Internetinhalte sicher und effizient filtern

Das Internet ist heute nicht nur Kommunikationsmedium Nr. 1, sondern auch ein beliebter Zeitvertreib. Neben den Vorteilen einer schnellen Kommunikation und der hohen Produktivität wird das Internet aber auch immer mehr zum Schauplatz krimineller Aktivitäten. Eine richtige Web-Content-Filtering-Strategie kann gezielt vor Angriffen schützen.

Hacker und Diebe nutzen die weltweite Verbreitung und Anwendungsvielfalt im Internet mittlerweile, um Dienste zu stören, Daten zu stehlen und auf kriminelle Weise an Geld zu kommen. Für Unternehmen, die sensible Daten zu verwalten haben, ist es daher umso wichtiger, frühzeitig eine umfassende Lösung zum Schutz dieser Daten einzuführen. Vor allem, wenn Daten über das Internet ausgetauscht werden, ist eine passende Lösung für das Filtern von Web-Inhalten notwendig, um vor bösen Überraschungen gefeit zu sein.

Spätestens seit ein Webzugang und E-Mail feste Bestandteile eines modernen Arbeitsplatzes sind, wird die Frage der privaten Internetnutzung in vielen Unternehmen diskutiert. In welchem Ausmass die Produktivität der Mitarbeiter tatsächlich darunter leidet, ist umstritten. Tatsache ist, dass die private Internetnutzung zulasten der Netzwerkperformance geht, da Bandbreite zusätzlich für andere als geschäftliche Zwecke abgezogen wird und Business-Applikationen «zu kurz» kommen. Abgesehen von der Infrastrukturbelastung geht es aber auch um den Schutz von Daten und Informationen. Über Chat-Seiten, Freemail-Systeme, Instant Messaging und Peer-to-Peer File-Sharing können vertrauliche Firmeninformationen gezielt weitergegeben werden oder auch an die breite Öffentlichkeit gelangen. Ausserdem steigt die Gefahr webbasierter Bedrohungen wie Viren, Würmer, Trojaner und Spyware, wenn Mitarbeiter Internetseiten aufrufen, die keinen Business-Bezug haben. Wird dabei auf unangemessene oder beleidigende Inhalte zugegriffen oder werden Copyrights, etwa beim Download von Musikdateien und Filmen, verletzt, haftet im Ernstfall nicht der Mitarbeiter, sondern häufig der Arbeitgeber.

Bild: Digitalstock/P. Reppert

Darüber hinaus greift auch der Gesetzgeber zunehmend regulierend in die Internetnutzung ein, um die Informationssicherheit zu fördern und den Kinder- und Jugendschutz zu stärken.

Secure Content Management sorgt für effizienten Schutz

Damit gesetzliche oder unternehmensinterne Richtlinien zur Internetnutzung gezielt umgesetzt werden können, muss der Zugriff auf unerlaubte Webseiten überwacht und geblockt werden. Dass bei der Fülle an möglichen Bedrohungen herkömmliche Sicherheitsmassnahmen wie Firewalls, IDS und hostbasierte Antivirenprogramme nicht mehr ausreichen, ist den Verantwortlichen für Security und Corporate Governance in den Unternehmen bewusst. Nicht umsonst wächst die Nachfrage nach «Secure Content Management» (SCM) Appliances wie Antivirus, Web Content Filtering und Messaging Security. IDC-Studien zeigen, dass die Nutzung von SCM-Appliances seit 2002 erheblich zugenommen hat. Der jährliche Umsatz auf dem SCM-Markt stieg von 4,2 Milliarden US-Dollar 2004 auf 7,5 Milliarden US-Dollar 2008. Dies entspricht einer kumulierten Wachstumsrate von 16 Prozent zwischen 2003 und 2008.

Die Qual der Wahl

Der Markt bietet eine grosse Auswahl an Technologien für die Internetüberwachung sowie für das Aufzeichnen und das Filtern webbasierter Inhalte. Im Allgemeinen sind zwei Richtungen zu unterscheiden: Software-Lösungen für Intel-basierte Server, die über einen «gespiegelten» Netzwerkport mit dem Netzwerk verbunden sind, und dedizierte Appliances, die inline im Netzwerk installiert werden, jeglichen Internetverkehr beobachten und schnell auf nicht autorisierte und bösartige Inhalte reagieren können.

Die gängigsten Methoden für das Filtern von Web Content sind die sogenannte «schwarze Liste», die URL-Blockade und die Kate-

gorieblockade. Eine schwarze Liste enthält einzelne sowie zusammengesetzte Wörter. URL-Adressen und Internetinhalte werden mit dieser Liste an Stichwörtern verglichen und unerlaubte Webseiten geblockt. Auch die URL-Blockade ist eine schwarze Liste, die jedoch bekannte schädliche oder unerlaubte URL-Adressen umfasst. Sie ist beliebig erweiterbar und bietet sich auch dafür an, Richtlinien für Ausnahmefälle festzulegen, die dann beispielsweise nur bestimmte Teile einer Webseite zulassen. Die neueste Form des Filterns von Web Content ist die Kategorieblockade, die das Management der Prüf- und Filterprozesse erheblich vereinfacht. Diese Methode nutzt externe Dienste, die jederzeit den aktuellen Stand der verdächtigten Webseiten vorhalten und greift auf sogenannte Web-Kategorieserver zu, die anhand der aktuellsten URL-Bewertungen Internetinhalte filtern. Der Internetverkehr wird mit Datenbanken, die sich auf bestimmte Bewertungskriterien berufen und auf den Kategorieservern installiert sind, abgeglichen. Die als «positiv» oder «negativ» klassifizierten Ergebnisse werden zur Erhöhung der Performance zwischengespeichert. Diese Methode sorgt für Genauigkeit und die Einhaltung der Richtlinien zur Internetnutzung im Unternehmen.

Multifunktionale Lösungen als effektivste Methode

Für den effektiven Schutz von Netzwerken vor immer raffinierteren Bedrohungen aus dem Internet, sollten verschiedene Schlüsselfunktionen in einem dynamischen Abwehrsystem konsolidiert werden. Solch multifunktionale Security-Lösungen kombinieren diverse Funktionen mit automatisierten Updates zur Bewertung von Signaturen und Internetadressen. Auf diese Weise steigt die Erfolgsrate beim Entdecken und Blocken neuer so genannter «blended threats» gegenüber einzelnen Security-Anwendungen um ein Vielfaches. Wenn alle Komponenten Zugriff auf dieselben Informationen haben und leistungsstarke Firewall- und IPS-Funktionalitäten bestehen, können Bedrohungen bereits auf Netzwerkebene identifiziert und geblockt werden, bevor sie Schaden auf Endgeräten anrichten. Multifunktionale Lösungen sind derzeit daher die sicherste Methode, wenn es um das Filtern von Internetinhalten geht und sollten in Unternehmen Standard sein.

Umfassendes Reporting ein Muss

Die wichtigste Fähigkeit einer Security-Lösung für das Web Content Filtering aber ist eine umfangreiche, strukturierte Berichterstellung, die Einblick in die Internetaktivitäten im Unternehmen gibt. So kann bei Bedarf gezielt gegengesteuert werden. Auf diese Weise haben Unternehmen die Kontrolle über die hauseigenen Netzwerkressourcen und minimieren die Gefahr, dass bei unsachgemässer Nutzung des Internets rechtliche Konsequenzen drohen. Die technologischen Voraussetzungen sind bereits vorhanden, die Umsetzung kann also beginnen.

Autor: Franz Kaiser, Country Manager Austria, Switzerland and CEE bei Fortinet.
www.fortinet.com