Publication: Professional Computing (CH)
Publishing House: UTK Media Verlag
Publication date: 13.12.2011
Page: 13

Sicherer Umgang mit dem Internet im Unternehmen

Das Internet ist aus unserem Leben nicht mehr wegzudenken. Es ist nicht nur das wichtigste Kommunikations- und Informationsmedium, sondern auch ein täglich genutzter Zeitvertreib. Neben den Vorteilen des schnellen Austausches und hoher Produktivität ist es jedoch auch mehr und mehr Schauplatz krimineller Aktivitäten und Ausnutzung. Eine richtige Web-Content-Filtering-Strategie kann Unternehmen vor Angriffen schützen.

Spätestens seit ein Webzugang und E-Mail fester Bestandteil 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 vorrangig 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 von webbasierter Bedrohungen wie Viren, Würmern, Trojanern und Spyware, wenn Mitarbeiter Internetseiten aufrufen, die keinen Business-Bezug haben. 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.

Damit zudem 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 durchaus bewusst. Nicht

umsonst wächst die Nachfrage nach «Secure Content Management» (SCM) Appliances wie Antivirus, Web Content Filtering und Messaging Security stetig.

Black List, URL-Blockade oder Kategorieblockade

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» (Black List), die URL-Blockade und die Kategorieblockade. Eine schwarze Liste enthält generell einzelne sowie zusammengesetzte Wörter. URL-Adressen und Internetinhalte werden mit dieser Liste an Stichwörtern verglichen und unerlaubte Webseiten so geblockt. Auch die URL-Blockade ist eine schwarze Liste, die bekannt 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 in den Banken.

Multifunktionale Lösungen bieten effektiven Schutz

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 oder auch Unified-Threat-Management-(UTM)-Lösungen kombinieren diverse Funktionen mit automatisierten Updates zur Bewertung von Signaturen und Internetadressen. Auf diese Weise steigt die Erfolgsrate beim Entdecken und Blocken neuer sogenannter «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 oder UTM-Lösungen sind derzeit daher die sicherste Methode, wenn es um das Filtern von Internetinhalten geht.

Monitoring als Schlüssel zur Kontrolle

Die wichtigste Fähigkeit einer Security-Lösung für das Web Content Filtering aber sind eine umfangreiche, strukturierte Berichterstellung sowie ein Monitoring, die Einblick in die Internetaktivitäten im Unternehmen geben. 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 ist Regional Director Austria & Switzerland, Fortinet.

www.fortinet.ch