Seculution – Software Dienstleistung

In Zeiten von Ransomware und anderer Schadprogramme waren wir auf der Suche nach einer Ergänzung zu unserer vorhandenen Antivirus Lösung. Dabei sind wir auf Seculution gestoßen.

Kurz und knapp arbeitet das Programm nach einer managed Whitelist. Es können nur Programme gestartet werden, die in der Whitelist vorhanden sind. Die Idee ist gut.

Hier eine kurze Zusammenfassung **meiner Erfahrungen mit diesem Tool**.

Positives:

- (++) Performance des Agents. Man merkt keinen Performance Verlust. (Es gab einen Fehler im Offline Betrieb, in diesem Fall hat der Agent 40-50% Cpu verbraucht. Aber dieser Fehler wurde behoben).
- (o) Ich denke das Programm funktioniert gut, WENN man ein extrem homogenes Netz hat. Wenn alle Rechner absolut identisch sind und keiner Programme braucht die aus der Reihe sind.
- (+) Eine USB Device Control ist vorhanden.
- (+) Verschlüsslung der USB Devices (nur USB Sticks, USB HDD´s können leider nicht verschlüsselt werden).

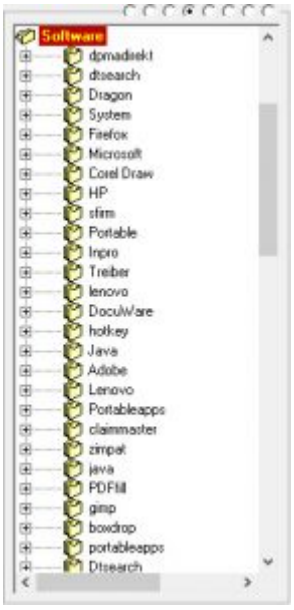
Negatives:

- (–) Extrem nervig ist die Geschwindigkeit des SeculutionAdminWizard. Das Regelwerk (whitelist) wird damit verwaltet. Eine negative Eigenschaft dabei ist: Es wird immer das **komplette**

Dieses Problem wurde etwa 09/2015 durch ein Update behoben.

Archive

Regelwerk gelesen und geschrieben, auch wenn nur **ein Regelsatz** geändert wird. Das herunterladen und hochladen des Regelsatzes ist abhängig von der größer der Datenbank, bei unseren 80 Rechner dauert das mittlerweile über **1 min.** Das hört sich wenig an, stört aber in der Praxis ungemein. Auch das einlesen und suchen innerhalb der Regeln ist nicht sehr logisch, beispielsweise wird beim suchen nicht chronologisch gesucht. Es handelt sich um **keine echte Datenbank** handelt, sondern um eine aufgebohrte CSV Datei. Außerdem kann immer nur ein Anwender an der Datenbank arbeiten. Sobald zwei Änderungen darin vornehmen, wird entweder einer Änderung überschrieben oder (auch nicht selten) der ADM Wizard hängt sich auf und alle Änderungen sind weg. Das macht das auditieren der Regeln während der Lernphase zu einer ungeliebten nervigen Tätigkeit, die auch immer nur von einer Person gleichzeitig durchgeführt werden kann. Die Datenbank wächst monatlich um ca. 3%, was nach und nach die Performance weiter sinken lässt.



Leider wird in der Datenbank nicht mal nach Buchstaben sortiert. Das erschwert das suchen und finden.

Dieses Problem wurde etwa 09/2015 durch ein Update behoben.

SecuLution verwendet als Format beim Export für Datensicherungen das CSV Format. Die Appliance arbeitet mit einer Berkeley DB.

Wie langsam das ist, seht ihr im Video: 0-1.21 ist nur der Login. 1.21-2.20 ist ein Upload der Regeln ohne eine Änderung! https://youtu.be/9fNAQsS9UMw

Bei Verwendung der Version aus dem Update 09/2015 oder neuer ist der gesamte Vorgang in 4 Sekunden erledigt.

- (–) Als negativ hervorzuheben ist leider auch der Support. Ich habe mich selten so ärgern müssen, wie beim Seculution Support. Das einzig positive ist, dass man sehr schnell antworten erhält. Der Inhalt der Antworten besteht allerdings immer aus dem gleichen Aussagen: *„Seculution ist das beste was es gibt auf Markt, aber 100% Sicherheit gibt es nicht“* und *„Schauen Sie zu dem Thema XY bitte in die FAQ´s“.* Das ist leider nicht immer hilfreich. Und wehe man bemerkt etwas Negatives über Seculution, dann fühlt sich der Support persönlich und das Produkt angegriffen, ab dann ist kein

Eine Aussage, hinter der wir stehen.

Wenn Kunden Fragen stellen, die bereits in der FAQ beantwortet sind, formulieren wir die Antwort in der Regel nicht neu, sondern weisen auf die entsprechende Stelle hin.

Bei SecuLution arbeiten Menschen. Bei persönlichen Angriffen reagieren diese entsprechend.

vernünftiges argumentieren mehr möglich und es wird mühsam. Wir sind dazu übergegangen uns den Aufwand zu sparen und eine Email an den Seculution Support zu schreiben, weil es keinen Sinn macht und zu keinem Ergebnis führt, außer Frust.

Einem Kunden kann nur geholfen werden, wenn er mit dem Support kommuniziert. Wer keine Updates macht und die Kommunikation mit dem Support einstellt, dem können wir nicht helfen.

- (–) Die von Seculution empfohlene „Schulung“ haben wir erst einige Monate nach Testlauf gebucht und hätte wir uns sparen können. Der Anfang der Schulung macht den Eindruck eines Verkaufsgesprächs, obwohl wir schon längst gekauft hatten. Der zweite Teil entspricht genau den empfohlenen Vorgehensweisen, die in den FAQ´s genau so beschrieben sind. Und beim Fragen und Antworten Teil, wurde der größte Teil unserer Fragen mit geht nicht oder gibts nicht beschrieben. Also wer nicht lesen möchte kann die Schulung mitmachen.
- (–) Richtig problematisch ist auch die Verteilung der Agent´s. Diese wird von Seculution empfohlen mit dem integrierten Tool RCM verteilt. Beim verteilen und beim Update sind auf den Clients bis zu **6 Neustarts** nötig, bist der Agent vollständig installiert ist. Und die ausstehenden Neustarts werden dem Anwender auch nicht gemeldet. Man merkt das als Nutzer nur dadurch, dass die UAC deaktiviert ist und das macht eine Vielzahl an Problemen, gerade bei Win 8 und Win 10. Erst wenn man den ganzen Prozess des RCM durchläuft wird die UAC wieder aktiviert. Seculution Kommentar dazu ist: *„ist ein Microsoft Problem“.*

Agent Installation oder Update-benötigen genau *einen* Neustart.

Das Management der Agent Versionen wird durch Gruppenrichtlinien durchgeführt. Auf den Zeitraum, der vergeht, bis diese auf den Client Computern angewandt werden, haben wir keinen Einfluss.

- (-) Für ein Produkt, dass damit wirbt „von Techniker für Techniker“ entwickelt worden zu sein, ist es umso unverständlicher, dass es keine Release Notes bei Updates gibt. Man bekommt eine Meldung, dass eine neue Version existiert, aber was wurde geändert?? Wenn man bei Seculution nachfrägt, dann kommt als Antwort: „Wir empfehlen immer die *offizielle release version* zu installieren“. Was aber geändert wurde erfährt man nicht. Aus meiner Sicht sollte es schon dem Nutzer überlassen werden, ob eine Änderung es einem Wert ist die doch recht aufwendigen und langwierigen Agent update weg zu gehen oder doch erst die nächste Version ab zu warten. Übrigens ist ein Agent Update eigentlich kein Update, sondern eine komplette de- und dann Neuinstallation des Agents bei der erneut bis zu 6 Neustarts nötig sind. Also ohne Release Notes hat man keine Grundlage eine Entscheidung zu treffen.
- (-) Das auf der Homepage vorgeschlagene *„Vollinstallation und Verteilung in 5 Stunden“* beinhalten eine Lernphase von 32 Tagen (wenn man das Produkt kennen lernt, weiß man ganz schnell was das ist.) Dieser Wert ist in der Praxis absolut unrealistisch. Wir

Selbstverständlich hängt die Dauer der kompletten Inbetriebnahme auch von Faktoren ab, die netzwerkspezifisch sind. Wir haben in unserer Dokumentation einen Durchschnittswert von ca. 5 Arbeitsstunden innerhalb von 32 Tagen angegeben, der unserer Erfahrung mit unseren Kunden entspricht. Manche Kunden brauchen weniger, manche etwas mehr.

hatten eine Lernphase von über 3 Monaten und es war immer noch nicht alles angelernt. Also die Werbeversprechen sind mit Vorsicht zu genießen. Nach Rückfrage sind die 32 Tage angeblich Erfahrungswerten von Seculution. Also der Einführungsvorgang dauerte bei uns wesentlich länger als angegeben.

- (-) Die Möglichkeiten am Agent sind minimal. In der Praxis wünscht man sich hier oft eine paar Features, wie den Lernmodus für den Client aktivieren oder dergleichen, aber Fehlanzeige. Man kann den Agent deaktivieren und aktivieren und das Offline DB kopieren das war´s. Oder den lahmen Wizard verwenden.
- (-) Unverständlich ist auch, dass das Popup, dass dem Anwender eigentlich melden sollte dass jetzt gerade eine Anwendung durch Seculution gesperrt wurde, hinter den geöffneten Fenstern erscheint und damit für den Anwender erstmal nicht sichtbar. Das ist nicht nur für unerfahrenere Anwender immer wieder eine Falle, die das arbeiten erstmal stoppt.
- (o) Was man außerdem einfach Wissen muss ist, dass man ohne Softwareverteilung Seculution in der Praxis kaum oder nur sehr umständlich nutzen kann. Also wer keine Softwareverteilung hat, braucht Seculution eigentlich nicht einführen.
- (o) In den am Anfang doch recht nützlich und anfangs öfter benötigten FAQ´s gibt es nicht mal eine such Funktion. Auf den Verbesserungsvorschlag dafür kam vom Seculution Support nur: „Zur suche darin benutzen Sie doch Goolge!“ Naja das geht, aber praktisch ist was anderes.
- (-) Eine nette Support Fall war auch, dass individuelle Übersetzungen, die man im Admin Wizzard durchführen kann, nicht an den Agent übertragen werden. Lt. FAQ hätte man verstehen können, dass dies eigentlich funktionieren sollte. Das Problem wurde von mir an Seculution gemeldet und dann ewig nichts mehr gehört. Nach Rückfrage von mir bei Seculution wurde dann einfach der Text in den FAQ´s so abgeändert dass es zum Fehler passt. Das ist schon mal komisch genug, aber dann noch zu erwarten, dass man zu einen Support Fall in Google suchen muss (weil eine eigene suche gibt es ja nicht), ob dieser evtl. durch ändern der Anleitung gelöst wurde? „**No Go, das geht gar nicht! Entspricht in keiner Weise das was ich von einem Unternehmen erwarte, dass u.a. Dienstleistungen verkaufen möchte.** Der Lösungsvorschlag nach Rückfrage um die Übersetzungen zu bekommen ist eine Neuinstallation der Agents… Also 6 Neustart von 80 Rechnern, um andere Übersetzungen in die Agents zu bekommen. Dabei

Es ist Designziel von SecuLution, den „normalen Benutzern“ keine Administrationstätigkeiten zu überlassen. Für Administratoren bestehen diese Möglichkeiten jedoch (z.B. über das Feature „PLU“).

Wir haben uns entschieden, nicht die aggressivste Form von „Fenster nach vorn“ umzusetzen, um den Microsoft Windows Guidelines zu entsprechen.

SecuLution setzt keine Softwareverteilung voraus. Ob mit oder ohne Softwareverteilungssystem kann SecuLution die zu installierenden Updates automatisch erfassen und damit problemlos auf sämtlichen Systemen betrieben werden, auch welchen, die eventuell aus Gründen der Kompatibilität nicht immer die aktuellsten Patche erhalten.

Wir stellen die Dokumentation zu SecuLution auf unserer WebSite und im AdminWizard über Microsoft Help zur Verfügung. Zur Suche in der Online Dokumentation empfehlen wir die Suchfunktion von Google zu verwenden: “site:seculution.com Suchbegriff“

Das „Problem“ war eine ungenaue Dokumentation. Diese haben wir korrigiert.Technisch werden die Übersetzungstexte zum Zeitpunkt der Installation des Agents in die Registry geschrieben. Eine nachträgliche Änderung ist damit nur durch Neuinstallation des Agents oder durch manuelles Eingreifen in die Registry möglich.

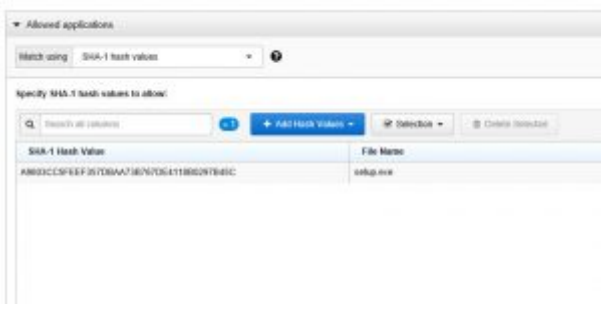
stehen die Übersetzten Texte in der Registry und können/könnten dort geändert werden, aber dieser Vorschlag kommt **nicht** von Seculution, sondern muss man sich selber suchen. So braucht man keinen tech. Support.

- (0) Die von Seculution angepriesenen Automatismen für die Whitelist bestehen eigentlich in der Praxis aus einer geplanten Aufgabe, die mit einer Batch Datei bestimmt Rechner, Ordner, Wsus Server usw. in die Whitelist aufnimmt. Das hört sich erst mal gut an, hat allerdings mehrere Probleme. Das größte ist die Zeit. Es muss ein Mittelweg gefunden werden, wann dieser Job läuft, damit rechtzeitig alle ohne Einschränkung arbeiten können. Denn bei Seculution bedeutet ein nicht eingelesenes Outlook Update, dass die User Outlook nicht mehr starten können. Und das ist bei Zeitverschiebungen. USA, Australien, DE nicht einfach zu lösen.
- (–) Wenn man Sonderfälle hat, die bei jedem Start einen neuen Hashwert generieren (wie z.B. Webex von Citrix oder Gotomeeting von Cisco), hat man ein richtiges Probleme. Bei jedem Meeting wird das Programm erstmal geblockt, weil das Programm unbekannt ist. Zur Freude der Mitarbeiter. Der Kommentar von Seculution Support war: *„bitte sehen Sie in Google nach, da findet man die Lösung, wir Supporten keine Fremdprogramme!“.* !! AHA !! Ich habe daraufhin bei Citrix und Cisco angefragt allerdings natürlich als nicht Kunde nie eine Antwort erhalten.
- (-) Offline Betrieb von Notebooks. Im Offline Betrieb, d.h. bei nicht Erreichbarkeit des Seculution Servers, gibt es für die Notebooks mehrere Betriebsarten zur Auswahl. Diese genau zu beschreiben würde den Rahmen sprengen, aber leider ist keiner für uns dabei, der vernünftig funktioniert. Wir haben eine Zwischenlösung gefunden, die wir mit einem eigenen kleinen Tools ergänzt haben. Seculution Offline Hash updater. Das ist leider auch keine optimale Lösung und daher ein dicker Minus Punkt.

Die Aufgabe einer Whitelisting Lösung wie SecuLution ist, dafür zu sorgen, dass nur noch als vertrauenswürdig eingestufte Software ausgeführt werden kann. Ein neues, unbekanntes Programm kann damit die neueste Ransomware oder ein GoToMeeting.exe von Cisco sein. Die Hersteller von Online Meeting Tools (WebEx, GoToMeeting) sind sich dieses Problems bewusst und bieten daher die Möglichkeit an, die Tools fest zu installieren, sodass sich der Hash nicht mehr ändert. Zur Teilnahme an einem Meeting werden dann nur noch die Session Daten ausgetauscht, nicht mehr .exe Dateien. Wie dies technisch umgesetzt wird, ist Sache der Hersteller. SecuLution kann nicht den Support für Fremdhersteller übernehmen. Inzwischen (Stand 11/2016) supportet SecuLution auch eine Methode, diese derartige Tools anhand deren Authenticode Signatur zu verifizieren und automatisch zu erlauben.

Hier kann nur vermutet werden, dass der Kunde nicht die aktuellste Version der SecuLution Software einsetzt.

Diese Funktion wird durch SecuLution schon seit Anfang 2015 unterstützt. Der Einsatz von 3rd Party Tools ist nicht notwendig.



SHA-1 statt MD5

- (o) Die Prüfung der Programme erfolgt mit MD5 Hashwerten. MD5 Prüfwerte lassen sich kopieren. Das ist kein wirklicher Nachteil aus User Sicht, aber wenn ich Seculution umgehen wollte, würde ich mir mein Schadprogramm einfach den gleichen MD5 Hashwert von dem Windows Taschenrechner geben, dann würde Seculution davon nichts mitbekommen. http://www.mathstat.dal.ca/~selinger/md5collision/ Unter dem Link findet man auch zwei Demo Dateien, mit denen man das testen kann. Andere Hersteller nutzen aus offensichtlich gutem Grund SHA-1 Hash Werte statt MD5. Hier ein Screenshot eines alternativen Anbieters, der auch noch dazu eine Weboberfläche bietet.
- Es gäbe leider noch wesentlich mehr negatives, aber irgendwann ist es gut.

Dies ist sachlich falsch. Herr Probst verwechselt „Kollision“ und „Pre-image“ Angriff. Kollisionen stellen in diesem Anwendungsfall keine sicherheitstechnische Einschränkung dar. Ein Preimage Angriff ist auch bei MD5 nicht möglich. Es ist daher nicht machbar ist, eine Datei (Schadsoftware) zu erzeugen, die den Hash von calc.exe haben wird.

Fazit:

Aus den ganzen Nachteilen ergibt sich für die User ein ständiges sperren und aufpoppen von Fehlermeldungen bei Programmen, die eigentlich gebraucht werden. Die Aufgabe die Whitelist zu führen hat voll und ganz der Admin, aber die Tools, die einem dazu zur Verfügung gestellt werden sind unausgereift, fehlerbehaftet und einfach nicht ausreichend um das in der Praxis vernünftig lösen zu können. Ich denke es gibt Abteilungen, bei denen das klappen könnte, aber bei Dienstleistern, die rund um die Uhr arbeiten müssen, Offline unterwegs sind und viele Webmeetings halten müssen, bremst das Tool die Arbeit erheblich bis zum nicht mehr arbeiten können. Das Prinzip ist wirklich gut, aber der Mittelweg zwischen Sicherheit und Komfort ist hier nicht gefunden.

Wie Herr Probst im Text selbst geschrieben hat, hat er die Kommunikation mit dem Support eingestellt. Nach der Veröffentlichung dieses „Erfahrungsberichtes“ durch Herrn Probst hat der Geschäftsführer der Firma SecuLution Herrn Probst persönlich kontaktiert und kostenlosen Vor Ort Support angeboten, um Herrn Probst bei der Lösung seiner Probleme behilflich zu sein. Herr Probst hat dies abgelehnt.

↑