DriveLock
securing your digital tomorrow

DriveLock Application Behavior Control: Applikationskontrolle mit noch mehr Sicherheit

Im Zuge der Digitalisierung kommt den Themen Datenschutz und -sicherheit in Unternehmen eine immer größere Bedeutung zu. Zu den effektivsten Lösungen, um Angriffe und Datenschutzverletzungen zu vermeiden, zählt die Applikationskontrolle. Application Behavior Control hebt diesen Schutz auf eine noch höhere Sicherheitsstufe.

Die Anzahl der Cyberangriffe wächst kontinuierlich. Angreifer gehen immer gezielter und trickreicher vor. Allein 2019 gab es über 1 Mrd. verschiedener Malware- und Ransomware-Varianten, mit verheerenden Folgen.

Applikationskontrolle in Kombination mit Application Behavior Control – der effektivste Schutz gegen jegliche Art von Schadsoftware.

Intelligente Applikationskontrolle mit Whitelisting ermöglicht Administratoren, die Ausführung jeder beliebigen Anwendung anhand einer Positivliste zugelassener Programme zu kontrollieren. Aber auch dieser Schutz lässt sich noch optimieren. Bei „traditionellen" Angriffsarten wird primär externe Malware auf dem Zielsystem installiert oder ausgeführt. Darüber hinaus nutzen Angreifer bei dateiloser Schadsoftware, z. B. „Living off the land"-Methoden, zugelassene Administrations- bzw. System-Tools, die bereits auf dem Zielsystem vorhanden sind, um einen Angriff zu initiieren.

Vorteile Application Behavior Control:

- + ERWEITERTE ANTI-MALWARE-FÄHIGKEITEN
- + KEINE UMGEHUNG DER APPLIKATIONS-WHITELIST
- + KEIN DURCHKOMMEN FÜR ANGREIFER
- + MINIMALER ADMINISTRATIVER AUFWAND
- + ZENTRALE VERWALTUNG
- + SELF-SERVICE FÜR ENDBENUTZER
- + CLOUD- UND ON PREMISE LÖSUNG
- + EINHALTUNG GESETZLICHER VORSCHRIFTEN

Kurzum – auch Anwendungen auf der Whitelist können eine potenzielle Gefahr darstellen, wenn sie in ihrem Verhalten und Berechtigungen nicht eingeschränkt werden.

Aufbauend auf DriveLock Application Control **bietet die Application Behavior Control zusätzliche Sicherheit, indem sie das Anwendungsverhalten mit Hilfe von Anwendungsberechtigungen kontrolliert**. Anwendungsberechtigungen stellen erweiterte Anti-Malware-Fähigkeiten bereit und bieten noch bessere Prävention gegen die eventuelle Umgehung der Anwendungs-Whitelist. Sie können legitime, auf einer Whitelist verzeichnete Programme auf minimal erforderliche Aktionen und Berechtigungen einschränken. So stellen Sie sicher, dass nur autorisierte Software und Skripte ausgeführt oder von Ihnen weitere Prozesse gestartet werden. Sie kontrollieren auch den Zugriff auf Skript-Werkzeuge wie MS PowerShell, VBS, Python und die Befehlszeile.

Cyberbedrohungen - Status Quo

- **DIGITALISIERUNG LÄSST UNTERNEHMENSGRENZEN VERSCHWINDEN**
- **MEHR ALS 50 % ALLER UNTERNEHMEN SIND ZIEL EINES ANGRIFFS**
- **DATEIBASIERTE ODER DATEILOSE ATTACKEN MIT HILFE VON SKRIPTS, MAKROS ODER MS OFFICE**
- **Ø FOLGEKOSTEN EINER ATTACKE: 3,9 MIO. €**

Vorteile der Anwendungsberechtigungen

- Sie verhindern, dass aus einer erlaubten Anwendung heraus eine weitere Anwendung (bzw. Prozess, Skript) gestartet wird, die eine potenzielle Gefahr für das System darstellen könnte.
- Sie legen fest, welche Art von Zugriff einer bestimmten Anwendung erlaubt wird (z. B. lesend/schreibend auf Dateien oder auf die Registry zugreifend).
- Sie bieten einen besseren Schutz gegen dateilose („fileless") Angriffe. Zudem können diese Regeln den Aufruf von bestimmten untergeordneten Prozessen blockieren.

Weitere Vorteile

- **AUTOMATISCHES LERNEN DES APP-VERHALTENS ERSTELLT LOKALE REGELN UND ENTLASTET ADMINISTRATOREN.**
- **DIE TEMPORÄRE ÜBERWACHUNG VON ANWENDUNGEN HILFT ADMINISTRATOREN, EINSCHRÄNKUNGEN DES ANWENDUNGSVERHALTENS GEZIELTER UND SCHNELLER FESTZULEGEN.**
- **SCHNELL ANWENDUNGSREGELN FÜR EINE GANZE ANWENDUNGSKATEGORIE ERSTELLEN**

Weniger Aufwand durch automatisches Lernen und Applikationskategorien

Um die Administration zu vereinfachen und IT-Abteilungen zu entlasten, kann das richtige Anwendungsverhalten automatisch gelernt werden. Dazu werden Anwendungen über einen gewissen Zeitraum beobachtet und deren Verhalten entweder als zentrale Richtlinien (Policies) übernommen oder wie bei einer lokalen Whitelist für den Computer gemerkt. Danach darf die Anwendung nur noch gelernte Operationen durchführen.

„Application Collections" sind eine Sammlung von Applikationen, die thematisch zusammengehören. Sie können Applikationen gleichen Typs enthalten, z. B. Browser oder E-Mail Clients. Anstatt für jede Anwendung individuelle Regeln zu erstellen, können Sie eine Regel für eine ganze Kategorie von Anwendungen erstellen. Dadurch reduzieren Sie Ihren Regelsatz und halten ihn einfach.

Wichtige Anwendungsfälle/Szenarien

- **Starten von PowerShell:** Sie wollen verhindern, dass Ihr Browser PowerShell startet und so womöglich Schadsoftware auf den Computer gelangt. **Lösung:** Sie erstellen eine Regel, die dem Browser und allen von ihm gestarteten Prozessen verbietet, PowerShell zu starten.
- **E-Mail-Client und Browser dürfen nur autorisierte Aktionen ausüben**, wie z. B. das Schreiben in bestimmten Verzeichnissen oder das Starten von legitimierten Anwendungen. **Lösung:** Laden einer DLL. Sie legen fest, dass Dynamic Link Libraries (DLLs) nur aus bestimmten Verzeichnissen geladen werden dürfen, um zu vermeiden, dass beispielsweise der Windows Media Player DLLs von Netzlaufwerken lädt.
- **Skriptausführung:** Sie wollen verhindern, dass Browser VB-Skripte ausführen.
- **Lesen eines bestimmten Verzeichnisses:** Sie wollen sicherstellen, dass nur eine bestimmte Applikation auf ein ganz bestimmtes Verzeichnis lesend zugreifen kann. Durch eine Sicherheitslücke im Browser wäre es möglich, dass eine Schadsoftware sich Lesezugriff auf dieses Verzeichnis verschafft und somit Ihre Bankdaten auslesen kann. Dies lässt sich durch Anwendungsberechtigungen verhindern.

DriveLock – Features

- + SELBSTLERNENDES APPLIKATIONSVERHALTEN
- + GEZIELTES BLOCKIEREN VON UNTERPROZESSEN
- + EINSCHRÄNKEN LEGITIMER APPLIKATIONEN AUF ERFORDERLICHE AKTIONEN UND BERECHTIGUNGEN
- + ZUGRIFFSREGELUNG DER APPLIKATIONEN AUF DATEISYSTEM UND REGISTRY
- + BERECHTIGUNGS-HIERARCHIEN REGLEMENTIEREN
- + BESCHRÄNKUNG VON DATEI- UND VERZEICHNISFILTER
- + ZENTRALES DASHBOARD

DriveLock: Experte für IT- und Datensicherheit seit mehr als 20 Jahren

Das deutsche Unternehmen DriveLock SE wurde 1999 gegründet und ist inzwischen einer der international führenden Spezialisten für cloud-basierte Endpoint-und Datensicherheit. Die Lösungen umfassen Maßnahmen der Prävention wie auch zur Erkennung und Eindämmung von Angreifern im System.

DriveLock ist Made in Germany mit Entwicklung und technischem Support aus Deutschland.