



## Fünf Best Practices zur Sicherheit am Webgateway für das Jahr 2009

Online-Sicherheit ist und bleibt eine der wichtigsten Angelegenheiten sowohl für einzelne Benutzer als auch für Unternehmen. Wir haben einige Tipps zusammengestellt, wie Sie wichtige Daten vor immer raffinierterer Malware und vor Netzwerkangriffen schützen können:

Im Folgenden werden fünf konkrete Beispiele beschrieben:

### 1 Treten Sie einer Community Watch bei

Aufgrund zunehmender Malware-Bedrohungen auf beliebten und vertrauenswürdigen Websites haben sich die Sicherheitsvorkehrungen maßgeblich verändert. Benutzer vereinigen sich in Community Watch-Systemen, die in Cloud-Diensten gehostet werden und so für gegenseitigen Schutz sorgen. Wenn eine Person auf mit Malware verseuchte Webinhalte stößt, wird die Community Watch durch eine entsprechende Anfrage aktualisiert und kann dank Cloud-Dienst alle Mitglieder der Community schützen. Die Community Watch kann eine größere Anzahl an Webinhalten erfassen als ein Einzelner und besitzt weitreichendere Verteidigungsmöglichkeiten und nutzbare Ressourcen als eine Einzelperson. Probieren Sie den Schutz durch eine Community Watch kostenlos von zu Hause aus. Informieren Sie sich unter [www.k9webprotection.com](http://www.k9webprotection.com).

### 2 Ändern Sie Ihre Verteidigungsstrategie „Einer gegen das Web“

Ihr Webgateway ist allein nicht in der Lage, gegen kriminelle Rechnetze zu bestehen, die von Datendiebstahl profitieren und ihre Reichweite und technische Überlegenheit kontinuierlich erweitern. Ihr Webgateway kann allein nicht mit den kollektiven Wissenssystemen mithalten, die Malware, Webbedrohungen und neue Webinhalte auf verschiedenen Sites aufdecken. Signaturen und tägliche Aktualisierungen gewährleisten keinen ausreichenden Schutz. Ihr Webgateway sollte stattdessen eine Kombination aus Community Watch-Diensten für den Schutz nutzen und Aktualisierungen im Abstand von fünf Minuten durchführen. Nutzen Sie diese umfangreiche Schutzmöglichkeit, die von über 50 Millionen Benutzern unterstützt wird.

### 3 Stellen Sie Ihre Richtlinien von Produktivität auf Schutz um

Wenn Ihr Webgateway über ein Jahr alt ist, wurde es wahrscheinlich zur Steigerung der Produktivität eingesetzt, indem unerwünschte und unproduktive Websites blockiert wurden. Über 90 % der Malware befindet sich jedoch auf vertrauenswürdigen und beliebten Websites und macht das Web somit zu einem führenden Infektionsherd. Viele beliebte Sites fallen Angriffen durch Einschleusung von schadhaftem Code zum Opfer. Diese Angriffe führen zu transparenten Malware-Downloads, die von nicht klassifizierten Hosts stammen. Ein Großteil der Webgateway-Richtlinien wurde vor dem Hintergrund entwickelt, die Produktivität der Benutzer zu steigern und lässt den Zugriff auf nicht klassifizierte Hosts und Downloads zu. Für einen verbesserten Schutz müssen Webgateway-Richtlinien so angepasst werden, dass Downloads von verdächtigen, nicht klassifizierten Hosts und Sites blockiert und Zugänge für Malware gesperrt werden.

### 4 Nutzen Sie Echtzeitdienste für Inhaltsklassifizierungen

URL-Filter-Methoden, die statische URL-Listen auf Kundensites nur täglich aktualisieren, sind von Webinhalten überfordert. Darüber hinaus kann eine URL-Filterliste keine Bewertung für alle bestehenden Websiteinhalte liefern und auch weder mit den häufigen Änderungen und neu hinzukommenden Webinhalten mithalten noch Kategorien im Minutentakt aktualisieren. Ein Rating-Service für Inhaltsklassifizierungen in Echtzeit, der neue Webinhalte bearbeitet, erhöht den Wert einer URL-Filterlösung. Zudem ist dieser Service auch für Remotebenutzer wertvoll, denn er bietet sofortige Inhaltsklassifizierungen und definiert angemessene Benutzerrichtlinien am Webgateway und für Remote-Laptops.



#### 5 Schützen Sie Ihre Remotebenutzer

De-Perimeterisierung schützt Benutzer an externen Standorten wie Flughäfen, Hotels, Cafés und zu Hause. Durch die Zunahme von Laptops und den Rückgang des Desktopmarkts wird die Anzahl an Remotebenutzern kontinuierlich zunehmen. Daher muss der Netzwerkaufbau mit dem Ziel erweitert werden, mehr Remotebenutzer außerhalb des Webgateways einzubeziehen. Durch das Hinzufügen eines Client-Agenten, der mit einer Community Watch verbunden ist, können Remotebenutzer besser geschützt werden. Eine zentralisierte Richtlinienverwaltung kann mithilfe von Inhaltsklassifizierungen sowie einer Malwareblockierung bekannter Hosts, die von der Community Watch erkannt werden, einen noch besseren Schutz gewährleisten.

### Informationen zu Blue Coat Systems

Die Application Delivery Network-Lösungen von Blue Coat sorgen für eine intelligente Steuerung Ihres Netzwerks. Transparenz, Beschleunigung und Sicherheit werden kombiniert, um die Anwendungsleistung für jeden Benutzer innerhalb verteilter Unternehmensnetzwerke zu optimieren. Mit den Lösungen für Application Performance Monitoring, WAN-Optimierung und Secure Web Gateway von Blue Coat kann die IT zu größerer Effizienz, Effektivität und Wettbewerbsfähigkeit beitragen. Über 15.000 anspruchsvolle Unternehmen, darunter 81% der Fortune Global 500®, vertrauen ihre wichtigsten Anwendungen Blue Coat an. Weitere Informationen können Sie unter [www.bluecoat.com](http://www.bluecoat.com) abrufen.

Blue Coat Systems | Tel: +49 89 360 36-750 | Fax: +49-89-36036-700 | [www.bluecoat.de](http://www.bluecoat.de)

Copyright © 2009 Blue Coat Systems, Inc. Alle Rechte vorbehalten. Dieses Dokument darf ohne die ausdrückliche schriftliche Genehmigung von Blue Coat Systems, Inc. weder vollständig noch auszugsweise reproduziert oder auf elektronische Medien übertragen werden. Änderungen vorbehalten. Die in diesem Dokument enthaltenen Informationen wurden mit größter Sorgfalt zusammengestellt.

Dennoch übernimmt Blue Coat Systems, Inc. keine Haftung für Schäden, die aus der Nutzung dieses Dokuments entstehen. Blue Coat ist eine eingetragene Marke von Blue Coat Systems, Inc. in den USA und weltweit. Alle anderen in diesem Dokument genannten Marken sind Eigentum der jeweiligen Rechteinhaber. v.DS-SBTOP5-WEBGATEWAY-v1-1208