

Bild 1: Schadsoftware-Infektionen werden mit dem industrietauglichen mGuard CIFS Integrity Monitoring Verfahren zuverlässig erkannt.

Windows-basierte Automatisierungskomponenten

Integritätsüberwachung zum Schutz gegen Schadsoftware

Automatisierungskomponenten mit Windows-Betriebssystemen sind weit verbreitet und durch eine Fülle von Schadsoftware bedroht. Insbesondere die zum Datenaustausch häufig genutzten Windows-Dateifreigaben auf Basis der Protokollfamilie CIFS/SMB (Common Internet File System / Server Message Blocks) sind ein gefürchtetes Einfallstor für Infektionen. Konventionelle Antivirus-Lösungen sind im industriellen Umfeld meist nicht einsetzbar. CIFS Integrity Monitoring ist eine innovative, industrietaugliche Lösung, mit deren Hilfe die Dateisysteme auf unerwartete Modifikationen von ausführbarem Code überwacht werden.

Vernetzte industrielle Automatisierungskomponenten mit Microsoft Windows Betriebssystemen sind heute weit verbreitet und wie ihre Pendanten in Büronetzen leider durch regelmäßig neu entdeckte Sicherheitslücken und eine Fülle von Schadsoftware gefährdet. Während dabei klassische Viren, die zu ihrer Verbreitung eine passende Wirtsapplikation benötigen, eine allgemein abnehmende und im industriellen Umfeld eher geringe Bedeutung haben, nimmt die Gefährdung durch Würmer und Trojaner, die aus eigener Kraft weitere Systeme befallen können, beständig

zu. Ein aktuelles Beispiel ist der sich seit Oktober 2008 aggressiv verbreitende Win32/Conficker Wurm, der seit Frühjahr 2009 auch industrielle Anlagen befallen und zum Stillstand gezwungen hat. Er blockiert Dienste wie Windows Update, Windows-Sicherheitscenter, Windows Defender und das Windows Systemprotokoll, um seine eigene Entfernung möglichst zu verhindern, und kann sich durch Nachladen von Code aus dem Netz selbst verändern. Insbesondere die häufig zum Datenaustausch mit der Umgebung genutzten Windows Dateifreigaben auf Basis der Protokollfamilie CIFS/SMB (Common In-

ternet File System / Server Message Blocks) sind ein gefürchtetes Einfallstor für Schadsoftware, welches auch der Conficker Wurm für seine Verbreitung nutzt. Regelmäßiges Einspielen von Sicherheits-Updates für das Betriebssystem – sofern überhaupt noch verfügbar und praktiziert – ist allein kein ausreichender Schutz gegen derlei Infektionen. Der als Defense-in-Depth-Strategie bekannte Einsatz von dezentralen Firewalls vor den zu schützenden Systemen kann das Risiko einer Infektion durch konsequente Beschränkung der überhaupt zulässigen Verbindungen im Netzwerk auf das notwendige



Bild 2: Industrie-PCs und eingebettete Komponenten auf Basis von Windows-Betriebssystemen sind in der industriellen Automatisierung weit verbreitet.

Maß immerhin stark reduzieren. Verbindungen über tatsächlich genutzte Protokolle und deren Ports müssen aber natürlich auch durch diese Firewalls hindurch möglich bleiben und stellen damit ein Restrisiko für das Eindringen von Schadsoftware dar.

Konventionelle Lösungen industriell nicht geeignet

Eine lokale Installation von Antivirus-Software ist auf industriellen Komponenten meist ausgeschlossen. Zum einen bieten die in der Regel unter

Kostendruck sparsam dimensionierten Hardware-Ressourcen dafür nicht genug Reserven an Speicher und CPU-Leistung. Zum anderen kann derlei Scan-Software ein recht ungewisses Echtzeitverhalten verursachen – für Office-Anwender vielleicht nur eine lästige Erfahrung, industriell jedoch nicht akzeptabel. Wer es dennoch versucht, sieht sich nicht selten konfrontiert mit eingefrorenen Bedienoberflächen und Systemen, die vor lauter Sicherheit ihre eigentliche Nutzfunktion verloren haben. Ein externes Scannen von Netzwerkverkehr auf Malware-Signaturen durch vorgeschaltete Network Security Appliances, wie es bislang etwa für Sicherheitsgeräte mit der Innominate mGuard Firmware angeboten wurde, bleibt aus technischen Gründen leider auf einige wenige dafür geeignete Protokolle (http, ftp, smtp, pop3) beschränkt. Ausgerechnet das so weit verbreitete Windows File Sharing Protokoll CIFS/SMB lässt sich infolge seiner blockweisen Datenübertragung auf diese Weise nicht filtern. Allen Scan-Methoden gemeinsam ist ferner der Bedarf nach entsprechenden Mustern bzw. Signaturen. Diese umfangreichen und schnell weiter wachsenden Signaturdatenbanken durch ständige Updates auf den Geräten aktuell zu halten ist schon für sich eine technisch-organisatorische Herausforderung und potentielle Quelle von Instabilitäten. Nicht oft, aber doch immer wieder kommt es mit den (neuen) Signaturen zu so genannten 'False Positives', also Fehlalarmen zu vermeintlichen Schädlingen, die gar keine sind. Werden Kommunikation und Produktion aufgrund solcher Fehlalarme unnötig unterbrochen, wird die erhoffte Sicherheit schnell zum wirtschaftlichen Ärgernis.

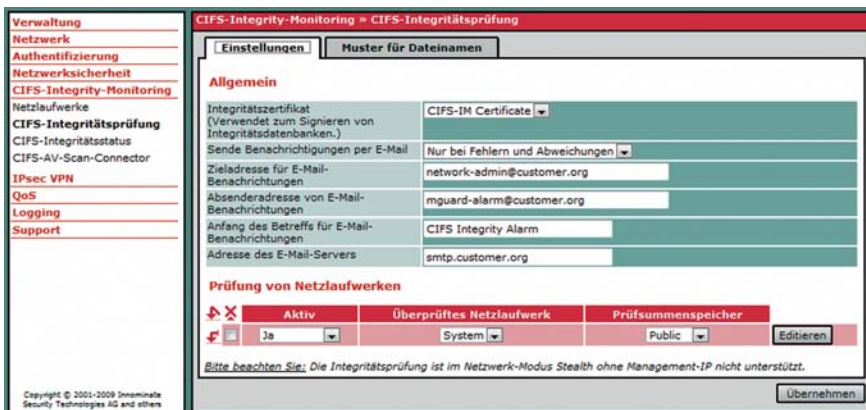


Bild 3: Konfiguration des mGuard CIFS Integrity Monitoring Verfahrens zur Überwachung eines Windows System-Verzeichnisses

CIFS Integrity Monitoring

Als innovative, industrietaugliche Lösung für die geschilderten Probleme hat Innominate das neuartige CIFS Integrity Monitoring entwickelt. Es besteht aus zwei Komponenten: dem CIFS Antivirus Scan Connector, mit dem Windows Netzwerkordner von einem externen Virens Scanner analysiert werden können, und dem CIFS Integrity Checking Verfahren, welches Dateisysteme auf unerwartete Modifikationen oder Hinzufügungen von Programmen, DLLs oder anderem ausführbaren Code überwacht. Letzteres ba-



Bild 4: Netzwerksicherheit für industriell eingesetzte Windows-Systeme lässt sich mit den Innominate mGuard Security Appliances transparent und kostengünstig in verschiedenen Bauformen nachrüsten.

siert allein auf der eigenständigen Berechnung und Überwachung von Hashcode-Signaturen für alle relevanten Dateien und kommt daher ohne externe Signaturdatenbanken und deren ständige Aktualisierung aus. Die Berechnungen selbst erfolgen ressourcenschonend auf einer vorgeschalteten mGuard Network Security Appliance. Die überwachten Windows Clients müssen lediglich die zu prüfenden Dateien bereitstellen und die dazu berechneten Signaturen speichern, was sie nur moderat belastet. Entdeckte Integritätsverletzungen lösen per E-Mail oder SNMP einen Alarm an den Administrator oder ein Netzwerkmanagementsystem aus. Über den Antivirus Scan Connector kann dann eine gezielte Überprüfung der beanstandeten Datei(en) mithilfe eines externen Antivirus-Scanners erfolgen, um die gemeldete Infektion genauer zu identifizieren und zu bereinigen oder als Fehlalarm zu erkennen. Netzwerkordner, die dem laufenden Datenaustausch dienen und sich daher ständig verändern, können über den Connector auch nach einem festen Zeitplan regelmäßig durch einen externen Scanner überprüft werden. Dabei werden dem Scanner nur Leserechte unter einer zusätzlichen Sammelkennung für alle angeschlossenen Netzlaufwerke eingeräumt. Die einzelnen tatsächlichen Kennungen mit Lese- und ggf. Schreibrechten für die jeweiligen Verzeichnisse werden nur dem Connector bekannt gemacht. Industrielle Network Security Appliances mit der mGuard CIFS Integrity Monitoring Technologie von Innominate lassen sich kostengünstig und punktgenau dezentral dort einsetzen, wo sie aus den hier diskutierten Gründen benötigt werden, und das nicht nur als Router. Im so genannten Stealth Mode lassen sich die Geräte auch völlig transparent in ein bestehendes Netzwerk nachrüsten. Mit ihrer integrierten Stateful Packet Inspection Firewall über-

wachen und filtern sie anhand eines konfigurierbaren Regelwerks außerdem den Netzwerkverkehr von und zu den geschützten Systemen, und dies dank bidirektionalem 'Wire Speed' ohne zum Flaschenhals für ein 100MBit/s Ethernet-Netzwerk zu werden. Die Geräte können durch eine flexible, skriptbare Flash- und Rollout-Prozedur sehr effizient ausgerollt und sowohl einzeln über ein integriertes Web Interface als auch gemeinsam zentral über den Innominate Device Manager verwaltet werden.

Fazit

Das dargestellte CIFS Integrity Monitoring Verfahren kann zwar nicht den Echtzeitschutz eines lokal installierten Scanners bieten und Infektionen mit Schadsoftware aktiv verhindern, leistet aber unter den gegebenen Umständen das Bestmögliche. Es lässt Infektionen nicht lange unentdeckt bleiben und riskiert nicht, kritische Kommunikation aufgrund von 'False Positive'-Fehlalarmen zu unterbrechen und die Produktion damit unnötig stillzulegen. Ferner findet es sogar Schäden von so genannten Zero Day Exploits, für die es noch gar keine Malware-Signaturen gibt. Es stellt damit eine industrietaugliche Alternative für den Schutz Windows-basierter Komponenten dar, auf denen konventionelle Antivirus-Lösungen nicht eingesetzt werden können. ■

www.innominate.de



Autor: Torsten Rössel, Director Business Development, Innominate Security Technologies AG