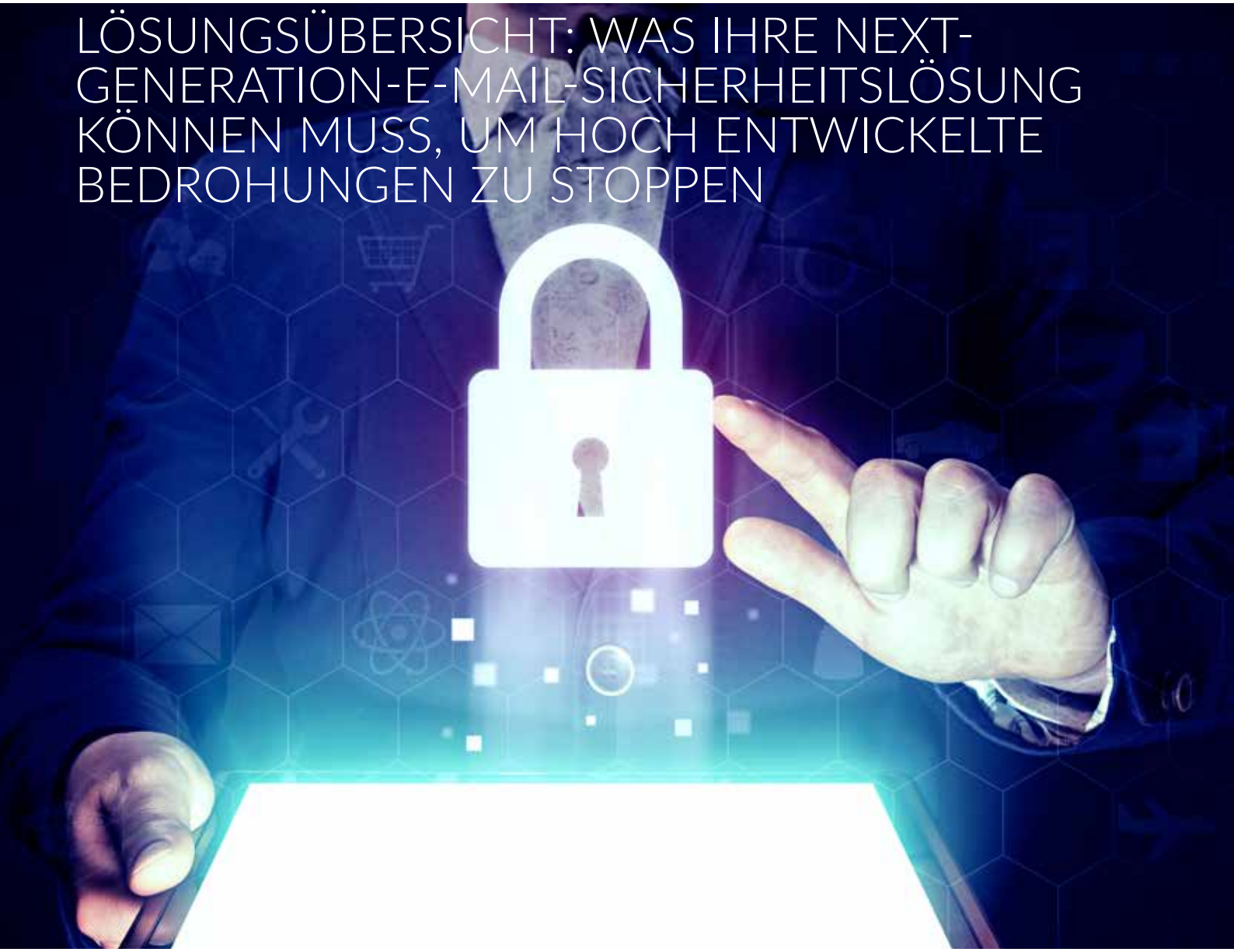
LÖSUNGSÜBERSICHT: WAS IHRE NEXT-GENERATION-E-MAIL-SICHERHEITSLÖSUNG KÖNNEN MUSS, UM HOCH ENTWICKELTE BEDROHUNGEN ZU STOPPEN



Zusammenfassung

Um extrem raffinierte Bedrohungen zu stoppen, wie sie heute an der Tagesordnung sind, braucht es neben herkömmlichen Lösungen ganz neue E-Mail-Sicherheitsfeatures. Unternehmen benötigen eine mehrschichtige Next-Generation-E-Mail-Sicherheitslösung mit umfassendem Bedrohungsschutz, um ihre geschäftliche Kommunikation effektiv zu schützen.

Die wachsende Bedeutung von Next-Generation-E-Mail-Sicherheitslösungen

E-Mails sind für Cyberkriminelle mittlerweile das wichtigste Vehikel für eine Reihe ein- und ausgehender Bedrohungen. Diese Cyberbedrohungen entwickeln sich extrem schnell weiter: Nutzten Hacker früher überwiegend Massen-Spammails, so setzen sie heute zunehmend auf gezielte Angriffe. Bei den meisten dieser Attacken wird die Payload über E-Mails übertragen. Dem SonicWall Annual Threat Report zufolge haben Ransomware-Angriffe im Jahresvergleich um das 167-Fache zugenommen und haben sich zur Payload der Wahl für bösartige E-Mail-Kampagnen entwickelt. Um ausgeklügelte Bedrohungen wie Ransomware und Zero-Day-Attacken zu stoppen, sind herkömmlich Schutzmethoden allerdings nicht mehr ausreichend – dagegen helfen nur E-Mail-Sicherheitslösungen der nächsten Generation.

Die wichtigsten Funktionen einer Next-Generation-E-Mail-Sicherheitslösung

Lesen Sie, welche Funktionen eine Next-Generation-E-Mail-Sicherheitslösung bieten muss, um Sicherheitslücken zuverlässig zu vermeiden:

Schutz vor raffinierten Bedrohungen

Die meisten Virenschutzlösungen sind signaturbasiert und daher nicht effektiv genug, um raffinierte Bedrohungen wie Ransomware und unbekannte Malware zu bekämpfen. Diese Malware-Typen verfügen über individuelle Hashcodes und lassen sich daher nicht mithilfe traditioneller Methoden erkennen. Gefragt ist eine zuverlässige Sandbox-Umgebung, um Ransomware- und Zero-Day-Angriffe zu erkennen und zu verhindern, bevor sie überhaupt das Netzwerk erreichen.

Eine effiziente Next-Generation-E-Mail-Sicherheitslösung muss folgende Funktionen bieten:

- Umfassender mehrschichtiger Schutz für die E-Mail-Kommunikation
- Sandboxing- und Quarantäne-Funktionen für unbekannte Dateien
- Auf dynamische Reputation basiertes Blacklisting
- Erweiterte Inhaltsanalyse und Mustererkennung
- Starke Verschlüsselung und Schutz vor Datenverlust für Compliance-Anforderungen und gesetzliche Vorgaben

Schutz vor bekannten Bedrohungen

Cyberkriminelle führen viele Angriffe mit bekannten Malware-Varianten durch. Eine Virensignaturen-Datenbank ist ein einfaches, effektives Instrument, um bösartige eingehende E-Mails zu durchleuchten und zu verhindern, dass Ihre Mitarbeiter infizierte E-Mails versenden. Für eine höhere Effizienz empfehlen wir, mehrere Engines zur Erkennung von Viren zu nutzen, die sowohl E-Mails als auch Anhänge nach Viren, Trojanern, Würmern und anderen bösartigen Inhalten prüfen.

Schutz vor Phishing-Angriffen

Phishing-Kampagnen sind mittlerweile ein beliebtes Mittel, um Payloads für Ransomware-Angriffe zu übertragen. Ihre E-Mail-Sicherheitslösung sollte Funktionen für eine erweiterte Inhaltsanalyse umfassen, die sämtliche E-Mails einschließlich Betreffzeile, Textkörper und Anhang überprüfen. Außerdem sollte sie eine Sandbox-Umgebung für verdächtige Anhänge sowie eine Echtzeit-Blacklist mit dynamischen IP-Adressen nutzen, um E-Mails mit bösartigen Links zu filtern.

Schutz vor Betrug

Hacker nutzen raffinierte Taktiken wie Spear-Phishing, Whaling und CEO-Fraud, um personenbezogene Daten zu erbeuten. Darüber hinaus erstellen sie für ihre betrügerischen Aktivitäten E-Mails, die aus einer vermeintlich authentischen Quelle zu stammen scheinen. Um zu verhindern, dass unrechtmäßige Nachrichten in Ihre Organisation gelangen, sind granulare Konfigurationen bei den E-Mail-Einstellungen nötig. E-Mail-Konfigurationen wie SPF (Sender Policy Framework), DKIM (Domain Keys Identified Mail) und DMARC (Domain-based Message Authentication, Reporting and Conformance) ermöglichen in Kombination mit der Mustererkennung und der Inhaltsanalyse eine angemessene Prüfung aller eingehenden Nachrichten.

Schutz vor Spammails

Spam kann Posteingänge und Netzwerkressourcen verstopfen, zusätzliche operative Kosten verursachen und Unternehmen wertvolle Zeit kosten. Eine effiziente E-Mail-Sicherheitslösung sollte mehrere Methoden zur Erkennung von Spam und anderen unerwünschten E-Mails bieten. Dazu gehören spezifische Freigabe- und Sperrlisten für Personen, Domains und Nachrichten, die Nutzung von Third-Party-Sperrlisten sowie Muster, die darauf basieren, was andere User als Junkmail markiert haben.

Schutz vor Datenverlust

Organisationen tun gut daran, ihre vertrauliche Kommunikation bestmöglich zu schützen. Besonders gut hat sich die Verschlüsselung sensibler E-Mails und E-Mail-Anhänge bewährt. Dabei sollten die Verschlüsselungsfunktionen aber eng mit der E-Mail-Sicherheitslösung verzahnt sein.

Fazit

Traditionelle E-Mail-Lösungen basieren auf statischen IP-Reputationen und signaturbasierten Erkennungsmechanismen, die den heutigen – hoch entwickelten und schwer zu fassenden – Malware-Varianten nichts entgegenzusetzen haben. Das bloße Erkennen von Bedrohungen reicht heute nicht mehr aus. Speziell bei einem Dauerbeschuss sind Benachrichtigungen allein oft nutzlos. E-Mail-Sicherheitslösungen sollten heute mehr als nur Funktionen zur Erkennung von Bedrohungen bieten. Sie müssen vor allem auch in der Lage sein, Angriffe zu verhindern und zu stoppen, bevor sie überhaupt Ihr Netzwerk erreichen.

Die Next-Generation-E-Mail-Sicherheitslösungen von SonicWall nutzen einen mehrschichtigen Ansatz auf Basis der prämierten Capture ATP-Sandbox-Technologie. Mit ihren einzigartigen Breach-Prevention-Funktionen bietet die Capture ATP-Technologie zuverlässigen Schutz vor raffinierten E-Mail-basierten Bedrohungen. Dazu kommt ein umfassender Multi-Engine-Virenschutz sowie ein überragender Schutz vor Phishing, Spoofing, Spam und Datenverlust.

Weitere Informationen erhalten Sie unter www.sonicwall.com/products/email-security-appliance.

SONICWALL®

Über uns

Seit über 25 Jahren schützt SonicWall kleine, mittlere und große Unternehmen weltweit vor Cyberkriminalität. Mit unseren Produkten und Partnerschaften können wir eine Echtzeit-Cyberabwehrlösung für die individuellen Anforderungen von über 500.000 globalen Organisationen in über 150 Ländern bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.

Wenn Sie Fragen zur Nutzung dieser Unterlagen haben, wenden Sie sich an:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, Kalifornien 95054, USA

Weitere Informationen finden Sie auf unserer Website.
www.sonicwall.com