeten die Programmierer die C-Funktion `strncmp()` – und übergaben als String-Länge die Angabe des Clients. Behauptete dieser, die Länge sei null, lieferte der Vergleich – Sie ahnen es – als Ergebnis „ok". Dabei ist der Fehler spätestens seit der Entdeckung des OpenSSL-Bugs Heartbleed im April 2014 (SSN 4/2014) ein Klassiker: Ein Server darf sich nie ungeprüft auf (nicht authentisierte) Längenangaben des Clients verlassen.

Interessenkollision

Am 05.05.2017 ist das Videoüberwachungsverbesserungsgesetz in Kraft getreten, das § 6b BDSG für die Überwachung öffentlich zugänglicher großflächiger Anlagen oder von Fahrzeugen und Einrichtungen des öffentlichen Personenverkehrs um eine Vorgabe für die Abwägung zwischen Betroffenen- und Überwachungsinteressen ergänzt: Der Schutz von Leben, Gesundheit oder Freiheit von Personen im Überwachungsbereich gilt danach als besonders wichtiges Interesse.

Der so entstandene § 6b BDSG ist auch bereits in dem (nun ebenfalls verabschiedeten) Datenschutz-Anpassungs- und Umsetzungsgesetz (DSAnpUG) enthalten. Ausdrückliches Ziel ist es, die Sicherheit der Bevölkerung präventiv zu erhöhen, auch durch private Videoüberwachung.

Dass es sich hierbei um eine geeignete Maßnahme handelt wird von Aufsichtsbehörden und Datenschützern bezweifelt. Auf die Einordnung in das System der Datenschutz-Grundverordnung, etwa das Verhältnis zur hierfür verlangten Datenschutz-Folgenabschätzung oder die herangezogene Öffnungsklausel, wird im DSAnpUG nicht eingegangen.

Für Unternehmen, die ihr Gelände oder ihr Hausrecht durch eine Videoüberwachung schützen möchten, ändert sich durch das Gesetz wenig. Die Abwägungsvorgabe ist jedoch eine weitere Abwertung der Betroffeneninteressen. Ungeachtet der Intention ist die Bezugnahme auf Leben, Gesundheit und Freiheit jedoch paradox, denn auch die informationelle Selbstbestimmung ist ein Freiheitsgrundrecht. Daher wäre der Formulierung nach auch dem Betroffeneninteresse, unbeobachtet zu bleiben, besonderes Gewicht beizumessen.

secorvo
security consulting

Phishing mit Unicode-Domains

Namen von Unicode-Domains können so gewählt werden, dass eine gefälschte URL visuell praktisch nicht vom Original unterschieden werden kann – eine Steilvorlage für Phisher. Neu ist das nicht, aber durchaus unterhaltsam – siehe den Blogeintrag von Xudong Xheng vom 14.04.2017. Danach zeigt der Firefox-Browser mit Standardeinstellungen die URL apple.com (bitte mit Firefox öffnen) mit grünem Schloss-Symbol an. Nur wer sich das Zertifikat genauer ansieht (wofür eigentlich kein Anlass besteht) wird erkennen, dass die Website eigentlich www.xn--80ak6aa92e.com heißt.

Gegen solche Angriffe hilft, URLs „vertrauter" Domains manuell oder via Symbolleiste auszuwählen und nicht auf angebotene Links zu klicken. Alternativ setze man in den erweiterten Einstellungen (`about:config`) von Firefox den Parameter `network.IDN_show_punycode` auf `true`: Die URL wird dann als „echte" Adresse angezeigt. Die aktuelle Version 58 des Chrome-Browsers ist für solche Unicode-Angriffe nicht (mehr) anfällig.

Secorvo News

PKI-Policy-Rahmenwerk

Im Mai 2017 wurde das – in einer ersten Fassung bereits 2007 veröffentlichte – Secorvo White Paper zum Policy Rahmenwerk einer PKI überarbeitet und auf einen aktuellen Stand gebracht. Es enthält praxiserprobte und konkrete Hinweise zur Gestaltung von *Certificate Policies* (CP), *Certification Practice Statements* (CPS) und *PKI Disclosure Statements* (PDS). Im Anhang ist zusätzlich die deutsche Übersetzung des Gliederungsrahmens für eine PKI-Policy nach RFC 3647 enthalten.

Zertifizieren Sie Ihr Know-how

Kurzentschlossene können sich noch einen Platz auf dem nächsten T.I.S.P.-Seminar vom **19. bis 23.06.2017** sichern. Im Anschluss können Sie Ihre Fachkenntnisse und Erfahrungen in der Informationssicherheit zertifizieren lassen. Zur Vorbereitung erhalten Sie gleich nach Ihrer Anmeldung das Begleitbuch „Zentrale Bausteine der Informationssicherheit" zugesandt. Programm, Online-Anmeldung und weitere Termine: secorvo.de/seminare.

9. Tag der IT-Sicherheit

Auf dem neunten Karlsruher „Tag der IT-Sicherheit", einer Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit der IHK Karlsruhe und dem CyberForum e.V., werden aktuelle Herausforderungen der IT-Sicherheit für Unternehmen aufgezeigt und Präventionsmöglichkeiten vorgestellt. Diesjähriger Keynote-Speaker ist Dr. Stefan Brink, Landesbeauftragter für den Datenschutz in Baden-Württemberg. Anschließend behandeln Fachvorträge die Themen Risikomanagement, Aufbau eines an der DIN ISO/IEC 27001 orientierten ISMS und Social Engineering.

Die Veranstaltung findet am **28.06.2017** im Saal Baden der IHK Karlsruhe statt. Das Programm sowie die Möglichkeit zur Anmeldung finden Sie auf unserer Webseite www.tag-der-it-sicherheit.de.

ISMS für alle

Wie viel kostet ein DIN ISO/IEC 27001-konformes Sicherheitsmanagement-System? Die (realistische) Antwort auf diese Frage hat schon die eine oder andere Geschäftsleitung erblassen lassen. Die Etablierung eines wirksamen Risiko-Managements und die Definition der für die systematische Organisation der Informationssicherheit erforderlichen Rollen, Regelwerke, Prozesse, Berichte und Dokumentationen – auch als Nachweise für eine Zertifizierung – sind unvermeidlich mit Aufwand verbunden.

Dabei unterscheiden sich ISM-Systeme in der Praxis meist nur geringfügig – Prozesse, Dokumentationen und oft sogar Regelwerke gleichen sich sogar über Branchengrenzen hinweg. Warum also das Rad jedes Mal neu erfinden?

Aus unseren über 15 Jahren Erfahrung mit dem Aufbau und der Zertifizierung von ISM-Systemen haben wir ISMS ready2go entwickelt – eine Lösung, die die Einführung eines ISMS mit sehr überschaubarem Aufwand und geringen Anpassungen in sehr kurzer Zeit ermöglicht und den Anforderungen und Vorgaben der DIN ISO/IEC 27001 genügt. Die ersten Kunden äußern sich begeistert. Zwei Beispiele:

„ISMS ready2go folgt dem Need-2-Have-Prinzip: Mehr braucht es nicht, weniger auch nicht. Ein übersichtliches, individuell anpassbares und schlankes CMS, der ideale Begleiter für Ihr ISMS-Projekt."
(Detlef Pouw, Stiftung Kirchliches Rechenzentrum Südwestdeutschland)

„Automatische Auswertungen auf Knopfdruck, ein hierarchischer Workflow, so haben wir unser Risikomanagement sicher im Griff!"
(Markus Hotz, 3iMedia GmbH).

Sollten Sie ebenfalls am Aufbau eines ISMS arbeiten, setzen Sie sich gerne mit uns in Verbindung.

Veranstaltungshinweise

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

Juni 2017	
07.-08.06.	Annual Privacy Forum 2017 (ENISA, EC DG Connect, Universität Wien, Wien/AT)
19.-23.06.	Audit Challenge 2017 (ARC Institute, Frankfurt)
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)
Juli 2017	
03.-05.07.	EssoS 2017 – International Symposium on Engineering Secure Software and Systems (EssoS, Bonn)
12.-14.07.	SOAPS 2017 – 13th Symposium on Usable Privacy and Security (USENIX, Santa Clara/US)
18.-21.07.	PETS 2017 – 17th Privacy Enhancing Technologies Symposium (Univ. of Minnesota, Minneapolis/US)
19.-20.07.	DuD 2017 (COMPUTAS, Berlin)
26.-27.07.	Blackhat USA 2017 (Blackhat, Las Vegas/US)
27.-30.07.	DEF CON 25 (DEFCON, Las Vegas/US)

Fundsache

Ein Forscherteam der Universität Braunschweig um Konrad Rieck fand in mehr als 200 Android-Apps Ultraschall-Seitenkanäle zum „Cross Device Tracking“ (SSN 01/2016). Eine (nicht nur) für Datenschützer beunruhigende Entwicklung – auch wenn sich die Zahl der betroffenen Apps mit 0,015% (noch) deutlich unterhalb der Relevanzschwelle bewegt.

Impressum

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

ISSN 1613-4311

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