Wie gut schützen Positivlisten und wie viel Aufwand bedeuten sie?

Alternative Whitelist

Es bietet sich an, beim Einsatz von Application Whitelisting die Unterschiede der einzelnen Angebote genau unter die Lupe zu nehmen, weil sie sich im Detail unterscheiden.

Application Whitelisting verspricht ein höheres Schutzniveau als Virenscanner, denn nur explizit erlaubte Software kann ausgeführt werden. Das heißt: nie mehr Schadsoftware. Die U.S. NIST Agency (National Institute of Standards and Technology) empfiehlt bereits seit 2015 Application Whitelisting als primäre Schutzmaßnahme für Netzwerke. [1] Viele scheuen allerdings den Aufwand, eine Software-Whitelist zu pflegen. Doch wie hoch ist dieser wirklich?

Das Prinzip ist einfach: Eine Application-Whitelisting-Lösung muss lediglich wissen, welche Software im Unternehmensnetzwerk ausgeführt werden soll. Alles andere ist unerwünscht und wird blockiert. Spiele etc. – die sogenannte Schatten-IT, die am Arbeitsplatz unerwünscht ist – oder eben jegliche Form von Malware: Alle werden an der Ausführung gehindert, ohne dass sie bekannt sein müssen.
Doch aus diesem Ansatz ergeben sich ganz automatisch auch Fragen: Bedeutet Application Whitelisting nicht einen erhöhten Aufwand bei der Pflege der erlaubten Anwendungen? Wie erstelle ich eine Whitelist mit allen Einträgen? Wie kann man Änderungen wie Updates und neue Software erfassen? Was ist mit dynamischen Anpassungen während des Betriebs? Wie lange dauert es, bis eine Änderung meiner Policies aktiv wird? Auch Detailfragen in Bezug auf das Verhalten auf mobilen Systemen, Reporting, Ausnahmen und individuelle Policies muss man sich beim Vorhaben, Application Whitelisting einzusetzen, stellen. Welches Schutzniveau im Vergleich zum Virenscanner kann tatsächlich erreicht werden? Wie ist die Performance? Fragen über Fragen.

Was kommt auf die Whitelist?

Authentifizierung des Elements
Eine zentrale Bedeutung kommt dem verwendeten Verfahren zu, das fragliche Elemente fälschungssicher authentifizieren soll. Hier stehen historisch verschiedene Methoden zur Verfügung, die sich bezüglich der erzeugten Sicherheit unterscheiden. Da frühe Application-Whitelisting-Produkte noch keine Features implementiert hatten, um den Aufwand für die Erstellung und Pflege der Whitelist durch Automatisierung auf ein machbares Maß zu reduzieren, wurden zum Beispiel von Microsofts AppLocker sehr einfach zu verwaltende Methoden der Authentifizierung bereitgestellt, die aber gleichzeitig trivial zu umgehen oder zu fälschen waren. Sie können daher den Anspruch einer modernen Sicherheitslösung heute nicht mehr erfüllen. Das nach dem Stand der Technik einzig sichere Vorgehen zur Authentifizierung des Elements ist ausschließlich das Hash-Verfahren. Die anderen hier aufgeführten Methoden werden nur aus historischen Gründen genannt und sollten in der Praxis nicht mehr eingesetzt werden.

Vielfalt möglicher Authentifizierungsverfahren

Welche Verfahren gibt es? [2]
Pfade (Sicherheit + Aufwand +): Sämtliche Software aus einem freigegebenen Pfad ist erlaubt. Dies ist trivial zu umgehen und bietet keinen nennenswerten Schutz.
Dateiname (Sicherheit + Aufwand +): Software ist nur abhängig von ihrem Namen erlaubt. Dies ist trivial zu umgehen und bietet keinen nennenswerten Schutz.
Dateirechte (Sicherheit +++ Aufwand +++): Das NTFS-Dateisystem von Microsoft ermöglicht die Auswertung, von welchem Benutzer-Account eine Datei angelegt wurde. Application-Whitelisting-Lösungen, die auf dieser Auswertung basierten, waren relativ einfach zu handhaben und boten bereits ein deutlich höheres Schutzniveau. Die Schwäche war auch hier die Umsetzung kurzfristig benötigter Anpassungen sowie die Umgehbarkeit des Schutzes durch sämtliche Codes, die mit erhöhten Rechten ausgeführt wurden. Bei Angriffen auf Systemdienste konnte die Schadsoftware die Berechtigungen im Dateisystem selbst festlegen, wodurch diese Methode keinen Schutz mehr bot.
Rechtevererbung (Sicherheit +++ Aufwand +++++): Ähnlich wie bei der Auswertung der Dateirechte werden auch hier Windows-Rechte ausgewertet (Benutzer-Account des Elternprozesses). Auch hierbei wurden Lücken bekannt: Ein Angriff auf

Um Hackern und Schadsoftware keine Chance zu geben, verspricht Application Whitelisting ein hohes Schutzniveau gegenüber anderen Methoden. Bilder: SecuLution

bereits mit Systemrechten laufende Prozesse hebelte den Schutz komplett aus. So konnte zum Beispiel der Angriff ‚WannaCry' trotz aktivem Microsoft AppLocker ungehindert Systeme befallen, da die Schadsoftware den SMB1-Dienst von Windows angegriffen hat. Dieser läuft unter Windows mit Systemrechten. Da WannaCry damit als Kindprozess dieses SMB1-Systemprozesses ausgeführt wurde, wurde der Code grundsätzlich erlaubt.

Digitale Signatur (Sicherheit ++++ Aufwand +++++): Als Merkmal für eine Authentifizierung wird (ebenfalls Microsoft AppLocker) eine gegebenenfalls vorhandene digitale Signatur einer Software ausgewertet. Obwohl hier das erzeugte Maß an Sicherheit deutlich höher ist als bei den bisher genannten Methoden, ist doch der Aufwand zur Implementation sehr hoch, da selbst Microsoft selbst nur einen kleinen Bruchteil seiner eigenen Software digital signiert. Über 95 Prozent aller Dateien einer Windows-10-Installation sind nicht digital signiert.

Zum Einsatz dieser Methode muss der Administrator eine eigene Zertifizierungsstelle (Certificate Authority) pflegen und warten. Darüber hinaus müssen alle Anwendungen und Updates vor dem Ausrollen zunächst vom Administrator signiert werden. Nur diese signierte Version kann dann auf den einzelnen Computern ausgeführt werden. Ein spontanes Freischalten kurzfristig benötigter Software ist nicht oder nur mit ganz erheblichem Mehraufwand möglich, was dieses Verfahren in der Praxis bereits für die meisten Einsatzfälle disqualifiziert.

Darüber hinaus wurden in der Vergangenheit Lücken bekannt, die bereits aktiv durch Angreifer ausgenutzt wurden. Wird beispielsweise der Private Key einer als vertrauenswürdig definierten Herstellersignatur kompromittiert, kann sich ein Angreifer seine eigene Signatur für seine Schadsoftware generieren und damit ungestört und unbemerkt das signaturbasierte Whitelisting umgehen.

Hashes (Sicherheit +++++ Aufwand +): Ein Hash ist eine Zeichen- und Zahlendarstellung fester Länge (zum Beispiel SHA256: 256 bits) einer beliebig langen Eingabedatei, hier vergleichbar mit einem Fingerabdruck. Basiert das Application-Whitelisting-Verfahren bei der Authentifizierung des fraglichen Elements auf dem Abgleich von Hashes, muss nicht jede Software vollständig als komplette Binärdatei in der Whitelist enthalten sein, sondern nur ihr Hash (Fingerabdruck). Die Verwendung kryptografisch sicherer Hashes ermöglicht, dass ausschließlich eindeutig authentifizierte Software ausgeführt werden kann. Hashes sind damit das mit Abstand sicherste Verfahren der Authentifizierung von Elementen, bringen aber auch die größten Anforderungen an die Verwaltung der Application-Whitelisting-Lösung mit sich.

Die Application-Whitelisting-Software SecuLution löst diese Anforderungen unter anderem mit einem cloudbasierten Reputationsservice mit Hashes vertrauenswürdiger Software. Aus dieser Datenbank können automatisiert Einträge in die Whitelist-Datenbank des Anwenders übernommen werden. Das Patchmanagement wird so vereinfacht. Der Administrator kann die Hashes jeglicher von ihm als vertrauenswürdig eingestufter Software (zum Beispiel selbst programmierte Spezialsoftware) mit einem Klick zu seiner individuellen, in seinem Netzwerk gültigen Whitelist-Datenbank hinzufügen. Dadurch wird die Sicherheit von Hash-basierendem Application Whitelisting mit der größtmöglichen Einfachheit bei der Administration kombiniert.

Welche Whitelisting-Lösung passt zu meinen Bedürfnissen?

Diese Vielfalt der möglichen Authentifizierungsverfahren findet sich fast in voller Bandbreite bei den verschiedenen Produkten. Hersteller wie Ivanti und Microsoft (AppLocker) setzen auf interne Schnittstellen, um auf Dateisystemebene eines oder mehrere der oben genannten Attribute zu prüfen. SecuLution verwendet ein eigenes Kernel-Modul, das die Zuweisung von RAM-Speicher für nicht erlaubte Codes unterbindet. Andere Anbieter dokumentieren das verwendete Verfahren gar nicht erst. Hier stellt sich die Frage: Welche Whitelisting-Lösung passt zu meinen Bedürfnissen? Der Aufwand für die Implementation und den folgenden Betrieb ist in der Regel entscheidend für die Auswahl einer dieser vielen Lösungen. Aufgrund der unterschiedlichen Konzepte stellen die Hersteller naturgemäß sehr verschiedene Ansätze zur Verfügung. So ergeben sich die größten Unterschiede zwischen den verfügbaren Produkten.

Dezentrale Policy: Lösungen, die auf Basis von Dateisystem-Attributen arbeiten, benötigen keine zentrale Datenbank, da durch das Dateisystem alles abgebildet wird. Eine der empfohlenen Vorgehensweisen für eine derartige Umsetzung besteht darin, Musterrechner zu erstellen und diese für Produktivsysteme zu duplizieren. Als Ergebnis hat der Administrator ein homogenes Netzwerk. Das wirkt sich positiv auf den Wartungsaufwand im Betrieb aus. Dieser Ansatz bringt jedoch auch den Nachteil mit sich, dass kurzfristige Änderungen im Alltag nur mit hohem Aufwand umgesetzt werden können oder sogar unmöglich sind. Für jede individuelle Softwareausstattung muss ein eigener Master gepflegt werden. Updates beispielsweise erfordern immer auch ein Update des jeweiligen Referenz-Images und aller Klone.

Zentrale Policy-Datenbank: Die Whitelist zentral im Netzwerk bereitzustellen ist ein zweiter Ansatz. Auf jedem Endpoint erzeugt eine Agent-Software vor dem Start einer Software deren individuellen Hash und gleicht so die Berechtigung in Echtzeit mit der zentralen Datenbank ab. Für den Anfang können Hashes für die zentrale Datenbank automatisch erfasst, klassifiziert und verwaltet werden, etwa durch einen Lernmodus, ohne dass der Administrator seine Infrastruktur selbst anpassen muss.
Einige Hersteller versprechen, so auch die komplizierte Software-Landschaft von Krankenhäusern zügig und ohne Mehraufwand in der Administration abbilden zu können. Lösungen dieser Art sind allerdings nur in entsprechend großen Netzwerken kosteneffizient einsetzbar. Alle Lösungen von Drittanbietern kosten mehr als klassische Virenscanner. Lediglich Microsofts AppLocker ist in bestimmten Versionen bereits Bestandteil von Windows. Reine Whitelisting-Lösungen finden sich zudem selten. Außerdem variiert der Leistungsumfang stark. Fast alle Application-Whitelists sind als Modul einer übergeordneten Produktlinie zu erwerben (sogenannte Multi-Layer-Ansätze).
Application Whitelisting als Hauptprodukt wird allerdings auch angeboten. Hier wird die Whitelist wiederum um weitere Features (zum Beispiel USB-Whitelists) modular ergänzt. Die Total Cost of Ownership sollte man dabei immer auch beachten: Das Produkt mit dem geringsten Wartungsaufwand ist nicht selten das teuerste in der Anschaffung. Weniger Folgekosten und ein positiver ROI (Return on Investment) stellen sich trotz höherer Anfangsinvestitionen teils schneller ein als gedacht.

Kann Whitelisting zu 100 Prozent schützen?

Naturgemäß kann auch Whitelisting nicht vor allem schützen. Auf internen Berechtigungen von Windows basierende Lösungsansätze beispielsweise sind dem Risiko ausgesetzt, dass ein Code mit Administrator- oder Systemrechten zur Ausführung kommt und damit das Whitelisting umgeht.
Eines der bekanntesten Beispiele ist ‚Eternalblue', die 2017 aufgedeckte Sicherheitslücke, die von der Ransomware WannaCry ausgenutzt wurde. Fehler im SMB-Dienst von Windows ermöglichten erfolgreiche Angriffe über diese Sicherheitslücke. Angreifer konnten ihren Code mit den gleichen Rechten ausführen, die der angegriffene Prozess besaß.
Der Payload des Angreifers kann gespeichert und gestartet werden, da der Code des Angreifers mit höchsten Rechten ausgeführt werden kann. Eine Application-Whitelisting-Lösung, die sich ausschließlich auf das Windows-interne Berechtigungsmodell stützt, bietet damit an dieser Stelle keinen Schutz. Mit AppLocker geschützte Netzwerke wurden in der Folge erfolgreich von WannaCry angegriffen.
Andere Whitelisting-Lösungen können in solchen Szenarien auch einen Code blockieren, der unter den Berechtigungen des Administrator- oder Systembenutzers ausgeführt werden soll, da hier der Code, weil unbekannt, einfach an der Ausführung gehindert wird.
Doch was sind die Schwachstellen der so sicher erscheinenden Hash-basierten Lösungen? Scripte werden nicht über denselben Weg ausgeführt wie Anwendungen. Ein Interpreter wie WScript, der in der Regel zu den erlaubten Anwendungen zählt, kann ein Script ungehindert ausführen, da es nicht der Kontrolle durch die Application Whitelist unterliegt.
In der Praxis bedeutet dies jedoch nicht zwangsläufig eine Einschränkung der Sicherheit. Makroviren-Angriffe zum Beispiel können technisch in zwei Stufen eingeteilt werden: Das Makro selbst dient als ‚Dropper', ist also gar nicht der Virus, wie der Name vermuten lässt. Dieser Dropper legt die eigentliche Schadsoftware auf dem angegriffenen System ab und versucht sie zu starten. Dieser Startversuch unterliegt dann jedoch wieder der Kontrolle des Whitelisting und wird demzufolge unterbunden, da die eingeschleuste Malware nicht bekannt ist.
Ein Sonderfall ist die PowerShell: Damit hat Microsoft einen Interpreter bereitgestellt, der jedem Benutzer zur Verfügung steht und derart mächtig ist, dass damit sogar komplette Ransomware geschrieben werden kann. Schutz bietet hier die sogenannte Application Control. In der Whitelist selbst beschränkt der Administrator die Ausführung der PowerShell auf bestimmte Benutzer oder verbietet die Anwendung gar vollständig.
Application-Whitelisting-Produkte sind vielfältig und so unterschiedlich, dass sich Erfahrungen mit einzelnen Lösungen keineswegs eins zu eins auf andere übertragen lassen. Prüfverfahren, Implementierung, Alltagsbetrieb, Wartung usw. unterscheiden sich bei den Lösungen so grundsätzlich voneinander, dass letztlich nur ein individueller Test im eigenen Netzwerk aussagekräftig sein kann.
Jeder Administrator stellt seine eigenen Anforderungen an seine Sicherheitslösung und jedes Netzwerk stellt andere Kompatibilitätsanforderungen an die eingesetzte Lösung. Kostenfreie Teststellungen einiger Hersteller können hier jedoch helfen, die richtige Lösung für das Netzwerk zu finden.
Wichtig ist jedoch, dass Application Whitelisting fast alle Angriffe, die wir in den letzten zwei Jahren kennengelernt haben, verhindert hätte [3] und hat. Moderne Lösungen bieten zudem denselben Komfort wie es ein Virenscanner im Alltag tut, sie sind allerdings sicherer.

Torsten Valentin

Kontakt

SecuLution GmbH
Torsten Valentin
Alter Hellweg 6b
59457 Werl
Tel.: +49 2922 958-9210
info@seculution.com
www.seculution.de

Literatur

1. Sedgewick, A., Souppaya, M., Scarfone, K.: Guide to Application Whitelisting. NIST Special Publication 800-167, Oktober 2015, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-167.pdf
2. Definition von Application Whitelisting: Was ist Application Whitelisting und wie kann es Netzwerke vor Schadsoftware jeglicher Art schützen? www.application-whitelisting.de/#Application%20Whitelisting%20im%20Detail
3. www.cubespotter.de/cubespotter/rsac2018-einblicke-von-der-rsa-konferenz/