3 | 17 Sonderdruck für SecuLution

IT Administrator

Das Magazin für professionelle System- und Netzwerkadministration

Test:

SecuLution

www.it-administrator.de

SecuLution

Erlauben statt verbieten

von Sandro Lucifora

Sich um die Sicherheit eines Netzwerks zu kümmern, ist mittlerweile mühsamer, als es stabil am Laufen zu halten. Die meisten Administratoren setzen dabei auf Standardtechnologien wie Virensignaturen. Im Test von SecuLution haben wir herausgefunden, dass sich der Aufwand mit einem einfachen Mittel wie Whitelisting um ein Vielfaches verringern lässt.

Quelle: LIU MING – 123RF

Mit Internet und E-Mails etablierten sich neue Gefahren für ein Unternehmensnetzwerk. Hacker versuchen, sich Zugang zu verschaffen, und Viren wollen das Netzwerk infizieren. Mit dem Auftauchen von Ransomware erreichte die Bedrohung von außen neue Dimensionen. Aber auch Gefährdungen von innen verdienen die Beachtung von Administratoren. Kollegen etwa, die an ihrem Rechner der Sicherheits-Policy zuwiderhandeln, verursachen oft schwerwiegende Schäden. Und dabei muss noch nicht mal ein böser Vorsatz vorhanden sein.

Schutztechniken aus den 80er Jahren

Um den geschilderten Bedrohungen Herr zu werden, setzen Unternehmen vorrangig auf Virenscanner. Dabei handelt es sich um eine Technologie der frühen 80er Jahre des letzten Jahrhunderts. Dieser Schutzmechanismus prüft, ob Daten bekannt sind oder sicher erscheinen. Um erlaubte, aber unbekannte Daten nicht ungewünscht zu blockieren, betreiben die Hersteller dieser Software einen hohen Aufwand. Sie erstellen Signaturen und entwickeln Algorithmen, die herausfinden sollen, ob Daten "gut" oder "böse" sind – im Grunde ein Ratespiel mit Wahrscheinlichkeitsrechnungen.

Um den Betrieb von unerwünschter Software einzuschränken, setzen IT-Verantwortliche oft auf die Einschränkung von Rechten am Arbeitsplatz. Doch das Vorgehen verhindert lediglich die Installation neuer Software am Arbeitsplatz. Portable Software zeigt sich von dieser Einschränkung gänzlich unbeeindruckt. Sie benötigt lediglich Schreibrechte auf einem Speicherort im Netzwerk und lässt sich dann ganz einfach per Doppelklick starten.

Verboten ist, was nicht erlaubt ist

Schauen wir uns das Prinzip des Security-Klassikers Firewall an: Die erste zu setzende Regel ist immer "Deny all" – verbiete alles. Darüber setzt der Administrator dann die Regeln, die explizit erlaubt sind, etwa den Zugriff auf bestimmte Ports oder Portforwarding an spezielle Rechner. Damit ist im Datenverkehr nur das erlaubt, was nicht verboten ist. Genau dieses Prinzip macht sich SecuLution zu eigen und übergibt damit wieder dem Administrator die Verantwortung für die Software im eigenen Netzwerk. Denn Benutzer sollen nicht jede Software ausführen dürfen. Welche Software erlaubt ist, legt der Administrator fest und nicht der Algorithmus eines Softwareherstellers.

Der Unterschied zu anderen Lösungen liegt im Detail: SecuLution überwacht jede Software, auch wenn sie sich ohne Installation, durch einen Doppelklick auf die EXE-Datei, starten lässt. Eine ausführbare Datei muss dabei nicht unbedingt Schadsoftware sein, lässt sich aber trotzdem blockieren. Nehmen wir zum Beispiel "dropbox.exe", ein Programm ohne Installationsroutine. Das Speichern von Daten in der Cloud widerspricht aber der Unternehmens-Policy, keine Informationen außerhalb des Netzwerkes abzulegen. Ein Virenscanner würde die Software erlauben, da sie ja keine Bedrohung darstellt.

Um die Nutzung trotzdem zu verhindern, führen Admins meist einen gezielte Suche nach der Datei auf dem Computer durch. Problem dabei: Dieser Scan prüft lediglich den Dateinamen. Ein Anwender, der die Software dennoch nutzen will, benennt die Datei einfach um und der Scan findet sie nicht mehr.

Dateierkennung durch Hashwerte

Um diese Probleme zu lösen, arbeitet SecuLution mit einer Positivliste der erlaubten ausführbaren Programme. Und nutzt damit genau dasselbe Prinzip, wie es bei einer Firewall zum Einsatz kommt. Im Grunde ist es ganz einfach: Es darf nur die Software starten, die auch zugelassen ist. Nicht zugelassene Programme lassen sich nicht starten – egal, ob es sich um

eine Schadsoftware oder ein ungefährliches Programm handelt. SecuLution erkennt Dateien anhand eines eigens gebildeten Hashwertes und einer darauf basierenden Klassifizierung. Damit spielt auch der Dateiname keine Rolle mehr.

SecuLution besteht aus drei Teilen: Zunächst ist da der Agent. Er erstellt die Hashwerte und überwacht den Computer. Ihn gibt es nur für Windows, sodass Macintosh- und Linux-Arbeitsplätze außerhalb dieses Schutzmechanismus bleiben. Dann gibt es noch die SecuLution-Appliance. Sie dient als zentrale Datenbank und versorgt die Agenten. Im Regelfall läuft sie als virtuelle Maschine, kann aber auch ein eigenständiger physischer Computer sein. Als Drittes gibt es den AdminWizard für die Administration der Appliance.

Vor der Installation mussten wir dem Hersteller-Support Angaben zu unserer Netzwerkkonfiguration bereitstellen. Denn die virtuelle Appliance liefert SecuLution vorkonfiguriert aus. Das gelieferte Paket enthielt eine virtuelle VMware-Maschine, die sich auch für Hyper-V konvertieren und einsetzen ließ. Zusätzlich erhielten wir die Installationsdateien für den Agenten und den AdminWizard. Zur Inbetriebnahme importierten wir die VM unter vSphere. Sie stellt nur geringe Anforderungen an die Hardware und kam im Test mit einer CPU, einem halben GByte Arbeitsspeicher und einer 520-MByte-Festplatte aus. Allerdings wachsen die Anforderungen je nach Anzahl der Agenten.

Replikation mit dem Active Directory

Als Nächstes installierten wir den AdminWizard auf unserem Server, auf dem wir auch den WSUS betrieben. Das ist notwendig, damit SecuLution Windows-Updates vor dem Ausrollen als erlaubte Applikationen auf die Positivliste schreiben kann. Danach richteten wir den Syslog-Server ein. Nach dem Start des AdminWizard nahmen wir die Grundkonfiguration vor. Dazu gehörte etwa festzulegen, wie der Agent reagieren soll, wenn er den Aufruf einer unbekannten Applikation verhindert. In den Einstellungen konnten wir hier etwa für verschiedene Standorte und Abteilungen bis zu drei IP-Gruppen festlegen, die Form der Reaktion bestimmen und den auszugebenden Text.

Im nächsten Schritt legten wir im Active Directory einen neuen Benutzer an. Dieser dient zukünftig als „Ständiger Lernbenutzer". Dieses Feature gab uns die Möglichkeit, manuell neue Software zum Regelsatz hinzuzufügen, indem wir das hinzuzufügende Programm mit den Berechtigungen des dafür angelegten Benutzer-Accounts durchführten. Darauf gehen wir später noch einmal im Detail ein. Wir fügten den neuen Benutzer einer von uns neu angelegten, globalen Sicherheitsgruppe hinzu, die wir "SecuLutionLearnuser" nannten. Ebenso fügten wir den Lernbenutzer der Gruppe "Administratoren" hinzu.

Da SecuLution das bestehende Active Directory noch gar nicht kannte, widmeten wir uns der Replikation des Verzeichnisdienstes mit SecuLution. Wir wählten im entsprechenden Menü den Eintrag "MS-Active-Directory / Jetzt Updaten" aus. Nach Abschluss der Replikation wurden die AD-Objekte auf der Positivliste gespeichert. Das mussten wir der Appliance noch mitteilen und sendeten die Daten per Mausklick an selbige ab.

"Ständiger Lernbenutzer" erleichtert die Arbeit

Jetzt richteten wir den neuen Lernbenutzer in der Appliance ein. Durch die Replizierung mit dem AD kannte die Lösung unsere AD-Objekte. Wir wechselten in den Tab "Server Konfiguration" und klickten dort auf "Lernmodus". Das Pull-Down-Menü "Ständigen Lernbenutzer setzen" zeigte uns die AD-Objekte an. Gut gefallen hat uns hier, dass eine Gruppe mit einem vorangestellten "G", ein Host mit einem "H" und ein Benutzer mit einem "U" direkt identifizierbar waren. Wir wählten hier die angelegte Gruppe "G – SecuLutionLearnuser" aus und bestätigten mit "Übernehmen".

Der Zweck des Lernbenutzers wurde im Tagesbetrieb ersichtlich, wenn ein Kollege anrief und eine neue Software nutzen wollte. Um diese zuzulassen, also der Positivliste hinzuzufügen, ist der Administrator gefragt. Dazu reicht es aus, die Software einmalig mit einem privilegierten Benutzer zu starten. In unserem Fall war jeder Benutzer, der Mitglied der Gruppe "SecuLutionLearnuser" war, dazu berechtigt. Es ist jedoch nicht ratsam, einen AD-Benutzer zu verwenden, den ein Anwender – wie zum Beispiel der Administrator selbst –

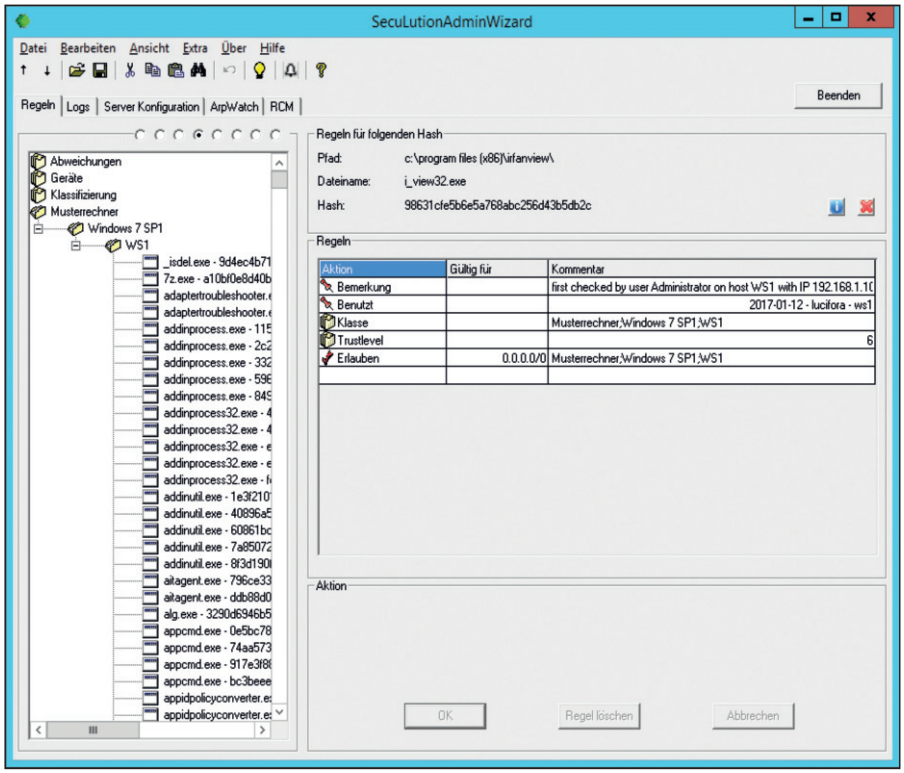

Bild 1: SecuLution erfasst die erlaubten Anwendungen auf einem Musterrechner anhand von Hashwerten und stellt diese in einer übersichtlichen Liste dar.

täglich nutzt. Denn damit kann es passieren, dass eine Software ungewollt auf die Positivliste kommt, zum Beispiel, weil der Administrator diese nur testet. Daher gibt es den "Ständigen Lernbenutzer".

In diesem Fall reicht ein Rechtsklick auf die auszuführende Datei und die Auswahl von "als anderer Benutzer ausführen". Hier trugen wir die Daten eines ständigen Lernbenutzers ein und führten die Software aus. Damit hat SecuLution den Hashwert für die ausführbare Datei registriert.

Ohne diese Hashwerte lässt sich keine Software ausführen. Das gilt auch für Windows-Updates. Zusammen mit dem WSUS-Server lassen sich die Hashwerte vorab erstellen. Dazu gingen wir pauschal davon aus, dass alle ausführbaren Programme, die über Windows Update kommen, vertrauenswürdig sind. Um diese in SecuLution entsprechend zu kennzeichnen, richteten wir die Automatisierung ein. Wir stellten den WSUS-Server so ein, dass er alle Update-Dateien lokal auf dem Server speicherte. Danach konfigurierten wir den automatischen Start einer von SecuLution gelieferten Batch-Datei über die Aufgabenplanung. Mit Hilfe dieser Batchdatei erstellt SecuLution für die von WSUS heruntergeladenen Daten die Hashwerte.

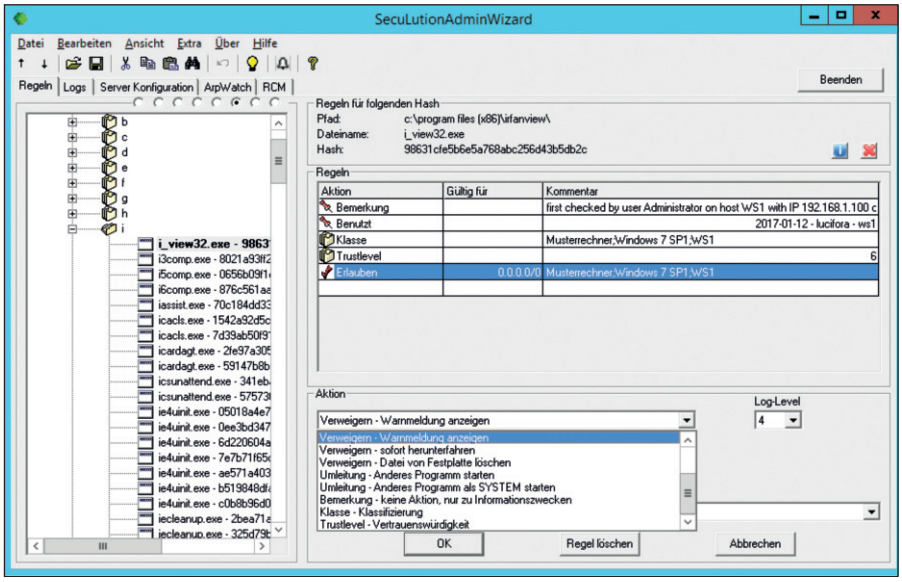

Bild 2: Durch das individuelle Bearbeiten erkannter Software kann der Admin auch Anwendungen verbieten, die keine Schadsoftware sind.

Andere Software-Updates muss der Administrator vor oder während des Update-Prozesses autorisieren. Wenn automatische Updates ausrollen sollen, wie zum Beispiel beim Browser Firefox, kann der Administrator das Update vorab auf einem Testrechner umsetzen, die Hashwerte übernehmen und das aktualisierte Programm zulassen. Dann funktionieren auch die Updates auf den anderen Rechnern.

Der Musterrechner als Vorlage

Damit waren alle serverseitigen Einstellungen getan. Doch bis dahin war noch keines unserer täglich benutzten Programme auf der Positivliste. Der Hersteller empfiehlt, für die eigene Positivliste einen Musterrechner zu konfigurieren. Dieser sollte möglichst mit allem konfiguriert sein, was im Unternehmen zukünftig erlaubt ist. Neben verschiedenen Tools, einem Virenscanner (der trotz der Nutzung von SecuLution für Dokumente natürlich noch notwendig ist), den Updates, Browser-Plug-ins und dem Office-Paket waren das bei uns im Test auch Grafikprogramme und Entwicklungstools. Für jedes Betriebssystem benötigten wir einen eigenen Muster-Rechner. Dieser galt uns als Vorlage für die Liste der vertrauenswürdigen Software.

Nachdem wir den AdminWizard auf unserem Musterrechner installiert hatten, starteten wir die Erstellung und den Import der Hashwerte. Für weitere im Netzwerk befindliche Software ließen wir die Hashwerte über einen UNC-Pfad generieren. Je nach Umfang eines Computers kommen somit einige tausend Hashwerte zusammen, die der Wizard übersichtlich sortiert anzeigt. Sehr gut gefallen hat uns, dass wir für jeden einzelnen Hashwert weitere Einstellungen vornehmen und damit die Ausführung der Software beschränken konnten. Zum Beispiel erlaubten wir den Start von administrativen Anwendungen wie der PowerShell und Putty lediglich Administratoren. Die Benutzung von DATEV gestatteten wir nur der AD-Gruppe "Buchhaltung" und so weiter.

Trustlevel schafft Vertrauen

Würden wir SecuLution jetzt im Netzwerk aktivieren, wäre die Wahrscheinlichkeit sehr groß, dass einige Kollegen gar nicht mehr arbeiten können, da wir sicher noch nicht jede Software berücksichtigt haben. Daher rät der Hersteller, anfangs einen Lernmodus zu aktivieren. Während dieser Zeit registriert SecuLution alle noch unbekannten Programme, blockiert sie aber nicht. Damit entdeckt der Agent auch Software, die sonst nicht bekannt ist. Dabei sollen in einigen Netz-

SecuLution

Produkt
Sicherheitswerkzeug, das den Start unerwünschter Anwendungen unterbindet und nur erlaubte Software zulässt.

Hersteller
SecuLution GmbH
www.seculution.de

Preis
In der kleinsten Ausführung mit 50 Arbeitsplätzen und allen Modulen kostet SecuLution 4675 Euro (93,50 Euro pro Computer). Bei 250 Arbeitsplätzen werden 16.675 Euro (66,70 Euro pro Computer), bei 1000 Arbeitsplätzen 63.100 Euro (63,10 Euro pro Arbeitsplatz) fällig.

Systemvoraussetzungen
Active Directory und WSUS-Server. Für den Agenten und den AdminWizard kommt Windows ab Version XP SP3 in Frage. Die Appliance benötigt mindestens 512 MByte RAM und eine CPU. Im Regelbetrieb sind 2 GByte RAM und vier CPUs empfohlen.

Technische Daten
www.it-administrator.de/downloads/datenblaetter

werken sogar Backdoor-Programme und Trojaner aufgetaucht sein, die auf Arbeitsplatzrechnern schlummerten.

Die Verteilung des Agenten erfolgt im Regelfall über die Gruppenrichtlinien oder andere Lösungen zur Softwareverteilung. In unserem Labor bedienten wir uns der GPO. Die im Laufe einiger Tage auf den verschiedenen Computern ermittelten Hashwerte analysierten wir zu einem späteren Zeitpunkt und klassifizierten die zusätzlich erkannte Software.

Um dem Administrator das Leben leichter zu machen, arbeitet SecuLution mit einem Trustlevel. Im Laufe der vergangenen Jahre haben die Entwickler viele Programme analysiert und mittels Trustlevel deren Vertrauensstellung klassifiziert. Diese Daten stellt das Unternehmen gegen Bezahlung seinen Kunden zur Verfügung. Generiert der Agent einen neuen Hashwert, prüft dieser gegen die Online-Datenbank, ob die Datei schon bekannt ist, und erhält einen entsprechenden Trustlevel zurück. Diese Angaben waren ein guter Anhaltspunkt für die weitere Bearbeitung.

Zwar ist es möglich, aufgrund des Trustlevels Software generell zu erlauben. Doch der Level sagt nur aus, ob die Software an sich schädlich ist, aber nicht, ob sie der Firmen-Policy entspricht.

Keine Zeile unerwünschter Code

Nun war es so weit, SecuLution scharf zu schalten. Das geschah, indem wir den Lernmodus zentral abschalteten. Nutzten wir nun auf unserem Arbeitsplatz die erlaubten Programme, lief alles ohne weitere Unterbrechungen ab. Starteten wir hingegen eine unbekannte Software, erschien eine Meldung und das Programm wurde blockiert.

Sehr gut gefallen hat uns, wie SecuLution die Blockade durchführt. Jede Software benötigt Speicher, den der Kernel verwaltet. Beim Start eines Programmes fragt die Software beim Speicher an und bekommt einen eigenen Bereich zugewiesen. SecuLution klinkt an dieser Stelle ein zusätzliches Kernel-Modul ein, das beim Aufruf der Speicherreservierung prüft, ob die anfragende Software vertrauenswürdig ist. Nur dann leitet das Modul die Anfrage an den Kernel weiter und er gibt den Speicher frei. Darf die Software nicht starten, erhält sie keinen Speicher zugeteilt. Durch diesen patentierten Weg stellt der Hersteller sicher, dass die unerwünschte Software wirklich keine Zeile Code ausführt.

Natürlich registriert SecuLution alle unerlaubten Programmausführungen und zeigt sie im AdminWizard an. Mit diesen Angaben kann der Administrator gut analysieren, welche Software zurecht blockiert und welche noch freizugeben ist.

Hashwert-Freigabe durch Bestätigungscode

Wir stellten uns zusätzlich die Frage, wie sich das System auf mobilen Arbeitsplätzen auswirkt. Denn nicht nur Arbeitsplatzrechner, die ständig mit dem Netzwerk verbunden sind, sollten richtig geschützt sein. Notebooks von Mitarbeitern im Home-Office etwa darf der Agent nicht ungewollt lahmlegen. Was ist zum Beispiel, wenn ein Mitarbeiter beim Kunden vor Ort einen Druckertreiber installieren soll? Der Administrator ist nicht anwesend, um die Setup-Datei zu autorisieren. Auch fehlt jegliche Verbindung zur SecuLution-Appliance, um den Hashwert zu aktualisieren.

Die Lösung liefert der Hersteller in Form eines Freischaltcodes. Im Grunde funktioniert das System wie ein Gutschein. Wir konfigurierten zunächst über den AdminWizard die Agenten und legten fest, dass der Benutzer im Offline-Modus die Möglichkeit erhält, einen Bestätigungscode einzutragen, sofern ein Hashwert unbekannt ist. Dann lösten wir von unserem Notebook die Netzwerkverbindung und starteten eine unbekannte EXE-Datei. Der Agent erkannte das und öffnete eine Dialogbox.

Hier erschien ein Zahlen-Buchstaben-Code, den der Mitarbeiter dem Administrator telefonisch durchgibt. Als Administrator wollten wir die Verwendung der Software gestatten, erstellten den Bestätigungscode und trugen ihn auf dem Notebook ein. Den Code generierten wir über den AdminWizard auf Basis des vom Mitarbeiter übermittelten Codes. Dabei konnten wir auch festlegen, ob das Programm zukünftig immer oder nur für eine bestimmte Zeit ausführbar sein sollte.

Verschlüsselung von USB-Geräten

Als Bonus sehen wir das Modul zur Gerätekontrolle. Genau wie bei Software kann SecuLution auch USB-Geräte und -Anschlüsse verwalten, sodass sich im gesamten Netzwerk nur noch die USB-Geräte verwenden lassen, die wir als erlaubt einstuften. Dies und eine Verschlüsselung der Daten soll sicherstellen, dass wir Daten auf einem USB-Speicher nur an vertrauenswürdigen Stellen öffnen und eventuell verloren gegangene USB-Speicher kein Datenleck im Unternehmen verursachen.

Die Verschlüsselung ist ein für die Benutzer unbemerkter und vollautomatischer Prozess. Wir konnten auf diesem Weg Daten auf einem USB-Speicher schreiben und diese an jedem anderen Gerät in unserem Netzwerk öffnen. Schlossen wir den USB-Stick jedoch an einen Computer an, der nicht mit dem SecuLution-Agenten unseres Netzwerks lief, sahen wir nur codierte Daten. Diese konnten wir dann, mit einem Passwort geschützt, durch eine

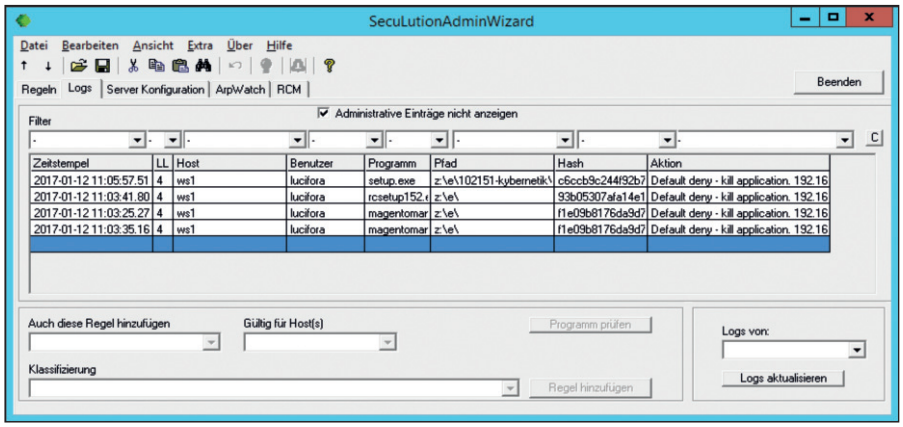

Bild 3: Unerlaubte Programmzugriffe bereitet SecuLution in einer übersichtlichen Zusammenfassung auf.

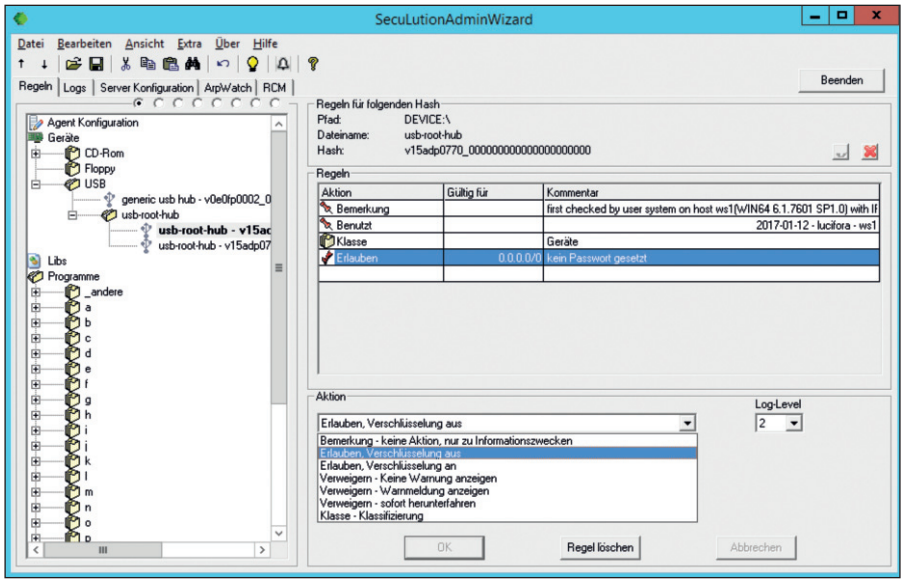

Bild 4: Wie SecuLution mit der Nutzung eines USB-Anschlusses umgeht, stellten wir im AdminWizard ein.

auf dem Stick befindliche Software temporär entschlüsseln. Mit diesem Prozess lassen sich Daten über USB-Massenspeicher, die auch Festplatten sein können, problemlos im Netzwerk nutzen. Geht der USB-Speicher verloren oder wird geklaut, sind die Daten geschützt.

Fazit

Mit SecuLution haben wir eine seit mehr als zehn Jahren gewachsene Software getestet. Der Hersteller geht einen einfachen und logischen Weg: Er übergibt dem Administrator die volle Kontrolle und auch Verantwortung über die im Netzwerk erlaubte Software. Dabei lässt sich alles kontrollieren, was beim Kernel Speicherplatz anfordert. Reine Arbeitsdateien sind davon nicht betroffen.

Dadurch, dass der Start von ausführbaren Programmen explizit erlaubt sein muss, umgeht SecuLution ein Ratespiel bei unbekannter Software und verhindert mögliche Fehlentscheidungen. Sehr gut gefallen hat uns, dass der Agent verhindert, dass auch nur eine Zeile Code in den Speicher gelangt, wenn die Anwendung unbekannt ist. Das Modul zur Verschlüsselung von USB-Speichern ist eine sehr sinnvolle Ergänzung, um vor allem verlorengegangene oder gestohlene USB-Speicher zu schützen.

Schade finden wir, dass sich das Angebot klar an mittlere bis große Unternehmen richtet. Denn die Lizenz ist erst ab 50 PC-Arbeitsplätzen erhältlich. Nach Meinung von SecuLution sind kleinere Netzwerke ohne Spezialwerkzeug in den Griff zu bekommen. Wir sehen das etwas anders und meinen, dass SecuLution auch für kleine Unternehmen eine große Bereicherung wäre. Durch die Art der Umsetzung, den geringen zeitlichen Aufwand zur Implementierung und die durchdachte Anwendung hat uns SecuLution voll überzeugt. *(ln)*

So urteilt IT-Administrator

Erstellen der Positivliste	7
Einrichten auf den Arbeitsplätzen	6
Erkennung nicht erlaubter Software	8
Hinzufügen von Software	6
Schützen von USB-Speichern	6

Die Details unserer Testmethodik finden Sie unter www.it-administrator.de/testmethodik

Dieses Produkt eignet sich

optimal für Netzwerke ab 50 Arbeitsplätzen zum Schutz vor unerwünschter Software und als Ergänzung zu Anti-Viren-Lösungen.

bedingt für die Vorgabe und Umsetzung von Unternehmens-Policies.

nicht als Ersatz für Anti-Viren-Software und für Netzwerke mit weniger als 50 Arbeitsplätzen.