DriveLock Application Control

Dokumentation 2021.2

DriveLock SE 2021

Inhaltsverzeichnis

1 DriveLock Applikationskontrolle

1.1 Lizenzierungsmodell DriveLock Application Control

DriveLock bietet verschiedene Lizenzen mit einem unterschiedlichen Leistungsspektrum an.

Wenn Sie eine EDR-Lizenz haben, steht Ihnen ein Teil der Application Control-Funktionalität zur Verfügung, die Sie zur Erkennung von Angriffen verwenden können.

	Application Control (Legacy)	Application Control	Application Behavior Control (ABC)	EDR
White-/Blacklisting von Anwendungen	ja	ja	-	-
Datei-Eigenschaften-Regel	ja	ja	-	-
Hash-Datenbank-Regel	ja	ja	-	-
Spezielle Regel	ja	ja	-	-
White-/Blacklisting von DLLs	-	ja	-	-
White-/Blacklisting von Skripten	-	ja	-	-
Lokale Whitelist	-	ja	-	-
Predictive Whitelisting	-	ja	-	-
Anwendungslisten	-	ja	ja	ja

Lokales Lernen	-	ja	ja	-
Anwendungs-Verhaltensregeln	-	-	ja	Reporting
• Dateizugriffe	-	-	ja	Reporting
• Registryzugriffe	-	-	ja	Reporting
• Skriptausführung	-	-	ja	Reporting
• Starten von Anwendungen	-	-	ja	Reporting
• Laden von DLLs	-	-	ja	Reporting
Verhaltensaufzeichnung	-	-	ja	-

Hinweis: Die klassische Anwendungskontrolle (Legacy) ist nicht kombinierbar. Sowohl die Anwendungskontrolle mit Maschinenlernfunktion (Application Control) als auch die Anwendungsverhaltenskontrolle können einzeln eingesetzt oder kombiniert werden.

1.2 Funktionsumfang

Setzen Sie DriveLock Application Control ein, um die Verwendung von Anwendungen auf Ihren Unternehmensrechnern gezielt einzuschränken oder zu erlauben.

Hinweis: Beachten Sie bitte, dass die Applikationskontrolle nicht automatisch zum Standardumfang von DriveLock gehört. Wenn Sie keine Lizenz dafür eingetragen haben, erscheint dieser Knoten nicht in Ihrer DriveLock Management Konsole. Je nach Lizenz stehen manche Funktionalitäten, wie z.B. Anwendungs-Verhaltenskontrolle nicht zur Verfügung.

Die DriveLock Applikationskontrolle beinhaltet verschiedene Funktionalitäten:

- Anwendungsregeln: Mithilfe von Black- und/oder Whitelisting können Sie einfache Regeln festlegen, welche Anwendungen ausgeführt und welche gesperrt werden. Somit kann die Ausführung jeder beliebiger Anwendung auf Computern kontrolliert werden, auf denen DriveLock installiert ist. Diese Freigabe oder Sperre kann anhand verschiedener Kriterien definiert werden.
- Anwendungs-Verhaltensregeln: Konfigurieren Sie, was die von Ihnen erlaubten Anwendungen dürfen, d.h. Sie bestimmen beispielsweise, welche Berechtigungen die Anwendungen erhalten, in welche Verzeichnisse Anwendungen schreiben oder welche Prozesse diese starten dürfen. Durch Aufzeichnen des Anwendungsverhaltens über die Agenten-Fernkontrolle können automatisch Anwendungs-Verhaltensregeln erzeugt werden.
- Lokales Lernen: Zusätzlich zu den in Richtlinien definierten Regeln kann auch auf dem DriveLock Agenten selbst gelernt werden, was durch die Applikationskontrolle zugelassen wird.

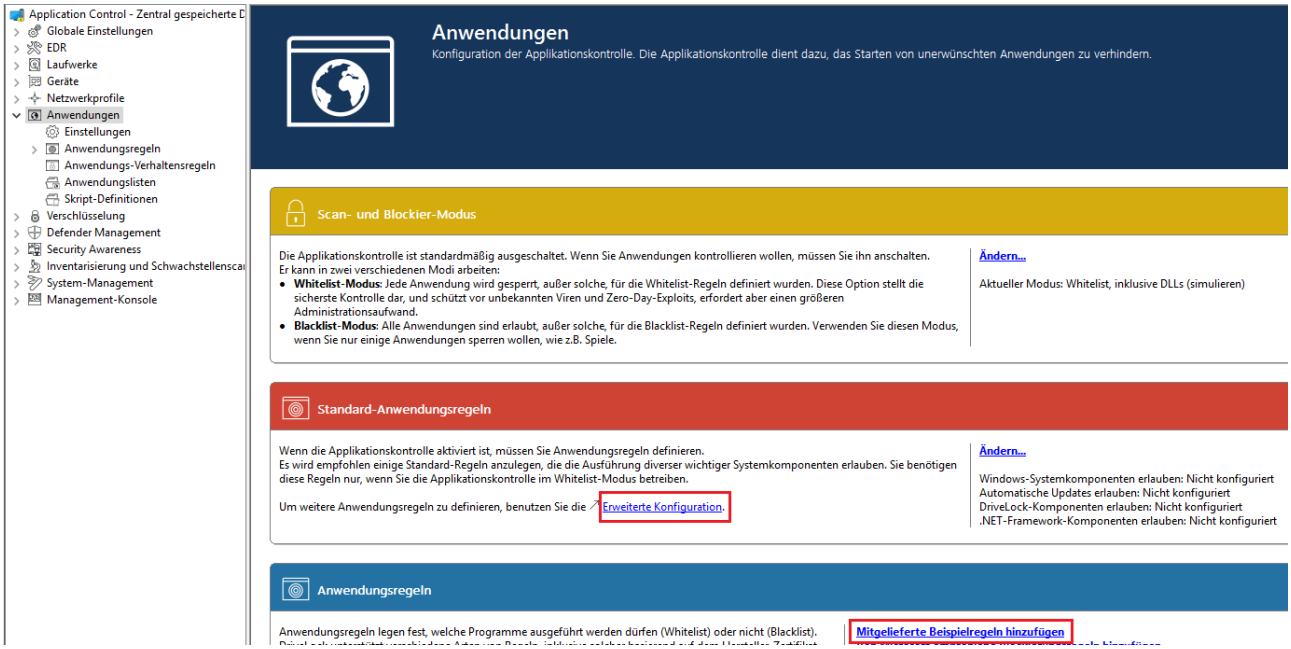
2 Übersicht in der DriveLock Management Konsole

In der Taskpad-Ansicht des Knotens **Anwendungen** lassen sich grundlegende Einstellungen für die Applikationskontrolle konfigurieren. Aus dieser Übersicht heraus können Sie schnell den Scan- und Blockiermodus einstellen, Standard-Anwendungsregeln (vier Spezialregeln) sowie weitere Anwendungsregeln, Anwendungs-Verhaltensregeln, Anwendungslisten und Skript-Definitionen konfigurieren.

Zusätzlich werden Ihnen mitgelieferte Beispiele für Regeln angeboten, die bereits voreingestellt sind und sinnvolle Szenarien abbilden. Wenn Sie die Option **Von Microsoft empfohlene Blockierungsregeln hinzufügen** bzw. **Sonstige Blockierungsregeln hinzufügen** auswählen, wird ein neuer Ordner **Empfohlene Blockierungregeln** angelegt, der diese Blacklist-Regeln enthält.

Wenn Sie Änderungen vornehmen, beispielsweise den **Scan- und Blockier-Modus** ändern, wird dies farblich angezeigt (z.B. grün, wenn als aktueller Modus Whitelist aktiviert ist).

Die einzelnen Einstellungen lassen sich auch auf der linken Seite in der DriveLock Management Konsole auswählen. Durch Klicken auf **Erweiterte Konfiguration** gelangen Sie in den jeweiligen Unterknoten.



3 Einstellungen

Folgende Einstellungen lassen sich für die DriveLock Applikationskontrolle setzen:

1. Allgemeine Einstellungen:
   - Scan- und Blockiermodus
   - Hash-Algorithmus für Hash-basierte Regeln einstellen
   - Anwendungsausführung immer protokollieren
   - Angepasste Benutzer-Benachrichtigung erstellen
2. Einstellungen für die Fehlersuche (Treibereinstellungen)

   Hinweis: Wir empfehlen, diese Einstellungen nur in Zusammenarbeit mit dem DriveLock Support zu verwenden.

   - Anwendungskontroll-Cache
   - Cache-Lebensdauer ("Time-to-live")
   - Pfade ohne Hash-Erzeugung für ausgeführte Anwendungen
3. Einstellung für vertrauenswürdige Prozesse
4. Lokale Whitelist aktivieren:
   - Lokale Whitelist und Predictive Whitelisting
5. Einstellungen für lokales Lernen:
   - Verzeichnisse, die für die lokale Whitelist gelernt werden
   - Zusätzliche Erweiterungen, die für die lokale Whitelist gelernt werden
   - Lokale Whitelist zum DriveLock Enterprise Service hochladen
   - Lernen der lokalen Whitelist automatisch starten
6. Einstellungen für die Verhaltenskontrolle
   - Dauer der Lernphase für die Anwendungs-Verhaltenskontrolle
   - Benutzer bei ungewöhnlichem Anwendungsverhalten fragen

Hinweis: Die Verwendung von bedingten Einstellungen (Konfigurationsfilter) ist auch in der Applikationskontrolle möglich. Weitere Informationen finden Sie im entsprechende Kapitel des Administationshandbuchs unter DriveLock Online Help.

3.1 Scan- und Blockiermodus

Wenn ausführbare Programme gescannt/geblockt werden, prüft DriveLock die Datei während sie vom Windows-Betriebssystem in den Speicher geladen wird. Abhängig vom Ergebnis der Prüfung und den konfigurierten Regeln in der DriveLock Richtlinie erlaubt oder verweigert DriveLock die Programmausführung.

Scannen/Blockieren von DLLs funktioniert im Prinzip genauso. Wenn Programme DLLs laden, werden alle diese DLLs während des Ladens geprüft.

> Achtung: Wenn Sie planen, die Applikationskontrolle im Whitelist-Modus inklusive DLLs zu aktivieren, müssen Sie sicherstellen dass Sie keine DLLs blockieren, die für ein vollständiges Funktionieren ihres Systems erforderlich sind.

Windows installiert viele DLLs, die weder als Teil des Betriebssystems noch des .NET Frameworks markiert sind. Manche dieser DLLs sind auch nicht im Windows Systemverzeichnis installiert und manche haben nicht einmal eine (gültige) Microsoft Signatur. Deshalb werden solche DLLs von keiner der Spezial-Regeln erfasst.

Beispiel:

Standardmäßig wird von manchen Windows Versionen Microsoft OneDrive mit installiert. OneDrive wird im Benutzerprofil installiert und ist nicht Teil des Betriebssystems. Leider lädt der Windows Explorer OneDrive DLLs nach. Der Windows Explorer wird jedoch beendet, wenn diese DLLs nicht in ihren Regeln gewhitelistet sind.

Bewährte Praxis:

Wir empfehlen, Predictive Whitelisting bzw. die lokale Whitelist zu aktivieren, bevor Sie Blockieren von DLLs einschalten. In jedem Fall sollten Sie im Simulationsmodus beginnen und die Ereignisse der Applikationskontrolle auswerten, um so alle vom System benötigten DLLs zu whitelisten.

3.1.1 Simulation

Bevor Sie wirklich mit der Sperrung von Programmen beginnen, sollten Sie einen der beiden Simulations-Modi (Whitelist (simulieren) oder Blacklist (simulieren)) verwenden, um die Auswirkungen Ihrer Regeln vorab zu testen. Während einer Simulation erzeugt DriveLock entsprechend den Regeln Ereignismeldungen für gestartete oder blockierte Anwendungen, die Ausführung selbst wird dabei aber noch nicht verhindert.

Der Simulationsmodus kann sehr hilfreich dabei sein, um zu ermitteln, welche Anwendungen gesperrt worden wären. Verwenden Sie zur Analyse die Windows Ereignisanzeige

oder untersuchen Sie die Daten mit Hilfe des DriveLock Operations (DOC) oder Control Centers (DCC) auf einfache Art und Weise, um entsprechende Ereignisse schnell zu finden.

3.1.2 Whitelist oder Blacklist

Um die Applikationskontrolle vollständig zu aktivieren, wählen Sie Whitelist oder Blacklist aus der Dropdown-Liste aus.

Wenn Sie Whitelist selektieren, werden grundsätzlich alle Anwendungen gesperrt, sofern es nicht eine passende Anwendungsregel dafür gibt, die diese Sperrung aufhebt.

Bei Blacklist hingegen wird zunächst keine Anwendung an der Ausführung gehindert, es sei denn es existiert eine entsprechende Regel, die diese verbietet.

3.1.2.1 Whitelist-Modus

Im Whitelist-Modus sind alle Anwendungen erlaubt, zu der es eine passende Whitelist-Regel gibt. Mit Hilfe von Blacklist-Regeln können Sie in diesem Fall einzelne Anwendungen als Ausnahme einer bestehenden Whitelist-Regel oder einer Vorlage sperren.

Priorisierung: Blacklist-Regel – Whitelist-Regel – andere Einstellungen

Beispiel: Da in der Regel kein Benutzer außer einem Administrator für das Verzeichnis “C:\Programme” Schreibzugriff hat, ist es denkbar, dass Sie eine Verzeichnisregel für diesen Ordner als Whitelist-Regel erstellen und somit alle Anwendungen, die von dort aus aufgerufen werden (d.h. bereits dort installiert sind), zugelassen sind. Müssen Sie nun aber z.B. für einzelne Computer eine ganz bestimmte Anwendung sperren, reicht bei DriveLock eine einzelne zusätzliche Blacklist-Regel für genau diese Anwendung, um dieses Ziel zu erreichen.

3.1.2.2 Blacklist-Modus

Im Blacklist-Modus werden die Blacklist-Regeln (bzw. auch die Blacklist-Vorlage) verwendet, um diejenigen Applikationen festzulegen, deren Ausführung verhindert werden soll. In diesem Fall können nun wiederum Whitelist-Regeln eingesetzt werden, um Ausnahmen von der Sperrung zu definieren.

Priorisierung: Whitelist-Regel – Blacklist-Regel – andere Einstellungen

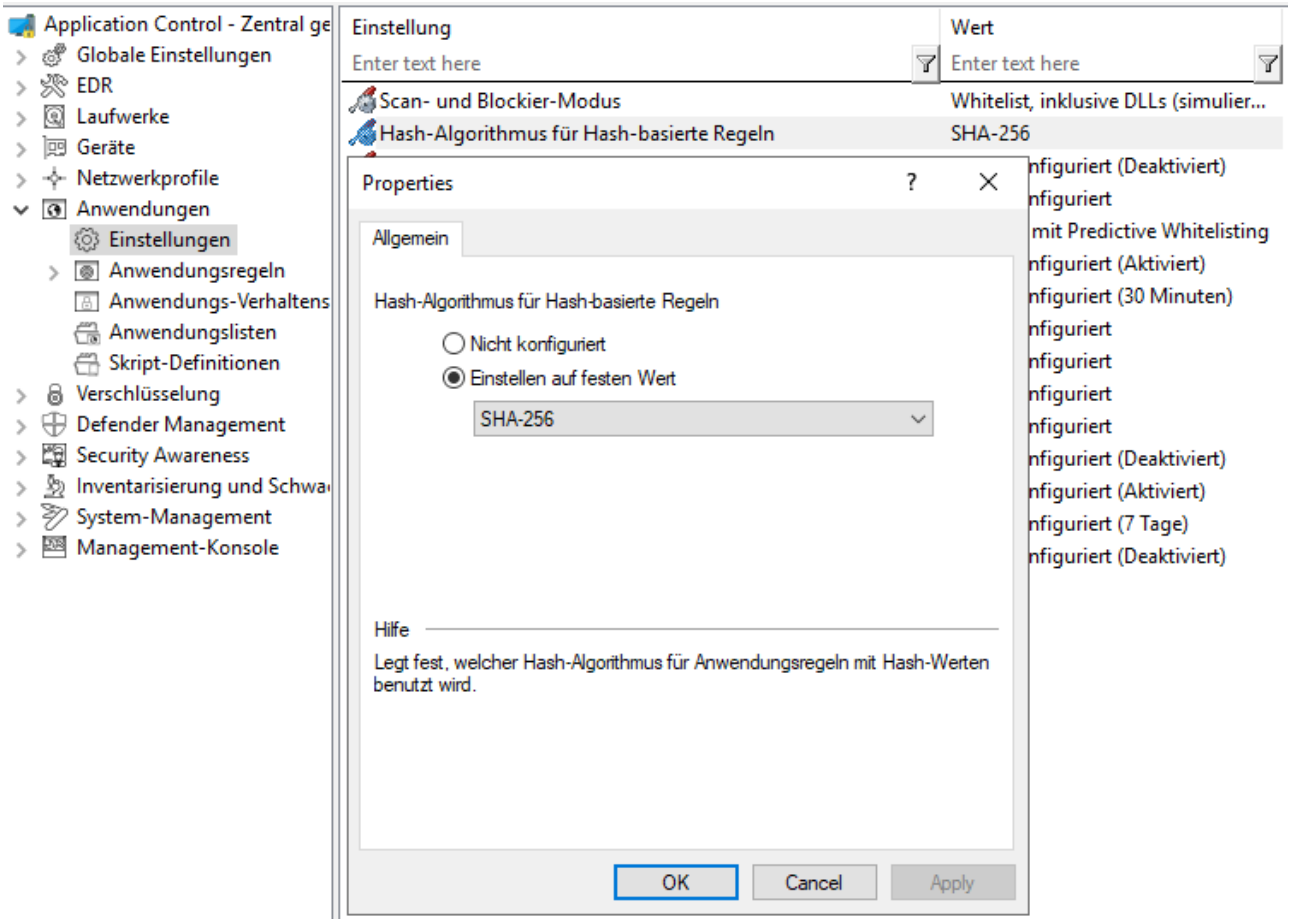
Beispiel: Innerhalb Ihres Unternehmensnetzwerkes ist es nicht erlaubt, das Programm “Skype” zu verwenden, eine entsprechende Blacklist-Regel existiert. Allerdings möchte Ihr Geschäftsführer es benutzen, während er unterwegs und außerhalb des Büros ist. Mit Hilfe einer einzelnen Whitelist-Regel, die für Ihren Geschäftsführer gilt, können Sie ihm die Verwendung auf einfache Art und Weise ermöglichen.

3.2 Hash-Algorithmus für Hash-basierte Regeln einstellen

Mit dieser Einstellung geben Sie ein fest eingestelltes Hash-Verfahren für alle Regeln an. Der eingestellte Wert bestimmt den Hash, der bei Prüfung einer Datei berechnet wird.

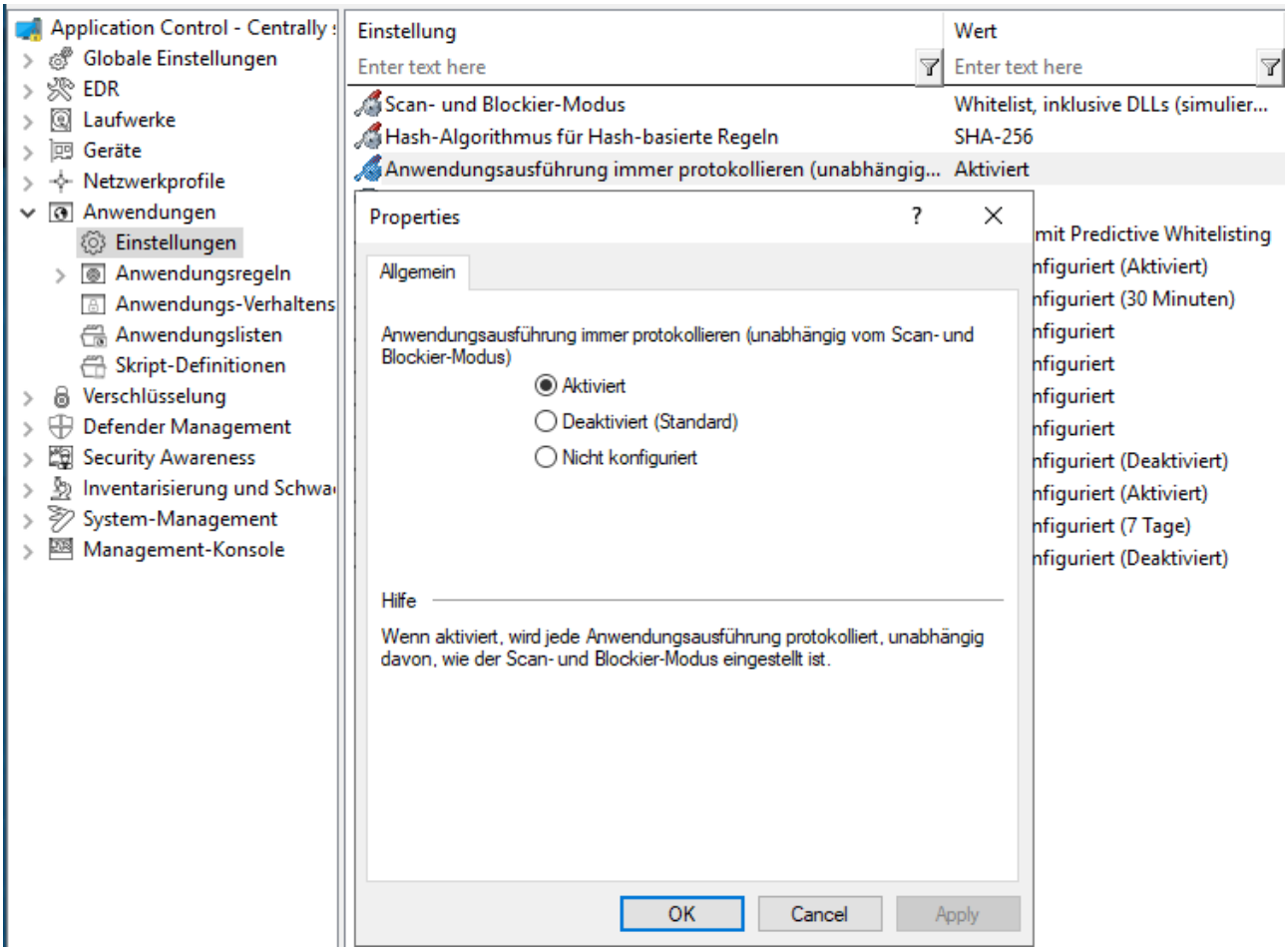
> Achtung: Beachten Sie, dass dieser Wert mit dem in den Anwendungsregeln verwendeten Hash-Algorithmus übereinstimmt. Sollten Sie das Hash-Verfahren im Nachhinein ändern, müssen Sie auch die Regeln entsprechend anpassen.

Das im Beispiel verwendete Hash-Verfahren SHA-256 ist empfehlenswert.



3.3 Anwendungsausführung immer protokollieren

Um unabhängig vom ausgewählten Betriebsmodus Informationen über gestartete Programme als Ereignis zu generieren, klicken Sie auf **Anwendungsausführung immer protokollieren (unabhängig vom Scan- und Blockier-Modus)** und wählen Sie die Option **Aktiviert** aus.



Hinweis: Die Protokollierung jedes erfolgreichen Programmstarts, kann die Performance des Computers verringern. Wenn die Ereignisse zum DriveLock Enterprise Service gesendet werden, erhöht es auch die Netzwerklast und die Datenbankgröße.

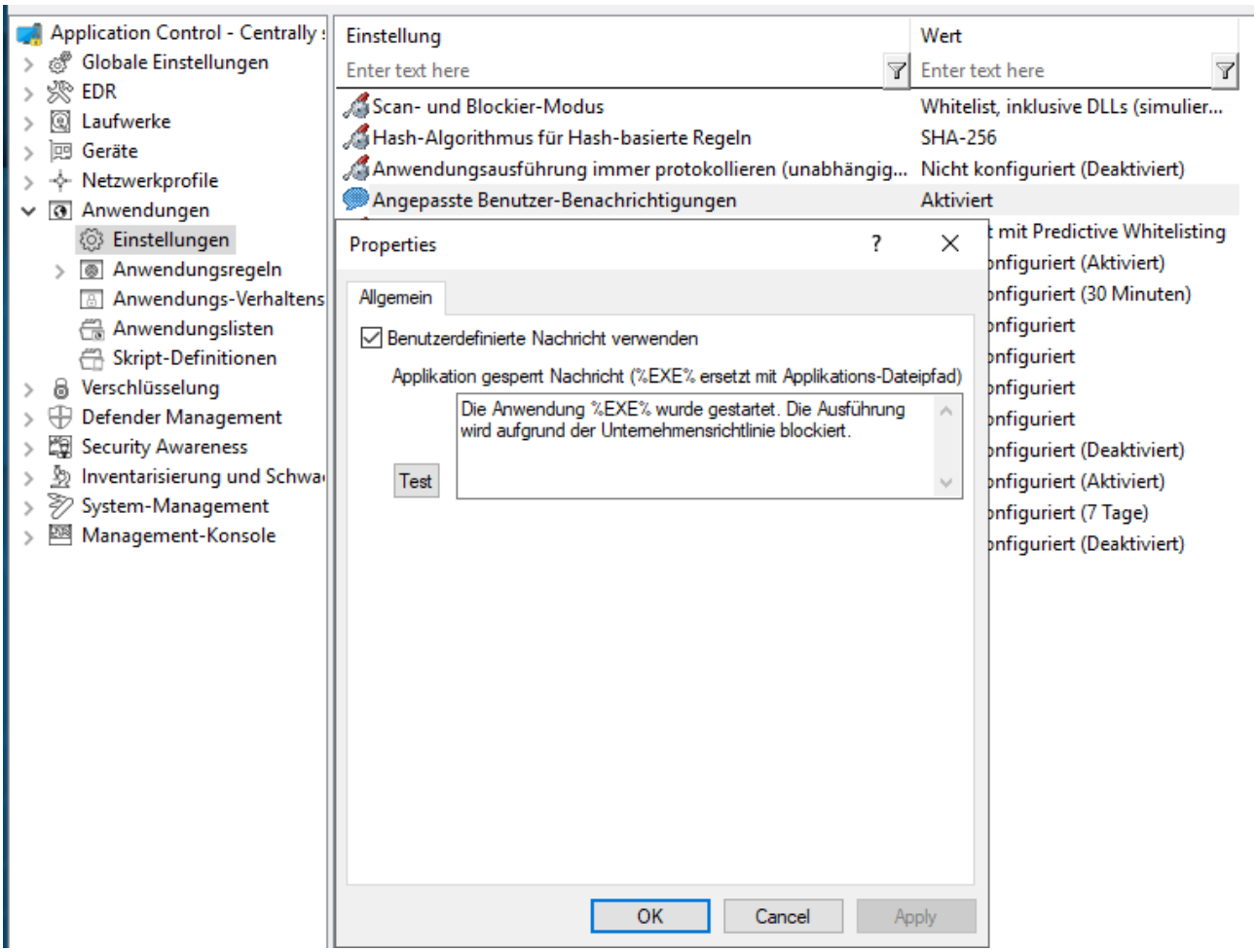
3.4 Angepasste Benutzer-Benachrichtigung erstellen

Klicken Sie auf **Angepasste Benutzer-Benachrichtigungen**, um eigene Meldungen zu konfigurieren, welche einem Benutzer bei einer Programmsperrung angezeigt werden.

Wenn Sie mehrsprachige Benutzermeldungen konfiguriert haben, zeigt DriveLock an Stelle dieser Meldungen die Standardmeldungen in der aktuellen Sprache an.

Aktivieren Sie dazu **Benutzerdefinierte Nachricht verwenden** und geben Sie den gewünschten Text ein. Damit der Anwender auch über den Namen der Applikation, die gesperrt wurde, informiert wird, können Sie die Variable `%EXE%` innerhalb der Meldung verwenden. Diese wird zur Laufzeit durch den Pfad und den Dateinamen ersetzt.

Klicken Sie auf Test, um die Meldung vorab anzuzeigen.



3.5 Vertrauenswürdiger Prozess

Diese Einstellung kann gesetzt werden, wenn Sie eine Client-Management-Software für die Software-Verteilung in Ihrem Unternehmen einsetzen. Auf dem Reiter Lokales Lernen in einigen Anwendungs- und Anwendungslisten-Regeln können Sie außerdem angeben, ob diese Client-Management-Software besondere Berechtigungen erhält (z.B. ob sie andere Programme starten darf, die nicht auf der Whitelist sind) und deshalb als vertrauenswürdig gilt.

Folgende Konfigurationsoptionen stehen zur Verfügung:

1. **Nicht konfiguriert**: Standardoption
2. **Einstellen auf feste Liste**:
   Fügen Sie den Namen der Software hinzu. Diese Software wird dann beim Start des DriveLock Enterprise Service überprüft.

3.6 Lokale Whitelist und Predictive Whitelisting

Mit dieser zentralen Einstellung aktivieren oder deaktivieren Sie die Verwendung der lokalen Whitelist.

Folgende Konfigurationsoptionen stehen zur Verfügung:

1. **Lokale Whitelist aktivieren**:
   Sobald die Richtlinie mit dieser Einstellung dem Agenten zugewiesen ist, startet der DriveLock Agent den Lernmodus und aktiviert danach die lokale Whitelist mit den gelernten Anwendungen.

2. **Predictive Whitelist aktivieren** in Zusammenhang mit **Vorhersagen basierend auf Publisher-Zertifikaten**:
   Diese Option bietet vor allem bei Update-Prozessen folgenden Automatismus: Dateien werden dann automatisch der lokalen Whitelist hinzugefügt, wenn sie entweder die gleiche Produktbeschreibung haben oder von einem ähnlichen Zertifikat signiert sind, wie die Zertifikate der in der lokalen Whitelist gelernten Dateien.
   Wenn Sie schnell und ohne viel Aufwand Update-Prozesse (z.B. von Browsern) zulassen wollen, können Sie diese Option auswählen. Die Erstellung von exakt definierten Regeln zur Aktualisierung von Anwendungen über das lokale Lernen (z.B. mithilfe von Aufzeichnung des Lernverhaltens, Verwendung der Aufzeichnungsergebnisse in Anwendungs-Verhaltensregeln oder der genauen Angabe der Berechtigungen) ist zwar zeitaufwändiger, aber Sie erzielen dadurch ein zuverlässigeres Ergebnis.

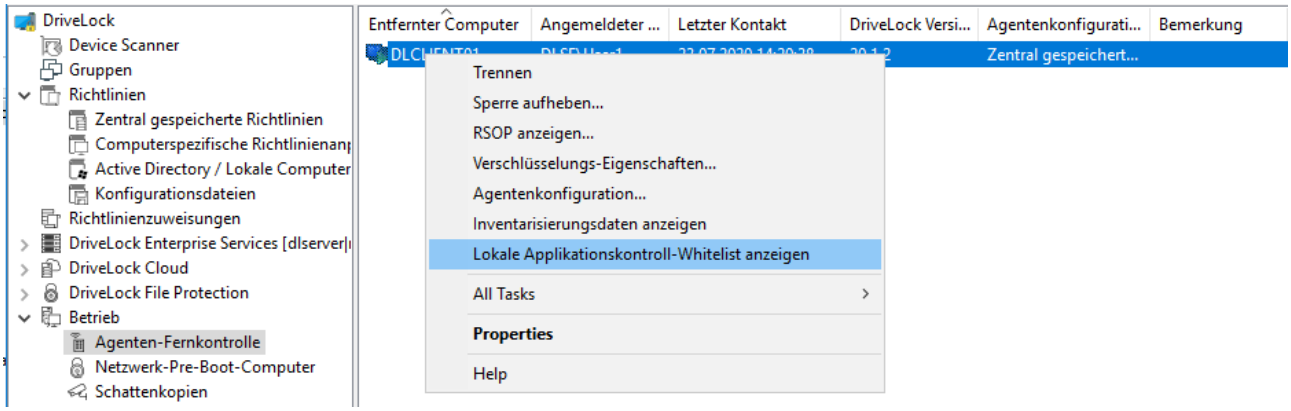
3.6.1 Lokale Whitelist über die Agenten-Fernkontrolle anzeigen

Wenn Sie die Applikationskontrolle in Verbindung mit lokalem Lernen verwenden, wird auf dem DriveLock Agenten eine Datenbank mit den für diesen Computer freigegebenen Anwendungen angelegt (lokale Whitelist). Sie können sich mit einem Agenten verbinden und den Inhalt dieser Datenbank anzeigen bzw. einzelne Einträge löschen.

Applikationskontroll-Whitelist anzeigen:

1. Öffnen Sie in der DriveLock Management Konsole den Knoten **Betrieb** und **Agenten-Fernkontrolle**.

2. Wählen Sie im Kontextmenü des betreffenden DriveLock Agenten den Menübefehl **Lokale Applikationskontroll-Whitelist anzeigen**.



Um einzelne Einträge zu löschen, beispielsweise weil zu viele Applikationen gelernt wurden, gehen Sie folgendermaßen vor:

1. Doppelklicken Sie den betreffenden Agenten, um sich die Eigenschaften anzeigen zu lassen.
2. Wählen Sie auf dem Reiter **Applikationskontrolle** die Schaltfläche **Anzeigen...**
3. Es öffnet sich ein Fenster mit einer Windows Explorer ähnlichen Struktur. Das Öffnen selbst kann je nach Datenbankgröße etwas dauern.
4. Hier sehen Sie die gelernten Applikationen. Wählen Sie den Eintrag aus, den Sie löschen wollen.

Hinweis: Weitere Informationen zur Agenten-Fernkontrolle finden Sie im Administrationshandbuch auf DriveLock Online Help.

3.6.2 Lokales Lernen

Die DriveLock Applikationskontrolle stellt eine Lernfunktionalität zur Verfügung, mit der das Verhalten von Applikationen auf DriveLock Agenten gelernt werden kann.

Dazu wird der Client-Computer in den Lernmodus versetzt und eine lokale Whitelist (Hash-Datenbank) der installierten Programme und DLLs erstellt. Diese individuelle lokale Whitelist enthält dann die lokal gelernten zugelassenen Dateien. Sobald der Lernmodus abgeschlossen ist, wird die lokale Whitelist aktiviert und es können nur noch die "gelernten" Programme ausgeführt werden. Damit Programme, die zu einem späteren Zeitpunkt installiert oder aktualisiert werden, von der Applikationskontrolle nicht blockiert werden, kann der Lernmodus für die Installation bzw. Aktualisierung vorübergehend wieder eingeschaltet werden.

Die Verwendung der lokalen Whitelist wird durch die Einstellung Lokale Whitelist und Predictive Whitelisting oder durch Erstellung einer Predictive-Whitelisting-Regel aktiviert.

Das lokale Lernen wird ausgelöst

- durch Setzen der entsprechenden Lerneinstellungen in einer Anwendungslisten-Regel oder
- durch Verwendung einer Anwendungs-Verhaltensregel, die aus einer Verhaltensaufzeichnung automatisch erstellt wurde.

Wenn die lokale Whitelist aktiviert ist, können Sie zusätzliche Einstellungen zur Konfiguration der Lernfunktionalität setzen.

Die lokale Whitelist wird inkrementell zur Anwendungsdatenbank am DriveLock Enterprise Service (DES) gemischt. Wenn Sie Datei-Eigenschaften-Regeln erstellen, können Sie auch aus dieser globalen Anwendungsdatenbank auswählen.

3.6.2.1 Verhaltensaufzeichnung und Verhaltenskontrolle

Es gibt zwei Möglichkeiten die Anwendungs-Verhaltenskontrolle teilweise oder vollständig zu automatisieren.

1. Verwendung eines Referenzcomputers
   Mithilfe einer Verhaltensaufzeichnung können Sie ohne großen Aufwand Hintergrundaktionen, beispielsweise bestimmte Zugriffe von Applikationen, ausgeführte Programme oder geschriebenen Dateien, nachvollziehen und lernen und die Ergebnisse anschließend in einer Datei speichern lassen.
   - Aktivieren Sie auf einem Referenzcomputer über die Agenten-Fernkontrolle die Verhaltensaufzeichnung für eine oder mehrere Applikationen.
   - Anschließend wird mit diesen Applikationen gearbeitet, wobei darauf zu achten ist, dass alle wichtigen Aktionen durchgeführt werden, insbesondere auch Updates und Konfigurationsänderungen. Hierbei wird das Verhalten der Applikationen aufgezeichnet, z.B. welche Dateien geschrieben und welche anderen Programme gestartet werden.
   - Anschließend können aus den aufgezeichneten Daten Anwendungs-Verhaltensregeln generiert werden.
2. Automatisches Lernen auf jedem einzelnen DriveLock Agenten
   - In einer Anwendungslisten-Regel kann angegeben werden, dass das Verhalten einer Applikation auf das eingeschränkt werden soll, was während einer Lernphase gelernt wird. Dabei werden nur die Zugriffsmodi Ausführen, DLL laden und Datei schreiben unterstützt.

- Während einer Lernphase wird gelernt, wie sich die Anwendung verhält und nach Abschluss der Lernphase wird davon abweichendes Verhalten geblockt.

3.6.2.1.1 Verhaltensaufzeichnung konfigurieren

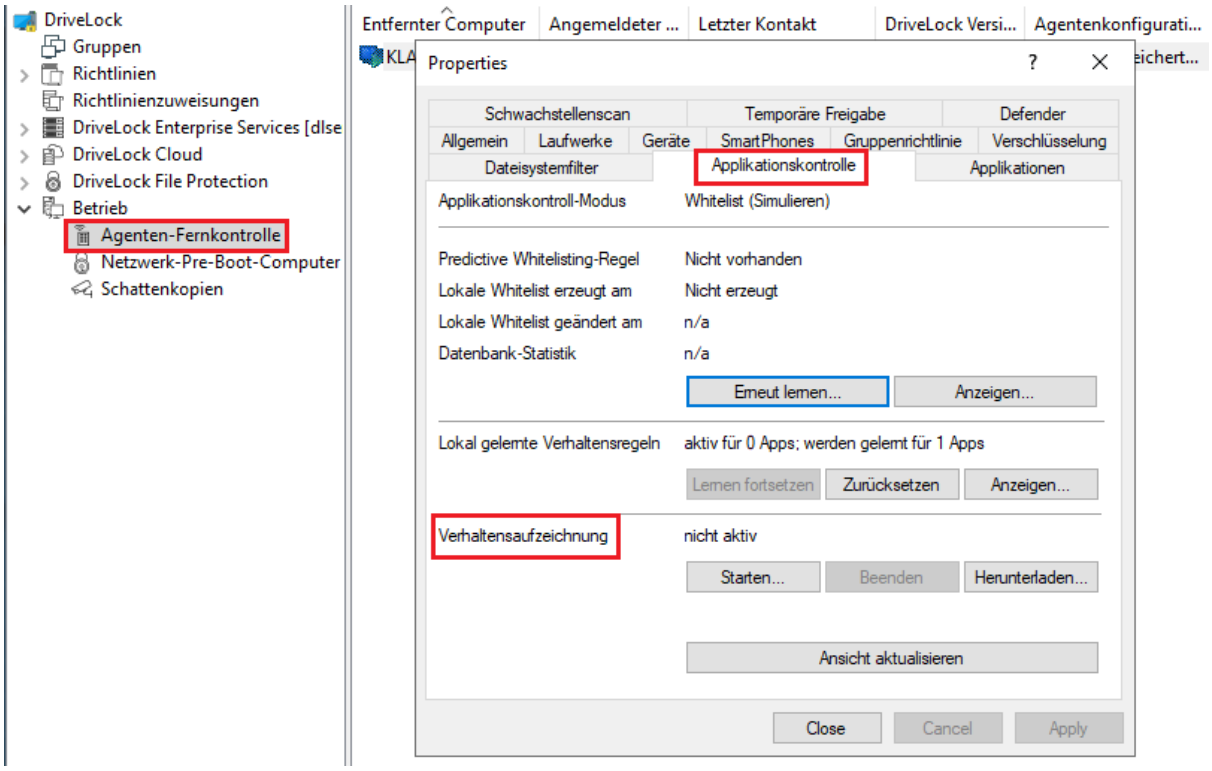
Starten Sie eine Verhaltensaufzeichnung, um herauszufinden, wie sich eine Applikation verhält.

Hinweis: Für die Applikation muss eine entsprechende Whitelist-Regel vorhanden sein.

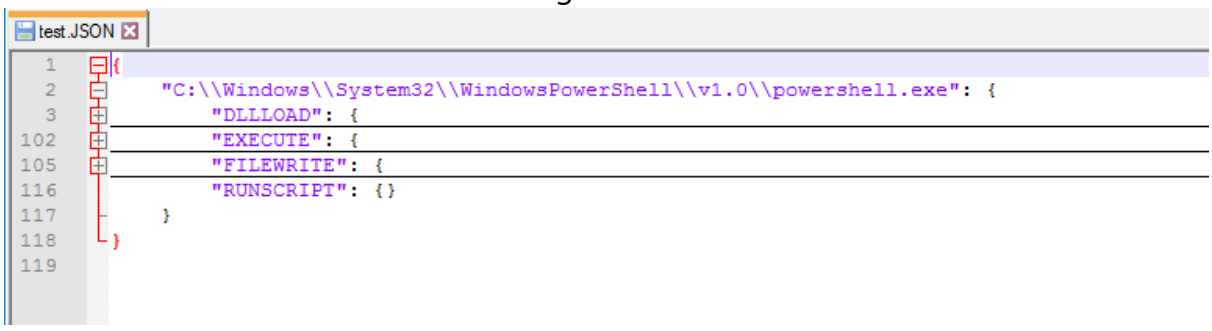
Die gespeicherte Verhaltensaufzeichnung können Sie im Anschluss dazu verwenden, Verhaltensregelen erzeugen zu lassen, die sich exakt auf das gelernte Verhalten beschränken. So wird nur das Verhalten zugelassen, das tatsächlich benötigt wird, alles andere wird geblockt.

Gehen Sie folgendermaßen vor:

1. Öffnen Sie in der DriveLock Management Konsole den Knoten **Betrieb** und **Agenten-Fernkontrolle**.
2. Doppelklicken Sie den betreffenden Agenten, um sich die Eigenschaften anzeigen zu lassen.
3. Wählen Sie auf dem Reiter **Applikationskontrolle** unter **Verhaltensaufzeichnung** die Schaltfläche **Starten...**.
4. Fügen Sie Verzeichnisse oder Programme hinzu, deren Verhalten Sie aufzeichnen wollen.
5. Wählen Sie aus, welche Art von Zugriffen aufgezeichnet werden sollen, Beispiel s. Abbildung.



6. Wenn Sie einen bereits existierende Aufzeichnung löschen wollen, setzen Sie das entsprechende Häkchen.
7. Die Aufzeichnung sollte auf einen beistimmten Zeitraum limitiert werden. Maximal können Sie hier 10 Tage eingeben, es empfiehlt sich aber ein deutlich kürzerer Zeitraum.
8. Nachdem Sie die Anwendung beispielsweise auf einem Referenzcomputer über einen bestimmten Zeitraum getestet und so ausreichend Daten gesammelt haben, klicken Sie die Schaltfläche **Herunterladen...**, um die Aufzeichnung des Verhaltens in einer JSON-Datei herunterzuladen und die Ergebnisse auswerten zu können.



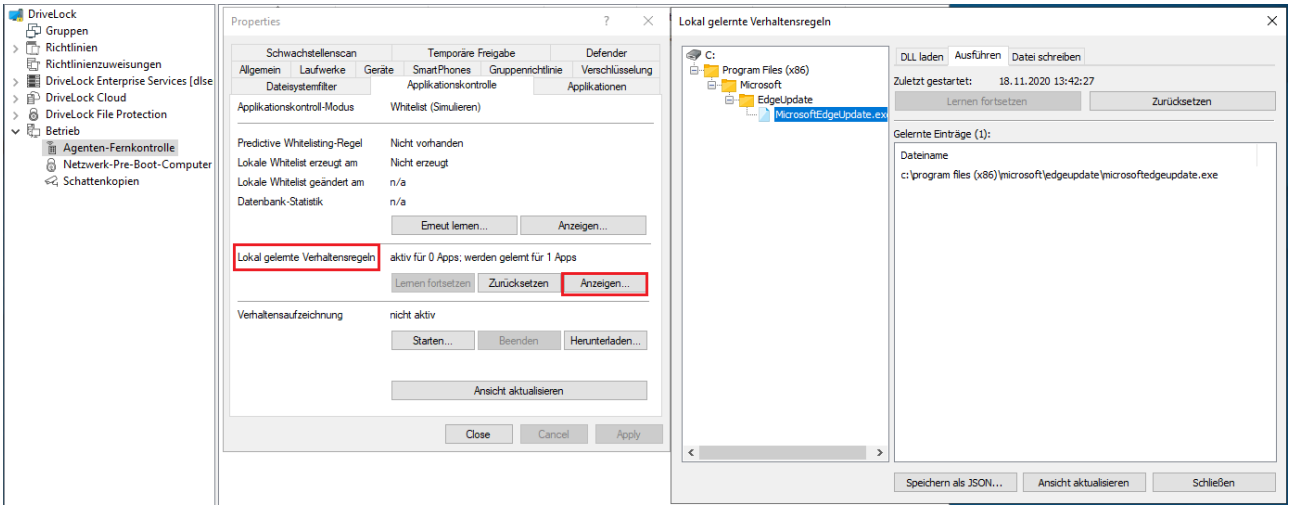
9. Sie können nun diese Ergebnisdatei in einer Verhaltensregel verwenden.

3.6.2.1.2 Lokal gelernte Anwendungs-Verhaltensregeln

Die Anzeige unter **Lokal gelernte Anwendungs-Verhaltensregeln** basiert auf den Einstellungen, die Sie in den Anwendungslisten-Regeln auf dem Reiter **Lokales Lernen** gesetzt haben. Sobald ein Agent eine Richtlinie mit diesen Einstellungen verwendet, wird eine Lernphase gestartet und aktiviert somit die Anwendungs-Verhaltenskontrolle. Die Lernphase für die drei Modi (DLL laden, Ausführen, Dateien schreiben) sind unabhängig voneinander.

Folgende Zustände und Schaltflächen sind verfügbar:

- **nicht aktiv**: Es sind noch keine Anwendungen angegeben, die gelernt oder kontrolliert werden müssten.
- **aktiv für**: Die angegebene Anzahl an Applikationen wird geblockt, wenn ein Verhalten auftritt, das nicht gelernt worden ist.
- **werden gelernt für**: Die Applikationen befinden sich noch in der Lernphase.
- **Lernen fortsetzen**: Der Startzeitpunkt der Lernphase wird neu gesetzt, die bereits gelernte Liste wird weitergeführt.
- **Zurücksetzen**: Die bereits gelernte Liste wird gelöscht. Die Aktivitätsanzeige geht zurück auf **nicht aktiv**.
- **Anzeigen...**: Durch Klicken auf diese Schaltfläche öffnet sich ein Dialog, in dem die gelernten Einträge angezeigt werden, siehe Abbildung.
  Wenn Sie das Ergebnis in einer JSON-Datei speichern, können Sie diese verwenden, um daraus Anwendungs-Verhaltensregeln erzeugen zu lassen. Gehen Sie dazu so vor, wie in Kapitel Anwendungs-Verhaltensregeln aus der Verhaltensaufzeichnung erzeugen beschrieben.



3.7 Einstellungen für lokales Lernen

Folgende Einstellungen können im Zusammenhang mit lokalem Lernen konfiguriert werden:

Einstellung	Konfigurationsoptionen
Lokale Whitelist zum DriveLock Enterprise Service hochladen	Nach Erstellung können Sie die lokale Whitelist an den DriveLock Enterprise Service (DES) schicken lassen, der eine Liste mit allen lokal gelernten Dateien pflegt. Diese Liste kann dann zur Erzeugung von Hash-Regeln verwendet werden. Die Standardoption ist **Deaktiviert**.
Lernen der lokalen Whitelist automatisch starten	Mit dieser Einstellung können Sie festlegen, ob das Lernen der lokalen Whitelist automatisch (d.h. sobald die entsprechende Richtlinie dem DriveLock Agenten zugewiesen ist) oder von Benutzern gestartet wird. Die Standardoption ist **Aktiviert**. Wählen Sie **Deaktiviert**, wenn mit dem Lernen gewartet werden soll, bis ein Benutzer dieses aktiv startet. Das initiale Lernen der lokalen Whitelist ist somit dem Benutzer überlassen. Sie können die Einstellungen der Agenten-Benutzeroberfläche dahingehend konfigurieren. Wählen Sie hierzu im Knoten **Globale Einstellungen** den Unterknoten **Einstellungen der Agenten-Benutzeroberfläche** und dann **Einstellungen für Taskbar-Informationsbereich**. Hier können Sie **Initiales Lernen der lokalen Whitelist** als Kontextmenü-Element auswählen. Hinweis: Beachten Sie, dass in diesem Fall das Blockieren von Anwendungen so lange deaktiviert ist, bis der Benutzer das Lernen initiiert hat.

Einstellung	Konfigurationsoptionen
Zusätzliche Erweiterungen, die für die lokale Whitelist gelernt werden	Zusätzlich zu den Standard-Dateitypen können weitere Dateitypen angegeben werden, die in die lokale Whitelist aufgenommen werden sollen. Dies ist sinnvoll, wenn eine Anwendung eine andere Dateiendung für einen Dateityp verwendet oder damit z.B. Skripte gelernt werden, die bereits auf dem System laufen.
Verzeichnisse, die für die lokale Whitelist gelernt werden	Normalerweise werden die Dateien von allen lokalen Festplatten gelernt. Es ist möglich dies auf bestimmte Verzeichnisse zu beschränken, in denen sich die Software befindet, die gelernt werden soll. Aktivieren Sie die Einstellung, in dem Sie die entsprechenden Verzeichnisse in der Liste angeben.

3.8 Einstellungen für die Anwendungs-Verhaltenskontrolle

Folgende Einstellungen können im Zusammenhang mit der Anwendungs-Verhaltenskontrolle konfiguriert werden:

Einstellung	Konfigurationsoptionen
Dauer der Lernphase für die Anwendungs-Verhaltenskontrolle	In dieser Einstellung können Sie einen Zeitraum bestimmen, während dessen gelernt und aufgezeichnet wird, was eine Anwendung auf dem DriveLock Agenten macht. Die entsprechenden Regeln werden aufgrund des gelernten Verhaltens generiert. Die Standardoption ist **Nicht konfiguriert**. Wählen Sie **Auf festen Wert setzen**, um einen Zeitraum anzugeben. Sobald die Anwendung zum ersten Mal gestartet wird, beginnt ein Countdown. Wenn die Zeit vorbei ist, wird alles geblockt, was nicht dem gelernten Verhalten entspricht.
Benutzer bei ungewöhnlichem Anwendungsverhalten fragen	Ist die Anwendungs-Verhaltenskontrolle für einen DriveLock Agenten aktiviert und die Lernphase abgeschlossen, ist jedes Verhalten einer Anwendung, das von dem gelernten abweicht, 'ungewöhnlich'. Die Standardoption ist **Deaktiviert**. Wählen Sie **Aktiviert**, wenn ein Benutzer das ungewöhnliche Verhalten bestätigen oder ablehnen muss. Das bestätigte Verhalten wird dann nachträglich gelernt.

4 Anwendungsregeln

Folgende Anwendungsregeln stehen zur Verfügung:

- Anwendungs-Hashdatenbank:
  Mithilfe von Hashdatenbanken können Sie durch Verwendung einer einzigen Regel alle in der Datenbank enthaltenen Anwendungen freigeben bzw. sperren. Eine Hashdatenbank wird durch das automatische Durchsuchen von vorgegebenen Verzeichnissen erstellt. Klicken Sie auf Anwendungs-Hashdatenbank, um eine derartige Datenbank zu erstellen und über eine Regel freizuschalten. Sie können z.B. eine Hashdatenbank von einem Referenz-PC erstellen, auf dem sich all Ihre Unternehmensprogramme befinden. Wenn Sie diese Regel auf andere Computer in Ihrem Unternehmen übernehmen, sind automatisch alle Programme freigeschaltet, die auch auf dem Referenz-PC installiert sind, während alle anderen Programme von DriveLock gesperrt werden.
- Datei-Eigenschaften-Regel:
  Diese Regel erlaubt das Filtern nach einer Reihe von verschiedenen Dateieigenschaften.
  Folgende Regeln aus Vorgängerversionen (vor 2020.2) werden dabei in einer einzigen Regel zusammengefasst: Dateipfad-, Datei-Eigentümer-, Hash- und Hersteller-Zertifikat-Regel.

  > Achtung: Wenn in einer Richtlinie aus einer älteren DriveLock Version (vor 2020.2) bereits eine oder mehrere dieser Einzelregeln (Pfad, Eigentümer, Hash) verwendet wurden, werden diese automatisch zu einer Datei-Eigenschaften-Regel konvertiert, wobei die in den Einzelregeln gesetzten Eigenschaften übernommen werden. Datei-Eigenschaften-Regel sind kompatibel mit DriveLock Agenten vor Version 2020.2, sofern nur Kombinationen von Eigenschaften geprüft werden, die exakt den Einstellungsmöglichkeiten der jeweiligen alten Regeltypen entsprechen.

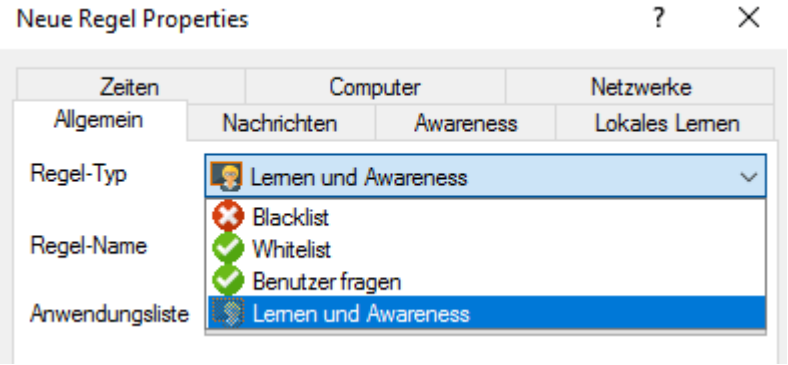
- Spezielle Regel:
  Mit den speziellen Regeln kann man einfach alle Programmdateien, die einem bestimmten Kriterium erfüllen, auf einem Computer identifizieren, z.B. ob eine Datei Teil des Microsoft Betriebssystems ist, oder ein Teil von DriveLock ist, oder ein .NET Programm ist. Man kann die spezielle Regel auch verwenden, um z.B. eine Blacklist-Regel zu überschreiben, damit manche Benutzer, wie die Dienst-Administratoren, alle Programme ausführen dürfen.
- Predictive-Whitelisting-Regel:

Mit dieser Regel aktivieren Sie Predictive Whitelisting. Die Einstellungen in dieser Regel überschreiben die Einstellung Lokale Whitelist und Predictive Whitelisting.

- Anwendungslisten-Regel:
  Verwenden Sie diese Regel (ab Version 2020.1), wenn Sie bereits vorhandene Anwendungslisten verwenden wollen, vor allem aber um die Lerneinstellungen für Anwendungen zu aktivieren.
- (veraltet) Anwendungs-Vorlage:
  Diese Regel ist nur noch für die Abwärtskompatibilität für ältere DriveLock Versionen vorhanden.
- Legen Sie **Ordner** im Knoten **Anwendungsregeln** an, um Regeln thematisch zu gruppieren, z.B. nach Hersteller oder Art der Software, und sie besser verwalten zu können. Um beispielsweise den Prozess eines Browser-Updates zu regeln, ist es sinnvoll und übersichtlich, alle hierfür benötigten Anwendungsregeln in einem Ordner zu speichern, dem Sie dann den Namen des Browsers geben. Sie können auch entsprechende Zugriffsrechte vergeben.

4.1 Verschiedene Regel-Typen

Bei der Konfiguration von Anwendungsregeln können Sie verschiedene Regeltypen festlegen:



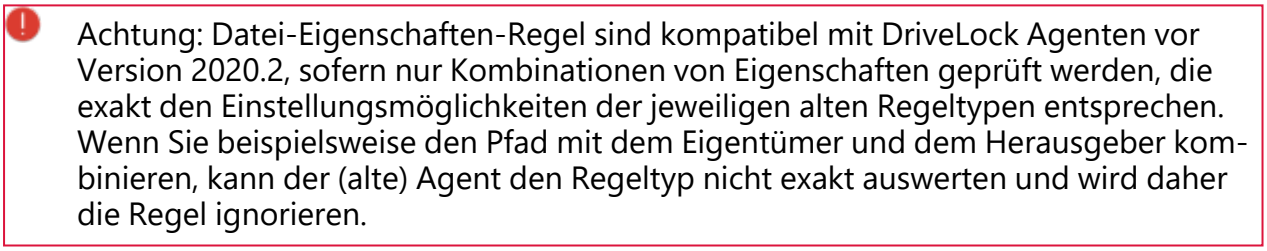
- **White- oder Blacklist**-Regeln: Mit diesen Regeltypen legen Sie fest, welche Anwendungen auf dem DriveLock Agenten erlaubt sind und ausgeführt werden dürfen oder welche Anwendungen verboten sind und blockiert werden.
- **Benutzer fragen**: Mit diesem Regeltyp wird eine Anwendung zwar erlaubt (Whitelist), aber der Benutzer muss den Start bestätigen.
- **Lernen und Awareness**: Der Regeltyp dient dazu, dass nur die Lerneinstellungen auf dem Reiter **Lokales Lernen** greifen oder die auf dem Reiter **Awareness** angegebenen Awareness-Kampagnen angezeigt werden. Dies bedeutet, dass Sie für eine

Anwendung Einstellungen setzen können, ohne diese aktiv zu erlauben (Whitelist) oder zu blockieren (Blacklist).

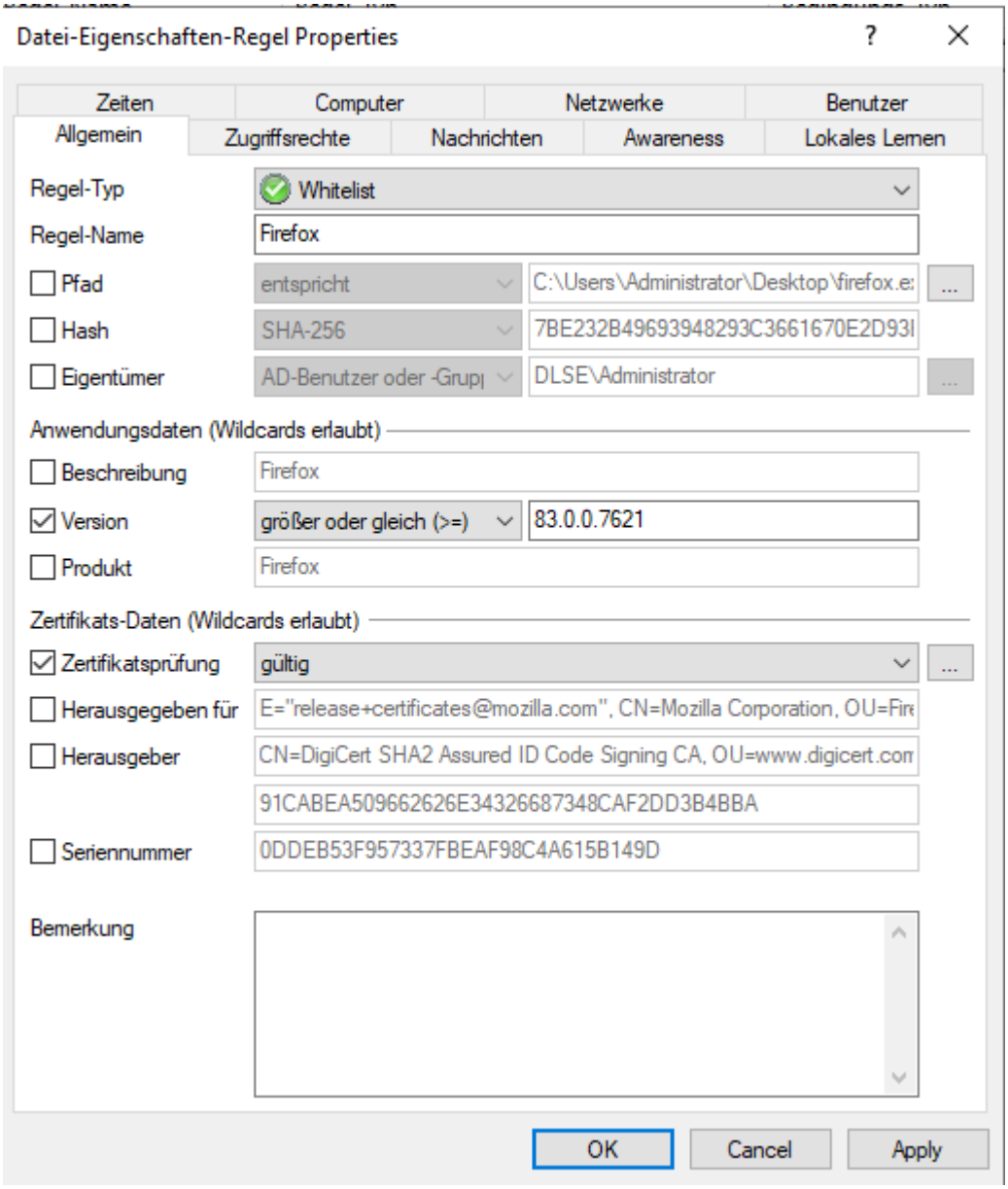
- Der Reiter **Lokales Lernen** findet sich in folgenden Regeln: Datei-Eigenschaften- und Anwendungslisten-Regel.
- Wie die Einstellungen auf dem Reiter **Lokales Lernen** verwendet werden können, wird hier erklärt.
- Ein Konfigurationsbeispiel für das Anzeigen einer Awareness-Kampagne finden Sie hier.

4.2 Datei-Eigenschaften-Regel

Mit dieser Regel können Sie verschiedene Dateieigenschaften angeben, nach denen gefiltert werden soll. Neben einigen zusätzlichen Auswahlmöglichkeiten vereint diese Regel die Optionen der Dateieigentümer-, Dateipfad-, Hash- und Hersteller-Zertifikatsregeln aus früheren Versionen.



Gehen Sie folgendermaßen vor:



1. **Pfad**: Wählen Sie hier als erstes einen Pfad aus, von dem aus Anwendungen gestartet werden dürfen (bzw. geblockt werden sollen) oder eine bestimmte Datei innerhalb eines vorgegebenen Verzeichnisses. Klicken Sie hierzu die Schaltfläche **...** . Diese Option überprüft, ob der Pfad der Datei bestimmte Bedingungen erfüllt.

   Hinweis: Sobald Sie hier eine Auswahl getroffen haben, werden die anderen Felder im Dialog automatisch ausgefüllt. Sie können dann ein Häkchen bei den Optionen setzen, nach denen Sie filtern wollen.

   Sie können eine Anwendung auch aus der Liste der gerade gestarteten Programme (Option **Aus laufenden Prozessen...**) oder aus der Anwendungsdatenbank (Option **Aus Applikations-Inventar...**) auswählen.

Um sich über die Remoteverbindung Informationen über aktuell laufende Anwendungen von einem anderen Rechner, auf dem DriveLock installiert und gestartet ist, anzeigen zu lassen, wählen Sie die Option **auf Agent**, geben den Namen des Rechners ein und klicken dann **Verbinden**.
Wählen Sie außerdem eine der beiden Optionen in der Dropdown-Liste:

- **entspricht**: trifft dann zu, wenn der Pfad dem angegebenen Text entspricht, wobei Platzhalter verwendet werden können. Enthält der Text keine Backslashes, wird nur der Dateiname überprüft.
- **enthält**: trifft dann zu, wenn der angegebene Text an irgendeiner Stelle im Dateipfad vorkommt.

2. Vergeben Sie dann einen **Regelnamen** und wählen Sie den **Regeltyp**, d.h. wie die Regel angewendet werden soll. Weitere Informationen finden Sie hier.
3. **Hash**: Diese Option überprüft, ob der Hashwert des Dateiinhalts mit dem angegebenen Wert übereinstimmt. Dieser wird bei der Regelerstellung gespeichert und zur Laufzeit mit dem aktuell berechneten verglichen. Stimmen beide überein, wird die Regel aktiviert. Diese Option eignet sich z.B. für eine einzelne Applikation, die per Whitelist oder Blacklist erlaubt oder gesperrt werden soll.

> Hinweis: Beachten Sie dabei, dass die Hash-Berechnung auf dem DriveLock Agenten immer auf Basis des in den **Einstellungen** angegebenen Hash-Algorithmus für Hash-basierte Regeln erfolgt.

4. **Eigentümer**: Mit dieser Option wird der Start von Anwendungen vom Datei-Eigentümer abhängig gemacht, z.B. können Sie mit dieser Einstellung alle Programme, die von einem Administrator oder einem vertrauenswürdigem Installationskonto installiert wurden, erlauben. Alle Programme, die von anderen Benutzern installiert wurden, sind hingegen gesperrt. So können auch automatisch alle Programme gesperrt werden, die ohne vorherige Installation ausgeführt werden können.
Folgende Optionen können ausgewählt werden bzw. sind je nach Auswahl automatisch eingetragen:
   - **Administratoren-Gruppe**: Diese Option deckt alle lokalen Administratoren ab. Die Administratoren-Gruppe muss explizit Datei-Eigentümer sein, damit die Datei zugelassen ist.
   - **Trusted Installer** und **Local System**: Diese Standard-Windows-Konten müssen Datei-Eigentümer sein, damit die Datei zugelassen ist.

- **AD-Benutzer oder Gruppe**: Wählen Sie hier einen AD-Benutzer oder eine Gruppe als Datei-Eigentümer aus. Hierbei wird die SID überprüft.
- **Name (Benutzer / Gruppe)**: Sie können hier manuell einen Benutzer oder eine Gruppe hinzufügen. Hierbei wird der Name überprüft.

> Hinweis: Wenn Sie eine Gruppe zuweisen, muss der Datei-Eigentümer die Gruppe sein, nicht ein Mitglied der Gruppe.

5. **Beschreibung**: Hier wird die Dateibeschreibung eingetragen, z.B. 'Paint' bei der mspaint.exe-Datei.
6. **Version**: Sie können die Version überprüfen lassen, damit Benutzer keine anderen oder älteren Programmversionen ausführen können, z.B. können Sie die Firefox-Version 83.0.0.7621 oder höher erlauben und alle vorherigen Versionen blocken, die Sicherheitslücken enthalten könnten. Wählen Sie die entsprechende Option im Auswahlmenü aus, z.B. größer oder gleich.
7. **Produkt**: Hier wird der Produktname eingetragen, z.B. Betriebssystem Microsoft Windows.
8. **Zertifikatsprüfung**: Mit dieser Prüfung können Sie signierte Software whitelisten oder unsignierte Software blacklisten.
   Über die Browse-Schaltfläche können Sie auch Zertifikate über das Applikations-Inventar aussuchen.

> Hinweis: Beachten Sie, dass Windows Dateien nicht signiert sind. Hier muss zusätzlich z.B. ein Dateipfad angegeben werden.

9. **Herausgegeben für**, **Herausgeber**, **Thumbprint** und **Seriennummer** sind weitere Eigenschaften des Zertifikats. Die Seriennummer ist nur in Kombination mit dem Herausgeber eindeutig.

4.3 Anwendungs-Hashdatenbank

Um die Konfiguration der Applikationskontrolle zu vereinfachen, bietet DriveLock die Möglichkeit, Anwendungs-Hashdatenbanken zu erstellen und im White- oder Blacklist-Modus zu verwenden. Hashdatenbanken können erstellt werden, indem ein oder mehrere Verzeichnisse (und deren Unterverzeichnisse) automatisch nach Anwendungen durchsucht, von diesen Hashwerte berechnet und in einer Datei gespeichert werden. Auch von der Fest-

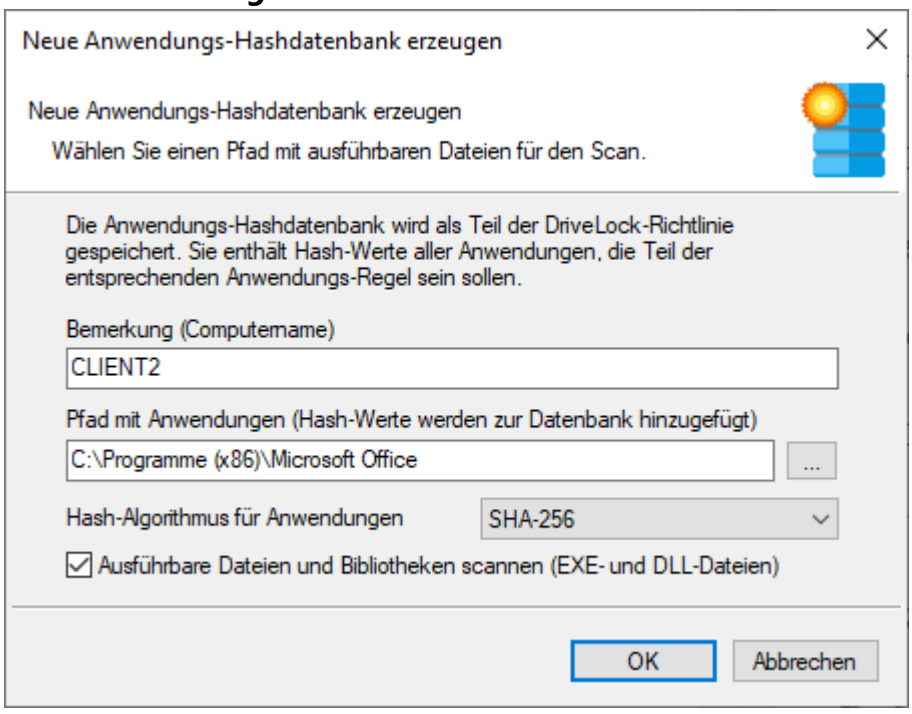
platte eines Referenzsystems kann eine Hashdatenbank aller installierten Programme erzeugt werden.

So erstellen Sie eine Anwendungs-Hashdatenbank:

1. Wählen Sie im Knoten **Anwendungen** den Unterknoten **Anwendungsregeln**. Öffnen Sie dann über das Kontextmenü **Neu** den Dialog **Anwendungs-Hashdatenbank**.
2. Zunächst ist auf dem Reiter **Allgemein** noch keine Datenbank ausgewählt. Sie können entweder eine neue Datei anlegen oder eine bereits bestehende Datei auswählen.

> Hinweis: DriveLock stellt ein Hilfsprogramm **DriveLock Application Hash Database Tool** zur Verfügung, mit dem ebenfalls eine Hashdatenbank generiert werden kann. Dieses Tool befindet sich im Installationsverzeichnis von DriveLock (C:\Program Files\CenterTools\DriveLock MMC\Tools\DLExeHasher.exe).

3. Unter **Benutzter Hash-Algorithmus** steht der im Hash-Verfahren bereits voreingestellte Wert.
4. Um eine neue Hashdatenbank zu erzeugen, klicken Sie auf **Datenbank-Datei** und wählen **Neu anlegen** aus dem Menü.



5. Tragen Sie in das erste Eingabefeld den Namen des Computers ein, dessen Verzeichnis durchsucht werden soll. Diese Information erleichtert bei einer später möglichen Migration mehrerer Datenbankdateien die Zuordnung. Geben Sie einen Dateipfad an oder klicken Sie **...** um einen entsprechenden Auswahldialog zu öffnen.

> Hinweis: Wenn Sie als Dateipfad einen UNC-Pfad eingeben, können Sie auch ein Verzeichnis auf einem anderen Computer durchsuchen lassen.

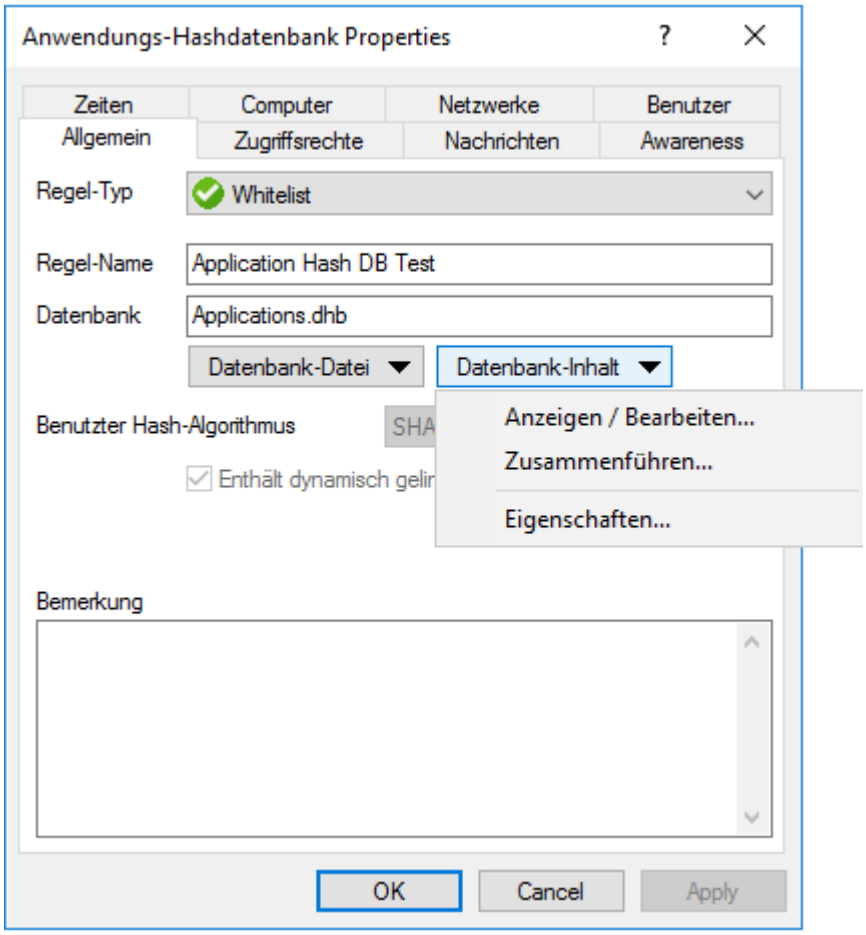
Der **Hash-Algorithmus für Anwendungen** definiert den für diese Datenbank verwendeten Algorithmus. Das Hash-Verfahren legen Sie am zuvor global fest, bevor Sie Hash-Datenbanken erzeugen, um die Interoperabilität zwischen mehreren Datenbanken und Regeln sicherzustellen. Wählen Sie **Ausführbare Dateien und Bibliotheken scannen**, um neben EXE- auch DLL-Dateien zu scannen.

6. Sobald Sie auf **OK** klicken, beginnt DriveLock damit, das angegebene Verzeichnis rekursiv nach Anwendungsdateien zu durchsuchen.

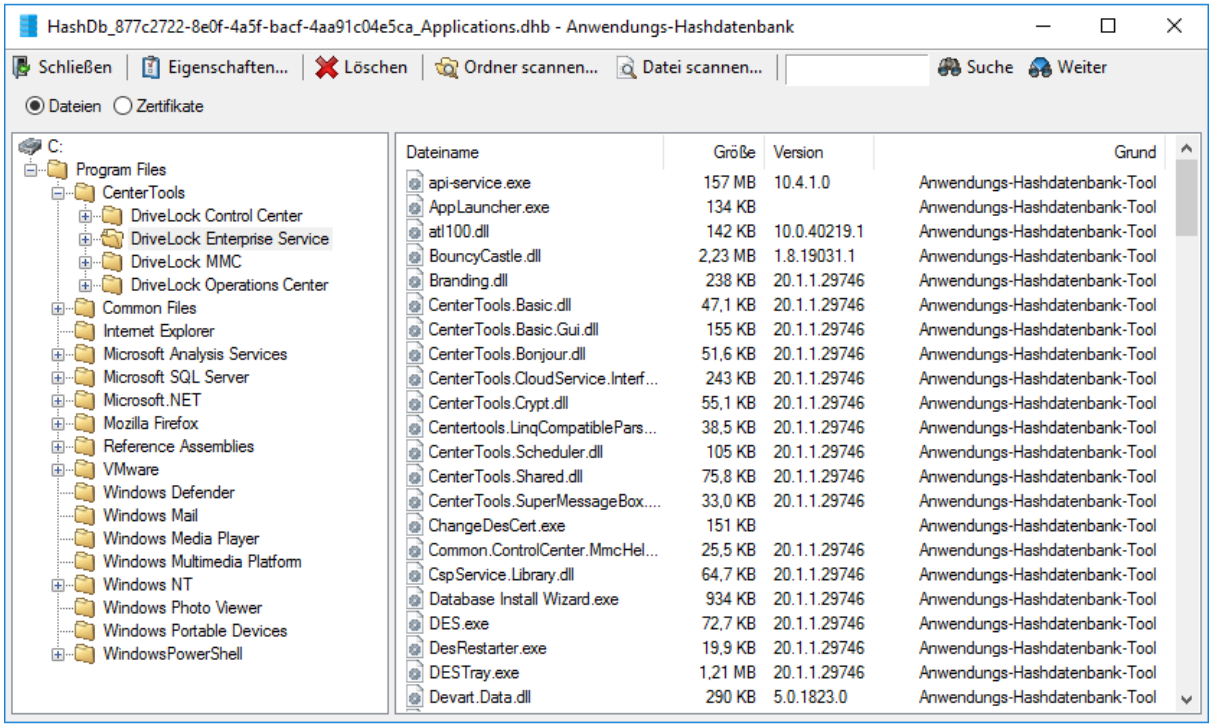
> Hinweis: Bitte beachten Sie, dass das Auslesen größerer Verzeichnisse oder UNC-Pfade etwas dauern kann. Der Vorgang sollte nicht unterbrochen werden.

> Hinweis: Beim Durchsuchen werden keine doppelten Einträge generiert. Wenn die gleiche Datei ein weiteres Mal in einem anderen Verzeichnis gefunden wird, fügt DriveLock den Hashwert nicht noch einmal der Hashdatenbank hinzu. Das hat jedoch auf die Sperrung oder Freigabe keine Auswirkung und ermöglicht so, einen sogenannten Differenz-Scan zu erstellen, bei dem dann nur neu hinzugekommene Anwendungen mit aufgenommen werden.

7. Sobald alle Hashwerte berechnet und in die Hashdatenbank-Datei geschrieben wurde, kehrt DriveLock zum Ausgangsdialog zurück und wählt die soeben generierte Datei als Datenbank für diese Vorlage aus.
8. Fügen Sie eine aussagekräftige Beschreibung (**Regel-Name**) hinzu und tragen ggf. ergänzende Informationen in das Textfeld **Bemerkung** ein.
9. Über die Schaltfläche **Datenbank-Inhalt** können Sie sich nun die gefundenen Programme ansehen, den Inhalt der Datenbank nachbearbeiten oder Daten aus einer weiteren Hashdatenbank-Datei migrieren.
10. Klicken Sie auf **Datenbank-Inhalt** und wählen Sie den Eintrag **Anzeigen/Bearbeiten**, um manuelle Änderungen am Inhalt vorzunehmen.



11. Im Dialog sehen Sie links die durchsuchte Verzeichnisstruktur, rechts finden sich die Hashwerte aller in einem bestimmten Verzeichnis enthaltenen Programmdateien wieder.



12. Über die Schaltflächen **Ordner scannen** und **Datei scannen** lassen sich weitere Programmdateien der bestehenden Hashdatenbank hinzufügen. Mit Hilfe der Schaltfläche **Löschen** können einzelne Dateien (rechts) oder ganze Verzeichnisse (links) aus der Datenbank entfernt werden. Klicken Sie auf **Eigenschaften**, um zusätzliche Informationen zur Hashdatenbank zu erhalten.
13. Beenden Sie die Bearbeitung der Hashdatenbank, indem Sie auf **Schließen** klicken.

> Hinweis: Die gleiche Funktionalität – und auch die Möglichkeit, zwei Datenbanken zu einer zusammenzuführen – steht Ihnen auch über das Hilfsprogramm zur Verfügung.

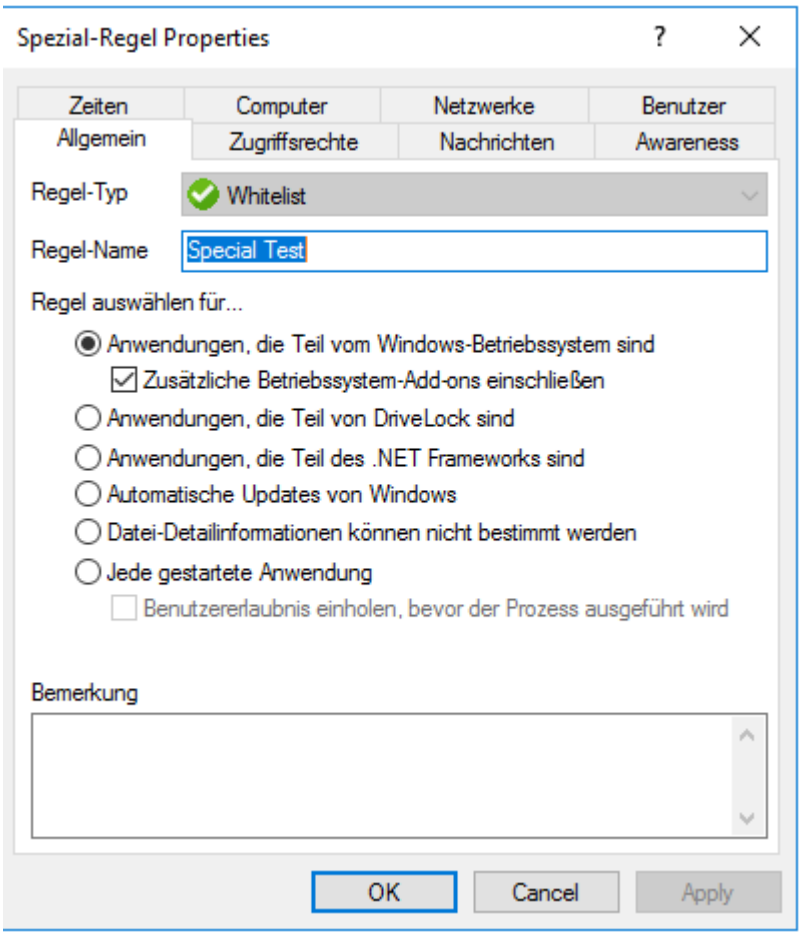
14. Klicken Sie auf **Datenbank-Inhalt** und wählen Sie den Eintrag **Zusammenführen**, um Daten aus einer weiteren Hashdatenbank in die ausgewählte Datenbank zu migrieren.
15. Geben Sie den Pfad und den Dateinamen der Hashdatenbank an, die hinzugefügt werden soll. Alternativ können Sie den Dateiauswahldialog verwenden.
16. Sobald Sie **OK** klicken, beginnt DriveLock mit der Zusammenführung der beiden Datenbanken.
17. Anschließend kehrt DriveLock wieder zum Ausgangsdialog zurück:
18. Klicken Sie **OK**, um den Dialog zu verlassen und die Änderungen zu speichern.

> Hinweis: Auch wenn Sie für einen Computer eine Hashdatenbank mit allen installierten Anwendungen zur Konfiguration einer Whitelist-Regel verwenden, sollten Sie zusätzlich immer noch spezielle Anwendungsregeln (siehe Spezielle Regeln verwenden) insbesondere für die Betriebssystemdateien verwenden. Diese werden technisch bedingt schneller geladen als die Informationen aus der Hashdatenbank und stehen dem DriveLock Agenten somit beim Start der Applikationskontrolle wesentlich früher zur Verfügung.

4.4 Spezielle Regel

> Hinweis: Spezielle Regeln können nur als Whitelist-Regel verwendet werden.

Folgende Auswahlmöglichkeiten stehen im Dialog zur Verfügung:



1. Anwendungen, die Teil vom Windows Betriebssystem sind
   - beinhaltet alle durch Windows System File Protection (WFP) geschützten Programme

   Zusätzliche Betriebssystem-Add-ons einschließen beinhaltet Programme in:
   - C:\windows
   - C:\windows\system32
   - C:\windows\servicing
   - C:\windows\pchealth\helpctr\binaries (Help Center)
   - C:\windows\application compatibility scripts
   - C:\windows\explorer.exe
   - C:\Programme\Internet Explorer
   - C:\Programme\Windows Defender
2. Die Anwendung ist Bestandteil von DriveLock

- Programme in den DriveLock Installations-Verzeichnissen

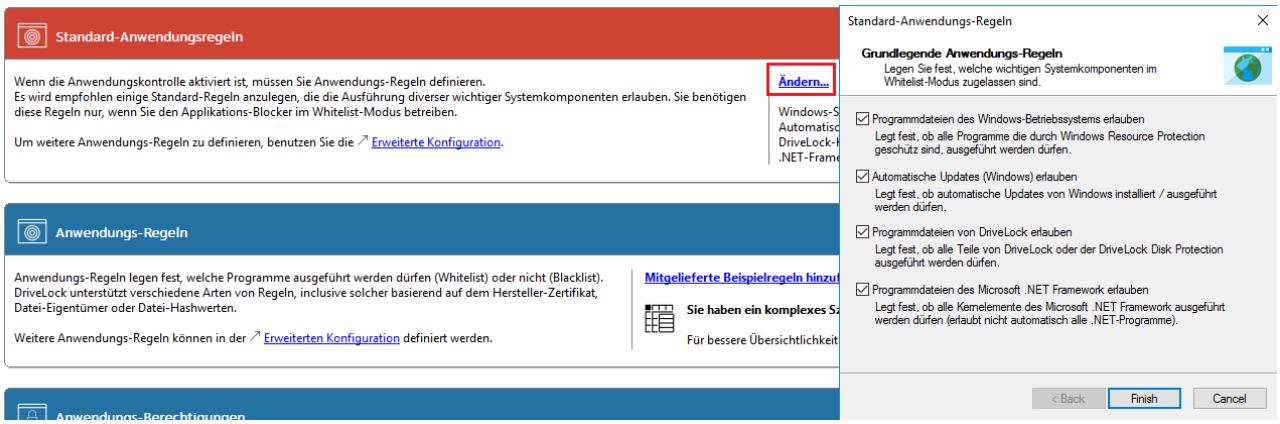
3. Die Anwendung ist Bestandteil des .NET Frameworks
   - Programme in C:\Windows\Microsoft.NET
4. Automatisches Update von Windows
   - Es wird überprüft, ob der Prozess durch den Windows Update Agent initialisiert wurde.
5. Datei-Detailinformationen können nicht bestimmt werden
   - Notlösung, falls DriveLock auf benötigte Datei-Detailinformationen von einer bestimmten Datei nicht zugreifen oder diese nicht lesen kann.
6. Jede gestartete Anwendung
   - Ermöglicht einen Zugriff auf alle Anwendungen und kann in Verbindung mit einer der weiteren Einschränkungen verwendet werden, um zum Beispiel der Gruppe der Administratoren den Zugriff auf alle Anwendungen zu ermöglichen. Optional kann eine Benutzererlaubnis eingeholt werden, bevor der Prozess gestartet wird.

> Hinweis: Diese Benutzererlaubnis wirkt sich nicht auf die Priorität der Regel aus.

4.4.1 Standard-Anwendungsregeln

Um grundlegende Anwendungsregeln zu erstellen, klicken Sie in der Taskpad-Ansicht auf **Ändern**.

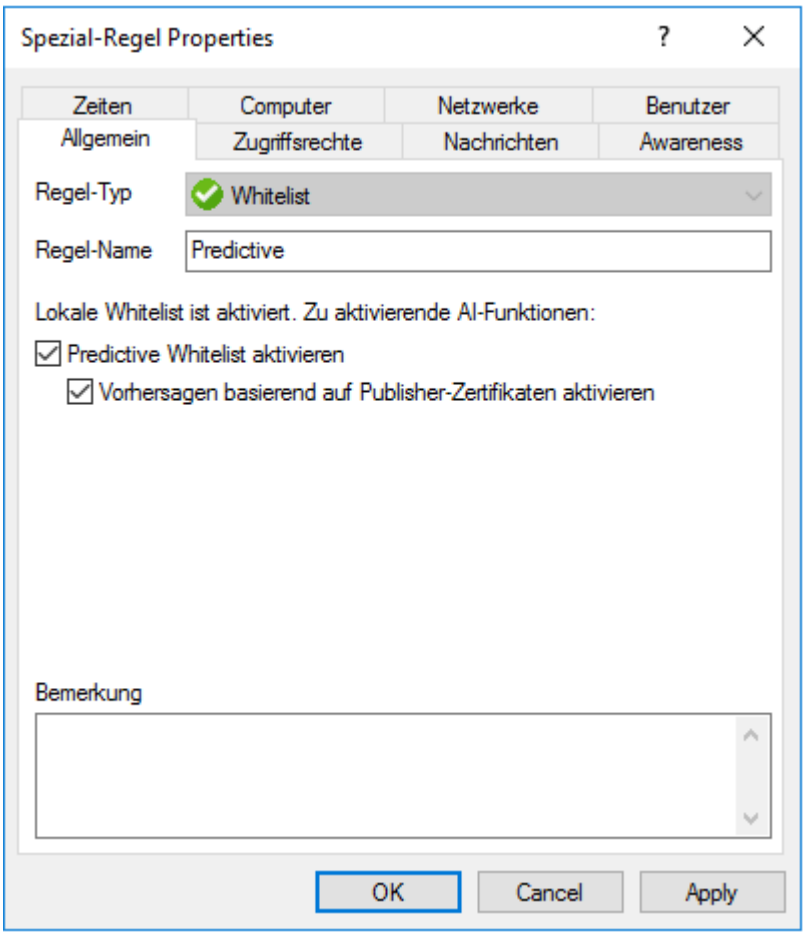
Wählen Sie die zu verwendenden Regel-Typen aus und klicken auf Fertig stellen. DriveLock erstellt die dazugehörigen Spezial-Regeln.



4.5 Predictive-Whitelisting-Regel

Die Predictive-Whitelisting-Regel ist nur als Whitelist zu verwenden.

Setzen Sie folgende Optionen im Dialog:



Durch Auswahl der Option **Vorhersagen basierend auf Publisher-Zertifikaten** setzt DriveLock Algorithmen ein, um neue Versionen von signierter Software zu erkennen, auch wenn die Zertifikate nicht völlig identisch sind.

Siehe auch Einstellung Lokale Whitelist und Predictive Whitelisting.

Hinweis: Dies funktioniert nur, wenn die neue Version ausreichend wiedererkennbar ist.

4.6 Anwendungslisten-Regel

Hinweis: Die Regel wird ohne Benutzereinschränkung eingesetzt.

In der Task-Pad-Ansicht werden Ihnen zwei mitgelieferte und sofort einsetzbare Beispiele angeboten. Mit der einen Regel können Sie das Verhalten verschiedener Browser und mit der anderen das verschiedener E-Mail-Clients lernen und kontrollieren (die dazugehörigen Anwendungslisten werden zeitgleich im Ordner **Anwendungslisten** angelegt).

Anhand des Beispiels für das Verhalten von Browsern bei Updates lassen sich die Dialogoptionen folgendermaßen erklären:

1. Auf dem Reiter **Allgemein** ist folgendes angegeben:
   - **Regel-Typ**: Lernen und Awareness
     Die Option **Lernen und Awareness** regelt nur die Lerneinstellungen, trifft aber keine Entscheidung darüber, ob ein Programm gestartet werden darf oder nicht (wie dies bei White- oder Blacklist der Fall wäre).

     Hinweis: Die Entscheidung, ob ein Programm gestartet werden darf, erfolgt über die Hashes der Dateien (in Hash-Regeln), die von Application Control automatisch verwaltet werden.

   - **Regel-Name**: Lernverhalten von Browsern
   - **Anwendungsliste**: Browser
     Die Anwendungsliste sollte alle gängigen Browser enthalten und muss bereits vorhanden sein.
2. Auf dem Reiter **Lokales Lernen** stehen folgende Optionen zur Verfügung:
   - **Die Anwendung darf Programme starten, die in keiner Whitelist enthalten sind**:
     Wenn diese Option ausgewählt ist, kann ein Service-Prozess, der ein Browser-Update ausführen soll, gestartet werden, auch wenn dieser Service-Prozess nicht explizit erlaubt ist. Außerdem erhält der Service-Prozess durch diese Option die Erlaubnis, das eigentliche Browser-Update starten zu dürfen, das ebenfalls nicht 'gewhitelistet' ist.
   - **Alle Programmdateien lernen, die von dieser Anwendung (inklusive untergeordneter Prozesse) geschrieben werden**:
     Damit das Browser-Update den eigentlichen Browser und den Service-Prozess beenden und die entsprechenden Dateien durch die aktualisierte Version des

Browsers ersetzen kann, müssen alle untergeordneten Prozesse des Service-Prozesses automatisch einer Whitelist hinzugefügt werden.
Als Folge kann der eigentliche Browser als untergeordneter Prozess des Service-Prozesses Programme starten, die nicht explizit erlaubt sind. Außerdem werden dann alle Dateien, die vom Browser geschrieben werden, automatisch auf die Whitelist gesetzt.

Da die beiden Optionen im Falle eines Browsers nicht erwünscht sind, muss der Browser so konfiguriert werden, dass diese Berechtigungen nicht an den Prozess vererbt werden. Daher wird folgende Option ausgewählt:

- **Die Anwendung erhält nie die oben genannten Berechtigungen**

Außerdem wird im Abschnitt **Anwendungsverhalten lernen und kontrollieren** für die Browser angegeben, dass lokal gelernt wird

- welche Programme sie starten,
- welche DLLs sie laden und
- in welche Verzeichnisse sie ihre Dateien schreiben dürfen.

Fazit: Die in der Regel angegebenen Anwendungen bekommen durch diese Einstellungen genau die Rechte, die sie auf dem jeweiligen DriveLock Agenten brauchen, auf dem das Anwendungsverhalten aufgezeichnet wird. So können auf unterschiedlichen Agenten beispielsweise auch unterschiedliche Download-Verzeichnisse für Anwendungen gelernt werden.

4.7 Anwendungs-Vorlage (veraltet)

Anwendungsvorlagen können eine oder mehrere Applikationen enthalten, die entweder gesperrt (Blacklist) oder erlaubt (Whitelist) werden.

Achtung: Wir weisen darauf hin, dass diese Anwendungsregel veraltet ist und nicht mehr verwendet werden sollte. Sollten Sie dennoch Informationen hierzu benötigen, finden Sie diese im Administrator-Handbuch. Wir empfehlen stattdessen die Verwendung von Anwendungs-Hashdatenbanken-Regeln.

5 Anwendungs-Verhaltensregeln

Mit der Anwendungs-Verhaltenskontrolle erreichen Sie folgende Ziele:

- Sie verhindern, dass aus einer erlaubten Anwendung heraus eine weitere Anwendung (bzw. Prozess, Skript) gestartet wird, die eine potentielle Gefahr für Ihr System darstellen könnte und
- Sie legen fest, welche Art von Zugriff Sie einer bestimmten Anwendung erlauben wollen (z.B. lesend oder schreibend auf Dateien oder auf die Registry zuzugreifen).

Dazu stehen Ihnen unter anderem folgende Funktionen zur Verfügung. Sie können

- bestimmen, in welcher Reihenfolge (Priorität) Anwendungs-Verhaltensregeln abgearbeitet werden,
- angeben, welche Maßnahme ergriffen werden soll, wenn ein Zugriff durch eine bestimmte Anwendung erfolgt (z.B. die Anwendung wird geblockt oder nicht),
- bestimmen, ob eine Anwendungs-Berechtigung an untergeordnete Prozesse vererbt werden soll,
- verschiedene Datei- und Verzeichnisfilter angeben oder
- Skript-Typen festlegen, die bei der Ausführung von Skripten verwendet werden dürfen.

Außerdem können Sie ab Version 2020.1 eine Verhaltensregel erzeugen, die auf einer gespeicherten Aufzeichnung des Anwendungsverhaltens auf dem DriveLock Agenten basiert.

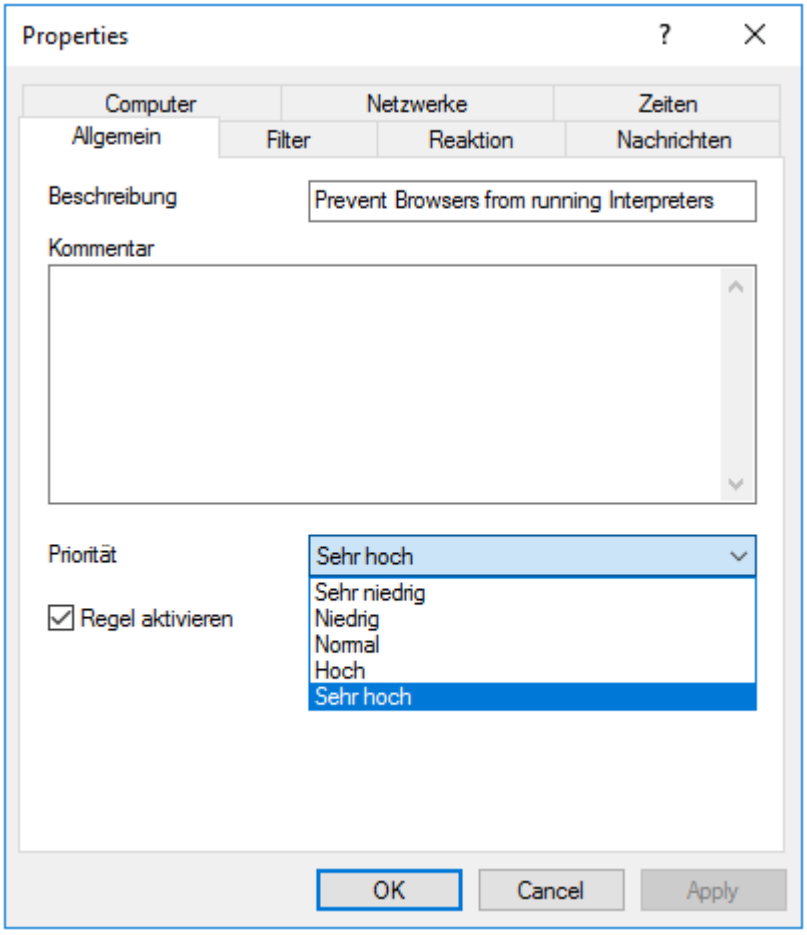
In der DriveLock Management Konsole werden alle Anwendungs-Verhaltensregeln in einer vom Benutzer definierbaren Ordnerstruktur dargestellt.

5.1 Anwendungs-Verhaltensregeln definieren

Anwendungs-Verhaltensregeln lassen sich folgendermaßen erstellen:

1. Wählen Sie in der Taskpad-Ansicht **Verhaltensregel hinzufügen** oder klicken Sie auf **Neu** im Kontextmenü des Unterknotens **Anwendungs-Verhaltensregeln**, und erstellen so eine neue Verhaltensregel. In diesem Kontextmenü können Sie auch **Ordner** anlegen, um zusammengehörige Anwendungs-Verhaltensregeln zu gruppieren.
2. In beiden Fällen öffnet sich der unten abgebildete Eigenschaftendialog, in dem Sie Ihre Angaben vornehmen können.

3. Geben Sie auf der Registerkarte **Allgemein** eine sprechende Beschreibung ein und fügen Sie ggf. einen Kommentar hinzu.
   In der Abbildung unten sehen Sie eine der mitgelieferten Beispiel-Berechtigungen.
4. Die Option **Regel aktivieren** ist standardmäßig gesetzt.
5. Unter **Priorität** haben Sie verschiedene Auswahlmöglichkeiten.



Hinweis: Allgemein gültige Anwendungs-Verhaltensregeln bekommen eine niedrigere Priorität, spezielle eine höhere. Die Priorisierung richtet sich nach den Anwendungsfällen. Regeln mit hohen Prioritäten werden vor denen mit niedrigen Prioritäten abgearbeitet. Das System prüft die Regeln in der angegebenen Reihenfolge und sobald eine Regel zutrifft, wird diese angewendet.

Die **Priorität** lässt sich auch in der DriveLock MMC verringern oder erhöhen.
Beispiel: Kombinieren Sie Regeln miteinander, z.B. erstellen Sie eine Regel, die dem Browser erlaubt, den Windows Media-Player zu starten (hohe Priorität) und eine weitere Regel, die dem Browser verbietet, andere Programme zu starten (niedrigere Priorität).

6. Setzen Sie Ihre Angaben auf den Reitern Filter, Reaktion, Nachrichten und den allgemeinen Einstellungen für Regeln und Berechtigungen (Computer, Netzwerke, Zeiten) fort.

Konkrete Beispiele finden Sie in den beschriebenen Anwendungsfällen.

5.1.1 Angaben auf dem Reiter Filter

Folgende Einstellungen stehen hier zur Verfügung:

1. **Ausführende Anwendung**
   Hier kann entweder der volle Pfad oder der Name der Anwendung angegeben werden, die Sie kontrollieren wollen, z.B. C:\Program Files\Mozilla Firefox\firefox.exe oder nur firefox.exe. Bei der Angabe sind Platzhalter zulässig.
   Beachten Sie bitte, dass Sie hier auch Anwendungslisten auswählen können, sofern Sie diese bereits erstellt haben. Mehr dazu im entsprechenden Kapitel.
2. **An untergeordnete Prozesse vererben**
   Wählen Sie diese Einstellung, damit Ihre Anwendungs-Berechtigung nicht nur für die Prozesse gilt, die dem Kriterium **Ausführende Anwendung** entsprechen, sondern auch für alle Kind-Prozesse. Diese Einstellung wirkt demnach nicht nur auf die unmittelbar untergeordneten Prozesse, sondern auf sämtliche untergeordnete Prozesse.

   > Hinweis: Dies ist insbesondere dann interessant, wenn Sie auf dem Reiter **Filter** als Maßnahme **Blockieren** auswählen, weil dadurch Ihre Anwendungs-Verhaltensregeln nicht durch Starten eines anderen Prozesses umgangen werden können.

   Beispiel: Sie erstellen eine Anwendungs-Berechtigung, die es verbietet, dass Ihr Browser Powershell starten darf. Um zu verhindern, dass Powershell trotzdem aus der Kommandozeile (in diesem Fall wäre dies ein untergeordneter Prozess) gestartet wird, wählen Sie diese Option.
3. **Zugriffsmodus**
   Der Zugriffsmodus ist ein Filterkriterium für die Anwendungs-Berechtigung. Hier definieren Sie welche Aktion die ausführende Anwendung durchführen soll.
4. Weitere Angabe (Ziel)
   Je nachdem, welchen Zugriffsmodus Sie gewählt haben, geben Sie im nächsten Textfeld unterschiedliche Ziele an (eine Pfadangabe ist in allen Fällen möglich).

Hinweis: Ab Version 2020.1 können Sie hier mehrere Angaben machen. Dadurch lässt sich die Anzahl der Regeln reduzieren.

Zugriffsmodus	Ziel	Erklärung
Ausführen	Aufgerufene Anwendung	Geben Sie hier die Anwendung an, deren Aufruf Sie beispielsweise unterbinden wollen (als Maßnahme wählen Sie in diesem Fall Blockieren aus). Optional können Sie hier einen **Kommandozeilenparameter** angeben, der die Ausführung des aufgerufenen Programms weiter einschränkt. Anwendungsfall 1 Beachten Sie bitte, dass die Eingabe von Parametern unter Windows XP nicht unterstützt wird!
DLL laden	Name der DLL	Geben Sie hier die DLL an, die beispielsweise nur aus einem bestimmten Verzeichnis geladen werden darf. Anwendungsfall 2
Skript ausführen	Name des Skripts	Geben Sie hier das Skript an, dessen Ausführung Sie einschränken wollen. Anwendungsfall 3 Beachten Sie bitte bei Auswahl dieser Option, dass nur die im Unterknoten Skript-Definition definierten Skript-

Zugriffsmodus	Ziel	Erklärung
		Typen berücksichtigt werden.
Datei lesen / schreiben	Name der Datei	Geben Sie hier entweder einen Dateinamen oder ein Verzeichnis an, auf das die ausführende Anwendung lesend oder schreibend zugreifen darf (oder nicht darf). Anwendungsfall 4 für Lesezugriff Anwendungsfall 5 für Schreibzugriff
Registry lesen / schreiben	Registry-Schlüssel	Geben Sie hier den entsprechenden Registry-Schlüssel an (z.B. `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\`), auf den lesend oder schreibend zugegriffen werden darf. Platzhalter sind auch hier zulässig. Anwendungsfall 6 Beachten Sie bitte, dass der Zugriffsmodus Registry lesen/schreiben erst ab Windows 7 funktioniert!

5.1.2 Angaben auf dem Reiter Reaktion

Auf diesem Reiter geben Sie an, wie die Applikationskontrolle auf die Angaben auf dem Reiter **Filter** reagieren soll.

Gehen Sie folgendermaßen vor:

1. Wählen Sie die entsprechende Maßnahme:

   - **Nicht blockieren**: Wählen Sie diese Option, wenn keine weitere Aktion erforderlich ist. Diese Maßnahme entspricht einem 'Erlauben'.
   - **Blockieren**: Wählen Sie Blockieren, wenn Sie bestimmte Ereignisse in Abhängigkeit vom Zugriffsmodus bzw. vom Ziel unterbinden wollen. Beispielsweise wird durch diese Maßnahme die Ausführung einer weiteren Anwendung oder eines Skripts oder das Laden einer DLL verhindert. Dies ist die Standard-Einstellung.
   - **Benutzer fragen**: Wenn Sie den Benutzer entscheiden lassen wollen, ob eine bestimmte Aktion zugelassen werden soll, wählen Sie diese Option. Dann entscheidet der Benutzer beispielsweise, ob ein Powershell-Skript gestartet wird oder nicht.

     Hinweis: Die Auswertung der Regeln wird bei diesen Optionen (Nicht blockieren, Blockieren und Benutzer fragen) abgebrochen.

   - **Reporting anpassen**: Mit dieser Option wird keine weitere Maßnahme durchgeführt, sondern es wird lediglich das Reporting verändert. Sie können dann weiter unten angeben, ob die Kommandozeile in dem Ereignis abgebildet wird. Beachten Sie, dass bei dieser Option die Auswertung der Regeln weitergeführt wird.

Hinweis: Beachten Sie bitte, dass diese Maßnahmen zusätzlichen Schutz für besonders anfällige Prozesse bieten. Die Einstellung 'Nicht blockieren' kann von einer Einstellung in einer White- bzw. Blacklist trotzdem blockiert werden, die Einstellung 'Blockieren' überschreibt hingegen die Einstellung in einer Whitelist-Regel!

2. Wählen Sie den Mechanismus aus, der für andere Ziele greift, die nicht auf dem Reiter **Filter** definiert worden sind:
   - **Den Zugriff auf andere Ziele blockieren**
     Zugriff wird nur auf die Ziele erlaubt, für die eine explizite Erlaubnis existiert, alle anderen Ziele werden blockiert.

- **Den Zugriff durch andere Anwendungen blockieren**
  Zugriff wird nur für die Anwendungen erlaubt, für die eine explizite Erlaubnis existiert, alle anderen Anwendungen werden blockiert.
  Beispiel: Nur die Bank-Anwendung aus Anwendungsfall 4 darf auf das Bank-Verzeichnis zu greifen aber keine andere Anwendung.

3. Geben Sie an, welche Ereignisse erzeugt werden sollen:
   Standardmäßig ist die Option **Ereignisse erzeugen wenn Zugriff verweigert wird** ausgewählt. Sie können zusätzlich oder alternativ die Option **Ereignisse erzeugen wenn Zugriff erlaubt wird** auswählen. Diese Option ist z.B. sinnvoll, wenn Sie in einer Regel die Ausführung von bestimmten Skripten erlauben wollen und die dazugehörigen Ereignisse erzeugen wollen. Alle Ereignisse werden im DriveLock Control Center (DCC) bzw. DriveLock Operations Center (DOC) angezeigt. Beide Optionen eignen sich auch für den Simulationsmodus.

   Hinweis: Beachten Sie bitte, dass eine große Anzahl Ereignisse erzeugt wird, wenn Sie beide Optionen auswählen.

4. Die Option **Kommandozeile im Ereignis anzeigen** legt fest, dass das entsprechende Ereignis, das einen (erlaubten oder geblockten) Prozessstart meldet, im Knoten **EDR**, Unterknoten **Applikationskontrolle**, auch Kommandozeilenparameter anzeigen darf. Die Option ist standardmäßig deaktiviert.

   Hinweis: Beachten Sie dabei, dass die Kommandozeile sensible Daten, wie z.B. Passwörter, enthalten kann!

5.1.3 Angaben auf dem Reiter Nachrichten

Die Standard-Nachrichtentexte für die Applikationskontrolle, die auf dem DriveLock Agenten angezeigt werden, sind im Knoten **Globale Einstellungen**, Unterknoten **Mehrsprachige Benachrichtigungstexte**, Option **Sprachen / Standardnachrichten** auf dem Reiter **Applikationen** hinterlegt. Weitere Informationen zur Erstellung von Benachrichtigung finden Sie im Administrationshandbuch auf DriveLock Online Help.

1. Bei **Anwendungs-Verhaltensregeln** gibt es nur eine Option auf diesem Reiter, die standardmäßig aktiviert ist:
   - **Benachrichtigung anzeigen, wenn Zugriff verweigert wird**: Über die Dropdown-Liste können Sie einen Standardtext auswählen oder hier Ihren eigenen Text definieren, der beim Blockieren des Zugriffs angezeigt werden soll.

- Je nach Zugriffsmodus sind folgende Platzhalter dabei zulässig:
  - Zugriffsmodus Ausführen:
    %EXE% für den Namen der Anwendung; %PARENT% für den Namen des Programms, das die Anwendung startet
  - Alle anderen Zugriffsmodi:
    %EXE% für den Namen der Anwendung; %TARGET% für das Ziel des Zugriffs

2. Bei **Anwendungsregeln** gibt es drei Optionen:
   - **Speziellen Text bei Benutzerbenachrichtigung anzeigen**: Auch hier können Sie einen Standardtext auswählen oder Ihren eigenen Text definieren.
   - Wählen Sie die Option **Keine Benachrichtigung anzeigen (Anwendung ignorieren)** aus, wenn Sie den Benutzer nicht darüber informieren wollen, dass eine Anwendung (durch eine Blacklist) blockiert wird.
   - Standardmäßig werden Ereignisse erzeugt, wenn Anwendungen blockiert werden. Wenn Sie diese Ereignisse nicht benötigen, können Sie die Option **Keine Ereignisse für diese Anwendung erzeugen** auswählen.

5.1.4 Allgemeine Einstellungen für Regeln

Folgende Reiter kommen in verschiedenen Anwendungs- und Verhaltensregeln vor.

1. Reiter **Angemeldete Benutzer**:
   Als Standadoption ist die Regel aktiv für alle angemeldeten Benutzer und Gruppen.
2. Reiter **Computer**:
   - Legen Sie hier fest, auf welchen Computern die Regel gültig sein soll.
   - Sie können beispielsweise eine Verhaltensregel nur für eine spezielle Computer-Gruppe erstellen, in der Computer mit einer neueren Version des DriveLock Agenten gruppiert sind.
3. Reiter **Nachrichten**:
   Weitere Informationen zu den Optionen auf diesem Reiter für Anwendungsregeln bzw. Anwendungs-Verhaltensregeln finden Sie hier.
4. Reiter **Netzwerke**:
   Legen Sie hier fest, für welche aktiven Netzwerkverbindungen die Regel angewendet werden soll.
5. Reiter **Zeiten**:

- Wenn Sie möchten, dass die Regel nur für einen ganz bestimmten Zeitraum gelten soll, dann können Sie hier einen individuellen Zeitrahmen vorgeben (z.B. nur werktags von 09:00 Uhr bis 17:00 Uhr)
- Es ist ebenso möglich, ein Datum für den Beginn und das Ende der Gültigkeitsdauer anzugeben.
- Markieren Sie den gewünschten Zeitraum, indem Sie entweder ein einzelnes Feld aktivieren, oder jeweils links einen Wochentag oder oben eine Zeit anklicken. Zusätzlich wählen Sie für die Auswahl entweder **Regel aktiv** oder **Regel nicht aktiv**.

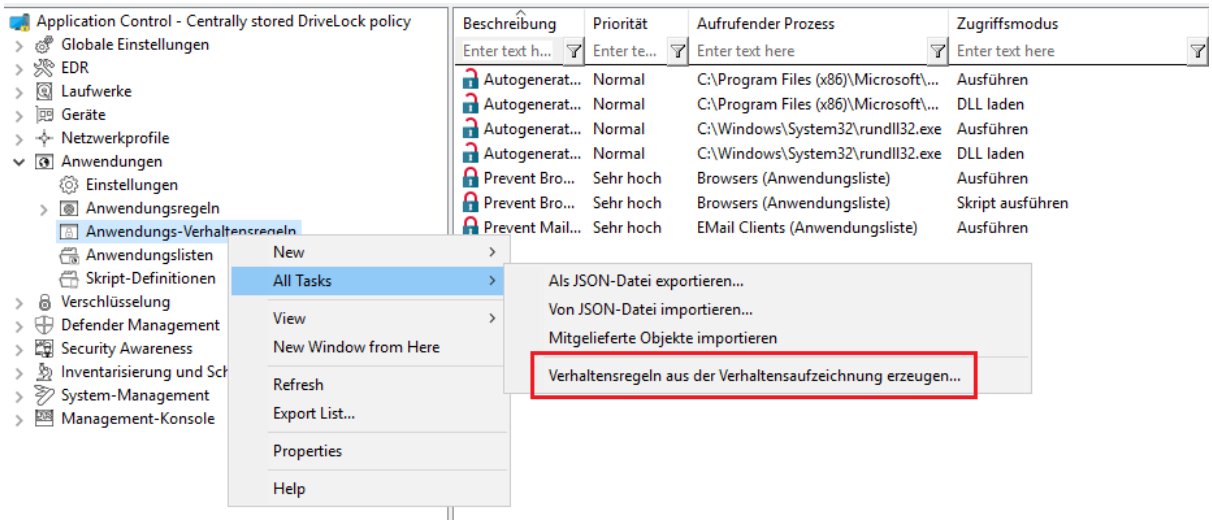
6. Reiter **Zugriffsrechte**:
   - Legen Sie hier fest, für welche Benutzer bzw. Gruppen die Regel aktiv sein soll.
   - Aktivieren Sie **Definierte Benutzer und Gruppen**, um die Regel nur für einen bestimmten Benutzerkreis zu aktivieren. Klicken Sie auf Hinzufügen, um eine weitere Gruppe oder einen Benutzer zur angezeigten Liste hinzuzufügen. Mit Entfernen wird der zuvor ausgewählte Eintrag gelöscht.

5.2 Anwendungs-Verhaltensregeln aus der Verhaltensaufzeichnung erzeugen

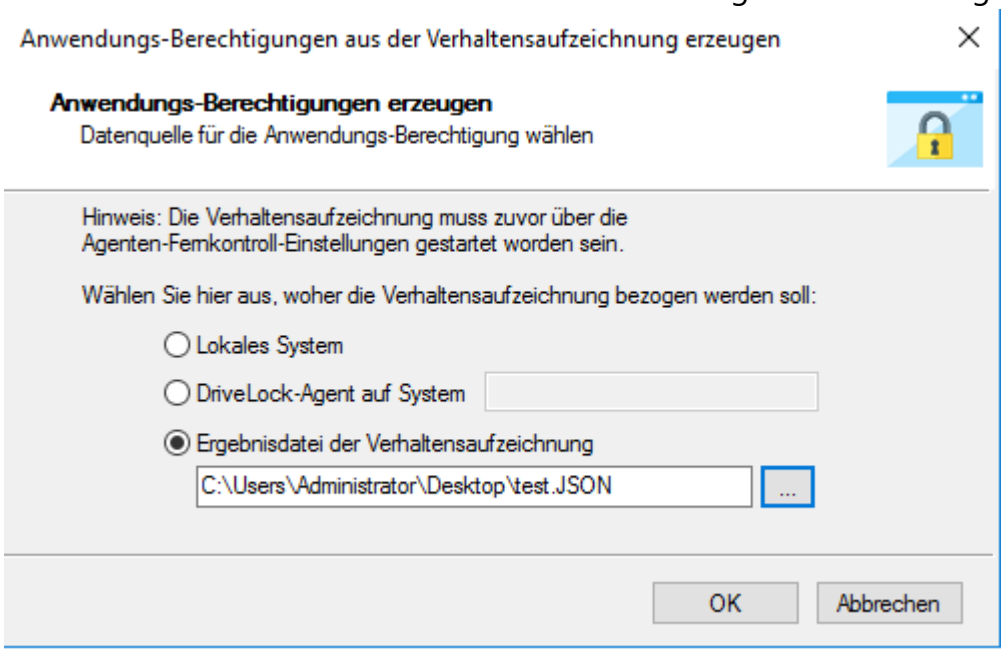
Da manche Programme für ihre Funktion Zugriffe benötigen, die für den Benutzer nicht unmittelbar erkennbar sind (Schreiben von temporären Dateien, Anlegen von Konfigurationsdateien oder Caches usw.), zeichnet DriveLock diese Zugriffe auf und erlaubt Ihnen, diese dadurch zu kontrollieren.

Um aus dem Ergebnis der Verhaltensaufzeichnung automatisiert Anwendungs-Verhaltensregeln erzeugen zu lassen, gehen Sie folgendermaßen vor:

1. Klicken Sie im Kontextmenü der **Anwendungs-Verhaltensregeln** unter Alle Aufgaben (All Tasks) auf den Menüpunkt **Verhaltensregeln aus der Verhaltensaufzeichnung erzeugen...** .

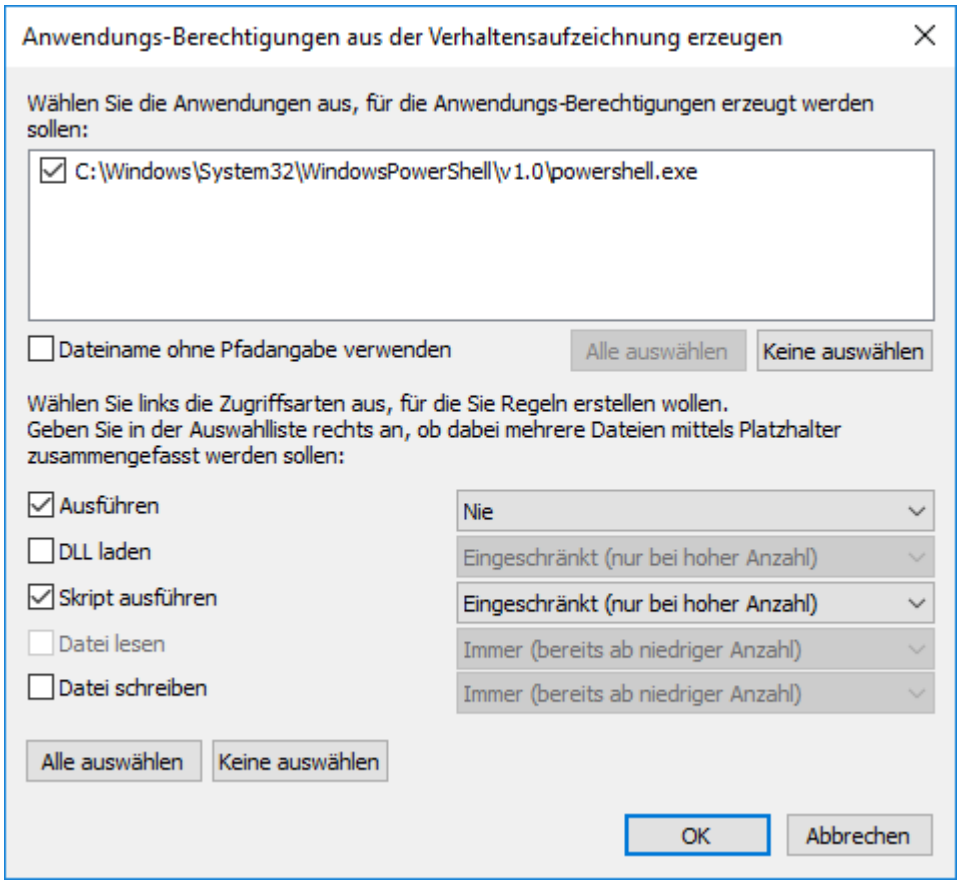


2. Wählen Sie im folgenden Dialog die Datenquelle für die Aufzeichnungsergebnisse aus. Diese können entweder vom DriveLock Agenten auf dem lokalen oder auf einem entfernten Rechner stammen oder aus einer bereits geschriebenen Ergebnisdatei.

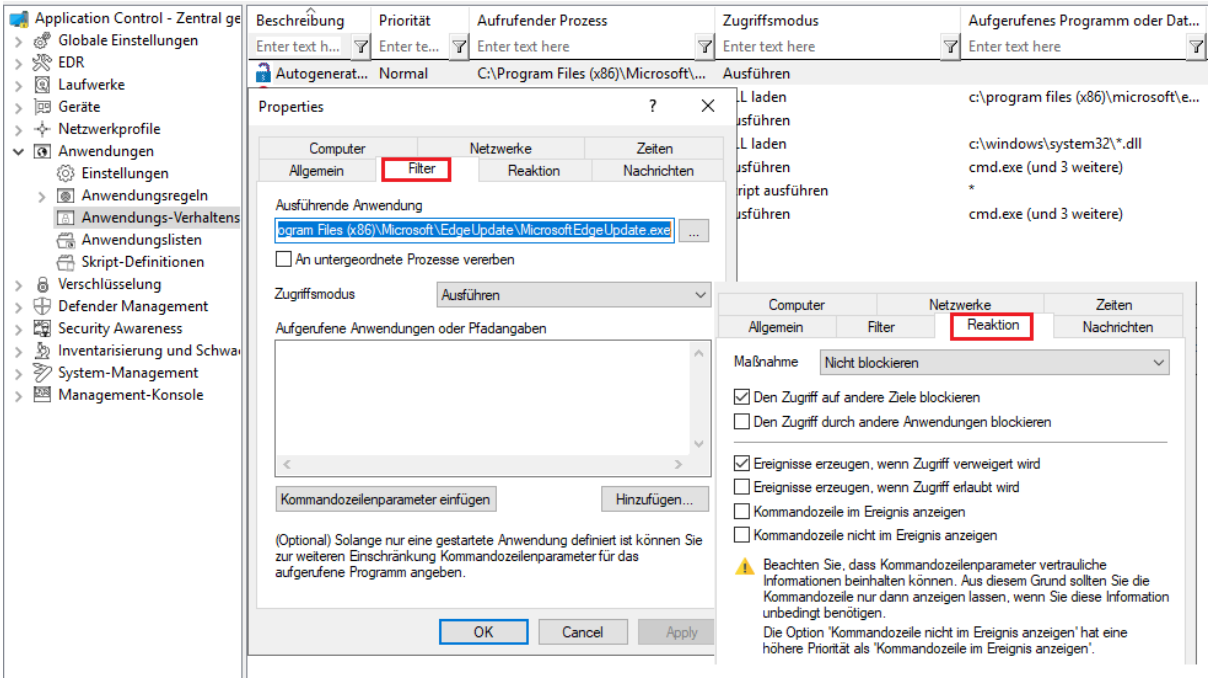


3. Im nächsten Dialog konfigurieren Sie folgendes:
   - Wählen Sie die Anwendung (auch mehrere) aus und legen Sie fest, ob der ganze Pfad oder nur die Datei unabhängig vom Ablageort verwendet werden soll. Im Fall von Browsern z.B. ist es sinnvoll, den Namen ohne Pfad zu verwenden.
   - Geben Sie an, für welche Zugriffsmodi Regeln erstellt und inwieweit dabei mehrere Dateien mittels Platzhaltern zusammengefasst werden sollen. Für den Zugriff **Ausführen** ist die Einstellung **Nie** sinnvoll, denn es handelt sich dabei um eine geringe Anzahl an Dateien (und daraus resultierend dann zu erstellenden Regeln), die nicht zusammengefasst werden müssen. Hingegen bei

Datei schreiben ist es **Immer (bereits ab niedriger Anzahl)** sinnvoll, Platzhalter einzusetzen und nicht für jede einzelne geschrieben Datei Regeln erstellen zu lassen.



4. Im nächsten Schritt werden die automatisch erzeugten Regeln als **Autogenerated rule** im Knoten **Anwendungs-Verhaltensregeln** angezeigt. Auf dem Reiter **Reaktion** wird ersichtlich, dass die ausführende Anwendung erlaubt ist (Nicht blockieren), alles anderen Zugriffe werden geblockt.



Tipp: Erstellen Sie einen eigenen Ordner für diese Anwendungs-Verhaltensregeln, damit sie einfach von den bereits bestehenden zu unterscheiden sind.

Fazit: Die automatische Erstellung von Anwendungs-Verhaltensregeln schafft ein deutlich schlankeres und übersichtlicheres Regelwerk und erspart aufwändiges Monitoring oder Analyse von Ereignissen.

6 Anwendungslisten

Anwendungslisten sind eine Sammlung von thematisch oder programmatisch zusammengehörenden Anwendungen, die Sie in den entsprechenden Verhaltens- oder Anwendungslisten-Regeln einsetzen können.

Anstatt für jede einzelne Anwendung eigene Regeln zu erstellen, erstellen Sie auf diese Weise eine Regel für mehrere Anwendungen (auf der Anwendungsliste) gleichzeitig. Somit reduziert sich Ihr Regelwerk und bleibt übersichtlich.

Beispiel: Drei Anwendungs-Verhaltensregeln sollen für jeweils drei Anwendungen gelten:

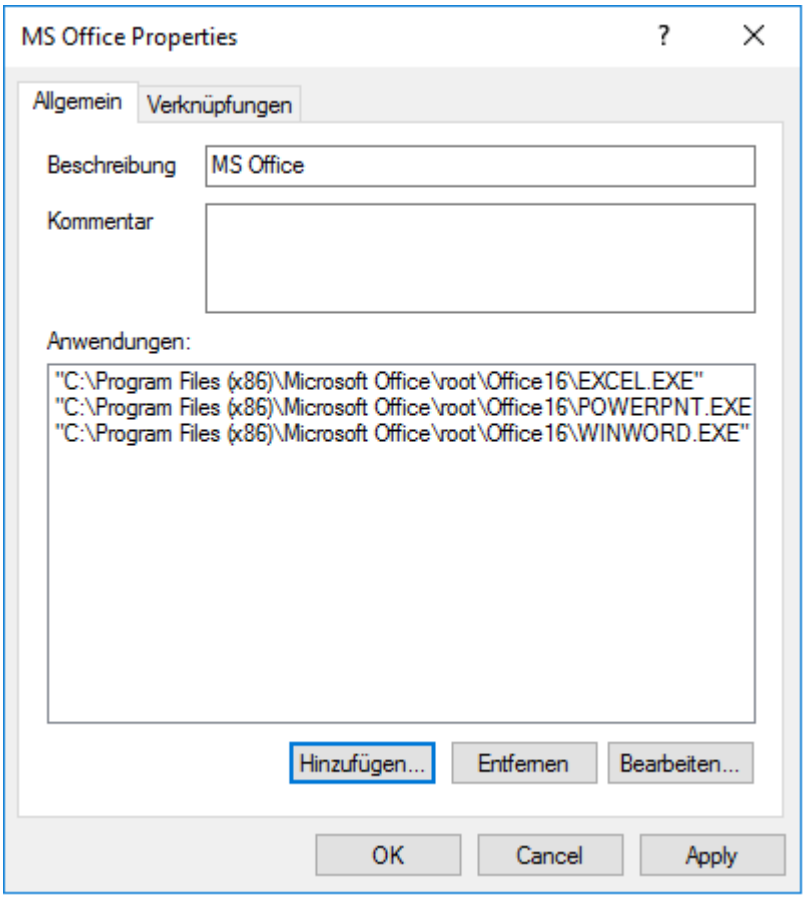
- In Regel 1 bestimmen Sie, dass beim Start der Anwendungen keine weiteren Anwendungen gestartet werden dürfen.
- In Regel 2 bestimmen Sie, dass die Anwendungen nicht in ein bestimmtes Verzeichnis schreiben dürfen.
- In Regel 3 bestimmen Sie, dass die Anwendungen nur Textdateien in ein bestimmtes Verzeichnis schreiben dürfen.

Hinweis: Durch Verwendung von Listen lässt sich die Anzahl der Regeln reduzieren.

Erstellen Sie Anwendungslisten anhand des folgenden Beispiels oder verwenden Sie die mitgelieferten Anwendungslisten, die Ihnen in der Taskpad-Ansicht angeboten werden.

6.1 Anwendungsliste für Microsoft Office-Produkte

Szenario: Sie wollen verschiedene Microsoft Office-Produkte in einer Anwendungsliste gruppieren, um diese dann in Anwendungs-Verhaltensregeln oder Anwendungslisten-Regeln verwenden zu können.



1. Wählen Sie den Unterknoten **Anwendungslisten** und öffnen Sie das Kontextmenü.
2. Wählen Sie **Neu** und dann **Anwendungsliste**.
3. Geben Sie eine eindeutige Beschreibung ein, hier MS Office.
4. Optional können Sie einen **Kommentar** eingeben.
5. Über die Schaltfläche **Hinzufügen** fügen Sie die Pfade zu den von Ihnen gewünschten Anwendungen hinzu. Sie können später Anwendungen entfernen oder die Pfade bearbeiten.
6. Speichern Sie Ihre Liste und verwenden Sie diese jetzt in Anwendungs-Verhaltensregeln.

Auf dem Reiter **Verknüpfungen** werden die Verhaltens- und Anwendungsregeln angezeigt, für die diese Liste verwendet wird.

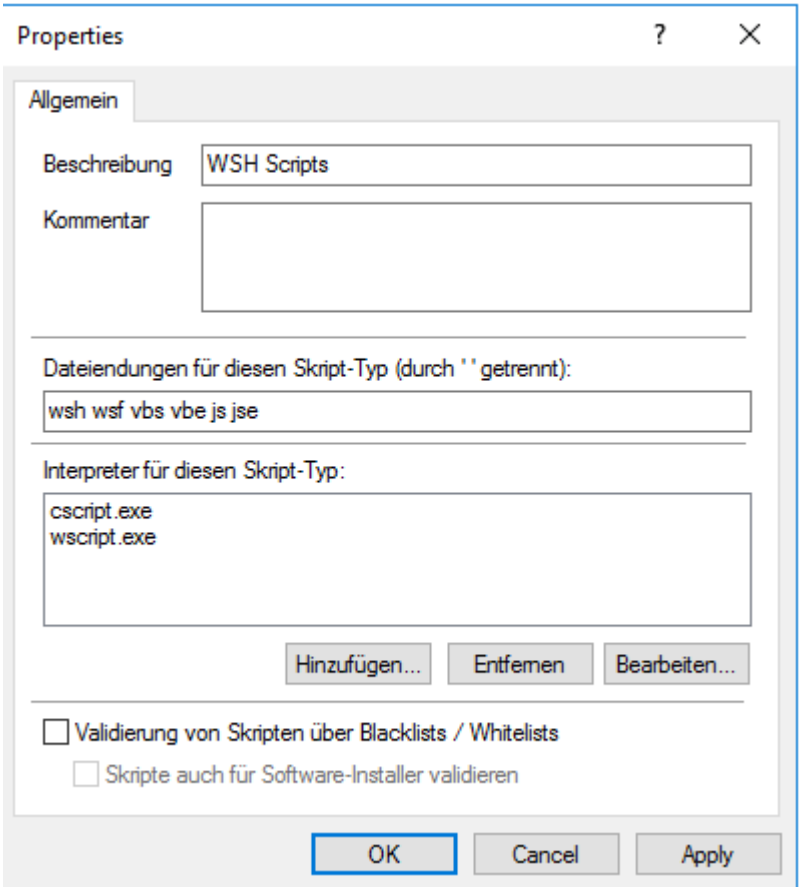
7 Skript-Defintionen

Um den Zugriffsmodus Skript ausführen bei den Anwendungs-Verhaltensregeln verwenden zu können, müssen Sie die entsprechenden Skript-Typen definieren.

Mit dieser Definition erhält die Anwendungskontrollfunktion von DriveLock die Information, welche Dateizugriffe als Skriptausführung zu interpretieren sind.

Gehen Sie folgendermaßen vor:

1. Öffnen Sie das Kontextmenü des Unterknotens **Skript-Definitionen**.
2. Klicken Sie auf **Neu** und erstellen dann in folgendem Dialog Ihre Definition.
   Im Anwendungsfall wird Windows Scripting Host näher definiert:



3. Im Textfeld **Dateiendungen für diesen Skript-Typ** geben Sie die entsprechenden Dateiendungen an. Trennen Sie diese nur durch ein Leerzeichen.
4. Im Textfeld **Interpreter für diesen Skript-Typ** geben Sie an, welche Interpreter Windows Scripting Host Skripte lesen können.
5. Mit der Option **Validierung von Skripten über Blacklists / Whitelists** können Sie festlegen, dass Skripte auf dieselbe Art und Weise in Black- oder Whitelists überprüft

werden, wie das für DLL- oder EXE-Dateien der Fall ist. Weitere Informationen zu Black- bzw. Whitelisting erhalten Sie in den entsprechenden Kapiteln.

6. Die Option **Skripte auch für Software-Installer validieren** verwenden Sie, wenn die Validierung auch für Skripte gelten soll, die durch Software-Update-Prozesse gestartet werden.
   Beispiel: msiexec.exe ist als vertrauenwürdiger Installer darf nur dann gestartet werden, wenn die entsprechende MSI-Datei auch vertrauenwürdig ist.
   Die Einstellung Vertrauenswürdiger Prozess bietet die Option, eine feste Liste für diese Prozesse zu erstellen.

8 Beispiele

8.1 Anwendungs-Verhaltensregeln

8.1.1 Anwendungsfall 1: Starten von PowerShell verhindern

Szenario: Sie wollen verhindern, dass bei der Verwendung eines Browsers (hier Internet Explorer) beim Benutzer Powershell gestartet wird und womöglich Schadsoftware auf den Agenten-Computern einspielt.

1. Geben Sie auf dem Reiter **Allgemein** eine eindeutige Beschreibung ein und fügen ggf. einen **Kommentar** hinzu. Da es sich um eine relativ allgemeine 'Regel' handelt, geben Sie in diesem Fall eine niedrige **Priorität** an. Durch das Häkchen ist die **Regel aktiv**.
2. Auf dem Reiter **Filter** geben Sie folgendes an:
   - Als **Ausführende Anwendung** wird hier im Beispiel der gesamte Pfad zur iexplore.exe angegeben. Alternativ könnten Sie hier auch eine Anwendungsliste verwenden, in der Sie verschiedene Browser angegeben haben.
   - Setzen Sie ein Häkchen bei **An untergeordnete Prozesse vererben**, um zu verhindern, dass der Browser die Powershell.exe von der Kommandozeile (cmd.exe) aus aufrufen kann (hierbei handelt es sich um einen untergeordneten Prozess).
   - Weil Sie verhindern wollen, dass Powershell vom Internet Explorer aus ausgeführt wird, geben Sie als **Zugriffsmodus** Ausführen an.
   - Unter **Aufgerufene Anwendung oder Pfadangabe** wählen Sie hier entweder eine Datei oder einen Ordner aus, z.B. hier als Dateiname powershell.exe.

   > Hinweis: Bei Blockier-Regeln ist es sinnvoll nur den Dateinamen anzugeben, um alle Vorkommnisse einschließen zu können. Bei der Angabe des vollen Pfades müssen Sie beachten, dass teilweise mehrere Versionen eines Programms existieren, z.B. könnte die powershell.exe in zwei verschiedenen Verzeichnissen liegen C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe oder in C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.

3. Auf dem Reiter **Reaktion** geben Sie folgendes an:
   - Als Maßnahme wollen Sie den Aufruf **Blockieren**.
4. Bei allen anderen Optionen lassen Sie die Standardeinstellungen.

Fazit: Immer wenn die Datei iexplore.exe aufgerufen wird und dabei versucht, PowerShell zu starten, wird es geblockt.

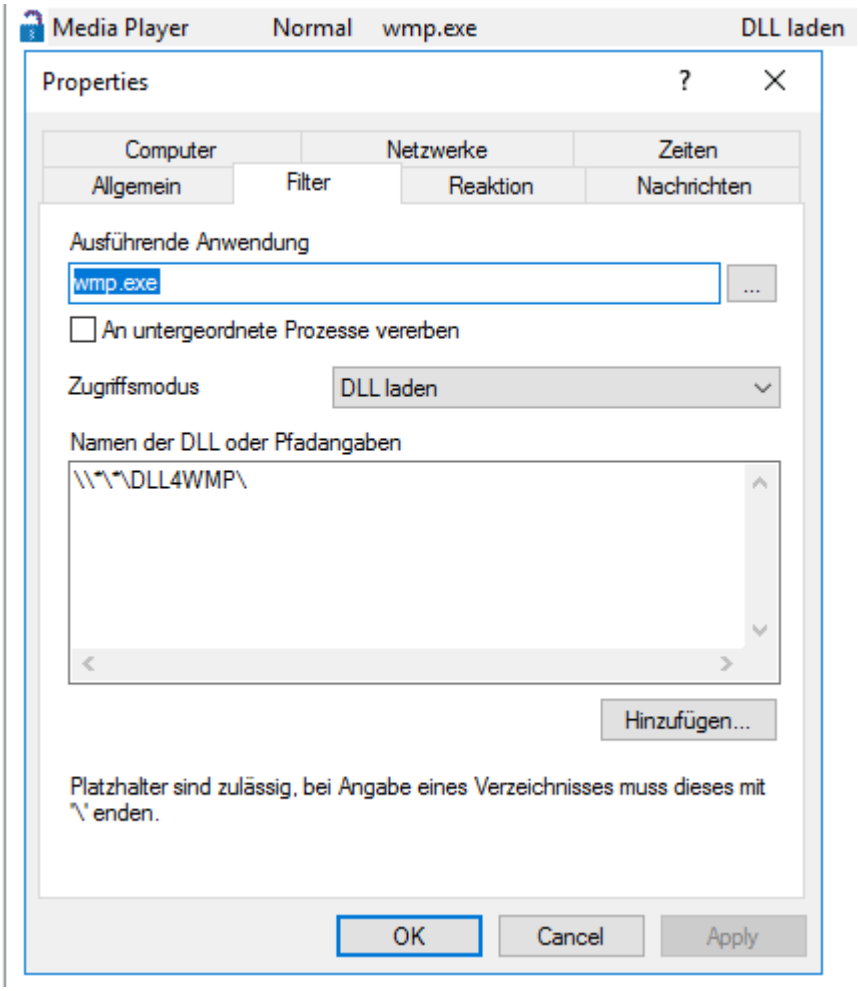
8.1.2 Anwendungsfall 2: Laden einer DLL einschränken

Szenario: Sie wollen festlegen, dass DLLs nur aus bestimmten Verzeichnissen geladen werden dürfen.

Im konkreten Fall soll verhindert werden, dass der Windows Media Player DLLs von Netzlaufwerken lädt.

Gehen Sie wie in der Abbildung angegeben vor:

1. Erstellen Sie eine Anwendungs-Berechtigung, in der Sie angeben, dass die Windows Media Player-Anwendung wmp.exe nur DLLs aus dem Verzeichnis **\DLL4WMP\ laden darf.



2. Wählen Sie auf dem Reiter **Reaktion** folgende Optionen aus:

- Wählen Sie als Maßnahme **Nicht Blockieren** aus und setzen Sie ein Häkchen bei **Den Zugriff auf andere Ziele blockieren**, um sicherzustellen, dass die DLL ausschließlich aus dem angegebenen Ziel geladen werden darf.
- Wählen Sie **Ereignisse erzeugen, wenn Zugriff erlaubt wird**.

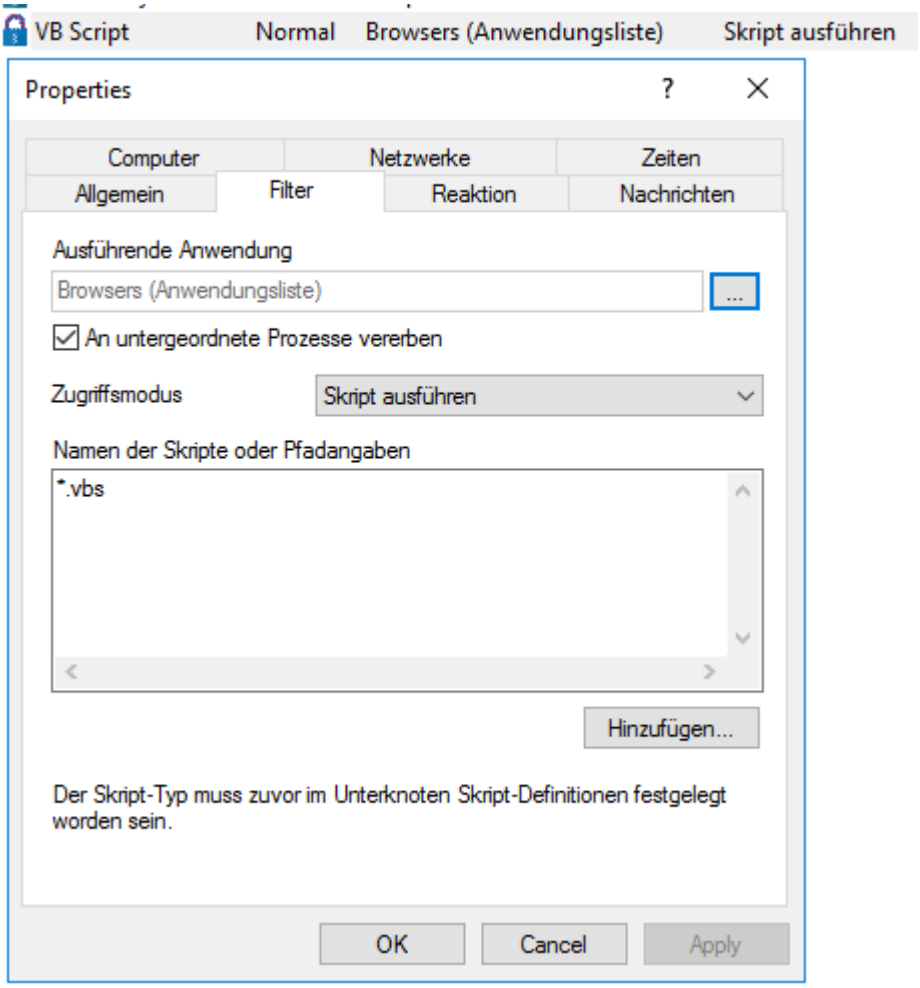
Hinweis: Beachten Sie, dass Regeln mit 'Nicht blockieren' (also Erlauben) Vorrang vor 'Blockieren' haben!

8.1.3 Anwendungsfall 3: Ausführen von Skripten

Szenario: Sie wollen verhindern, dass VB Skripte (*.vbs) von Browsern ausgeführt werden.

Gehen Sie wie in der Abbildung angegeben vor:

1. Wählen Sie als **Ausführende Anwendung** die Anwendungsliste, die Sie für Ihre Browser erstellt haben.
2. Sie können die Option **An untergeordnete Prozesse vererben** in diesem Fall setzen. Dadurch lässt sich verhindern, dass das angegebene VB-Skript aus einem untergeordneten Prozess (z.B. aus der Kommandozeile) heraus gestartet wird.



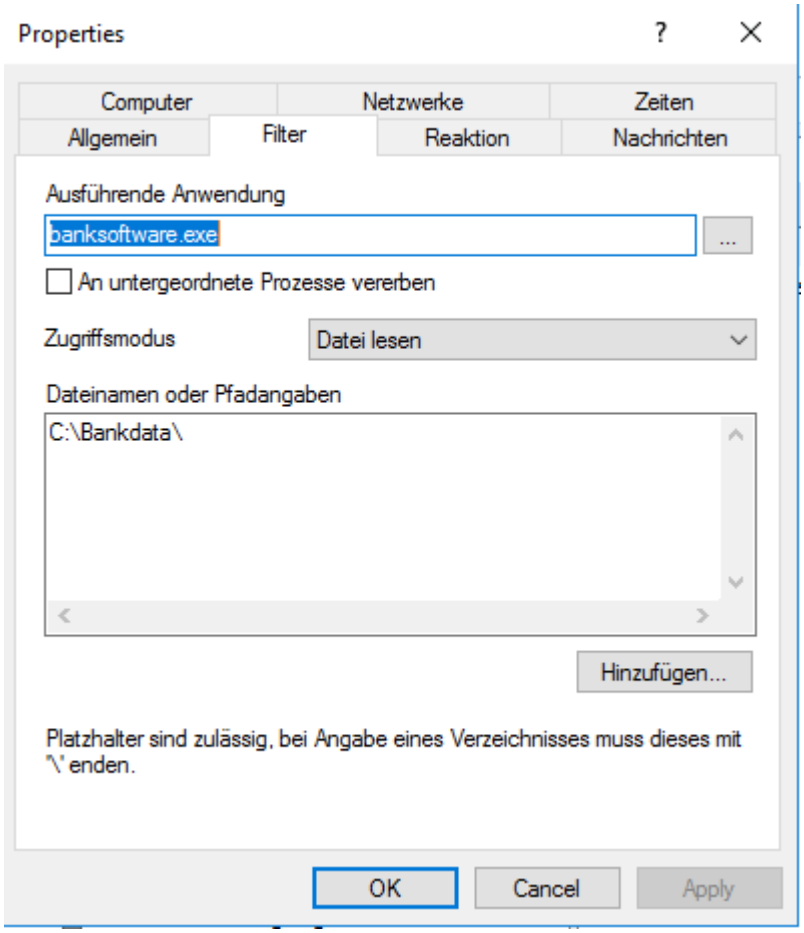
3. Auf dem Reiter **Reaktion** wählen Sie als Maßnahme **Blockieren**.
4. Bei allen anderen Optionen lassen Sie die Standardeinstellungen.

8.1.4 Anwendungsfall 4: Lesen eines bestimmten Verzeichnisses

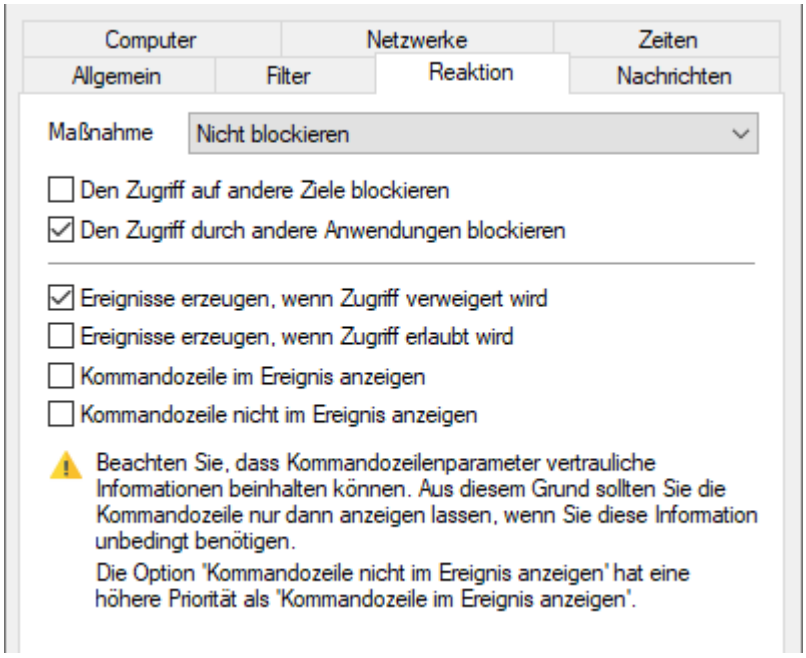
Szenario: Sie wollen sicherstellen, dass nur Ihre eigene Bank-Anwendung lesend auf ein ganz bestimmtes Verzeichnis zugreifen kann. Keine andere Anwendung soll Lesezugriff auf dieses Verzeichnis erhalten. Durch eine Sicherheitslücke im Browser wäre es möglich, dass eine Schadsoftware sich Lesezugriff auf dieses Verzeichnis verschafft und somit Ihre Bankdaten auslesen kann. Das muss verhindert werden.

Gehen Sie wie in der Abbildung angegeben vor:

1. Geben Sie auf dem Reiter **Allgemein** eine eindeutige Beschreibung ein und fügen ggf. einen **Kommentar** hinzu.
2. Auf dem Reiter **Filter** geben Sie als **Ausführende Anwendung** Banksoftware.exe an. Als **Zugriffsmodus** wählen Sie **Datei lesen** und unter **Dateinamen** geben Sie den Pfad an (im Beispiel C:\Bankdaten\).



3. Auf dem Reiter **Reaktion** wählen Sie folgende Optionen:
   - Wählen Sie als Maßnahme **Nicht Blockieren** aus und setzen Sie bei **Den Zugriff durch andere Anwendungen blockieren** ein Häkchen, um sicherzustellen, dass ausschließlich ihre eigene Banksoftware Lesezugriff auf das angegeben Ziel hat.
   - Lassen Sie die Standardeinstellung **Ereignisse erzeugen, wenn Zugriff verweigert wird**.

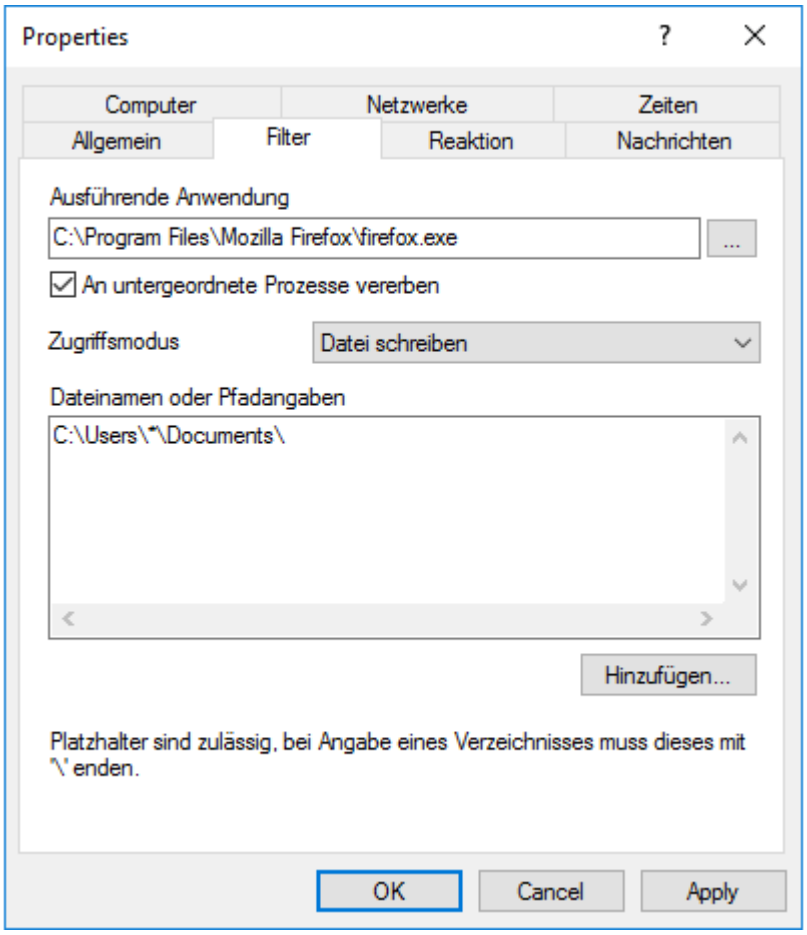


8.1.5 Anwendungsfall 5: Schreiben in ein bestimmtes Verzeichnis

Szenario: Sie wollen festlegen, dass ein bestimmter Browser nicht in den Ordner Documents schreiben darf. Da Sie dies nicht nur für bestimmte Benutzer festlegen wollen, sondern für alle, verwenden Sie einen Platzhalter.

Gehen Sie wie in der Abbildung angegeben vor:

1. Geben Sie auf dem Reiter **Allgemein** eine eindeutige Beschreibung ein und fügen ggf. einen **Kommentar** hinzu.
2. Auf dem Reiter **Filter** wählen Sie als **Ausführende Anwendung** den Pfad zum Browser aus.
   - Um zu verhindern, dass der Browser über untergeordnete Prozesse trotzdem in das Verzeichnis schreiben kann, setzen Sie das entsprechende Häkchen.
   - Als **Zugriffsmodus** wählen Sie **Datei schreiben** und unter **Dateinamen** geben Sie den Pfad mit Platzhalter an (im Beispiel C:\Users*\Documents\).



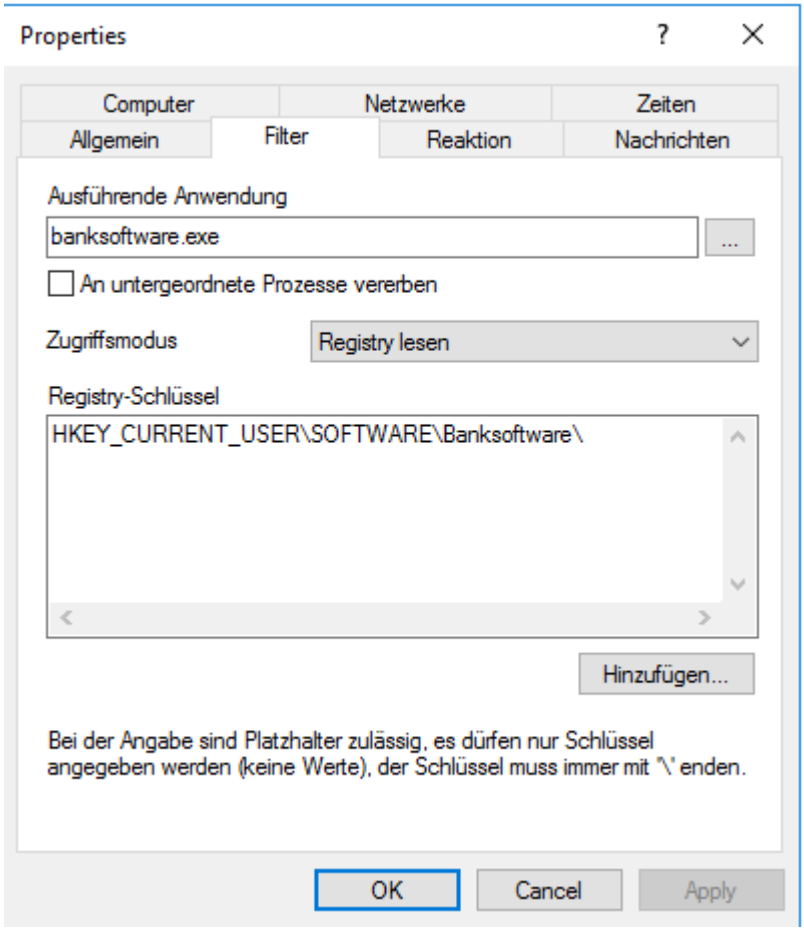
3. Auf dem Reiter **Reaktion** wählen Sie als Maßnahme **Blockieren**.
4. Bei allen anderen Optionen lassen Sie die Standardeinstellungen.

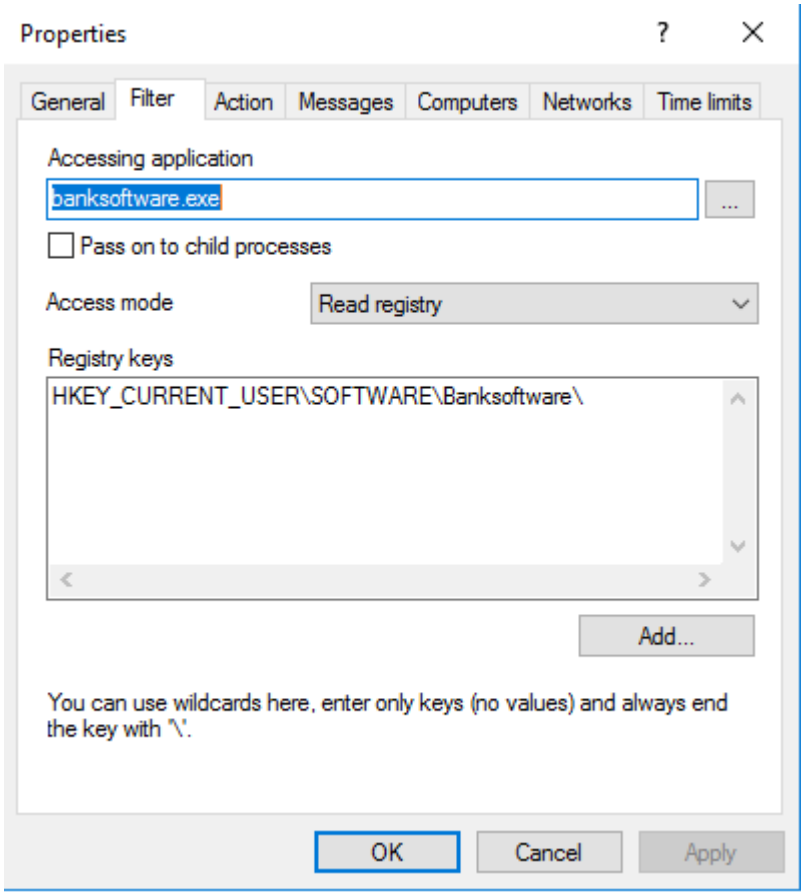
8.1.6 Anwendungsfall 6: Registry-Zugriff beschränken

Szenario: Sie wollen den Registry-Zugriff für Ihre Banksoftware aus Anwendungsfall 4 regeln. Damit nur die Banksoftware.exe die Registry unter dem angegebenen Registry-Schlüssel lesen kann, erstellen Sie folgende Anwendungs-Berechtigung.

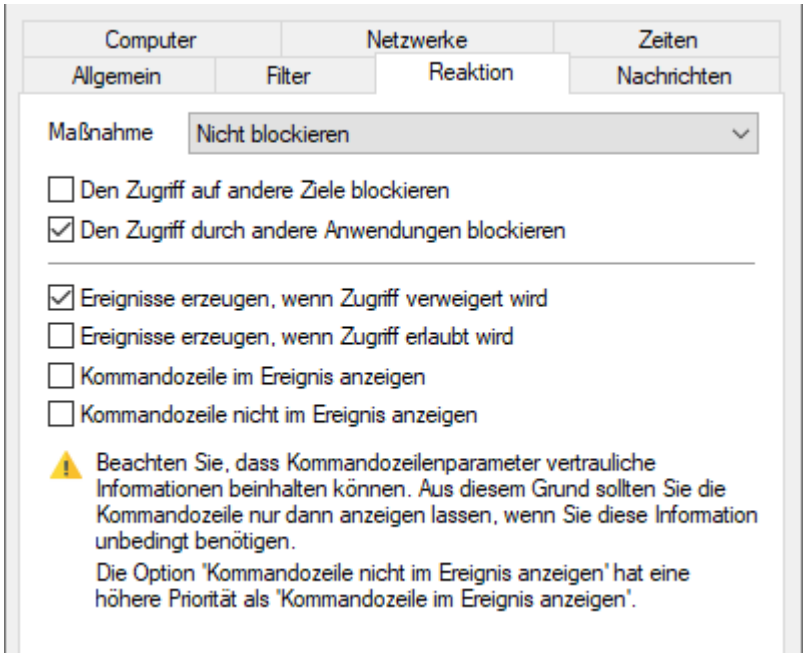
Gehen Sie wie in der Abbildung angegeben vor:

1. Geben Sie auf dem Reiter **Allgemein** eine eindeutige Beschreibung ein und fügen ggf. einen **Kommentar** hinzu.
2. Auf dem Reiter **Filter** geben Sie als **Ausführende Anwendung** banksoftware.exe an. Als **Zugriffsmodus** wählen Sie **Registry lesen** und unter **Registry-Schlüssel** geben Sie den Schlüssel an (im Beispiel HKEY_CURRENT_USER\SOFTWARE\Banksoftware\).


Properties
Computer
Netzwerke
Zeiten
Allgemein
Filter
Reaktion
Nachrichten
Ausführende Anwendung
banksoftware.exe
...
An untergeordnete Prozesse vererben
Zugriffsmodus
Registry lesen
Registry-Schlüssel
HKEY_CURRENT_USER\SOFTWARE\Banksoftware\
Hinzufügen...
Bei der Angabe sind Platzhalter zulässig, es dürfen nur Schlüssel angegeben werden (keine Werte), der Schlüssel muss immer mit '\' enden.
OK
Cancel
Apply


Properties
General
Filter
Action
Messages
Computers
Networks
Time limits
Accessing application
banksoftware.exe
...
Pass on to child processes
Access mode
Read registry
Registry keys
HKEY_CURRENT_USER\SOFTWARE\Banksoftware\
Add...
You can use wildcards here, enter only keys (no values) and always end the key with '\'.
OK
Cancel
Apply

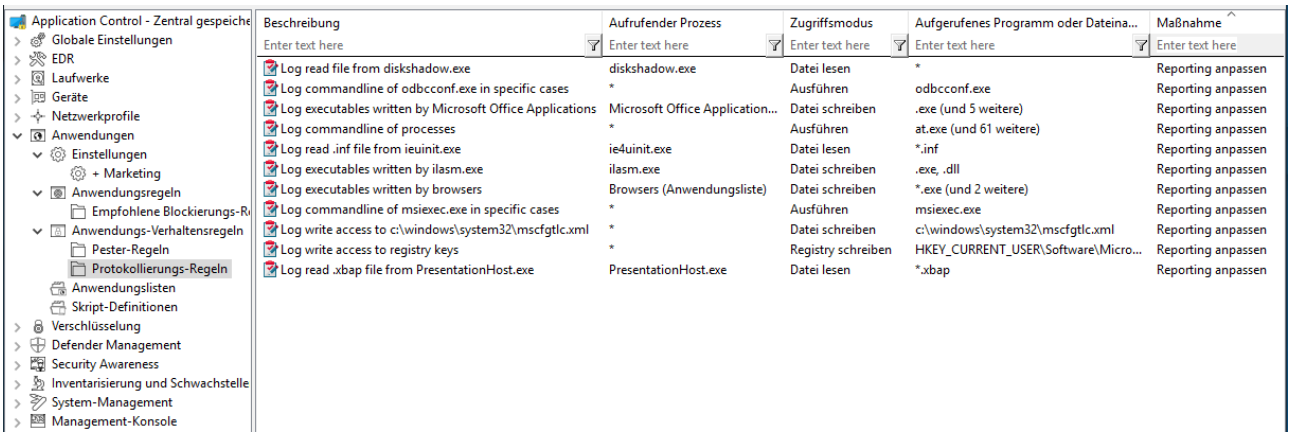
3. Auf dem Reiter **Reaktion** wählen Sie folgende Optionen:
   - Wählen Sie als Maßnahme **Nicht Blockieren** aus und setzen Sie bei **Den Zugriff durch andere Anwendungen blockieren** ein Häkchen, um sicherzustellen, dass ausschließlich ihre eigene Banksoftware Lesezugriff auf den Registry-Schlüssel hat.
   - Lassen Sie die Standardeinstellung **Ereignisse erzeugen, wenn Zugriff verweigert wird**.



8.1.7 Anwendungsfall 7: Angriffe erkennen am Beispiel von MITRE ATT&CK™ Regeln

DriveLock liefert Regeln mit, die auf dem auf dem MITRE ATT&CK-Framework basieren. Diese Regeln können Sie im Knoten **EDR** importieren.

Einige dieser Regeln werden im Knoten **Anwendungs-Verhaltensregeln** in separaten Ordnern gespeichert, siehe Abbildung.



Hinweis: Diese Regeln dienen nicht dazu, Aktionen zu blockieren oder zu erlauben, sondern sie melden lediglich bestimmte Ereignisse auf dem jeweiligen Computer, die anschließend von den Event-Filtern und Alerts verarbeitet werden.

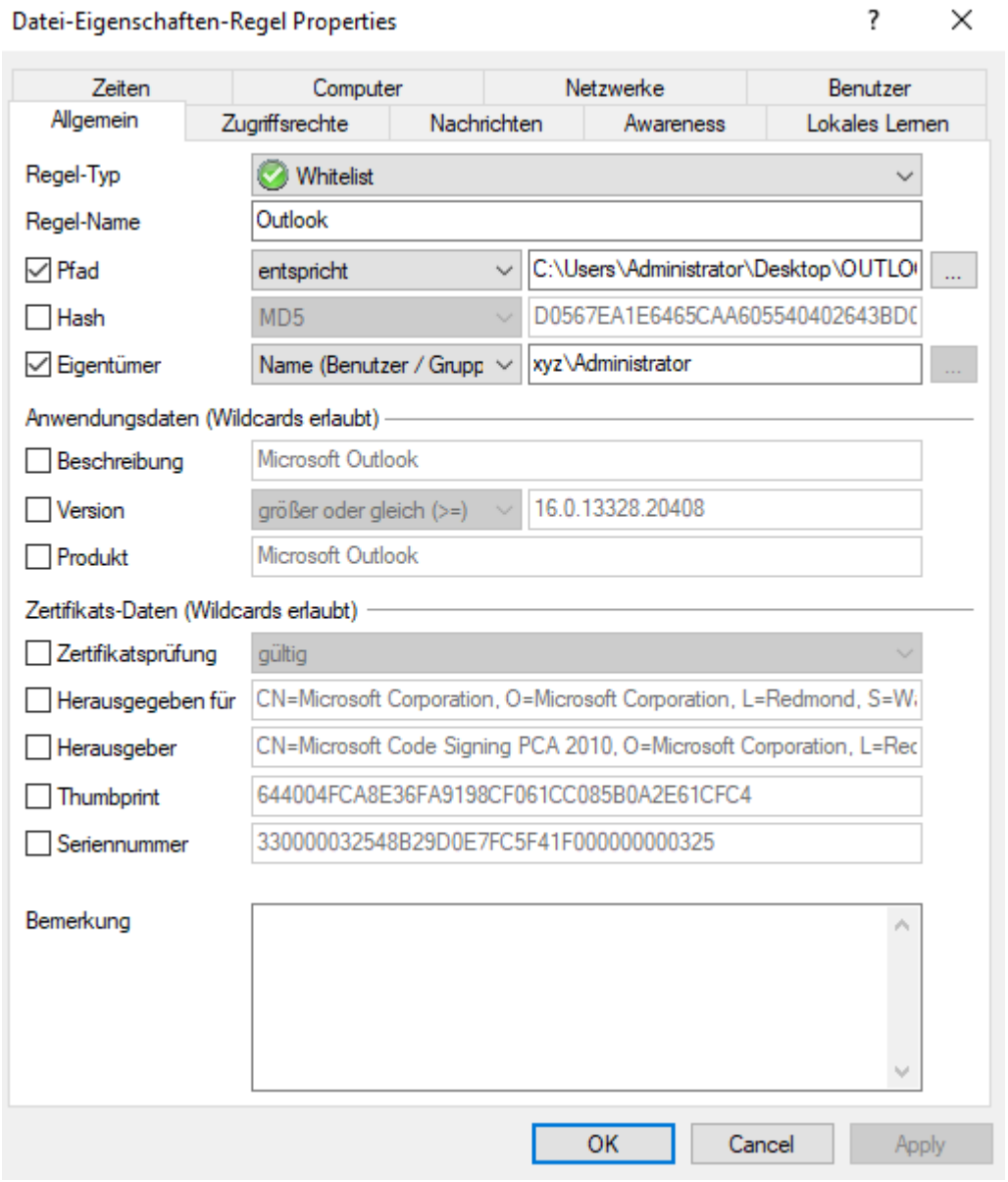
8.2 Anwendungsregeln

8.2.1 Anwendungsfall 8: Security-Awareness-Kampagne beim Starten von Outlook anzeigen

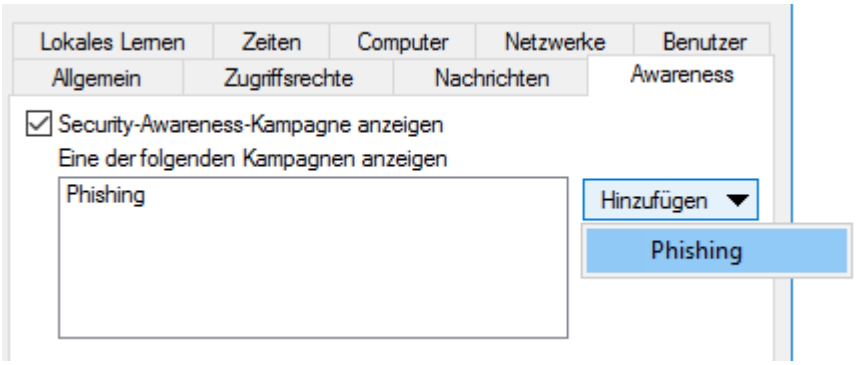
Szenario: Sie wollen eine Security-Awarenss-Kampagne immer dann anzeigen lassen, wenn der Benutzer Outlook startet. Erstellen Sie zu diesem Zweck eine neue Datei-Eigenschaften-Regel.

Gehen Sie wie in der Abbildung angegeben vor:

1. Geben Sie auf dem Reiter **Allgemein** folgendes an:
   - **Regel-Typ**: Lernen und Awareness
   - **Regel-Name**: Outlook
   - Suchen Sie den entsprechenden Pfad aus. Die anderen Felder werden automatisch ausgefüllt.
   - Wählen Sie aus, nach welchen Filtern Sie die Regel erstellen wollen und setzen Sie die entsprechenden Häkchen.
   - Geben Sie ggf. eine **Bemerkung** hinzu.



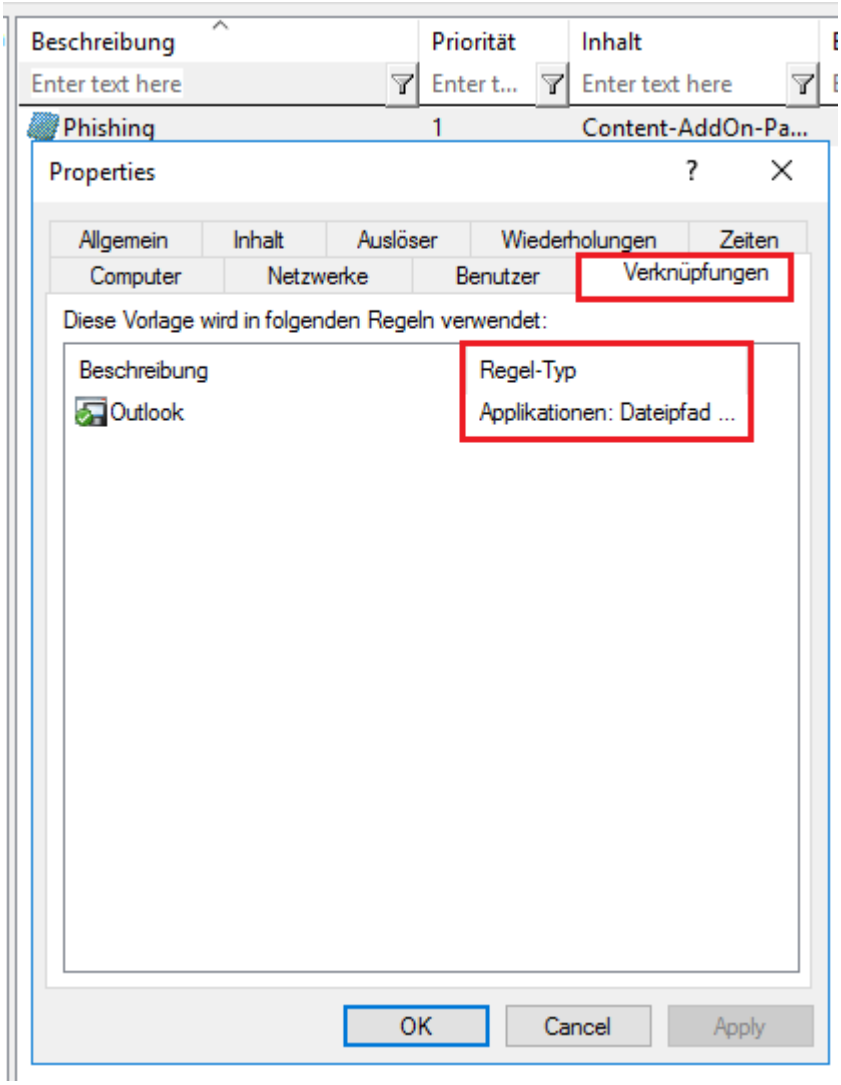
2. Öffnen Sie den Reiter **Awareness**.



Wählen Sie die entsprechende Kampagne in der Dropdown-Liste unter **Hinzufügen** aus.

Hinweis: Beachten Sie, dass zuvor im Eigenschaftendialog der Security-Awareness-Kampagne auf dem Reiter **Auslöser** die Option **Bei Verwendung in Regeln** gesetzt sein muss.

In der Security-Awareness-Kampagne **Phishing** wird auf dem Reiter **Verknüpfungen** folgende Information gezeigt:



Hinweis: Weitere Informationen zur Erstellung von Security-Awareness-Kampagnen finden Sie in der entsprechenden Dokumentation auf DriveLock Online Help.

3. Bei allen anderen Optionen können Sie die Standardeinstellungen belassen.

9 Begriffserklärungen

Begriff	Erklärung
Anwendungsliste	Eine Gruppierung mehrerer thematisch oder programmatisch zusammengehöriger Anwendungen. Die Anwendungsliste wird eingesetzt in der gleichnamigen Regel oder in der Anwendungs-Verhaltensregel.
Anwendungsregeln	Mit Anwendungsregeln können einzelne Anwendungen erlaubt oder blockiert werden, sowie lokales Lernen und die Anzeige von Awareness-Kampagnen konfiguriert werden.
Anwendungsverhalten	Anwendungsverhalten beinhaltet alle Aktionen, die eine Anwendung durchführt, z.B. Starten von zusätzlichen Anwendungen oder DLLs, Schreiben in bestimmte Verzeichnisse.
Anwendungs-Verhaltenskontrolle	Überwachung des Anwendungsverhaltens: DriveLock kontrolliert, was eine Anwendung auf dem Agenten tun darf.
Anwendungs-Verhaltensregel	Anwendungs-Verhaltensregeln bestimmen, welche Aktionen eine Anwendung ausführen darf oder nicht (z.B. ob sie andere Programme starten, DLLs laden, Dateien und Registry lesen/schreiben, Skripte ausführen darf).
Blacklist	Negativliste, die nicht zulässige und nicht vertrauenswürdige Ziele enthält. Durch Blacklisting lassen sich gezielt Anwendungen verbieten.
Lokales Lernen	Während einer Lernphase lernt der DriveLock Agent, was auf dem jeweiligen Client-Computer erlaubt ist: Anwendungen oder DLLs starten oder Aktionen durchführen, wie z.B. Schreiben in bestimmte Verzeichnisse.
Lokale Whitelist	Die lokale Whitelist ist eine lokal erzeugte Hashdatenbank-Regel. Sie kann initial befüllt werden mit ausführbaren (erlaubten) Dateien in bestimmten

Begriff	Erklärung
	Verzeichnissen und entsprechend erweitert werden.
Simulationsmodus	Während einer Simulation erzeugt DriveLock anhand konfiguriertet Regeln Ereignismeldungen für gestartete oder blockierte Anwendungen, die Ausführung selbst wird dabei aber weder erlaubt noch verhindert.
Verhaltensaufzeichnung	Aufzeichnung des Anwendungsverhaltens auf dem DriveLock Agenten zum Speichern als JSON-Datei und daraus Generierung von Anwendungs-Verhaltensregeln.
Whitelist	Positivliste, die erlaubte und vertrauenswürdige Ziele enthält. Ausschließlich diese dürfen ausgeführt werden.

Copyright