HIRSCHMANN
A BELDEN BRAND

HOPF
PARTNER | SOLUTIONS | COMPONENT

Technical Bulletin

TB 1002HG

Hirschmann™ EAGLE20 Tofino™

Einsatz von EAGLE20 Tofino™ zur Eindämmung des Schadprogramms Stuxnet

In diesem Anwendungshinweis wird die Verwendung der industriellen Sicherheitslösung EAGLE20Tofino beschrieben, mit der die Verbreitung des Stuxnet-Wurms in Siemens-Netzwerken und anderen Netzwerkumgebungen verhindert werden kann

Was ist Stuxnet?

Stuxnet ist ein Computer-Wurm, der insbesondere industrielle Systeme befällt, die Siemens SPS (Speicherprogrammierbare Steuerungen) verwenden. Ziel dieses Schadprogramms ist die Zerstörung bestimmter industrieller Prozesse.
Stuxnet infiziert Windows-basierte Computer auf einem beliebigen Steuerungs- oder SCADA-System. Dabei spielt es keine Rolle, ob es sich um ein System von Siemens oder um ein anderes System handelt. Der Wurm wird nicht versuchen, Änderungen an Steuerungen vorzunehmen, die keine SPS des Typs S7-300 oder S7-400 sind. Der Wurm verhält sich aber auch in allen Netzwerken äußerst aggressiv und kann auf jedem Steuerungssystem zu negativen Auswirkungen führen. Infizierte Computer können auch als Ausgangsbasis für künftige Angriffe dienen.

Wie verbreitet sich Stuxnet?

Stuxnet ist einer der komplexesten und am besten programmierten Würmer. Er nutzt mindestens vier Zero-Day-Schwachstellen aus, besitzt mehrere Ausbreitungswege und hat besonders ausgeklügelte Mechanismen für die Ausnutzung von Siemens-Steuerungssystemen.
Eine essentielle Herausforderung bei der Vermeidung von Stuxnet-Infektionen sind die zahleichen Wege, die dieser Wurm für den Befall anderer Computer anwendet. Der Wurm breitet sich über die folgenden drei Hauptpfade aus:

1. über infizierte USB-Wechsellaufwerke
2. über LAN-Verbindungen
3. über infizierte Siemens-Projektdateien

Auf diesen drei Pfaden nutzt der Wurm sieben unabhängige Mechanismen für den Befall anderer Computer. Stuxnet besitzt außerdem ein P2P-Netzwerksystem (Peer-to-Peer), das automatisch alle vorhandenen Installationen des Stuxnet-Wurms aktualisiert, selbst wenn diese keine Rückverbindung zum Internet herstellen können. Zudem verfügt Stuxnet über einen Internet-basierten Befehls- und Steuerungsmechanismus, der derzeit zwar deaktiviert ist, in Zukunft jedoch jederzeit aktiviert werden könnte.

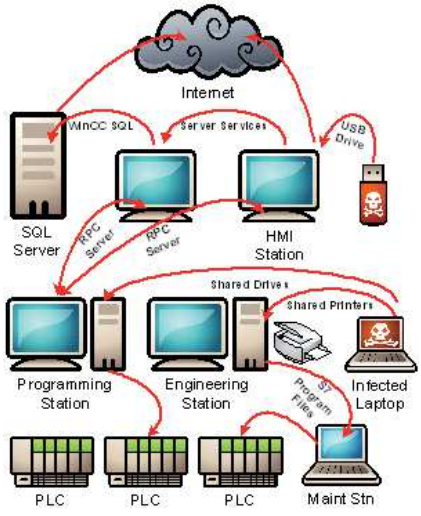

Abbildung 1: Verschiedene Pfade für Stuxnet-Infektionen

Ein weit verbreiteter Irrglaube ist, dass mit der Verhinderung von Infektionen über das USB-Laufwerk das Risiko eines Stuxnet-Befalls gleich Null ist. Dem ist aber leider nicht so. Durch die Vielfalt der Angriffsformen ist es äußerst schwer, die Verbreitung von Stuxnet unter Kontrolle zu halten. Wirkungsvolle Sicherheit kann dabei nur mit einem mehrschichtigen Konzept erreicht werden. Ein solches Sicherheitskonzept muss alle Pfade von Stuxnet berücksichtigen, also alle über USB, Netzwerk und Projektdateien ausgelösten Infektionen. Im Mittelpunkt dieses Anwendungshinweises steht die Vermeidung von Infektionen über das Netzwerk. Aber auch für andere Pfade werden Anleitungen und Empfehlungen bereitgestellt.

Vermeidung von Infektionen über USB

Stuxnet infiziert Computer über USB-Laufwerke (auch wenn AutoRun deaktiviert ist) anhand einer bisher unbekannten Schwachstelle in Windows-Verknüpfungen (d.h. *.lnk-Dateien). Die meisten Analytiker sehen darin den Ausgangspunkt für neue Infektionen. Aber auch andere Mechanismen, wie z.B. infizierte Laptops, kommen hierbei in Frage. Informationen über die Vermeidung von Infektionen über USB finden Sie im White Paper "Analysis of the Siemens WinCC / PCS7 "Stuxnet" Malware for Industrial Control System Professionals" unter http://www.tofinosecurity.com.

Vermeidung von Infektionen über das Netzwerk

Viele Stuxnet-Analytiker haben wiederholt darauf hingewiesen, wie schwierig es ist, den Wurm von einem infizierten Steuerungssystem zu entfernen. Wenn Stuxnet einen Eingang gefunden hat, verbreitet er sich äußerst aggressiv über lokale Netzwerke (LAN) zu anderen Computern. Sicherheitsexperten stimmen darin überein, dass die wirkungsvollste Methode für die Vermeidung einer schnellen Ausbreitung die Verwendung von zonenbasierten Verteidigungsmechanismen ist, die in den Normen ANSI/ISA99.02.01 und IEC63443 beschrieben werden. Dahinter steht die Idee, das Netzwerk in Sicherheitszonen aufzuteilen. Zwischen den Zonen werden Industrie-Firewalls installiert, auf denen mittels spezifischer Regeln die Protokolle blockiert werden, die Stuxnet für Infektionen und für die Kommunikation verwendet. Sollte es doch einmal zu einer Stuxnet-Infektion kommen, ist mit dieser Vorgehensweise gewährleistet, dass nur eine kleine Anzahl von Systemen in einer einzelnen Zone davon betroffen ist.

Aufteilung des Steuerungsnetzwerks in Sicherheitszonen

Der erste Schritt bei der Vermeidung von Stuxnet-Infektionen ist die Aufteilung des Steuerungssystems in Zonen. Eine Zone ist einfach eine Gruppierung von Ressourcen, für die die gleichen Sicherheitsanforderungen im Hinblick auf Faktoren wie Steuerungsfunktion, operative Anforderungen und Prioritätsstufe gelten. Die einfachste Lösung ist dabei die Erstellung der folgenden Zonen basierend auf dem ISA-95/Purdue-Modell:

1. SIS-Zone (Safety Integrated System)
2. Basissteuerungs-/PLC-Zone
3. Überwachungs-/HMI-Zone
4. Prozessinformations-/Data-Historian-Zone
5. IT-Netzwerkzone

Sicherheitsverletzungen in diesen Systemen haben unterschiedliche Folgen. Daher sollten diese auch getrennt behandelt werden. Zur Erhöhung der Sicherheit und Zuverlässigkeit können diese Primärzonen in weitere Unterzonen basierend auf den operativen Funktionen unterteilt werden. Die schrittweise Erhöhung der Anzahl an Zonen grenzt die Verbreitung von Stuxnet auf weniger Computer ein. Damit können die Risiken und die Kosten für die Beseitigung von Infektionen deutlich reduziert werden.

Installation der EAGLE20 Tofino Security Appliances

Nach der Definition der Zonen werden zwischen den Zonen EAGLE20 Tofino Security Appliances installiert, um den Netzwerkverkehr auf die Daten zu beschränken, die für den Betrieb des Systems erforderlich sind. Abbildung 2 zeigt eine typische Implementierung in einer Erdölraffinerie.

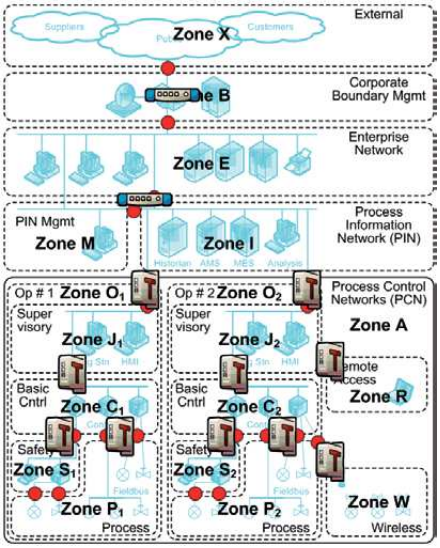

Abbildung 2: Installation von EAGLE20 Tofino Appliances zwischen den operativen Zonen

Blockierung der von Stuxnet verwendeten Protokolle

In die zwischen den Zonen installierten EAGLE20 Tofino Appliances müssen die entsprechenden Loadable Security Modules (LSMs) geladen werden. Im Fall von Stuxnet werden die folgenden Module empfohlen

1. EAGLE20 Tofino Firewall LSM
2. EAGLE20 Tofino Secure Asset Management LSM
3. EAGLE20 Tofino OPC Enforcer LSM
4. EAGLE20 Tofino Event Logger LSM

Wenn die LSMs geladen sind, werden die einzelnen Appliances so konfiguriert, dass die von Stuxnet verwendeten Protokolle bei der Kommunikation zwischen den Zonen blockiert werden. Insbesondere geht es dabei um die drei Protokolle für den Web-Datenverkehr (HTTP), den RPC-Datenverkehr (Remote Procedure Call) und, in Siemens-Systemen, den MSSQL-Datenverkehr.

Blockierung des ausgehenden HTTP-Datenverkehrs

Die einfachsten Datenverkehrsströme, die blockiert werden müssen, sind die HTTP-Nachrichten, die Stuxnet für die Rückverbindung zu seinem Befehlszentrum im Internet verwendet. Die EAGLE20 Tofino Firewall blockiert standardmäßig alle Protokolle. Wenn also HTTP im Steuerungssystem nicht unbedingt benötigt wird, sollte es zwischen den Zonen

blockiert bleiben. Wird HTTP benötigt (um beispielsweise der IT den Zugriff auf einen Data Historian zu ermöglichen), sollte es nur für den betreffenden Web-Server und nur für eingehende Zugriffe freigegeben werden. Abbildung 3 zeigt die typischen Regeln, mit denen verschiedenen IT-Clients der Zugriff auf den Data Historian per Web-Datenverkehr ermöglicht wird. Beachten Sie, dass die Richtung auf "Eingehend" gesetzt ist.

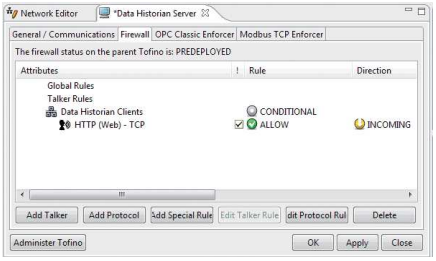

Abbildung 3: Beschränkung der HTTP-Web-Client-Nachrichten auf den Data Historian Server

Blockierung des RPC-Datenverkehrs

SRPC wird von Stuxnet umfassend genutzt, die Kontrolle dieses Protokolls ist daher essentiell. Wie bereits erwähnt, blockiert die EAGLE20 Tofino Firewall standardmäßig alle Protokolle. Wenn also RPC nicht benötigt wird, kann EAGLE20 Tofino mit den Standard-einstellungen verwendet werden, um den RPC-Datenverkehr von Stuxnet zwischen den Zonen zu blockieren.

Leider ist das nur selten so einfach. Das RPC-Protokoll wird nämlich auch für die Datei- und Druckerfreigabe von Windows, für das Microsoft Event Log, für OPC Classic und für verschiedene andere kritische Dienste verwendet. Wird der gesamte RPC-Datenverkehr blockiert, kann das daher negative Auswirkungen für den industriellen Prozess haben.
Um die Auswirkungen auf das Steuerungssystem so gering wie möglich zu halten, wird eine Kombination aus freigegebenen und blockierten RPC-Ports empfohlen. Alle standardmäßigen Varianten des RPC-Protokolls sind im Protokollsatz von EAGLE20 Tofino enthalten und können bei Bedarf einfach per Drag & Drop eingebunden werden.
Als ersten Schritt zur Vermeidung der Ausbreitung von Stuxnet über das Netzwerk müssen die Protokolle NetBIOS Session Service und Server Message Block (TCP-Ports 139 und 445) entweder vollständig blockiert oder nur für bestimmte Server freigegeben werden. Damit wird aber auch die Datei- und Druckfreigabe zwischen den Zonen unterbunden, weshalb diese Regeln nur nach sorgfältiger Überlegung anzuwenden sind.
Wenn die Protokolle NetBIOS Session Service und Server Message Block freigegeben werden müssen, können spezifische Regeln festgelegt werden, um den Datenverkehr auf die entsprechenden Server zu beschränken. Beispielsweise verwaltet der Dienst Event Log die Nachrichten, die von den Programmen und vom Windows-Betriebssystem erzeugt werden. Dieser Dienst nutzt dieselben Protokolle wie Stuxnet. Eine vollständige Blockierung dieser Protokolle ist daher nicht ratsam. Jedoch ist es möglich, diese Protokolle nur für einen bestimmten Event Log Server unter Verwendung von ähnlichen Regeln wie in Abbildung 4 freizugeben. In diesem Fall erlaubt eine globale Regel (Global Rule) den RPC-Datenverkehr zum Event Log Server. Alle anderen RPC-Nachrichten werden standardmäßig blockiert.

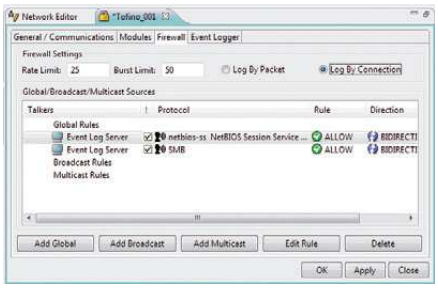

Abbildung 4: Beschränkung von SMB- und NetBIOS-Session-Service-Nachrichten auf den Event Logging Server

Ähnliche Regeln werden unter Umständen auch für Druck- und Dateiserver benötigt. Das Ziel ist es nicht, den unkontrollierten RPC-Datenverkehr zu allen Computern zu erlauben, sondern den Datenverkehr auf spezifische Server zu beschränken, die jederzeit auf dem aktuellen Patch-Stand sind und umfassend auf Infektionen überwacht werden.
Der NetBIOS Name Service (UDP-Port 137) und der NetBIOS Datagram Service (UDP-Port 138) kann bei Bedarf freigegeben werden, da Stuxnet diese Dienste offensichtlich nicht verwendet. Das ermöglicht die Suche nach Computer basierend auf dem Namen, jedoch nicht die Dateifreigabe.

Wenn OPC Classic-Datenverkehr anfällt, muss für dessen Verwaltung das Modul EAGLE20 Tofino OPC Enforcer™ verwendet werden. Die Kerntechnologien von OPC Classic, also RPC und DCOM, wurden entwickelt, bevor ein umfassendes Verständnis im Bereich Sicherheit vorhanden war. Deshalb verwendet OPC Classic die Technologie der dynamischen Portzuweisung, für die mit Hilfe herkömmlicher IT-Firewalls kein effizienter Schutz möglich ist. Der Grund dafür ist, dass OPC-Server im Gegensatz zu den meisten anderen Netzwerkanwendungen (z.B. Web-Server oder Modbus-TCP-Slave) TCP-Portnummern dynamisch jedem ausführbaren Prozess zuweisen, der Objekte für Clients bereitstellt. Die OPC-Clients ermitteln dann die Portnummern, die einem bestimmten Objekt zugewiesen wurden, indem sie eine Verbindung zum Server herstellen und nachfragen, welcher TCP-Port verwendet werden soll. Da OPC-Server jede beliebige Nummer zwischen 1024 und 65535 frei verwenden können, ist OPC äußerst „Firewall-unfreundlich". Denn wenn die Firewall so konfiguriert wird, dass diese unzähligen Ports offen sind, entsteht ein ernsthaftes Sicherheitsleck. In der Praxis gilt diese Vorgehensweise daher als inakzeptabel.
Dieses Problem kann mit dem EAGLE20 Tofino OPC Enforcer aus der Welt geschafft werden. Dieses Modul wendet ein spezielles Verfahren – die so genannte Deep Packet Inspection – an, um die dynamische Port-Nutzung von OPC Classic nachzuverfolgen und zu koordinieren. Die Firewall kann in jedem Netzwerk installiert werden, in dem OPC DA-, HDA- oder A&E-Datenverkehr übertragen wird. An den vorhandenen OPC-Clients und -Servern müssen keine Änderungen vorgenommen werden.
Wenn Sie EAGLE20 Tofino OPC Enforcer so konfigurieren möchten, dass Datenverkehr zwischen einem OPC-Server und einem OPC-Client übertragen werden darf, öffnen Sie das Firewall-Register des entsprechenden OPC-Servers. Ziehen Sie dann das Symbol des OPC-Clients per Drag & Drop auf die Liste Server Talkers, wählen das Protokoll "OPC Classic" und ändern die Regel von "Allow" zu "Enforcer". Abbildung 5 zeigt diese Einstellungen. Ausführliche Informationen finden Sie im Anwendungshinweis AN-105 "Protecting OPC Systems Using the Tofino OPC Enforcer".

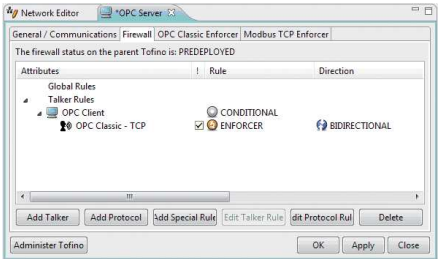

Abbildung 5: Verwenden von OPC Enforcer zur Koordinierung des OPC-Datenverkehrs zwischen einem Client und einem Server

Blockierung des MSSQL-Datenverkehrs

Bei Verwendung von WinCC-Produkten von Siemens kann Stuxnet Computer infizieren, indem die "internen" Kennwörter des Siemens-Systems für die Anmeldung am WinCC SQL-Server verwendet werden. Anschließend überträgt Stuxnet eine Kopie von sich an den Server und führt diese lokal aus.
Die beste Lösung wäre in diesem Fall, den gesamten MSSQL-Datenverkehr im Netzwerk zu blockieren. Das ist jedoch nicht empfehlenswert, da die WinCC-Clients dadurch keine Prozessinformationen mehr erhalten könnten. Stattdessen werden Anwender von WinCC angewiesen, das aktuellste SIMATIC Security Update von der Siemens-Website zu installieren.

Testen der Firewall-Konfigurationen

Da Stuxnet viele Protokolle verwendet, die auch von Anwendungen des Steuerungssystems genutzt werden, muss besonders sorgfältig darauf geachtet werden, dass der industrielle Prozess durch die Firewall-Regeln nicht gestört wird.
Glücklicherweise bietet die Sicherheitslösung EAGLE20 Tofino einen speziellen Testmodus. In diesem Modus wird der gesamte Netzwerkverkehr zugelassen und der Datenverkehr, der im normalen Betriebsmodus von der Firewall blockiert werden würde, wird dokumentiert. Die entsprechenden Berichte werden als ein Firewall-Ausnahmealarm in der Ereignisansicht (Event View) der EAGLE20 Tofino Central Management Platform (CMP) dargestellt und außerdem vom Event Logger LSM (sofern installiert) aufgezeichnet.

Mit dem Testmodus können die Firewall-Regeln sorgfältig geprüft werden, ohne versehentlich Datenverkehr zu blockieren, der eigentlich zugelassen werden soll. Damit werden negative Auswirkungen auf die industriellen Betriebsabläufe verhindert. Wir empfehlen, alle EAGLE20 Tofino-Installationen mindestens 24 Stunden lang im Testmodus zu betreiben, bevor sie in den Betriebsmodus übernommen werden.

WARNUNG:
Klären Sie jede Gegenmaßnahme vor der Implementierung auf einem aktiven Steuerungssystem mit dem Systemhersteller ab und führen Sie einen Test auf einem nicht kritischen System durch.

Erkennen von Stuxnet-Infektionen

Sobald die EAGLE20 Tofino Appliances implementiert, konfiguriert und gestestet sind, dienen sie als hervorragende "Spürhunde" und warnen zuverlässig vor einer drohenden Infektion. Stuxnet erzeugt eine enorme Menge an Ereignis-Datenverkehr, der entweder mit der EAGLE20 Tofino CMP oder mit dem EAGLE20 Tofino Event Logger LSM erfasst werden kann. Insbesondere die Versuche von Stuxnet, externe Web-Server zu kontaktieren, sind gute Hinweise auf eine Infektion.

Zusätzliche Hinweise für Siemens WinCC- und PCS7-Anwender

Siemens WinCC und PCS7 nutzen sehr häufig RPC für die Kommunikation zwischen verschiedenen WinCC-Servern und -Clients. Eine Blockierung der gesamten RPC-Kommunikation zwischen Zonen kann daher dazu führen, dass der Überblick oder die Kontrolle verlorengeht. Mit dem Testmodus von EAGLE20 Tofino kann bestimmt werden, welche Regeln für die Freigabe des Siemens RPC-Datenverkehrs benötigt werden.

Benutzer von Siemens-Produkten sollten sich vor der Anwendung von Firewall-Regeln an ihren Siemens-Ansprechpartner wenden oder das Siemens-Dokument "Security concept PCS 7 and WinCC" lesen.

Weitere Informationen

Im Folgenden werden Informationen zu weiteren Methoden für die Eindämmung von Stuxnet bereitgestellt:
Überblick über die Maßnahmen gegen Stuxnet (Stuxnet Mitigation Matrix):
http://www.tofinosecurity.com/professional/stuxnet-mitigation-matrix

Analyse der Siemens WinCC / PCS7 "Stuxnet"-Malware für Experten für Steuerungssysteme:
http://www.tofinosecurity.com/professional/siemens-pcs7-wincc-malware

Informationen von Siemens zu Schadprogrammen:
http://support.automation.siemens.com/WW/view/en/43876783

Zusammenfassung

Stuxnet ist ein komplexer und aggressiver Computerwurm, der Computer in beliebigen Steuerungssystemen infizieren kann. Die Vermeidung einer Infektion ist nicht nur für Siemens-Produkte von essentieller Bedeutung. Auch für andere Produkte und Systeme können negative Auswirkungen entstehen. Die Verhinderung einer Ausbreitung von Stuxnet über Steuerungsnetzwerke ist Grundvoraussetzung für sichere und zuverlässige industrielle Systeme. Mit der Sicherheitslösung EAGLE20 Tofino können die Auswirkungen des Stuxnet-Virus auf ein Minimum reduziert werden. Gleichzeitig wird Ihr industrielles Netzwerk zuverlässig vor zahleichen anderen schädlichen Angriffen geschützt.

Phone **+49 (0) 7127/14-1809**
www.beldensolutions.com