



E-BOOK
**MICROSOFT DEFENDER
MIT GRUPPENRICHTLINIEN
UND POWERSHELL
VERWALTEN**

Inhalt

Übersicht	4
Antivirus	4
Manipulationsschutz	5
Blockieren von Greyware	6
Schutz vor riskanten Downloads	7
Phishing-Schutz	8
Abwehr von Ransomware	8
Verringerung der Angriffsfläche	9
Management	9
Defender Antivirus konfigurieren	11
Ausschlüsse	12
Echtzeitschutz	13
Überprüfung anpassen	14
Reaktion auf gefundene Bedrohungen	15
Updates für Viren-Signaturen steuern	17
Defender mit Manipulationsschutz absichern	22
Reputationsbasierter Schutz	25
Warnung vor problematischen Websites	25
Abwehr von heruntergeladener Malware	25
Erweiterter Phishing-Schutz	25
Interaktive Konfiguration von SmartScreen	26
SmartScreen über Gruppenrichtlinien konfigurieren	27
Kein natives PowerShell-Management	29
Potenziell unerwünschte Anwendungen blockieren	30
Exploit Guard	33
Netzwerkschutz: Blockieren unliebsamer Websites	33
Reduktion der Angriffsfläche	36
Überwacher Ordnerzugriff gegen Ransomware	43
Microsoft Defender mit ACMP verwalten	48
Defender-Konfiguration über Profile	48
Flexible Zuweisung von Profilen	49
Schutz gegen Ransomware	50
Manipulationsschutz	51
Update der Signaturen	52
Reaktion auf gefundene Bedrohungen	53
Dashboard und Reports	54
Zusammenfassung	56

Über den Autor



Das E-Book wurde erstellt von Wolfgang Sommergut – Fachautor, Berater und Konferenzsprecher zu verschiedenen Themen der IT.

Übersicht

Unter der Marke *Defender* fasst Microsoft zahlreiche Windows-Features und Cloud-Services zusammen. Einige Schutzmechanismen sind erst kürzlich dazugekommen, andere wiederum wurden nachträglich umbenannt oder haben Namen, die sich schwer auseinanderhalten lassen (zum Beispiel *Exploit-Schutz versus Exploit Guard*).

Hinzu kommen Überlappungen in den Funktionen der diversen Komponenten, beispielsweise zwischen *SmartScreen* und *Netzwerkschutz*. Um mit den Bordmitteln eine gute Abwehr gegen verschiedene Bedrohungen aufzubauen, muss man sich also erst einen Überblick über deren Fähigkeiten verschaffen.

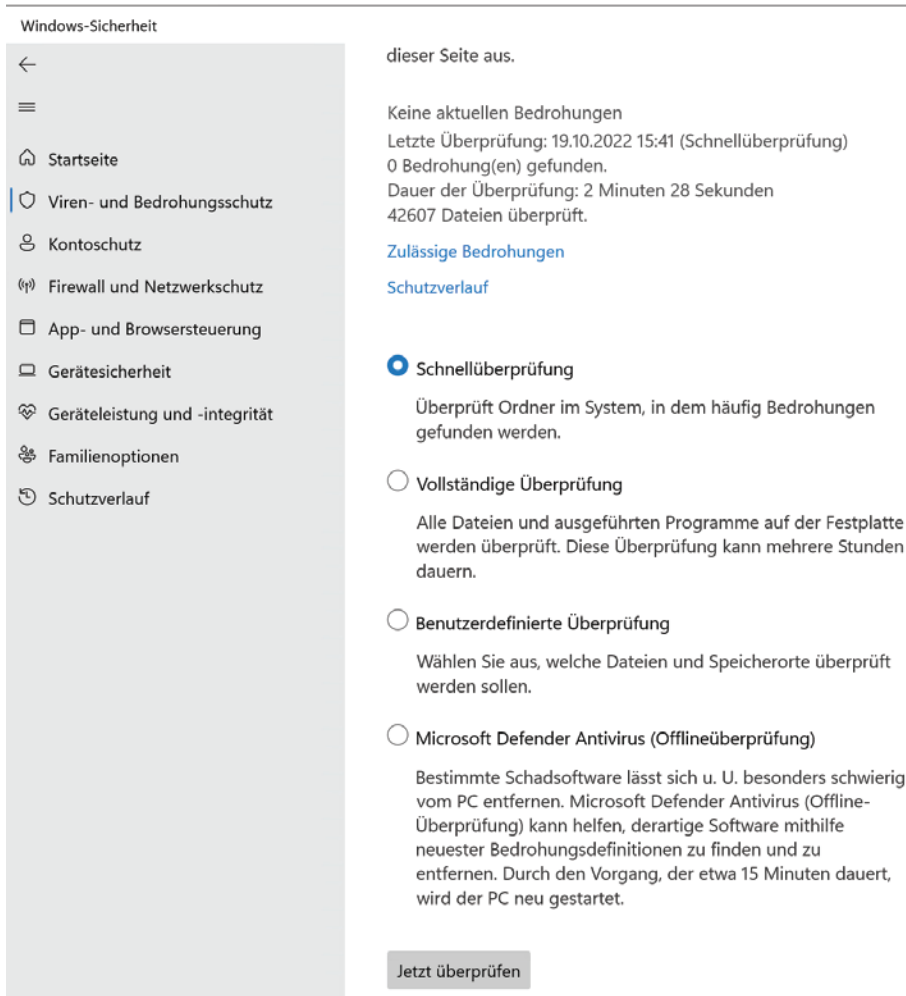
Aufgrund der inflationären Verwendung der Marke *Defender* umfasst diese auch Funktionen, die nicht unmittelbar oder ausschließlich der Abwehr von Malware oder Phishing gelten. Dazu zählt etwa die Sandbox Defender *Application Guard* für Edge und Office oder *Application Control* (WDAC), eine Lösung für das Whitelisting von Programmen.

Ähnliches gilt für die Defender Firewall, die natürlich auch einen Beitrag für die Sicherheit des Systems gegen alle Arten von Bedrohungen leistet. Das folgende E-Book widmet sich dagegen den Funktionen, die unmittelbar der Erkennung und dem Blockieren von schädlichen Programmen und Aktivitäten dienen.

Antivirus

Ein unabkömmlicher Schutzmechanismus für Endgeräte ist heutzutage ein Virens scanner, der auf Basis regelmäßig aktualisierter Signaturen das Dateisystem prüft. Dies kann in Echtzeit oder nach Zeitplan erfolgen. Ein zeitgemäßes Produkt beschränkt sich aber nicht nur auf die Entdeckung bekannter Malware, sondern bemerkt auch ein auffälliges Verhalten von Programmen.

Defender Antivirus schneidet in puncto Erkennung und bei der Zahl falscher Alarme ähnlich gut ab wie die Produkte führender Drittanbieter. Die [Tests von AV Comparatives](#) belegen die gute Performance von Microsofts Virens scanner.



Scan-Optionen für Microsoft Defender Antivirus

Während der Defender auf Consumer-PCs fast immer in der Standardkonfiguration läuft, muss der Scanner in professionellen Umgebungen oft an verschiedene Anforderungen angepasst werden. Das betrifft etwa Ausschlüsse für bestimmte Anwendungen oder das Update von Signaturdateien.

Die Mittel der Wahl sind für diesen Zweck die Gruppenrichtlinien und PowerShell. Die GUI der Windows-Sicherheit bietet dafür entweder keine Funktionen oder diese sind für Benutzer ohne administrative Rechte ohnehin nicht zugänglich.

Manipulationsschutz

Da Hacker nach einem erfolgreichen Einbruch meist versuchen, den Virenschanner zu deaktivieren, um ungestört ihre Schadprogramme platzieren zu können, erhielt Defender Antivirus einen Manipulationsschutz ("Tamper Protection").

The screenshot shows the Windows Security settings interface. On the left is a navigation pane with the following items: Startseite, Viren- & Bedrohungsschutz (highlighted), Kontoschutz, Firewall- & Netzwerkschutz, App- & Browsersteuerung, Gerätesicherheit, Geräteleistung und -integrität, and Familienoptionen. A red arrow points to the 'Manipulationsschutz' section in the main content area. This section is currently turned 'Ein' (On). Above it, 'Cloudbasierter Schutz' and 'Automatische Übermittlung von Beispielen' are also turned 'Ein'. On the right side of the screen, there are links for 'Datensch...' and 'Datensch...'.

Der Manipulationsschutz hindert sogar privilegierte User am Deaktivieren des Virenschanners

Er sorgt dafür, dass nicht einmal lokale Admins die Anti-Malware abschalten können. Dafür benötigt man eigens zugelassene Management-Tools wie Intune.

Blockieren von Greyware

Während der Virenschanner bedrohliche Software im Visier hat, sieht Microsoft für lästige, aber nicht unmittelbar gefährliche Programme eine separate Funktion vor. Es geht dabei um so genannte Greyware.

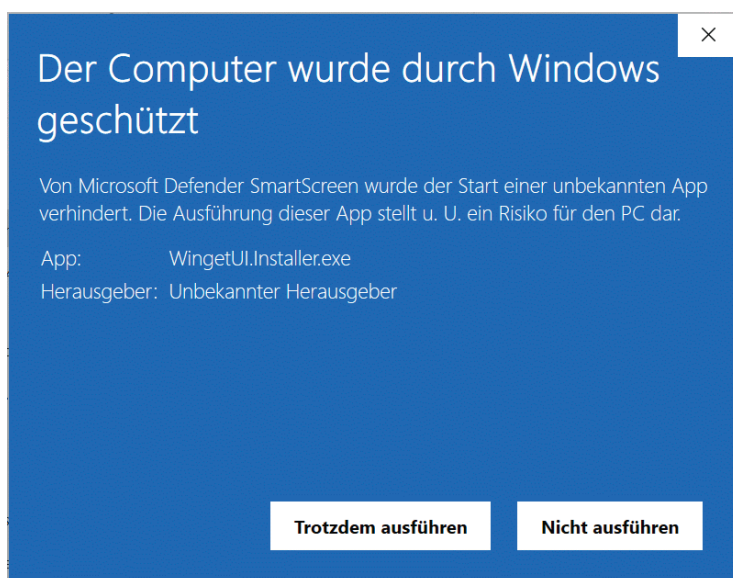
Zu den Aktivitäten solcher Programme gehört das Anzeigen von Werbung aus dubiosen Quellen, das Umleiten der Browser-Startseite oder die heimliche Nutzung des Computers für Krypto-Mining.

Um deren Download zu blockieren, bietet Windows eine Funktion gegen *potenziell unerwünschte Apps*. Sie unterstützt aktuell nur Microsofts Edge-Browser und ist seit Mitte 2021 per Voreinstellung aktiviert. Ihr Status lässt sich über eine Gruppenrichtlinie steuern.

Schutz vor riskanten Downloads

SmartScreen ist wie das Blockieren potenziell unerwünschter Apps ein reputationsbasierter Mechanismus. Er erfüllt zwei Aufgaben, nämlich Benutzer vor dem Besuch von wahrscheinlich schädlichen Websites zu warnen bzw. sie daran zu hindern, sowie das Herunterladen und Ausführen von Schadprogrammen zu unterbinden.

Um die Zuverlässigkeit von Apps zu bewerten, sammelt der Hersteller umfangreiche Daten zur Häufigkeit ihrer Downloads oder zur Vertrauenswürdigkeit von Websites, auf denen sie angeboten werden.



SmartScreen kann vor riskanten Downloads warnen oder deren Ausführung blockieren

Die Browser-Integration beschränkt sich auch hier auf Edge und ergänzt somit die Funktion gegen potenziell unerwünschte Apps. Es ist fraglich, warum Microsoft den Schutz vor problematischen Downloads in zwei separate Features aufteilt.

Möchte man eine systemweite Abwehr vor dubiosen Downloads, dann bietet Microsoft dafür einen weiteren Mechanismus namens [Netzwerkschutz](#) an. Er ist eine Funktion von Exploit Guard und operiert auf Kernel-Ebene.

```
Windows PowerShell
PS C:\Users\wolf.WINDOWSPRO> Get-MpPreference | select *NetworkProtection* | fl_
AllowNetworkProtectionDownLevel      : False
AllowNetworkProtectionOnWinServer    : False
DisableNetworkProtectionPerfTelemetry : False
EnableNetworkProtection                : 0
```

Status des Netzwerkschutzes mit PowerShell abfragen

Die zweite Fähigkeit von SmartScreen, nämlich vor dem Ausführen von wenig vertrauenswürdigen Apps zu warnen oder diese zu unterbinden, ist unabhängig davon, mit welcher Anwendung diese Programme heruntergeladen wurden. Neben einem Web-Browser könnte dies auch ein Mail-Client oder die *App* für den Microsoft Store sein. Den Schutz vor bösartigen Store-Apps muss man aber extra aktivieren.

In dieser Prüfung heruntergeladener Programme ergänzt SmartScreen den Virenschanner, indem es deren Reputation als zusätzliches Kriterium ins Spiel bringt.

Phishing-Schutz

Seit der Version 22H2 bietet Windows 11 einen Schutz gegen Phishing. Auch dieser fällt in die Kategorie der reputationsbasierten Funktionen, weil er die Eingabe von Passwörtern auf gefährlich erachteten Websites überwacht und die Benutzer dann zum Wechsel der Kennwörter auffordert.

Ein nützlicher Effekt des Phishing-Schutzes besteht darin, dass er die weit verbreitete Gewohnheit vieler User abstellt, ihre Passwörter für das Firmenkonto auch für alle möglichen Online-Dienste wiederzuverwenden.

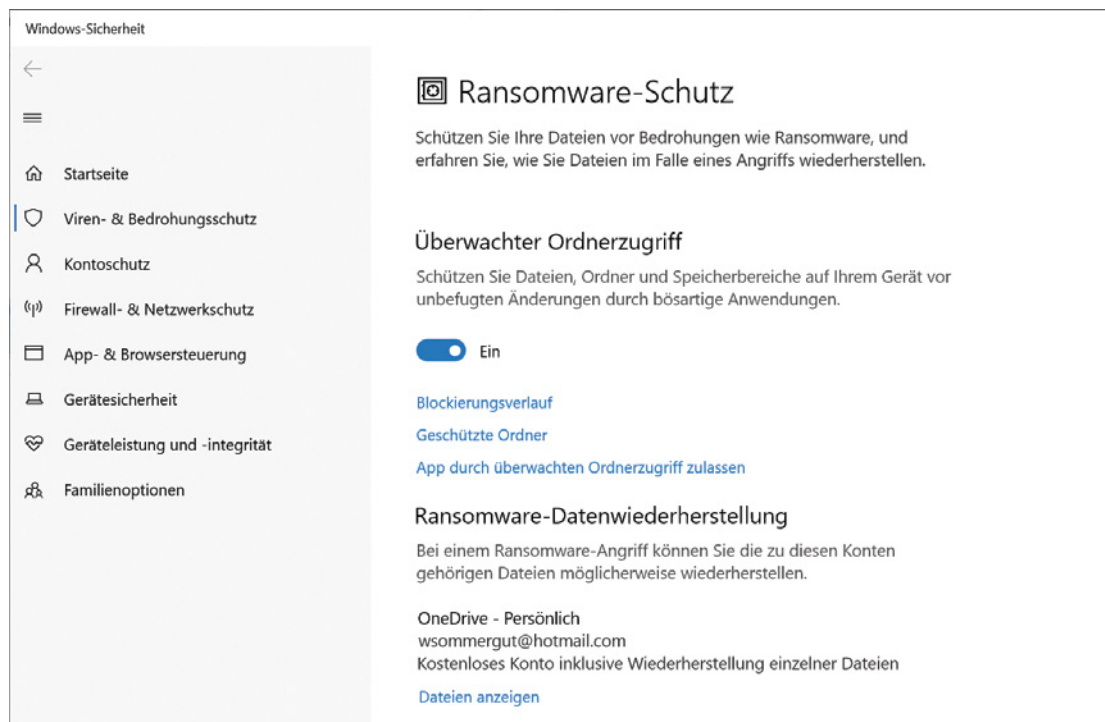
Darüber hinaus wacht das Tool darüber, dass Benutzer ihre Windows-, AD-, Azure-AD- und Microsoft-Kennwörter nicht in Office-Dokumenten oder Textdateien speichern.

Abwehr von Ransomware

Wie bei der Prüfung zweifelhafter Downloads ergänzt Microsoft den Virenschanner auch bei Ransomware um einen weiteren Mechanismus. Es handelt sich dabei um den [Überwachten Ordnerzugriff](#).

Sollte eine Ransomware trotz aktiviertem Antivirus auf den Rechner gelangen und keine Warnung von SmartScreen auslösen, dann bildet diese Funktion die letzte Verteidigungslinie. Sie blockiert in den gängigen Verzeichnissen des Benutzerprofils den Schreibzugriff durch suspekten Programme.





Flankierender Schutz vor Ransomware durch Blockieren von verdächtigen Schreibzugriffen

Es kommt jedoch regelmäßig vor, dass legitime Anwendungen am Schreiben gehindert werden. Diese kann man in eine Whitelist aufnehmen, was jedoch Admin-Rechte erfordert und sehr umständlich ist. In verwalteten Umgebungen wird man also nicht umhinkommen, die erlaubten Apps per GPO festzulegen.

Verringerung der Angriffsfläche

Unter dem Label Exploit Guard versammelt Microsoft drei Security-Features. Dazu gehören der bereits erwähnte Netzwerkschutz, der Überwachte Ordnerzugriff sowie die [Verringerung der Angriffsfläche](#) (Attack Surface Reducation, ASR).

Während die anderen hier vorgestellten Mechanismen auf Bedrohungen durch Programme oder Benutzeraktivitäten reagieren, besteht die ASR aus mehreren präventiven Maßnahmen.

Diese können Anwendungen wie Office oder Acrobat Reader härten, indem sie diese am Erzeugen von ausführbarem Code, am Einfügen von Code in untergeordnete Prozesse oder am Erstellen von Kindprozessen hindern.

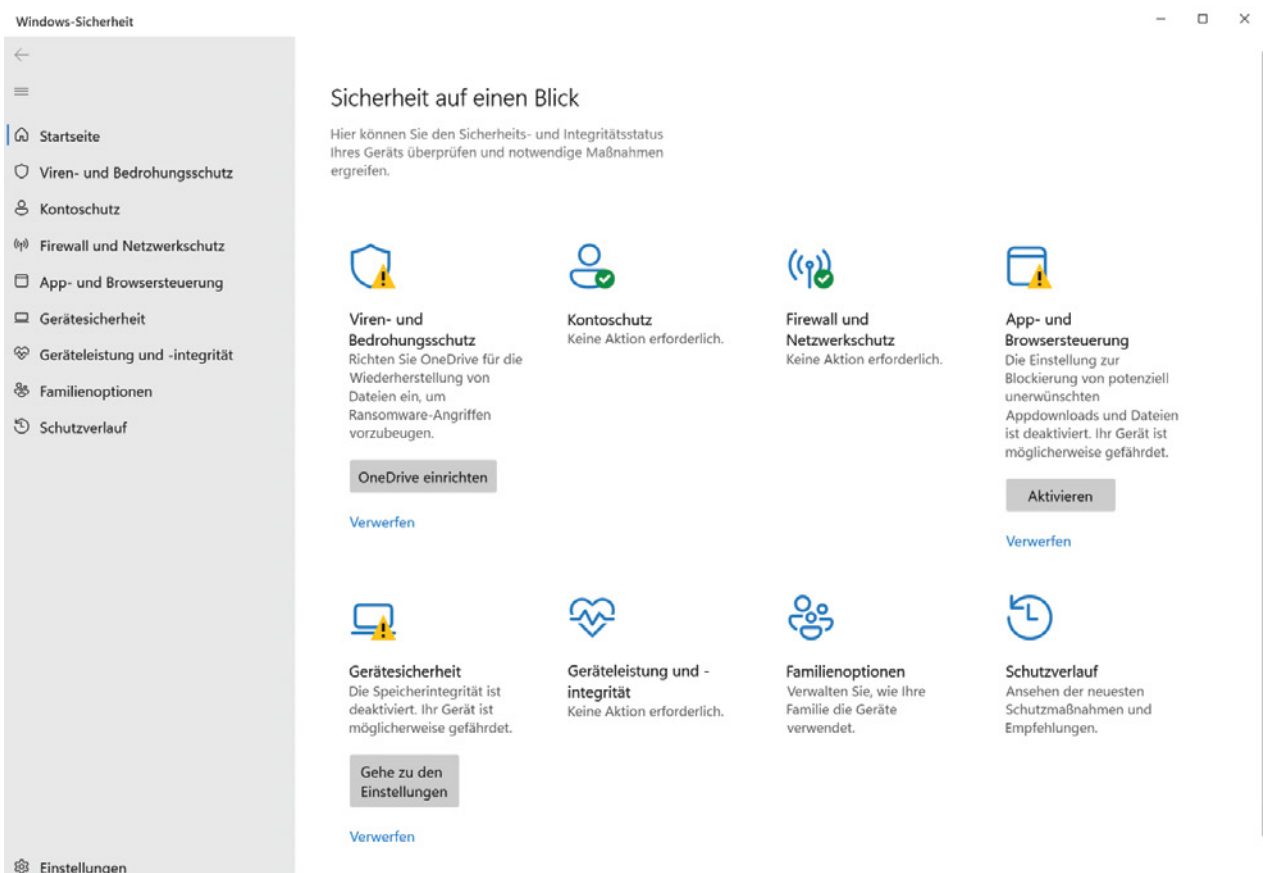
Management

Alle erwähnten Defender-Sicherheitsfunktionen gehören zum Lieferumfang von Windows und haben somit gegenüber Produkten von Drittanbietern den Vorteil, dass sie keine zusätzlichen Kosten verursachen.

Auf Rechnern von privaten Anwendern laufen sie in der Regel so, wie von Microsoft vorgegeben. Die Aufgabe der User besteht dort höchstens darin, die standardmäßig deaktivierten Funktionen einzuschalten. Hinzu kommt unter Umständen noch das Freigeben von Apps, die der überwachte Ordnerzugriff zu Unrecht blockiert.

In professionellen Umgebungen herrschen dagegen andere Anforderungen und Admins möchten dort sicherstellen, dass die gewünschten Sicherheitsfunktionen von den Benutzern nicht deaktiviert oder verändert werden.

Für das zentrale Management beschränken sich die Bordmittel jedoch auf die Gruppenrichtlinien und PowerShell. Damit fehlen beispielsweise die essentiellen Reporting-Funktionen für Security, um einen Überblick über den Status der Clients sowie eventuelle Vorkommnisse zu erhalten.



Das Sicherheits-Dashboard bietet Statusinformationen für einzelne PCs, ein übergreifendes Reporting bieten die Bordmittel nicht

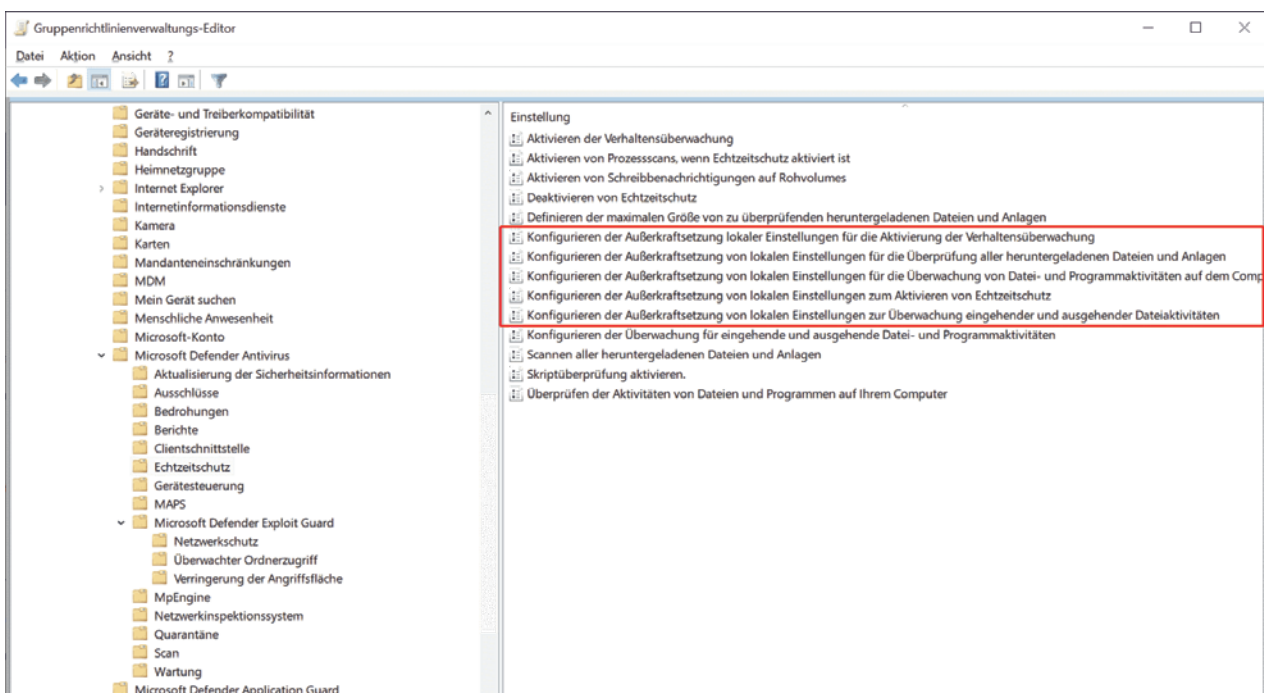
Microsoft bietet für diesen Zweck verschiedene kostenpflichtige Tools und Cloud-Services an, beispielsweise Defender for Endpoint, Defender for Business oder Intune. Stattdessen kann man natürlich auch zu Produkten von Drittanbietern greifen.

Defender Antivirus konfigurieren

Bevor man das Standardverhalten des Virenschutzes ändert, sollte man sich über die geplanten Maßnahmen im Klaren sein. Viele der verfügbaren Einstellungen mögen zwar die Performance erhöhen oder die Kompatibilität mit Anwendungen verbessern, aber falsch angewendet, vermindern sie den Schutz gegen Angriffe.

Viele Einstellungen lassen sich interaktiv in der Security App anpassen. In zentral verwalteten Umgebungen wird man diese Möglichkeit jedoch ausschließen, indem man die Konfiguration etwa über Gruppenrichtlinien vorgibt und damit eine lokale Änderung durch den User verhindert.

Microsoft sieht aber in den Gruppenrichtlinien eine ganze Reihe von Optionen vor, die es erlauben, **zentral vorgegebene Einstellungen lokal zu überschreiben**. Ihre Bezeichnung beginnt durchgängig mit "Konfigurieren der Außerkraftsetzung von lokalen Einstellungen für ..." ("Configure local setting override for ..."). Damit kann man etwa fortgeschrittene User von allgemeinen Vorgaben ausnehmen.



Mehrere Einstellungen sorgen dafür, dass die zentrale Konfiguration von Defender lokal überschrieben werden kann

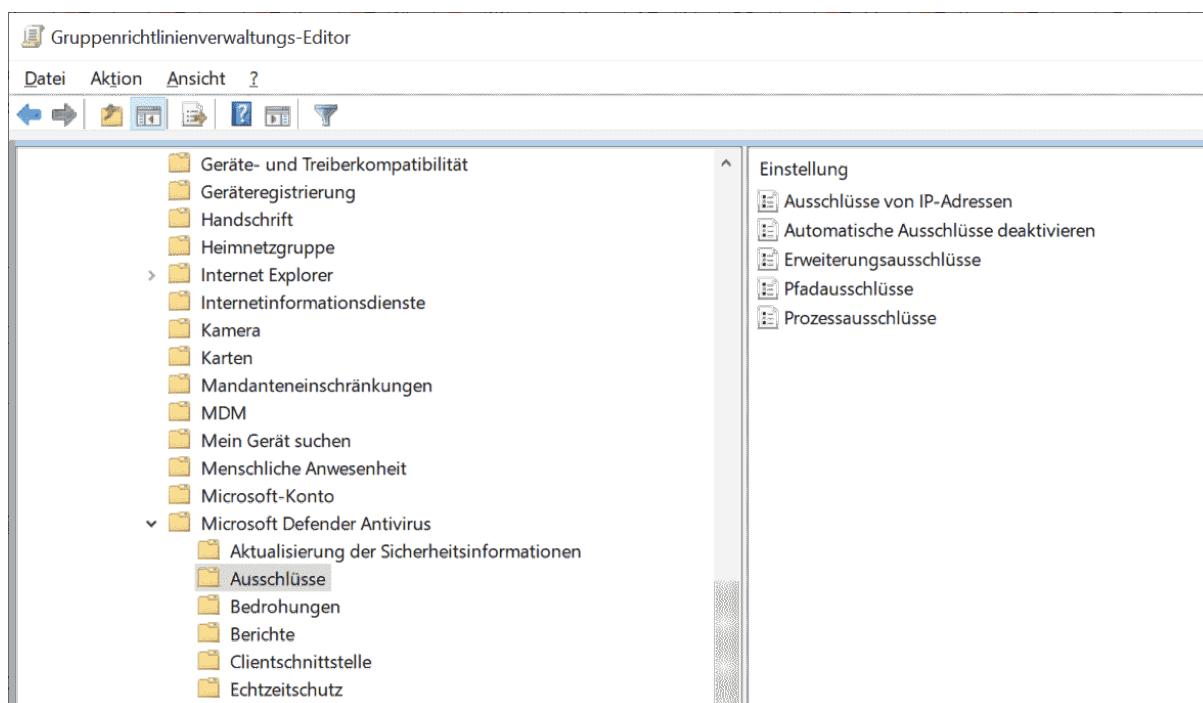
Neben Gruppenrichtlinien und der Security-App kann man auch PowerShell nutzen, um Defender den eigenen Anforderungen anzupassen. Zuständig dafür sind die Cmdlets `Set-MpPreference` und `Add-MpPreference`.

Ausschlüsse

Der Virenschanner kann bei bestimmten Anwendungen Probleme bereiten oder Performance-Probleme verursachen, wenn er etwa aktive Datenbanken prüft oder womöglich kritische Dateien unter Quarantäne stellt.

Aus diesem Grund ist es empfehlenswert, den Aktionsradius von Defender Antivirus einzuschränken. Es liegt jedoch auf der Hand, dass man dadurch auch den Schutz verringert.

Die Gruppenrichtlinien sehen für diesen Zweck fünf Einstellungen vor. Eine davon definiert keine Ausschlüsse, sondern deaktiviert jene, die Microsoft standardmäßig vorgibt. So vermeidet der Virenschanner etwa auf Domänen-Controllern die AD-Datenbank *ntds.dit*. Durch *Automatische Ausschlüsse deaktivieren* kann man dies verhindern.



Gruppenrichtlinien zur Definition von Ausschlüssen

Die vier anderen Einstellungen erlauben hingegen die Definition eigener Ausnahmen, entweder nach Pfad, Dateiendung, Prozessen oder IP-Adressen. Die beiden ersten sind selbsterklärend.

Bei Ausschlüssen nach Prozessen kann man Defender daran hindern, Dateien zu untersuchen, die von einem bestimmten Programm geöffnet wurden.

Antivirus prüft nicht nur das Dateisystem, sondern auch mehrere Protokolle, die als anfällig gelten. Über den Ausschluss von IP-Adressen kann man die Untersuchung von Anfragen verhindern, die von diesen Systemen kommen.

Definiert man Ausschlüsse mit PowerShell, dann sind für *Set-MpPreference* die Parameter *DisableAutoExclusions*, *ExclusionExtension*, *ExclusionIpAddress*, *ExclusionPath* und *ExclusionProcess* zuständig.

Ein Beispiel dafür wäre

```
Set-MpPreference -ExclusionExtension ".dat,.db"
```

Damit würde man Dateien mit der Endung .dat und .db vom Scan ausnehmen. Entfernen könnte man diese Ausschlüsse mit

```
Remove-MpPreference -ExclusionExtension ".dat,.db"
```

Echtzeitschutz

Ein wesentliches Feature von Defender Antivirus besteht darin, dass es Änderungen im Dateisystem oder der Registry laufend überwacht, um verdächtige Aktivitäten oder Objekte zu entdecken.

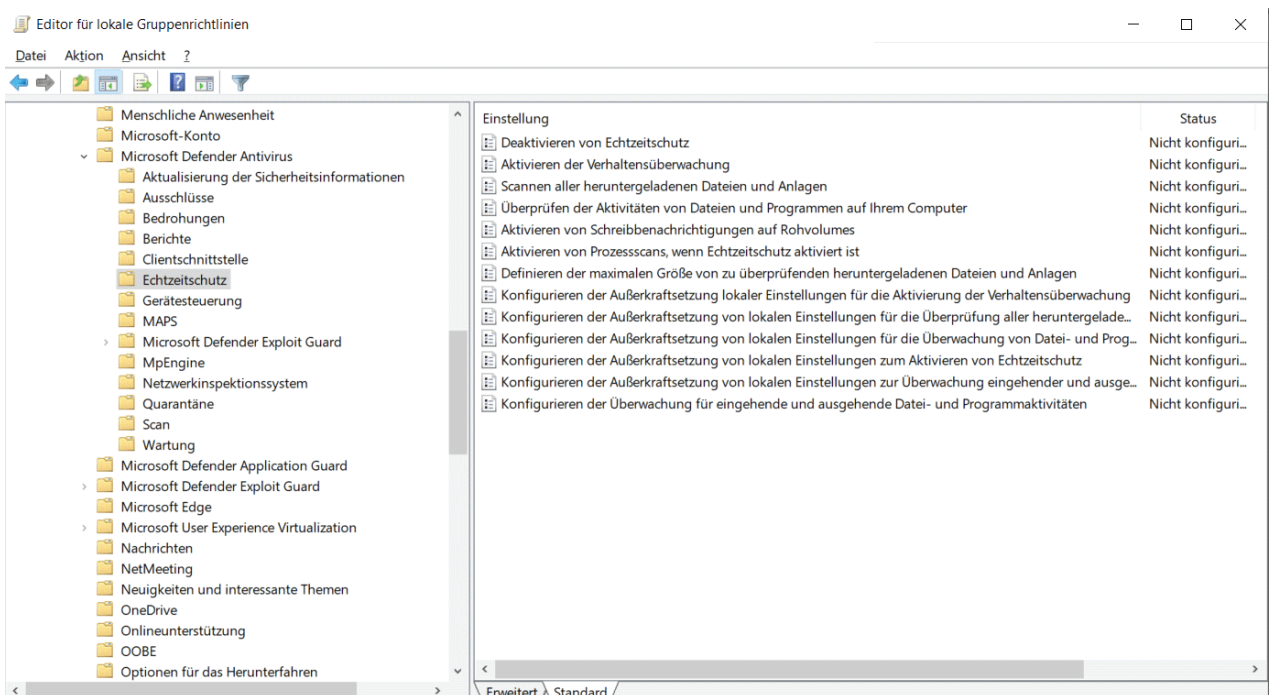
Defender Antivirus lässt sich zwar auf Client-Betriebssystemen nicht deinstallieren, man kann jedoch den Echtzeitschutz über eine entsprechende Richtlinie abschalten. Das klappt aber nur, wenn der Manipulationsschutz (Tamper Protection) deaktiviert ist.

Viele vernünftige Gründe dürfte es dafür indes nicht geben. Läuft nämlich ein weiterer Virenschanner eines anderen Anbieters, dann [schaltet sich Defender ohnehin selbständig ab](#). Die Einstellung *Microsoft Defender Antivirus deaktivieren* ("Turn off Microsoft Defender Antivirus") hat laut Dokumentation keine Auswirkung.

In PowerShell lässt sich das mit

```
Set-MpPreference -DisableRealtimeMonitoring $true
```

erledigen.



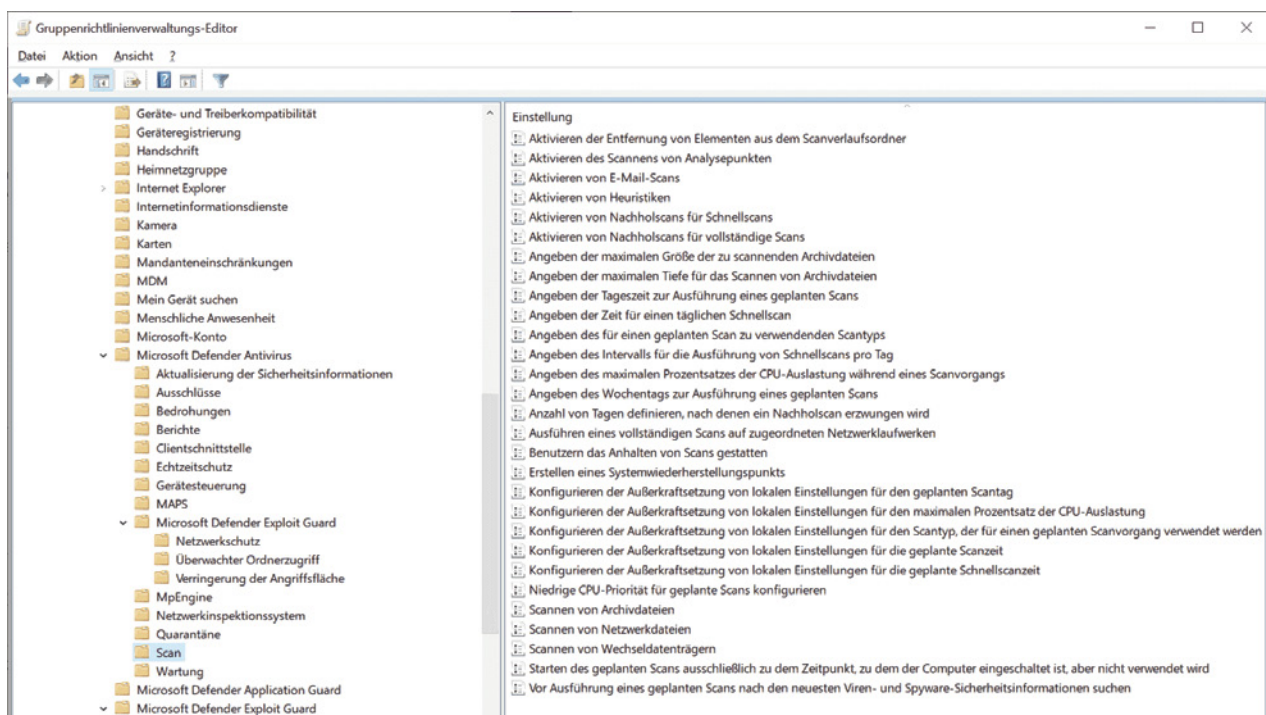
Einstellungen für das Anpassen des Echtzeitschutzes

Die meisten Funktionen für den Echtzeitschutz, die sich per GPO konfigurieren lassen, sind [von Haus aus aktiviert](#), so dass man sie über die Richtlinien abschalten kann. Das gilt etwa für die Verhaltensüberwachung, das Scannen heruntergeladener Dateien oder von Scripts. In der Regel wird man es bei den Vorgaben belassen.

Überprüfung anpassen

Über mehrere Einstellungen können Admins steuern, wann und wie oft Defender das System auf Malware prüft. Damit kann man etwa die Scans so planen, dass sie die User möglichst wenig beeinträchtigen. Dies spielt etwa auf einem Multiuser-System wie einem RD Session Host eine wichtige Rolle.

Wenn man für das Scan-Timing nicht ausgesprochen ungünstige Werte wählt, sollte es keine Auswirkungen auf die Sicherheit haben. Anders sieht es bei anderen Scan-Richtlinien aus. Mit ihnen kann man etwa das Überprüfen von E-Mails, Archivdateien, Wechseldatenträger oder die Verwendung von Heuristiken deaktivieren.



Einstellungen zur Steuerung des Scan-Verhaltens

All diese Optionen sind per Voreinstellung aktiv und sollten es ohne triftigen Grund auch bleiben. Die [Dokumentation](#) enthält auch die PowerShell-Pendants zu den Gruppenrichtlinien.

Eine spezielle Regelung gilt für Netzlaufwerke. Diese werden nur geprüft, wenn sie auf Systemebene zugeordnet wurden. Hat der Benutzer selbst das Mapping eingerichtet, dann ignoriert Defender diese Shares per Default. Dies lässt sich mit *Scannen von Netzwerkdateien* ("Scan files on the network") ändern.

Das Äquivalent in PowerShell würde so aussehen:

```
Set-MpPreference -DisableScanningNetworkFiles $false
```

In der Regel wird aber auf einem File-Server ohnehin ein eigener Virenschanner laufen, um einen übermäßigen Ressourcenverbrauch zu verhindern, wenn alle Clients ihre Scans über das Netzwerk ausführen.

Reaktion auf gefundene Bedrohungen

Microsoft bietet Admins mehrere Möglichkeiten, die Reaktion von Defender Antivirus auf gefundene Bedrohungen zu beeinflussen. Eine Variante besteht darin, die automatischen Mechanismen des Tools ganz außer Kraft zu setzen. Diesem Zweck dient die irreführend übersetzte Einstellung *Regelmäßige Wartung deaktivieren* ("Turn off routine remediation").

Diese wird man in den meisten Umgebungen nicht nutzen, weil dann die Benutzer entscheiden müssen, welche Maßnahmen ergriffen werden sollen.

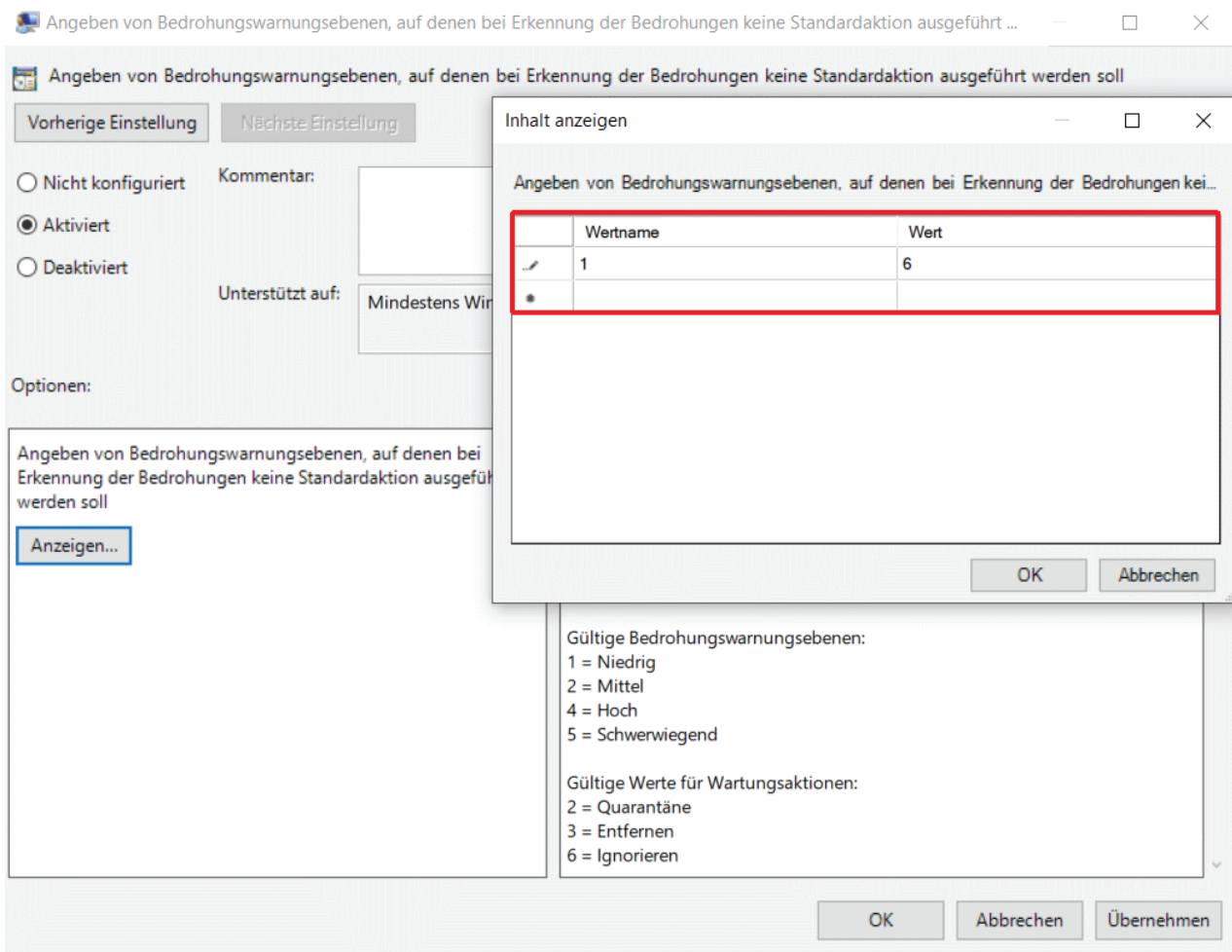
Alternativ bietet es sich daher an, die Reaktion von Defender auf bestimmte Ereignisse über Richtlinien festzulegen, wenn man mit dem Standardverhalten nicht zufrieden ist. Für diesen Zweck existieren zwei Einstellungen:

- Angeben von Bedrohungswarnungsebenen, auf denen bei Erkennung der Bedrohungen keine Standardaktion ausgeführt werden soll ("Specify threat alert levels at which default action should not be taken when detected")
- Angeben von Bedrohungen, bei deren Erkennung keine Standardaktion ausgeführt werden soll ("Specify threats upon which default action should not be taken when detected")

Beide Richtlinien enthalten eine zweispaltige Tabelle, in der man links die Bedrohung und rechts die Aktion einträgt. Bei der ersten Einstellung gibt man nur den Schweregrad an, bei der zweiten die ID der Bedrohung. Eine vollständige Liste der IDs kann man mit

```
Get-MpThreatCatalog
```

abrufen. Ihnen ordnet man Maßnahmen zu, die beim Auftreten dieser Ereignisse ausgeführt werden sollen (Quarantäne, Entfernen, Ignorieren).



Aktionen zu den Schweregraden der Bedrohung zuordnen

In PowerShell stehen zu diesem Zweck für *Set-MpPreference* folgende Parameter zur Verfügung:

- `ThreatIDDefaultAction_Ids <Int64[]>`
- `ThreatIDDefaultAction_Actions <ThreatAction[]>`
- `UnknownThreatDefaultAction <ThreatAction>`
- `LowThreatDefaultAction <ThreatAction>`
- `ModerateThreatDefaultAction <ThreatAction>`
- `HighThreatDefaultAction <ThreatAction>`
- `SevereThreatDefaultAction <ThreatAction>`

Um zum Beispiel auf schwerwiegende Bedrohungen mit dem Löschen des betreffenden Objekts zu reagieren, würde man so vorgehen:

```
Set-MpPreference -SevereThreatDefaultAction Remove
```

Die Aktionen für bestimmte Threat-IDs lassen sich auf diesem Weg ebenfalls festlegen:

```
Set-MpPreference -ThreatIDDefaultAction_Actions @(2,2) `
-ThreatIDDefaultAction_Ids @(15112,15113)
```

In diesem Beispiel würden die Bedrohungen mit den IDs 15112 und 15113 in Quarantäne gesteckt. Diese Option ist aktuell nicht durch die Tamper Protection geschützt und eröffnet etwa mit der Aktion *Allow* Möglichkeiten des Missbrauchs. So ließe sich damit etwa ein Bypass für Mimikatz einrichten.

Eine weitere Einstellung unter *Quarantäne* grenzt die Dauer für das Isolieren von Dateien ein, bevor sie gelöscht werden. Sie heißt *Konfigurieren des Entfernens von Elementen aus dem Quarantäneordner* ("Configure removal of items from Quarantine folder").

Updates für Viren-Signaturen steuern

Microsoft räumt dem regelmäßigen Download der Definitionsdateien für den Virenschanner eine so große Bedeutung ein, dass es dafür eigene Update-Einstellungen vorsieht. Wenn man die Patches für Windows von einem WSUS-Server bezieht, dann holt Defender standardmäßig seine Signaturen trotzdem von Microsoft Update.

Private Anwender und kleinere Umgebungen fahren damit in der Regel gut. Sie erhalten auf diesem Weg die neuen Virendefinitionen am schnellsten, die Update-Intervalle sind dort kürzer als etwa bei WSUS. Wenn man bei Letzteren keine automatische Genehmigung für die Signaturen eingerichtet hat, dann können durch die manuelle Freigabe zusätzliche Verzögerungen entstehen.

Wechselnde Update-Quellen

In Unternehmen mit einem großen Netzwerk, mehreren Niederlassungen oder mobilen Mitarbeitern können die Anforderungen jedoch ein differenziertes Management der Defender-Updates verlangen. So mag es etwa wünschenswert sein, die Virensignaturen im LAN von den WSUS zu beziehen. Wenn sich Mitarbeiter jedoch länger auswärts aufhalten, dann sollte Defender die Definitionen von Microsoft Update holen.

Denkbar sind auch Konstellationen, wo Rechner keinen Zugang zum Internet haben und zudem kein WSUS-Server verfügbar ist. In diesem Fall wäre es ideal, wenn die Updates von einer Netzfreigabe kommen könnten.

Quellen mit unterschiedlicher Priorität

Eine solche Konfiguration, bei der Defender der Reihe nach verschiedenen Quellen kontaktiert, wenn die bevorzugten nicht erreichbar sind, lässt sich über die *Signature Fallback Order* abbilden.

Sie unterstützt als Quellen WSUS (InternalDefinitionUpdateServer), Microsoft Update (MicrosoftUpdateServer), Netzfreigaben (FileShares) sowie Security Intelligence Updates and Platform Updates for Microsoft Defender Antivirus (MMPC).

Ihre Priorität bestimmt sich durch die Reihenfolge, die man über folgende Syntax festlegt:

```
InternalDefinitionUpdateServer | MicrosoftUpdateServer | FileShares | MMPC
```

In diesem Beispiel kämen die WSUS zuerst zum Zug, dann Microsoft Update, die Netzfreigaben und schließlich MMPC.

Konfiguration über PowerShell

Mittels PowerShell kann man sich im ersten Schritt die aktuelle Konfiguration für Signatur-Updates anzeigen lassen:

```
Get-MpPreference | Select SignatureFallbackOrder
```

Standardmäßig erhält man

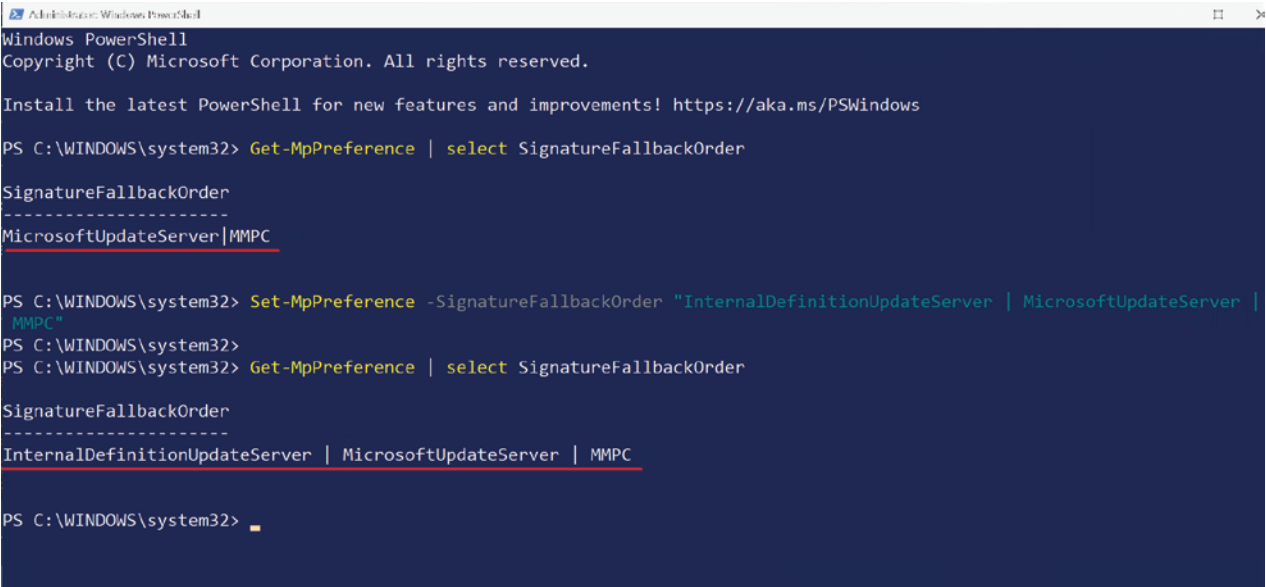
```
MicrosoftUpdateServer | MMPC
```

als Ergebnis.

Um diese Einstellung zu ändern, geht man nach diesem Muster vor:

```
Set-MpPreference -SignatureFallbackOrder `
```

```
"InternalDefinitionUpdateServer | MicrosoftUpdateServer | MMPC"
```



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> Get-MpPreference | select SignatureFallbackOrder

SignatureFallbackOrder
-----
MicrosoftUpdateServer | MMPC

PS C:\WINDOWS\system32> Set-MpPreference -SignatureFallbackOrder "InternalDefinitionUpdateServer | MicrosoftUpdateServer | MMPC"
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Get-MpPreference | select SignatureFallbackOrder

SignatureFallbackOrder
-----
InternalDefinitionUpdateServer | MicrosoftUpdateServer | MMPC

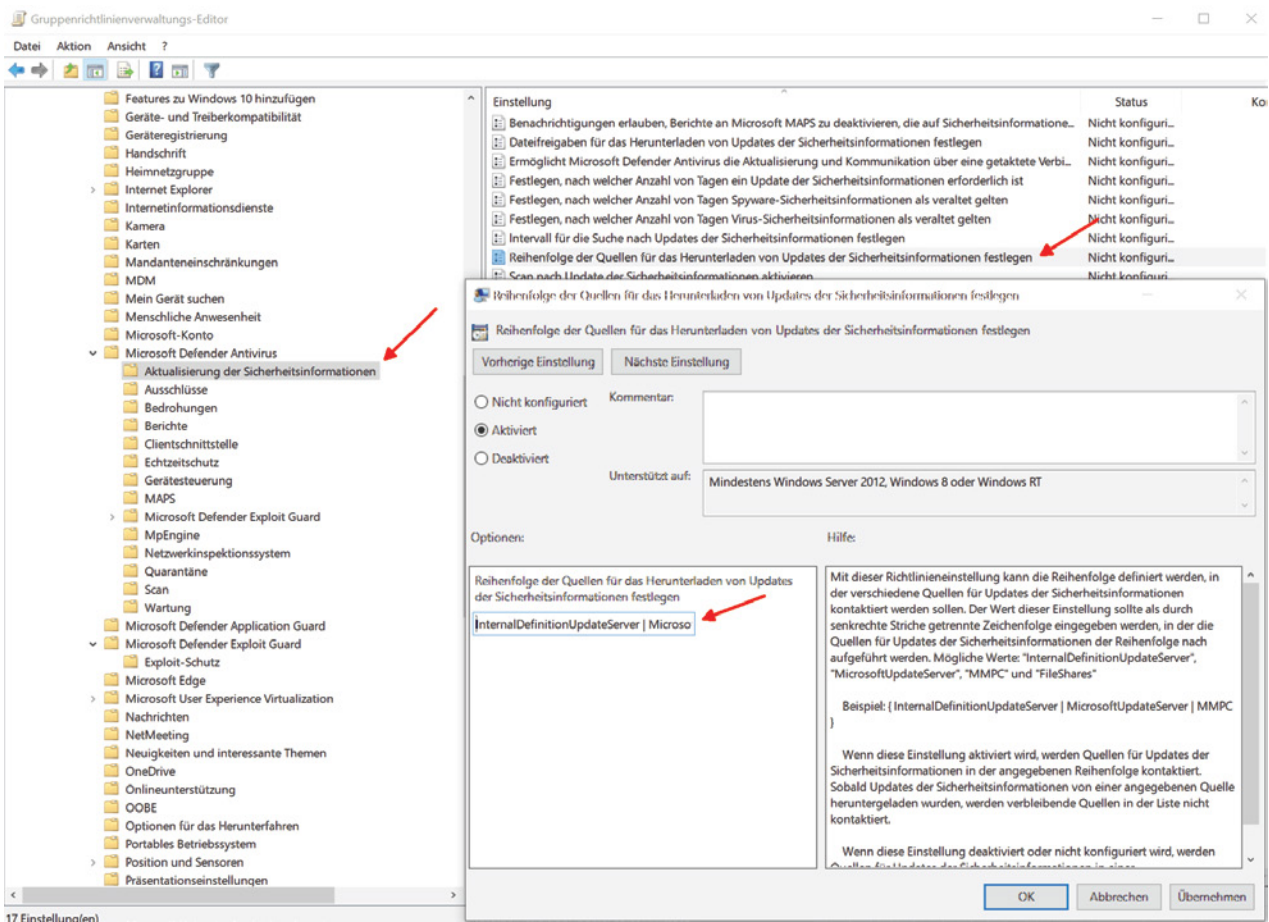
PS C:\WINDOWS\system32> 
```

Reihenfolge der Update-Quellen für die Virendefinitionen über PowerShell festlegen

Fallback-Order über Gruppenrichtlinien festlegen

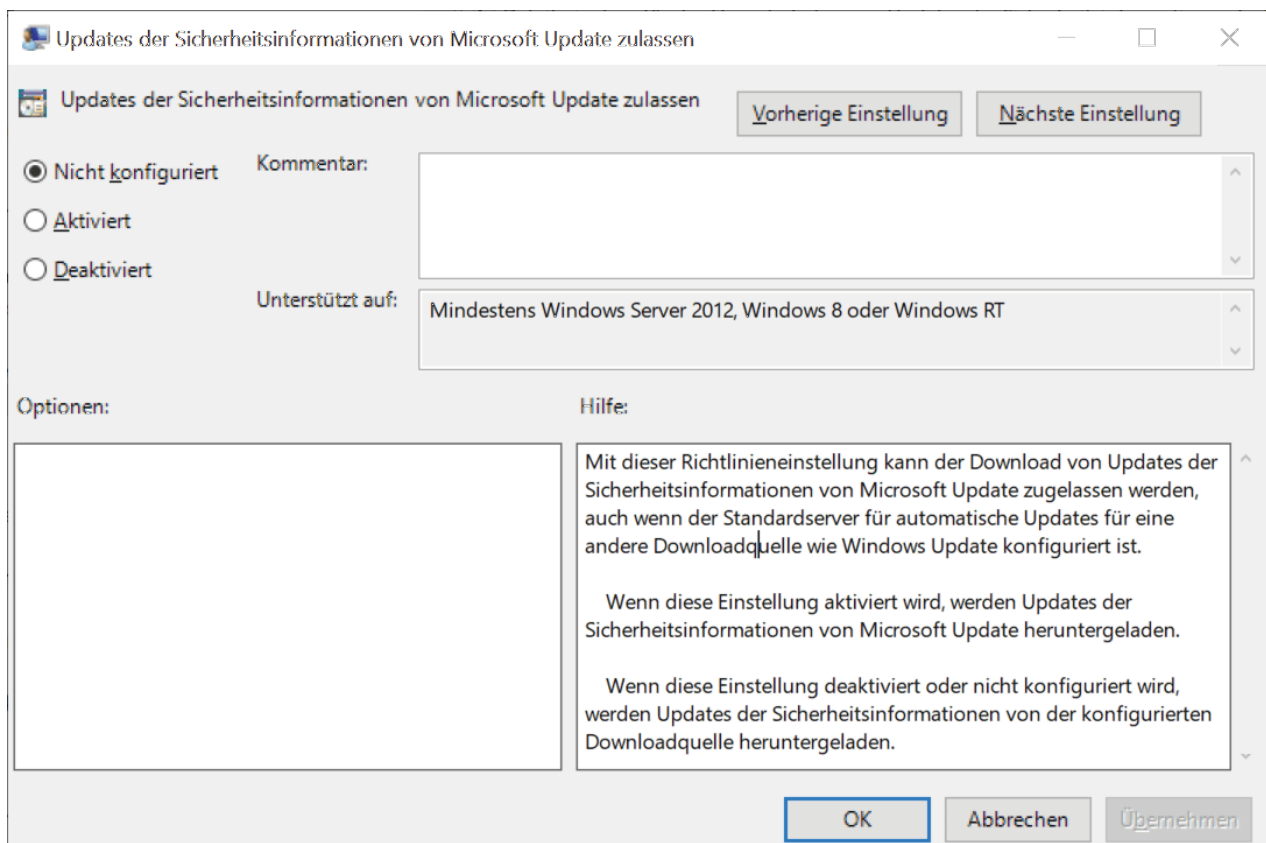
Die Einstellung für diesen Zweck findet sich unter *Computerkonfiguration => Richtlinien => Administrative Vorlagen => Windows-Komponenten => Microsoft Defender Antivirus => Aktualisierung der Sicherheitsinformationen* und heißt *Reihenfolge der Quellen für das Herunterladen von Updates der Sicherheitsinformationen festlegen* ("Define the order of sources for downloading security intelligence updates").

Wenn man diese aktiviert, kann man die Quellen wie gehabt in das Eingabefeld übernehmen.



Reihenfolge der Update-Quellen für Microsoft Defender über Gruppenrichtlinien steuern

Die Gruppenrichtlinien kennen dazu eine ergänzende Einstellung, mit der Microsoft Update als Quelle für mobile Geräte zugelassen werden soll, wenn ein interner Update-Server nicht verfügbar ist. Sie heißt *Updates der Sicherheitsinformationen von Microsoft Update zulassen* ("Allow security intelligence updates from Microsoft Update").



Einstellung für das Opt-in zu Microsoft Update

Unklar ist jedoch, wann man Microsoft Update explizit zulassen muss. Die [Dokumentation](#) spricht davon, dass dies dann notwendig sei, wenn "Sie WSUS so festgelegt haben, dass Microsoft Update außer Kraft gesetzt wird".

Pfad zu Download-Verzeichnis festlegen

Sollen Rechner ihre Definitions-Updates von einer Netzfreigabe beziehen, dann muss man diese separat konfigurieren. Dabei ist es möglich, die UNC-Pfade für mehrere Verzeichnisse anzugeben, und zwar wieder in der oben beschriebenen Syntax:

```
\\server1\fileshare | \\server2\fileshare
```

Mit PowerShell kann man auch hier den aktuellen Status einfach abfragen:

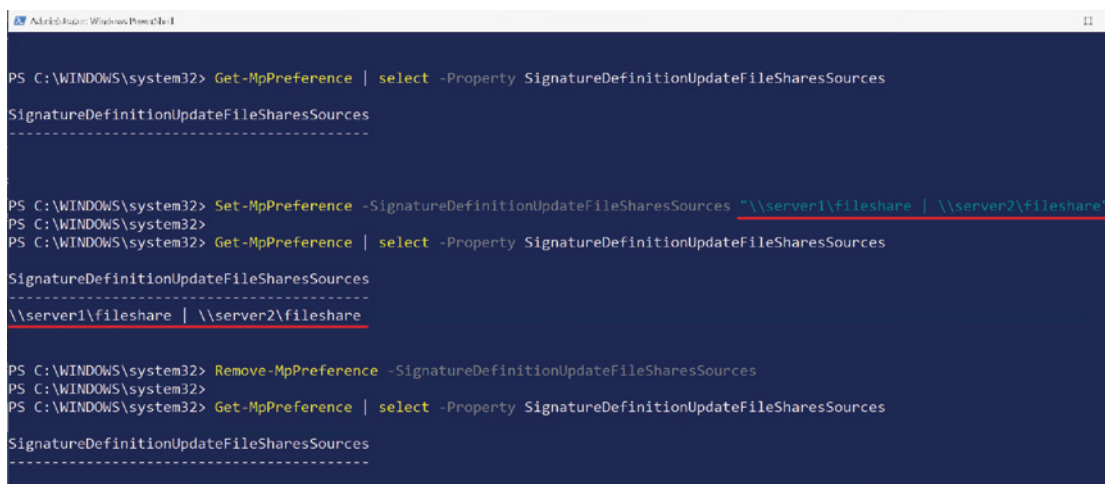
```
Get-MpPreference |  
Select -Property SignatureDefinitionUpdateFileSharesSources
```

Standardmäßig sind keine Verzeichnisse hinterlegt. Um solche zu definieren, setzt man einen Befehl nach diesem Muster ab:

```
Set-MpPreference -SignatureDefinitionUpdateFileSharesSources `  
"\\server1\fileshare | \\server2\fileshare"
```

Wenn man diese Einstellung wieder zurücksetzen möchte, dann führt man dieses Kommando aus:

```
Remove-MpPreference -SignatureDefinitionUpdateFileSharesSources
```

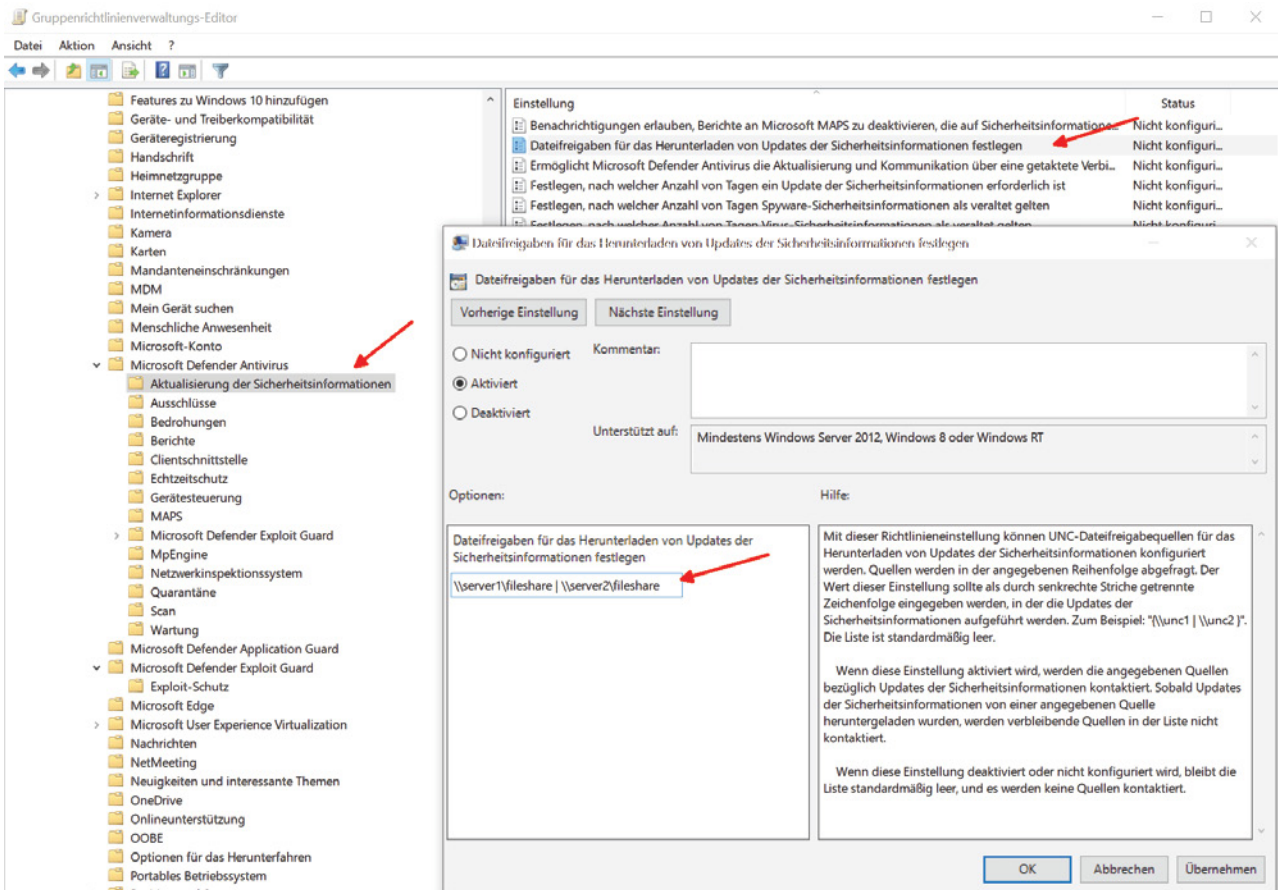


```
PS C:\WINDOWS\system32> Get-MpPreference | select -Property SignatureDefinitionUpdateFileSharesSources  
SignatureDefinitionUpdateFileSharesSources  
-----  
  
PS C:\WINDOWS\system32> Set-MpPreference -SignatureDefinitionUpdateFileSharesSources "\\server1\fileshare | \\server2\fileshare"  
PS C:\WINDOWS\system32>  
PS C:\WINDOWS\system32> Get-MpPreference | select -Property SignatureDefinitionUpdateFileSharesSources  
SignatureDefinitionUpdateFileSharesSources  
-----  
\\server1\fileshare | \\server2\fileshare  
-----  
  
PS C:\WINDOWS\system32> Remove-MpPreference -SignatureDefinitionUpdateFileSharesSources  
PS C:\WINDOWS\system32>  
PS C:\WINDOWS\system32> Get-MpPreference | select -Property SignatureDefinitionUpdateFileSharesSources  
SignatureDefinitionUpdateFileSharesSources  
-----
```

Freigegebene Verzeichnisse für den Download der Viren-Signaturen mit PowerShell festlegen

Bevorzugt man für diese Aufgabe die Gruppenrichtlinien, dann findet sich die zuständige Einstellung ebenfalls im Ordner *Aktualisierung der Sicherheitsinformationen* und heißt *Dateifreigaben für das Herunterladen von Updates der Sicherheitsinformationen festlegen* ("Define file shares for downloading security intelligence updates").

Dort kann man ebenfalls mehrere Pfade eingeben, die man mittels '|' voneinander trennt.



Festlegen von Fileshares für das Herunterladen der Viren-Signaturen

Aktualisierung über mobile Netzwerke

Um sicherzustellen, dass Geräte auch dann aktuelle Signaturen erhalten, wenn sie längere Zeit über mobile Netze mit dem Internet verbunden sind, kann man den Download über getaktete Verbindungen zulassen.

In PowerShell verwendet man dafür folgenden Befehl:

```
Set-MpPreference -MeteredConnectionUpdates $true
```

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Set-MpPreference -MeteredConnectionUpdates $true
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Get-MpPreference | select MeteredConnectionUpdates

MeteredConnectionUpdates
-----
                          True

PS C:\WINDOWS\system32>
```

Download der Definitions-Updates über getaktete Verbindungen zulassen

Das Pendant dazu in den Gruppenrichtlinien lautet *Ermöglicht Microsoft Defender das Aktualisieren und Kommunizieren über eine getaktete Verbindung* ("Allows Microsoft Defender Antivirus to update and communicate over a metered connection").

Defender mit Manipulationsschutz absichern

Der mit Windows 10 1903 eingeführte Manipulationsschutz verhindert, dass die vorgegebene Konfiguration von Microsoft Defender verändert oder das Tool deaktiviert wird. Seit einiger Zeit ist diese Option per Voreinstellung eingeschaltet und auch auf älteren Systemen ab Windows Server 2012 R2 verfügbar.

Die Tamper Protection überwacht unter anderem folgende Ereignisse und blockiert alle Änderungen:

- Deaktivieren des Viren- und Bedrohungsschutzes
- Abschalten des Echtzeitschutzes
- Ausschalten der Überwachung von auffälligen Aktivitäten
- Entfernen von Signatur-Updates
- Ändern von Aktionen als Reaktion auf Bedrohungen
- Deaktivieren des Script-Scanners

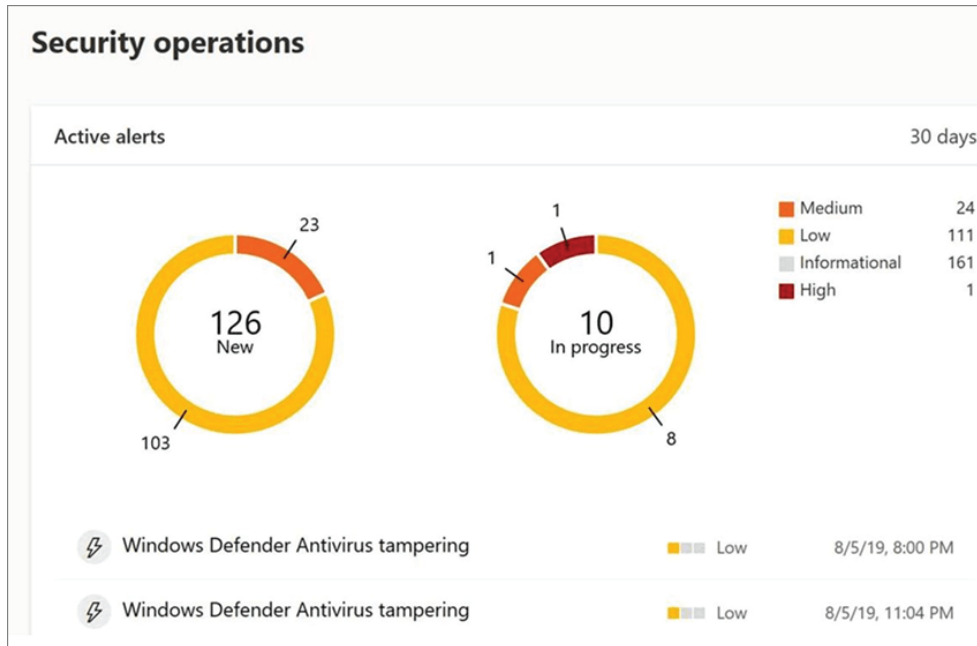
Kein Management über lokale Tools

Beim Verwalten des Manipulationsschutzes stellt sich das Problem, dass alle lokalen Mittel als unsicher gelten. Wenn ein Angreifer die Privilegien eines lokalen Admins erlangt, dann wäre er auch in der Lage, auch die Tamper Protection abzuschalten. Aus diesem Grund lässt sich diese weder durch Gruppenrichtlinien, PowerShell oder direktes Editieren der Registry beeinflussen.

Es besteht allerdings die Möglichkeit, den Status dieses Features mit PowerShell abzufragen:

```
Get-MpComputerStatus | Select IsTamperProtected
```

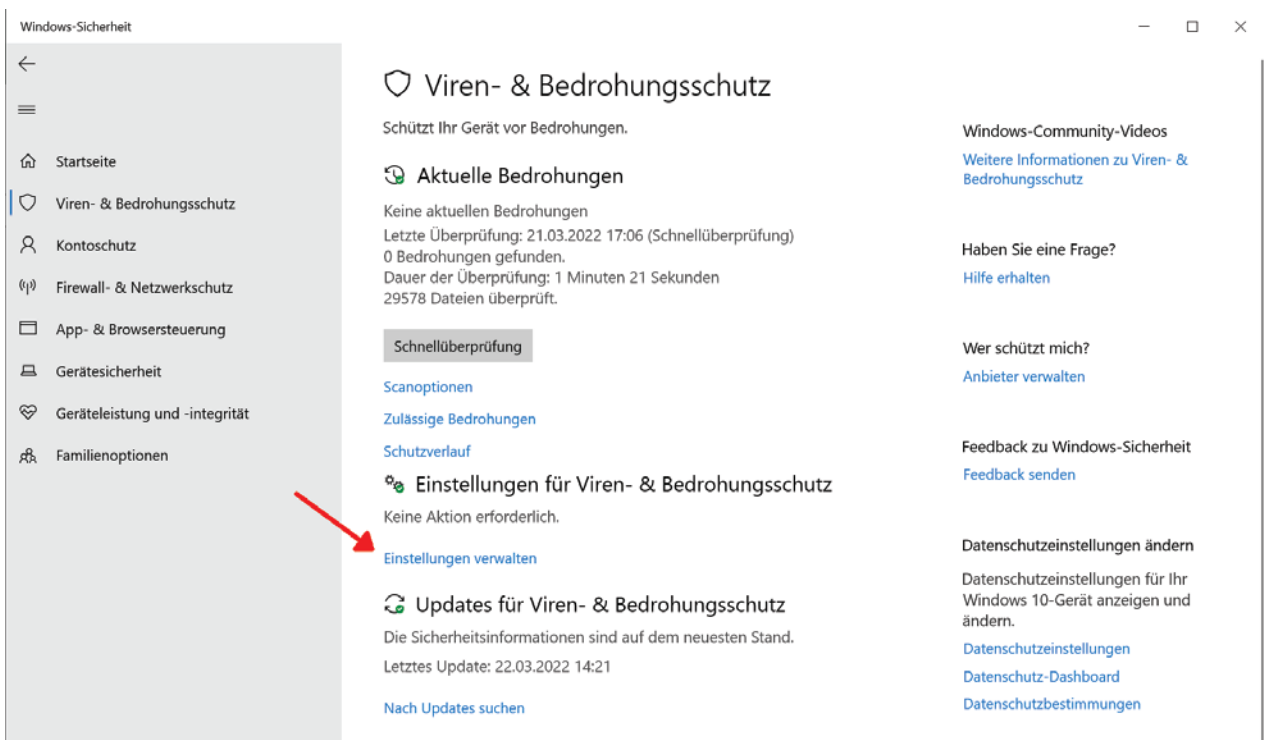

Ist es aktiv, dann hat diese Eigenschaft den Wert *True*. Verwaltet man die Tamper Protection über die Cloud, dann bietet das Defender Portal ein Dashboard, das alle Aktivitäten im Zusammenhang mit diesem Feature anzeigt.



Das Dashboard im Defender Portal zeigt Vorkommnisse bei der Tamper Protection

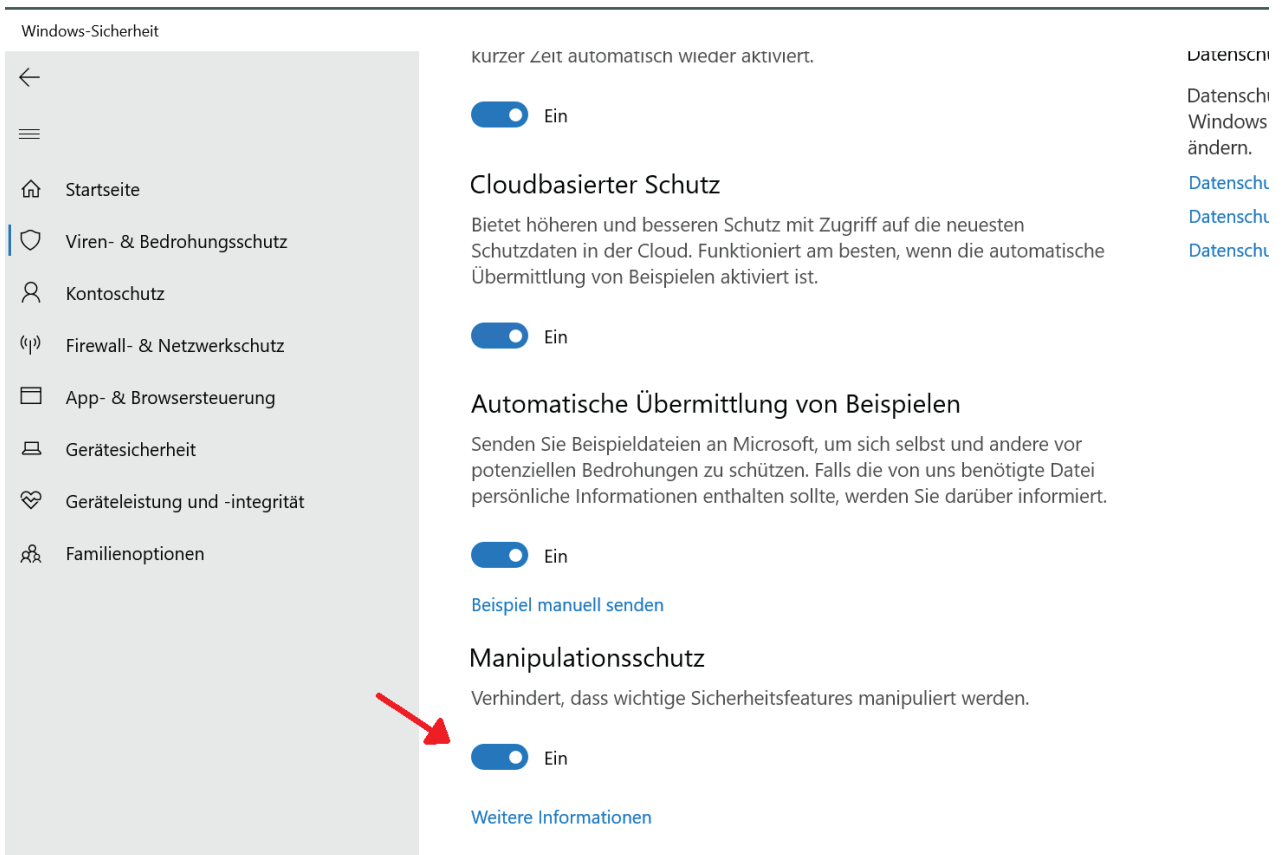
Interaktive Konfiguration

Auf nicht verwalteten PCs können Benutzer den Manipulationsschutz interaktiv steuern, und zwar über die App *Einstellungen* unter *Update & Sicherheit* => *Windows-Sicherheit* => *Viren- & Bedrohungsschutz* => *Einstellungen für Viren- & Bedrohungsschutz* => *Einstellungen verwalten*.



Link zu Seite, auf der sich die Tamper Protection konfigurieren lässt

Benutzer mit lokalen Admin-Rechten können sie hier abschalten. Es liegt auf der Hand, dass die Tamper Protection wenig Schutz bietet, wenn die Benutzer unter einem privilegierten Account arbeiten. Angreifer erlangen dadurch oft remote Zugang zum Rechner und können dabei keine GUI-Apps ausführen. In diesem Fall lässt sich der Manipulationsschutz nicht aushebeln.

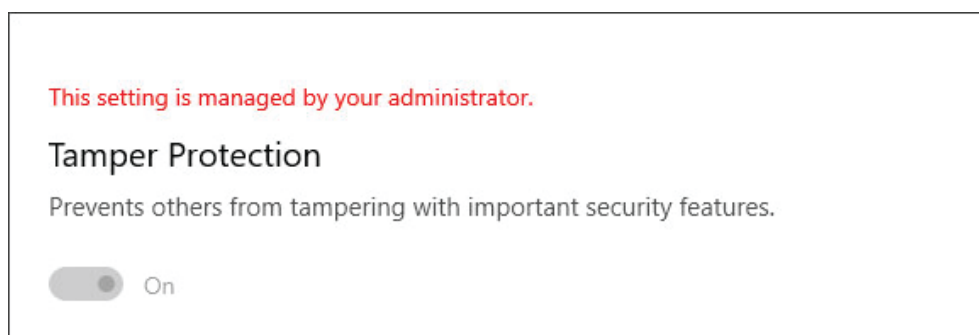


Der Manipulationsschutz ist standardmäßig aktiv und lässt sich interaktiv mit Admin-Rechten ausschalten

Verwaltung über die Cloud

Aus diesem Grund sieht Microsoft ein zentrales Management der Tamper Protection über die Cloud vor, was jedoch entsprechende Abos für Defender for Endpoint voraussetzt.

Anwender können dann diese Einstellung global über das M365 Defender Portal ändern. Sie wirkt sich dann auf alle Geräte aus, die diesem Tenent zugeordnet sind. Auf dem Client wird die entsprechende Option in der App *Einstellungen* abgeblendet, so dass lokale Admins sie nicht mehr ändern können.



Verwaltet man den Manipulationsschutz zentral, dann lässt er sich lokal nicht mehr konfigurieren

Reputationsbasierter Schutz

Mit SmartScreen ergänzt Microsoft die Antiviren-Engine um einen reputationsbasierten Schutz. Während der Virenschanner periodisch oder in Echtzeit das Dateisystem prüft und auf verdächtige Aktivitäten achtet, wirkt SmartScreen präventiv.

Warnung vor problematischen Websites

Es warnt Benutzer beim Besuch von Websites, die Microsoft als bedenklich einstuft und blockiert den Download von Apps, von denen eine Gefahr ausgehen könnte. Der Hersteller greift dazu auf Listen mit bekannten Phishing- oder Malware-Sites zurück. Darüber hinaus prüft SmartScreen besuchte Websites auf verdächtige Merkmale.

Während sich der Schutz vor dem Laden bössartiger Websites auf den Microsoft-eigenen Web-Browser Edge beschränkt, untersucht SmartScreen jeden Internet-Download auf potenzielle Risiken.

Abwehr von heruntergeladener Malware

Dies erfolgt nicht durch Scannen des Inhalts (dies ist Aufgabe der Antiviren-Engine), sondern ebenfalls auf Basis von Reputation. Dazu verfügt Microsoft über eine Liste wohlbekanntere Dateien, die unbehellig passieren können.

Umgekehrt kann es daher vorkommen, dass SmartScreen ein harmloses, aber relativ exotisches Programm beanstandet. Um solche falschen Alarme zu minimieren, kommt als weiteres Kriterium die Zuverlässigkeit der Quelle hinzu, von der eine Datei heruntergeladen wurde.

Erweiterter Phishing-Schutz

Windows 11 2022 erweitert den Schutz von SmartScreen gegen Phishing-Angriffe. Dazu überwacht es die Eingabe von Passwörtern in Web-Browser, wobei es alle Chromium-basierten Produkte unterstützt. Dabei bietet es die folgenden drei Funktionen:

Eingabe von Passwörtern in unsichere Seiten

Verwenden Benutzer dafür das Kennwort, mit dem sie sich an Windows angemeldet haben (Microsoft-Konto, Active Directory, Azure AD oder eines für lokale Accounts), dann fordert SmartScreen zum Wechsel des Passworts auf.

Wenn Unternehmen Microsoft Defender for Endpoint einsetzen, dann scheint dieser Vorfall im MDE-Portal auf. Admins erfahren auf diese Weise, dass ein Passwort möglicherweise gestohlen wurde und können den Wechsel des Passworts erzwingen, falls der User die entsprechende Warnung ignoriert hat.

Wiederverwendung von Kennwörtern

Die Überwachung von Passwörtern, die in Web-Anwendungen eingegeben werden, hilft auch dabei, die weit verbreitete Unsitte abzustellen, nämlich der Nutzung des gleichen Passworts für alle möglichen Konten.

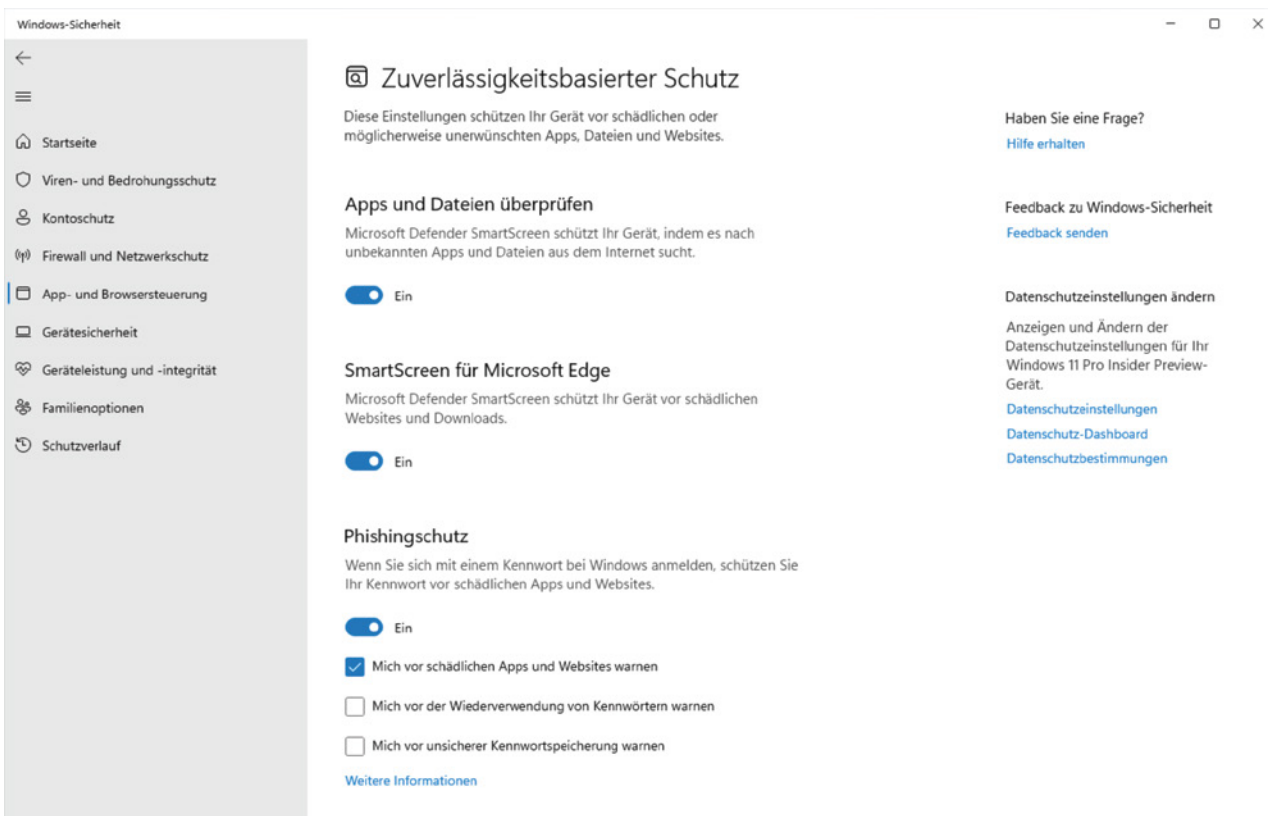
Besonders problematisch ist es, wenn Mitarbeiter das Kennwort für ihr Firmenkonto in Social Media oder Online-Shops wiederverwenden. Falls eine dieser Websites geknackt wurde und die Passwörter im Internet kursieren, dann machen sich Angreifer solche Listen für Brute-Force-Attacken zunutze.

Speichern von Passwörtern in Dateien

Darüber hinaus überwacht der erweiterte Phishing-Schutz, ob Anwender ihre Passwörter in Office-Dokumenten, in Wordpad oder in Textdateien speichern und warnt sie gegebenenfalls vor diesem Verhalten.

Interaktive Konfiguration von SmartScreen

Wenn man Defender SmartScreen interaktiv konfigurieren möchte, dann befinden sich die Einstellungen dafür in der App *Windows-Sicherheit* unter *App- und Browsersteuerung* => *Zuverlässigkeitsbasierter Schutz*.



The screenshot shows the Windows Security application window. On the left is a navigation pane with the following items: Startseite, Viren- und Bedrohungsschutz, Kontoschutz, Firewall und Netzwerkschutz, App- und Browsersteuerung (highlighted), Gerätesicherheit, Geräteleistung und -integrität, Familienoptionen, and Schutzverlauf. The main content area is titled 'Zuverlässigkeitsbasierter Schutz' and contains the following sections:

- Zuverlässigkeitsbasierter Schutz**: Description: 'Diese Einstellungen schützen Ihr Gerät vor schädlichen oder möglicherweise unerwünschten Apps, Dateien und Websites.' A link 'Hilfe erhalten' is present.
- Apps und Dateien überprüfen**: Description: 'Microsoft Defender SmartScreen schützt Ihr Gerät, indem es nach unbekanntem Apps und Dateien aus dem Internet sucht.' A toggle switch is set to 'Ein'.
- SmartScreen für Microsoft Edge**: Description: 'Microsoft Defender SmartScreen schützt Ihr Gerät vor schädlichen Websites und Downloads.' A toggle switch is set to 'Ein'.
- Phishingschutz**: Description: 'Wenn Sie sich mit einem Kennwort bei Windows anmelden, schützen Sie Ihr Kennwort vor schädlichen Apps und Websites.' A toggle switch is set to 'Ein'. Below it are three checkboxes:
 - Mich vor schädlichen Apps und Websites warnen
 - Mich vor der Wiederverwendung von Kennwörtern warnen
 - Mich vor unsicherer Kennwortspeicherung warnenA link 'Weitere Informationen' is at the bottom.

On the right side of the window, there are additional links: 'Haben Sie eine Frage? Hilfe erhalten', 'Feedback zu Windows-Sicherheit Feedback senden', and 'Datenschutzeinstellungen ändern Anzeigen und Ändern der Datenschutzeinstellungen für Ihr Windows 11 Pro Insider Preview-Gerät. Datenschutzeinstellungen, Datenschutz-Dashboard, Datenschutzbestimmungen'.

Einstellungen für SmartScreen in der App Windows-Sicherheit

Die Optionen

- Apps und Dateien überprüfen
- SmartScreen für Microsoft Edge

beziehen sich auf die ursprünglichen Funktionen von SmartScreen, die auch in Windows 10 und 11 21H2 enthalten sind. Sie lassen sich hier nur ein- oder ausschalten, während die Gruppenrichtlinien mehr Optionen bieten. Hinzu kommt am unteren Ende dieses Dialogs die Einstellung für das Prüfen von Store-Apps.

Für den neuen Phishing-Schutz stehen die drei besprochenen Optionen zur Verfügung, mit denen User bei der Eingabe von Passwörtern in schädliche Apps und Websites, vor der Wiederverwendung von Kennwörtern und vor dem Speicher derselben in Dateien gewarnt werden.

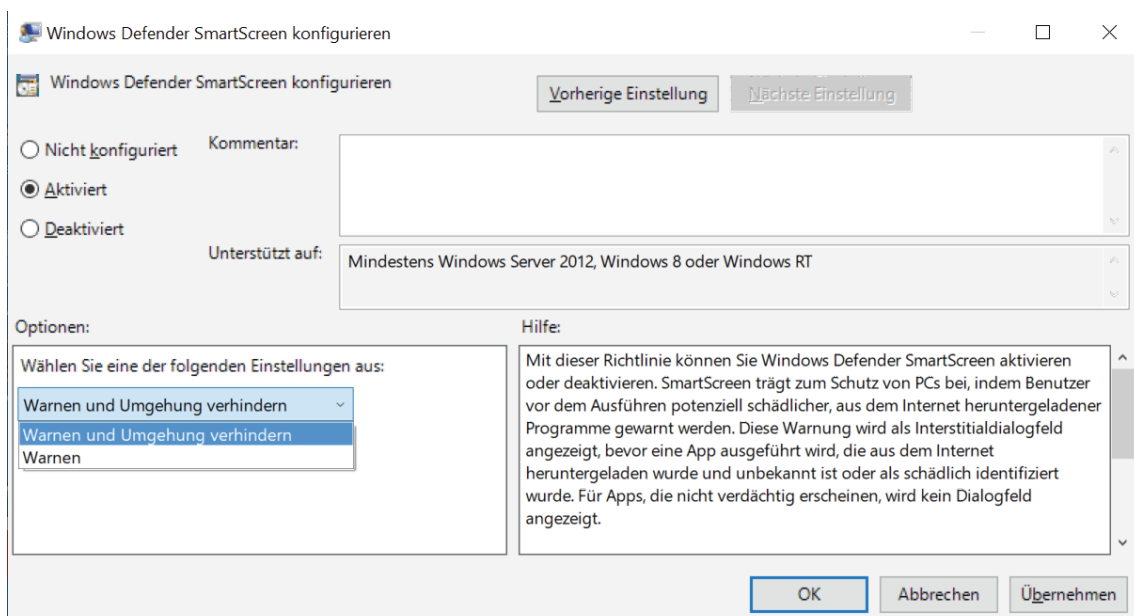
SmartScreen über Gruppenrichtlinien konfigurieren

In verwalteten Umgebungen wird man SmartScreen zentral über GPOs konfigurieren. Die Einstellungen dafür finden sich unter *Computerkonfiguration => Richtlinien => Administrative Vorlagen => Windows-Komponenten => Windows Defender SmartScreen*.

In den Ordnern Explorer und Microsoft Edge finden sich jeweils zwei Einstellungen. Jene für den Datei-Explorer dienen dazu, die Installation oder das Ausführen von problematischen Anwendungen zu verhindern.

Mit der Option *App Install Control konfigurieren* kann man dafür sorgen, dass User nur Store-Apps hinzufügen dürfen. Da Standardbenutzer in verwalteten Umgebungen normalerweise keine Berechtigung für das Installieren von Programmen erhalten, wird diese Option dort kaum benötigt.

Hingegen kann *Windows Defender SmartScreen konfigurieren* die Risiken bei der Ausführung von portablen Anwendungen reduzieren. Diese lassen sich damit vollständig blockieren, wenn sie verdächtig erscheinen.

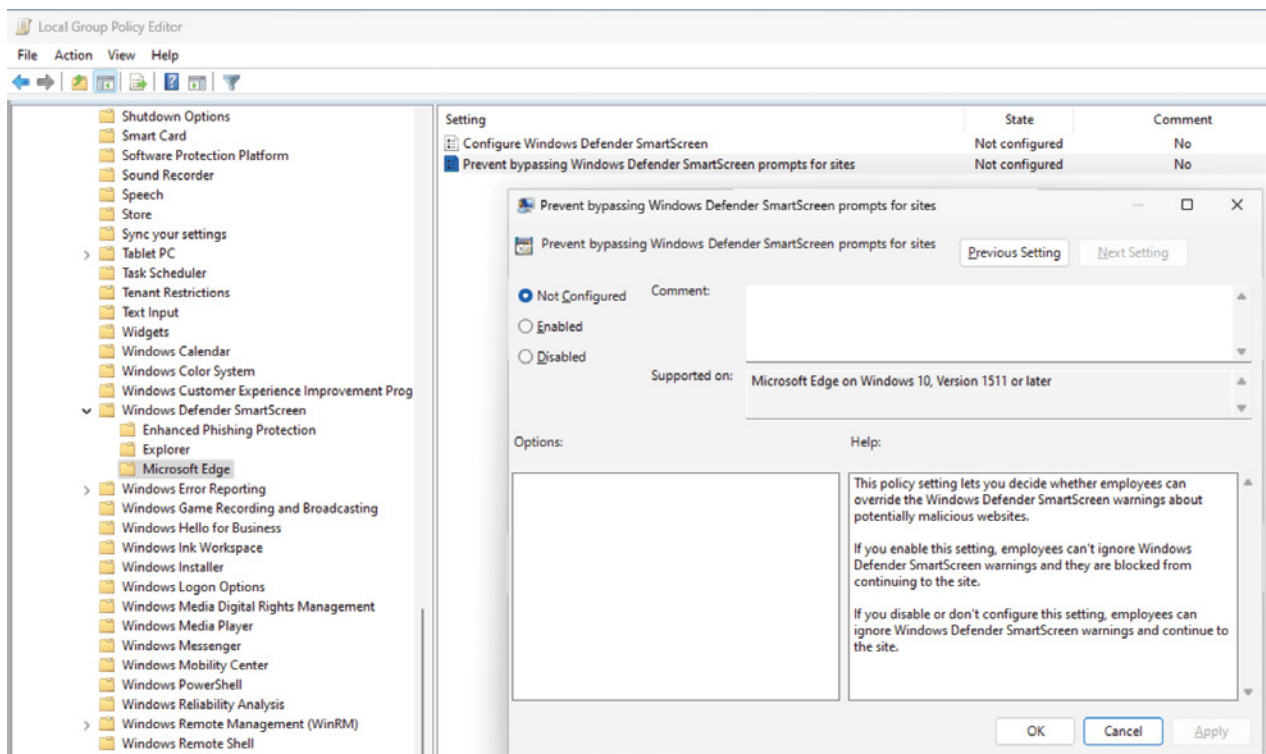


SmartScreen kann vor der Ausführung potenziell schädlicher Programme warnen oder diese blockieren

Für Edge gibt es hingegen nur diese simple Auswahl (als einzige auch im Zweig für die *Benutzerkonfiguration*):

- Windows Defender SmartScreen konfigurieren ("Configure Windows Defender SmartScreen")
- Umgehung der Windows Defender SmartScreen-Aufforderungen für Websites verhindern ("Prevent bypassing Windows Defender SmartScreen prompts for sites")

Mit der ersten Einstellung kann man die Benutzer am Abschalten von SmartScreen hindern (Einstellung aktiviert) oder das Feature verbindlich abschalten (deaktiviert).

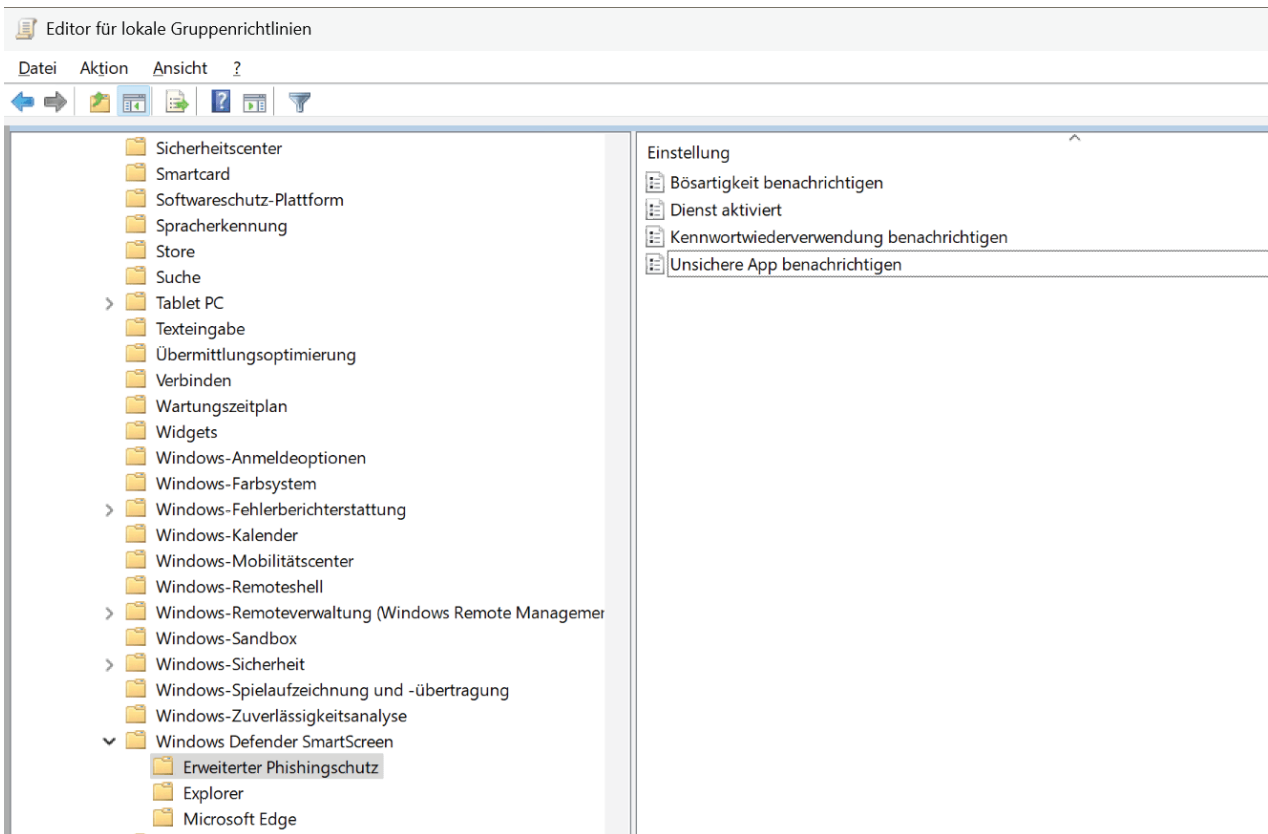


Gruppenrichtlinien zur Steuerung von SmartScreen für Microsoft Edge

Mit der zweiten Option legen Admins fest, ob Benutzer die Warnungen vor gefährlichen Websites ignorieren dürfen (Standard). Aktiviert man diese Einstellung, dann blockiert SmartScreen die betreffende URL.

Im Ordner Erweiterter Phishingschutz finden sich vier Einstellungen für das neue Feature:

- **Bösartigkeit benachrichtigen** ("Notify Malicious"): warnt bei Besuch von verdächtigen oder potenziell gefährlichen Websites
- **Kennwortwiederverwendung benachrichtigen** ("Notify Password Reuse"): erinnert die User, dass ihr im Unternehmen verwendetes Passwort nirgendwo anders nutzen sollen
- **Unsichere App benachrichtigen** ("Notify Unsafe App"): erkennt, wenn Benutzer das Passwort in einer Datei speichern.
- **Dienst aktiviert**: schaltet den erweiterten Phishing-Schutz ein



Kein natives PowerShell-Management

Das Cmdlet `Set-MpPreference` kann zahlreiche Defender-Einstellungen konfigurieren, jedoch nicht solche für SmartScreen. Hier bleibt somit nur die Möglichkeit, die entsprechenden Registry-Schlüssel direkt zu setzen.

Um zum Beispiel SmartScreen für Explorer daran zu hindern, die Ausführung von Programmen zu blockieren, könnte man diesen Aufruf nutzen:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Policies\Microsoft\Windows\System\
-Name EnableSmartScreen -Value 0 -PropertyType DWORD
```

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> New-ItemProperty -Path HKLM:\SOFTWARE\Policies\Microsoft\Windows\System\ -Name EnableSmartScreen -Value 0 -PropertyType DWORD

EnableSmartScreen : 0
PSPath              : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System\
PSParentPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
PSChildName         : System
PSDrive             : HKLM
PSProvider          : Microsoft.PowerShell.Core\Registry

PS C:\WINDOWS\system32> Get-Item HKLM:\SOFTWARE\Policies\Microsoft\Windows

Hive: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows

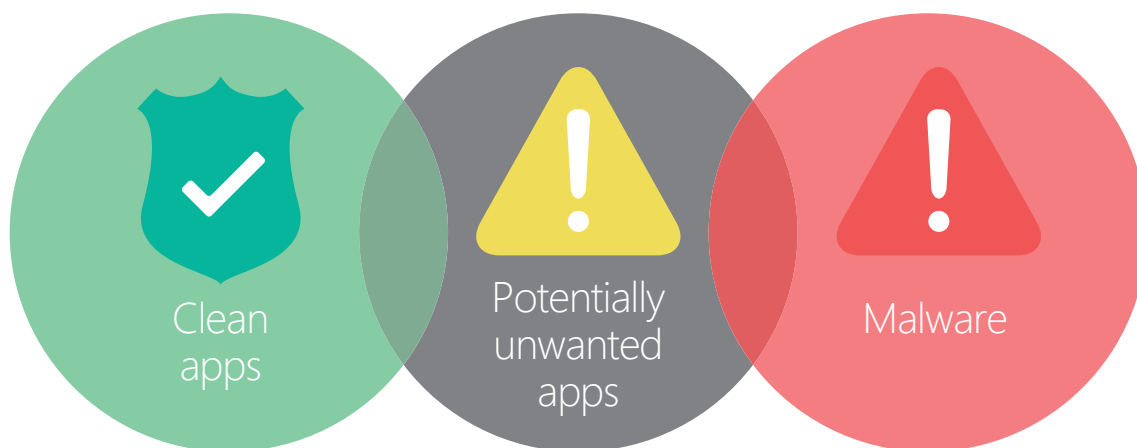
Name                Property
----                -
System              AllowClipboardHistory : 1
                   AllowDomainPINLogon   : 1
                   EnableSmartScreen     : 0
```

Smartscreen für Explorer über PowerShell konfigurieren

Entsprechendes gilt für den erweiterten Phishing-Schutz. Die Schlüssel dafür finden sich unter HKLM:\Software\Policies\Microsoft\Windows\WTDS\Components und heißen *ServiceEnabled*, *NotifyMalicious*, *NotifyPasswordReuse* sowie *NotifyUnsafeApp*.

Potenziell unerwünschte Anwendungen blockieren

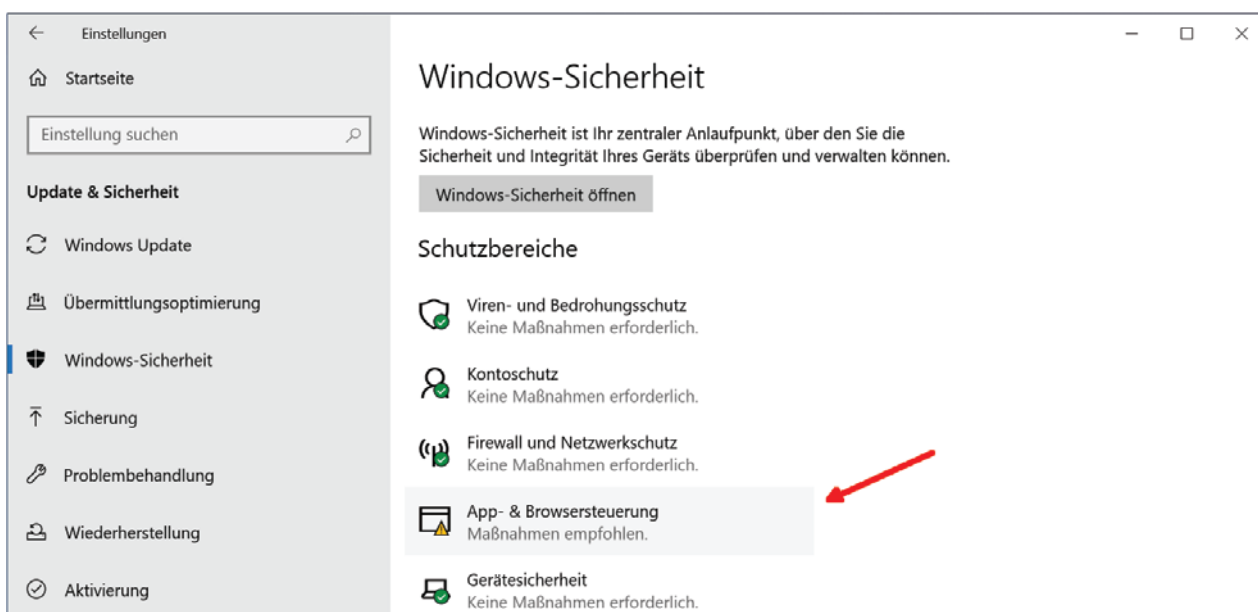
Potenziell unerwünschte Anwendungen (PUAs) sind zwar nicht bösartig, aber zumindest störend. Der Schutz vor ihnen ist seit Windows 10 2004 verfügbar. Es handelt sich dabei ebenfalls um eine reputationsbasierte Lösung.



Potenziell unerwünschte Anwendungen laufen auch unter der Bezeichnung Greyware

Schutz vor PUAs aktivieren

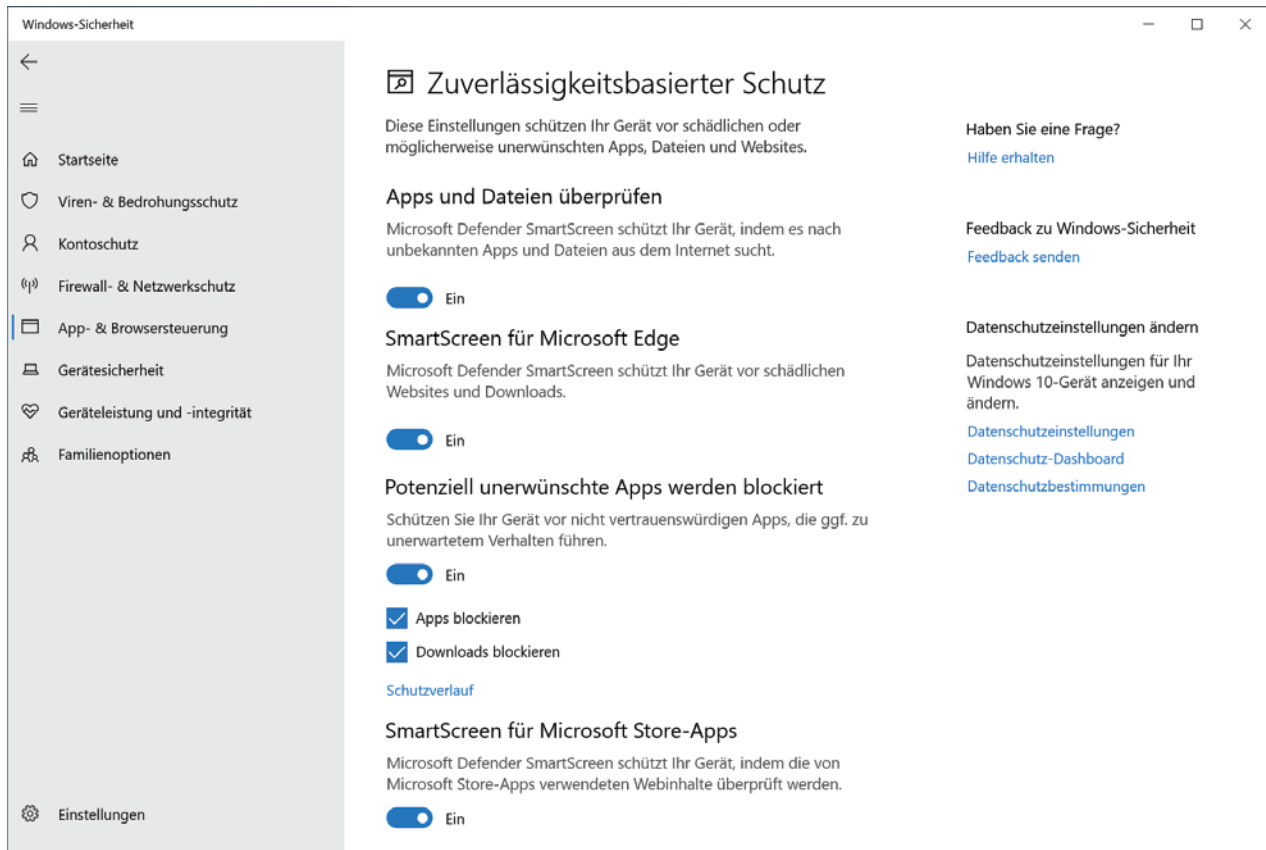
Der Schutz vor potenziell unerwünschten Apps in Windows lässt sich einfach einrichten. Die entsprechende Einstellung finden man unter *Updates & Sicherheit* => *Windows-Sicherheit* => *App- und Browsersteuerung*.



App- & Browsersteuerung in den Einstellungen öffnen

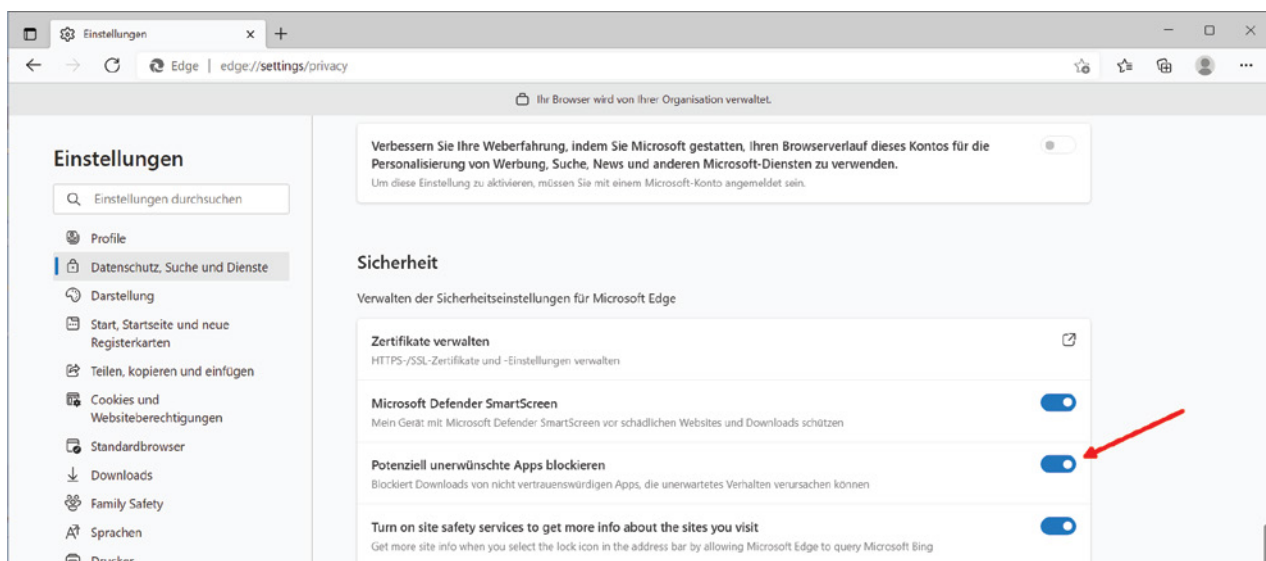
Folgt man diesem Eintrag, dann öffnet sich ein eigenes Fenster, wo man unter *Zuverlässigkeitsbasierter Schutz* ("Reputation-based protection") auf die Schaltfläche *Aktivieren* klickt.

Anschließend kann man das Feature über den Link *Einstellungen für zuverlässigkeitsbasierter Schutz* ("Reputation-based protection settings") konfigurieren.



Einstellungen für den Reputations-basierten Schutz

Anschließend wird diese Funktion automatisch auch in Edge Chromium eingeschaltet



Der Schutz gegen potenziell unerwünschte Apps wird in Microsoft Edge aktiviert

Schutz gegen PUA mit PowerShell verwalten

PowerShell bietet die nötigen Cmdlets zur Steuerung des PUA-Schutzes. Er lässt sich damit aktivieren, überprüfen und deaktivieren, außerdem kann man damit Ereignisse anzeigen.

Schutz für potenziell unerwünschte Anwendungen aktivieren:

```
Set-MpPreference -PUAProtection Enabled
```

PUA-Schutz für den Audit-Modus konfigurieren, problematische Anwendungen werden dann protokolliert, aber nicht blockiert:

```
Set-MpPreference -PUAProtection AuditMode
```

Schutz gegen unerwünschte Anwendungen deaktivieren:

```
Set-MpPreference -PUAProtection Disabled
```

Um anzuzeigen, welche Apps erkannt wurden:

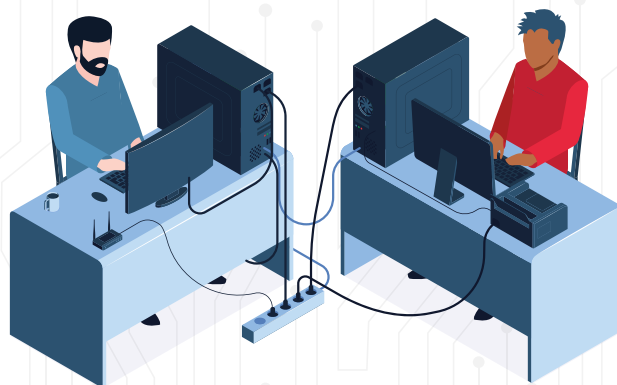
```
Get-MpThreat
```

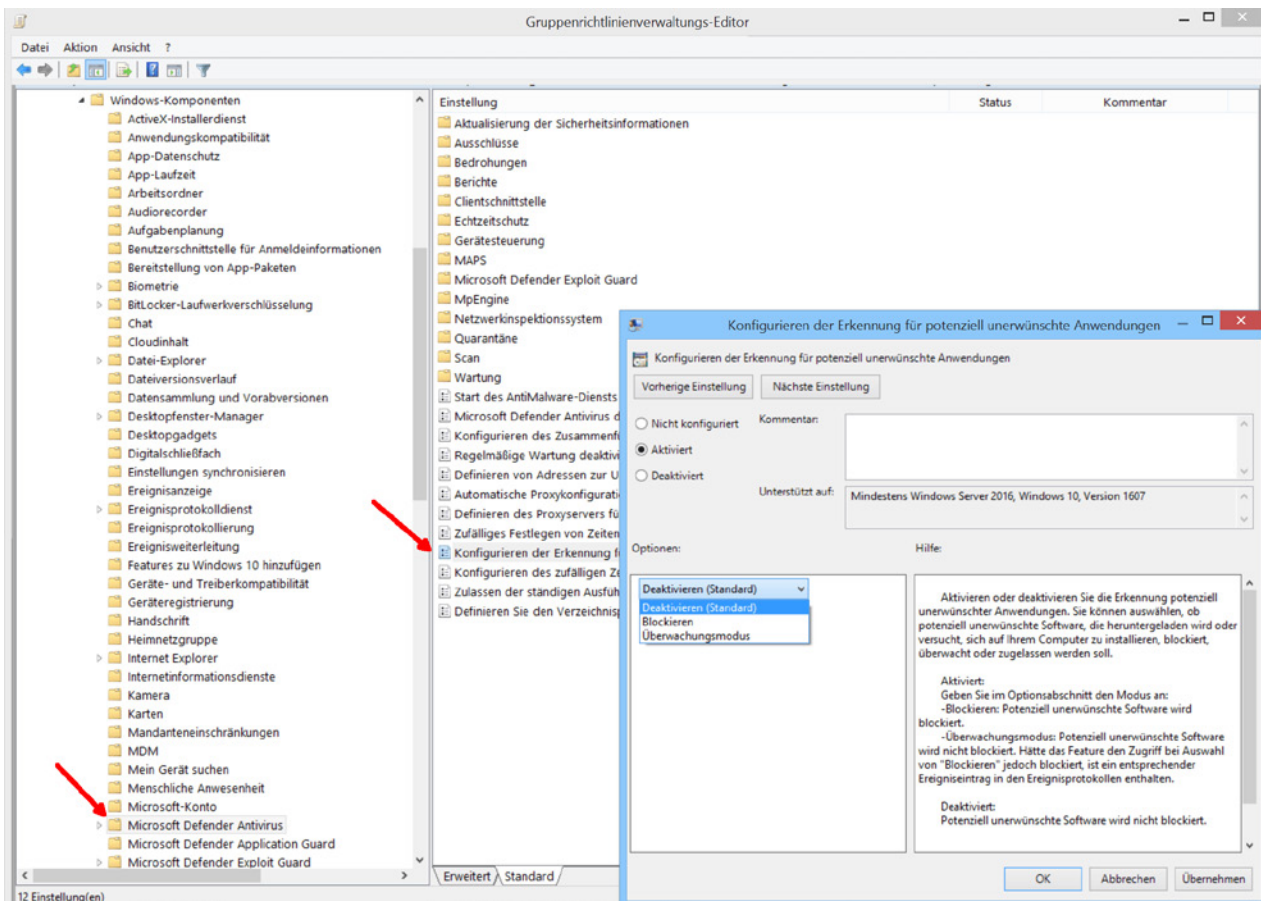
Schutz vor PUAs über GPO verwalten

Für das zentrale Management des PUA-Schutzes bietet Microsoft eine Einstellung in den Gruppenrichtlinien. Allerdings benötigt man dafür aktuelle administrative Vorlagen, und zwar mindestens die ADMX für Windows 10 20H2, damit die Option verfügbar ist.

Die Einstellung heißt *Konfigurieren der Erkennung für potenziell unerwünschte Anwendungen* ("Configure detection for potentially unwanted applications") und findet sich unter *Computerkonfiguration => Richtlinien => Administrative Vorlagen => Windows-Komponenten => Microsoft Defender Antivirus*.

Wie bei PowerShell hat man hier drei Optionen, nämlich den Schutz vor PUA zu deaktivieren, den Überwachungsmodus zu wählen oder solche Apps zu blockieren. Die Möglichkeit, den PUA-Schutz zu deaktivieren, ist deshalb von Bedeutung, weil Microsoft dieses Feature seit Windows 10 2004 für die [Enterprise Edition E5 standardmäßig einschaltet](#).





Einstellungen für potenziell unerwünschte Anwendungen mithilfe von Gruppenrichtlinien konfigurieren

Exploit Guard

Unter dem Begriff Exploit Guard (nicht zu verwechseln mit dem [Exploit-Schutz](#)) versammelt Microsoft mehrere Techniken zur Abwehr von Phishing-Angriffen und Malware. Dazu gehören der *Überwachte Ordnerzugriff*, die *Reduktion der Angriffsfläche* sowie der *Netzwerkschutz*.

Letzterer ist ein enger Verwandter von SmartScreen, das ebenfalls den Zugriff auf bedrohliche Websites unterbinden oder zumindest davor warnen kann. Dieses beschränkt sich indes nur auf Microsofts Web-Browser.

Netzwerkschutz: Blockieren unliebsamer Websites

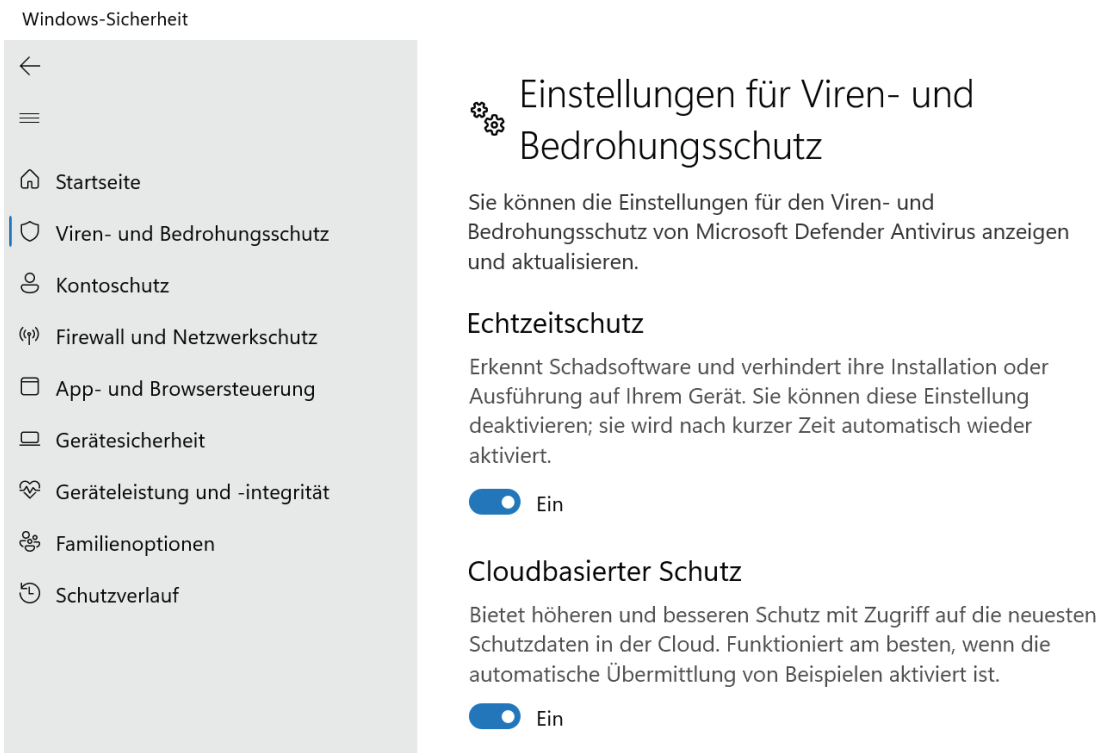
Der Netzwerkschutz hingegen operiert als Filtertreiber auf Kernel-Ebene und betrifft daher alle Anwendungen auf dem gesamten Network-Stack. Um die Reputation einer Domäne oder einer IP-Adresse zu bewerten, greift er auf den gleichen Intelligent Security Graph zurück wie SmartScreen.

Wie dieses lässt sich der Netzwerkschutz auf zwei Arten betreiben. Im Überwachungsmodus beschränkt er sich darauf, die Benutzer vor möglichen Gefahren zu warnen und einen Eintrag in das Eventlog zu schreiben. Alternativ kann man das Feature so konfigurieren, dass es Verbindungen zu bedrohlichen Hosts blockiert.

Netzwerkschutz konfigurieren

Der Schutzmechanismus ist standardmäßig nicht aktiviert und lässt sich nicht über die App Einstellungen oder eine andere lokale GUI konfigurieren. Um ihn nutzen zu können, müssen folgende Voraussetzungen gegeben sein.

- Windows 10 / 11 (Pro oder Enterprise), Windows Server 1803 oder neuer
- Der Echtzeitschutz von Defender Antivirus muss aktiviert sein
- Cloudbasierter Schutz
- Die Clients müssen in der Lage sein, `.smartscreen.microsoft.com` und `.smartscreen-prod.microsoft.com` zu kontaktieren.



The screenshot shows the Windows Security application window. On the left is a navigation pane with the following items: Startseite, Viren- und Bedrohungsschutz (highlighted), Kontoschutz, Firewall und Netzwerkschutz, App- und Browsersteuerung, Gerätesicherheit, Geräteleistung und -integrität, Familienoptionen, and Schutzverlauf. The main content area is titled 'Einstellungen für Viren- und Bedrohungsschutz'. It contains the following text and settings:

Einstellungen für Viren- und Bedrohungsschutz
Sie können die Einstellungen für den Viren- und Bedrohungsschutz von Microsoft Defender Antivirus anzeigen und aktualisieren.

Echtzeitschutz
Erkennt Schadsoftware und verhindert ihre Installation oder Ausführung auf Ihrem Gerät. Sie können diese Einstellung deaktivieren; sie wird nach kurzer Zeit automatisch wieder aktiviert.
 Ein

Cloudbasierter Schutz
Bietet höheren und besseren Schutz mit Zugriff auf die neuesten Schutzdaten in der Cloud. Funktioniert am besten, wenn die automatische Übermittlung von Beispielen aktiviert ist.
 Ein

Network Protection verlangt, dass der Echtzeitschutz und der Cloudbasierte Schutz aktiviert sind

PowerShell

Die einzige Möglichkeit für die interaktive Konfiguration von Network Protection bietet PowerShell. Mit Hilfe des Cmdlets `Get-MpPreference` kann man den aktuellen Status des Features anzeigen:
`Get-MpPreference | select *NetworkProtection* | Format-List`

```
Windows PowerShell
PS C:\Users\wolf.WINDOWSPRO> Get-MpPreference | select *NetworkProtection* | fl_

AllowNetworkProtectionDownLevel      : False
AllowNetworkProtectionOnWinServer     : False
DisableNetworkProtectionPerfTelemetry : False
EnableNetworkProtection               : 0
```

Verfügbare Einstellungen für den Netzwerkschutz

Die Ausgabe des Befehls enthält gleich vier Einstellungen. Über *EnableNetworkProtection* kann man den Netzwerkschutz einschalten, und zwar wahlweise mit den Werten *Enabled* oder *AuditMode*:

```
Set-MpPreference -EnableNetworkProtection Enabled
```

Mit *AllowNetworkProtectionOnWinServer* kann man die Aktivierung des Features auf einem Windows Server erlauben. Standardmäßig ist dies nicht möglich, so dass man erst

```
Set-MpPreference -AllowNetworkProtectionOnWinServer $true
```

ausführen muss.

Network Protection sendet anonymisierte Performance-Daten betreffend die überwachten Verbindungen an Microsoft. Mit

```
Set-MpPreference -DisableNetworkProtectionPerfTelemetry $true
```

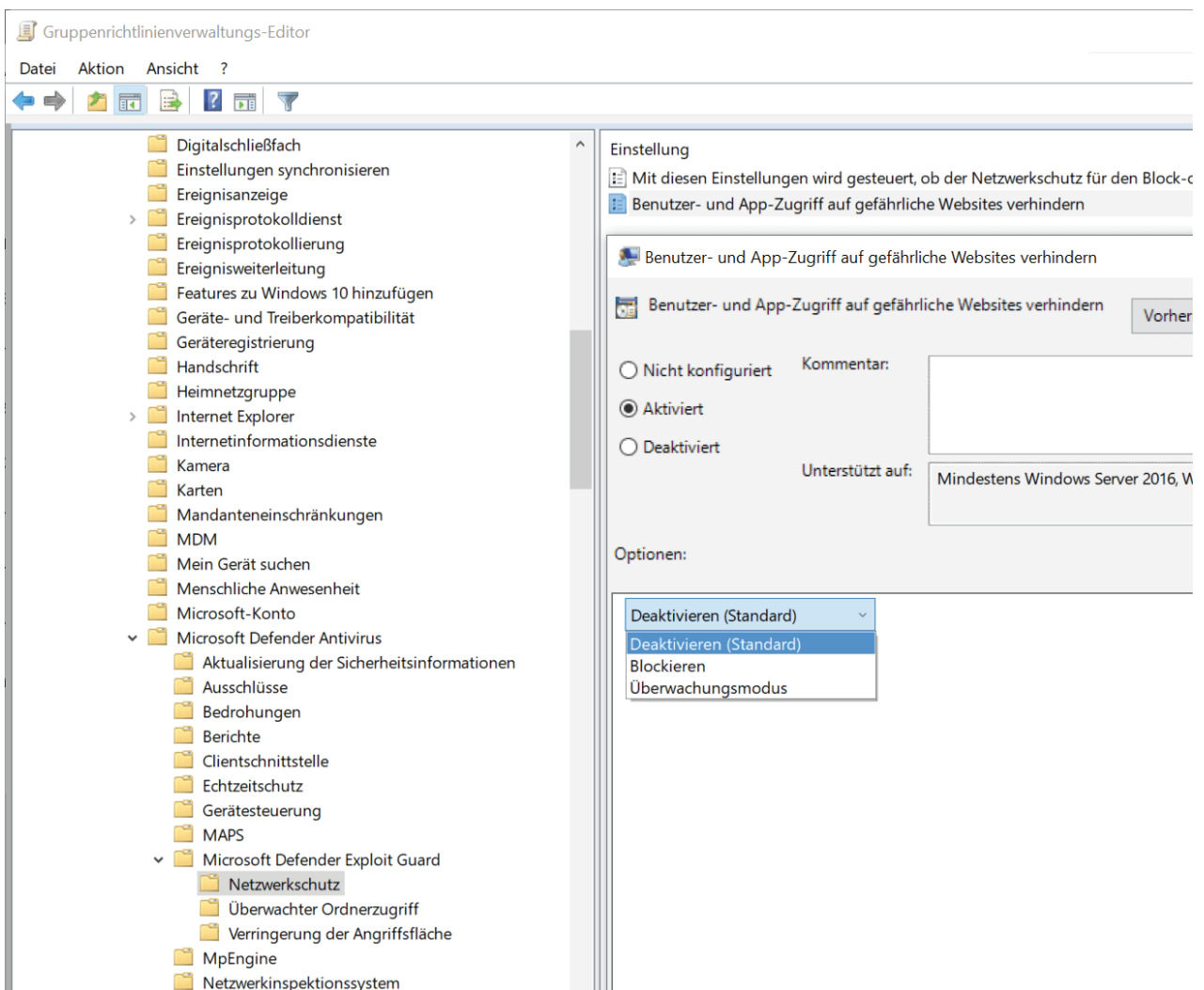
kann man das verhindern. Die Einstellung *AllowNetworkProtectionDownLevel* diente dazu, den Netzwerkschutz auch für Versionen von Windows 10 älter als 1709 zu aktivieren. Dies ist mittlerweile jedoch hinfällig.

Gruppenrichtlinien

Die Gruppenrichtlinien bieten unter *Computerkonfiguration => Richtlinien => Administrative Vorlagen => Windows-Komponenten => Microsoft Defender Antivirus => Microsoft Defender Exploit Guard => Netzwerkschutz* zwei Einstellungen:

- Benutzer- und App-Zugriff auf gefährliche Websites verhindern ("Prevent users and apps from accessing dangerous websites")
- Mit dieser Einstellung wird gesteuert, ob der Netzwerkschutz für den Block- oder Überwachungsmodus unter Windows Server konfiguriert werden darf ("This setting controls whether Network Protection is allowed to be configured into block or audit mode on Windows Server").





Netzwerkschutz über Gruppenrichtlinien aktivieren, Modus auswählen

Wenn man die erste der beiden aktiviert, dann kann man zwischen dem Überwachungs- und Blockiermodus wählen. Bei der zweiten handelt es sich um das Gegenstück zur oben beschriebenen Eigenschaft `AllowNetworkProtectionOnWinServer` in PowerShell.

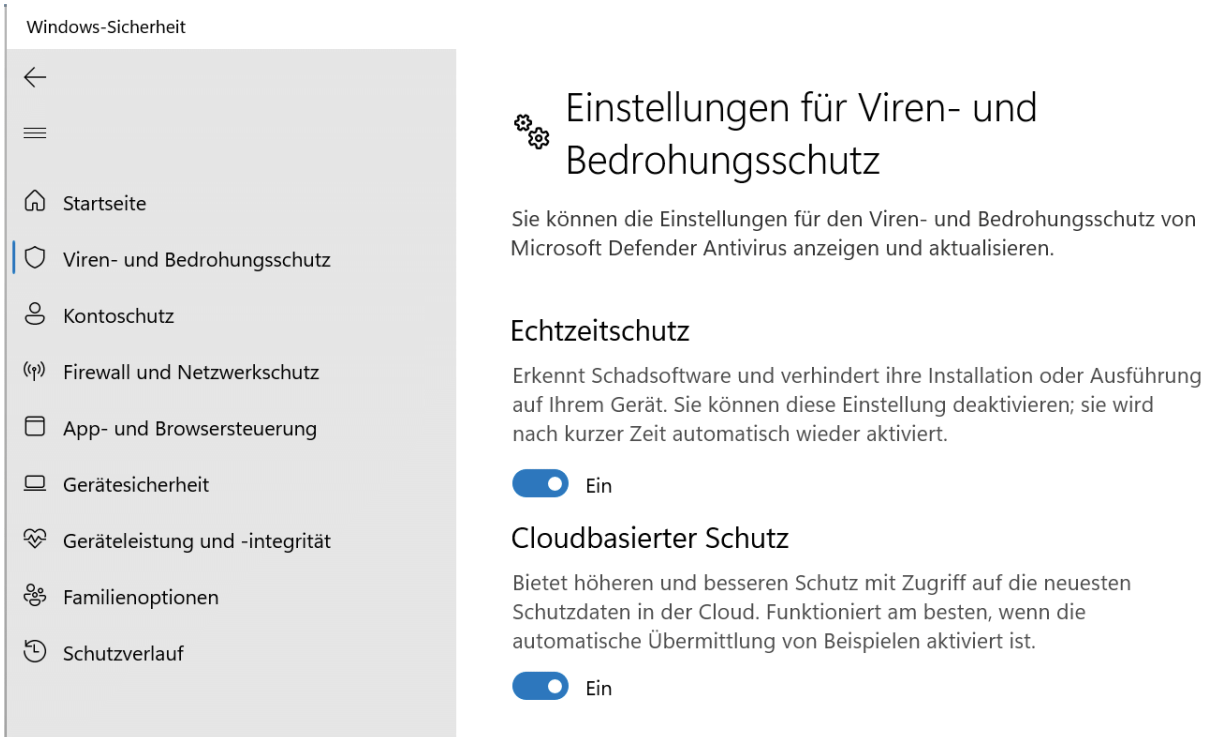
Reduktion der Angriffsfläche

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.

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 einschränken, 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.



The screenshot shows the Windows Security application interface. On the left is a navigation pane titled 'Windows-Sicherheit' with a list of settings: Startseite, Viren- und Bedrohungsschutz (highlighted), Kontoschutz, Firewall und Netzwerkschutz, App- und Browsersteuerung, Gerätesicherheit, Geräteleistung und -integrität, Familienoptionen, and Schutzverlauf. The main content area is titled 'Einstellungen für Viren- und Bedrohungsschutz'. It contains the following text and controls:

- Text: 'Sie können die Einstellungen für den Viren- und Bedrohungsschutz von Microsoft Defender Antivirus anzeigen und aktualisieren.'
- Section: 'Echtzeitschutz' with description: 'Erkennt Schadsoftware und verhindert ihre Installation oder Ausführung auf Ihrem Gerät. Sie können diese Einstellung deaktivieren; sie wird nach kurzer Zeit automatisch wieder aktiviert.' and a toggle switch set to 'Ein'.
- Section: 'Cloudbasierter Schutz' with description: 'Bietet höheren und besseren Schutz mit Zugriff auf die neuesten Schutzdaten in der Cloud. Funktioniert am besten, wenn die automatische Übermittlung von Beispielen aktiviert ist.' and a toggle switch set to 'Ein'.

Der erweiterte Schutz vor Ransomware benötigt Daten aus der Microsoft-Cloud

Limitierte Management-Optionen

Die Reduktion der Angriffsfläche 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.

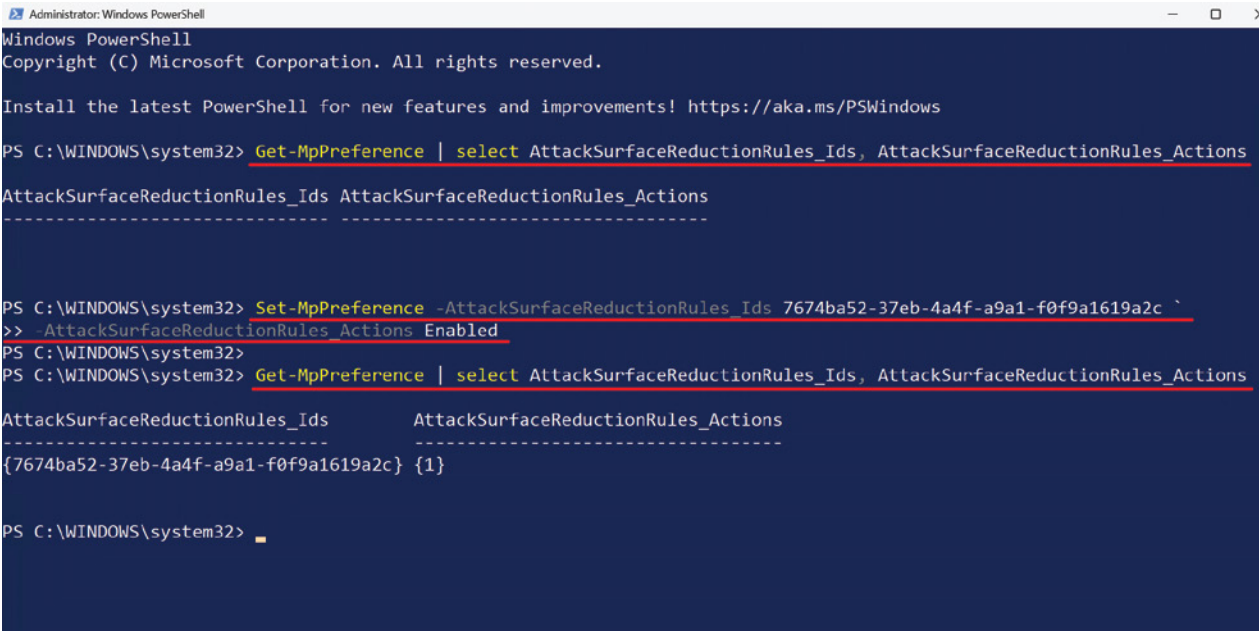
ASR über PowerShell verwalten

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 Kapitels (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 Regel ausgelöst würde) sowie 6 für Warnung, bei der User einen Hinweis auf die mögliche Gefahr erhalten, aber die Blockierung umgehen können.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> Get-MpPreference | select AttackSurfaceReductionRules_Ids, AttackSurfaceReductionRules_Actions

AttackSurfaceReductionRules_Ids AttackSurfaceReductionRules_Actions
-----
PS C:\WINDOWS\system32> Set-MpPreference -AttackSurfaceReductionRules_Ids 7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c `
>> -AttackSurfaceReductionRules_Actions Enabled
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Get-MpPreference | select AttackSurfaceReductionRules_Ids, AttackSurfaceReductionRules_Actions

AttackSurfaceReductionRules_Ids      AttackSurfaceReductionRules_Actions
-----
{7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c} {1}

PS C:\WINDOWS\system32> .
```

Status von ASR abfragen (per Default leer) und neue Regel für Adobe Reader hinzufügen

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"
```

In diesem Beispiel würden die ASR-Regeln bei Programmen im Verzeichnis c:\windows nicht greifen. Den Status dieser Eigenschaft fragt man dann mit diesem Befehl ab:

Get-MpPreference | Select AttackSurfaceReductionOnlyExclusions

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> Set-MpPreference -AttackSurfaceReductionOnlyExclusions "c:\windows"
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Get-MpPreference | select AttackSurfaceReductionOnlyExclusions

AttackSurfaceReductionOnlyExclusions
-----
{c:\windows}

PS C:\WINDOWS\system32>
```

Ausschlüsse für die ASR-Regeln mit PowerShell verwalten

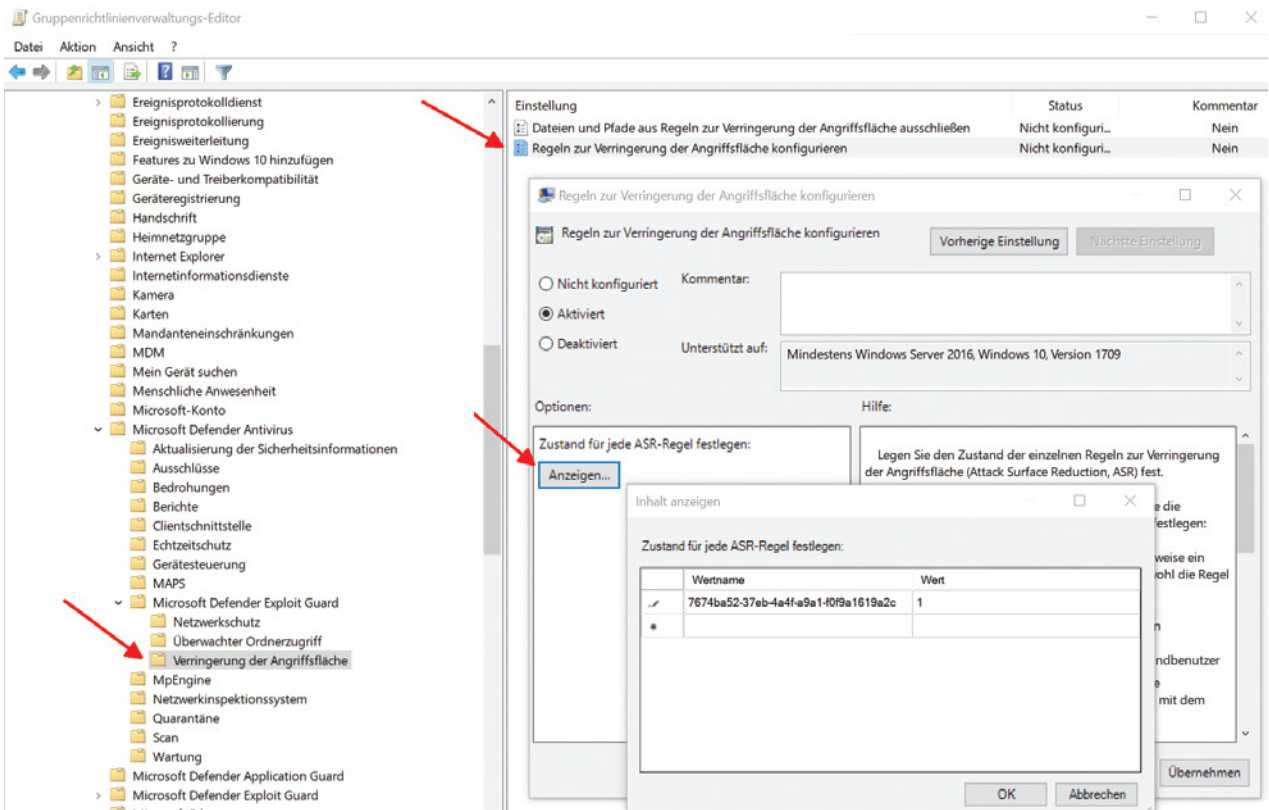
ASR-Regeln über Gruppenrichtlinien konfigurieren

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*.

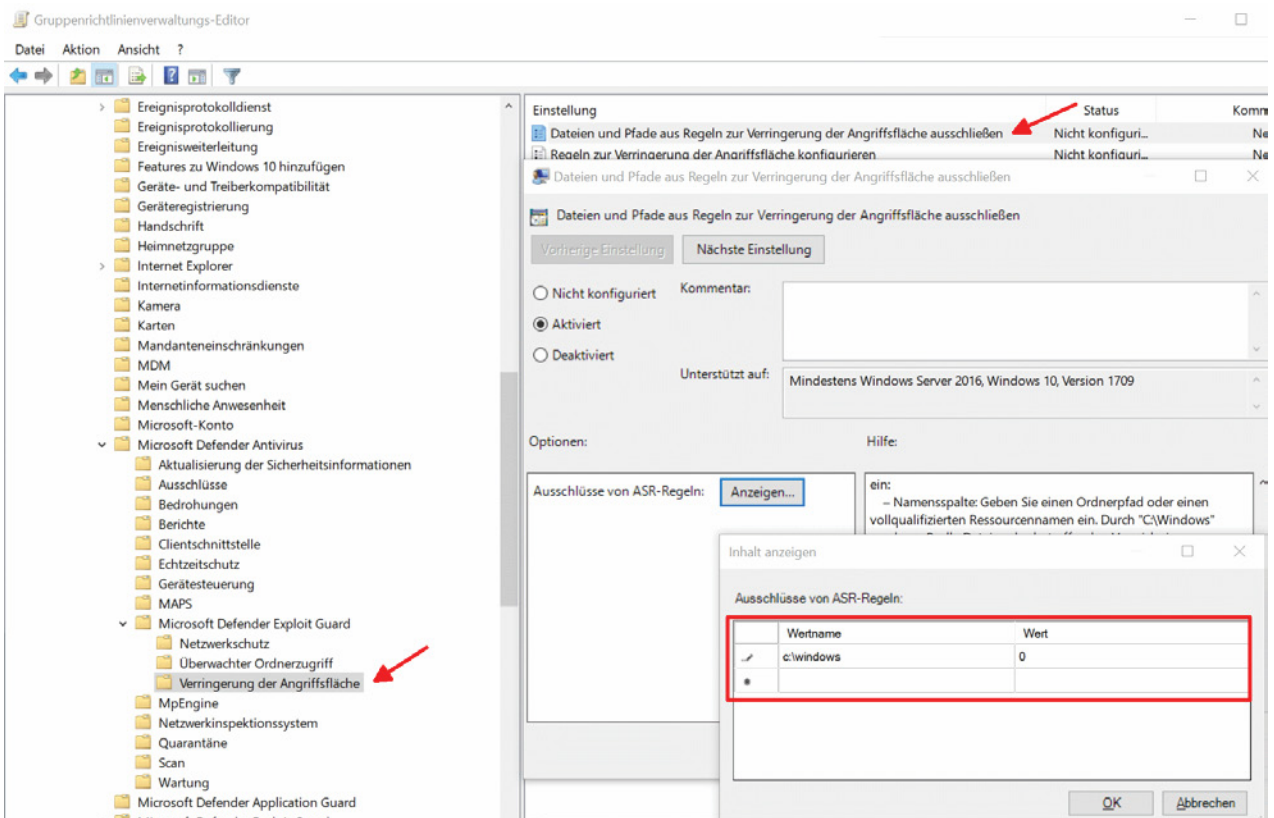
Anstatt einfach für jede Regel eine eigene Option zu aktivieren, muss man für alle eine gemeinsame Einstellung verwenden ("Regeln zur Verringerung der Angriffsfläche konfigurieren"). Dort trägt man die oben erwähnte GUID sowie den Wert für die Action in eine Tabelle ein.





GUID für eine ASR-Regel und Wert für die Aktion (Deaktivieren=0, Blockieren=1, Audit=2, Warnung=6) in die GPO-Einstellung eintragen

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-Ausschlüsse über Gruppenrichtlinien definieren

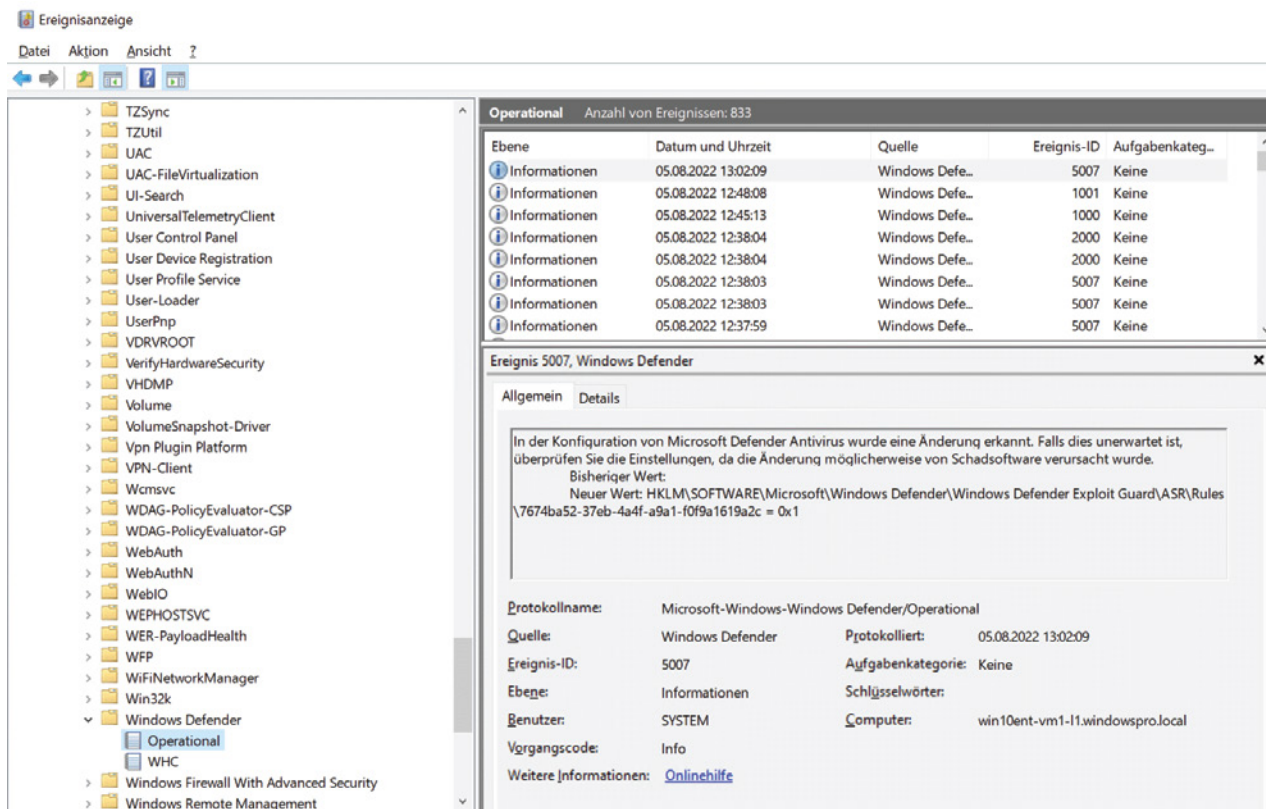
ASR im Eventlog beobachten

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.



Eventlog für Windows Defender

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?"}
```

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

Regelname	Regel-GUID
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

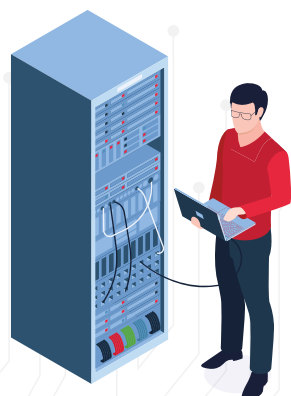
Überwacher Ordnerzugriff gegen Ransomware

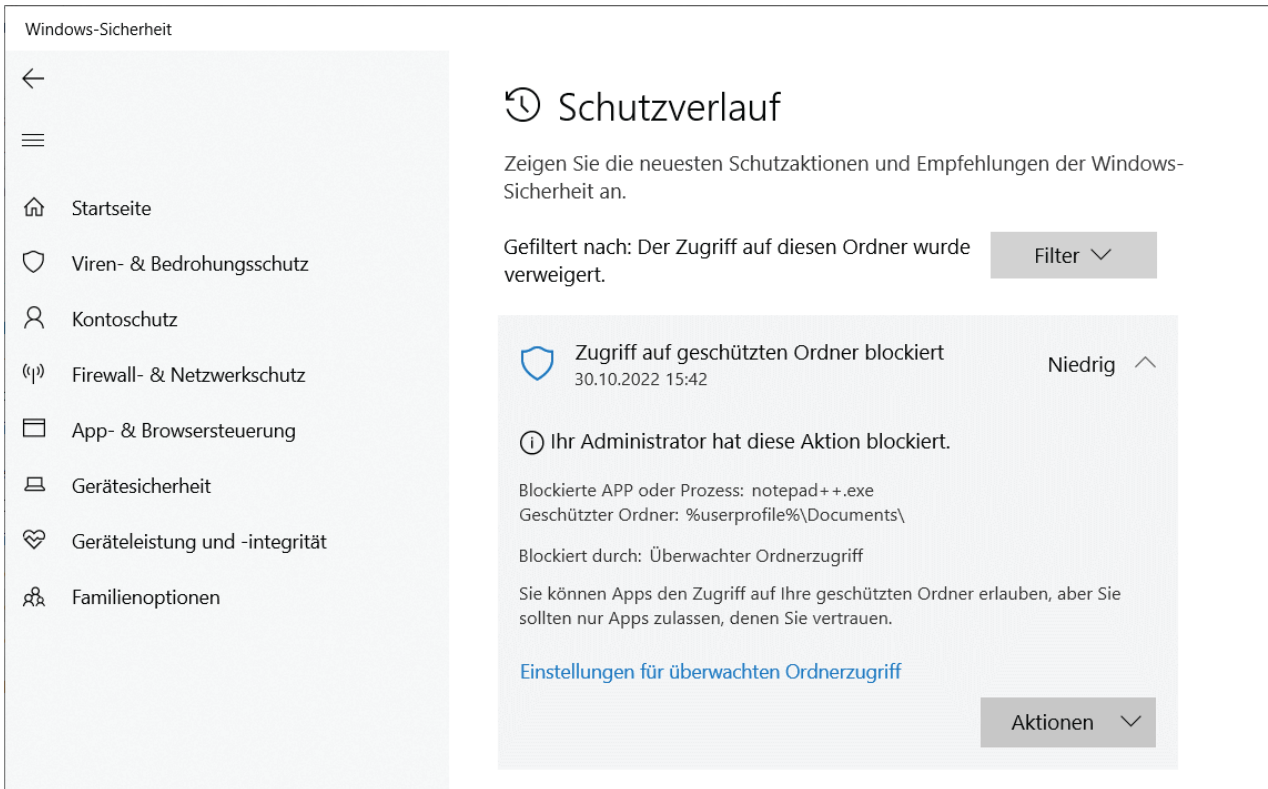
Bei Controlled Folder Access handelt es sich wie bei Smartscreen um ein reputations-basiertes Verfahren, das die Bedrohung durch Programme anhand der Häufigkeit ihres Auftretens, ihrer Herkunft oder ihres Verhaltens beurteilt.

Auf dieser Grundlage entscheidet der *Überwachte Ordnerzugriff*, ob ausführbare Dateien (.exe, .scr, .dll, etc.) Zugriff auf die Ordner des Benutzerprofils schreibend zugreifen dürfen. Die Zahl der zu Unrecht blockierten Programme ist allerdings erstaunlich hoch. Der Ransomware-Schutz schlägt nicht nur bei vielen harmlosen Apps an, sondern auch bei Bordmittel wie PowerShell.

Die Anwender können die vom System erstellte Blacklist zwar nicht ändern, aber dafür die Liste der unbedenklichen Anwendungen erweitern. Dieser Vorgang ist jedoch ziemlich umständlich, da man sich manchmal gleich zweimal mit einem administrativen Konto anmelden muss.

Welche Anwendungen blockiert wurden, erkennt man zum einen durch eine entsprechende Toast-Benachrichtigung und durch den Blockierungsverlauf in der App *Windows-Sicherheit*. Außerdem erzeugt das Feature bei dieser Gelegenheit einen Eintrag in der Ereignisanzeige.





Per Voreinstellung werden populäre Anwendungen wie Notepad++ und sogar PowerShell blockiert

Benutzer können außerdem die Liste der Ordner erweitern, aber die per Vorgabe geschützten Verzeichnisse nicht abwählen. Der *überwachte Ordnerzugriff* akzeptiert dabei nicht nur lokale Laufwerke, vielmehr kann er auch auf Netzfreigaben aufpassen.

Evaluierung im Audit-Modus

Grundsätzlich empfiehlt es sich, den überwachten Ordnerzugriff aufgrund der vielen falsch Positiven erst im Audit-Modus zu starten und über einen bestimmten Zeitraum zu untersuchen, welche Auswirkungen er im praktischen Betrieb hätte.



Als Administrator kann man den überwachten Ordnerzugriff interaktiv ein- und ausschalten

Konfiguriert man das Feature interaktiv über die App *Einstellungen*, dann stehen nur die Optionen *Ein* und *Aus* zur Verfügung (man benötigt dafür administrative Rechte). Um den Audit-Modus zu aktivieren, muss man daher zu PowerShell oder den Gruppenrichtlinien greifen. Der Aufruf von

```
Set-MpPreference -EnableControlledFolderAccess AuditMode
```

würde diese Aufgabe in PowerShell erfüllen.

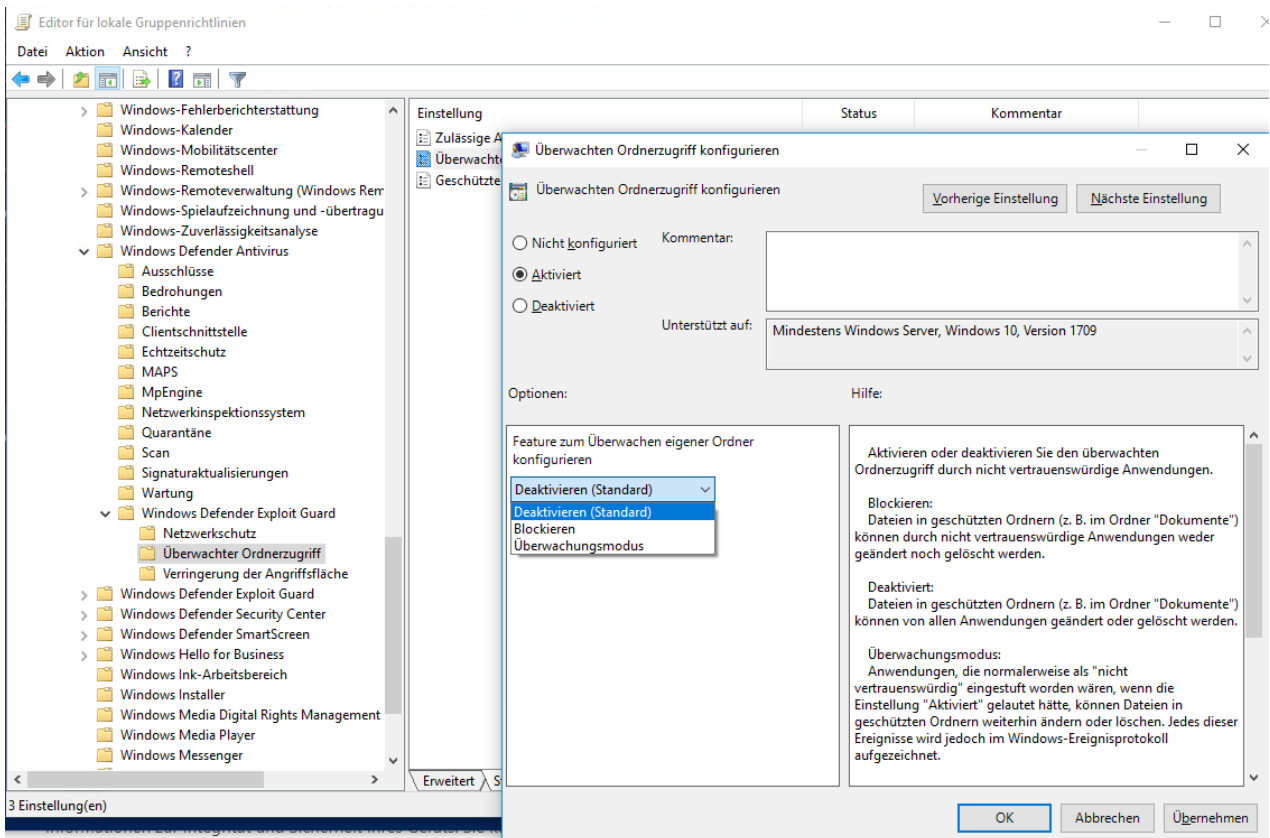
Blockiermodus aktivieren

Ersetzt man *AuditMode* durch *Enabled*, dann wird das Feature scharf geschaltet:

```
Set-MpPreference -EnableControlledFolderAccess Enabled
```

Aktiviert man Controlled Folder Access mit Hilfe von Gruppenrichtlinien, dann hat man dort ebenfalls die Auswahl zwischen diesen beiden Modi.

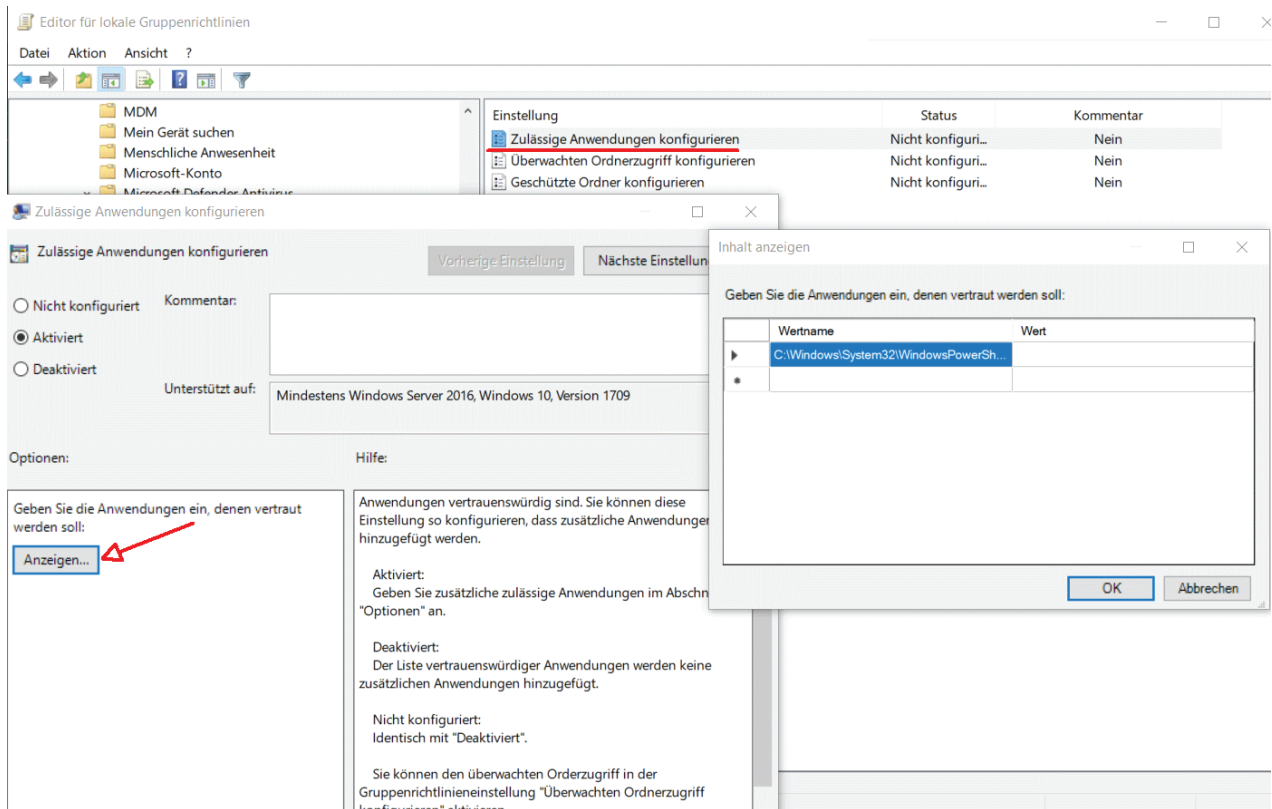
Die dafür vorgesehene Einstellung *Überwachten Ordnerzugriff konfigurieren* findet sich unter *Computerkonfiguration => Richtlinien => Administrative Vorlagen => Windows-Komponenten => Microsoft Defender Antivirus => Microsoft Defender Exploit Guard => Überwacher Ordnerzugriff*.



Aktivieren des Controlled Folder Access über Gruppenrichtlinien

Zusätzliche Ordner und Apps festlegen

Die Gruppenrichtlinien bieten zwei weitere Einstellungen, mit denen man jeweils die Liste der Ordner bzw. der Anwendungen erweitern kann, die geschützt bzw. zugelassen werden sollen. Sie heißen *Geschützte Ordner konfigurieren* und *Zulässige Anwendungen konfigurieren*.



Zulässige Anwendungen über eine Gruppenrichtlinie definieren

In PowerShell ist dafür ebenfalls das Cmdlet `Set-MpPreference` zuständig, und zwar mit den Parametern `ControlledFolderAccessProtectedFolders` (für zusätzliche Ordner) und `ControlledFolderAccessAllowedApplications` für weitere zulässige Programme. Sie verlangen den Pfad zu den Verzeichnissen bzw. Anwendungen:

```
Set-MpPreference -ControlledFolderAccessProtectedFolders "c:\temp"
```

Die Existenz des betreffenden Verzeichnisses wird dabei nicht geprüft.

Auswertung der Logs

Microsoft stellte nach der Einführung dieses Features ein *Exploit Guard Evaluation Package* zur Verfügung, das Tools zum Testen des überwachten Ordnerzugriffs enthielt. Dieses ist mittlerweile sang- und klanglos von Microsofts Website verschwunden.

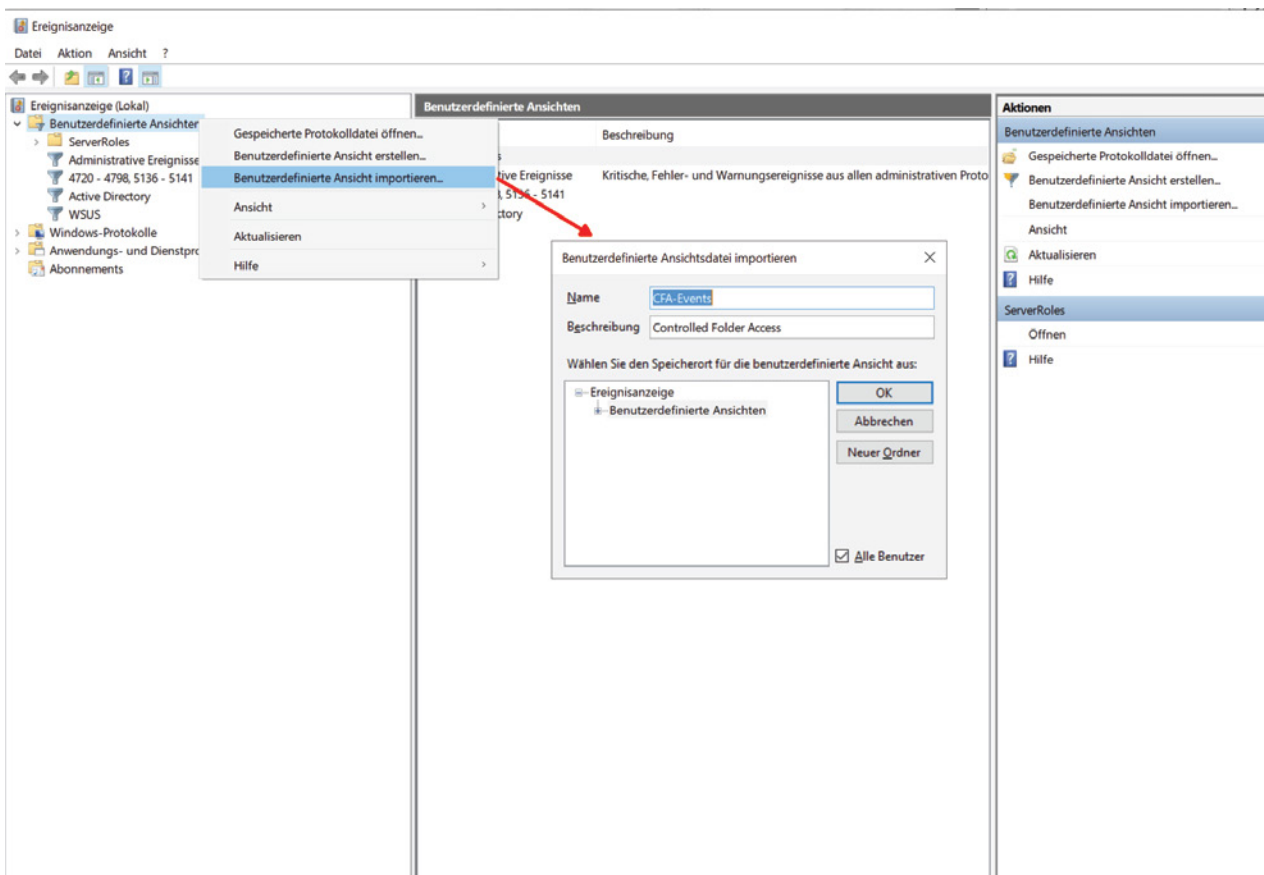
Im Paket enthalten war unter anderem die Exportdatei einer benutzerdefinierten Log-Ansicht, die einen Filter für alle Log-Einträge von Controlled Folder Access enthält:


```

<ViewerConfig> <QueryConfig>
<QueryParams> <UserQuery /> </QueryParams>
<QueryNode> <Name>CFA-Events</Name> <Description>Controlled Folder Access</Description>
<QueryList> <Query Id="0" Path="Microsoft-Windows-Windows Defender/Operational">
<Select Path="Microsoft-Windows-Windows Defender/Operational">*[System[(EventID=1123 or
EventID=1124 or EventID=5007)]]</Select>
<Select Path="Microsoft-Windows-Windows Defender/WHC">*[System[(EventID=1123 or EventID=1124 or
EventID=5007)]]</Select>
</Query> </QueryList>
</QueryNode>
</QueryConfig> </ViewerConfig>

```

Wenn man obigen Code in einer Datei namens *cfa-events.xml* speichert, dann kann man sie in die Ereignisanzeige importieren, um die Logs für den überwachten Ordnerzugriff auszuwerten.



Importieren einer benutzerspezifischen Ansicht für den überwachten Ordnerzugriff in die Ereignisanzeige

Microsoft Defender mit ACMP verwalten

Die bisherigen Ausführungen zeigen, dass Windows unter der Bezeichnung *Defender* eine ganze Palette von Schutzmechanismen gegen Malware und Phishing umfasst. Auch wenn einzelne davon durchaus verbesserungswürdig sind, so braucht besonders der Virenscanner den Vergleich mit kommerziellen Produkten nicht zu scheuen.

Diese Security-Komponenten leiden in professionellen Umgebungen jedoch unter den limitierten Management-Funktionen. Diese beschränken sich auf Gruppenrichtlinien, PowerShell und Utilities wie [MpCmdRun](#). Microsoft füllt diese Lücke mit kostenpflichtigen Cloud-Services (Defender for Endpoint, Intune, etc.) sowie dem Configuration Manager.

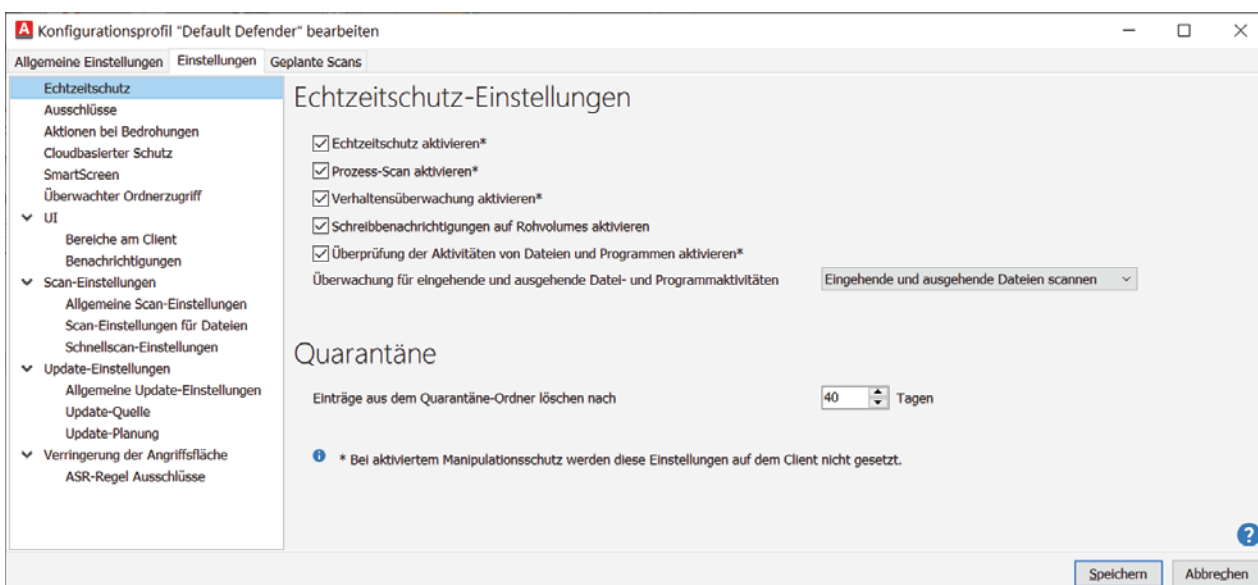
Als Alternative empfehlen sich Produkte von Drittanbietern wie ACMP von Aagon. Diese reine On-prem-Lösung für das Endpoint-Management umfasst ein Modul für eine vollständige Verwaltung von Microsoft Defender.

Dieses bietet eine große Flexibilität bei der Zuweisung von Konfigurationen, Benachrichtigungen, dem Erstellen von Reports, die sich um eigene Berichte erweitern lassen, ein anpassbares Dashboard oder die Integration mit dem Active Directory.

Defender-Konfiguration über Profile

Dreh- und Angelpunkt der Defender-Verwaltung in ACMP sind Profile. Sie enthalten sämtliche Einstellungen, mit denen sich das Verhalten des Virenscanners steuern lässt. Die meisten davon entsprechen jenen, welche auch die Gruppenrichtlinien bieten.

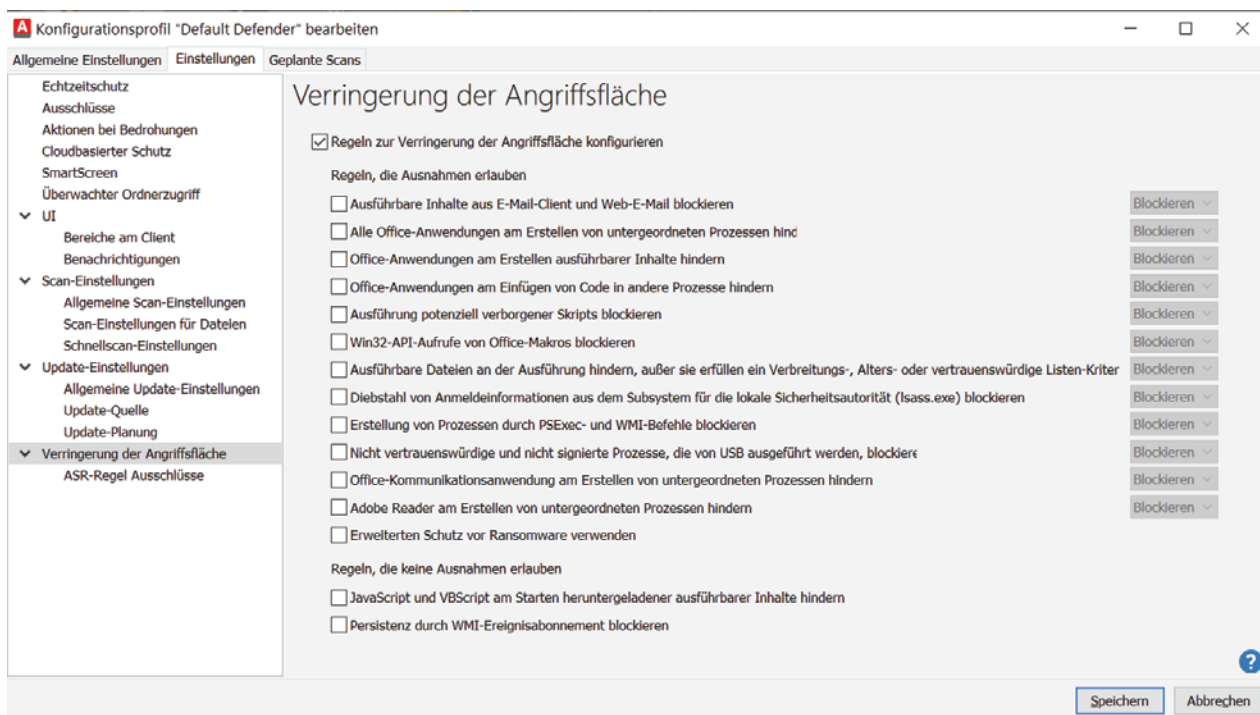
Dazu gehören sämtliche Optionen für die Anpassung des Echtzeitschutzes, der Ausschluss von Verzeichnispfaden, Dateitypen oder Prozessen von der Überprüfung, das Festlegen der Reaktionen auf gefundene Bedrohungen sowie eine Vielzahl von Scan-Einstellungen.



Einstellungen zum Anpassen des Echtzeitschutzes durch Windows Defender Antivirus

In der Regel wird kaum ein Unternehmen mit einem einzigen Profil auskommen, das allen PCs die gleiche Defender-Konfiguration zuweist. So empfiehlt Microsoft beispielsweise den Ausschluss von mehreren Pfaden und Dateien auf einem SQL- oder Exchange-Server, um deren Performance nicht zu beeinträchtigen.

Denkbar wäre etwa auch, dass Admins die Regeln zur Reduktion der Angriffsfläche je nach Anwendergruppe verschieden einsetzen. Mit diesen Policies erhöht Defender die Sicherheit der Systeme, indem es diverse Funktionen etwa in Office blockiert. Das mag nicht auf allen PCs gleichermaßen erwünscht sein.



Über Profile lassen sich auch die Einstellungen zur Reduktion der Angriffsfläche konfigurieren

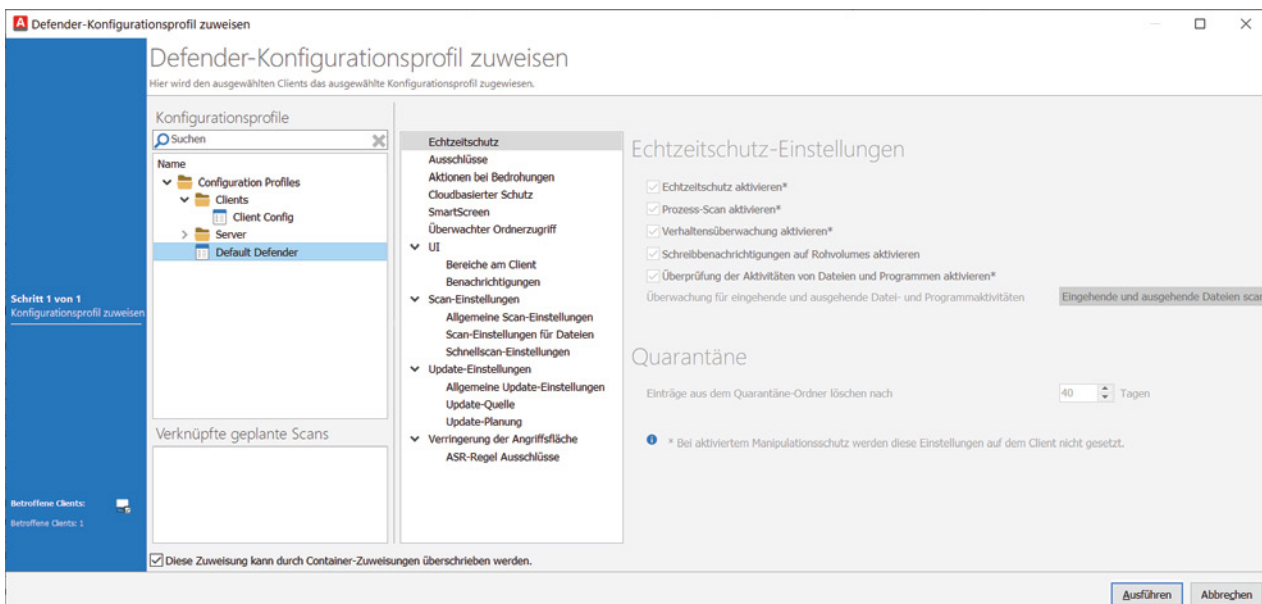
Flexible Zuweisung von Profilen

Die Lösung besteht hier im Anlegen mehrerer Profile, welche für die jeweilige Zielgruppe maßgeschneidert sind.

Bei den Gruppenrichtlinien würde man dafür verschiedene GPOs anlegen, die sich dann jedoch nur an Domänen oder OUs zuweisen ließen. Man müsste mithin die Rechner in eigene OUs einsortieren oder umständlich mit Sicherheits- bzw. WMI-Filtern hantieren, damit sie die passende Defender-Konfigurationen erhalten.

ACMP erlaubt hingegen das Erzeugen dynamischer Gruppen anhand zahlreicher Kriterien. So könnte man ein Defender-Profil mit Ausschlüssen für SQL-Server erstellen und dieses automatisch allen Rechnern zuweisen, auf denen die Microsoft-Datenbank installiert ist.

Dieses Konzept ist äußerst flexibel, weil der Agent das Inventar automatisch aktualisiert. Würde etwa ein Software-Entwickler auf seinem PC einen SQL-Server installieren, dann taucht der Rechner automatisch in der entsprechenden dynamischen Gruppe auf und erhält somit das SQL-Profil.



Profile lassen sich an bestimmte Clients oder an statische und dynamische Gruppen zuweisen

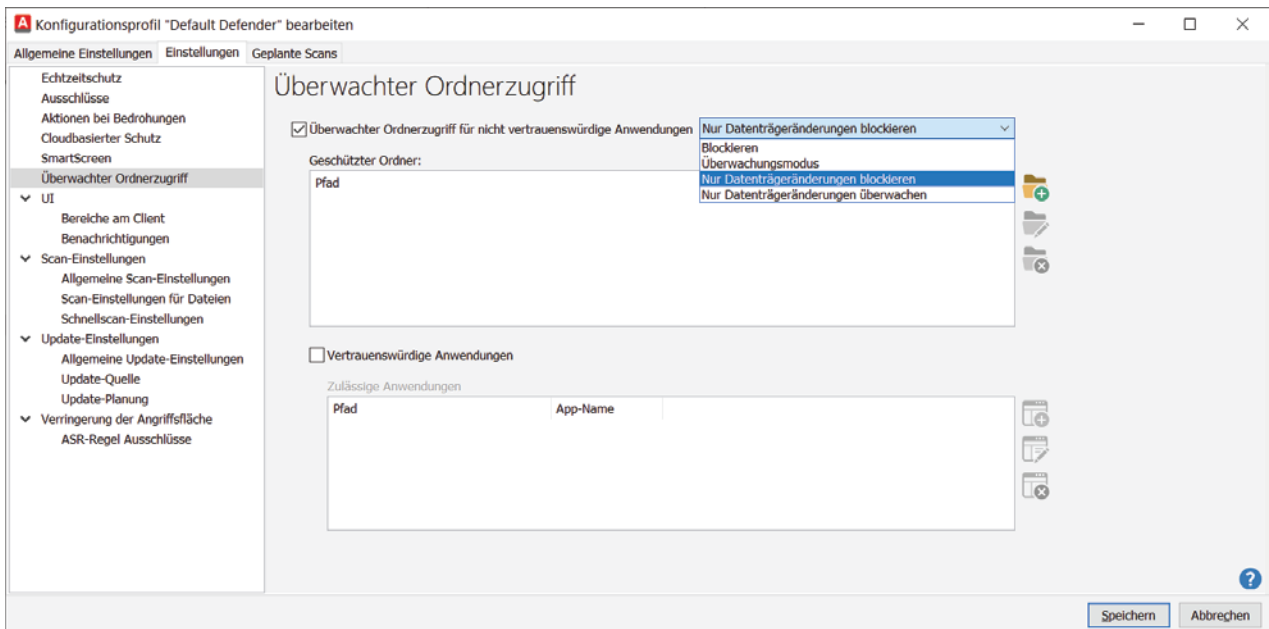
Ähnlich ließen sich Profile abhängig vom Netzwerk des Computers zuweisen, so dass etwa im Firmen-LAN andere Einstellungen greifen als im Home Office. Auch hier muss der Systemverwalter nicht manuell nachjustieren, weil eine solche dynamische Gruppe ihre Mitglieder über die IP-Adresse automatisch aktualisiert.

Schutz gegen Ransomware

Microsoft Defender bietet neben dem Scannen von Dateien auf mögliche Malware einige zusätzliche Schutzfunktionen. Dazu gehört die Ransomware Protection ("Überwacher Ordnerzugriff"). Grundsätzlich handelt es sich dabei um ein nützliches Feature, das bei einer interaktiven Konfiguration jedoch kaum brauchbar ist.

Jedes Mal, wenn eine legitime Anwendung beim Zugriff auf einen geschützten Ordner blockiert wird, muss der Nutzer über die entsprechende Benachrichtigung die App Einstellungen öffnen und das Programm dann freischalten. Dabei muss man sich gleich zwei Mal über ein privilegiertes Konto authentifizieren.

In einer verwalteten Umgebung verfügen die Anwender jedoch über kein Admin-Passwort, so dass diese Möglichkeit entfällt. Wie die Gruppenrichtlinien erlaubt das ACMP Defender Management daher, zulässige Applikationen zu hinterlegen, die auf die Benutzerverzeichnisse zugreifen dürfen.



Admins können Anwendungen vorgeben, die vom Ransomware-Schutz nicht blockiert werden sollen

Zudem lässt sich der Ransomware-Schutz in einem Überwachungsmodus betreiben, über den Admins herausfinden können, welche Anwendungen in die Whitelist aufgenommen werden sollten.

Manipulationsschutz

Ein weiterer Schutz gegen böswillige Akteure ist die so genannte Tamper Protection ("Manipulationsschutz"), die das Deaktivieren von Defender verhindert. Dies würde Hackern das Platzieren von Trojanern und anderer Malware deutlich erleichtern.

Diese Funktion lässt sich aber nicht über Gruppenrichtlinien oder PowerShell steuern, weil ein Angreifer mit administrativen Rechten einen entsprechenden Schlüssel in der Registry nach Gutdünken ändern und so die Tamper Protection aushebeln könnte.

Computer Name	Defender Manipulationsschutz aktiviert	Primäre IP	Computer Domäne	Defender Scan Daten
ACMP-2022	✓ Ja	192.168.0.61	ACMP	27.07.2022 23:13:06
TEST-WIN11	✓ Ja	192.168.100.21	ACMP	25.02.2022 14:52:08
TRAIN7	✓ Ja	192.168.50.29	SCHULUNG	17.02.2022 15:25:00
WIN11PRO-VM1-L2	✓ Ja	192.168.0.74	ACMP	27.07.2022 13:45:08
1-Mobil	■ nicht verfügbar	123.123.123.123	ACMP	nicht verfügbar
1-RDP01	■ nicht verfügbar	192.168.50.3	SCHULUNG	nicht verfügbar
1-SCHSW01	■ nicht verfügbar	192.168.50.4	SCHULUNG	nicht verfügbar
4-CODSKI-W10	■ nicht verfügbar		WORKGROUP	nicht verfügbar
4-COFFUH-W10	■ nicht verfügbar		WORKGROUP	nicht verfügbar
4-CORLOE-W10	■ nicht verfügbar		WORKGROUP	nicht verfügbar
4-COSLIM-W10	■ nicht verfügbar		WORKGROUP	nicht verfügbar
ACMP-2016	■ nicht verfügbar	192.168.50.2	SCHULUNG	nicht verfügbar
DC-2016	■ nicht verfügbar	192.168.50.1	SCHULUNG	nicht verfügbar
ESXI-1	■ nicht verfügbar	192.168.50.1	SCHULUNG	nicht verfügbar

ACMP Defender Management zeigt, auf welchen PCs die Tamper Protection aktiviert ist

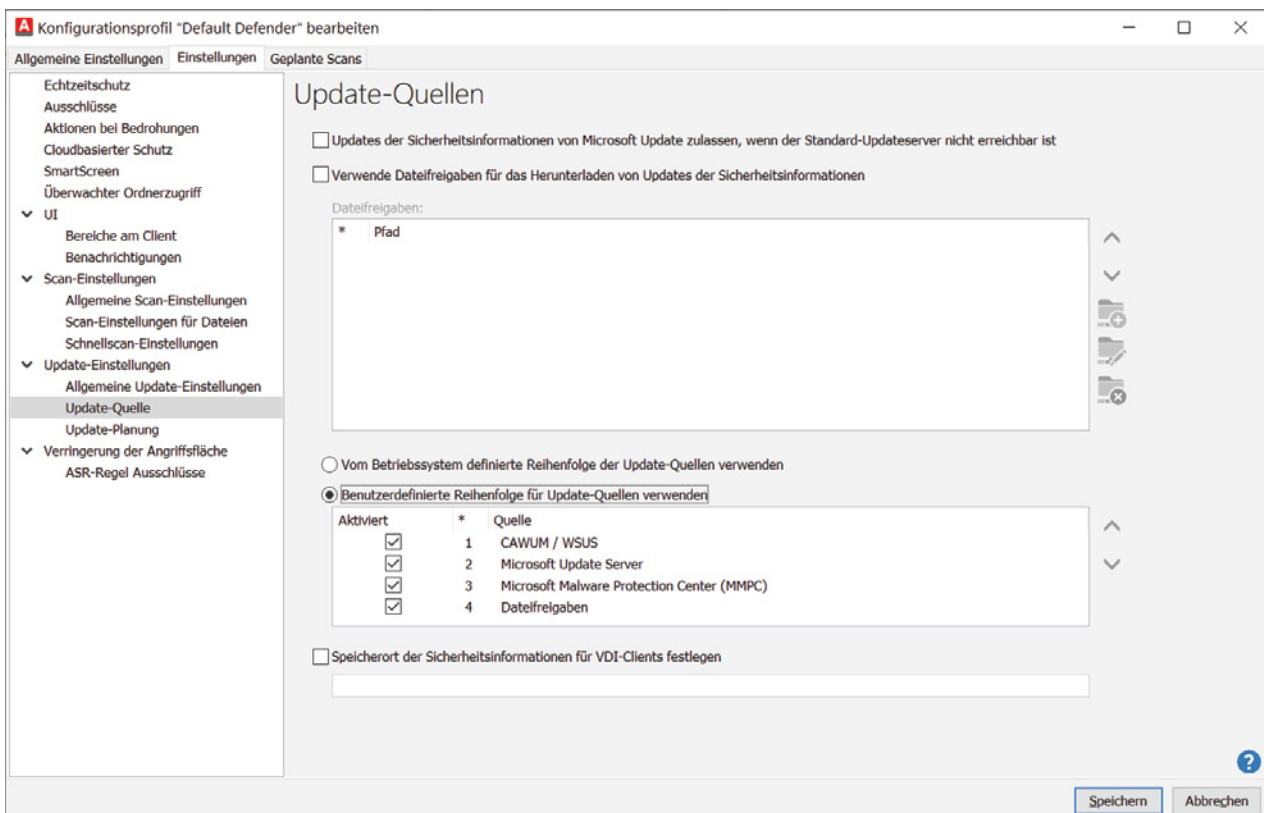
Microsoft behält das An- und Ausschalten des Manipulationsschutzes daher Management-Tools wie Intune vor, die dafür ein bestimmtes Zertifikat des Herstellers benötigen.

ACMP unterstützt diese Möglichkeit aktuell noch nicht, bietet aber eine vorkonfigurierte Abfrage, aus welcher der Status dieser Einstellung ersichtlich ist.

Update der Signaturen

Die Wirksamkeit eines Malware-Schutzes hängt auch von der Aktualität der Virensignaturen ab. Daher müssen IT-Verantwortliche darauf achten, dass diese stets auf dem neuesten Stand sind.

Microsoft sieht für den Download der Defender-Signaturen redundante Quellen vor. Selbst wenn Windows seine Updates grundsätzlich über WSUS bezieht, kann Defender parallel dazu prüfen, ob neue Signaturdateien auf Windows Update, dem Microsoft Malware Protection Center oder auf einer dafür vorgesehenen Netzfreigabe vorliegen.

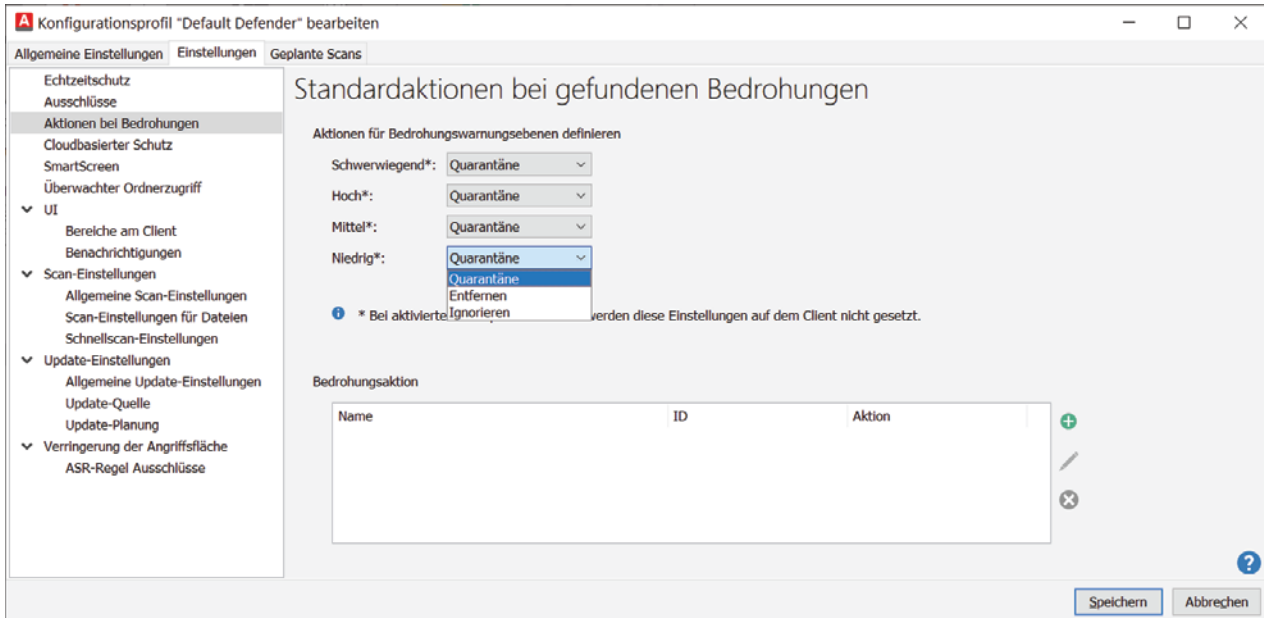


Konfiguration der Update-Quellen für die Viren-Signaturen

Wie in den Gruppenrichtlinien lassen sich diese Quellen auch in ACMP hinzufügen bzw. entfernen sowie in eine Reihenfolge bringen, um damit ihre Priorität zu bestimmen. Das ACMP Defender Management integriert zudem das Update-Modul [CAWUM](#) (Complete Aagon Windows Update Management) dessen Verteilerringe kürzlich erweitert wurden, um die Verteilung der Antiviren-Updates zu beschleunigen.

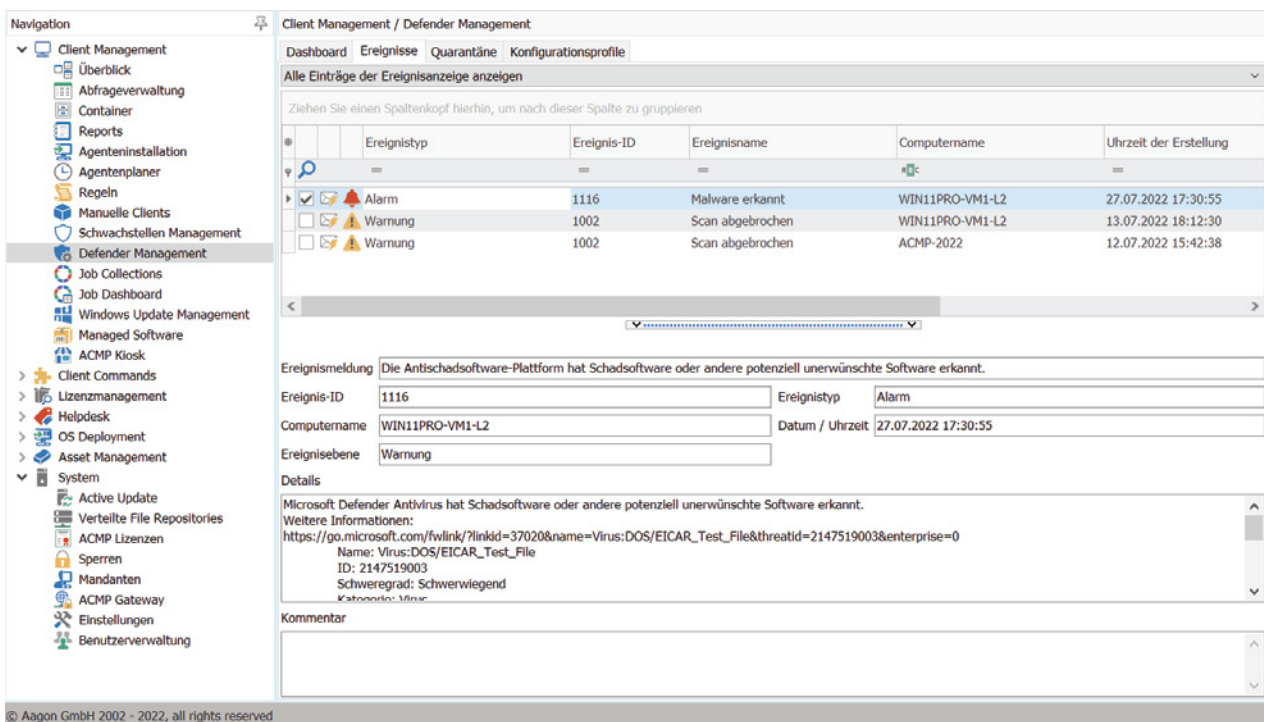
Reaktion auf gefundene Bedrohungen

Wie praktisch alle Antiviren-Lösungen sieht auch Microsoft Defender verschiedene Aktionen für den Fall vor, dass es potenziellen Schadcode oder unerwünschte Aktivitäten entdeckt. Je nach Schweregrad der Bedrohungen kann man die betroffenen Dateien löschen, in Quarantäne stellen oder den Vorfall ignorieren.



Optionen für die Reaktion auf erkannte Bedrohungen

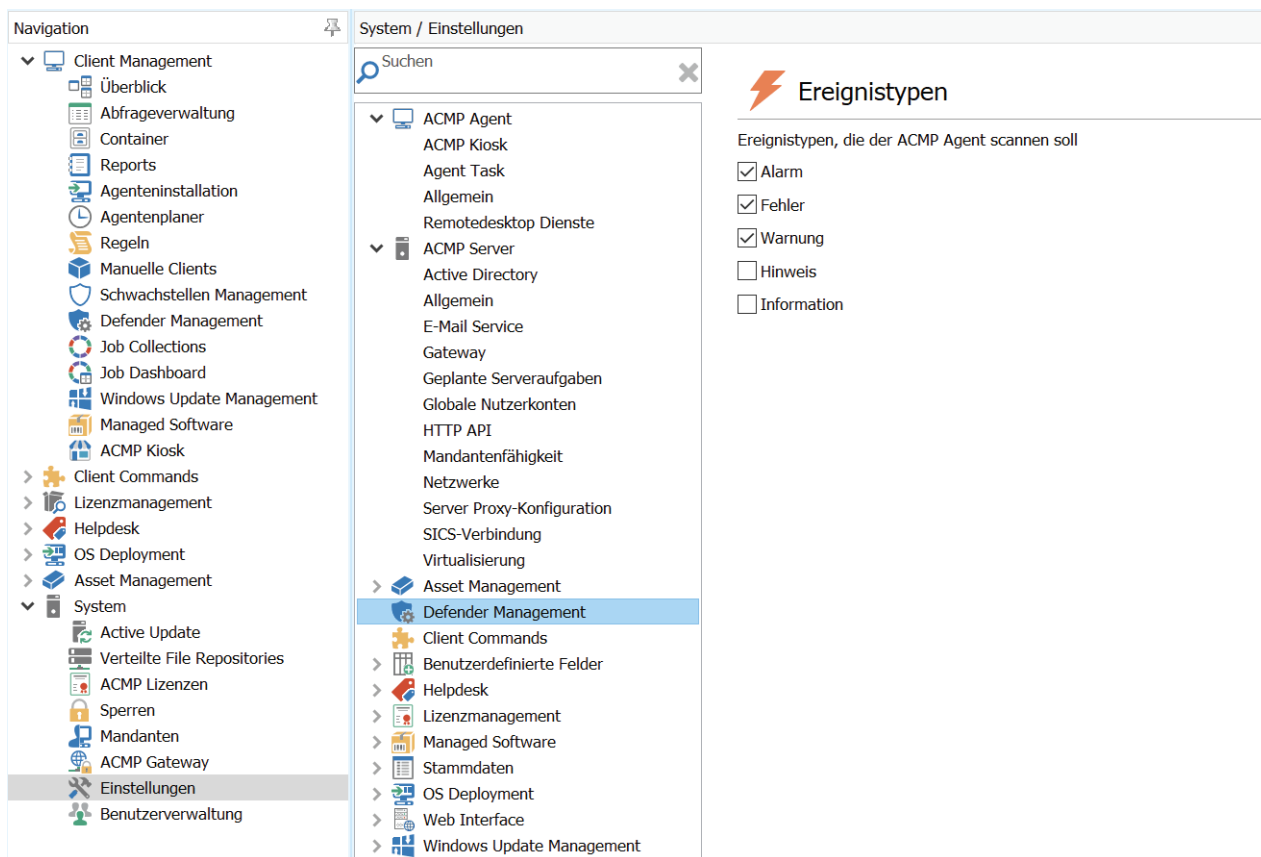
Dabei handelt es sich um lokale Ereignisse, von denen ein Admin ohne ein zentrales Defender-Management nichts erfährt. ACMP unterstützt die Systemverwaltung hier auf zweierlei Art.



Übersicht über alle im Netzwerk aufgetretenen Ereignisse

Zum einen bietet es eine übergreifende Quarantäneverwaltung, die sämtliche verdächtigen und isolierten Dateien auf allen PCs zeigt. Falls eine solche zu Unrecht als Bedrohung eingestuft wurde, kann der Admin sie von seiner Konsole aus auf dem ursprünglichen Ort des jeweiligen PCs wiederherstellen.

Zum anderen ist es wichtig, dass Systemverwalter umgehend vom Auftreten einer Bedrohung erfahren. Der ACMP-Agent überträgt deshalb einen Alarm per Push-Nachricht an den Server, so dass er sofort in der Konsole erscheint. Andere Ereignisse wie Warnungen oder Fehlermeldung werden hingegen nur in regelmäßigen Intervallen abgefragt.

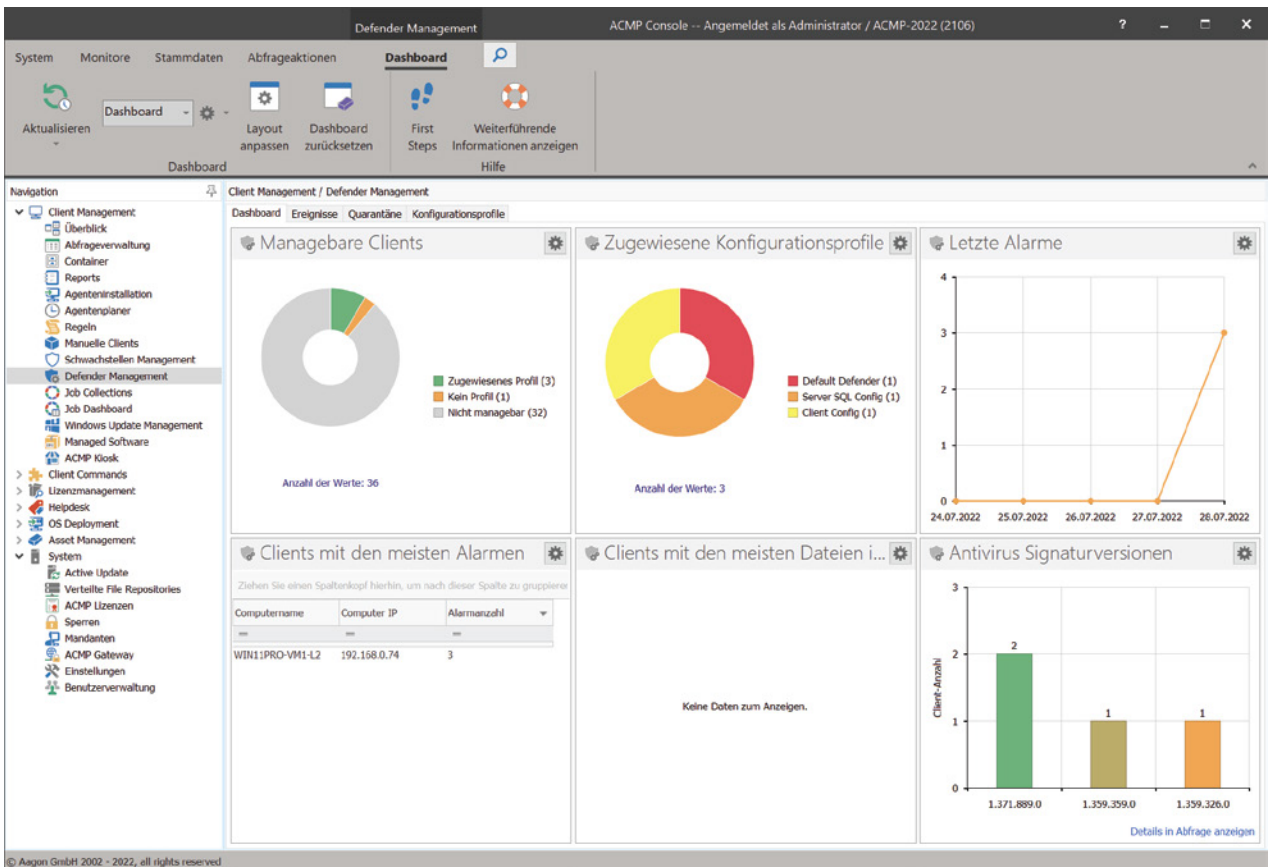


In ACMP kann man wählen, welche Arten von Ereignissen im Defender Management berücksichtigt werden sollen

Da Admins nicht ständig die ACMP-Konsole beobachten, könnte ihnen ein Alarm leicht entgehen. Daher bietet das Tool die Möglichkeit, die zuständigen Mitarbeiter zu benachrichtigen, beispielsweise per E-Mail.

Dashboard und Reports

Neben der unmittelbaren Benachrichtigung über kritische Ereignisse informiert ACMP die Systemverwaltung über alle möglichen Aspekte des Malware-Schutzes mittels Dashboard. Daraus lässt sich mit einem Blick entnehmen, wie viele Clients über das Defender-Management verwaltet werden und welche davon ein Profil erhalten haben.



Das Defender Management enthält ein vorkonfiguriertes Dashboard, das sich bei Bedarf anpassen lässt

Weitere Widget geben Auskunft über die zugewiesenen Profile, aufgetretenen Alarme, besonders häufig betroffene Clients oder die Aktualität der Virensignaturen.

Um Rechenschaft über den Zustand des Virenschutzes abzulegen, können IT-Verantwortliche eigene Reports für das Defender Management generieren. Die Erstellung der Berichte erfolgt mit Hilfe eines Wizards, der diese Aufgabe erleichtert.

The wizard guides the user through the process of creating a report. The current step is 'Angezeigte Felder auswählen' (Select displayed fields). The user can search for fields and select them for inclusion in the report. The selected field is 'Defender Ereignis Gelesen Status'.

Das Erstellen eines neuen Reports fällt dank der Wizard-Unterstützung sehr einfach

Zusammenfassung

Die Aagon GmbH bietet mit Defender Management eine zentrale Verwaltung des Windows-eigenen Malware-Schutzes, der in eine umfassende Client-Management-Lösung eingebettet ist und von der es auf vielfältige Weise profitiert.

Selbst in der Minimalausstattung, die zusätzlich nur ACMP Core umfasst, steht dem Defender Management die gesamte Infrastruktur der Lösung zur Verfügung, darunter anpassbare Dashboards, ein Berichtswesen inklusive Wizard, Benachrichtigungen über kritische Ereignisse oder ein vielseitig nutzbares Inventory.

Das Konzept des Defender-Managements beruht im Wesentlichen auf Konfigurationsprofilen, die sich über dynamische Gruppen anhand zahlreicher Kriterien sehr flexibel an Endgeräte zuweisen lassen. Insgesamt erhalten Admins damit ein leicht verständliches Werkzeug, dessen Fähigkeiten weit über jene der Bordmittel hinausgehen.

Interessenten können eine [kostenlose Testversion](#) über die Website des Herstellers anfordern.



ÜBER AAGON

„Manage any device in a connected world!“ – Aagon entwickelt seit 30 Jahren Client-Management- und -Automation-Lösungen und ist der Spezialist für die Verwaltung von Endgeräten und die Automatisierung von Standardaufgaben. Durch sorgfältige Entwicklungen, mehr als 20 Jahre Marktreife und die enge Zusammenarbeit mit unseren Kunden und Partnern sind unsere Produkte perfekt auf Ihre Anforderungen und Bedürfnisse zugeschnitten.

Individuelle Beratung und die beste Unterstützung von Kunden und Partnern bei der Installation und ersten Einrichtung gehören deshalb zum Standard von Aagon. Ein umfassendes Verständnis von Kundenbedürfnissen und der ständige Kontakt zu unseren Kunden und Partnern ermöglichen Softwareentwicklung auf Augenhöhe.

Webinare-on-Demand, zahlreiche Whitepaper und die beliebten Treffen zum Anwendertreffen an Standorten in ganz Deutschland sind nur drei Beispiele, wie nahe am Kunden ACMP wirklich entwickelt wird.

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

EIN PRODUKT DER

Aagon GmbH

Lange Wende 33

D-59494 Soest

Fon: +49 (0)2921 - 789200

Fax: +49 (0)2921 - 789244

sales@aagon.com

www.aagon.com

