Der digitale Erstschlag ist erfolgt

Fieberhaft arbeiten die besten Sicherheitsexperten der Welt an der Analyse eines völlig neuartigen Computervirus. Jetzt legen erste Indizien einen erstaunlichen Verdacht nahe: Offenbar hat die digitale Waffe das iranische Atomprogramm sabotiert. Wenn das zutrifft, kann von nun an keine Industrieanlage der Welt mehr als sicher gelten.

Von Frank Rieger

Auf den ersten Blick sah das kleine Programm aus wie Hunderte anderer Varianten von Schadsoftware, die jedes Jahr entdeckt werden, weil sie sich wie eine Seuche von Computer zu Computer verbreiten. Einzig verwunderlich war, dass es, um sich zu verbreiten, einen Fehler in Microsofts Betriebssystem ausnutzte, den zuvor noch niemand bemerkt hatte. In der Sprache der Branche nennt man so etwas einen „Zero Day Exploit", einen Angriff, der besonders schlagkräftig ist, weil er seit null Tagen – also noch gar nicht – bekannt ist. Angreifbare Schwachstellen, die schon länger bekannt sind, werden meist vom Hersteller mit einem Software-Update behoben. Solange das noch nicht geschehen ist, können Antivirus-Programme, die täglich aktualisiert werden, Schadsoftware wie diesen Trojaner möglicherweise erkennen oder sogar am Einsatz hindern.

Bei Trojanern handelt es sich um kleine Programme, die verdeckt die Kontrolle über einen Computer übernehmen können, so wie die antiken Krieger aus dem Holzpferd die Stadt Troja listig von innen eroberten. Durch das Netz verbreiten sich täglich Dutzende neue Varianten von Trojanern, meist geschrieben und benutzt von Kriminellen, die so versuchen, an Konto-Zugangsdaten oder Passwörter für Online-Spiele zu gelangen. Üblicherweise verwenden sie dafür durchaus erfolgreich ältere Sicherheitslücken.

Das anfangs „LNK" genannte Problemprogramm wäre normalerweise bald in Vergessenheit geraten, die Durchschlagskraft des Angriffes, der für die Verbreitung dieses spezifischen Trojaners genutzt wurde, jedoch war aufsehenerregend. Sie zeigte sich, wenn ein Nutzer einen infizierten USB-Stick in einen Computer steckte, auch wenn dieser mit den bisher üblichen, vom Hersteller verordneten Sicherheitsmaßnahmen gegen einen Angriff über die USB-Schnittstelle geschützt wurde. Es genügt, den USB-Stick einfach nur einzustecken, und die Schadsoftware wird auf dem Computer – ganz ohne Zutun des Benutzers – heimlich installiert. Und das nicht nur, wie sonst bei Trojanern vielfach üblich, auf einer bestimmten Windows-Version. LNK funktionierte einfach überall, vom uralten Windows 2000 bis zu den allerneuesten, als relativ sicher angesehenen Versionen Windows Vista Plus und Windows 7.

> Eine Angriffs-Software mit dieser Durchschlagskraft hat die Welt noch nicht gesehen.

Üblicherweise sind Schwachstellen, aus denen man so zuverlässig funktionierende Angriffe konstruieren kann, sehr selten zu finden und werden daher in der entsprechenden Szene für einige hunderttausend Dollar gehandelt. Die Käufer sind zum einen Computer-Sicherheitsberater, die Hersteller der betroffenen Software, aber auch Geheimdienste und Regierungsstellen. Wenn man versuchen wollte, ein Äquivalent in der Welt der physischen Waffen zu finden, wäre LNK eine Haubitze, angewendet in einer Situation, für die auch eine Pistole ausreichen würde. Dass jemand ein derart wertvolles Werkzeug nicht verkauft, sondern für möglicherweise kriminelle Zwecke verwendet, ist äußerst ungewöhnlich, da etwa das Ausspähen von Kontoinformationen auch mit weitaus weniger großkalibrigen Mitteln zu erreichen wäre.

Die Neugier der Experten war geweckt. Bei der Analyse ergab sich ein Bild, ähnlich einer russischen Matroschka. Einmal über den USB-Stick auf den Computer gebracht, wird eine zweite Ebene im Programmcode des Trojaners aktiv, der ein kleines unauffälliges Programm tief in den Innereien des Betriebssystems installiert. Dazu wurde ein zweiter „Zero Day Exploit" verwendet. Immer, wenn die Experten eine Schicht der digitalen Matroschka entfernten, trat eine weitere, gut gegen ihre Analysemethoden geschützte Schicht des Programmcodes zutage. Die Analysen sind auch nach wochenlanger Arbeit noch nicht vollständig abgeschlossen.

Bisher förderte die Untersuchung vier großkalibrige „Zero Day Exploits" zutage. Zusätzlich dazu wurden zwei gestohlene digitale Unterschriften verwendet. Diese Signaturen dienen in modernen Betriebssystemen wie etwa Windows 7 dazu, dass zum Beispiel ein Hersteller von Graphikkarten die für seine Produkte nötige Software unterschreiben und damit bestätigen kann, dass sie echt und unschädlich sind. Das Betriebssystem prüft diese Unterschriften, um zu verhindern, dass sich Schadsoftware im sensiblen Inneren des Systems installieren kann. Die Schadsoftware, inzwischen „stuxnet" getauft, kam gleich mit zwei verschiedenen dieser Signaturen daher, gestohlen bei zwei taiwanischen Hardware-Herstellern. Das Betriebssystem hielt das stuxnet-Programm für unschädlich – es wies ja die richtige Unterschrift auf – und ließ es gewähren.

Diese Ballung und Qualität von Angriffsmethoden in einer einzigen Schadsoftware hatte es bis dahin nicht gegeben. Richtig nervös wurden die Experten und kurz danach diverse Regierungen, als klar wurde, wozu all dieser Aufwand getrieben wurde.

Die innerste Matroschka, die bisher analysiert wurde, enthält ein Programm zur gezielten Manipulation von Industrieanlagen. Großtechnische Anlagen werden heut-

zutage vollständig von Computern gesteuert. Industrielle Prozesse in Raffinerien, Chemie- oder Kraftwerken werden durch Computer so austariert, dass ihre Temperaturen, Drücke und Zusammensetzungen im kontrollierten, ungefährlichen Bereich gehalten werden. Software überwacht die Temperatur einer chemischen Reaktion und entsprechend auch Kühlung und Zufluss neuer Grundstoffe. Fehler und Manipulationen können zu ernsten Katastrophen führen. Die Herzen dieser Industrie-Computersteuerungen basieren häufig auf dem von Siemens entwickelten S-7-System. Es besteht aus vielen einzelnen Computer-Bausteinen, sogenannten speicherprogrammierbaren Steuerungen, kurz SPS. Sie überwachen jeweils eine Handvoll Messfühler – etwa elektronische Thermometer – und steuern Ventile, Motordrehzahlen oder den Durchsatz von Kühlwasserpumpen. stuxnet dient also einem einzigen Ziel: der verdeckten Installation einer Manipulationssoftware in einer Industrieanlage. Zwar gab es seit einigen Jahren Vorträge auf Sicherheitskonferenzen, in denen die Auswirkungen von Manipulationen dieser Industriesteuerungen – auch SCADA für „Supervisory Control and Data Acquisition" genannt – diskutiert wurden, aber in der freien Wildbahn wurden solche Angriffe bisher nicht beobachtet.

Nun kamen die spannenden Fragen: Gegen welche Anlagen richtet sich der Angriff? Wer steckt dahinter? Wo ist das eigentliche Ziel? Der Programmcode von stuxnet gibt einige spärliche Hinweise.

Jede Industriesteuerung ist hochgradig individuell. Sie wird vom Erbauer aus Hunderten vernetzten Einzelkomponenten zusammengestellt, entsprechend den Anforderungen der konkreten Anlage. Industriesteuerungen haben standardisierte grafische Oberflächen, die dann in der Leitwarte den Zustand der einzelnen Prozesse visualisieren und für den Bediener Möglichkeiten zum Eingriff in das Geschehen bieten. Die Software für diese Visualisierung der Parameter und die zentralisierte Programmierung der einzelnen kleinen SPS-Steuercomputer heißt bei Siemens WinCC und läuft unter Windows. stuxnet sucht nun von einmal infizierten Computern aus gezielt nach den WinCC-Installationen im gesamten Netz. Über diese gelingt dem Schadprogramm dann der Sprung auf die eigentlichen SPS-Steuercomputer der Anlage. stuxnet könnte – hier ist die Analyse noch nicht abgeschlossen – auch die Visualisierung der Anlagenparameter manipulieren. Das würde dazu führen, dass die gezielten Veränderungen an den Einstellungen der Anlage für den Bediener gar nicht sichtbar werden. Er hätte keine Chance mitzubekommen, dass etwas schiefläuft, bevor es zu spät ist. Üblicherweise sind nur noch wenige „echte" Messgeräte in Großanlagen installiert, die eine manuelle Überprüfung von Temperaturen oder Drehzahlen bieten. Die einzige Möglichkeit, alles im Blick zu behalten, sind die computerisierten Anzeigen. Und die wären im Falle der angegriffenen Anlage unter der Kontrolle der Schadsoftware.

> Alle Spuren deuten auf Iran als Ziel. Aber wer kann eine solche Waffe bauen?

Der extreme Aufwand, der von den Autoren von stuxnet getrieben wurde, schließt Hobbyhacker oder lumpige Cyber-Kriminelle aus. Die Entwicklung sowie der Ankauf der notwendigen Angriffskomponenten in dieser Qualität und Zuverlässigkeit verursachen Kosten im siebenstelligen Euro-Bereich. Auf vielen Ebenen stellt stuxnet sicher, dass die Verbreitung absolut zuverlässig und unbemerkt vor sich geht. Am Ziel angekommen, also auf einer passenden Siemens-Industrieanlage, stellen umfangreiche Überprüfungen sicher, dass wirklich nur die spezifische Anlage, auf die stuxnet zielt, manipuliert wird. Auf allen anderen Anlagen passiert – trotz heimlichen Festsetzens des Trojaners – nichts. Die Angreifer verfügten also über hochpräzise Informationen zum Aufbau der Anlage und der darin verwendeten Software. Ohne exakte Kenntnisse der Konstruktionsdetails und der Art des Zusammenwirkens der einzelnen S-7-Komponenten wäre ein Angriff dieser Präzision unmöglich. Angesichts dieses Aufwandes bleiben als Autoren nur Nationalstaaten übrig, die über entsprechende Ressourcen verfügen, um eine derart hochgezüchtete Cyber-Waffe zu entwickeln und zu testen – und zwar, bis sie nahezu nebenwirkungsfrei ist. „Cyber-Kriege" können aufgrund des nötigen langfristigen Entwicklungsaufwandes für die digitalen Angriffswerkzeuge de facto nur von Entitäten in der Größenordnung von Staaten geführt werden.

Wer also könnte diese Präzisionswaffe entwickelt, wer sie eingesetzt haben? Mit letzter Sicherheit weiß das nur der Auftraggeber. Es ist eine Kerneigenschaft von Computer-Netzwerkangriffen, dass die Identifikation des Urhebers eines kompetenten Angriffes fast unmöglich ist. Letztlich gestaltet sich die Suche anhand der technischen Indizien als das Tasten durch ein großes Spiegellabyrinth, in dem es keine verlässlichen Bilder gibt. Ähnlichkeiten im Programmierstil, in der Art des Aufbaus der Software können manchmal Anhaltspunkte bieten, so, wie man einen bestimmte Graffiti-Sprayer finden könnte, indem man nach Sprühereien sucht, die einen verwandten Stil aufweisen. Doch das ist immer eine unscharfe Methode, die auf dem Bauchgefühl der beteiligten Experten beruht, die aus langer Erfahrung und Kenntnis darüber, wer über die Talente für so einen Angriff verfügen könnte, unscharfe Schlüsse ziehen.

Auch bei der Suche nach dem möglichen Ziel des Angriffs ist man auf kleine Hinweise, zeitliche Korrelationen und Gerüchte angewiesen. Aus Gesprächen mit Insidern aus verschiedenen europäischen Ländern ergibt sich aber eine Indizienkette. Sechzig Prozent der Infektionen mit stuxnet wurden in Iran verzeichnet. Der Trojaner war so programmiert, dass er eigentlich im Januar 2009 aufhören sollte, sich weiter zu verbreiten. Offenbar durch Computer, auf denen das Datum nicht korrekt gesetzt ist – ein durchaus häufiges Vorgehen, um das Auslaufen von zeitgebundenen Software-Lizenzen zu umgehen –, verbreitete er sich trotzdem immer weiter, bis er schließlich entdeckt wurde.

Ausgehend von Anfang 2009 als Akti-

onsdatum, ergibt sich eine faszinierende Kette von Indizien. Mitte Juli 2009 publizierte Wikileaks eine kryptische Notiz mit dem Hinweis eines Informanten aus Iran auf einen nuklearen Unfall in Natanz, der sich kurz zuvor ereignet haben soll. In Natanz wird ein Großteil des iranischen Urans mit Hilfe von Zentrifugen angereichert. Die BBC meldete zur gleichen Zeit, dass der Leiter der iranischen Atombehörde, Gholam Reza Aghazadeh, zurückgetreten sei. Schon damals gab es Spekulationen über ein Einwirken im Rahmen des klandestinen Antiproliferationsprogrammes, das westliche Geheimdienste seit Jahren gegen den Iran betreiben. Die Dienste versuchen durch allerlei Methoden, das iranische Atomprogramm zu behindern und zu verzögern. Statistiken, die aus Daten der Internationalen Atomenergiebehörde erstellt wurden, legen nahe, dass nach dem Frühjahr 2009 die Zahl der tatsächlich betriebenen Anreicherungszentrifugen in Iran deutlich abgenommen hat, trotz Installation von immer mehr Zentrifugen. Ereignisse im Frühjahr 2009 haben die Kapazität des iranischen Anreicherungsprogrammes offenbar nachhaltig beschränkt. War stuxnet womöglich der Auslöser?

Anreicherungszentrifugen sind komplexe Präzisionsmaschinen, die eine sehr genaue Steuerung von Vakuum, Drehzahl und Gasfluss erfordern. Tausende Zentrifugen müssen in Serie geschaltet werden, um am Ende die nötige Anreicherung des spaltbaren Atommaterials zu erreichen. Ohne entsprechende Computersteuerung ist eine solche Anlage effektiv nicht zu betreiben. Die Analyse von stuxnet weist nun ein faszinierendes Detail auf: Ein Teil der Schadsoftware, die in die Steuerungsprozesse eingreift, scheint darauf ausgelegt, sich auf viele einzelne Steuercomputer in einem Netz zu verbreiten und die Schadensroutinen zeitlich zu synchronisieren. Der logische Weg zur Steuerung von vielen tausend Anreicherungszentrifugen ist es, jede mit einem kleinen separaten Steuercomputer zu versehen, der seine aktuellen Parameter über das Netz an die zentrale Überwachungseinheit meldet und von dort Kommandos empfängt. Das, was den Experten bisher über die Struktur der eigentlichen Schadenskomponente in stuxnet – der innersten Matroschka – bekannt ist, würde perfekt dazu passen.

Stuxnet: die erste von einem Nationalstaat eingesetzte Cyberwaffe der Geschichte?

Dass Iran gern Siemens-Industriesteueranlagen verwendet, ist aus verschiedenen Vorfällen bekannt, bei denen Exporte abgefangen wurden, die an Firmen gehen sollten, die dem iranischen Nuklearkomplex zugeordnet werden. Dass die Manipulation solcher Steueranlagen zu katastrophaler Sabotage genutzt werden kann, wurde spätestens im März 2007 klar, als ein Team am Idaho National Laboratory in den Vereinigten Staaten mit Hilfe eines Computerangriffes einen Kraftwerks-Stromgenerator im eigenen Labor gezielt zerstörte. Ein Video dieses Versuchs wurde im September des gleichen Jahres publik und löste eine kleine Welle von Panik angesichts der Verwundbarkeit der Infrastrukturen im Westen aus. Möglicherweise liegt hier auch die Keimzelle der Idee, das iranische Anreicherungsprogramm per Computerangriff zu sabotieren.

Bleibt die Frage, wie die Angreifer in den Besitz der notwendigen Detailkenntnisse, inklusive Zugang zur Software der angegriffenen Anlage, kamen. Ohne perfekte Informationen über das Ziel wäre die aus der Analyse von stuxnet ersichtliche Schadensfunktion nicht realisierbar. Denkbar wäre, dass einer der diversen iranischen Überläufer, die in den letzten Jahren in den Westen kamen, die notwendigen Daten mitbrachte. Denkbar ist auch, dass die Informationen von Agenten vor Ort erlangt wurden. Der ungewöhnliche, aber spezifisch für stuxnet gewählte Verbreitungsweg legt nahe, dass für den Angreifer zumindest die Möglichkeit bestand, einen USB-Stick irgendwo im Umfeld der Zielanlage in einen Computer stecken zu lassen. Möglicherweise war der Informant auch in der Lage, die Blaupausen und Konfigurationsinformationen zu besorgen.

stuxnet wird wohl als erste offensichtlich von einem Nationalstaat eingesetzte Cyberwaffe in die Geschichte eingehen. Einer der Gesprächspartner beschrieb Qualität und Aufwand der Erstellung des Trojaners mit den Worten: „So etwas bauen große Staaten zusammen, wenn die Alternative bei einem Misserfolg wäre, einen Krieg anzufangen." Mit den üblichen Mitteln der IT-Sicherheit ist eine Verteidigung gegen derartige Angriffsmethoden nicht möglich. Es lässt sich wohl kaum ausschließen, dass kritische Systeme nicht einmal mit einem potentiell infizierten USB-Stick – zum Beispiel mit einem Software-Update des Herstellers – in Berührung kommen. Die von den deutschen Energieversorgern dieser Tage vorgebrachten Beteuerungen, ihre Atomkraftwerke könnten auf keinen Fall durch einen Angriff in der Art von stuxnet manipuliert und mit möglicherweise katastrophalen Folgen konfrontiert werden, erscheinen angesichts der Qualität und Durchschlagskraft dieses Trojaners wie das Pfeifen im Walde. Die Kriterien zur Beurteilung der Sicherheit von Atomanlagen können sich zukünftig jedenfalls nicht mehr nur auf die Dicke von Betonhüllen und Tests der Elektrik beschränken.

Quelle: FAZ vom 22.9.10