
Bitdefender ENTERPRISE
BITDEFENDER
SMALL OFFICE
SECURITY
Berichterstatterhandbuch ››

Bitdefender Small Office Security
Berichterstatterhandbuch

Veröffentlicht 2014.06.10


Bitdefender

Inhaltsverzeichnis

1. Über Small Office Security

Mit Small Office Security-On-Premise können Unternehmen die Sicherheit auf ihrer eigenen Infrastruktur hosten und den Schutz für ihre PCs, Macs und Dateiserver selbst schnell und einfach bereitstellen, verwalten und überwachen. Dabei profitieren Sie von der führenden Malware-Erkennung und der neuesten Verwaltungskonsole aus dem Hause Bitdefender.

Anders als die Cloud-Version, die von Bitdefender gehostet wird und keine eigene Infrastruktur benötigt, wird diese Small Office Security-Version in der kundeneigenen Umgebung installiert.

Small Office Security besteht aus den folgenden Komponenten:

- Control Center
- Security for Endpoints
- Security for Mobile Devices

Control Center

Ein web-basiertes Dashboard und zentrale Verwaltungskonsole, die die Sicherheitslage im Unternehmen sowie allgemeine Sicherheitsrisiken transparent macht und dabei die Steuerung der Sicherheitsdienste erlaubt, die die virtuellen und physischeb Arbeitsplatzrechner, Server und Mobilgeräte schützen.

Control Center lässt sich mit den bestehenden Systemverwaltungs- und Überwachungssystemen integrieren und vereinfacht so die automatische Bereitstellung von Schutz auf nicht verwalteten Arbeitsplatzrechnern und Servern.

Security for Endpoints

Bitdefender Security for Endpoints Die Lösung schützt Computer im Hintergrund und setzt dabei auf vielfach ausgezeichnete Malware-Schutz-Technologien kombiniert mit einer Firewall, Angriffserkennung, der Steuerung und Filterung des Internet-Zugangs, dem Schutz von sensiblen Daten und einer Anwendungssteuerung. Security for Endpoints bietet Sicherheit für Computer mit Mac OS X oder Windows sowie für Windows-Server. Die Produktivität der Mitarbeiter wird durch effizienten Ressourceneinsatz, optimierte System-Scans und automatisierte Sicherheit, die ohne Eingriffe des Benutzers auskommt, sichergestellt.

Security for Mobile Devices

Verwaltet und steuert iPhones, iPads und Android-Geräte mit einem universellen auf den Einsatz in Unternehmen ausgelegten Ansatz, der die Geräte durch Echtzeit-Scans schützt

und die Sicherheitsrichtlinien des Unternehmens auf mobilen Geräten anwendet, so z. B. Bildschirmsperrung, Passwortschutz, Verschlüsselung von Wechseldatenträgern, Ortung verlorener Geräte und Zugriffsverweigerung für nicht konforme oder inoffiziell entsperrte Geräte.

2. Erste Schritte

Bitdefender Small Office Security-Lösungen können über eine zentrale Verwaltungsplattform namens Control Center konfiguriert und verwaltet werden.Control Center hat eine Web-basierte Oberfläche, auf die Sie mit einem Benutzernamen und einem Passwort zugreifen können.

2.1. Verbinden mit dem Control Center

Der Zugriff auf die Control Center erfolgt über Benutzerkonten. Sie erhalten Ihre Anmeldeinformationen per E-Mail, sobald Ihr Konto angelegt wurde.

Vorbereitende Maßnahmen:

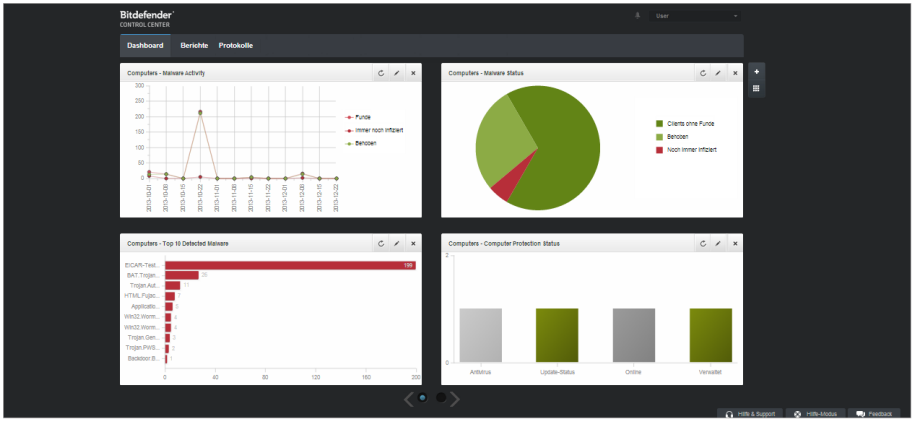
- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+
- Empfohlene Bildschirmauflösung: 1024x768 oder höher.

So stellen Sie eine Verbindung zum Control Center her:

Beachten Sie
Sollten Sie Ihr Passwort vergessen haben, verwenden Sie den Link für die Passwortwiederherstellung, um ein neues Passwort anzufordern. Sie müssen die E-Mail-Adresse Ihres Kontos angeben.

2.2. Control Center auf einen Blick

Control Center ist so aufgebaut, dass Sie schnellen Zugriff auf alle Funktionen erhalten.Verwenden Sie die Menüleiste im oberen Bereich, um durch die Konsole zu navigieren.



Das Dashboard

Berichterstatter können über die Menüleiste auf die folgenden Bereiche zugreifen:

Dashboard
Übersichtliche Diagramme anzeigen, die wichtige Sicherheitsinformationen über Ihr Netzwerk enthalten.

Berichte
Sicherheitsberichte über verwaltete Clients erhalten.

Protokolle
Das Benutzeraktivitätsprotokoll einsehen.

Außerdem erhalten Sie oben rechts in der Konsole über das Symbol **Benachrichtigungen** schnellen Zugriff auf die Seite **Benachrichtigungen**.

Wenn Sie den Mauszeiger über den Benutzernamen in der rechten oberen Ecke der Konsole bewegen, erhalten Sie die folgenden Optionen:

- **Mein Konto**. Klicken Sie auf diese Option, um Ihre Benutzerkontoinformationen und -einstellungen zu bearbeiten.
- **Abmelden**. Klicken Sie auf diese Option, um sich bei Ihrem Konto abzumelden.

In der rechten unteren Ecke der Konsole stehen die folgenden Links zur Verfügung:

- **Hilfe und Support**. Klicken Sie auf diese Schaltfläche, um Hilfe- und Support-Informationen zu erhalten.
- **Hilfe-Modus**. Klicken Sie auf diese Schaltfläche, um die Hilfefunktion zu aktivieren, mit der vergrößerbare Tooltipps für Control Center-Objekte angezeigt werden. Dadurch erhalten Sie nützliche Informationen zu den Funktionen des Control Center.
- **Feedback**. Klicken Sie auf diese Schaltfläche, um ein Formular anzuzeigen, in dem Sie uns Rückmeldung zu Ihren Erfahrungen mit Small Office Security zusenden können.

2.2.1. Tabellendaten

Tabellen kommen in der Konsole häufig zum Einsatz, um die Daten in einem übersichtlichen Format zu organisieren.

Die Berichtsübersicht - Berichtstabelle

Durch Tabellenseiten blättern

Tabellen mit mehr als 10 Einträgen haben mehr als eine Seite. Standardmäßig werden nur 10 Einträge pro Seite angezeigt.Verwenden Sie die Navigationsschaltflächen am unteren Rand der Tabelle, um zwischen den Seiten zu wechseln.Sie können die Anzahl der Einträge, die pro Seite angezeigt werden, ändern, indem Sie eine andere Option aus dem Menü neben den Navigationsschaltflächen wählen.

Nach bestimmten Einträgen suchen

Über die Suchfelder unter den Spaltenüberschriften können Sie leicht bestimmte Einträge finden.

Geben Sie den Suchbegriff in das entsprechende Feld ein.Passende Suchtreffer werden bereits während der Eingabe in der Tabelle angezeigt.Um den Inhalt der Tabelle wieder herzustellen, löschen Sie einfach die Suchfelder.

Daten sortieren

Sie können die Daten in der Tabelle nach dem Inhalt einer bestimmten Spalte sortieren, indem Sie auf die entsprechende Spaltenüberschrift klicken.Mit einem erneuten Klick auf die Spaltenüberschrift kehren Sie die Sortierreihenfolge um.

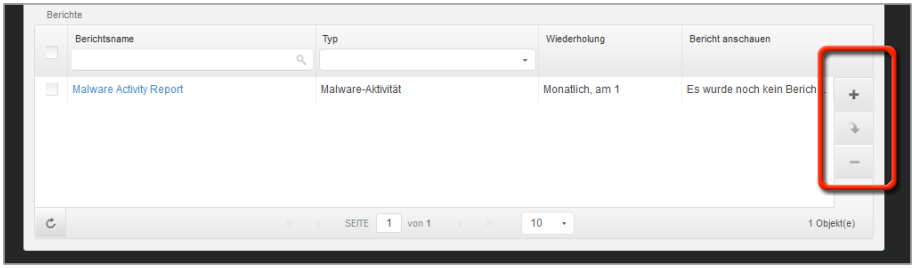
Tabellendaten aktualisieren

Um sicherzustellen, dass die aktuellsten Informationen angezeigt werden, klicken Sie im unteren linken Bereich der Tabelle auf **Aktualisieren**.

2.2.2. Symbolleisten

Im Control Center können Sie über Symbolleisten bestimmte Operationen ausführen, die zu dem Bereich gehören, indem Sie sich gerade befinden.Jede Symbolleiste besteht aus mehreren Symbolen, die meistens auf der rechten Seite der Tabelle angezeigt werden.Über die Symbolleiste im Bereich **Berichte** können Sie zum Beispiel die folgenden Aktionen ausführen:

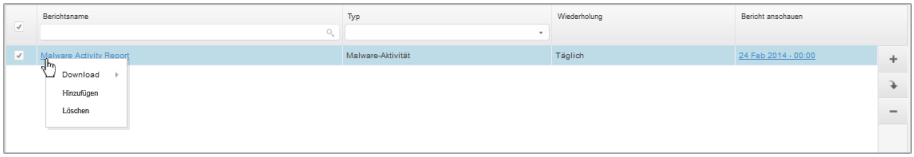
- Neuen Bericht erstellen.
- Geplant erstellte Berichte herunterladen.
- Einen geplanten Bericht löschen.



Die Berichtsübersicht - Symbolleisten

2.2.3. Kontextmenü

Die Symbolleistenbefehle stehen auch über das Kontextmenü zur Verfügung. Klicken Sie mit der rechten Maustaste auf den Bereich des Control Centers, den Sie gerade benutzen, und wählen Sie den gewünschten Befehl aus der Liste.



Die Berichtsübersicht - Kontextmenü

2.2.4. Dienstauswahl

Als Administrator oder Berichterstatter können Sie die Control Center-Dienste einzeln verwalten.Wählen Sie den gewünschten Dienst aus dem **Dienstmenü** in der rechten oberen Ecke der Seite.

Beachten Sie
Das Dienstmenü ist nur auf denjenigen Seiten vorhanden, auf denen es einen Sinn hat, Daten nacht Diensttyp zu filtern.

Das Dienstmenü enthält die folgenden Optionen:

- **Computer** (Security for Endpoints)
- **Mobilgeräte** (Security for Mobile Devices)

Beachten Sie
Es werden Ihnen nur diejenigen Dienste angezeigt, für die Ihnen der Administrator, der Ihren Benutzer zum Control Center hinzugefügt hat, Rechte erteilt hat.

2.3. Ändere Login Passwort

Nachdem Ihr Konto angelegt wurde, erhalten Sie eine E-Mail mit den Anmeldedaten.

Sofern Sie keine Active-Directory-Zugangsdaten für den Zugriff auf Control Center verwenden, sollten Sie wie folgt vorgehen:

- Ändern Sie das Standardpasswort nach dem ersten Aufrufen von Control Center.
- Ändern Sie Ihr Kennwort regelmäßig.

Um das Anmeldepasswort zu ändern:

1. Bewegen Sie den Mauszeiger auf Ihren Benutzernamen in der rechten oberen Ecke der Konsole, und wählen Sie **Mein Konto**.
2. Klicken Sie unter **Kontodetails** auf **Passwort ändern**.
3. Geben Sie Ihr aktuelles Passwort und das neue Passwort in die entsprechenden Felder ein.
4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

2.4. Verwalten Ihres Kontos

So überprüfen oder ändern Sie Ihre Kontodetails und -Einstellungen:

1. Bewegen Sie den Mauszeiger auf Ihren Benutzernamen in der rechten oberen Ecke der Konsole, und wählen Sie **Mein Konto**.

Das Benutzerkontomenü

2. Korrigieren oder aktualisieren Sie Ihre Kontoinformationen unter **Kontodetails**.Wenn Sie ein Active-Directory-Benutzerkonto verwenden, können Sie die Kontodetails nicht ändern.
   - **Nutzername.** Der Benutzername ist der eindeutige Identifikator eines Benutzerkontos und kann daher nicht geändert werden.
   - **Vollständiger Name.** Geben Sie Ihren vollen Namen ein.
   - **E-Mail.** Dies ist Ihre E-Mail-Adresse für die Anmeldung und den Kontakt.An diese Adresse werden Berichte und wichtige Sicherheitsbenachrichtigungen geschickt.Es werden automatisch E-Mail-Benachrichtigungen versandt, sobald wichtige Risikobedingungen im Netzwerk erkannt werden.
   - **Passwort.** Über den Link **Passwort ändern** können Sie Ihr Anmeldepasswort ändern.
3. Konfigurieren Sie die Kontoeinstellungen unter **Einstellungen** nach Ihren Wünschen.
   - **Zeitzone.** Wählen Sie im Menü die Zeitzone für das Konto. Die Konsole zeigt die aktuelle Zeit entsprechend der ausgewählten Zeitzone.
   - **Sprache.**Wählen Sie im Menü die Anzeigesprache für die Konsole aus.
   - **Zeitüberschreitung der Sitzung.** Legen Sie den Inaktivitätszeitraum fest, nach dem Ihre Sitzung abläuft.
4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

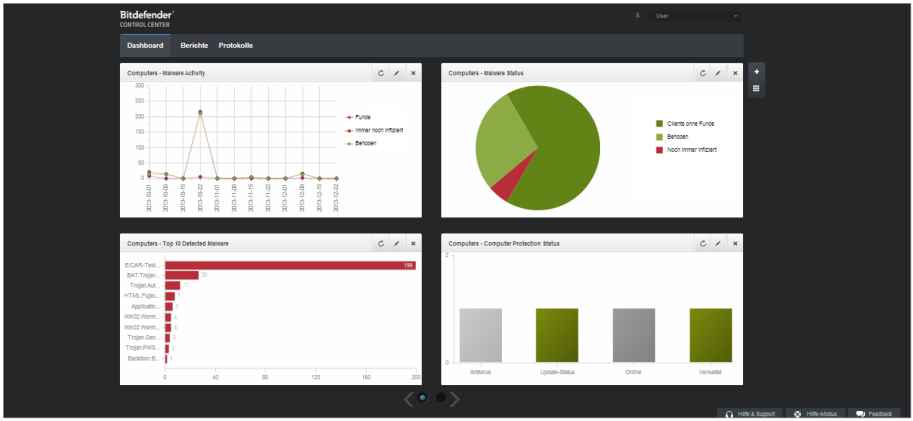
Beachten Sie

Sie können Ihr eigenes Konto nicht löschen.

3. Überwachungs-Dashboard

Das Control Center-Dashboard ist eine individuell anpassbare Anzeige, die Ihnen einen schnellen Überblick über die Sicherheitslage der geschützten Netzwerkobjekte verschafft.

In den Dashboard-Portlets werden verschiedenste Echtzeit-Sicherheitsinformationen in übersichtlichen Diagrammen angezeigt. Sie bieten einen schnellen Überblick über Bereiche, die Ihre Aufmerksamkeit erfordern.



Das Dashboard

Was Sie über Dashboard-Portlets wissen sollten:

- Die Control Center hat verschiedene vordefinierte Dashboard-Portlets für jeden Small Office Security-Sicherheitsdienst.
- Jedes Dashboard-Portlet enthält im Hintergrund einen detaillierten Bericht, der mit einem einfachen Klick auf das Diagramm abgerufen werden kann.
- Es gibt eine Reihe verschiedener Portlet-Arten, die unterschiedliche Informationen über den Schutz Ihrer Netzwerkobjekte enthalten, so zum Beispiel Update-Status, Malware-Status, Firewall-Aktivität usw. Weitere Informationen zu den verschiedenen Arten von Dashboard-Portlets finden Sie unter „Verfügbare Berichtstypen“ (S. 16).
- Die von den Portlets angezeigten Informationen beziehen sich ausschließlich auf die Netzwerkobjekte, die zu Ihrem Benutzerkonto gehören. Sie können mit dem **Portlet bearbeiten**-Befehl das Ziel für jedes Portlet individuell anpassen.

- Klicken Sie auf die einzelnen Einträge in der Diagrammlegende, um die entsprechende Variable, falls verfügbar, auf dem Graphen anzuzeigen bzw. auszublenden.
- Die Portlets werden in Vierergruppen angezeigt. Verwenden Sie den Schieberegler unten auf der Seite, um zwischen den Portlet-Gruppen umzuschalten.

Das Dashboard lässt sich nach individuellen Vorlieben leicht konfigurieren. Sie können Portlet-Einstellungen bearbeiten, neue Portlets hinzufügen, Portlets entfernen oder die bestehenden Portlets neu anordnen.

3.1. Portlet-Daten aktualisieren

Um sicherzustellen, dass das Portlet die aktuellsten Informationen anzeigt, klicken Sie auf das **Neu laden**-Symbol in der entsprechenden Titelleiste.

3.2. Portlet-Einstellungen bearbeiten

Einige der Portlets enthalten Statusinformationen, andere zeigen die Sicherheitsereignisse im letzten Berichtszeitraum an.Sie können den Berichtszeitraum eines Portlets anzeigen und konfigurieren, indem Sie auf die das Symbol **Portlet bearbeiten** in der entsprechenden Titelleiste klicken.

3.3. Ein neues Portlet hinzufügen

Sie können weitere Portlets hinzufügen, um bestimmte Informationen angezeigt zu bekommen.

So fügen Sie ein neues Portlet hinzu:

1. Gehen Sie zur Seite **Dashboard**.
2. Klicken Sie auf die Schaltfläche **Portlet hinzufügen** auf der rechten Seite des Dashboards.Das Konfigurationsfenster wird geöffnet.
3. Im Reiter **Details** können Sie die Details des Portlets konfigurieren:
   - Sicherheitsdienst (**Computer** oder **Mobile Geräte**)
   - Art des Hintergrundberichts
   - Aussagekräftiger Portlet-Name
   - Update-Intervall

   Weitere Informationen zu verfügbaren Berichtstypen finden Sie unter „Verfügbare Berichtstypen“ (S. 16).
4. Wählen Sie im Reiter **Ziele** die Netzwerkobjekte und Gruppen, die Sie einbeziehen möchten.
5. Klicken Sie auf **Speichern**.

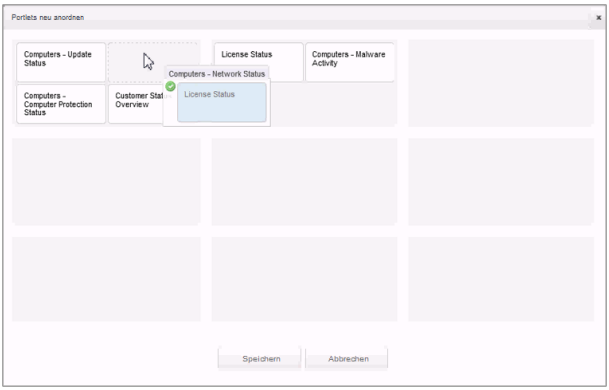
3.4. Ein Portlet entfernen

Sie können ein Portlet ganz einfach entfernen, indem Sie in seiner Titelleiste auf das Symbol **Entfernen** klicken.Wenn Sie ein Portlet einmal entfernt haben, können Sie es nicht wiederherstellen. Sie können aber ein neues Portlet mit genau denselben Einstellungen erstellen.

3.5. Portlets neu anordnen

Sie können die Portlets im Dashboard ganz nach Ihren Bedürfnissen anordnen. So ordnen Sie die Portlets neu an:

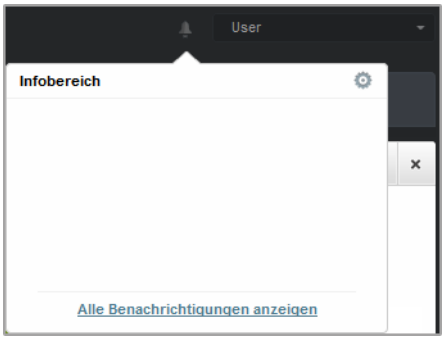
1. Gehen Sie zur Seite **Dashboard**.
2. Klicken Sie auf die Schaltfläche **Portlets neu anordnen** auf der rechten Seite des Dashboards.Die Portlet-Übersicht wird angezeigt.
3. Ziehen Sie die einzelnen Portlets mit der Maus an die gewünschte Stelle.
4. Klicken Sie auf **Speichern**.



Rearrange dashboard portlets

4. Benachrichtigungen

Je nach den Ereignissen, die in Ihrem Netzwerk auftreten, wird das Control Center verschiedene Benachrichtigungen anzeigen, die Sie über den Sicherheitsstatus Ihrer Umgebung auf dem Laufenden halten.Die Benachrichtigungen werden im **Benachrichtigungsbereich** in der oberen rechten Ecke des Control Center angezeigt.



Infobereich

Wenn ein neues Ereignis im Netzwerk gefunden wird, wird im Benachrichtigungsbereich ein rotes Symbol angezeigt, dass die Zahl der neu gefundenen Ereignisse angibt. Klicken Sie auf das Symbol, um eine Liste der gefundenen Ereignisse anzuzeigen.

4.1. Benachrichtigungstypen

Hier eine Liste der verfügbaren Benachrichtigungstypen:

Malware-Ausbruch
Diese Benachrichtigung wird an Benutzer gesendet, die mindestens 5 % ihrer verwalteten Netzwerkobjekte mit derselben Malware infiziert haben.

Update verfügbar
Informiert Sie über ein neues zur Verfügung stehendes Small Office Security-Update.

Lizenz läuft ab
Diese Benachrichtigung wird 30 und 7 Tage vor Ablauf der Lizenz sowie am Tag des Ablaufs selbst gesendet.

Benutzergrenze der Lizenz ist bald erreicht

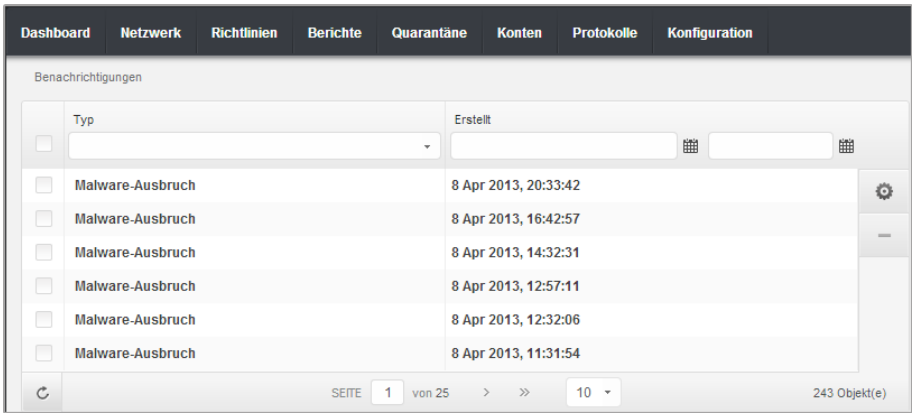
Diese Benachrichtigung wird gesendet, wenn 90 % der verfügbaren Lizenzen vergeben sind.

Die Benutzergrenze der Lizenz ist erreicht

Diese Benachrichtigung wird gesendet, wenn alle verfügbaren Lizenzen vergeben sind.

4.2. Benachrichtigungen anzeigen

Sie können die Benachrichtigungen anzeigen, indem Sie auf die Schaltfläche **Benachrichtigungsbereich** und anschließend auf **Alle Benachrichtigungen anzeigen** klicken. Eine Tabelle mit allen Benachrichtigungen wird angezeigt.



Die Benachrichtigungsübersicht

Abhängig von der Anzahl der Benachrichtigungen kann sich die Benachrichtigungstabelle über mehrere Seiten erstrecken (standardmäßig werden nur 10 Einträge pro Seite angezeigt).

Verwenden Sie die Navigationsschaltflächen am unteren Rand der Tabelle, um zwischen den Seiten zu wechseln.

Um die Anzahl der Einträge zu ändern, die pro Seite angezeigt werden, wählen Sie die entsprechende Option aus dem Menü neben den Navigationsschaltflächen aus.

Sollten zu viele Einträge angezeigt werden, können Sie die Suchfelder unterhalb der Spaltenüberschriften oder das Filtermenü über der Tabelle verwenden, um die angezeigten Daten zu filtern.Sie können zum Beispiel nach einem bestimmten Typ von Benachrichtigung suchen oder nur die in einem bestimmten Zeitraum erstellten Benachrichtigungen anzeigen.

- Sie können die Benachrichtigungen Filtern, indem Sie den gewünschten Benachrichtigungstyp aus dem Menü **Typ** wählen. Optional können Sie auch den Zeitraum, in dem die Benachrichtigungen erstellt wurden, eingrenzen, um die Zahl der in der Tabelle

angezeigten Einträge zu verringern, besonders wenn sehr viele Benachrichtigungen erstellt worden sind.

- Wenn Sie auf den Namen einer Benachrichtigung in der Tabelle klicken, werden weitere Details zu ihr angezeigt. Unter der Tabelle wird der Bereich **Details** angezeigt, in dem das Ereignis angezeigt wird, dass die Benachrichtigung verursacht hat.

4.3. Benachrichtigungen löschen

So löschen Sie Benachrichtigungen:

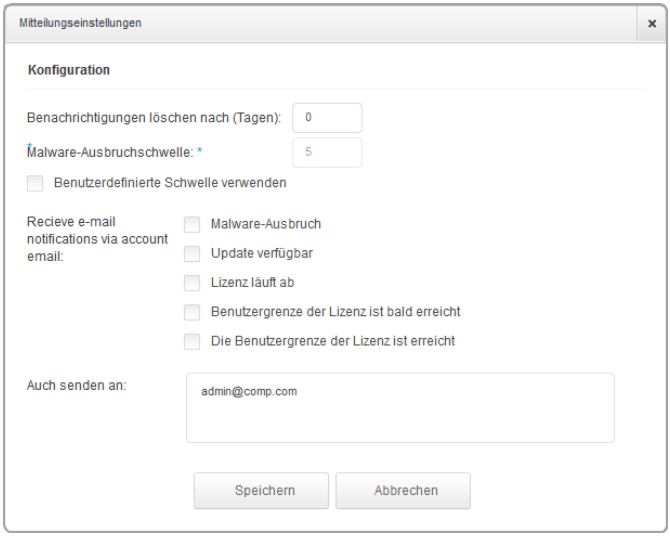
1. Klicken Sie auf die Schaltfläche **Benachrichtigungsbereich** auf der rechten Seite der Menüleiste und anschließend auf **Alle Benachrichtigungen anzeigen**. Eine Tabelle mit allen Benachrichtigungen wird angezeigt.
2. Wählen Sie die Benachrichtigungen, die Sie löschen möchten.
3. Klicken Sie auf die Schaltfläche **Löschen** auf der rechten Seite der Tabelle.

4.4. Benachrichtigungseinstellungen konfigurieren

Die Benachrichtigungstypen, die gesendet werden, sowie die E-Mail-Adresse, an die sie gesendet werden, können für jeden Benutzer einzeln festgelegt werden.

So konfigurieren Sie die Benachrichtigungseinstellungen:

1. Klicken Sie auf die Schaltfläche **Benachrichtigungsbereich** auf der rechten Seite der Menüleiste und anschließend auf **Alle Benachrichtigungen anzeigen**. Eine Tabelle mit allen Benachrichtigungen wird angezeigt.
2. Klicken Sie auf die Schaltfläche **Konfigurieren** auf der rechten Seite der Tabelle. Das Fenster **Benachrichtigungsseinstellungen** wird angezeigt.



Notifications Settings

Beachten Sie

Sie können das Fenster für die **Benachrichtigungseinstellungen** auch direkt über das **Konfigurieren**-Symbol oben rechts im **Infobereich**-Fenster aufrufen.

3. Wählen Sie die gewünschten Benachrichtigungstypen aus der Liste.Weitere Informationen finden Sie unter „Benachrichtigungstypen“ (S. 12)
4. Wenn Sie möchten, können Sie die Benachrichtigungen per E-Mail an eine bestimmte E-Mail-Adresse senden lassen. Geben Sie die E-Mail-Adressen in das dafür vorgesehene Feld ein; drücken Sie die Eingabetaste zwischen mehreren Adressen.
5. Klicken Sie auf **Speichern**.

5. Berichte verwenden

Mit Control Center können Sie Berichte über den Sicherheitsstatus der verwalteten Netzwerkobjekte zentral erstellen und anzeigen. Die Berichte können zu verschiedenen Zwecken eingesetzt werden, wie zum Beispiel:

- Einhaltung der Unternehmenssicherheitsrichtlinien überwachen und sicherstellen.
- Überprüfung und Bewertung des Netzwerksicherheitsstatus.
- Sicherheitsprobleme, Bedrohungen und Sicherheitslücken im Netzwerk erkennen.
- Sicherheitsvorfälle und Malware-Aktivität überwachen.
- Bereitstellung von übersichtlichen Daten zur Netzwerksicherheit für die Unternehmensführung.

Es stehen verschiedene Berichtstypen zur Verfügung, damit Sie einfachen Zugriff auf die von Ihnen benötigten Informationen erhalten. Diese Informationen werden in übersichtlichen interaktiven Diagrammen und Grafiken dargestellt, so dass Sie schnell den Sicherheitsstatus des Netzwerkes überprüfen und eventuelle Sicherheitsprobleme erkennen können.

Die Berichte können Daten vom gesamten Netzwerk der verwalteten Netzwerkobjekte beinhalten oder sich auf ausgewählte Gruppen konzentrieren. So können Sie mit einem einzigen Bericht folgendes erfahren:

- Statistische Daten zu allen oder Gruppen von verwalteten Netzwerkobjekten.
- Detailinformationen für jedes verwaltete Netzwerkobjekt.
- Die Liste von Computern, die bestimmte Kriterien erfüllen (zum Beispiel solche, deren Malware-Schutz deaktiviert ist).

Alle geplanten Berichte stehen im Control Center zur Verfügung, Sie können sie aber auch auf Ihrem Computer speichern oder per E-Mail versenden.

Verfügbare Formate sind u.a. Portable Document Format (PDF) und Comma-Separated Values (CSV).

5.1. Verfügbare Berichtstypen

Für jeden Sicherheitsdienst stehen eine Reihe von Berichtstypen zur Verfügung:

- Computer-Berichte
- Berichte zu mobilen Geräten

5.1.1. Computer-Berichte

Für Computer stehen die folgenden Berichtstypen zur Verfügung:

Update-Status

Zeigt Ihnen den Update-Status des auf den ausgewählten Computern installierten Endpoint Security an. Der Update-Status bezieht sich auf die Produktversion und die Version der Engines (Signaturen).

Über die verfügbaren Filter können Sie schnell feststellen, welche Clients über einen festgelegten Zeitraum aktualisiert oder nicht aktualisiert wurden.

Malware-Status

Hilft Ihnen dabei herauszufinden, wie viele und welche der ausgewählten Computer über einen bestimmten Zeitraum von Malware-Infektionen betroffen waren und wie mit der Bedrohung umgegangen wurde.

Computer werden nach diesen Kriterien in Gruppen aufgeteilt:

- Computer ohne Funde (über den festgelegten Zeitraum wurde keine Malware-Bedrohung gefunden).
- Computer mit behobener Malware (alle als infiziert erkannte Dateien wurden erfolgreich desinfiziert oder in die Quarantäne verschoben)
- Immer noch mit Malware infizierte Computer (der Zugriff auf einige der infizierten Dateien wurde verweigert)

Malware-Aktivität

Zeigt Ihnen übergreifende Informationen zu Malware-Bedrohungen, die über einen festgelegten Zeitraum auf den ausgewählten Computern gefunden wurden. Sie sehen:

- Anzahl der Funde (gefundene Dateien, die mit Malware infiziert sind)
- Anzahl der behobenen Infektionen (Dateien, die erfolgreich desinfiziert oder in die Quarantäne verschoben wurden)
- Anzahl der nicht behobenen Infektionen (Dateien, die nicht desinfiziert werden konnten, auf die der Zugriff aber verweigert wurde; so z. B. eine infizierte Datei, die mit einem proprietären Archivformat gespeichert wurde)

Netzwerkstatus

Zeigt Ihnen detaillierte Information zum allgemeinen Sicherheitsstatus der ausgewählten Computer. Computer werden nach diesen Kriterien in Gruppen aufgeteilt:

- Problemstatus
- Verwaltungsstatus
- Infektionsstatus
- Status des Malware-Schutzes
- Produktupdate Status
- Lizenzierungsstatus

- Der Netzwerkaktivitätsstatus jedes Computers (online/offline). Wenn der Computer zum Zeitpunkt der Berichtserstellung offline ist, werden Datum und Uhrzeit angezeigt, zu der er zuletzt vom Control Center gesehen wurde.

Computer-Schutzstatus

Liefert Ihnen verschiedene Statusinformationen zu ausgewählten Computern in Ihrem Netzwerk.

- Status des Malware-Schutzes
- Endpoint Security-Update-Status
- Status der Netzwerkaktivität (online/offline)
- Verwaltungsstatus

Sie können nach Sicherheitsaspekt und -status filtern, um die Informationen zu erhalten, nach denen Sie suchen.

Top-10 der infizierten Computer

Zeigt von den ausgewählten Computern die 10 Computer mit den meisten Infektionen an, sortiert nach der Anzahl der Funde während eines bestimmten Zeitraums.

Beachten Sie

In der Detailtabelle wird sämtliche Malware angezeigt, die auf den Top-10 der infizierten Computer gefunden wurde.

Top-10 der gefundenen Malware

Zeigt Ihnen die 10 häufigsten Malware-Bedrohungen, die über einen bestimmten Zeitraum auf den ausgewählten Computern erkannt wurden.

Beachten Sie

In der Detailtabelle werden alle Computer angezeigt, die von einer der Top-10 der gefundenen Malware infiziert wurden.

Firewallaktivität

Informiert Sie über den Status des Firewall-Moduls von Endpoint Security. Hier sehen Sie die Anzahl der blockierten Verbindungsversuche und Port-Scans auf den ausgewählten Computern.

Blockierte Webseiten

Informiert Sie über den Status des Moduls Web-Steuerung von Endpoint Security. Hier sehen Sie die Anzahl der blockierten Websites auf den ausgewählten Computern.

Blockierte Anwendungen

Informiert Sie über den Status des Anwendungssteuerungsmoduls von Endpoint Security. Hier sehen Sie die Anzahl der blockierten Anwendungen auf den ausgewählten Computern.

Identitätsschutz

Informiert Sie über den Status des Identitätsschutzmoduls von Endpoint Security. Hier sehen Sie die Anzahl der blockierten E-Mails und Websites auf den ausgewählten Computern.

Phishing-Schutz-Aktivität

Informiert Sie über den Status des Phishing-Schutz-Moduls von Endpoint Security. Hier sehen Sie die Anzahl der blockierten Websites auf den ausgewählten Computern.

Vom Verhaltens-Scan blockierte Anwendungen

Informiert Sie über die von der Active Virus Control (AVC) / dem Angrifferkennungssystem (IDS) blockierte Anwendungen. Sie können die Anzahl der von AVC / IDS blockierten Anwendungen für jeden ausgewählten Computer einsehen. Klicken Sie auf die Anzahl der blockierten Anwendungen für den gewünschten Computer, um die Liste der blockierten Anwendungen und die dazugehörigen Informationen anzuzeigen (Anwendungsname, der Blockierungsgrund, die Anzahl der blockierten Versuche sowie das Datum und der Zeitpunkt des zuletzt blockierten Versuchs).

5.1.2. Berichte zu mobilen Geräten

Beachten Sie

Malware-Schutz und damit verbundene Berichte stehen nur für Android-Geräte zur Verfügung.

Für mobile Geräte stehen die folgenden Berichtstypen zur Verfügung:

Malware-Status

Hilft Ihnen dabei herauszufinden, wie viele und welche der mobilen Zielgeräte über einen bestimmten Zeitraum von Malware-Infektionen betroffen waren und wie mit der Bedrohung umgegangen wurde. Mobil Geräte werden nach diesen Kriterien in Gruppen aufgeteilt:

- Mobile Geräte ohne Funde (über den festgelegten Zeitraum wurde keine Malware-Bedrohung gefunden).
- Mobile Geräte mit gehobener Malware (alle gefundenen Dateien wurden entfernt)
- Mobile Geräte mit bestehender Malware (einige der gefundenen Dateien wurden nicht gelöscht)

Malware-Aktivität

Liefert detaillierte Informationen zu den Malware-Bedrohungen, die über einen bestimmten Zeitraum auf den mobilen Zielgeräten gefunden wurden. Sie sehen:

- Anzahl der Funde (gefundene Dateien, die mit Malware infiziert sind)
- Anzahl der behobenen Infektionen (Dateien, die vom Gerät entfernt wurden.)
- Anzahl der nicht behobenen Infektionen (Dateien, die nicht vom Gerät entfernt wurden)

Top-10 der infizierten Geräte

Zeigt von den mobilen Zielgeräten die 10 Geräte mit den meisten Infektionen an, sortiert nach der Anzahl der Funde während eines bestimmten Zeitraums.

Beachten Sie

In der Detailtabelle wird sämtliche Malware angezeigt, die auf den Top-10 der infizierten mobilen Geräte gefunden wurde.

Top-10 der gefundenen Malware

Zeigt Ihnen die 10 häufigsten Malware-Bedrohungen, die über einen bestimmten Zeitraum auf den mobilen Zielgeräten erkannt wurden.

Beachten Sie

In der Detailtabelle werden alle mobilen Geräte angezeigt, die von einer der Top-10 der gefundenen Malware infiziert wurden.

Gerätekonformität

Informiert Sie über den Konformitätsstatus der mobilen Zielgeräte. Hier sehen Sie den Namen, den Status, das Betriebssystem und den Grund für die Nichtkonformität des Geräts.

Gerätesynchronisation

Informiert Sie über den Synchronisationsstatus der mobilen Zielgeräte. Hier können Sie den Namen des Geräts, den zugewiesenen Benutzer, den Synchronisationsstatus, das Betriebssystem und den Zeitpunkt, zu dem das Gerät zuletzt online gesehen wurde einsehen.

Blockierte Webseiten

Informiert Sie über die Anzahl der Versuche der Zielgeräte, über einen bestimmten Zeitraum auf Websites zuzugreifen, die durch **Internetzugangs**regeln blockiert wurden.

Bei Funden auf einen Gerät können Sie auf die Nummer in der Spalte **Blockierte Websites** klicken, um detaillierte Informationen für jede blockierte Webseite anzuzeigen, so zum Beispiel:

- Website-URL
- Richtlinienkomponente, die die Aktion vorgenommen hat
- Anzahl blockierter Versuche
- Zeitpunkt, zu dem die Website zuletzt blockiert wurde

Web-Sicherheit-Aktivität

Informiert Sie über die Anzahl der Versuche der Zielgeräte, über einen bestimmten Zeitraum auf Websites mit Sicherheitsbedrohungen (Phishing, Betrug, Malware oder unsichere Websites) zuzugreifen. Bei Funden auf einen Gerät können Sie auf die Nummer in der Spalte Blockierte Websites klicken, um detaillierte Informationen für jede blockierte Webseite anzuzeigen, so zum Beispiel:

- Website-URL
- Art der Bedrohung (Phishing, Malware, Betrug, unsicher)
- Anzahl blockierter Versuche
- Zeitpunkt, zu dem die Website zuletzt blockiert wurde

5.2. Berichte erstellen

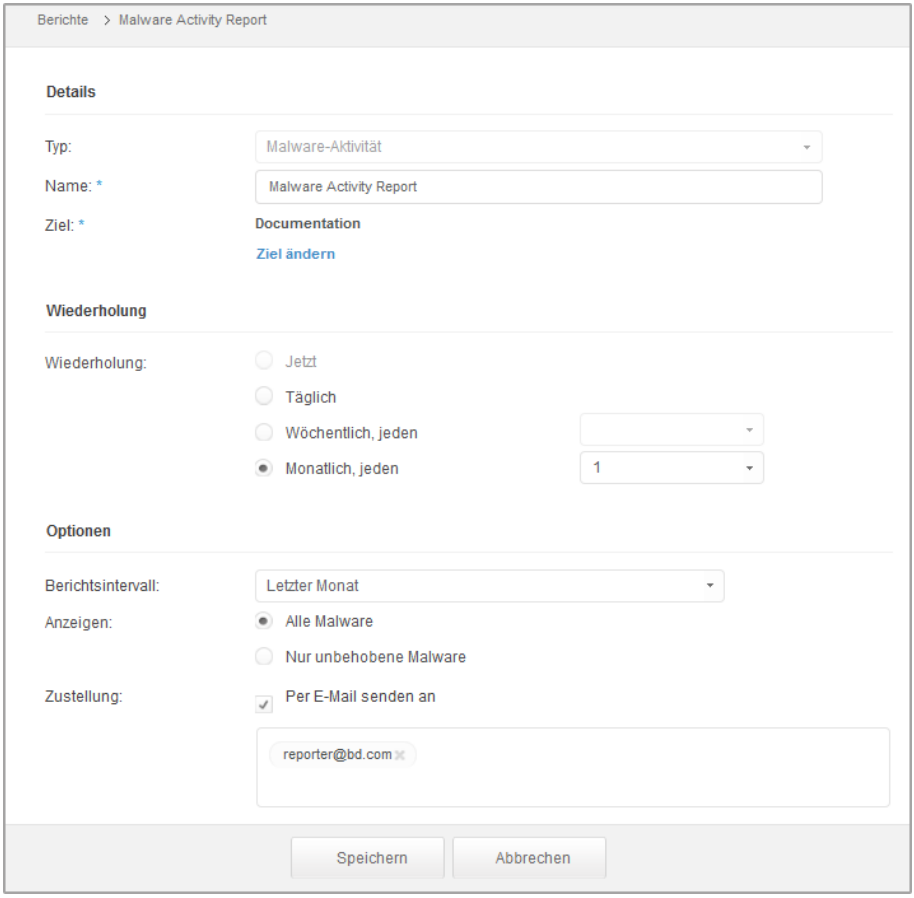
Sie können zwei verschiedene Kategorien von Berichten erstellen:

- **Sofortberichte.** Sofortberichte werden automatisch angezeigt, sobald sie erstellt wurden.
- **Geplante Berichte.** Geplante Berichte können so konfiguriert werden, dass sie zu einem bestimmten Zeitpunkt erstellt werden. Eine Liste aller geplanten Berichte finden Sie auf der Seite **Berichte**.

Wichtig
Sofortberichte werden automatisch gelöscht, wenn Sie die Berichtsseite schließen. Geplante Berichte werden auf der Seite **Berichte** gespeichert und angezeigt.

Um einen Bericht zu erstellen:

1. Gehen Sie zur Seite **Berichte**.
2. Wählen Sie den gewünschten Netzwerkobjekttyp aus der Dienstauswahl.
3. Klicken Sie auf die Schaltfläche + **Hinzufügen** auf der rechten Seite der Tabelle.



Optionen für Computer-Berichte

4. Wählen Sie den gewünschten Berichtstyp aus dem Menü aus.
5. Geben Sie einen eindeutigen Namen für den Bericht ein. Wenn Sie einen Namen festlegen, berücksichtigen Sie den Berichtstyp, das Berichtsziel und unter Umständen auch die Berichtsoptionen.
6. Konfigurieren Sie das Berichtsziel, indem Sie auf den Link **Ziel ändern** klicken. Wählen Sie die Gruppe, zu der Sie den Bericht erstellen möchten.
7. Berichtwiederholung konfigurieren (Zeitplan). Sie haben die Wahl, ob Sie den Bericht sofort (Sofortbericht) erstellen oder so planen, dass er täglich, wöchentlich (an einem bestimmten Tag der Woche) oder monatlich (an einem bestimmten Tag des Monats) erstellt wird.

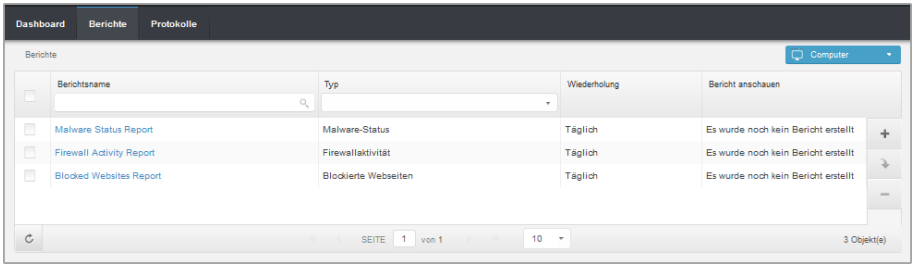
Beachten Sie
Geplante Berichte werden am geplanten Datum sofort nach 00:00 Uhr UTC (das ist die Standardzeitzone der GravityZone-Appliance) erstellt.

8. Konfigurieren Sie die Berichtsoptionen.
   a. Für die meisten Berichtstypen müssen Sie das Update-Intervall angeben. Der Bericht wird nur Daten für den ausgewählten Zeitraum enthalten.
   b. Viele Berichtsarten enthalten Filtermöglichkeiten, damit Sie die für Sie interessanten Informationen schnell finden können. Verwenden Sie die Filtermöglichkeiten, um nur die gewünschten Informationen abzurufen.

      Für Berichte über den **Update-Status** können Sie zum Beispiel auch nur die Computer anzeigen, die im ausgewählten Zeitraum aktualisiert wurden (bzw. nicht aktualisiert wurden) oder solche, die neu gestartet werden müssen, um ein Update abzuschließen.
   c. Um eingeplanten Bericht als E-Mail geschickt zu bekommen, wählen Sie die entsprechende Option.
9. Klicken Sie auf **Generieren**, um einen Sofortbericht zu erstellen, oder auf **Speichern**, um einen geplanten Bericht zu erstellen. Die Schaltfläche **Speichern** ändert sich automatisch zu **Generieren**, wenn Sie angegeben haben, einen Sofortbericht erstellen zu wollen.
   - Wenn Sie einen Sofortbericht erstellen, wird er sofort angezeigt, nachdem Sie auf **Generieren** geklickt haben. Die Zeit, die bis zur Fertigstellung eines Berichts benötigt wird, hängt von der Anzahl der verwalteten Computer ab. Bitte warten Sie, bis der angeforderte Bericht erstellt wurde.
   - Wenn Sie einen geplanten Bericht erstellt haben, wird dieser in der Liste auf der Seite **Berichte** angezeigt. Nachdem der Bericht erstellt wurde, können Sie ihn anzeigen, indem Sie auf den entsprechenden Link in der Spalte **Bericht anzeigen** auf der Seite **Berichte** klicken.

5.3. Geplante Berichte anzeigen und verwalten

Gehen Sie zum Anzeigen und Verwalten geplanter Berichte zur Seite **Berichte**.



Die Berichtsübersicht

Alle geplanten Berichte werden in einer Tabelle angezeigt. Sie können alle erstellten geplanten Berichte und nützliche Informationen dazu einsehen:

- Name und Art des Berichts.
- Den Zeitpunkt, zu dem der Bericht erstellt wird.

Beachten Sie
Geplante Berichte sind nur für den Benutzer verfügbar, der diese auch erstellt hat.

Um Berichte nach einer Spalte zu ordnen, klicken Sie einfach auf die Überschrift der jeweiligen Spalte. Mit einem erneuten Klick auf die Spaltenüberschrift können Sie die Sortierungsrichtung ändern

Die Berichtdetails werden in einer Tabelle angezeigt, die in mehreren Spalten verschiedene Informationen darstellt. Die Tabelle kann sich über mehrere Seiten erstrecken (standardmäßig werden pro Seite nur 10 Einträge angezeigt). Mit den Schaltflächen am unteren Rand der Tabelle können Sie durch die Detailseiten blättern.

Um die Suche nach Informationen zu beschleunigen, verwenden Sie die Suchfelder oder die Filtermöglichkeiten unter den Spaltenüberschriften.

Um die Berichtdetails nach einer bestimmten Spalte zu sortieren, klicken Sie einfach auf die entsprechend Spaltenüberschrift. Mit einem erneuten Klick auf die Spaltenüberschrift können Sie die Sortierungsrichtung ändern

Sie können das Suchfeld leeren, indem Sie mit dem Mauszeiger darüber fahren und auf das **Löschen**Symbol klicken.

Um sicherzustellen, dass die neuesten Informationen angezeigt werden, klicken Sie im unteren linken Bereich der Tabelle auf das Symbol **Aktualisieren**.

5.3.1. Berichte betrachten

So zeigen Sie einen Bericht an:

1. Gehen Sie zur Seite **Berichte**.

2. Sortieren Sie die Berichte nach Namen, Typ oder Wiederholung, um den gewünschten Bericht leichter zu finden.
3. Klicken Sie in der Spalte **Bericht anschauen** auf den entsprechenden Link, um den Bericht anzuzeigen.

Alle Berichte haben eine Zusammenfassungsteil (die obere Hälfte der Berichtsseite) und einen Detailsteil (die untere Hälfte der Berichtsseite).

- Der Zusammenfassungsbereich enthält statistische Daten (Kuchendiagramme und Grafiken) für alle ausgewählten Netzwerkobjekte oder Gruppen sowie allgemeine Informationen über den Bericht wie den Berichtszeitraum (sofern anwendbar), Berichtsziel, usw.
- Der Detailbereich enthält detaillierte Informationen zu jedem verwalteten Netzwerkobjekt.

Beachten Sie

- Sie können die im Diagramm angezeigten Informationen anpassen, indem Sie auf die Einträge in der Legende klicken und damit die entsprechenden Daten anzeigen oder ausblenden.
- Klicken Sie auf den Bereich der Grafik, der Sie interessiert, um die dazugehörigen Details in der Tabelle unter dem Diagramm anzuzeigen.

5.3.2. Geplante Berichte bearbeiten

Beachten Sie

Wenn Sie einen geplanten Bericht bearbeiten, werden sämtliche Änderungen mit der nächsten Ausführung des Berichts wirksam. Zuvor erstellte Berichte sind von den Änderungen nicht betroffen.

Um die Einstellungen eines geplanten Berichts zu ändern:

1. Gehen Sie zur Seite **Berichte**.
2. Klicken Sie auf den Berichtnamen.
3. Ändern Sie die Berichtseinstellungen nach Bedarf. Sie können die folgenden Änderungen vornehmen:
   - **Berichtsname.** Geben Sie dem Bericht einen eindeutigen Namen, der seinen Inhalt widerspiegelt. Wenn Sie einen Namen festlegen, berücksichtigen Sie den Berichtstyp, das Berichtsziel und unter Umständen auch die Berichtsoptionen. Berichte die anhand eines geplanten Berichts erstellt werden, erhalten auch den entsprechenden Namen.
   - **Berichtsziel.** Die ausgewählte Option weist auf die Art des aktuellen Berichtsziels hin (entweder Gruppen oder einzelne Netzwerkobjekte). Klicken Sie auf den entsprechenden Link, um das aktuelle Berichtsziel anzuzeigen. Sie können das Berichtsziel ändern, indem Sie die Gruppen oder Netzwerkobjekte auswählen, die in dem Bericht eingeschlossen werden sollen.

- **Berichtwiederholung (Planen).** Sie können festlegen, ob der Bericht täglich, wöchentlich (an einem bestimmten Tag der Woche) oder monatlich (an einem bestimmten Tag des Monats) automatisch erstellt werden soll. Abhängig von dem ausgewählten Zeitplan wird der Bericht nur Daten vom letzten Tag, aus der letzten Woche oder dem letzten Monat enthalten.
- **Berichtsoptionen.** Der Bericht wird nur Daten aus dem ausgewählten Update-Intervall enthalten. Sie können das Intervall ab der nächsten Ausführung ändern. Sie können den Bericht auch per E-Mail erhalten. Die meisten Berichte enthalten Filtermöglichkeiten, damit Sie die für Sie interessanten Informationen schnell finden können. Wenn Sie den Bericht in der Konsole anzeigen, sind unabhängig von den gewählten Optionen immer alle Informationen verfügbar. Wenn Sie den Bericht herunterladen oder per E-Mail versenden, werden nur die Berichtszusammenfassung und die ausgewählten Informationen in der PDF-Datei enthalten sein. Die Berichtsdetails sind nur im CSV-Format verfügbar.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

5.3.3. Geplante Berichte löschen

Wenn ein geplanter Bericht nicht mehr benötigt wird, empfiehlt es sich, diesen zu löschen. Durch das Löschen eines geplanten Berichts werden alle Berichte, die dieser bis zu diesem Zeitpunkt automatisch erstellt hat, gelöscht.

Um einen geplanten Bericht zu löschen:

1. Gehen Sie zur Seite **Berichte**.
2. Wählen Sie den Bericht, die Sie löschen möchten.
3. Klicken Sie auf die Schaltfläche − **Löschen** auf der rechten Seite der Tabelle.

5.4. Berichte speichern

Standardmäßig werden geplante Berichte automatisch im Control Center gespeichert.

Wenn Sie Berichte über einen längeren Zeitraum hin benötigen, können Sie sie auf Ihrem Computer abspeichern. Die Zusammenfassung des Berichts ist im PDF-Format verfügbar; die Berichtsdetails sind jedoch nur im CSV-Format verfügbar.

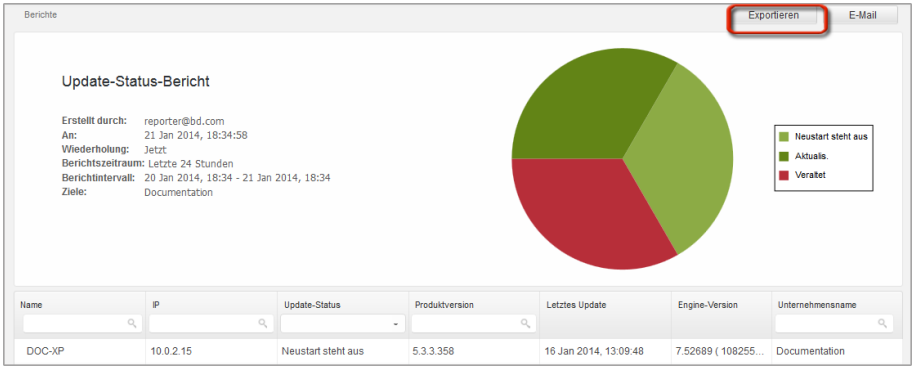
Sie können Berichte auf zweierlei Weise speichern:

- Exportieren
- Download

5.4.1. Berichte exportieren

So exportieren Sie den Bericht auf Ihren Computer:

1. Klicken Sie in der oberen rechten Ecke der Berichtseite auf **Exportieren**.



Berichte - Exportoption

2. Wählen Sie das gewünschte Format für den Bericht:
   - Portabeles Dokumentenformat (PDF) oder
   - Comma-separated values (CSV)
3. Je nach Ihren Browser-Einstellungen wird die Datei automatisch an einen Standard-Speicherort heruntergeladen, oder es wird ein Download-Fenster angezeigt, in dem Sie den Zielordner angeben können.

5.4.2. Berichte herunterladen

Einen Berichtsarchiv enthält sowohl die Zusammenfassung als auch die Details eines Berichts.

So laden Sie ein Berichtsarchiv herunter:

1. Gehen Sie zur Seite **Berichte**.
2. Wählen Sie den Bericht, den Sie speichern möchten.
3. Klicken Sie auf die Schaltfläche **Herunterladen** und wählen Sie entweder **Letzte Instanz**, um die zuletzt erstellte Instanz des Berichts herunterzuladen, oder **Vollständiges Archiv**, um ein Archiv herunterzuladen, das sämtliche Instanzen enthält.

   Je nach Ihren Browser-Einstellungen wird die Datei automatisch an einen Standard-Speicherort heruntergeladen, oder es wird ein Download-Fenster angezeigt, in dem Sie den Zielordner angeben können.

5.5. Berichte per E-Mail versenden

Sie können Berichte mit den folgenden Optionen per E-Mail versenden:

1. Um einen Bericht, den Sie gerade anzeigen, per E-Mail zu versenden, klicken Sie auf die Schaltfläche **E-Mail** in der rechten oberen Ecke der Berichtsseite. Der Bericht wird an die mit Ihrem Konto verknüpften E-Mail-Adresse gesendet.
2. So konfigurieren Sie den Versand geplanter Berichte per E-Mail:
   a. Gehen Sie zur Seite **Berichte**.
   b. Klicken Sie auf den gewünschten Berichtnamen.
   c. Wählen Sie unter **Optionen > Zustellung** den Punkt **Per E-Mail senden an**.
   d. Geben Sie die gewünschte E-Mail-Adresse im Feld darunter ein. Sie können beliebig viele E-Mail-Adressen hinzufügen.
   e. Klicken Sie auf **Speichern**.

Beachten Sie
In der PDF-Datei, die per E-Mail gesendet wird, sind nur die Berichtszusammenfassung und das Diagramm enthalten. Die Berichtsdetails sind in der CSV-Datei enthalten.

5.6. Berichte ausdrucken

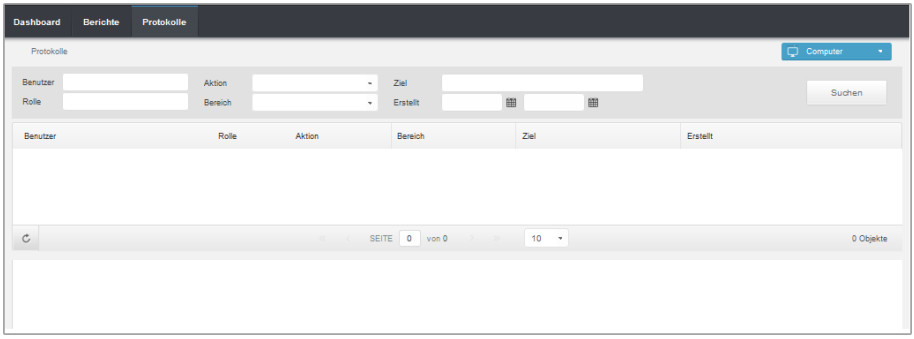
Das Control Center verfügt derzeit über keine Druckoptionen.Um einen Bericht zu drucken, müssen Sie ihn zunächst auf Ihrem Computer speichern.

6. Benutzeraktivitätsprotokoll

Das Control Center protokolliert alle von Benutzer ausgeführten Operationen und Aktionen. Protokolllisten enthalten je nach Ihrem Administratorrechten die folgenden Ereignisse:

- Anmelden und Abmelden
- Berichte erstellen, bearbeiten, umbenennen und löschen
- Dashboard-Portlets hinzufügen und entfernen

Einzelheiten zu den Benutzeraktivitäten können Sie einsehen, indem Sie zur Seite **Protokolle** gehen und das gewünschte Netzwerkobjekt aus der Dienstauswahl auswählen.



Die Protokollübersicht

Um aufgezeichnete Ereignisse anzuzeigen, an denen Sie interessiert sind, müssen Sie eine Suche definieren. Geben Sie die Suchkriterien in die verfügbaren Felder ein und klicken Sie auf **Suchen**. Alle zu Ihren Kriterien passenden Einträge werden in der Tabelle angezeigt.

Die Spalten geben nützliche Informationen zu den aufgelisteten Ereignissen:

- Der Name des Benutzers, der die Aktion durchgeführt hat.
- Benutzerrolle.
- Aktion, die das Ereignis ausgelöst hat.
- Art des Konsolenobjekts, das von der Aktion betroffen ist.
- Bestimmtes Konsolenobjekt, das von der Aktion betroffen ist.
- Zeitpunkt, zu dem das Ereignis eingetreten ist.

Um Ereignisse nach einer Spalte zu ordnen, klicken Sie einfach auf die Überschrift der jeweiligen Spalte. Klicken Sie erneut auf die Spaltenüberschrift, um die Sortierungsreihenfolge umzukehren.

Um Details zu einem Ereignis anzuzeigen, wählen Sie es aus und sehen Sie in den Abschnitt unter der Tabelle.

Um sicherzustellen, dass die neuesten Informationen angezeigt werden, klicken Sie im unteren linken Bereich der Tabelle auf **Aktualisieren**.

7. Hilfe erhalten

Sollten Probleme oder Fragen im Zusammenhang mit dem Control Center auftreten, wenden Sie sich bitte an einen Administrator.

Glossar

Adware

Adware wird häufig mit einer anderen Anwendung kombiniert, die kostenlos ist, solange der Nutzer die Adware akzeptiert. Adware-Anwendungen werden in der Regel installiert, nachdem der Nutzer einer Lizenzvereinbarung zugestimmt hat. In der Lizenzvereinbarung wird auch der Zweck der Anwendung genannt, und somit liegt keine Rechtswidrigkeit vor.

Allerdings können Popup-Anzeigen mit der Zeit sehr lästig werden und in manchen Fällen die Systemperformance beeinträchtigen. Zudem kann aufgrund der Daten, die manche dieser Programme sammeln, die Privatsphäre von Nutzern verletzt werden, die sich über die Bedingungen in der Lizenzvereinbarung nicht völlig im Klaren waren.

Antivirus-Storm

Eine intensive Beanspruchung von Systemressourcen, die auftritt, wenn Virenschutz-Software gleichzeitig mehrere virtuelle Maschinen auf einem einzigen physischen Host scannt.

Archive

Ein Datenträger, ein Magnetband oder ein Ordner mit Dateien, die von einer Datensicherung/BackUp erzeugt wurden.

Eine Datei, die eine oder mehrere Dateien in einem komprimierten Format enthält.

Backdoor (Hintertür)

Eine Sicherheitslücke eines Systems, die der Entwickler oder Administrator absichtlich hinterlässt. Der Grund dafür muss nicht immer bösartig sein. Manche Betriebssysteme haben schon standardmäßig privilegierte Konten eingerichtet, damit diese von den Kundendienst-Technikern oder Programmierern der Hersteller benutzt werden können.

Befehlszeile

Die Befehlszeile ist eine zeichenorientierte Benutzerschnittstelle. Die Kommunikation zwischen Benutzer und Computer findet ausschließlich durch die Eingabe von bestimmten Befehlen statt, die sich aus einzelnen Buchstabenfolgen zusammensetzen. Als Eingabegerät wird eine Tastatur benutzt. Die Verwendung einer Maus ist nicht möglich. Auf der Befehlszeile werden die einzelnen Anweisungen in einer bestimmten Befehlssprache eingegeben, die vom Computer und seiner Software ausgewertet und mit den entsprechenden Ergebnissen auf dem Ausgabegerät (meistens ein Monitor) wieder an den Benutzer übergeben werden.

Bootsektor

Der erste Sektor einer Festplatte oder Diskette. Hier liegen Daten, die das Betriebssystem zum Booten (Starten) braucht.

Bootvirus

Ein Virus, der den Bootsektor einer Festplatte oder eines Diskettenlaufwerks infiziert. Beim Versuch von einer Diskette, die mit einem Bootvirus infiziert ist, zu booten wird dieser im Arbeitsspeicher aktiviert. Bei jedem Neustart wird der Virus so im Arbeitsspeicher aktiviert und überträgt sich auf eingelegte Wechselmedien.

Cookie

In der Internetbranche werden mit Cookies kleine Dateien bezeichnet, die Daten über einzelne Computer enthalten und die von den Werbetreibenden analysiert und verwendet werden, um die Interessen und Vorlieben der Benutzer herauszufinden. Die Cookie-Technologie wird stetig weiterentwickelt mit dem Ziel Benutzern nur noch solche Werbung anzuzeigen, die ihren Interessen entspricht. Für viele ist dies ein zweischneidiges Schwert. Einerseits ist es praktisch, nur Anzeigen zu sehen, an denen man interessiert ist. Anderseits bedeutet es, dass Online-Aktivitäten der Benutzer gewissermaßen auf Schritt und "Klick" verfolgt werden. Es ist also verständlich, dass in diesem Zusammenhang Datenschutz ein umstrittenes Thema ist und viele sich unwohl fühlen, quasi als SKU-Nummer (die Strichcodes auf den Packungen, die im Geschäft an der Theke gescannt werden) betrachtet zu werden. Auch wenn diese Sicht etwas extrem erscheint, ist sie doch manchmal korrekt.

Dateierweiterung

Der Teil hinter dem Punkt im Dateinamen. Die Erweiterung oder Extension beschreibt die Art der Daten, die in einer Datei gespeichert sind.

Viele Betriebssysteme benutzen Dateierweiterungen, z.B. Unix, VMS, MS-DOS. Sie sind gewöhnlich ein bis drei Buchstaben lange (alte Betriebssysteme können oft nicht mehr als drei Buchstaben unterstützen). Beispiele sind "exe" ausführbare Dateien, "ps" für PostScript oder "txt" für Text-Dateien.

Durchsuchen

Kurzform für Web-Browser, ein Programm, mit dem Internetseiten aufgerufen und angezeigt werden können. Die bekanntesten Browser sind Mozilla Firefox und Microsoft Internet Explorer. Beide sind graphische Browser, was bedeutet, dass sie sowohl Grafiken als auch Texte anzeigen können. Weiterhin können die meisten Browser Multimedia-Daten wie Klang- und Videodateien anzeigen, wobei sie für diverse Formate Plug-Ins (zusätzliche Softwarekomponenten) benutzen.

Ereignisanzeige

Ereignisse oder Erscheinungen, die in einem Programm vorkommen. Ereignisse können Benutzeraktionen, wie zum Beispiel Mausklicks oder Tastatureingaben, oder Systemereignisse, wie zum Beispiel ungenügender Speicher, sein.

Fehlalarm

Erscheint, wenn ein Virenscanner eine Datei als infiziert erkennt, obwohl dies nicht der Fall ist.

Heuristik

Eine Methode, um neue Viren zu identifizieren. Diese Scan-Methode benötigt keine spezifischen Virussignaturen. Der Vorteil eines heuristischen Scans ist, dass man nicht von einer neuen Variante eines alten Virus getäuscht werden kann. Manchmal kann jedoch auch ein verdächtiger Code in einem normalen Programm gemeldet werden, ein sogenannter Fehlalarm oder "falsch-positive Meldung" wird angezeigt.

IP

Internet Protocol - Das TCP/IP Protokoll ist verantwortlich für die korrekte IP Adressierung und die korrekte Zustellung der Datenpakete.

Keylogger

Ein Keylogger ist eine Anwendung, die alles aufzeichnet, was Sie tippen.

Keylogger sind an sich nicht schädlich. Sie können auch legitim eingesetzt werden, um beispielsweise die Aktivitäten von Angestellten oder Kindern zu überwachen. Sie werden jedoch zunehmend von Cyber-Kriminellen mit bösartiger Absicht eingesetzt (um beispielsweise private Daten wie Benutzernamen oder Passwörter zu sammeln).

Logdatei (Berichtsdatei)

Eine Datei, die stattgefundene Aktivitäten aufzeichnet. Zum Beispiel speichert Bitdefender eine Prokolldatei mit den gescannten Pfaden, Ordnern, der Anzahl der gescannten Archive und Dateien sowie der Anzahl der gefundenen infizierten oder verdächtigen Dateien.

Makrovirus

Eine Virusform, die in einem Dokument als eingebettetes Makro verschlüsselt wird. Viele Anwendungen, wie Microsoft Word und Excel, unterstützen leistungsstarke Makrosprachen.

Diese Anwendungen ermöglichen das Einbetten eines Makros in ein Dokument, welches dann bei jedem Öffnen des Dokuments ausgeführt wird.Ein Makro ist eine Aufzeichnung des Ablaufs von Routineaufgaben innerhalb des makrofähigen Programms, das dann immer wieder verwendet werden kann.

Malware

Malware ist der Sammelbegriff für alle Software-Arten, die darauf ausgelegt sind, Schaden zu verursachen - das Wort setzt sich zusammen aus den englischen Begriffen malicious und software, also bösartige Software. Der Begriff hat sich noch nicht vollständig durchgesetzt, wird aber immer häufiger als Oberbegriff gebraucht, wenn von Viren, Trojanern, Würmern und Malicious Mobile Code die Rede ist.

Malware-Signatur

Malware-Signaturen sind Codebruchstücke, die aus aktuellen Malware-Beispielen extrahiert werden. Diese werden von Antiviren-Programmen zum Musterabgleich und zur Aufspürung von Malware verwendet.Signaturen werden auch genutzt, um den Malware-Code aus infizierten Dateien zu entfernen.

Die Bitdefender Malware-Signatur-Datenbank ist eine Sammlung von stündlich durch Bitdefender-Mitarbeiter upgedateten Malware-Signaturen.

Nicht heuristisch

Diese Scan-Methode beruht auf spezifischen Virussignaturen. Der Vorteil eines nicht-heuristischen Scans ist, dass er nicht von einem Scheinvirus getäuscht werden kann und so Fehlalarme verhindert.

Phishing

Das Senden einer E-Mail an einen Benutzer, in der der Sender sich als Vertreter eines legitimen Unternehmens ausgibt und versucht, den Empfänger so zu manipulieren, dass er persönliche Informationen preisgibt, die dann zum Diebstahl der Identität verwendet werden können. Die E-Mail leitet den Benutzer dann auf eine Webseite, auf der er aufgefordert wird, vertrauliche Daten wie Kreditkartennummern, TANs oder PINs preiszugeben. Es wird oft vorgegeben, dass dies aus Gründen der Aktualisierung geschehen soll. Diese Webseiten sind jedoch gefälscht und wurden eigens für den Diebstahl dieser Daten eingerichtet.

Polymorpher Virus

Ein Virus, der seine Form mit jeder Datei, die er infiziert, ändert. Da diese Viren kein beständiges binäres Muster haben, sind sie sehr schwer zu erkennen.

Rootkit

Bei einem Rootkit handelt es sich um eine Sammlung von Software-Tools, mit denen auf ein System mit Administratorrechten zugegriffen werden kann. Der Begriff wurde ursprünglich nur für UNIX-Systeme verwendet und beschrieb rekompilierte Tools, mit denen sich Angreifer Administratorrechte verschaffen und so ihre Anwesenheit vor den tatsächlichen Administratoren verbergen konnten.

Die Hauptaufgabe eines Rootkits besteht darin, Prozesse, Dateien und Protokolle zu verstecken. Sie können auch Daten von Terminals, Netzwerkverbindungen oder Peripheriegeräten abfangen, falls Sie eine entsprechende Software eingebaut haben.

Rootkits sind nicht grundsätzlich schädlich. Einige Systeme und Anwendungen verstecken z. B. wichtige Dateien mithilfe von Rootkits. Sie werden jedoch oft dazu missbraucht, Malware zu verbergen oder unbemerkt einen Eindringling einzuschleusen. In Kombination mit Malware stellen sie eine große Gefahr für Ihr System dar. Denn sie können den Datenverkehr abhören, Sicherheitslücken in Ihrem System schaffen, Dateien und Zugangsdaten verändern, und das alles, ohne entdeckt zu werden.

Schnittstelle

Stelle eines Rechners, an die ein Gerät angeschlossen werden kann. Rechner haben verschiedenartige Schnittstellen. Im Inneren gibt es Schnittstellen zum Anschluss von Festplatten, Grafikkarten und Tastaturen. Extern haben Rechner Schnittstellen zum Anschluss von Modems, Druckern und anderen Peripheriegeräten.

In TCP/IP und UDP Netzwerken, ein Endpunkt zu logischen Verbindungen. Die Schnittstellennummer gibt die Art der Schnittstelle an. Zum Beispiel, Schnittstelle 80 wird für HTTP Traffic verwendet.

Script

Ein anderer Begriff für Makro- oder Batchdatei. Ein Skript ist eine Befehlsliste, die ohne Benutzereingriff ausgeführt werden kann.

Spam

Junk-E-Mail oder Junk-Postings in Newsgroups. Im Allgemeinen versteht man darunter jede Art von unerwünschter E-Mail.

Spyware

Software, die unentdeckt vom Nutzer private und geheime Anwenderdaten über seine Internetverbindung abgreift. Dies geschieht in der Regel zu Werbezwecken. Typischerweise sind Spyware-Anwendungen als verborgene Komponenten in Freeware- oder Shareware-Programmen enthalten, die aus dem Internet heruntergeladen werden können. Die große Mehrzahl von Shareware- und Freeware-Anwendungen ist natürlich frei von Spyware. Ist die Spyware einmal installiert, überwacht sie die Nutzeraktivitäten und überträgt diese Daten im Hintergrund an einen Dritten. Spyware kann auch Informationen über E-Mail-Adressen und sogar Passwörter und Kreditkartennummern sammeln.

Einem Trojanischen Pferd ähnelt Spyware darin, dass die Anwender das Produkt unwissentlich gemeinsam mit etwas anderem installieren. Opfer von Spyware wird man oft dann, wenn man sich bestimmte Peer-to-Peer-Dateiaustauschprogramme herunterlädt.

Ganz abgesehen von den Fragen der Ethik und des Datenschutzes belegt Spyware auch unnötig Systemressourcen und Bandbreite, indem über die Internetverbindung des Nutzers Informationen an den Spyware-Heimatserver gesendet werden. Da Spyware Speicher und Systemressourcen verbraucht, können die im Hintergrund laufenden Anwendungen zu Systemabstürzen oder allgemeiner Systeminstabilität führen.

Symbolleiste

Die Symbolleiste wurde mit Windows 95 eingeführt und befindet sich auf der Windows Task-Leiste (gewöhnlich unten rechts, dort wo sich auch die Uhrzeit befindet). Sie enthält kleine Symbole zur Information und zum leichteren Zugriff auf Systemfunktionen wie Drucker, Modems, Lautstärke und anderes. Um auf die Details und Optionen dieser

Funktionen zuzugreifen, ist ein Doppelklick oder ein Klick mit der rechten Maustaste erforderlich.

TCP/IP

Transmission Control Protocol/Internet Protocol – im Internet weit verbreiteter Netzwerkprotokollsatz, der die Kommunikation zwischen verbundenen Computernetzwerken mit verschiedenen Hardware-Architekturen und Betriebssystemen ermöglicht. TCP/IP bietet eine Möglichkeit, all diese unterschiedlichen Komponenten zu Kommunikationszwecken miteinander zu verbinden.

Trojaner

Ein bösartiges Programm, das sich als eine legitime Anwendung ausgibt. Im Unterschied zu Viren vervielfältigen sich die Trojaner (auch "trojanische Pferde" genannt) nicht, aber sie können ebenso schädlich sein. Einer der heimtückischsten Trojaner ist ein Programm, das behauptet Ihren Rechner von Viren zu befreien, stattdessen aber den Rechner infiziert.

Der Begriff entstammt einer Geschichte in Homers "Ilias", in der die Griechen ihren Feinden, den Trojanern, angeblich als Sühnegabe ein riesiges hölzernes Pferd schenkten. Aber nachdem die Trojaner das Pferd in die Stadt gebracht hatten, schlichen sich die im Bauch des hölzernen Pferdes versteckten Soldaten bei Nacht heraus, öffneten die Tore der Stadt und ermöglichten somit ihren Landsleuten, in die Stadt einzudringen und auf diese Weise Troja zu besetzen.

Update

Eine neue Software- oder Hardwareversion, die eine ältere Version desselben Produkts ersetzt. Die Update-Installationsroutine eines Programms prüft oft, ob eine ältere Versionen auf dem Rechner installiert ist, da sonst kein Update installiert werden kann.

Bitdefender verfügt über ein eigenes Update-Modul, das die manuelle oder automatische Suche nach Updates ermöglicht.

Virus

Ein Programm oder ein Stück Code, das auf einen Rechner kopiert wird und sich allein ausführt, ohne dass es der Besitzer des Rechners will oder merkt. Die meisten Viren können sich auch selbst vervielfältigen. Alle Computerviren wurden von Menschen programmiert. Ein Virus, der sich immer wieder vervielfältigen kann, ist sehr einfach zu programmieren. Sogar ein solch einfacher Virus kann gefährlich sein, da er im Handumdrehen sämtlichen Arbeitsspeicher belegen und so das System lahmlegen kann. Noch gefährlicher sind Viren, die sich über Netzwerke selbst weiterversenden und Sicherheitssysteme umgehen.

Wurm

Ein Programm, das sich selbst kopiert und über ein Netzwerk verbreitet. Es kann sich nicht an andere Programme anhängen.