



DIE VERSCHIEDENEN ARTEN VON
CYBERANGRIFFEN UND WIE SIE
SICH DAGEGEN WEHREN KÖNNEN

Einleitung

Immer wieder gelingt es Cyber-kriminellen, mit raffinierten Methoden unerkannt in Unternehmensnetzwerke einzudringen, um geistiges Eigentum zu stehlen oder Lösegeld für Dateien zu erpressen, auf die der Besitzer nicht mehr zugreifen kann. Häufig werden diese Bedrohungen verschlüsselt, um eine Erkennung zu vermeiden.

Hat sich ein Hacker erfolgreich Zugang zu einem System verschafft, versucht er normalerweise, Malware zu laden und zu installieren. Oft kommen dabei neue Malware-Varianten zum Einsatz, die von herkömmlichen Virenschutzlösungen nicht erkannt werden.

Dieses E-Book erläutert, welche Strategien und Tools Cyberkriminelle bei ihren Eindringversuchen verwenden und wie sich Angriffe wirksam abwehren lassen.





Cyberkriminelle sind rund um die Uhr aktiv.

Cyberangriffe – Strategie 1

Dauerbombardement von Netzwerken mit Malware

Angriffe werden über viele verschiedene Vektoren ausgeführt: über E-Mails, Mobilgeräte, automatisierte Exploits und über den Webverkehr. Die Größe Ihres Unternehmens spielt dabei keine Rolle. Für den Hacker sind Sie lediglich eine IP-Adresse, eine E-Mail-Adresse oder ein potenzielles Opfer für einen Watering-Hole-Angriff. Cyberkriminelle nutzen automatisierte Tools, mit denen sie rund um die Uhr Exploits ausführen oder Phishingmails versenden können.

Das Problem ist, dass viele Organisationen nicht über die richtigen Tools verfügen, um sich gegen die Angreifer zur Wehr zu setzen. Viele von ihnen haben keine automatisierten Tools, um den Datenverkehr zu durchleuchten, Endpunkte zu schützen oder bedenkliche E-Mails herauszufiltern. Andere haben Firewalls, die den verschlüsselten Verkehr nicht auf verborgene Bedrohungen überprüfen können, oder verlassen sich auf ihre begrenzten Systemspeicher, um Malware-Signaturen zu speichern.

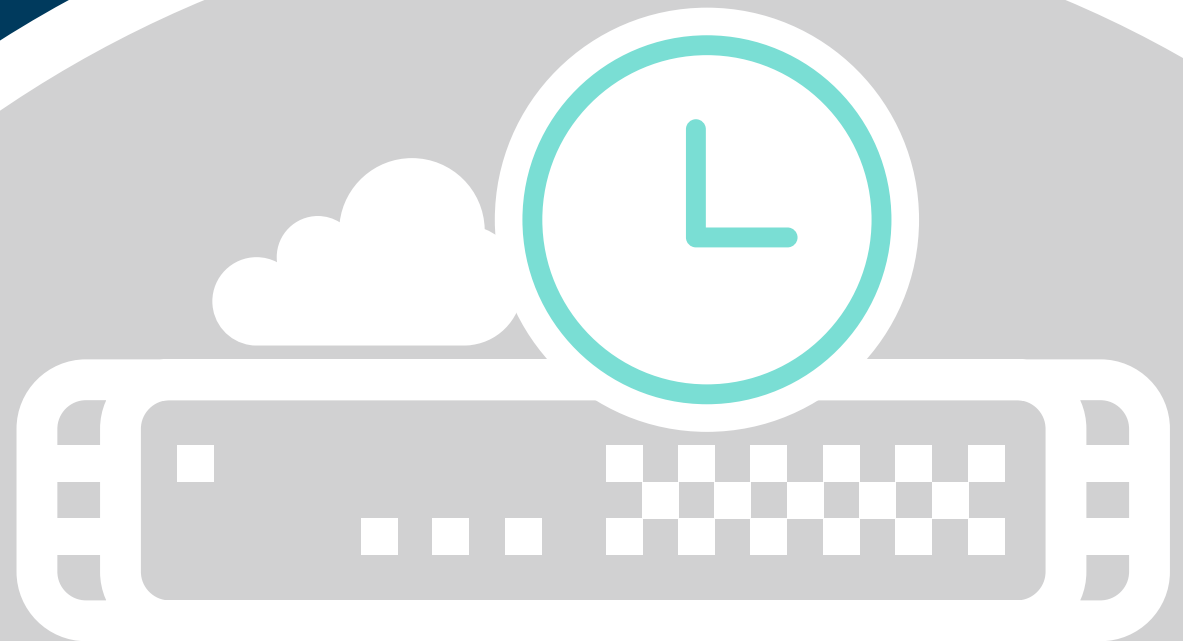
Gegenmaßnahme 1

Schützen Sie Ihr Netzwerk zu jeder Tages- und Nachtzeit

Stündlich kommen Hunderte neuer Malware-Varianten hinzu. Organisationen benötigen deshalb einen wirksamen Echtzeitschutz, um jederzeit gegen die neuesten Bedrohungen gewappnet zu sein. Eine effektive Sicherheitslösung muss kontinuierlich aktualisiert werden – 24 Stunden am Tag, sieben Tage die Woche. Doch aufgrund der immensen Anzahl von Malwaretypen und -varianten verfügt keine Firewall über genügend Speicher.

Daher sollten Firewalls mit einer Netzwerk-Sandbox arbeiten und an die Cloud angeschlossen sein, um einen größtmöglichen Einblick in Malware zu gewähren und neue Varianten bestmöglich zu identifizieren. Wichtig ist auch, dass Ihre Sicherheitslösung einen dynamisch aktualisierten Schutz nicht nur am Firewall-Gateway, sondern auch an mobilen und Remote-Endpunkten und für Ihre E-Mails gewährleistet.

Setzen Sie auf eine Sicherheitsplattform, die alle Vorteile der Cloud nutzt und einen Echtzeitschutz vor den neuesten Malware-Bedrohungen bietet.



Cyberangriffe – Strategie 2

Infizierung von Netzwerken mit verschiedenen Malware-Varianten

Cyberkriminelle nutzen verschiedene Arten von Angriffsvektoren und Malware, um Netzwerke zu kompromittieren. Zu den fünf häufigsten Formen von Malware gehören Viren, Würmer, Trojaner, Spyware und Ransomware.

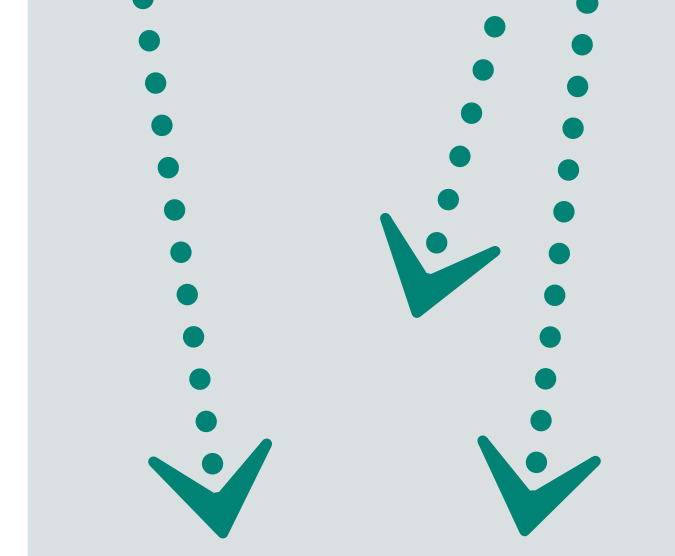
Computerviren wurden in den Anfängen der PCs durch die gemeinsame Nutzung infizierter Disketten verbreitet. Mit der Weiterentwicklung der Technik vollzog sich auch bei den Verbreitungsmethoden eine „Evolution“. Heute werden Viren üblicherweise durch Filesharing, Internetdownloads und E-Mail-Anhänge verbreitet.

Computerwürmer existieren seit den späten 80er-Jahren, traten aber erst mit dem flächendeckenden Einsatz von Netzwerken in Organisationen häufiger auf. Im Gegensatz zu Computerviren können sich Würmer ohne menschliches Zutun in Netzwerken verbreiten.


Trojaner sind speziell dafür konzipiert, sensible Daten in Netzwerken zu finden und zu erbeuten. Viele Arten von Trojanern übernehmen die Steuerung des infizierten Systems und öffnen dem Angreifer eine Hintertür für spätere Zugriffe. Häufig werden mithilfe von Trojanern mehrere Computer zu einem Botnet zusammengeschlossen.

Spyware ist in der Regel nicht bösartig, stellt jedoch ein großes Ärgernis dar, weil Webbrowser nach einer Infizierung oft kaum mehr funktionsfähig sind. Manchmal ist Spyware auch als seriöse Anwendung getarnt, die dem Benutzer bestimmte Vorteile vorgaukelt, während sie im Hintergrund das Benutzerverhalten und die Nutzungsmuster ausspioniert.

Ransomware ist eine Schadsoftware, bei der häufig die Dateien auf einem Endgerät oder Server verschlüsselt werden. Der Endbenutzer wird aufgefordert, ein Lösegeld in Form von Bitcoins für den Chiffrierschlüssel zu zahlen. Verbreitet sich die Ransomware auf geschäftskritische Systeme, kann die Höhe des Lösegelds auf Hunderttausende von Dollar steigen.



Cyberkriminelle nutzen alle möglichen Arten von Malware, um mögliche Lücken zu finden.



Gegenmaßnahme 2

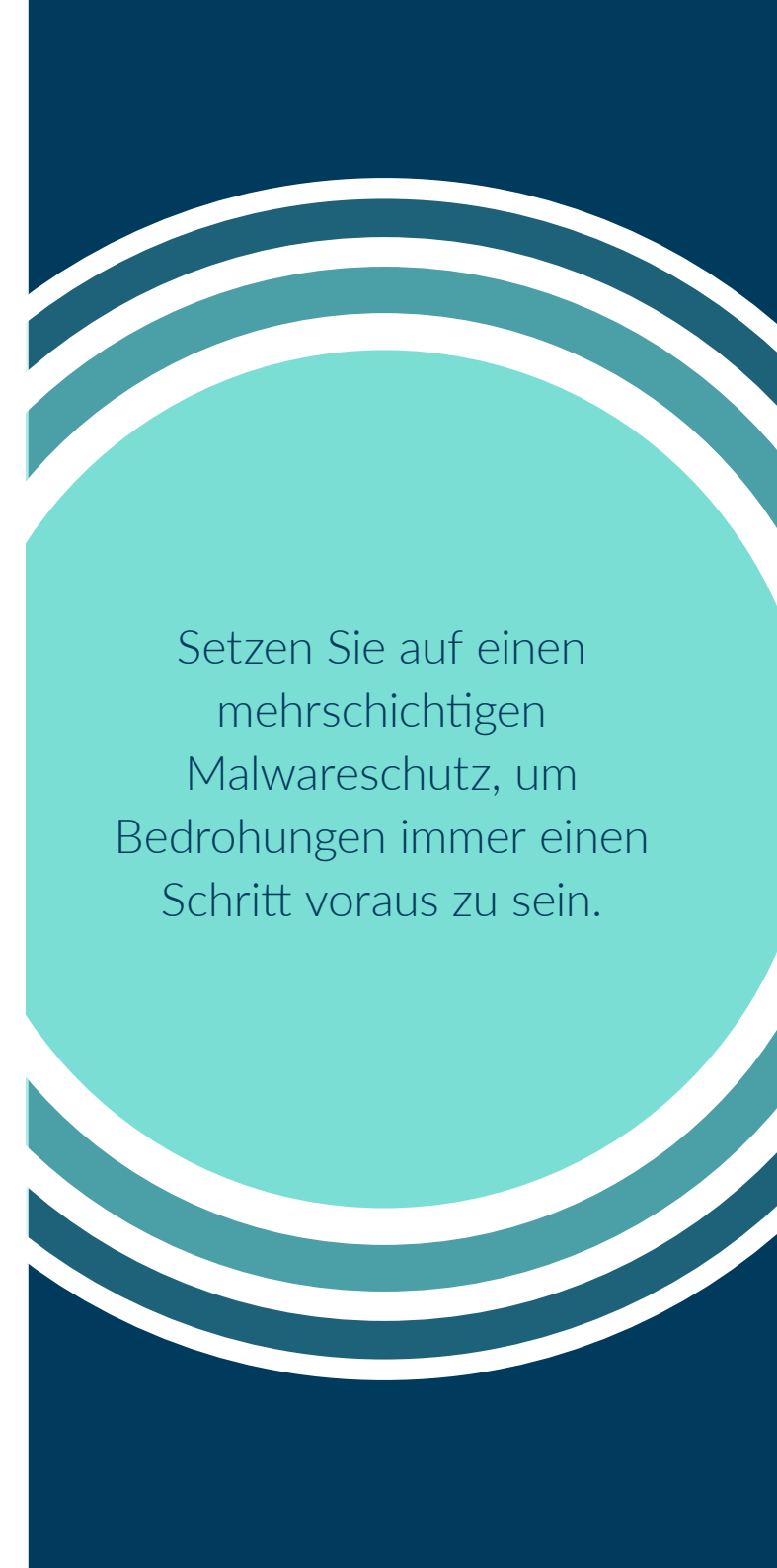
Schützen Sie Ihr Netzwerk vor den unterschiedlichsten Arten von Malware

Jede Firewall sollte Organisationen effektiv vor Viren, Würmern, Trojanern, Spyware und Ransomware schützen. Dies gelingt am ehesten, wenn alle Schutzmechanismen in einen Single-Pass-Ansatz mit niedriger Latenz integriert werden, mit dem sich Angriffsvektoren nicht nur am Gateway, sondern auch an den Endpunkten über die traditionelle Netzwerkgrenze hinaus blockieren lassen. Folgende Funktionen sind besonders wichtig:

- **Netzwerkbasierter Malware-Schutz:** hindert Angreifer daran, Malware in ein kompromittiertes System zu laden oder zu übertragen
- **Laufende und zeitnahe Updates:** stellen sicher, dass Netzwerke vom ersten Augenblick an rund um die Uhr vor Millionen neuer Malware-Varianten geschützt sind
- **Intrusion Prevention Service (IPS):** verhindert, dass Angreifer Schwachstellen im Netzwerk ausnutzen

- **Netzwerk-Sandboxing:** verdächtiger Code wird an eine Cloud-basierte isolierte Umgebung zur Detonation und Analyse weitergeleitet, um komplett neue Malware zu finden
- **Zugriffssicherheit:** Anwendung von Schutz- und Abwehrmechanismen auf mobile und Remote-Endpunkte, sowohl innerhalb als auch außerhalb der Netzwerkgrenze
- **E-Mail-Sicherheit:** Blockieren von Trojanern sowie Phishing-, Spam- und Social-Engineering-Angriffen, die via E-Mail übertragen werden

Sie können Ihr Netzwerk noch besser vor Malware schützen, indem Sie jedes Gerät, das Zugriff auf Ihr Netzwerk hat, mit einer aktuellen Virenschutzsoftware ausstatten. Organisationen können Cyberkriminellen das Leben etwas schwerer machen, indem sie PCs, die mit einer Virenschutzsoftware ausgestattet sind, mit Netzwerk-Firewalls kombinieren.



Setzen Sie auf einen mehrschichtigen Malwareschutz, um Bedrohungen immer einen Schritt voraus zu sein.

Cyberangriffe - Strategie 3

Aufspüren und Infizieren schwacher Netzwerke

Viele Firewall-Anbieter werben zwar damit, dass ihre Lösungen einen erstklassigen Schutz vor Bedrohungen bieten, jedoch konnten sich im Praxiseinsatz nur wenige bewähren. Während sich Organisationen mit zweitklassigen Firewalls in Sicherheit wiegen, umgehen gewiefte Hacker mithilfe komplizierter Algorithmen unbemerkt deren Intrusion-Prevention-Systeme und infizieren das Netzwerk.

Bei vielen Firewalls geht der Schutz zu Lasten der Performance. Nicht selten deaktivieren die Anwender deswegen Schutzfunktionen oder setzen die Sicherheitsstufe herab, um die benötigte Netzwerkperformance zu erreichen – eine äußerst riskante Praxis, von der dringend abzuraten ist.

Eine weitere Schwachstelle in der Netzwerksicherheit ist der Faktor Mensch. Kriminelle nutzen Phishingmails, um Anmelde- und andere Autorisierungsinformationen zu erhalten, mit denen sie die Schutzmechanismen der Firewall ganz einfach umgehen können, indem sie Angriffe von innen heraus veranlassen. Hinzu kommt, dass Mitarbeiter Mobilgeräte verlieren oder eine Datenlücke verursachen können, wenn sie sie außerhalb der Netzwerk-Sicherheitsgrenze verwenden.

Cyberkriminelle wählen ihr Angriffsziel oft anhand der identifizierten Schwachstellen im Netzwerk aus.



Gegenmaßnahme 3

Wählen Sie eine umfassende Sicherheitsplattform mit optimalem Bedrohungsschutz und starker Performance

Sie sollten sich für Sicherheitslösungen entscheiden, die unabhängig getestet und von ICSA Labs für netzwerkbasiereten Malwareschutz zertifiziert wurden.

Zusätzlich sollten Sie eine Multicore-Plattform in Betracht ziehen, mit der Sie Dateien jeder Größe und jeden Typs überprüfen und auf Änderungen im Datenverkehr reagieren können. Alle Firewalls benötigen eine Engine, die Netzwerke vor internen und externen Angriffen schützt, und zwar ohne die Leistung zu beeinträchtigen.

Achten Sie darauf, dass die Firewall eine Netzwerk-Sandbox bietet, um brandneue Malware aufzuspüren, die vielleicht auf Ihre Umgebung zielt. Dies könnte den Unterschied bedeuten zwischen einem normalen Arbeitstag und einem Tag, an dem Ihre Daten in die Hände von Hackern fallen.

Ihre Sicherheitsstrategie muss mobile und Remote-Endpunkte sowohl innerhalb als auch außerhalb der Netzwerkgrenze schützen.

Darüber hinaus muss Ihre E-Mail-Sicherheitsfunktion Schutz vor Phishing-, Spam-, Viren- und Social-Engineering-Angriffen und anderen Bedrohungen bieten, die via E-Mail übertragen werden.

Alle Firewalls benötigen eine Engine, die Netzwerke vor internen und externen Angriffen schützt, und zwar ohne die Leistung zu beeinträchtigen.



Stündlich tauchen rund um den Globus
neue Sicherheitsbedrohungen auf.



Cyberangriffe – Strategie 4

Weltweite Angriffe mit ständig neuen Malware-Varianten

Viele Cyberkriminelle sind mit ihren Angriffen erfolgreich, weil sie kontinuierlich neue Malware erfinden und diese mit ihren weltweiten Verbündeten austauschen. Stündlich tauchen so überall auf der Welt neue Sicherheitsbedrohungen auf. Viele Cyberkriminelle führen Blitzangriffe durch: Sie verschaffen sich Zugriff auf das System, nehmen, was sie bekommen können, und sind wieder weg, bevor jemand Alarm schlagen kann. Dann wiederholen sie den Angriff woanders.

Andere lassen sich mehr Zeit und versuchen, über einen längeren Zeitraum eine größere Menge an Daten zu erbeuten. Manche Angriffe auf das Netzwerk werden über das Internet oder über E-Mails ausgeführt, andere über infizierte Geräte, die sich zuvor außerhalb der Netzwerk-Sicherheitsgrenze befanden.

Gegenmaßnahme 4

Wählen Sie eine Firewall, die Schutz vor globalen Bedrohungen bietet

Für einen größtmöglichen Schutz ist es äußerst wichtig, schnell auf Bedrohungen zu reagieren. Achten Sie daher darauf, dass der Anbieter von Sicherheitslösungen über ein eigenes schnell einsatzbereites internes Team mit Experten für Gegenmaßnahmen verfügt, sodass Abwehrmechanismen gegen neue Bedrohungen schnell auf Ihrer Firewall angewendet werden. Außerdem sollte dieses Team mit zahlreichen anderen Sicherheitsexperten zusammenarbeiten, um seine Reichweite zu vergrößern.

Breit aufgestellte Lösungen nutzen einen globalen Cloud-basierten Malware-Katalog, um die lokale Firewall-Analyse zu ergänzen.

Einfache Firewalls bieten Funktionen zur Identifizierung und zum Blockieren von Daten anhand geographischer Regionen. Hoch entwickelte Firewalls blockieren den Datenverkehr aus gefährlichen Domänen sowie eingehende und ausgehende Verbindungen zu bestimmten Orten. So profitieren Sie zusätzlich von Funktionen zur Botnet-Filterung, mit denen das Risiko durch bekannte globale Bedrohungen reduziert werden kann.

Rundum-Schutz vor den neuesten Bedrohungen erhalten Sie nur mit einer Sicherheitslösung, die auf globale Daten zurückgreift.





Fazit

Die Anzahl an Cyberangriffen nimmt ständig zu, doch es gibt effektive Abwehrmöglichkeiten. Sie möchten wissen, welche Abwehrmechanismen sich am besten für Ihre Netzwerkumgebung eignen? Dann laden Sie unser Whitepaper *Achieving Deeper Network Security* (Verbessern Sie Ihre Netzwerksicherheit) herunter.

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.

Wenden Sie sich bei Fragen zu den Nutzungsmöglichkeiten dieses Materials an:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Weitere Informationen finden Sie auf unserer Website.

www.sonicwall.com

© 2017 SonicWall Inc. ALLE RECHTE VORBEHALTEN.

SonicWall ist eine Marke oder eingetragene Marke von SonicWall Inc. und/oder deren Tochtergesellschaften in den USA und/oder anderen Ländern. Alle anderen Marken und eingetragenen Marken sind Eigentum der jeweiligen Inhaber.

Die Informationen in diesem Dokument werden in Verbindung mit den Produkten von SonicWall Inc. und/oder deren Tochtergesellschaften bereitgestellt. Sie erhalten durch dieses Dokument oder in Verbindung mit dem Verkauf von SonicWall-Produkten keine Lizenz (weder ausdrücklich noch stillschweigend, durch Rechtsverwirkung oder anderweitig) für geistige Eigentumsrechte. SONICWALL UND/ODER DESSEN TOCHTERGESELLSCHAFTEN ÜBERNEHMEN KEINE HAFTUNG UND KEINERLEI AUSDRÜCKLICHE, STILLSCHWEIGENDE ODER GESETZLICHE GEWÄHRLEISTUNG FÜR DEREN PRODUKTE, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG FÜR DIE HANDELSÜBLICHKEIT, DIE VERWENDUNGSFÄHIGKEIT FÜR EINEN BESTIMMTEN ZWECK UND DIE NICHTVERLETZUNG VON RECHTEN DRITTER, SOWEIT SIE NICHT IN DEN BESTIMMUNGEN DER LIZENZVEREINBARUNG FÜR DIESES PRODUKT NIEDERGELEGT SIND. SONICWALL UND/ODER DESSEN TOCHTERGESELLSCHAFTEN HAFTEN NICHT FÜR IRGENDWELCHE UNMITTELBAREN, MITTELBAREN, STRAFRECHTLICHEN, SPEZIELLEN, ZUFÄLLIGEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF SCHÄDEN AUS ENTGANGENEM GEWINN, GESCHÄFTSUNTERBRECHUNG ODER VERLUST VON INFORMATION), DIE AUS DER VERWENDUNG ODER DER UNMÖGLICHKEIT DER VERWENDUNG DIESES DOKUMENTS ENTSTEHEN, SELBST WENN SONICWALL UND/ODER DESSEN TOCHTERGESELLSCHAFTEN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDEN. SonicWall und/oder dessen Tochtergesellschaften übernehmen keine Gewährleistungen in Bezug auf die Genauigkeit oder Vollständigkeit dieses Dokuments und behalten sich das Recht vor, Spezifikationen und Produktbeschreibungen jederzeit ohne Vorankündigung zu ändern. SonicWall Inc. und/oder deren Tochtergesellschaften übernehmen keinerlei Verpflichtung, die in diesem Dokument enthaltenen Informationen zu aktualisieren.