Reduktion der Angriffsfläche in Microsoft Defender mit Gruppenrichtlinien oder PowerShell aktivieren

Microsoft Defender bietet neben dem Virenscanner noch weitere Sicherheitsfunktionen. Zu diesen gehört die Reduktion der Angriffsfläche, mit der sich Anwendungen wie Office, Browser oder Adobe Reader härten lassen. Das Feature ist standardmäßig nicht aktiv und lässt sich per Gruppenrichtlinie oder PowerShell konfigurieren.

Zu den gängigen Einfallstoren für Angreifer gehören Anhänge von E-Mails, die schädlichen Code in Form von Scripts, ausführbaren Dateien oder in Office eingebettete Makros enthalten. Zu den weiteren Angriffspunkten zählen ganz besonders auch Web-Browser sowie weit verbreitete Programme wie Adobe Reader, die regelmäßig durch Schwachstellen auffallen.

Ergänzung zu App-spezifischen Maßnahmen

Neben den Maßnahmen, die Admins durch die Konfiguration der Anwendungen selbst ergreifen können, bietet Defender eine zusätzliche Schutzschicht. So lassen sich etwa Makros in Office mit Hilfe von Gruppenrichtlinien weitgehend zähmen, aber die Regeln zur Reduktion der Angriffsfläche (Attack Surface Reduction, ASR) dichten diese noch weiter ab.

So kann man damit Office am Erzeugen von ausführbarem Code, am Einfügen von Code in untergeordnete Prozesse oder am Erstellen von Kindprozessen hindern. Letzteres lässt sich auch für den Adobe Reader durchsetzen. Defender kann zudem ausführbare Inhalte blockieren, wenn diese über einen Mail-Client auf den Rechner gelangen.

Interessant ist zudem die Einstellung für den erweiterten Schutz vor Ransomware. Sie bezieht Informationen zu einer verdächtigen Datei aus der Microsoft Cloud und prüft etwa anhand der Häufigkeit ihres Auftretens oder erwiesener Harmlosigkeit, ob von ihr eine Gefahr ausgeht. Die Funktion setzt voraus, dass der Cloud-basierte Schutz aktiv ist.

Limitierte Management-Optionen

Die Reduktion der Angriffsfläche ist nicht nur in kostenpflichtigen Produkten wie Defender for Endpoint enthalten, sondern gehört zum Lieferumfang von Windows 10 / 11 sowie von Windows Server, wobei auf älteren Versionen einige Regeln nicht unterstützt werden.

Der große Nachteil der kostenlosen Version besteht in den reduzierten Möglichkeiten für das Management und Reporting. Eine GUI in der App Einstellung existiert dafür überhaupt nicht, die Administration der Regeln erfolgt über Gruppenrichtlinien oder PowerShell.

Sie beschränkt sich auf das Aktivieren bzw. Deaktivieren einzelner Regeln sowie auf das optionale Definieren von Verzeichnissen und Dateien, die davon ausgenommen sein sollen.

Evaluierung über den Audit-Modus

Per Voreinstellung ist ASR nicht aktiviert. Admins sollte aber in jedem Fall einen Blick auf die Regeln werfen und prüfen, welche sich für ihre Umgebung eignen.

Man muss diese nicht gleich scharf schalten, sondern kann sie erst im Audit-Modus betreiben und beobachten, welche Auswirkungen sie haben würden.

ASR über PowerShell verwalten

PowerShell kommt die Aufgabe zu, den aktuellen Status der ASR-Regeln abzurufen:

```
Get-MpPreference | select AttackSurfaceReductionRules_Ids, AttackSurfaceReductionRules_Actions
```

Dieser Aufruf zeigt an, welche Regeln konfiguriert wurden und welchen Status sie haben. Allerdings erhält man dabei nicht ihren Namen, sondern nur eine GUID. Die Tabelle am Ende des Textes (Quelle) löst diese auf.

Für den Status ("Actions") sind die Werte 0, 1, 2 und 6 vorgesehen. Dabei steht 0 für deaktiviert, 1 für aktiviert, 2 für den Audit-Modus (bloße Protokollierung, sobald eine Regeln ausgelöst würde) sowie 6 für Warnung, bei der User einen Hinweis auf die mögliche Gefahr erhalten, aber die Blockierung umgehen können.

Wenn man Regeln konfigurieren möchte, dann sieht das Cmdlet Set-MpPreference für den Parameter

AttackSurfaceReductionRules_Actions statt dieser numerischen Werte die Konstanten Disabled, Enabled und AuditMode vor. Dagegen gibt man für AttackSurfaceReductionRules_Ids wieder die GUID an.

Um beispielsweise Adobe Reader am Starten von Kindprozessen zu hindern, geht man mit PowerShell so vor:

```
Set-MpPreference `
-AttackSurfaceReductionRules_Ids 7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c `
-AttackSurfaceReductionRules_Actions Enabled
```

Um Ausschlüsse für Verzeichnisse und Dateien zu definieren, ruft man Set-MpPreference nach diesem Muster auf:

Set-MpPreference -AttackSurfaceReductionOnlyExclusions "c:\windows"

Den Status dieser Eigenschaft fragt man dann mit diesem Befehl ab:

Get-MpPreference | select AttackSurfaceReductionOnlyExclusions

ASR-Regeln über Gruppenrichtlinien konfigurieren

Für das zentrale Management von ASR stehen in den Gruppenrichtlinien zwei Einstellungen zur Verfügung, eine für die Aktivierung bzw. Deaktivierung von Regeln und die andere für die Definition der Ausschlüsse.

Beide befinden sich unter Computerkonfiguration => Richtlinien => Administrative Vorlagen => Windows-Komponenten => Microsoft Defender Antivirus => Microsoft Defender Exploit Guard => Verringerung der Angriffsfläche.

Anstatt einfach für jede Regel eine eigene Option zu aktivieren, muss man für alle eine gemeinsame Einstellung verwenden ("Regeln zur Verringerung der Angriffsfläche konfigurieren"). Dort trägt man die oben erwähnte GUID sowie den Wert für die Action in eine Tabelle ein.

Um Ausschlüsse für Verzeichnisse und Dateien einzurichten, konfiguriert man die andere Einstellung in diesem Ordner. Auch hier trägt man alle Wertnamen in eine Tabelle ein, für den Wert in der rechten Spalte wählt man hier grundsätzlich 0.

ASR im Eventlog beobachten,

Nachdem die Bordmittel für ASR kein Reporting vorsehen, muss man sich auf die Auswertung der Logs beschränken. Die Aufzeichnung erfolgt unter Anwendungs- und Dienstprotokolle => Microsoft => Windows => Windows Defender => Operational.

Von Interesse sind hier die folgenden IDs:

Ereignis-ID Beschreibung

5007 Einstellungen wurden geändert

1121 Auslösen einer Regel im Blockierungsmodus

1122 Auslösen Einer Regel Im Überwachungsmodus (Audit-Modus)

Um diese Events zu beobachten, kann man in der Ereignisanzeige eine benutzerdefinierte Ansicht erstellen.

Alternativ kann man die Log-Einträge auch mit PowerShell abfragen:

```
Get-WinEvent -LogName 'Microsoft-Windows-Windows Defender/Operational' |

where {$_.ID -eq "5007" -or $_.ID -like "112?"}
```

Fazit

Die Reduktion der Angriffsfläche kann einen wichtigen Beitrag leisten, um die Sicherheit der am meisten attackierten Anwendungen zu erhöhen. Das Feature gehört zum Lieferumfang aller aktuellen Windows-Versionen, ist aber per Voreinstellung nicht aktiviert.

Möchte man keinen kostenpflichtigen Service wie Defender for Endpoint oder ein Management-Tool wie ConfigMgr bzw. von einem Drittanbieter einsetzen, dann ist man auf die Verwaltung mittels Gruppenrichtlinien und PowerShell beschränkt. Dabei fehlen vor allem vernünftige Fähigkeiten für das Reporting.

Wenn man ASR im Unternehmen einführt, dann sollte man mit dem Überwachungsmodus starten und anhand des Eventlogs studieren, welche Auswirkungen die Regeln in der Praxis hätten. Ist keine größere Beeinträchtigung der User zu erwarten, dann kann man sie scharf schalten.

Namen der Regeln und ihre GUIDs

Regelname Regel-GUID

Missbrauch von gefährdeten signierten Treibern blockieren
56a863a9-875e-4185-98a7-b882c64b5ce5

Adobe Reader am Erstellen von untergeordneten Prozessen hindern 7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c

Alle Office-Anwendungen am Erstellen von untergeordneten Prozessen hindern d4f940ab-401b-4efc-aadc-ad5f3c50688a

Diebstahl von Anmeldeinformationen aus dem Subsystem für die lokale Sicherheitsautorität (lsass.exe) blockieren 9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2

Ausführbare Inhalte aus E-Mail-Client und Web-E-Mail blockieren
be9ba2d9-53ea-4cdc-84e5-9b1eeee46550

Ausführbare Dateien an der Ausführung hindern, außer sie erfüllen ein Verbreitungs-, Alters- oder vertrauenswürdige Listen-Kriterium 01443614-cd74-433a-b99e-2ecdc07bfc25

Ausführung potenziell verborgener Skripts blockieren 5beb7efe-fd9a-4556-801d-275e5ffc04cc

JavaScript und VBScript am Starten heruntergeladener ausführbarer Inhalte hindern
d3e037e1-3eb8-44c8-a917-57927947596d

Office-Anwendungen am Erstellen ausführbarer Inhalte hindern
3b576869-a4ec-4529-8536-b80a7769e899

Office-Anwendungen am Einfügen von Code in untergeordnete Prozesse hindern
75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84

Office-Kommunikationsanwendung am Erstellen von untergeordneten Prozessen hindern 26190899-1602-49e8-8b27-eb1d0a1ce869

Persistenz durch WMI-Ereignisabonnement blockieren

(Datei- und Ordnerausschlüsse werden nicht unterstützt). e6db77e5-3df2-4cf1-b95a-636979351e5b

Erstellung von Prozessen durch PSExec- und WMI-Befehle blockieren d1e49aac-8f56-4280-b9ba-993a6d77406c

Nicht vertrauenswürdige und nicht signierte Prozess, die von USB ausgeführt werden, blockieren b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4

Win32-API-Aufrufe von Office-Makros blockieren 92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b

Erweiterten Schutz vor Ransomware verwenden c1db55ab-c21a-4637-bb3f-a12568109d35

Eindeutige ID: #1017
Verfasser: n/a
Letzte Änderung: 2022-08-19 11:08