secorvo
security consulting

Secorvo Security News

Oktober 2010

Stuxnet - mythenfrei

Auch wenn dem sich über USB-Sticks und Netze verbreitenden Wurm „Stuxnet“ technische Raffinesse und den Autoren viel Know-how zugestanden werden muss, ist sein Erscheinen wenig erstaunlich. Sowohl USB-Würmer als auch Zero-Day-Exploits (noch nicht veröffentlichte Schwachstellen) gab es bereits. Neu ist, dass industrielle Regelungs- und Steuerungssysteme befallen wurden, hier Siemens PCS 7 und WinCC. Was lässt sich aber, ohne über Auftraggeber und Zielsetzung zu spekulieren, aus dem Vorfall lernen?

Fakt 1: Virenschutz hat Grenzen. Stuxnet verbreitete sich unerkannt über einen Zeitraum von einem Jahr. Verlässlichen Schutz vor neuartigen Viren und Trojanern können Scanner nicht bieten. Ein wirksamer Schutz kritischer Systeme benötigt umfassendere Konzepte.

Fakt 2: Datenträger sind Gefahrenquellen. Die verbreitete Nutzung von USB-Sticks über Systemgrenzen (privat/dienstlich, intern/extern, Office/Produktionssystem) hinweg ist leichtsinnig – und Bequemlichkeit keine Rechtfertigung. Hier sollte im Detail geregelt werden.

Fakt 3: Vertrauen ist gut, Kontrolle besser. Sie trauen Ihrem Dienstleister oder Lieferanten. Aber haben Sie sich auch davon überzeugt, dass er ebenso auf Sicherheit achtet wie Ihr Unternehmen?

Fakt 4: Netzsegmentierung und Firewalls helfen. Viel zu häufig werden kritische Systeme nicht von weniger kritischen entkoppelt und Verbindungswünsche von innen ins Internet großzügig zugelassen. Einmal eingedrungen, haben Trojaner so leichtes Spiel.

Fakt 5: Schutzbedarfsanalysen identifizieren das Wesentliche. Erst anhand einer Klassifikation kritischer und weniger kritischer Systeme ist es möglich, geeignete Maßnahmen zur Vorsorge auszuwählen – und bei einem Vorfall angemessen und zeitnah zu reagieren.

Unsere Empfehlung: Rechnen Sie mit weiteren derartigen „Neuheiten“ bei Schadsoftware. Beugen Sie möglichen Schäden wirksam vor – durch Schutzmaßnahmen und definierte Sicherheitsprozesse.

Inhalt

secorvo
security consulting

Security News

Autoritätsfrage

Im Jahr 1906 schlüpfte der Schuster Wilhelm Voigt in die Uniform eines preußischen Hauptmanns. Die verlieh ihm so viel Autorität, dass er ohne Rückfrage die Stadtkasse von Köpenick ausgehändigt bekam. Heutige Betrüger nutzen ausgefeilte Trojaner, um in den Browser ihrer Opfer zu schlüpfen und deren Online-Konten zu übernehmen. Gegen derartige „Man-in-the-Browser"-Angriffe bietet es sich an, zusätzlich zum möglicherweise infizierten PC ein weiteres, vertrauenswürdiges Gerät einzusetzen – so etwa bei der mobileTAN das eigene Handy.

Allein: Mit der Autorität der angezeigten Original-Webseite der Bank oder des Online-Anbieters kann der (Haupt-)Mann im Browser dem Anwender nahe legen, die Warnungen seines externen Geräts zu ignorieren – oder sogar es selbst zu manipulieren. Dass dies nicht bloße Theorie ist, wurde am 25.09. 2010 bekannt: Eine Variante des Trojaners ZeuS drängt ihren Opfern ein Update des Sicherheits-Zertifikats (sic!) für ihr Handy auf – und installiert tatsächlich einen Trojaner, der zusammen mit seinem „Partner" auf dem PC die mobileTAN aushebelt.

Hosentaschenforensik

Mit dem FTK-Imager ist seit dem 08.10.2010 die grundlegend überarbeitete Windows-Version 3.0 des bewährten und kostenfreien forensischen Werkzeugs verfügbar. Neu ist die Unterstützung für Images mit den Dateisystemen VxFS, exFAT und Ext4 sowie des forensischen Festplattenabbildformats AFF. Damit ist eine Einbindung der Formate AFF, DD, RAW, E01 und S01 als schreibgeschützte physische Laufwerke unter Windows möglich. Für FAT und NTFS kann bei Bedarf auch eine Schreibemulation genutzt werden, ohne dass die Integrität der Abbilddatei beeinträchtigt wird. Besonders die unkomplizierte Einbindung der Dateisysteme unter Ext3, Ext4 und HFS+ (iPhone) spart Zeit. Ein kleiner Wermutstropfen bleibt: verschlüsselte Abbildformate sind derzeit nicht nutzbar.

Firefox als Vorratsdatenspeicher

Eines der Argumente gegen insbesondere staatliche Vorratsdatenspeicherung ist, dass niemand sicher sein kann, dass nicht eines Tages die angehäuften Daten von weniger wohlmeinender Seite missbraucht werden. Wie einfach das geht, führt gerade der Trojaner Trojan-PWS-Nslog vor: Wie am 06.10. 2010 gemeldet schaltet er kurzerhand in der Firefox-Konfiguration das Speichern eingegebener Passwörter ein und die Rückfrage dazu ab, um sich später der kompletten Sammlung zu bemächtigen.

Cyber Security Month

Den Oktober 2010 erklärte das Internet Storm Center ISC am 01.10.2010 zum "Cyber Security Month". Täglich erschien seitdem ein Tagebucheintrag mit praktischen Hinweisen zur IT-Sicherheit. Die Einträge der ersten Woche wendeten sich an Familien, die der nächsten an Kinder, danach wurden im Bereich "Bosses" Führungskräfte angesprochen und im letzten Teil die Mitarbeiter von Unternehmen. Die Einträge (sowie die zahlreichen Kommentare) enthalten viele hilfreiche Empfehlungen.

De-Mail ... zum Zweiten

Das Bundeskabinett hat am 13.10.2010 den zweiten Gesetzentwurf für De-Mail-Dienste beschlossen – eingestuft als „besonders eilbedürftig", denn Umsetzungsziel ist das Jahr 2011. Das schon im April 2009 von der Großen Koalition initiierte Gesetzgebungsverfahren wurde Ende der Legislaturperiode mit einem Appell des Bundestages an die neue Regierung zur Weiterführung des Projekts abgebrochen.

In dem neuen Entwurf sind weitere Regelungen enthalten. So ist die Verpflichtung des Anbieters, die Verbindung des Nutzers zu seinem Konto zu verschlüsseln, jetzt ausdrücklich geregelt, dafür ist die Verpflichtung zur Bereitstellung pseudonymer Adressen für natürliche Personen entfallen. Neu ist auch die Abholbestätigung einer E-Mail durch den Dienstanbieter des Empfängers gegenüber öffentlichen Stellen und die Verpflichtung der Anbieter, eine automatische Weiterleitung zu ermöglichen.

Zu besserer Verständlichkeit haben die Überarbeitungen nicht geführt. Einige Regelungen, wie die automatische Weiterleitung oder das Streichen der Verpflichtung zum Pseudonymangebot, konterkarieren gar den ursprünglichen Gesetzeszweck.

Perlen sicherer Softwareentwicklung

Sicherheit genießt meist nicht höchste Priorität bei Softwareentwicklern. Dabei gibt es praktikable Vorgehensweisen, die – nach Absolvieren der Lernkurve – nachweislich zu signifikant sichererem Code führen, wie z. B. Design by Contract, ein Ansatz, für den mittlerweile Unterstützung für viele gängige Programmiersprachen existiert.

Ein anderer, vom NIST am 06.10.2010 als SP 800-142 veröffentlichter Ansatz beschäftigt sich mit dem Problem, wie man der Masse an Testfällen effektiv Herr werden kann. Bekanntlich explodiert die Zahl der Testfälle mit der Anzahl der zu testenden Parameter und der Zahl der Werte, die diese annehmen können. Die Autoren präsentieren

Untersuchungsergebnisse, nach denen Programmierfehler selbst in komplexen Systemen sehr oft durch die Interaktion von nur drei bis vier Parametern ausgelöst wird, aber praktisch nie von mehr als sechs. Es ist daher nicht nötig, alle Kombinationen von Parametern durchzuprobieren, um alle Fehler aufzuspüren.

Erfreulicherweise haben die Autoren auch gleich ein frei verfügbares Werkzeug geschrieben, welches einen (fast) minimalen Satz an Kombinationen von Parametern erzeugt, dessen Umfang ganz erheblich geringer ist, als die Zahl sämtlicher Kombinationen. Weder das Werkzeug noch die Vorgehensweise wird Sicherheits-Wunder bewirken, jedoch gibt es nun - bei angemessener Anwendung - ein gutes Argument mehr gegen Ausflüchte, Systeme nicht sicher zu entwerfen und zu implementieren.

HTTPS soll HTTPS bleiben

Die Veröffentlichung des Firefox-Add-On Firesheep am 24.10.2010 auf der Toorcon in San Diego hat einem altbekannten Problem, der unsicheren Übertragung von Cookies als Session-IDs, neue Aufmerksamkeit zu teil werden lassen.

Mit dem Add-On ist es möglich, Netzwerkverkehr mitzuschneiden und automatisiert unverschlüsselt übertragene Session-IDs zu sammeln. Die durch diese IDs authentifizierten Accounts werden direkt in Firesheep angezeigt; ein Anmelden unter fremdem Account ist durch Doppelklick möglich.

Da viele populäre Seiten, u. a. auch Facebook, nach der Anmeldung über eine mit SSL geschützte Seite wieder auf unverschlüsseltes HTTP zurückschalten, geben sie die im Cookie gespeicherte Session-ID jedem preis, der den Netzverkehr mitlesen kann.

So lange dieses Problem nicht von Anwendungsseite durch konsequente Verschlüsselung, beispielsweise durch die Verwendung von HSTS, aus der Welt geschafft ist, bleibt nur, sich mit Werkzeugen wie Force TLS oder NoScript zu behelfen.

Neue Jagdreviere

Die Entfernung von SIM-Locks bei Mobiltelefonen ruft die Strafverfolgungsbehörden inzwischen nicht mehr nur bei gewerblichem Handeln auf den Plan. Nach Auskunft der Polizeiinspektion Göttingen vom 12.10.2010 sind im Zusammenhang mit solchen Entsperrungen nun auch Ermittlungsverfahren gegen 600 Kunden eingeleitet worden.

Zwar ist die Verletzung von Markenrechten durch die gewerbliche Entsperrung schon vor sechs Jahren höchstrichterlich festgestellt worden; ob es sich für die Endanwender dabei um einen Straftatbestand handelt, ist jedoch bislang ungeklärt. Daher ist eine Anklageerhebung in diesen Verfahren eher unwahrscheinlich, zumal die Einschlägigkeit der meisten geprüften Straf-, Urheber- und Wettbewerbsrechtsvorschriften gegenüber privaten Endkunden zweifelhaft ist.

Sollte aus dieser Initiative jedoch eine generelle Strafverfolgung resultieren, könnte sich dies schnell auf weitere Bereiche auswirken, in denen die Funktionsfähigkeit von Software oder Hardware durch das Entfernen von Sperren erweitert werden kann. Dabei wird es für private Nutzer auch auf die Haltung der Hersteller und Rechteinhaber ankommen, denn die Verfolgung vieler der in Erwägung gezogenen Straftatbestände, wie etwa Computerbetrug, setzt einen Strafantrag des Geschädigten voraus.

Secorvo News

Unser Seminarangebot 2011

Zum Jahresende geben wir Ihnen mit der TISP-Schulung vom 22.-26.11.2010 noch einmal die Gelegenheit, Ihr Wissen im Bereich IT-Sicherheit zu zertifizieren. Auch 2011 bietet unser Seminarangebot (jetzt mit Teilnehmer-Rating) Rahmen, Referenten und Teilnehmer für einen intensiven Erfahrungsaustausch unter Experten. Wir freuen uns auf Sie!

Kronjuwelen-Hacking

SAP-Systeme sind das Rückgrat unserer hochautomatisierten Wirtschaft. In den meisten größeren Unternehmen steuern SAP-Anwendungen die kritischen Unternehmensprozesse: Fertigung, CRM, Lieferantenmanagement, Personalplanung, Finanzen, Controlling. Sie verarbeiten sensitivste Daten – die Kronjuwelen des Unternehmens. Auf der nächsten Veranstaltung der Karlsruher IT-Sicherheitsinitiative beleuchtet Dr. Markus Schumacher (Virtual Forge) in seinem Vortrag „SAP Anwendungen im Visier von Hackern“ am **11.11.2010** (18 Uhr im Schlosshotel Karlsruhe) typische Angriffsmöglichkeiten, erläutert deren Ursachen und gibt Handlungsempfehlungen zum Schutz (Anmeldung).

Secorvo hören und sehen

Auf dem kommenden 18. DFN-Workshop „Sicherheit in vernetzten Systemen“ vom 15.-16.02.2011 in Hamburg wird Secorvo gleich mit zwei Vorträgen zu aktuellen Themen der IT-Sicherheit zu hören sein: Klaus J. Müller wird zu „Datenschutz und Datensicherheit in Smart Grids“ vortragen, und Jörg Völker aktuelle Erkenntnisse zur „Sicherheit von iPhones“ vorstellen.

Veranstaltungshinweise

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

November 2010	
03.-04.11.	#days Workshops: Exploit Laboratory / Protecting from GSM attacks (DEFCON, Luzern/CH)
05.-06.11.	#days Conference (DEFCON, Luzern/CH)
09.-12.11.	PKI (Secorvo College)
15.-17.11.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
18.-19.11.	Datenschutzsaudit: Best Practice (Secorvo College)
18.-19.11.	34. DAFTA (GDD e.V., Köln)
22.-26.11.	T.I.S.P.-Schulung (Secorvo College)
23.-26.11.	ISDC 2010 Europe (DeepSec GmbH, Wien/AT)
Dezember 2010	
05.-09.12.	AsiaCrypt 2010 (IACR, Singapur/SGP)
06.-07.12.	IsSec/ZertiFA 2010 (Computas, Berlin)
27.-30.12.	27th Chaos Communication Congress (27C3) (Chaos Computer Club, Berlin)
Januar 2011	
18.-20.01.	Omnicard 2011 (inTIME, Berlin)

Fundsache

Eine technisch tiefer gehende Analyse des Stuxnet-Wurms bietet ein am 12.10.2010 erschienenes 50seitiges Dossier der Firma Symantec, verfasst von Nicolas Falliere, Liam O Murchu und Eric Chien. Unter anderem zeigt es die wahrscheinliche Verbreitung – die mindestens von Juni 2009 bis Juni 2010 unbemerkt blieb.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch, 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