



## Ein Leitfaden zur Bewertung von E-Mail-Sicherheitslösungen

**Die neuen E-Mail-Schutzsysteme auf dem Markt gewährleisten Sicherheit und Datenschutz für die Mitarbeiter und das Netzwerk eines Unternehmens.**

**E-Mail-Sicherheitslösungen sind heute ausgereifter, flexibler und wirksamer. Mit ihrer großen Benutzerfreundlichkeit bieten sie transparenten, einfach zu verwaltenden Schutz vor Spam, Phishing und anderen Bedrohungen in eingehenden E-Mails. Zudem unterstützen sie die Einhaltung behördlicher und unternehmensinterner Richtlinien.**

### INHALT

Einleitung	2
Wichtige Aspekte bei der Entscheidung für eine E-Mail-Sicherheitslösung	2
– Technische Anforderungen	2
– Administrative Überlegungen	4
Lösung mit Rundumschutz zur Sicherung der Messaging-Umgebung	4
– Umfassender Schutz	5
– Effiziente Administration	6
Zusammenfassung	7

## Einleitung

E-Mail-Sicherheit kann bösartigen Angriffen nur durch einen Rundumschutz und den Einsatz der neuesten Technologien einen Schritt voraus sein. Täglich werden neue Bedrohungen entwickelt. Die heutigen E-Mail-Sicherheitslösungen sind leistungsstark und flexibel genug, um mit den Möglichkeiten der Hacker mitzuhalten bzw. sie sogar vorherzusagen. Die Wirksamkeit des Schutzsystems kann bei nur minimalen Einbußen für Mitarbeiter, Computersysteme und Geschäftsabläufe ausgedehnt werden. Neben der Abwehr von eingehenden Angriffen, wie z.B. Spam und Phishing, werden dann auch ausgehende Angriffe, wie z.B. der Diebstahl von Unternehmensdaten oder die unbeabsichtigte Weiterleitung persönlicher Daten oder bösartiger Web-Inhalte an Empfänger außerhalb des Unternehmens, verhindert.

Umfassender E-Mail-Schutz ist erschwinglicher geworden. Die Lösungen sind so weit ausgereift, dass ein Rundumschutz nicht nur internationalen Konzernen mit weitläufigen, kritischen Systemen vorbehalten ist, sondern auch in kleinen Unternehmen mit einer begrenzten Anzahl zu schützender Systeme eingesetzt werden kann. Durch die Entscheidung für eine dynamische End-to-End-Lösung zum Schutz der Messaging-Umgebung mit einer konsolidierten, hochperformanten Architektur und geringem Administrationsaufwand können Unternehmen jeder Größe ihre wertvollen Ressourcen einfach und zuverlässig schützen.

## Wichtige Aspekte bei der Entscheidung für eine E-Mail-Sicherheitslösung

Viele Hersteller bieten mittlerweile hochperformante E-Mail-Sicherheitslösungen für Unternehmen aller Größenordnungen an. Diese sind jedoch oft so komplex, dass sie in den Unternehmen nicht problemlos eingesetzt werden können. Sicherheitsbedrohungen entwickeln sich rasend schnell weiter und haben so weit reichende Auswirkungen, mit denen leicht administrierbare und kostengünstige Lösungen nur schwer Schritt halten können.

Glücklicherweise gibt es die so genannte prädiktive Technologie, die Voraussagen trifft, um schnell und wirksam auf Bedrohungen und Angriffe in E-Mails zu reagieren und gleichzeitig die Einhaltung behördlicher Bestimmungen und unternehmensweiter Sicherheitsrichtlinien umzusetzen. Nicht alle E-Mail-Sicherheitsprodukte bieten jedoch diese Funktionalität. Bei der Bewertung einer E-Mail-Sicherheitslösung spielen die Tiefe, die Flexibilität und die Skalierbarkeit der Technologie zusammen mit der Fähigkeit zur Bewältigung neuer Bedrohungsvarianten eine wichtige Rolle. Zusätzlich müssen E-Mail-Sicherheitslösungen die Unternehmensressourcen optimal nutzen, um den Kosten- und Wartungsaufwand gering zu halten und effizient und transparent zu arbeiten.

Je nach Art der Bedrohung stellt ihre Bewältigung ein eher technisches oder ein administratives Problem dar.

## Technische Anforderungen

### 1. Allgemeine Sicherheitslücken

Ein- und ausgehende Bedrohungen sind immer enger miteinander verzahnt. Sobald sich bösartiger Code in der Systemumgebung festgesetzt hat, kann er zerstörerische Aktionen im Unternehmensnetzwerk starten oder mit seinem Gefährdungspotenzial an die Systeme von Kunden und Partnern weitergeleitet werden. Der Austausch von E-Mails ist ein komplexer Prozess und besteht aus den sendenden Servern, dem Inhalt der E-Mail, verschiedenen Arten von Anhängen, eingebetteten URLs oder anderen Kontaktpunkten, den mit den eingebetteten URLs verknüpften Websites, den Empfängern und den Auswirkungen auf die internen und externen E-Mail-Teilnehmer. E-Mail-Sicherheitslösungen müssen speziell auf die Anforderungen der heutigen hochintegrierten und universellen E-Mail-Umgebungen eingehen, indem sie den Datenverkehr auf allen Ebenen und in alle Richtungen hin überwachen.

## **2. Weiterentwicklung der Bedrohungsvarianten**

Es gibt nicht nur viele verschiedene Arten von E-Mail-Bedrohungen, wie z.B. Spam, Viren, Phishing und Directory Harvest Attacks (DHA), sondern auch innerhalb der einzelnen Kategorien unterschiedliche Strategien und sich ständig weiter entwickelnde Techniken. Die Sicherheitstechnologie muss alle Arten von Angriffen erkennen, vorhersagen und abwehren können; sie muss stabil genug sein, neue Angriffsstrategien direkt bei ihrem ersten Auftreten zu erkennen, und sie muss eindeutig zwischen den einzelnen Angriffsarten unterscheiden und die jeweils angemessenen Maßnahmen einleiten können.

## **3. Bösartige Inhalte**

Durch die zunehmende Raffinesse der E-Mail-Angriffe müssen wirksame Filter in den Schutzlösungen die problematischen Inhalte mit immer größerer Detailgenauigkeit erkennen können. Abgewandelte Begriffe in Spam-Mails sind eines der bekanntesten Probleme dieser Art. Das Wort "Viagra" hat beispielsweise 600.426.974.379.824.381952 Varianten, je nach Verwendung von Leerstellen, weiteren Zeichen, usw. <sup>1</sup> Eine E-Mail-Sicherheitslösung muss stets auf alle neuen Einfälle der Spam-Schreiber reagieren können.

Virenbedrohungen, Phishing und andere Arten E-Mail-basierter Angriffe erfordern ebenfalls eine spezielle Inhaltsanalyse. Die Bestandteile einer Phishing-Mail unterscheiden sich beispielsweise von denen einer Spam-Mail und können nur mit einer zielgerechten Methodik erkannt werden. Analytische Methoden sollten sich nicht auf die Kontaktdaten im Header beschränken: Auch der Nachrichtentext selbst kann Inkonsistenzen enthalten, die auf ein Problem hindeuten.

## **4. Kombinierte Angriffsarten**

E-Mail-Angriffe bestehen in der Regel aus einer Mischung verschiedener Methoden, die entweder gleichzeitig oder nacheinander angewendet werden. Spam- und Phishing-E-Mails zielen zwar auf Einzelpersonen ab, können jedoch zudem Viren enthalten und dadurch das gesamte Unternehmensnetzwerk gefährden. E-Mail-Sicherheitslösungen müssen über einen integrierten Ansatz verschiedene Arten von E-Mail-basierten Bedrohungen entdecken und sperren können.

## **5. Komplexe Aufgabenstellung bei der Authentifizierung**

Die Server-Authentifizierung spielt beim Sperren von E-Mail-Angriffen eine wichtige Rolle. In der heutigen diversifizierten Internet-Umgebung kann dies zu einem komplexen Vorgang werden. Eine "gute" E-Mail wird beim Erhalt möglicherweise nicht authentifiziert, da sie von einem Dritten weitergeleitet wurde oder aus einer Quelle stammt, deren DNS-Einträge keine Authentifizierung unterstützen. Eventuell ist auch die "Reputation" des sendenden Servers (bestimmt durch externe Web-Dienste, die den Spam-Mail-Verkehr überwachen) nicht eindeutig. Bei einem kombinierten Ansatz mit Authentifizierungs- und Reputationstechniken lässt sich der tatsächliche Status des sendenden Servers mit größerer Genauigkeit bestimmen. Dadurch verringert sich auch die Anzahl der Fehlalarme, die den Geschäftsablauf beeinträchtigen, da unproblematische E-Mails irrtümlich ausgefiltert werden.

## **6. Anforderungen an die Antwortzeiten**

Optimale E-Mail-Sicherheitslösungen reagieren unmittelbar auf alle Arten von Bedrohungen und entfernen diese, bevor Schaden entstehen kann. Derart schnelle Antwortzeiten können jedoch nur erreicht werden, wenn frühzeitig Prognosen über die Wahrscheinlichkeit eines Angriffs oder die mögliche Verletzung von Unternehmensrichtlinien erstellt werden. Prädiktive Techniken erkennen nicht nur Gefahren in eingehenden E-Mails mit verdächtigen Anhängen, sondern auch Anomalien in den ausgehenden E-Mail-Daten des Unternehmens.

---

<sup>1</sup> "There are 600,426,974,379,824,381,952 Ways to Spell Viagra." Cockeyed.com. 7. April 2004. Quelle: <http://cockeyed.com/lessons/viagra/viagra.html>.

## **Administrative Überlegungen**

### **1. Steigende Kosten**

In den vergangenen zehn Jahren sind die Ausgaben für Sicherheitssoftware enorm gestiegen. Ein Ende dieser Entwicklung ist nicht abzusehen. E-Mail-Sicherheitslösungen, die den Systemschutz verbessern, ohne dabei die Kosten für Implementierung und Wartung in die Höhe zu treiben, sind äußerst gefragt. Die Ausgaben lassen sich am einfachsten eindämmen, wenn eine Rundumlösung mit einer einzigen E-Mail-Sicherheitsinfrastruktur zur Verwaltung des gesamten E-Mail-Sicherheitssystems verwendet wird. Die Systemkonsolidierung ist ein weiterer wichtiger Aspekt: Mit einer geringen Anzahl zuverlässiger, hochperformanter Server wird Rundumschutz und Hochverfügbarkeit mit angemessener Skalierbarkeit und Redundanz umgesetzt.

### **2. Komplizierte E-Mail-Sicherheitssysteme**

E-Mail-Sicherheitssysteme müssen aufgrund der benötigten Funktionalität komplex sein. So sind auch Softwareanwendungen häufig hoch kompliziert und können nur mit großem Zeitaufwand und umfassender Fachkenntnis betrieben werden. Effiziente Lösungen sollten hingegen über eine vereinfachte, wirksame, benutzerfreundliche und extrem wartungsarme Administrationsoberfläche verfügen. Die folgenden Funktionsmerkmale erleichtern die Systemwartung:

- Optionen zur schnellen Konfiguration
- Einfache Benutzeranpassung
- Die Auswahlmöglichkeit zwischen einer einheitlichen und einer geteilten Architektur
- Automatische Updates
- Integration in gebräuchliche Verzeichnisdienste (z.B. LDAP, Microsoft Active Directory, usw.)
- Zentrale Verwaltung
- Web-basierte Benutzeroberfläche
- Stabiles Reporting mit vollem Funktionsumfang

### **3. Einhaltung von Auflagen**

Einerseits erhöht sich die Anzahl behördlicher Auflagen beständig, andererseits erweitern auch die Unternehmen die internen Sicherheitsmaßnahmen zum Schutz ihrer kritischen Daten und Netzwerke sowie des Datenschutzes ihrer Mitarbeiter. In der Folge wächst die Belastung für die IT-Mitarbeiter, den entsprechenden Funktionsumfang und die Berichterstattung bereitzustellen. E-Mail-Sicherheitslösungen erleichtern die Arbeit mit speziellen Funktionen zur Einhaltung behördlicher Bestimmungen. Gleichzeitig sind sie flexibel genug, um auch mit einer Weiterentwicklung der Unternehmensrichtlinie Schritt zu halten. Grundlegende Funktionen umfassen Verschlüsselung, digitale Signaturen, Content-Filter und speziell auf Spam, Phishing, Viren und andere komplexe, E-Mail-basierte Bedrohungen ausgerichtete Maßnahmen zur Abwehr von Angriffen.

## **Lösung mit Rundumschutz zur Sicherung der Messaging-Umgebung**

E-Mail-Sicherheitssysteme müssen alle Bestandteile der Messaging-Umgebung umfassend schützen und dabei alle Eigenarten der verschiedenen Angriffstypen erfassen. Rundumlösungen bieten komplexe Funktionen und eine benutzerfreundliche Oberfläche mit flexibler Konfiguration und einfachem Zugriff auf die erstellten Berichte.

## Umfassender Schutz

### Überwachung des gesamten Bedrohungsverlaufs

Ohne ein echtes End-to-End-System zur Überwachung der E-Mails können Unzulänglichkeiten in der E-Mail-Sicherheitslösung des Unternehmens weit reichende Konsequenzen haben. Durch den Einsatz fortschrittlicher statistischer Methodik deckt eine wirksame E-Mail-Sicherheitslösung alle Komponenten der Messaging-Umgebung im Unternehmen ab. Dieser Rundumschutz verfügt über alle erforderlichen Funktionen zum Schutz vor Angriffen. Der Nachrichteninhalt und die Anhänge werden gründlich durchsucht, die Reputation von E-Mail Servern wird genau zurück verfolgt und die Auswirkung von Bedrohungen und Angriffen auf das gesamte Unternehmensnetzwerk wird ständig analysiert. Auch Datenschutzverletzungen werden aufgedeckt: Eine ausgereifte Erkennungstechnologie kann beispielsweise den E-Mail-Verkehr in Bezug auf Inkonsistenzen überwachen, die oftmals auf einen Versuch zur nicht autorisierten Übertragung von Unternehmensdaten hinweisen.

Ausgereifte Technologien, wie z.B. SonicWALL Email Security, ermöglichen zudem einen kollaborativen Ansatz. In diesem Fall geschieht dies durch das SonicWALL Self Monitoring Active Response Team (SMART) Network™, ein Echtzeitnetzwerk mit weltweit über einer Million Benutzern, deren Antworten die vorausschauende Reaktion auf neue Gefahren in E-Mails unterstützen.

### Schutz vor allen Arten von Bedrohungen

Spam- und Phishing-Angriffe zählen zu den bekanntesten E-Mail-Bedrohungen. Viele E-Mail-Sicherheitssysteme haben wirksame Techniken zur Bekämpfung dieser Probleme entwickelt. Die Frage ist, ob diese Lösungen komplex genug sind, um die raffinierten modernen Bedrohungen in ihrer Gesamtheit zu erfassen.

#### *Spam*

Die am weitesten verbreitete Methode zum Sperren von Junk-Mails ist das Ausfiltern von Spam gemäß einer Trefferquote. Hierbei müssen die Filtereinstellungen regelmäßig angepasst werden, da ständig neue Spam-Varianten entwickelt werden. Die Methode ist jedoch auch anfällig für Fehlalarme, da E-Mails irrtümlich als Spam eingestuft werden können, wenn sie Spam-Merkmale aufzuweisen scheinen. Ein genauerer, zeitsparender Ansatz verwendet eine Kombination analytischer Techniken, mit denen das E-Mail-Sicherheitssystem verdächtige E-Mails sicher und zuverlässig in Quarantäne stellt, während genau ermittelt wird, welche E-Mails problemlos an die Empfänger weitergeleitet werden können. Ein effektives E-Mail Security System sollte Spam mit einer Wirksamkeitsrate von rund 98 % sperren. Umfassende Datenbanken zur Server-Authentifizierung sind für eine fortschrittliche Lösung dabei ebenso wichtig wie eine hochgranulare Form der Suche in E-Mails, die auf einer Vielzahl verschiedener analytischer Methoden beruht.

#### *Phishing*

Phishing-E-Mails täuschen vor, von rechtmäßigen Unternehmen versandt worden zu sein. So versuchen sie, dem Empfänger persönliche oder unternehmensrelevante Daten, wie z.B. Sozialversicherungsnummern oder Gehaltszahlen, zu entlocken. Forschungsergebnisse belegen, dass Phishing 2004 weltweit einen Schaden von über 44 Milliarden USD verursachte<sup>2</sup>. Phishing benötigt eine eigene, speziell auf die spezifischen Bedrohungseigenschaften ausgerichtete Form des Schutzes. SonicWALL verwendet z.B. speziell entwickelte analytische Methoden zur Entdeckung von E-Mails mit Phishing-bezogenen Inhalten. Das System kann außerdem die Reputation der in den verdächtigen E-Mails enthaltenen Kontaktpunkte ermitteln, Inkonsistenzen in enthaltenen Links aufdecken und die Ausnutzung von Browser- oder Betriebssystemschwachstellen erkennen.

#### *Viren*

In den meisten Fällen verlassen sich die Benutzer bei der Bekämpfung von Viren auf so genannte Signaturen (speziell entwickelter Code), die so bald wie möglich nach dem Zeitpunkt Null (Ausbruchsbeginn) bereitgestellt werden. Bestimmte Sicherheitsprodukte verfügen bereits über

---

<sup>2</sup> "mi2g:Q3 2004: The Rise of Islamist Hacking and Criminal Syndicates." mi2g. 20. Oktober 2004.

Quelle:

<http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//www.mi2g.com/cgi/mi2g/press/201004.php>.

prädiktive Funktionen, die über die Suche nach bereits identifizierten (neuen und alten) Bedrohungen und die Bekämpfung von böartigem Code hinausgehen. Die SonicWALL Time Zero Virus Technology bietet beispielsweise Erkennungsmethoden zur Vorhersage von Anomalien. Diese Methoden werden durch Dual-Engine-Signaturtechnologien (von den SonicWALL Partnern McAfee und Kaspersky) verstärkt, mit denen die Antwortzeiten verkürzt und umfassender Schutz garantiert wird. Die SonicWALL Lösung kann diese fortschrittlichen Antivirentechniken einfach auf ein- und ausgehende Virenbedrohungen anwenden.

Zusätzlich verstärkt ein großes Netzwerk echter E-Mail-Nutzer die Reaktion auf Virenvorfälle, da sie schnelle und statistisch genaue Daten zu neuen Virenbedrohungen liefern. Als am 13. November 2004 der Virus "Sober.J" ausbrach, konnten SonicWALL Lösungen dank ihrer prädiktiven Technik umgehend vier der fünf Virusvarianten abwehren. Mithilfe der Daten des SonicWALL SMART Network wurde dann auch die fünfte Variante gestoppt. All dies fand noch vor der Bereitstellung einer Signatur statt.

#### *Zombies, DHA, DoS-Angriffe*

Eine umfassende E-Mail-Sicherheitslösung schützt auch vor den neueren und möglicherweise gefährlicheren Angriffsarten, wie z.B. Zombie-Computern, DHA- (Directory Harvest Attacks) und DoS- (Denial of Service) Angriffen. Zombie-Computer im Unternehmensnetzwerk werden von böartigem Code zur Versendung von Massen-Mails, die aus dem infizierten System zu stammen scheinen, fremd gesteuert. DHAs sind "gewaltsame" Angriffe, die den Mail-Server regelrecht mit Zufallsmails bombardieren, um rechtmäßige E-Mail-Knoten für die spätere Verwendung auszuspähen. Bei einem DoS wird versucht, die gesamte Systeminfrastruktur zum Absturz zu bringen, indem das Netzwerk zu einem bestimmten Zeitpunkt mit einem riesigen Datenvolumen überlastet wird.

Eine wirksame E-Mail-Sicherheitslösung muss technisch in der Lage sein, die speziellen Ausprägungen dieser Varianten zu bekämpfen. Sie sollte mit einer Vielzahl spezieller Techniken mögliche Zombie-Computer aufspüren und so die Weiterleitung ausgehender E-Mail-Bedrohungen verhindern. All dies muss in Echtzeit ohne negative Auswirkungen auf die Messaging-Dienste geschehen. Betrügerische Anfragen eines DHA sollten bereits an der Peripherie abgewehrt werden: Die Analyse von E-Mail-Mustern wird dabei mit Daten kombiniert, die durch die Synchronisierung mit dem Unternehmensverzeichnis gesammelt wurden. Dadurch wird der Diebstahl von Informationen über das Unternehmensverzeichnis abgewehrt. Bei DoS-Angriffen wird mit speziellen E-Mail-Patternanalysen und Erkennungstools der Mail-Server ermittelt, der den gefährlichen Datenverkehr ausgibt.

## **Effiziente Administration**

### **Benutzerfreundlichkeit**

E-Mail-Sicherheitssysteme erfordern regelmäßige Updates und die Überwachung aller Aktivitäten des Sicherheitsdienstes beim Erhalt und Versand von Daten. Moderne E-Mail-Sicherheitstechnologie kann die meisten dieser Schritte intern, ohne Eingreifen des Mitarbeiters, verarbeiten. Automatische Updates beispielsweise, wie sie SonicWALL Email Security Lösungen bieten, gewährleisten ein kostengünstiges, einfach zu verwaltendes E-Mail-Sicherheitssystem. Eine zentrale, Web-basierte Administrationsoberfläche vereinfacht zusätzlich alle Verwaltungs-Tasks. Zahlen belegen, dass ein SonicWALL Administrator in der Regel nur zehn Minuten pro Woche mit der Wartung des E-Mail-Systems befasst ist.

Ein weiterer wichtiger Aspekt ist die flexible Konfiguration. Der Administrator muss zwischen einer einheitlichen und einer getrennten Architektur sowie zwischen einer zentralen und einer dezentralen Konfiguration wählen können. Lösungen wie die von SonicWALL bieten diese Funktionalität mit einer Vielzahl von Konfigurationsoptionen. Die einfachste Konfiguration kann in weniger als einer Stunde eingerichtet werden. Eine effiziente Lösung erlaubt auch ein hohes Maß an Systemkonsolidierung, wodurch die Ausnutzung der Hard- und Softwareressourcen maximiert und die Aufgaben im IT-Bereich minimiert werden.

E-Mail-Sicherheitssysteme müssen flexibel auf Angriffssituationen reagieren können. Eine Technologie wie beispielsweise SonicWALL Email Security erlaubt dem Administrator, unter verschiedenen Aktionen bei der Reaktion auf Bedrohungen in eingehenden E-Mails auszuwählen. Durch diese Flexibilität kann je nach Bedrohungssituation eine Warnung versendet oder die betreffende E-Mail gelöscht, in Quarantäne verschoben, verschlüsselt oder zurückgewiesen werden.

## **Vereinfachte Richtlinienverwaltung und Einhaltung von Auflagen**

Heutige Sicherheitsumgebungen müssen sowohl behördliche Auflagen als auch unternehmensinterne Sicherheitsrichtlinien einhalten. In den meisten Fällen erfordert dies hochspezielle System- und Berichterstattungsfunktionen. Auch hier kann eine einfache Benutzeranpassung den Zeitaufwand minimieren und die Ergebnisse maximieren. SonicWALL Email Security bietet dem Systemadministrator beispielsweise eine einfache Möglichkeit zur Erstellung globaler oder spezieller Gruppenrichtlinien für den ein- und ausgehenden Datenverkehr. Dazu wird eine Identitäts-basierte Architektur mit vollständiger Integration von LDAP, Microsoft Active Directory und anderen gebräuchlichen Verzeichnissystemen verwendet. Der Administrator kann in kürzester Zeit auch ohne Programmierkenntnisse oder spezielles technisches Fachwissen Zugriffsberechtigungen einrichten und bearbeiten.

Weitere Funktionen, die die Einhaltung von Richtlinien unterstützen, sind ausgereifte Content-Analyse und der Einsatz entsprechender Wörterbücher, beispielsweise für juristische Terminologie, die einen unangemessenen Sprachgebrauch erkennen. Fortschrittliche Lösungen enthalten stabile Funktionen zur Berichterstattung, die wichtige Daten zu den Angriffsarten, der Wirksamkeit der durchgeführten Aktionen und der Systemleistung liefern.

## **Kostengünstige, hochperformante Architektur**

Um auch langfristig einen wirksamen und erschwinglichen Funktionsumfang zu gewährleisten, müssen E-Mail-Sicherheitssysteme die Informationsverarbeitung so weit wie möglich konsolidieren, dabei die Aspekte Hochverfügbarkeit und Skalierbarkeit nach Bedarf umsetzen und ein ausreichendes Maß an Redundanz bieten. Die einzigen Systeme, die diese Ansprüche erfüllen, sind Systeme wie beispielsweise SonicWALL Email Security, die extrem leistungsstark sind und sich flexibel konfigurieren lassen.

## **Zusammenfassung**

Systeme zur E-Mail-Sicherheit müssen sich den sich ständig weiterentwickelnden Bedrohungen anpassen können. Der Schwerpunkt liegt hierbei auf Flexibilität und umfassendem Schutz vor aktuellen und zukünftigen Bedrohungen. Unternehmen benötigen eine einfach verwaltbare, komplett anpassbare E-Mail-Sicherheitslösung mit einer hohen, garantierten Leistungsstärke ohne Ausfallzeiten und einem technischen Funktionsumfang, der speziell auf bestimmte Arten E-Mail-basierter Angriffe ausgerichtet ist. Trotz der Vielzahl der auf dem Markt verfügbaren E-Mail-Sicherheitslösungen verfolgen nur wenige einen End-to-End-Ansatz bei der Bekämpfung von Sicherheitsbedrohungen. Unternehmen können sich jedoch nur auf Lösungen verlassen, die über zielgerichtete analytische Prozesse für bestimmte Bedrohungstypen verfügen.

Ein weiterer wichtiger Aspekt ist die Integration in eine umfassendere Web-Sicherheitslösung. Die SonicWALL Technologie bietet beispielsweise die gesamte Produktpalette vollständig integrierter Web- und E-Mail-Sicherheitslösungen, die das Unternehmensnetzwerk in seiner Gesamtheit betrachten und so dauerhaft einen Rundumschutz gewährleisten. Besonders der SonicWALL Content Security Manager bietet grundlegenden Schutz vor Web-basierten Bedrohungen, wie z.B. Viren, Spyware, Trojanern und Würmern, und sperrt dabei erfolgreich unrechtmäßige Zugriffe auf unangemessene Web-Inhalte.

E-Mail-Angriffe sind heute zwar gefährlicher und kreativer als je zuvor, doch auch die Internet- und E-Mail-Sicherheitslösungen entwickeln sich weiter und werden zunehmend leistungsstärker und komplexer. Ein informierter Administrator kann problemlos eine Technologie zum Schutz der kritischen Systeme auswählen, so dass sich die Mitarbeiter ohne Einschränkung der Ressourcen auf das Tagesgeschäft konzentrieren können.

©2005 SonicWALL, Inc. ist eine eingetragene Marke von SonicWALL, Inc. Andere in diesem Dokument erwähnte Produktnamen können Marken und/oder eingetragene Marken ihrer jeweiligen Hersteller sein. Spezifikationen und Beschreibungen können sich ohne vorherige Ankündigung ändern.