



Beim Spam-Schutz gilt: 1 + 1 = 3

September 2010

Das vermehrte Auftreten von Spam stellt Unternehmen jeder Größenordnung heutzutage vor enorme Herausforderungen. Alleine die Anzahl solcher E-Mails ist durchaus in der Lage, wichtige Kapazitäten im Unternehmen zu binden – in personeller wie informationstechnischer Hinsicht. Ein aktueller Bericht von CommTouch zeigt, dass der Anteil von Spam-Nachrichten im täglichen E-Mail-Verkehr im Durchschnitt bei über 80 Prozent liegt. Deswegen kommt dem effektiven Spam-Schutz entscheidende Bedeutung zu. Selbst wenn die eingesetzte UTM-Lösung diese Funktion bereits integriert, lassen sich bei der Masse an Spam Schwächen im Hinblick auf Erkennung und Gesamt-Performance der Plattform nicht ausschließen. Hier bietet die Kombination einer UTM-Firewall und der Content Security Plattform XCS von WatchGuard einen enormen Mehrwert: Neben den vielfältigen Einzelfunktionalitäten der eingesetzten Threat-Management- und Content-Security-Lösung profitieren die Anwender insbesondere von einer maximalen Spam-Abwehr, wenn die leistungsstarken Möglichkeiten beider Plattformen sinnvoll ineinander greifen.

Die Frage der Notwendigkeit von Firewall und passgenauen Sicherheitsfunktionen stellt sich heutzutage kaum noch, der Schutz des Netzwerks genießt inzwischen oberste Priorität. Zur Abdeckung aller Erfordernisse hält WatchGuard ein umfassendes Leistungsspektrum bereit. Für Unternehmen, die bereits eine UTM-Firewall eines anderen Herstellers im Einsatz haben, bietet die Kombination mit einer XCS-Lösung entscheidenden Zusatznutzen. Denn in den meisten Fällen arbeiten UTM-Plattformen als transparenter Proxy, das heißt der Dateneingang wird gescannt und verdächtiger Inhalt abgewiesen. Der Durchgang für alle anderen Inhalte ist offen, wobei ausgefilterten Spammern mit immer trickreicheren Methoden nicht in jedem Fall sofort das Handwerk gelegt werden kann. Der Content-Security-Ansatz geht in dieser Hinsicht noch einen Schritt weiter und komplettiert die Abwehr von Spam: Als Message Transfer Agent (MTA) ist WatchGuard XCS in der Lage, den Dateneingang zwischenspeichern und Inhalte genauestens und im Rahmen tagesaktueller Cloud-Services zu prüfen, bevor die relevanten Nachrichten an den internen Mail-Server weitergeleitet werden.

Aber auch im Hinblick auf einen weiteren Aspekt lohnt sich das Zusammenspiel von XCS und UTM-Firewall: Denn die zunehmende Spam-Menge, mit denen UTM-Appliances jeden Tag zu kämpfen haben, wirkt sich auf deren Gesamt-Performance aus. Andere Funktionen der UTM-Lösung können ihre spezifischen Stärken möglicherweise nicht in vollem Umfang ausspielen. Der größte Vorteil der Kombination mit XCS liegt deshalb darin, dass die Reputationsdatenbankabfrage der Content Security Plattform bereits über 90 Prozent des aufkommenden Spams erkennt und abweist. Die UTM-Firewall wird so von Anfang an entlastet und kann alle ihre Aufgaben vollständig und hochperformant erfüllen.

Optimale Prozessabfolge sorgt für maximale Spam-Abwehr

Bei einer Verknüpfung von XCS und UTM-Firewall gestaltet sich der Ablauf der Spam-Erkennung wie folgt: Der Mail-Eingang trifft zunächst auf die UTM-Firewall. Entsprechende Einstellungen müssen nun sicherstellen, dass die XCS-Plattform die IP-Adresse und Absenderdomäne der Nachricht erhält. Diese gleicht die Daten mit der Reputationsdatenbank auf Connectionlevel ab. Ist der konfigurierte Schwellenwert der Spam-Identifikation erreicht, wird die Mail sofort – also bereits beim Verbindungsaufbau – abgewiesen. Auf diese Weise blockt XCS bereits 90 Prozent des eingehenden Datenunrats. Von den übrigen Mails werden anschließend weitere Daten der Prüfung unterzogen. Hier greift in vielen Fällen die UTM-Appliance ein und unterzieht zusätzliche Teilbereiche der Nachricht der genaueren Prüfung. Innerhalb kürzester Zeit findet die Bewertung statt und die Mail kann entsprechend verarbeitet und zugelassen, abgelehnt oder markiert werden. Die weitere Verarbeitung übernimmt anschließend wieder XCS. Über Regeln lässt sich für diesen Prozessschritt sicherstellen, dass die von UTM-Firewall markierten E-Mail-Eingänge nur noch abgelegt und nicht zusätzlich gescannt werden. An diesen E-Mails trainiert sich XCS über Token Analyse für zukünftige Optimierungen in Bezug auf Textinhalte zudem selbst. Gleichzeitig sendet die Lösung die Auswertung an die globale Reputationsdatenbank. Alle anderen Mails werden ganz normal der vorgesehen Prüfung unterzogen und beispielsweise mit weiteren Blacklists verglichen. Erst wenn die Nachrichten auch diese Stufe gemeistert haben, werden sie dem internen Server zugestellt. XCS arbeitet in diesem Sinne als zusätzlicher, empfehlenswerter Puffer. Denn selbst wenn die Firewall den Datenfluss kontrolliert, ist es grundsätzlich nicht ratsam, die Mails direkt von außen an den internen Server weiterzuleiten. Hier setzt die Verbindung mit XCS auf maximale Sicherheit.

Die Kombination und Administration beider Appliances ist einfach und ein Zusammenspiel verspricht neben dem höchstmöglichen Spam-Schutz auch im Hinblick auf die Virenerkennung klaren Mehrwert, da unterschiedlichste Virenscanner den eingehenden Bedrohungen konsequent den Garaus machen. XCS setzt dabei auf Kaspersky. Optional kann McAfee zusätzlich genutzt werden. In Kombination mit den Modulen der jeweils eingesetzten UTM-Firewall bleibt den Viren bei dieser geballten Abwehr keine Chance. Beim Thema Hochverfügbarkeit trumpft die Verknüpfung beider Lösungen ebenso: Denn beim Versand von Nachrichten durch den internen Server werden diese – falls diese Funktion überhaupt unterstützt wird – zunächst von der Firewall entgegen genommen. Für den Server gelten die Nachrichten im gleichen Moment als verschickt. Wenn die Firewall als alleinige Plattform bei der eigentlichen Aussendung jedoch ausfällt, sind alle Mails verloren, selbst wenn die Box als Cluster läuft. Hier bietet XCS eine spezielle Funktion, die im Markt einzigartig ist: Queue Replication. Alle auflaufenden Mails werden beim Versand sofort und automatisch auf das zweite Cluster-Mitglied repliziert. So bleiben auch bei Ausfall der Plattform alle Nachrichten erhalten.

Es lohnt sich für Anwender in jedem Fall, sich sowohl über die Kombination als auch die Einzelstärken von XCS genauer zu informieren und die Leistungen mit den individuellen Bedürfnissen und Prioritäten abzugleichen. So profitieren beispielsweise Unternehmen mit strengen Compliance-Vorgaben insbesondere auch von den Möglichkeiten der Data Loss Prevention oder Mail-Verschlüsselung, die eine XCS-Lösung zusätzlich mit sich bringt. Der gesamte ausgehende Datenverkehr rückt dabei in den Fokus und sichert Unternehmen gegen jegliche Form der Bedrohung von innen und außen ab.

Weitergehende Informationen zu den WatchGuard Sicherheitslösungen erhalten Sie unter www.watchguard.de oder von Ihrem Händler.

ANSWERSE:

Max-Planck-Str. 4
85609 Aschheim-Dornach
Germany

WEB:

www.watchguard.de

DACH

+49 (700) 92229333

**INTERNATIONAL
SALES:**

+1.206.613.0895

ÜBER WATCHGUARD

WatchGuard, gegründet 1996, entwickelt erschwingliche, ganzheitliche Netzwerk- und Content-Sicherheitslösungen, mit denen Unternehmen ihre Daten, Netzwerke und Geschäfte umfassend schützen können. Die preisgekrönten XTM-Netzwerksicherheitslösungen (Extensible Threat Management) kombinieren Firewall, VPN und Sicherheitsdienste und schützen Netzwerke so vor Spam, Viren, Schadprogrammen und Eindringversuchen. Die neuen XCS-Appliances (Extensible Content Security) schützen darüber hinaus Unternehmensinhalte sowohl in E-Mails als auch im Web und sichern sämtliche wichtigen Inhalte gegen einen Datenverlust ab. Der Hauptsitz von WatchGuard liegt in Seattle im US-Bundesstaat Washington.

©2010 WatchGuard Technologies, Inc. Alle Rechte vorbehalten. WatchGuard, das WatchGuard-Logo, Firebox und LiveSecurity sind in den USA und/oder anderen Ländern entweder Markenzeichen oder eingetragene Markenzeichen von WatchGuard Technologies, Inc. Alle anderen Markenzeichen oder Markennamen sind Eigentum ihrer jeweiligen Besitzer. Teilnr. Part.No. WGCE66716_083110