Funktioniert Application Whitelisting?

Was ist Application Whitelisting?

Application Whitelisting ist ein Konzept, bei dem eine Liste von Programmen existiert, die ausgeführt werden dürfen, während alles andere nicht funktionieren darf.

Die fortschrittlichsten Application-Whitelist-Technologien kombinieren eine Art Quell- und Ziellogik. Zum Beispiel könnte eine Application Whitelist besagen: „Windows Notepad darf auf den Ordner Steuern auf meinem Desktop zugreifen, Microsoft Word jedoch nicht.“

Wir werden dies weiter untersuchen, aber generell verlassen sich Verteidigungsstrategien mittels Application Whitelisting stark auf diese beiden Variablen:

1. Die Angreifer stimmen zu, sich an die Regeln zu halten, die Sie im Hinblick auf Ihr Application-Whitelisting-Cybersicherheitstool festgelegt haben.
2. Ihre Umgebung ist sehr klein, mit wenigen Anwendungen, die relativ stabil bleiben und keine Exploits aufweisen.

Nachteile von Application-Whitelisting-Technologien

Komplexität

IT-Netzwerke sind wie komplexe Organismen

Selbst kleine IT-Netzwerke sind sich ständig verändernde Gebilde mit einer Vielzahl von Verhaltensweisen. Anwendungen werden von Benutzern ständig hinzugefügt und entfernt. Module innerhalb von Anwendungen werden von den Programmherstellern ständig hinzugefügt und entfernt, insbesondere bei Updates. Schließlich werden Anwendungsverhalten – zusätzlich zu Codeänderungen, die zu Verhaltensänderungen führen – von verschiedenen Benutzern zu

unterschiedlichen Zeiten auf unterschiedliche Weise genutzt. Stellen Sie sich nun das Team vor, das diese ständige Verfolgung unterstützen müsste, sowie die IT-Helpdesk-Tickets, die dabei fortlaufend eingehen würden.

Realistisch betrachtet ist die einzige stabile IT-Umgebung eine, die durch Kioske angetrieben wird, bei denen Programme installiert werden, ohne dass sie aktualisiert, hinzugefügt oder entfernt werden können, und bei denen Benutzer nur eng begrenzt eine oder zwei Funktionen ausführen dürfen. Vielleicht ein Kiosk für den Fotodruck oder Ähnliches. In diesem Fall müsste die Application Whitelist nur jedes Mal aktualisiert werden, wenn das Kiosk-Terminal zum Beispiel zweimal jährlich ein Upgrade erhält.

Fortschrittlichere Application Whitelists bedeuten mehr Komplexität

Die einfachsten Application Whitelists bestehen lediglich aus Listen von Programmen, die im System eines Benutzers existieren dürfen.

Dies allein kann bereits eine Herausforderung im Management darstellen, führt aber zu einer Vielzahl möglicher Erweiterungen.

Zum Beispiel: Nur weil die Personalabteilung (Payroll) eine Anwendung zur Interaktion mit dem Gehaltsabrechnungssystem des Unternehmens hat, sollte es dann nicht ein separates Regelwerk für das Lagerteam geben, das andere (nicht mit der Gehaltsabrechnung zusammenhängende) Anwendungen nutzt?

Erweiterungen dahingehend, welche Abteilungen oder Benutzer welche Anwendungen ausführen dürfen, sind also eine naheliegende Erweiterung. Eine Erweiterung, die nun zusätzliche Komplexität schafft, zusätzlich zur bloßen Verfolgung der Anzahl, Art und Versionen der Programme in Ihrem Netzwerk.

Nehmen wir nun an, wir benötigen einen weiteren Satz von Erweiterungen – wir müssen entscheiden, welcher Benutzer Zugriff auf welche Anwendung für welchen Datensatz hat.

Das ergibt ebenfalls vollkommen Sinn, nicht wahr? Sie möchten nicht, dass Ihr Lagerteam Zugriff auf die HR-Daten hat, und das HR-Team benötigt vermutlich keinen Zugriff auf die Betriebsdaten des Lieferteams im Lager.

Das ist eine geradezu absurd komplexe Menge an Kombinationen, die es zu verfolgen gilt, jetzt, da Datenspeicherorte als zusätzliche Variable hinzugekommen sind.

Mit jeder notwendigen Erweiterung, um Application-Whitelisting-Technologien wirksam zu machen, wird also die Verwaltung, Konfiguration und der laufende (man könnte sagen nie endende, stets eskalierende) Support, der zur Aufrechterhaltung der Funktionsfähigkeit erforderlich ist, die Technologie unbrauchbar machen. Das Ergebnis ist normalerweise, dass großen Benutzergruppen

Zugriff auf große Gruppen von Anwendungen gewährt wird – und wahrscheinlich auf nahezu alle Daten. Damit entsteht eine nahezu nutzlose Konfiguration der Technologie, da kein Unternehmen über die Ressourcen verfügt, um sie ordnungsgemäß zu verwalten.

Anwendungen interagieren miteinander

In modernen Betriebssystemen ist es üblich, dass Anwendungen mit anderen Anwendungen interagieren. Manchmal beruht diese Interaktion auf einer Integration zwischen zwei Anwendungen, die das Benutzererlebnis verbessert – etwa wenn ein Word-Dokument Microsoft Photos öffnet. In anderen Fällen (dies kommt sehr häufig vor) gibt es Aufrufe zwischen Programmen, die auf eine Weise erfolgen, die für den Endbenutzer in der Regel unsichtbar ist.

Revision #1
Created 2026-07-24 04:24:25 UTC by Dennis Underwood
Updated 2026-07-24 04:24:25 UTC by Dennis Underwood