# DriveLock Security Awareness

## Handbuch 2020.2

DriveLock SE 2021

# Inhaltsverzeichnis

# 1 Willkommen bei DriveLock Security Awareness

Security Awareness ist als Feature der DriveLock Endpoint Protection Plattform standardmäßig in DriveLock-Produkten enthalten.

Smart SecurityEducation konzentriert sich ganz auf das Security-Awareness-Feature. Die DriveLock Funktionalitäten zur Laufwerks-, Geräte oder Applikationskontrolle stehen dabei nicht zur Verfügung.

Ob Sie nun Security Awareness innerhalb Ihrer gewohnten DriveLock-Umgebung verwenden oder mit Smart SecurityEducation nur sicherheitsrelevante Kampagnen verteilen wollen, sind Sie bestens ausgerüstet, um Ihrem Team sicherheitsrelevante Themen nahezubringen und das Sicherheitsbewußtsein zu schärfen.

Minimieren Sie mit Security Awareness die Gefahren für Ihre IT-Sicherheit!

# 2 Konzepte

## 2.1 DriveLock Security Awareness

Die in DriveLock verwendeten Security-Awareness-Kampagnen setzen sich aus Texten in unterschiedlichen Formaten (RTF, PDF, Text), Bildern, Videos, Web-Inhalte oder E-Learning-Modulen zusammen. Sie werden verwendet, um Benutzern gezielt Sicherheitsinformationen zukommen zu lassen, sie auf konkrete Ereignisse hinzuweisen, Anweisungen weiterzugeben und ihnen erforderliche Trainings zuzuweisen.

Security-Awareness-Kampagnen können so konfiguriert werden, dass sie zu bestimmten Zeitpunkten und bei bestimmten Ereignissen angezeigt werden, beispielsweise beim Einloggen eines Benutzers an seinem Rechner oder beim Verbinden eines Smartphones, Start einer Applikation, Einstecken eines USB-Sticks oder Verbinden eines externen Laufwerks. Sie lassen sich aber auch so konfigurieren, dass sie ohne bestimmtes Ereignis bei Benutzern angezeigt werden oder selbst vom Benutzer 'ad hoc' aufgerufen werden können. Die Häufigkeit der Anzeige lässt sich auch einstellen.

Um sicherzustellen, dass die Sicherheitsinformationen ihr Ziel erreicht haben und die Benutzer sich mit den Inhalten auseinandergesetzt haben, kann eine Bestätigung angefordert werden.

> Hinweis: Beim Einsatz der vollständigen DriveLock-Funktionalität können Kampagnen individuell für Laufwerke, Geräte und Applikationen innerhalb von Regeln definiert werden.

Wie Sie Kampagnen erstellen lesen Sie im Kapitel Security-Awareness-Kampagnen erstellen.

## 2.2 Das Security Awareness Content AddOn

Dieses lizenzierungspflichtige AddOn beinhaltet zusätzliche multimediale Inhalte (als komplette Sicherheitstrainings), mit denen Kampagnen erstellt werden können. Es kann ab DriveLock Version 7.8 mit dem bestehenden Security-Awareness-Feature sowie in Smart SecurityEducation verwendet werden. Die Inhalte werden auf Abonnement-Basis regelmäßig und automatisch über das Internet aktualisiert.

Wie die Aktualisierung der Content-AddOn-Pakete über den DriveLock Enterprise Service (DES) funktioniert, sehen Sie hier.

### 2.2.1 Lizensierung des Security Awareness Content AddOns

Um das Security Awareness Content AddOn zu lizensieren und so den zusätzlichen Kampagneninhalt in Form von Content-AddOn-Paketen nutzen zu können, gehen Sie wie folgt

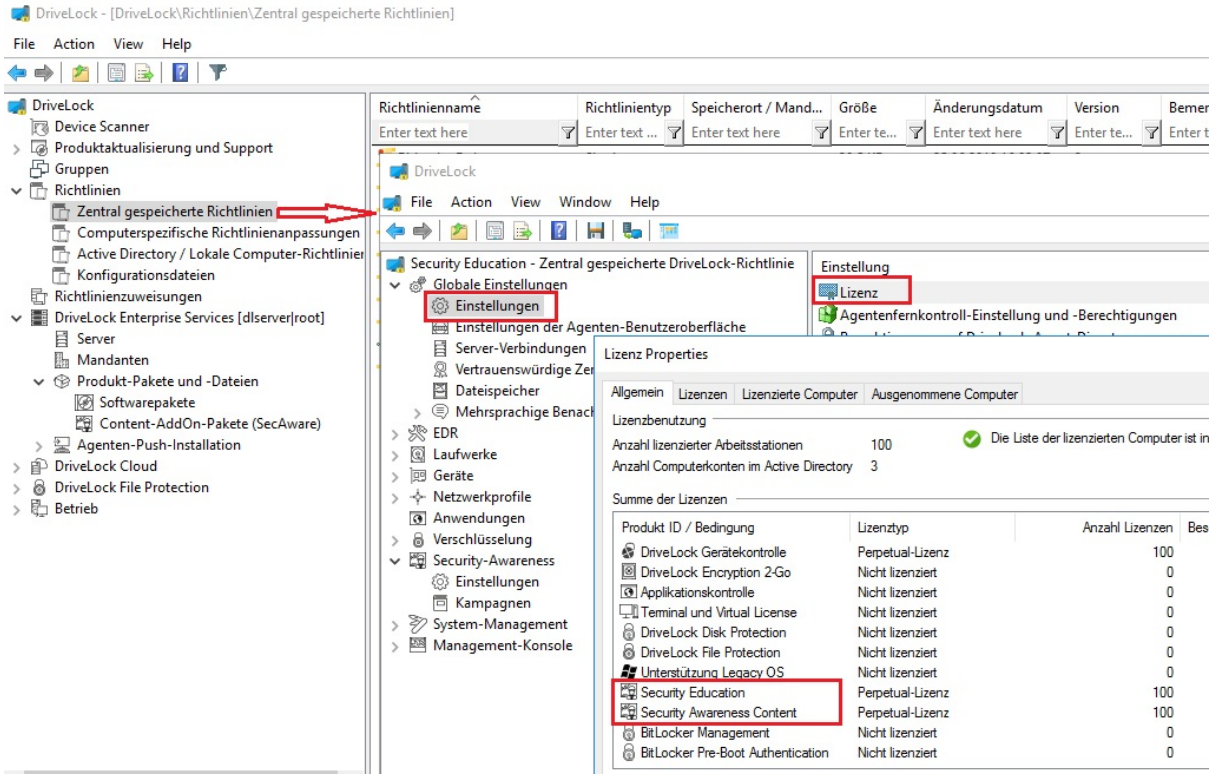
vor:

1. Öffnen Sie in der DriveLock Management Konsole den Knoten **Richtlinien**.
2. Wählen Sie die Richtlinie aus, für die Sie das AddOn lizensieren wollen.
3. Gehen Sie unter **Globale Einstellungen** zu den **Einstellungen** und wählen dann **Lizenz** aus.
4. Öffnen Sie über das Kontextmenü die Lizenzeigenschaften und hier den Reiter **Lizenzen**.
5. Klicken Sie die Schaltfläche **Lizenzdatei hinzufügen...** und folgen Sie den Anweisungen auf dem Bildschirm.
6. Wählen Sie als nächstes Ihre **Lizendatei** aus.
7. Im nächsten Dialog geben Sie an, wie Sie Ihre Lizendatei aktivieren möchten. Wir empfehlen die Online-Aktivierung.

   Hinweis: Bei der Online-Aktivierung ist eine Verbindung zum Internet erforderlich.

8. Abschließend bestätigen Sie, dass Ihre Lizenz für das Security Awareness Content AddOn dem DriveLock Enterprise Service hinzugefügt wird. Dadurch kann bei entsprechender Einstellung am Server der automatische Download neuer Content-AddOn-Pakete aktiviert werden. Siehe Kapitel Einstellung für Security Awareness am Server vornehmen.
9. Im letzten Dialog bestätigen Sie ihre Einstellungen und aktivieren so die Verwendung des AddOns.
10. Unter den Lizenzeigenschaften im Reiter **Allgemein** wird nun Ihre Lizenz angezeigt.

Siehe Abbildung:




## 2.3 Smart SecurityEducation

### 2.3.1 DriveLock Smart SecurityEducation

Smart SecurityEducation ist ein spezielles DriveLock-Modul, mit dem Sie schnell und leicht Security-Awareness-Kampagnen erstellen und verteilen können.

Die Einbindung der zusätzlichen Content-AddOn-Pakete über das Security Awareness Content AddOn durch Erwerb einer gesonderten Subskriptionslizenz ist dabei auch möglich.

Mehr zur Verwendung dieses Moduls finden Sie im folgenden Kapitel.

> Hinweis: Andere DriveLock-Funktionalitäten, bei denen Security-Awareness-Einstellungen über Regeln für Laufwerke, Geräte oder Anwendungen (je nach Kontext) vorgenommen werden können, sind bei Smart SecurityEducation nicht aktiviert.

### 2.3.2 Smart SecurityEducation einsetzen

Wenn Sie in Ihrem Unternehmen das DriveLock-Modul Smart SecurityEducation einsetzen, gehen Sie folgendermaßen vor:

1. Installieren Sie DriveLock wie im **Installationshandbuch** und im **Quick Start Guide** beschrieben. Diese Dokumente finden Sie unter https://drivelock.help/.

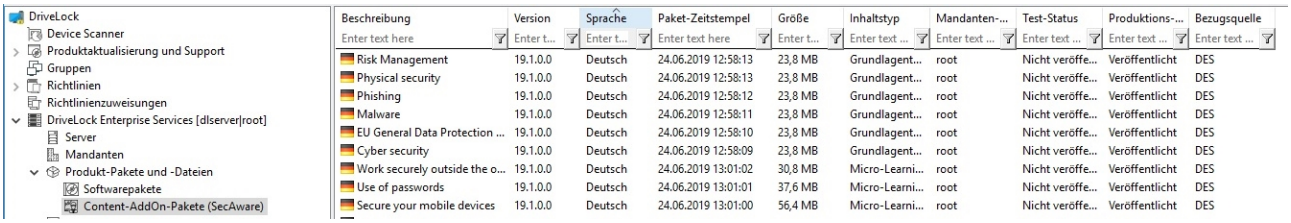
2. Öffnen Sie in der DriveLock Management Konsole den Knoten **Richtlinien**.
3. Markieren Sie die **Zentral gespeicherte DriveLock-Richtlinie** und wählen im Kontextmenü den Menüpunkt **Bearbeiten**.
4. Gehen Sie nun vor, wie in folgendem Kapitel beschrieben: Security Awareness für Richtlinien konfigurieren.

# 3 Content-AddOn-Pakete

In der DriveLock Management Konsole finden Sie Content-AddOn-Pakete an folgender Stelle:

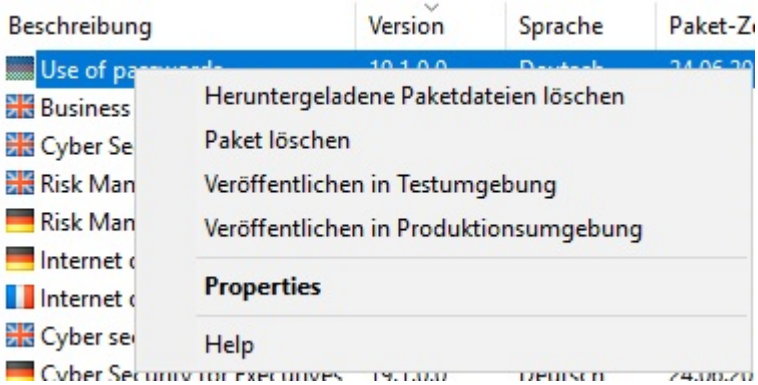
Im Knoten **DriveLock Enterprise Services** werden unter **Produkt-Pakete und -Dateien** die verfügbaren **Content-AddOn-Pakete** angezeigt.

> Hinweis: Nur wenn Sie das **Security Awareness Content AddOn** erworben haben, erhalten Sie hier eine detaillierte Übersicht über alle verfügbaren Pakete.
> Ist das AddOn nicht lizensiert, sehen Sie nur eine Auswahl an Demo-Paketen.




Neben allgemeinen Informationen, wie zum Beispiel Version, Sprache, Zeitstempel, Größe oder Inhaltstyp sind folgende Eigenschaften besonders hervorzuheben, da diese auch über das Kontextmenü des jeweiligen Pakets verändert werden können:

- **Test-Status und Produktions-Status**:
  Der Status kann entweder **Veröffentlicht** oder **Nicht veröffentlicht** sein, je nachdem ob Sie das Paket schon in der Test- oder Produktionsumgebung veröffentlicht haben. Dies kann entweder über das Kontextmenü oder über die Einstellungen in den Ser-vereigenschaften geschehen.

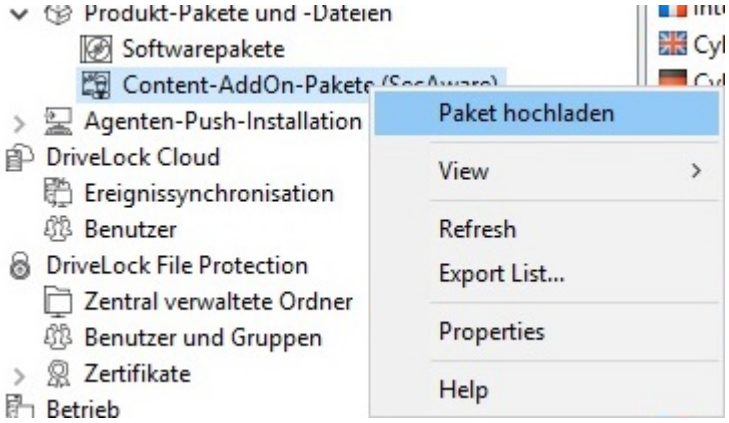



- **Bezugsquelle**:
  - **Noch nicht festgelegt**: Das Paket ist in der Cloud vorhanden, aber noch nicht auf dem DES verfügbar. Wählen Sie den Kontextmenübefehl **Auf den DES down-loaden**, um das Paket auf dem DES verfügbar zu machen.
  - **DES**: Das Paket ist auf dem DES verfügbar.

Hinweis: Die Einstellungen zur Aktualisierung und Veröffentlichung nehmen sie in den Servereigenschaften vor.

Hinweis: Bitte beachten Sie, dass eine Internetverbindung zwingend notwendig ist, um die Content-AddOn-Pakete auf dem aktuellen Stand zu halten.

Beachten Sie bitte, dass der Kontextmenübefehl **Paket hochladen** (siehe Abbildung) nur dazu verwendet werden kann, um eigenen Schulungsinhalt in einem standardisierten Format hochzuladen.
Für weitere Informationen dazu wenden Sie sich bitte an unseren Consulting Service.

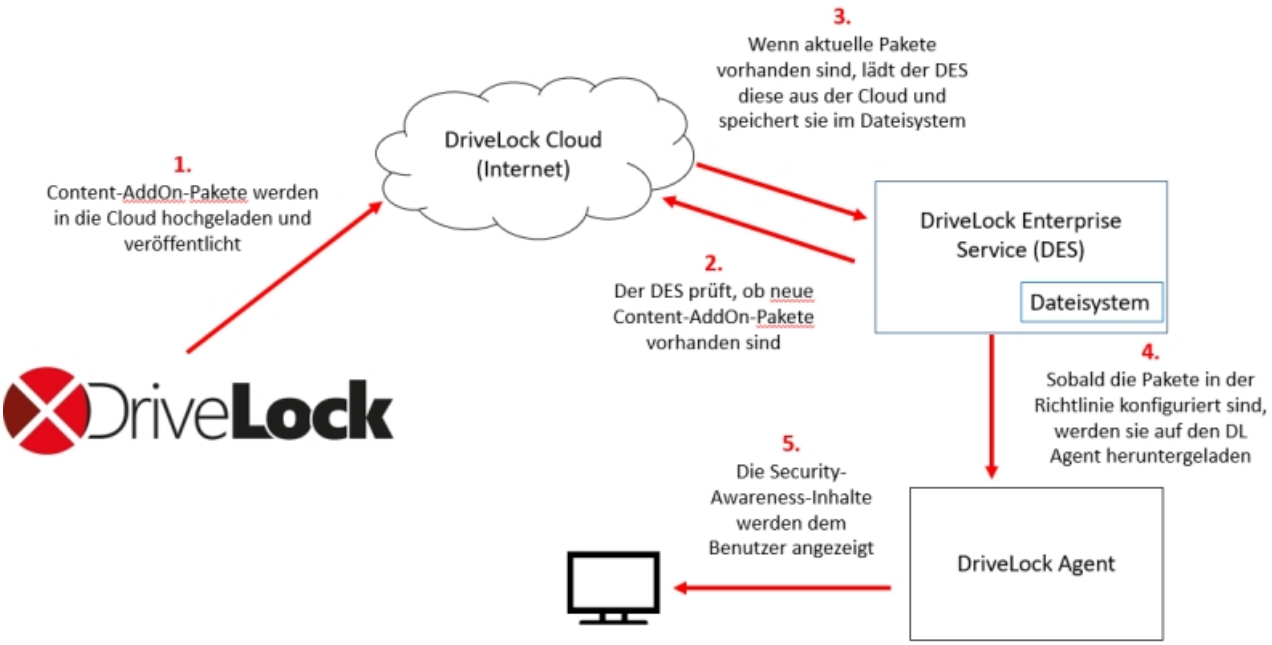



### 3.1 Verfügbare Sprachen

Ab Version 19.1 stehen Inhalte in den Sprachen **Deutsch**, **Englisch** und **Französisch** zur Verfügung.

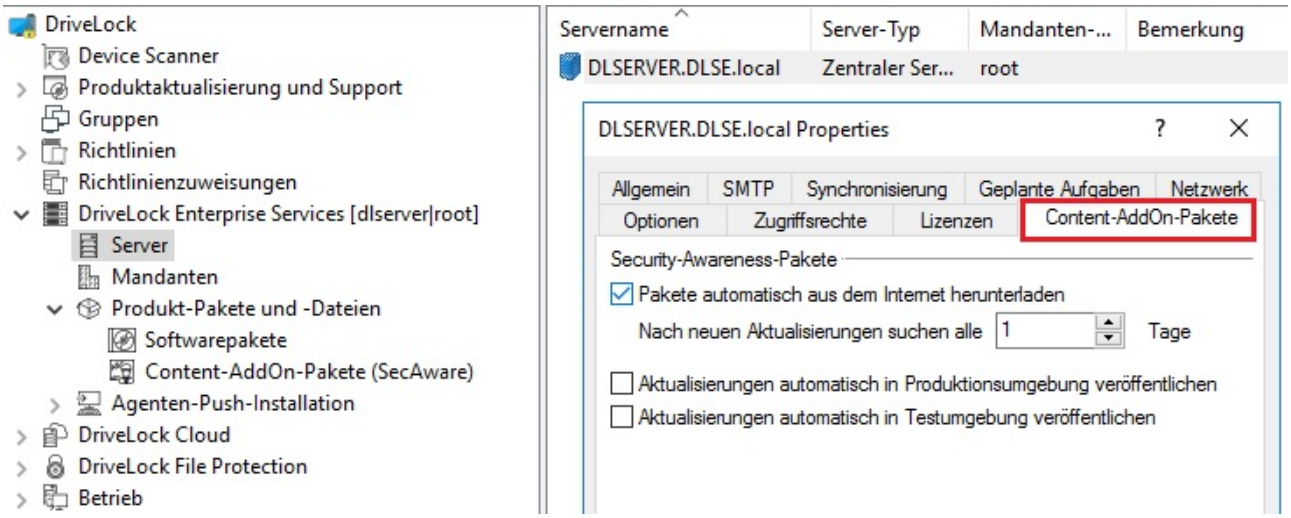
Achtung: Holländisch wird nicht mehr unterstützt, d.h. diese Pakete werden bei der Aktualisierung des DES auf diese Version automatisch gelöscht.

## 3.2 Prinzip: Content-AddOn-Pakete auf dem DriveLock Enterprise Service (DES)




## 3.3 Einstellungen für Security Awareness über Servereigenschaften vornehmen

Um Ihre Content-AddOn-Pakete immer auf dem neuesten Stand zu halten, können Sie Ihren Server automatisch nach Aktualisierungen suchen lassen. Gehen Sie dabei wie abgebildet vor:




1. Öffnen Sie in der DriveLock Management Konsole den Knoten **DriveLock Enterprise Services**.
2. Wählen Sie den **Server** aus, der für Ihre Content-AddOn-Pakete 'zuständig' ist.

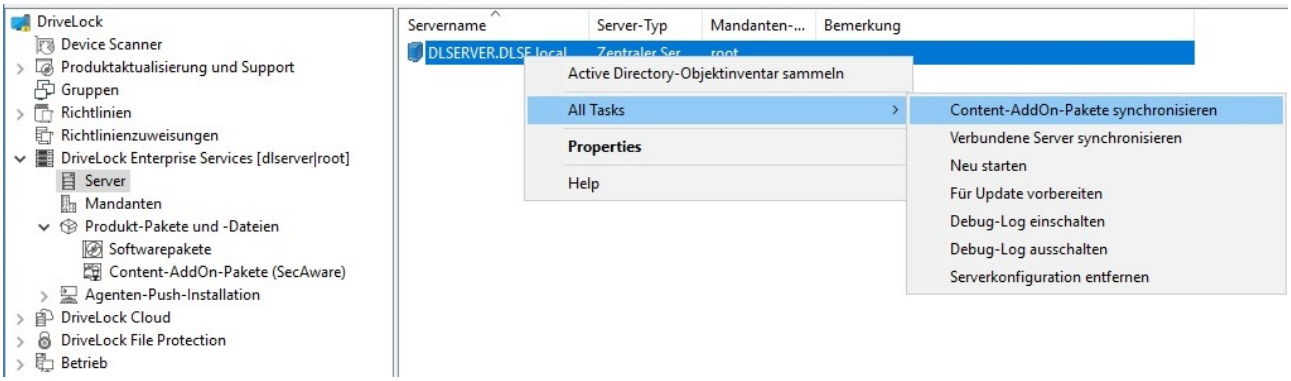
3. Öffnen Sie über das Kontextmenü die Servereigenschaften und hier den Reiter **Content-AddOn-Pakete**.
4. Wählen Sie die Option **Pakete automatisch aus dem Internet herunterladen** und dann wählen Sie aus, wie oft der Server nach Aktualisierungen suchen soll. Eine Angabe von 30 Tagen ist in diesem Fall ausreichend. Lesen Sie hier, wie das funktioniert.
5. Sie können auch angeben, ob die Aktualisierungen automatisch in der Produktions- und/oder Testumgebung veröffentlicht werden soll.

> Hinweis: Erst wenn ein Paket veröffentlicht ist, kann es von den Agenten heruntergeladen werden. Wenn Sie eine von beiden Optionen (oder beide) setzen, erfolgt dies automatisch nach dem Download der Pakete, je nach Auswahl für Produktions- und/oder Testumgebung.

6. Bestätigen Sie Ihre Einstellungen.

### 3.4 Content-AddOn-Pakete synchronisieren

Sie können Ihre Content-AddOn-Pakete auch manuell synchronisieren, indem Sie wie abgebildet vorgehen:




1. Öffnen Sie in der DriveLock Management Konsole (MMC) den Knoten **DriveLock Enterprise Services**.
2. Wählen Sie den **Server** aus, der für Ihre Content-AddOn-Pakete 'zuständig' ist.
3. Öffnen Sie das Kontextmenü und dann den Menübefehl **Alle Aufgaben**.
4. Klicken Sie den Menübefehl **Content-AddOn-Pakete synchronisieren**.
5. Alle Content-AddOn-Pakete sind nun auf dem neuesten Stand.

# 4 Security Awareness konfigurieren

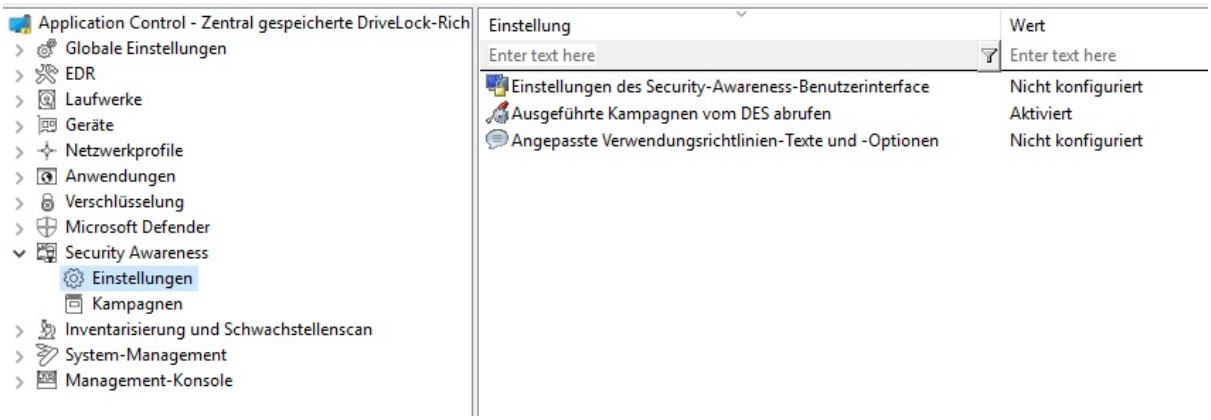
Um Security Awareness zu konfigurieren, gehen Sie folgendermaßen vor:

1. Wählen Sie in der DriveLock Management Konsole den Knoten **Richtlinien** aus.
2. Doppelklicken Sie eine Richtlinie Ihrer Wahl.
3. Im Knoten **Security Awareness** können Sie mit der Konfiguration starten:
   - Unter **Einstellungen** machen Sie allgemeine Angaben für alle Kampagnen.
   - Unter **Kampagnen** legen Sie neue Kampagnen an. Wie das geht, lesen Sie unter Kampagnen erstellen.

## 4.1 Allgemeine Security-Awareness-Einstellungen

**Gehen Sie folgendermaßen vor:**

1. Wählen Sie unter **Security-Awareness** den Menüpunkt **Einstellungen**.




2. Klicken Sie auf die Option **Einstellungen des Security-Awareness-Benutzerinterface**, um folgende Einstellungen festzulegen:

   - **Alle Kampagnen**
     Auf diesem Reiter nehmen Sie allgemeine Einstellungen vor, die **alle** Kampagnen betreffen.
     - Hier können Sie bestimmen, ob das Fenster, in dem Security-Awareness-Kampagnen angezeigt werden, beim Benutzer immer sichtbar ist.
     - Wenn Sie wollen, dass alle Kampagnen im Vollbildmodus angezeigt werden, setzen Sie ein Häkchen bei der entsprechenden Option.

     > Hinweis: Im Vollbildmodus kommen Ihre Kampagnen besonders gut zur Geltung.

- Wählen Sie die Option **Einstellungen zum Vollbildmodus auf Kampagnenebene ignorieren**, wenn Sie die Einstellungen in einzelnen Kampagnen hierzu außer Kraft setzen wollen (der Vollbildmodus kann in den Kampagneneigenschaften gesetzt werden).
- Wenn Sie noch keine mehrsprachigen Benachrichtigungstexte für Ihre Richtlinie erstellt haben, können Sie in diesem Dialog speziell auf Ihre Firma angepasste Überschriften und Texte für Ihre Kampagnen eingeben.
- Alternativ können Sie im MMC-Knoten **Globale Einstellungen** unter **Mehrsprachige Benachrichtigungstexte** Sprachen festlegen und an dieser Stelle entsprechende Benachrichtigungstexte definieren.

> Hinweis: Weitere Informationen zur Erstellung von mehrsprachigen Benachrichtigungstexten finden Sie im Administrationshandbuch unter DriveLock OnlineHelp.

3. Klicken Sie auf die Option **Angepasste Verwendungsrichtlinien-Texte und -Optionen**, um benutzerdefinierte Inhalte beim Zugriff auf ein Laufwerk und/oder Gerät anzeigen zu lassen. Dies betrifft ausschließlich die Anzeige von Verwendungsrichtlinien. Sie können folgende Einstellungen im Dialog vornehmen:

   - Text aus einer Datei laden oder Text selbst formulieren
   - Text für die Schaltflächen angeben (z.B. Zustimmen statt Akzeptieren)
   - Überschrift festlegen
   - Video laden und Einstellungen für dieses Video vornehmen

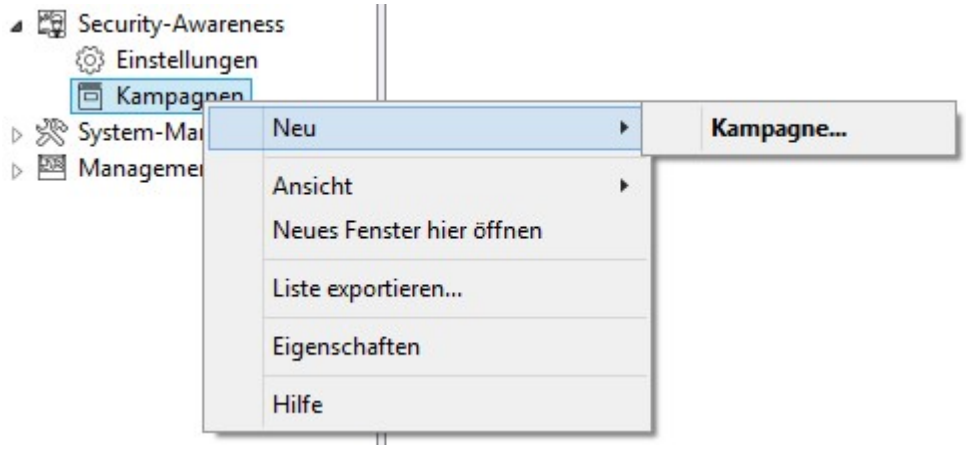
   > Hinweis: Mehr Informationen finden Sie im Kapitel **Verwendungsrichtlinien** im **DriveLock Administrationshandbuch**, das Sie unter DriveLock OnlineHelp finden.

4. Klicken Sie auf die Option **Ausgeführte Kampagnen vom DES abrufen**, um festzulegen, dass Benutzer ihre bereits durchgeführten Kampagnen auch bei Anmeldung an einem anderen Rechner "mitnehmen" können, d.h. die erledigten Kampagnen werden dort nicht mehr angezeigt. Hierzu wird ein Anfrage an den DriveLock Enterprise Service (DES) geschickt.
   Die Standardeinstellung ist **Deaktiviert**, da Benutzer in der Regel an einem festen Arbeitsplatz arbeiten.

## 4.2 Erstellung

### 4.2.1 Security-Awareness-Kampagnen erstellen

Erstellen Sie eine neue Kampagne, indem Sie wie in der Abbildung gezeigt vorgehen:




Über das Kontextmenü von **Kampagne** wählen Sie **Neu** und dann **Kampagne...**. Der **Neue Kampagne** Assistent wird geöffnet und Sie durchlaufen folgende Dialogseiten:

1. Inhalt einer neuen Kampagne
2. Auslöser für eine neue Kampagne
3. Wiederholungen einer neuen Kampagne
4. Allgemeine Einstellungen

> Hinweis: Um die neue Kampagne bestimmten Computern, Benutzern und Netzwerkverbindungen zuzuweisen, öffnen Sie die Eigenschaften der Security-Awareness-Kampagne. Hier können Sie auch alle Einstellungen ändern, die Sie im **Neue Kampagne** Assistent vorgenommen haben.

#### 4.2.1.1 Inhalt einer neuen Kampagne

Auf der ersten Dialogseite **Inhalt** bestimmen Sie, welche Inhalte (Elemente) Ihre Kampagne enthalten soll:

- **Bild**
  Wählen Sie hier ein beliebiges Bild aus Ihrem Dateisystem oder aus Ihrem Richtliniendateispeicher. Die üblichen Bildformate (*.png, *.jpg, *.bmp) werden unterstützt.
- **Content-AddOn-Paket**
  Wählen Sie hier ein Paket aus, das für Ihre Zwecke geeignet ist. Dies kann beispielsweise ein Training, ein Security Flash oder Wissenstest sein.

> Hinweis: Beachten Sie bitte, dass Content-AddOn-Pakete nur dann in dieser Liste angezeigt werden, wenn Sie die Lizenz für das DriveLock Security Awareness Content AddOn erworben haben. Ansonsten erscheinen lediglich die Demo-Pakete.

- **Eingebautes Bild**
  Wählen Sie hier eines der von DriveLock zur Verfügung gestellten Bilder aus.
- **PDF-Datei**
  Wählen Sie hier eine PDF-Datei, deren Inhalt dem Benutzer angezeigt wird. Überprüfen Sie bitte, ob der Inhalt korrekt angezeigt wird, da nicht alle PDF-Funktionalitäten unterstützt werden.
- **RTF-Datei**
  Wählen Sie hier eine RTF-Datei, deren Inhalt dem Benutzer angezeigt wird. Dies kann auch nur Text oder Unicode oder ANSI-Zeichencode sein.
- **Text**
  Geben Sie einen beliebigen Text für Ihre Kampagne ein.
- **URL (Web-Inhalt)**
  Geben Sie hier eine URL an, die auf Web-Inhalte verweist, die Sie für Ihre Kampagne einsetzen wollen.
- **Videodatei**
  Wählen Sie hier eine Videodatei aus (im Format *.mp4 oder *.avi), die dem Benutzer im Windows Media Player angezeigt wird.

> Hinweis: Die Fenstergröße wird bei der Anzeige immer dem Inhalt angepasst, außer bei Content-AddOn-Paketen und bei URL, wo die Fenstergröße 1280x1024 beträgt.

#### 4.2.1.2 Auslöser für eine neue Kampagne

Auf der zweiten Seite **Auslöser** geben Sie an, bei welchem Ereignis Ihre Kampagne angezeigt werden soll.

> Hinweis: Ein **Ereignis** ist beispielsweise das Einloggen eines Benutzers an seinem Rechner, das Einstecken eines externen Laufwerks, das Verbinden eines Geräts, z.B. eines Smartphones, oder auch die Aktualiserung einer Richtlinie, die über Regeln das Anzeigen einer Kampagne steuert.

Folgende Optionen stehen zur Auswahl:

- **Unabhängig von einem Ereignis**
  Wählen Sie diese Option, um eine Kampagne zum nächstmöglichen Zeitpunkt direkt bei Benutzern anzeigen zu lassen, unabhängig von den üblichen Ereignissen, die die Anzeige einer Kampagne auslösen. In diesem Fall prüft der DriveLock Agent in bestimmten Intervallen (alle 30 Minuten), ob unabhängige Kampagnen anstehen und zeigt diese dann entsprechend beim Benutzer an.

  Hinweis: Wenn Sie Benutzern möglichst schnell eine Security-Awareness-Kampagne, z.B. wichtige firmeninterne Informationen oder Warnungen, zukommen lassen ( 'pushen') wollen, wählen Sie diese Option.

- **Bei Anmeldung des Benutzers**
  Wählen Sie diese Option, um dem Benutzer eine Kampagne anzeigen zu lassen, sobald dieser sich an seinem Rechner anmeldet.
- **Bei Verwendung in Regeln**
  Wählen Sie diese Option, wenn Sie eine Kampagne in einer Regel verwenden wollen. Die Kampagne wird dem Benutzer angezeigt wie in der entsprechenden Regel für Laufwerke, Geräte oder Applikationen im Reiter **Awareness** definiert.

  Hinweis: Diese Option ist nur dann aktiv, wenn Sie sämtliche DriveLock-Funktionalitäten aktiviert haben.

Die beiden letzten Optionen sind nur bei DriveLock Smart SecurityEducation aktiviert:

- **Beim Anschliessen eines Geräts**
  Wählen Sie diese Option, um dem Benutzer eine Kampagne anzeigen zu lassen, sobald dieser ein Gerät an seinem Rechner ansteckt.
- **Beim Anschliessen eines Laufwerks**
  Wählen Sie diese Option, um dem Benutzer eine Kampagne anzeigen zu lassen, sobald dieser ein Laufwerk mit seinem Rechner verbindet.

#### 4.2.1.3 Wiederholungen einer neuen Kampagne

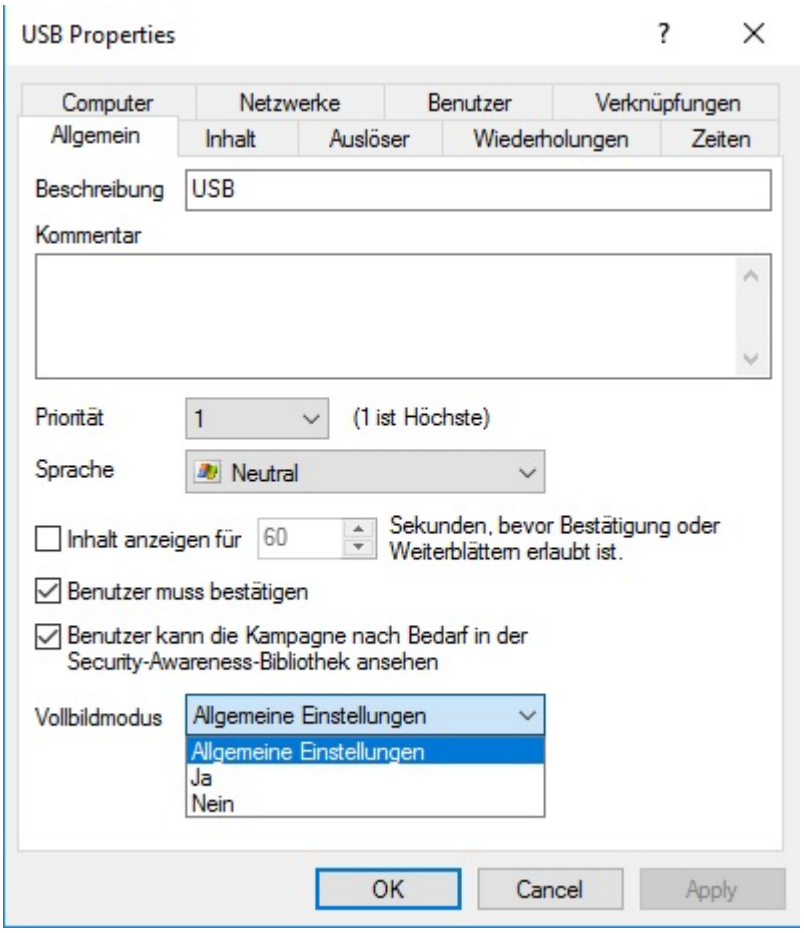
Auf der dritten Seite **Wiederholungen** geben Sie an, wie oft Ihre Kampagne angezeigt bzw. wiederholt werden soll.

Sie können hier folgendes einstellen:

- **Kampagne x mal anzeigen**
  Grenzen Sie hier die Kampagnenanzeige ein, indem Sie eine bestimmte Zahl angeben oder wählen Sie von der Dropdown-Liste **niemals** oder **unendlich oft** aus.
  Die Auswahl **niemals** ist dann sinnvoll, wenn Sie Ihre Kampagne zunächst noch nicht anzeigen lassen wollen. Sie können dies dann später in den Eigenschaften der Kampagne ändern.
- **Bei jedem Auftreten des Ereignisses**
- **Einmal pro Tag/Woche/Monat/Jahr**
- Sie können auch angeben, ob Ihre Kampagne **einmal alle paar Tage** (z.B. jeden dritten Tag) angezeigt wird.
- Falls eine Kampagne nur unvollständig angezeigt wurde oder ein Fehler aufgetreten ist, können Sie angeben, dass diese nach einer bestimmten Zeit wieder angezeigt wird.

#### 4.2.1.4 Allgemeine Einstellungen für die neue Kampagne

Auf der vierten Seite **Allgemein** geben Sie folgendes ein:



- **Beschreibung** Ihrer Kampagne und optional einen **Kommentar**. Die Beschreibung ist erforderlich, damit Sie Ihre Kampagne in der Kampagnenauflistung wiederfinden. Außerdem wird diese später auch für das Reporting verwendet.
- **Priorität**, nach der die Ausführungsreihenfolge der Kampagnen eingestellt wird (Einstellungen von 1 - 10, Reihenfolge absteigend). Kampagnen gleicher Priorität werden in zufälliger Reihenfolge angezeigt.
- Wählen Sie, für welche **Sprache** die Kampagne angezeigt werden soll. Wenn Sie z.B. Brasilianisch auswählen, dann wird Ihre Kampagne nur auf Agent-Rechnern angezeigt, deren Betriebssystemsprache Brasilianisch ist. Die Sprache auf Neutral zu belassen, schließt also alle Betriebssystemsprachen ein.

  Hinweis: Wenn Sie ein Security-Awareness-Paket aus dem Security-Awareness Content AddOn auswählen, wird die Sprache bereits durch diese Auswahl voreingestellt (nur Deutsch, Englisch oder Französisch).

- Geben Sie an, wie lange die Kampagne angezeigt bleibt, bevor der Benutzer bestätigen muss bzw. die Kampagne schließen kann.
- Geben Sie an, ob der Benutzer das Lesen des Kampagneninhalts bestätigen muss. In den allgemeinen Security-Awareness-Einstellungen können Sie einen entsprechenden Bestätigungstext für alle Kampagnen eingeben.
- Die Option **Benutzer kann die Kampagne nach Bedarf in der Security-Awareness-Bibliothek ansehen** ist standardmäßig aktiviert. Der Benutzer kann die Kampagnen aus der Security-Awareness-Bibliothek auswählen und zu einem passenden Zeitpunkt ansehen oder durcharbeiten.

  Hinweis: Sobald Sie DriveLock auf Version 2019.2 aktualisiert haben, ist diese Option für alle bereits vorhandenen Kampagnen voreingestellt. Bitte beachten Sie, dass auch die DriveLock Agenten auf diese Version aktualisiert werden müssen.

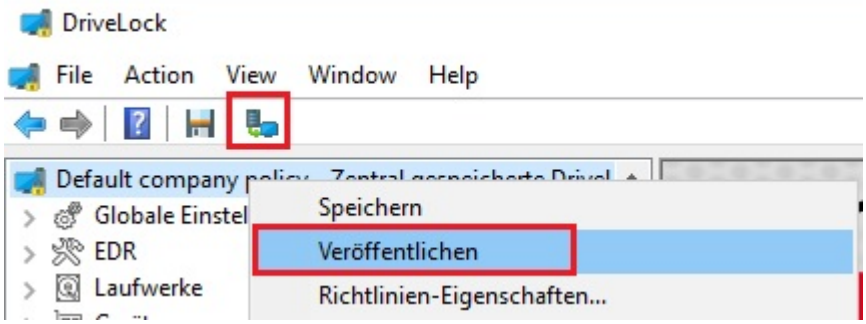
- Vollbildmodus:
  Wählen Sie hier **Ja**, wenn Sie wollen, dass diese Kampagne dem Benutzer im Vollbildmodus angezeigt wird.
  Wählen Sie die Option **Allgemeine Einstellungen**, um die Vollbildmodus-Einstellungen in den allgemeinen Security-Awareness-Einstellungen für diese Kampagne zu übernehmen.
  Wählen Sie **Nein**, wenn Sie keinen Vollbildmodus wollen.

> Hinweis: Diese Option ist nicht verfügbar, wenn für alle Kampagnen die Option **Einstellungen zum Vollbildmodus auf Kampagnebene ignorieren** gesetzt wurde.

### 4.2.2 Security-Awareness-Kampagne an Benutzer verteilen

Um eine neue Security-Awareness-Kampagne an die entsprechenden Benutzer (Computer mit DriveLock Agenten) zu verteilen, müssen Sie die Richtlinie zunächst veröffentlichen.

1. Öffnen Sie das Kontextmenü der Richtlinie und wählen Sie den Menüpunkt **Veröffentlichen**. Oder wählen Sie die Schaltfläche **Veröffentlichen** aus der Menüleiste.




2. Optional können Sie einen Kommentar eingeben.
3. Wenn Sie die Richtlinie signieren wollen, aktivieren Sie die entsprechende Option und wählen das Zertifikat aus.
4. Die Richtlinie ist nun veröffentlicht und wird von den DriveLock Agenten verwendet

Weitere Informationen zur Veröffentlichung von Richtlinien und Auswählen von Signaturzertifikaten finden Sie im **DriveLock Administrationshandbuch**, das unter https://drivelock.help/ verfügbar ist.

# 5 Verwendung

## 5.1 Security Awareness bei Aufruf einer Anwendung

Um Security-Awareness-Kampagnen beim Aufrufen von Anwendungen zu konfigurieren, gehen Sie wie unten beschrieben vor. Diese Vorgehensweise gilt für alle Anwendungs-Regeln.

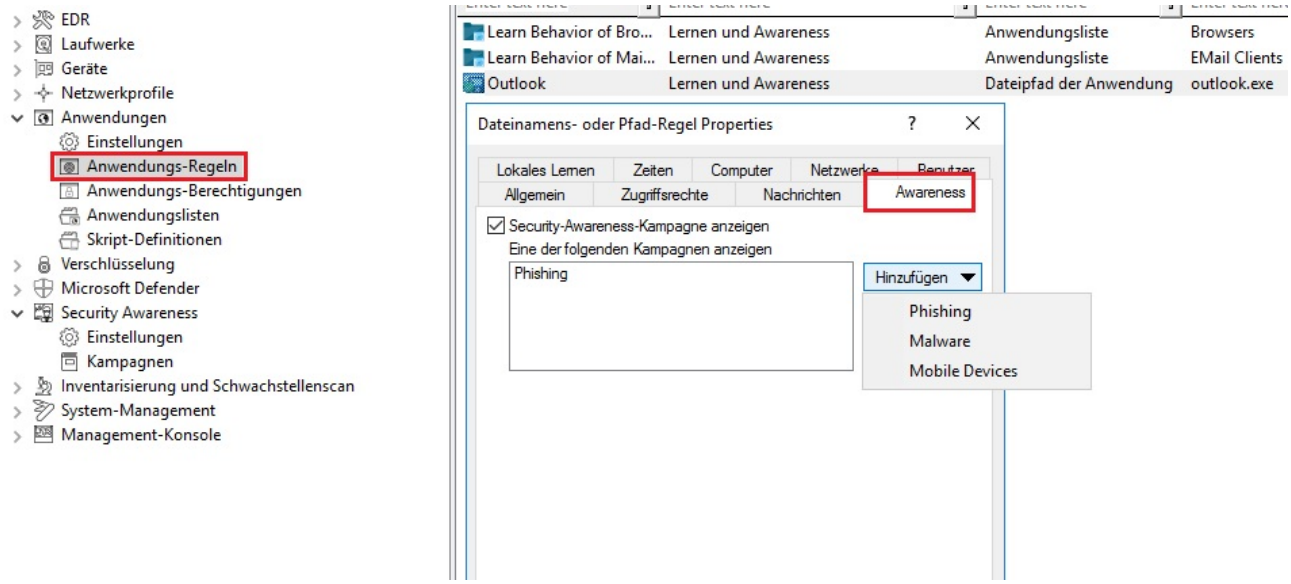
Hinweis: DriveLock Application Control unterliegt einer gesonderten Lizensierung und gehört nicht zum Standardumfang von DriveLock.

Hinweis: Wichtig zu beachten ist, dass die Anzeige einer Security-Awareness-Kampagne vom übergeordneten **Scan- und Blockier-Modus** abhängig ist, den Sie für die Anwendungsausführung definiert haben. So gibt im Whitelist-Modus die übergeordnete Regel eine bestimmte Anwendung frei, während im Blacklist-Modus die übergeordnete Regel die Anwendung sperrt. Erst wenn das System die bereits konfigurierte Regel geprüft und angewendet hat, wird die Regel zur Anzeige der Security-Awareness-Kampagne angewendet. Dieser Mechanismus ist im Administrationshandbuch unter Kapitel Applikationskontrolle beschrieben.

1. Wählen Sie in der Richtlinienkonfiguration den Knoten **Anwendungen**.
2. Wählen Sie die **Anwendungs-Regel** aus (Beispiel siehe Abbildung), für die Sie Security-Awareness einstellen wollen und öffnen das jeweilige Kontextmenü.
3. Klicken Sie den Menübefehl **Neu**, dann die jeweilige Regel und öffnen den Reiter **Awareness** im Eigenschaftendialog.
4. Wählen Sie **Security-Awareness-Kampagne anzeigen** und fügen eine zuvor erstellte Kampagne hinzu.

   Hinweis: Entsprechend der Einstellungen, die Sie bei Erstellung der Kampagne angegeben haben (z.B. wie oft und zu welchen Zeiten diese angezeigt bzw. wiederholt werden soll), wird die Kampagne auf dem DriveLock Agenten angezeigt. Kampagnen gleicher Priorität werden nach dem Zufallsprinzip angezeigt.

5. Bestätigen Sie Ihre Einstellungen.




## 5.2 Security Awareness beim Verbinden eines Laufwerks

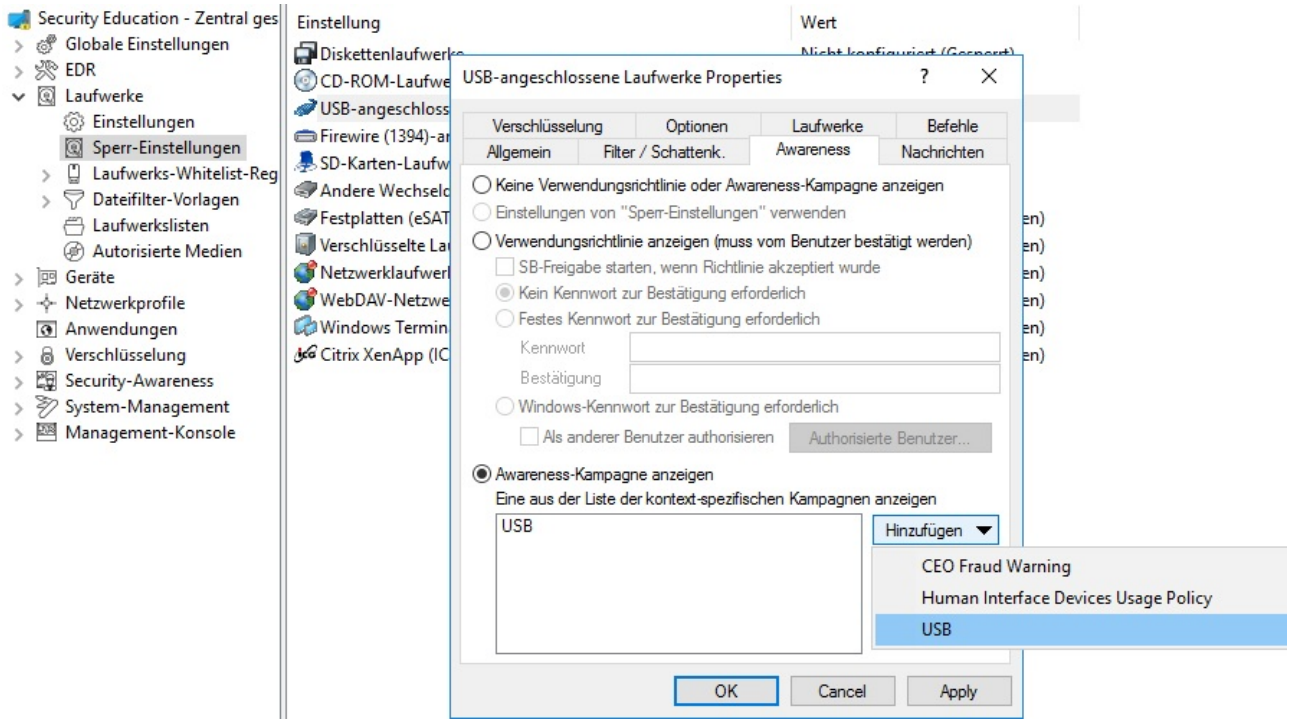
Um Security Awareness zu konfigurieren, so dass eine Kampagne bei der Verbindung eines Laufwerks angezeigt wird, gehen Sie wie in der Abbildung gezeigt vor. Diese Vorgehensweise gilt für alle Arten von Laufwerken.

1. Wählen Sie in der Richtlinienkonfiguration den Knoten **Laufwerke**.
2. Wählen Sie unter **Sperr-Einstellungen** das Laufwerk, für das Sie eine Security-Awareness-Kampagne anzeigen lassen wollen. Im Beispiel ein USB-Laufwerk.
3. Doppelklicken Sie das Laufwerk, um den Eigenschaftendialog zu öffnen.
4. Auf dem Reiter **Awareness** können Sie folgende Einstellungen machen:
   - Es soll weder eine Verwendungsrichtlinie noch eine Awareness-Kampagne angezeigt werden. Dies ist die Standardeinstellung.
   - Wenn Sie eine **Verwendungsrichtline anzeigen** lassen wollen, wählen Sie diese Option. Hierzu können Sie auch Passwörter vergeben, die bei der Bestätigung eingegeben werden müssen oder Sie haken die Option **SB-Freigabe starten, wenn Richtlinie akzeptiert wurde** an, damit ein Benutzer das Gerät verwenden kann, sobald die Richtlinie bestätigt wurde.
   - Wenn andere Benutzer als der in Windows angemeldete Benutzer die Richtlinie bestätigen soll, markieren Sie **Windows-Kennwort zur Bestätigung erforderlich** und **Als anderer Benutzer authorisieren**. Klicken Sie **Authorisierte Benutzer** um diese Benutzer in die Liste einzutragen und markieren Sie **Option "Als Benutzer anmelden" standardmäßig aktivieren**. Der SB-Freigabe-Assistent wird dann unter dem authorisierten Benutzer ausgeführt.

> Hinweis: Wie Sie eine Verwendungsrichtlinie erstellen, erfahren Sie hier.

- Beim Verbinden mit dem Gerät wollen Sie eine **Awareness-Kampagne anzeigen** lassen. Jetzt können Sie hier eine zuvor erstellte Kampagne hinzufügen. Wählen Sie diese aus der Liste aus, die nach Klick auf **Hinzufügen** geöffnet wird.

5. Bestätigen Sie Ihre Einstellungen.



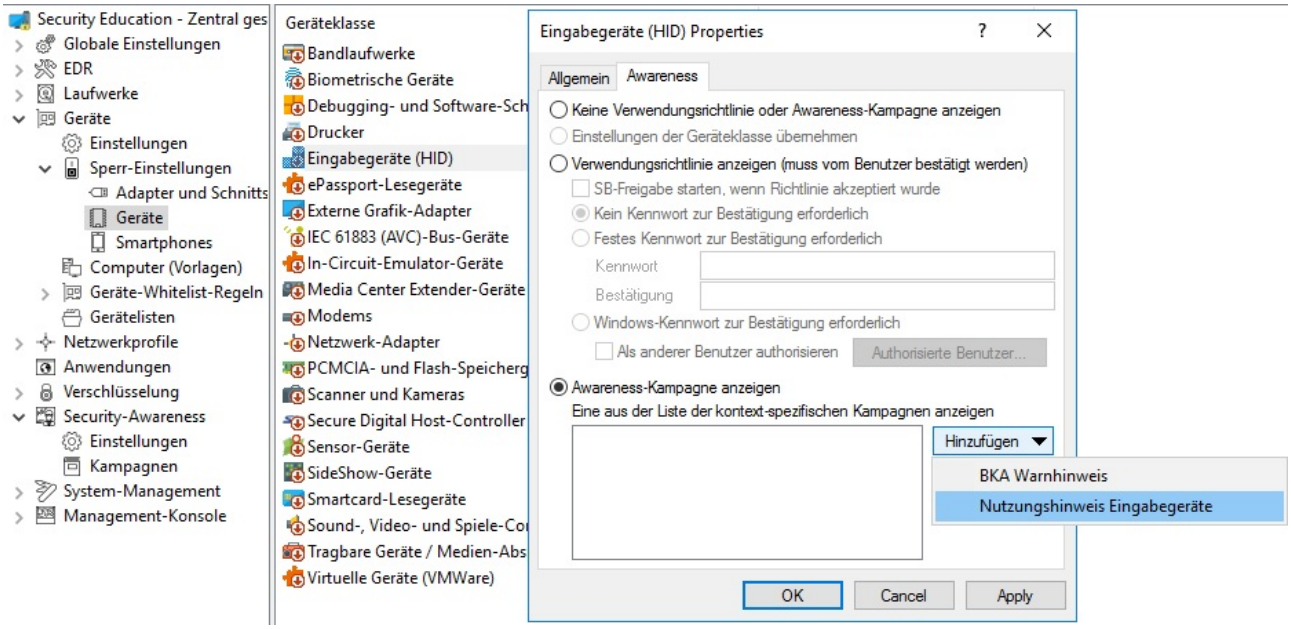

Bei **Laufwerk-Whitelist-Regeln** lässt sich das Security-Awareness-Feature für folgende Regeln einstellen:

- Geräte-Regel
- Gerätegröße-Regel
- Verschlüsselte Medien-Regel
- Basis-Regel

In diesen Fällen können Sie die Einstellungen für die einzelnen Laufwerke detaillierter vornehmen und angeben, ob eine übergeordnete Einstellung übernommen wird oder außer Kraft gesetzt wird. Auf dem Reiter **Awareness** wählen Sie in diesem Fall die Option **Einstellungen für "Sperr-Einstellungen verwenden"**.

### 5.3 Security Awareness bei Verwendung eines Geräts

Um Security-Awareness bei der Verwendung von Geräten zu konfigurieren, gehen Sie wie in der Abbildung gezeigt vor. Diese Vorgehensweise gilt für alle Geräte und alle Smartphones, sowie alle Adapter und Schnittstellen, außer COM und LPT, ebenso wie für alle Geräte-Whitelist-Regeln.




1. Wählen Sie in der Richtlinienkonfiguration den Knoten **Geräte**.
2. Wählen Sie unter **Sperr-Einstellungen** die Geräteklasse aus, bei der Sie Security-Awareness-Einstellungen vornehmen möchten.

   Im Beispiel oben soll eine Awareness-Kampagne oder eine Verwendungsrichtlinie angezeigt werden, sobald ein Benutzer versucht, ein Eingabegerät (HID) mit seinem Arbeitsrechner zu verbinden.
3. Sie wählen **Geräte** und doppelklicken dann **Eingabegeräte** zum Öffnen des Eigenschaftendialogs.
4. Auf dem Reiter **Awareness** können Sie folgende Einstellungen machen:
   - Es soll weder eine Verwendungsrichtlinie noch eine Awareness-Kampagne angezeigt werden. Dies ist die Standardeinstellung.
   - Wenn Sie eine Verwendungsrichtline anzeigen lassen wollen, wählen Sie diese Option. Hierzu können Sie auch Passwörter vergeben, die bei der Bestätigung eingegeben werden müssen oder Sie haken die Option **SB-Freigabe starten, wenn Richtlinie akzeptiert wurde** an, damit ein Benutzer das Gerät verwenden kann, sobald die Richtlinie bestätigt wurde.

- Wenn andere Benutzer als der in Windows angemeldete Benutzer die Richtlinie bestätigen soll, markieren Sie **Windows-Kennwort zur Bestätigung erforderlich** und **Als anderer Benutzer authorisieren**. Klicken Sie **Authorisierte Benutzer** um diese Benutzer in die Liste einzutragen und markieren Sie **Option "Als Benutzer anmelden" standardmäßig aktivieren**. Der SB-Freigabe-Assistent wird dann unter dem autorisierten Benutzer ausgeführt.

  Hinweis: Wie Sie eine Verwendungsrichtlinie erstellen, erfahren Sie hier.

- Beim Verbinden mit dem Gerät wollen Sie eine **Awareness-Kampagne anzeigen** lassen. Jetzt können Sie hier eine zuvor erstellte Kampagne hinzufügen. Wählen Sie diese aus der Liste aus, die nach Klick auf **Hinzufügen** geöffnet wird.

5. Bestätigen Sie Ihre Einstellungen.

# 6 Security-Awareness-Ereignisse

Alle Ereignisse auf den entsprechenden DriveLock Agenten werden in der DriveLock Management Konsole im Knoten **EDR** automatisch nach Feature geordnet angezeigt.

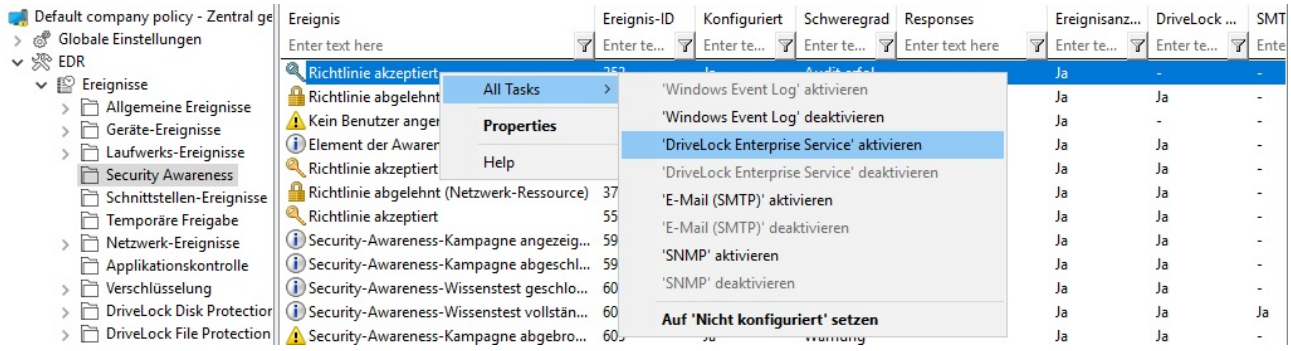
Unter **Ereignisse** sehen Sie im Unterknoten **Security Awareness** eine Liste aller Security-Awareness-Ereignisse.

> Achtung: Damit Sie die Security-Awareness-Ereignisse im DriveLock Control Center (DCC) und im DriveLock Operations Center (DOC) sehen können, müssen sie zunächst vom DriveLock Agenten auf den DriveLock Enterprise Service (DES) geladen (und somit aktiviert) werden.

## 6.1 Security-Awareness-Ereignisse auf dem DES aktivieren

**Gehen Sie folgendermaßen vor:**

1. Öffnen Sie im Knoten **EDR** unter **Ereignisse** den Unterknoten **Security Awareness**.
2. Markieren Sie alle Ereignisse, die Sie im DCC oder DOC angezeigt haben wollen und öffnen Sie das Kontextmenü.
3. Wählen Sie 'DriveLock Enterprise Service' aktivieren, damit die Ereignisse zum DES hochgeladen werden können.

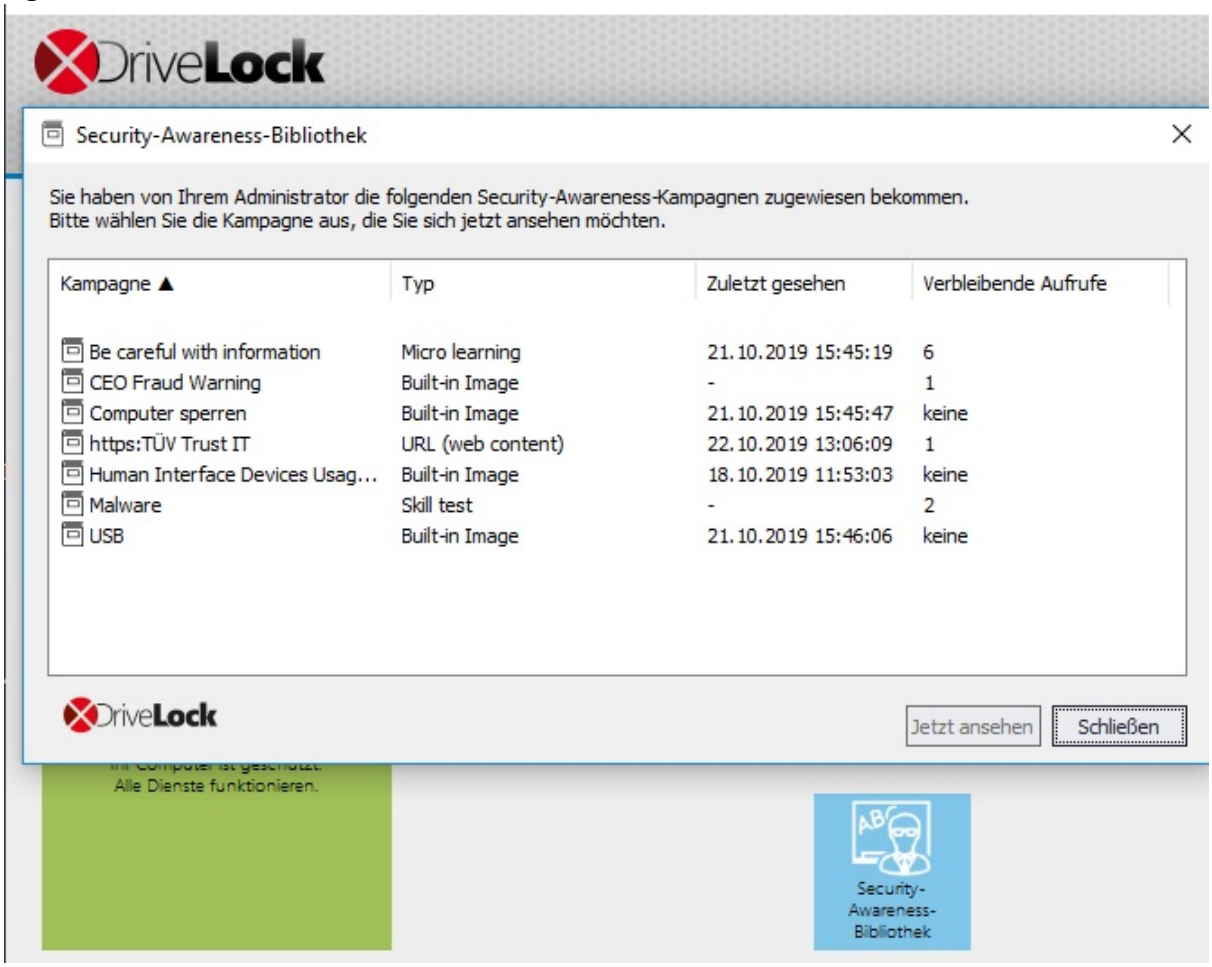


# 7 DriveLock Agent

## 7.1 Anzeige der Security-Awareness-Kampagnen auf dem DriveLock Agenten

Auf Agentenseite werden Kampagnen gemäß den Einstellungen in der Richtlinie angezeigt.

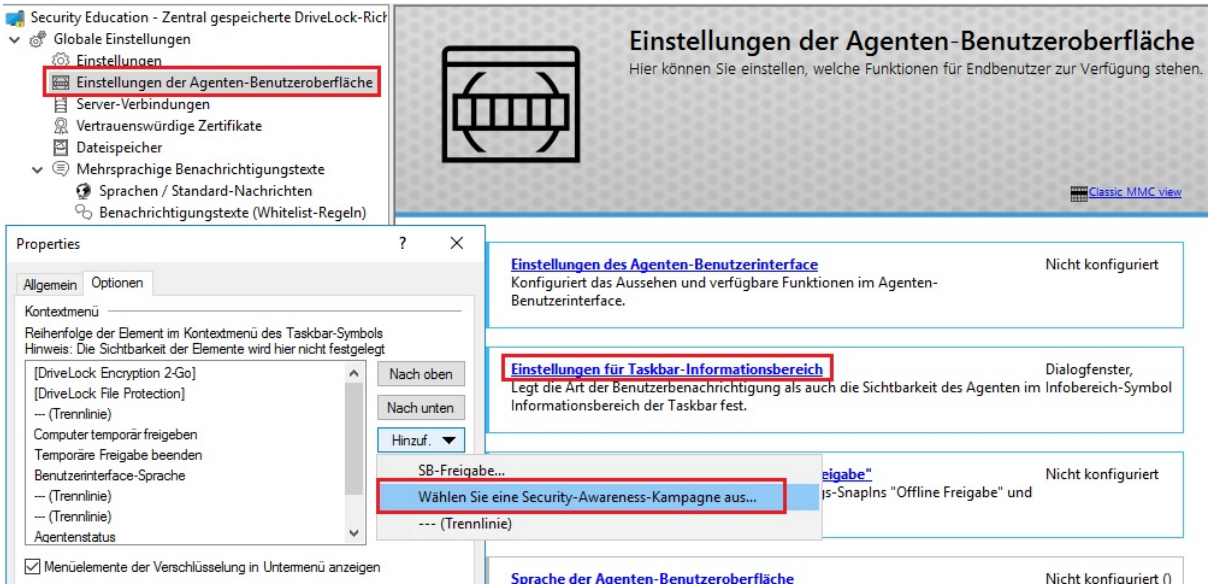
- Benutzer können die Security-Awareness-Bibiliothek in der Benutzeroberfläche des Agenten öffnen:




- Die Security-Awareness-Bibliothek kann alternativ über das Taskleistensymbol auf dem Agenten aufgerufen werden:


Hierzu müssen Sie vorher in der Richtlinie unter **Einstellungen der Agenten-Benutzeroberfläche** die Option **Einstellungen für Taskbar-Informationsbereich**

auswählen (Informationen finden Sie im Kapitel 6.5.2 im Administrationshandbuch unter DriveLock OnlineHelp).
Auf dem Reiter **Optionen** muss der Eintrag **Wählen Sie eine Security-Awareness-Kampagne ...** hinzugefügt werden (siehe Abbildung).
Dann erst kann der Benutzer auf dem Agenten eine Kampagne auswählen.



# 8 DOC (DriveLock Operations Center)

## 8.1 Security Awareness im DOC

Im DriveLock Operations Center bekommen Sie in der Ansicht **SecAware** einen Überblick über Ihre laufenden Security-Awareness-Kampagnen. Der Ablauf einer Kampagne wird im DOC als 'Session' bezeichnet.

Wenn Sie im Menü die Ansicht **SecAware** zum ersten Mal auswählen, erhalten Sie auf einer Tour wertvolle Tipps.

**Damit Kampagnen bzw. deren Sessions im DOC angezeigt werden können, müssen folgende Voraussetzungen erfüllt sein:**

1. Eine oder mehrere Security-Awareness-Kampagnen sind schon angelegt worden. Welchen Inhalt diese Kampagnen haben, spielt dabei keine Rolle.
2. Die Richtlinien mit den Kampagnen sind an die entsprechenden DriveLock Agenten zugewiesen worden. Angezeigt werden hierbei nur Kampagnen, die auf dem Agenten bereits gestartet, gerade aktiv oder schon beendet sind.

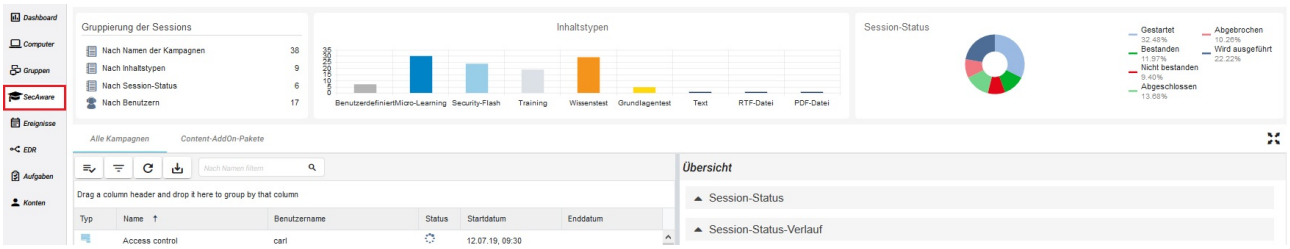
   > Achtung: Auf den Agenten muss mindestens DriveLock Version 19.2 installiert sein. Die Ausführung von Security-Awareness-Kampagnen auf Agenten mit älteren Versionen von DriveLock kann nicht im DOC angezeigt werden.

3. Die Security-Awareness-Ereignisse müssen auf dem DriveLock Enterprise Service aktiviert sein.

## 8.2 Die SecAware-Ansicht

In der Abbildung sehen Sie ein Beispiel für eine typische SecAware-Ansicht.

Jede Ansicht ist individuell und hängt von verschiedenen Faktoren ab, z.B. von der Anzahl und vom Typ der Kampagnen, die Sie bereits erstellt haben.




Der obere Bereich bietet Ihnen eine schnelle Übersicht über die Inhalte und Status Ihrer Kampagnen (Sessions).

Durch Klicken auf können Sie den Bereich verbergen und durch Klicken auf wieder anzeigen.

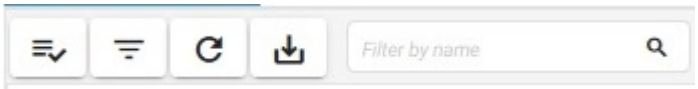
Die Sessions sind nach bestimmten Filtern gruppiert:

- Wenn Sie sich z.B. anzeigen lassen wollen, wie viele Benutzer gerade an einer Kampagne mit einem bestimmten Inhaltstyp arbeiten, wählen Sie im Widget **Gruppierung der Sessions** die Option **Nach Inhaltstypen**. Auf dem Reiter **Alle Kampagnen** erscheinen dann alle Inhaltstypen mit der jeweiligen Anzahl der Benutzer. Markieren Sie einen Benutzer und Sie sehen sofort alle Details der Session: Start- und Enddatum, Computer- und Benutzername und den jeweiligen Status.
- Im Widget **Inhaltstyp** können Sie nach einem bestimmten Kampagnen-Inhaltstyp filtern.
- Der **Session-Status** zeigt Ihnen in einem Kreisdiagramm die verschiedenen Status der Sessions an. Durch Klicken auf das Segment **Nicht bestanden** können Sie beispielsweise sehen, welcher Benutzer welche Sessions nicht bestanden hat.

Auf dem Reiter **Alle Kampagnen** im unteren Bereich sehen Sie eine Liste aller vorhandenen Sessions Ihrer Kampagnen mit den dazugehörigen Details.

Der Reiter **Content-AddOn-Pakete** zeigt Ihnen nur eine Liste der lizenzpflichtigen Pakete an (ohne Lizenz nur die Demo-Pakete) mit Informationen zu den verschiedenen Versionen und Sprachen. Am Status können Sie lediglich die Anzahl der Starts bzw. der bestandenen/nicht bestandenen Sessions sehen, weitere Informationen z.B. zu Benutzern oder Computern werden Ihnen aber nicht angezeigt.

Filtermöglichkeiten:



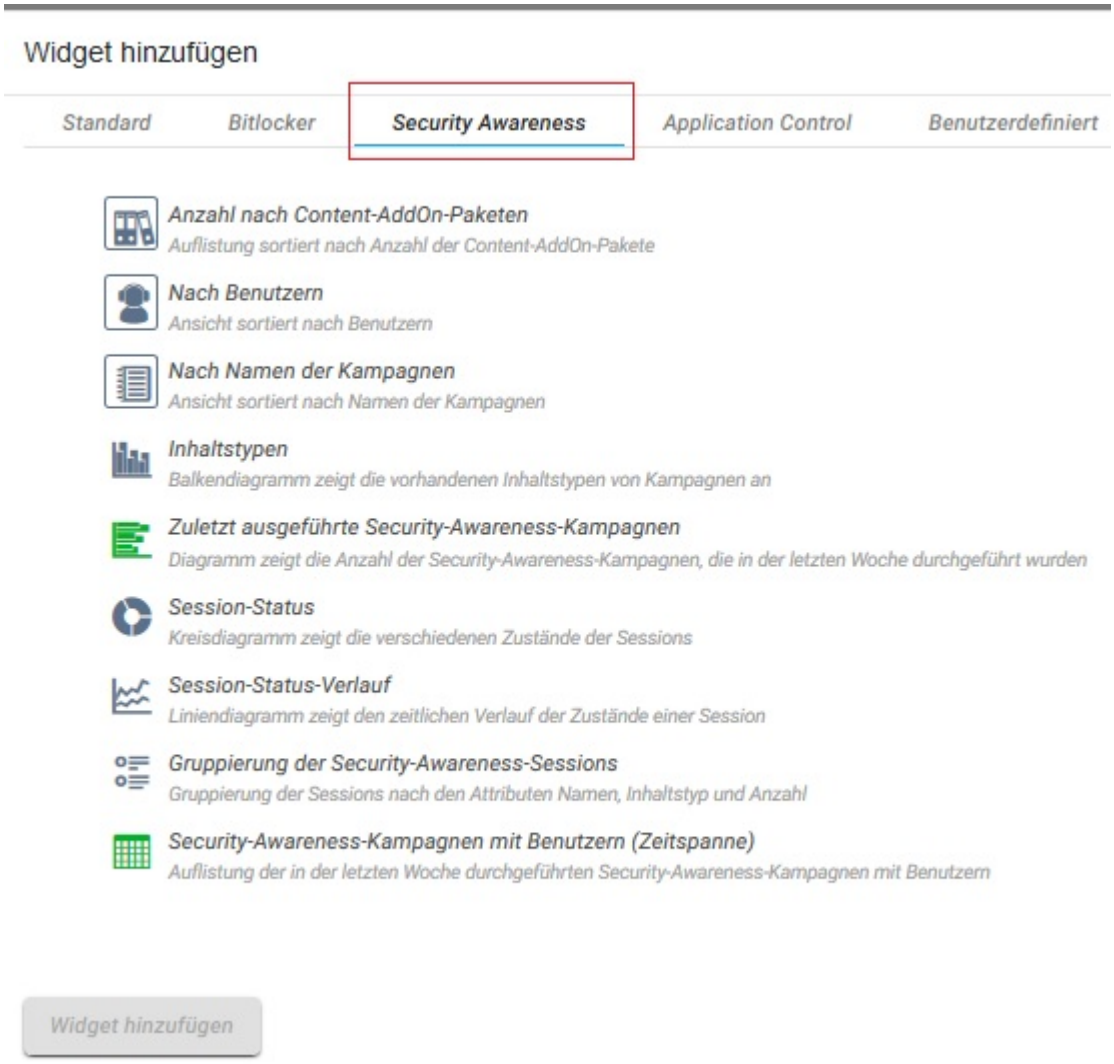

Durch Klicken auf die Schaltflächen können Sie sich Ihre Listen nach bestimmten Filterkriterien anzeigen lassen oder die Daten in eine Excel-Liste exportieren.

## 8.3 Security-Awareness-Dashboard

Sie können sich ein eigenes Security-Awareness-Dashboard anlegen.

### Gehen Sie folgendermaßen vor:

1. Klicken Sie im Standard-Dashboard des DOC auf das Symbol **+**.
2. Legen Sie ein neues Dashboard nach der Vorlage **Security Awareness** an.
3. Arrangieren Sie die Widgets nach Ihren Wünschen.
4. Fügen Sie ggf. neue Widgets von der Auswahlliste der Security-Awareness-Widgets hinzu.




5. Speichern Sie Ihr Dashboard.

# Copyright