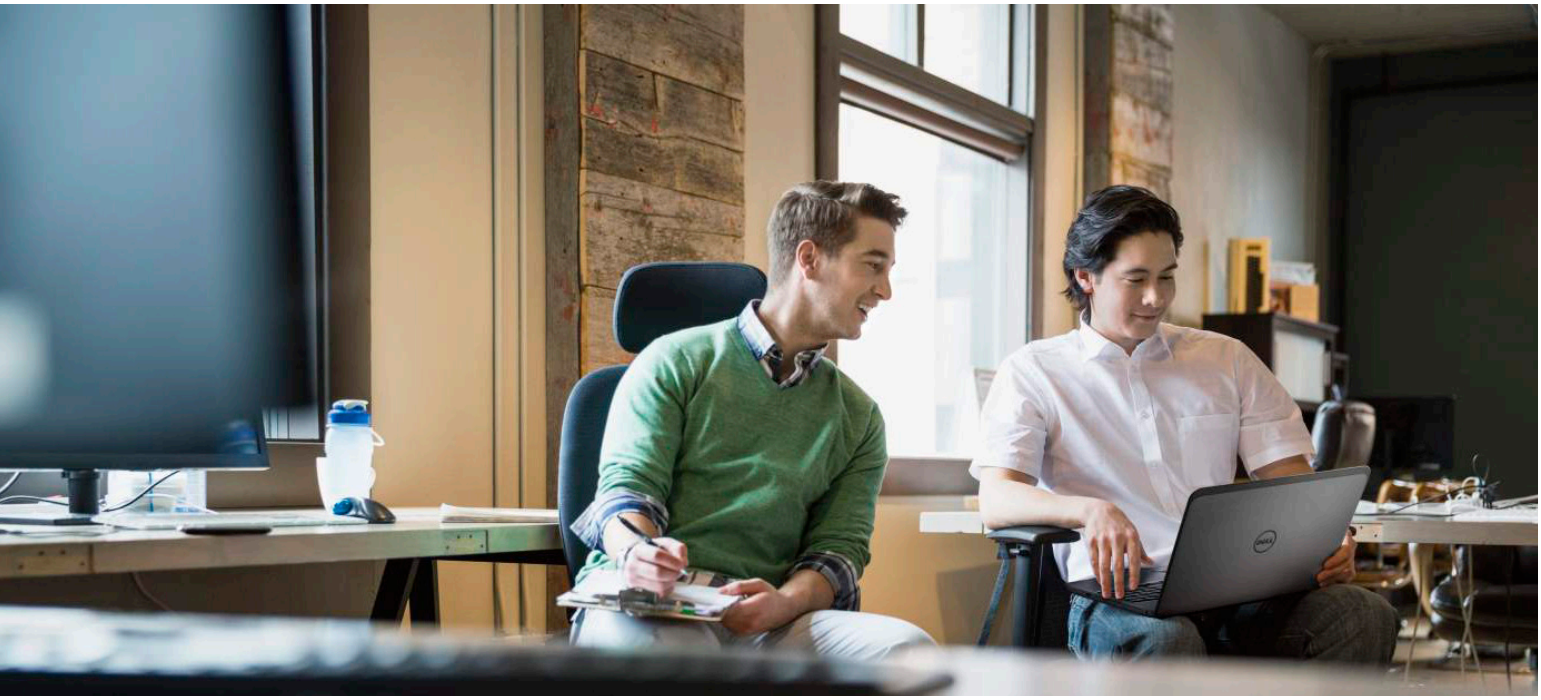
Verteilte Unternehmen und die SonicWALL TZ: Aufbau eines koordinierten Sicherheitsbereiches



Zusammenfassung

Zweigstellen, Einzelhandelsniederlassungen, Remote-Standorte und mobile Mitarbeiter in Unternehmen mit geografisch verteilter Infrastruktur benötigen eine Verbindung zum Hauptsitz. Doch je mehr das Netzwerk ausgedehnt wird, um sie anzubinden, desto schwieriger gestaltet sich die unternehmensweite Verwaltung, Absicherung und Compliance-Gewährleistung für die IT. Das Modell des koordinierten Sicherheitsbereichs bietet Unternehmen mit geografisch verteilter Infrastruktur die zentrale Verwaltung und sichere Wireless-Konnektivität, die sie benötigen, um sich vor den unaufhörlichen Angriffen auf ihr Netzwerk zu schützen.

Dieses Whitepaper erläutert die Hauptprobleme, vor denen Unternehmen mit geografisch verteilter Infrastruktur beim Thema Netzwerksicherheit stehen. Sie erfahren, was der koordinierte Sicherheitsbereich umfasst und wie Ihnen die SonicWALL TZ Series Firewalls dabei helfen können, ihn in Ihrer Organisation umzusetzen.

Einführung

Unternehmen mit Zweigstellen, Remote-Standorten und Einzelhandelsniederlassungen dehnen ihre Netzwerke physisch weit über ihren Hauptsitz hinaus aus und mobile Mitarbeiter erweitern sie nochmals, gleichsam virtuell. In einer geografisch derart verteilten Unternehmensinfrastruktur besteht die dringende Notwendigkeit, einen koordinierten Sicherheitsbereich zu schaffen, der das Netzwerk an allen Punkten schützt, an denen Daten ein- und ausgehen.

In diesem Whitepaper wird der koordinierte Sicherheitsbereich beschrieben, ein Modell, mit dem sich dank zentraler Verwaltung und sicherer Wireless-Konnektivität der Schutz für Unternehmensnetzwerke weit über die Grenzen des sicheren Hauptsitzes hinaus ausdehnen lässt. Wir erläutern Ihnen, wie eine Firewall der nächsten Generation Sicherheitsregeln zentral speichert und verwaltet und wie SonicWALL TZ, eine Firewall mit integriertem Wireless-Controller, diese Regeln an den Bereichsgrenzen durchsetzt.

Unternehmen entwickeln sich fast so schnell weiter wie Sicherheitslösungen. Die Bedrohungen jedoch entwickeln sich noch schneller weiter als beide.

Sicherheitsmaßnahmen halten nicht Schritt

Seit Cyberkriminalität und Angriffe auf Netzwerke allgegenwärtig geworden sind, können Sicherheitslösungen nur noch reagieren. Die Schlagzeile "Is insecurity the new normal?"[1] aus der US-amerikanischen Presse veranschaulicht die aktuelle Situation prägnant: Unternehmen und Verbraucher fühlen sich gleichsam im Belagerungszustand.

In seiner Analyse von 63.000 Vorkommnissen – darunter 1.367 bestätigte Verletzungen der Datensicherheit – kam Verizon zu dem Ergebnis, dass über 70 % der in 95 Ländern erfassten Fälle Angriffe auf Webanwendungen, Cyberspionage und Attacken auf POS (Point of Sale)-Systeme waren.[2]

Dabei entwickeln sich die Bedrohungen rasant weiter. Anfangs gaben sich Cybervandalen noch damit zufrieden, Webseiten zu verunstalten oder ihr Anliegen bekannt zu machen. Dann entstand die Cyberkriminalität, mit dem Ziel, an Geld und Informationen zu gelangen. Heute finden sich auf dem virtuellen Schlachtfeld des Cyberkriegs sogenannte "Hacktivisten" und Nationalstaaten, die versuchen, die Wirtschaft aus dem Gleichgewicht zu bringen und die Infrastruktur zu schädigen. Unternehmen – vor allem kleine Unternehmen – entwickeln sich fast so schnell weiter wie Sicherheitslösungen. Die Bedrohungen jedoch entwickeln sich noch schneller weiter als beide.

Netzwerksicherheitsprobleme in geografisch verteilten Unternehmen

Führen wir uns an dieser Stelle einige Fakten zum Thema Netzwerksicherheit in Unternehmen mit verteilter Infrastruktur vor Augen:

- Kompromiss Datendurchsatz vs. Sicherheit: Angesichts sinkender Kosten für Breitbandverbindungen und Onlinespeicher überträgt das typische Unternehmen immer mehr Daten über sein Netzwerk. Mit zunehmendem Datendurchsatz wird seine fünf Jahre alte Firewall jedoch zu einem Engpass. Das Unternehmen benötigt jetzt eine 1-Gbit/s-Firewall, die es sich aber nicht leisten kann – und entscheidet sich deswegen für einen Kompromiss zwischen Datendurchsatz und Sicherheit. Mit anderen Worten: Oft werden Sicherheitsfunktionen zugunsten der Leistung deaktiviert.
- PCI DSS: Einzelhändler, die Kreditkartendaten erfassen, müssen die Payment Card Industry Data Security Standards (PCI DSS) einhalten. Für die Implementierung und Aufrechterhaltung eines sicheren Netzwerks ist die erste Anforderung die "Installation und Wartung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten".[3] Die zweite Anforderung lautet "Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden." Zwar ist keine dieser beiden Anforderungen für IT-Administratoren in Einzelhandelsniederlassungen allzu kompliziert umzusetzen. Für die zentrale IT-Abteilung sind sie aber zwei weitere Faktoren, die verifiziert werden müssen, um Compliance zu gewährleisten.
- Steigender Umfang des Bereichs: Durch mobile Mitarbeiter, Telearbeiter und lange Lieferketten dehnt sich der Bereich immer weiter über die eigentliche Hauptniederlassung hinaus aus und umfasst auch das Zuhause der Mitarbeiter und Remote-Standorte. Die IT-Abteilung hat weniger Kontrolle und die Verwundbarkeit der Organisation steigt.
- Unterschiedliche Firewalls: Um ihre Verwundbarkeit zu reduzieren, kaufen, installieren und konfigurieren Remote-Standorte Firewalls. Deren Funktionsumfang variiert jedoch je nach Hersteller und Modell, was zu einem unternehmensweiten Flickenteppich aus inkompatiblen Verwaltungskonsolen, Sicherheitsrichtlinien, Signaturen und Updatezeitplänen führt.
- Wireless-Integration: Die meisten Remote-Standorte verwenden mehrere Wireless-Zugriffspunkte, damit Mitarbeiter am Arbeitsplatz flexibler sind. Viele Gastronomie- und Einzelhandelsbetriebe wiederum verwenden sie, um Kunden vor Ort zu halten und sie dazu zu bewegen, ihr Geld bei ihnen auszugeben. Wireless-Controller verursachen jedoch zusätzliche Kosten für die Infrastruktur des Remote-Standorts – und wenn sie nicht in die Firewall integriert sind, entstehen weitere Sicherheitslücken an den Bereichsgrenzen.

Das größte Problem in Unternehmen mit geografisch verteilter Infrastruktur ist also nicht der Umfang des Bereichs an sich, sondern die fehlende Koordination zwischen dem Hauptsitz und den Remote-Standorten an seinen Grenzen.

Stellen Sie sich beispielsweise vor, der Hauptsitz definiert eine Richtlinie, die den Zugriff auf Videowebseiten zwischen 9.00 Uhr und 17.00 Uhr blockiert, und implementiert diese auf der zentralen Firewall. Wie lässt

[1] *Elizabeth Weise, "Is insecurity the new normal?" (Ist Verwundbarkeit der neue Normalzustand?), USA Today, 11. Juni 2014*
[2] *"2014 Data Breach Investigations Report" (Untersuchungsbericht zu unbefugten Datenzugriffen), Verizon Enterprise, April 2014*
[3] *PCI Security Standards Council, "PCI Quick Reference Guide" (PCI Kurzübersicht). Dezember 2009*

sich eine solche Richtlinie auch auf den Firewalls an den Remote-Standorten implementieren, die alle von verschiedenen Herstellern stammen? Im besten Fall kann die IT-Abteilung die Firewalls remote verwalten, was allerdings bedeuten würde, jede von ihnen bei jeder Richtlinienänderung manuell zu konfigurieren. Im schlimmsten Fall muss die IT-Abteilung die Remote-Standorte per E-Mail oder Telefonanruf über die Richtlinie informieren und kann nur hoffen, dass alle Firewalls Regeln unterstützen und dass an jedem Standort ein Mitarbeiter zur Verfügung steht, der sie auch konfigurieren kann.

Ein derartig unkoordiniertes Sicherheitskonzept ist aufgrund der Komplexität der Verwaltung der unterschiedlichen Firewalls ein großes Verwaltungsproblem. Zusätzlich ist es auch ein Compliance-Risiko, da die IT-Abteilung nicht in der Lage ist, ohne viel Aufwand zuverlässige Berichte zur Umsetzung von Richtlinien an den Bereichsgrenzen zu erstellen. Nicht zuletzt ist es auch ein Sicherheitsproblem, da es zu inkonsistenten Regeln und inkonsistenten Sicherheitsstufen führt.

Die Zukunft der Netzwerksicherheit liegt im Aufbau eines koordinierten Sicherheitsbereichs, der die Verwundbarkeit geografisch verteilter Unternehmensnetzwerke selbst an ihren entferntesten Standorten reduziert.

Was umfasst ein koordinierter Sicherheitsbereich?

Um Sicherheitsmaßnahmen auch auf weit entfernte Standorte auszudehnen, braucht es nicht nur Hardware und Software, sondern auch Zentralisierung.

Stellen Sie sich folgendes Extrembeispiel eines geografisch verteilten Konzerns vor: Ein Unternehmen mit Remote-Standorten hat ein anderes Unternehmen mit Remote-Standorten übernommen. Beide Unternehmen haben unterschiedliche Netzwerke und unterschiedliche Sicherheitsstufen. Um einen koordinierten Sicherheitsbereich zu schaffen, müssen die folgenden drei Elemente zentralisiert werden:

1. Richtlinien: Der Hauptsitz muss Sicherheitsrichtlinien und alle für die Compliance erforderlichen internen Verfahren konsistent anwenden.
2. Benutzeroberfläche: Für die Anwendung dieser Richtlinien ist es erforderlich, dass die IT-Administratoren am Hauptsitz und an den Remote-Standorten jeweils dieselbe Benutzeroberfläche und Terminologie für ihre Kommunikation verwenden. Kenntnisse zu Akronymen wie SPI, DMZ und NAT reichen nicht aus. Sie müssen sicher sein können, dass die Firewalls an den verschiedenen Standorten die Sicherheitsmaßnahmen auf die gleiche Weise und mit derselben Benutzeroberfläche implementieren.
3. Sicherheitsfunktionen: Alle Firewalls sollten die gleichen oder einander ergänzende Sicherheitsfunktionen bieten, in dieser Reihenfolge:

a) Inhaltsfilterung, um Schadcode von riskanten Websites zu blockieren, die Benutzer besuchen
b) Angriffsvermeidung, für den Fall, dass Code eindringt und das System nach Sicherheitslücken wie veralteten Signaturen und Laufzeitbibliotheken durchsucht
c) Malwareschutz, um zu verhindern, dass heruntergeladene ausführbare Dateien Sicherheitslücken ausnutzen und sich über das Netzwerk verbreiten
d) Anwendungserkennung und -kontrolle, um zu verhindern, dass bösartige Anwendungen die Netzwerkeffizienz beeinträchtigen

Dieses hierarchische Konzept mit Sicherheitsfunktionen auf jeder Stufe ist ein wichtiger Schritt hin zu effektiver Bedrohungsbekämpfung und Netzwerksicherheit. Es muss jedoch auch von jeder Firewall unterstützt werden.

Eine Zentralisierung dieser Elemente löst die Probleme in puncto Verwaltung, Sicherheit und Compliance – und zwar unternehmensweit. Zentralisierung garantiert in einem geografisch verteilten Unternehmen auch, dass ein starker und koordinierter Sicherheitsbereich um das gesamte Netzwerk gespannt ist.

SonicWALL TZ und der koordinierte Sicherheitsbereich für geografisch verteilte Unternehmen

Die SonicWALL TZ Serie ist Bestandteil einer eng verzahnten Sicherheitslösung. Sie bietet die zentrale Verwaltung und sichere Wireless-Konnektivität, die viele Organisationen heute benötigen. Die TZ Series löst die größten Netzwerksicherheitsprobleme in geografisch verteilten Unternehmen:

- Da die Geschwindigkeit bei der Datenübertragung immer weiter steigt, müssen Unternehmen über eine Firewall verfügen, die Schritt halten kann. TZ Produkte bieten eine höhere Kernzahl und -geschwindigkeit und können für den gesamten Datenverkehr, der die Firewall passiert, Reassembly-Free Deep Packet Inspection® (RFDPI) durchführen, ohne Beeinträchtigung des Datendurchsatzes.
- Alle TZ Produkte verfügen über einen Installationsassistenten, der eine Änderung des werkseitig vorgegebenen Benutzernamens und Kennworts erzwingt, sodass die Organisation von Anfang an die PCI DSS Vorgaben einhält.
- Die TZ Series ist kompakt und erschwinglich genug für Remote-Standorte, Zweigstellen, Einzelhandelsniederlassungen sowie kleine Unternehmen und Heimbüros und bietet Schutz

Die Zukunft der Netzwerksicherheit liegt im Aufbau eines koordinierten Sicherheitsbereichs, der die Verwundbarkeit geografisch verteilter Unternehmensnetzwerke selbst an ihren entferntesten Standorten reduziert.

Alle SonicWALL Produkte basieren auf demselben Code und der Sicherheits-Engine SonicOS, für die die Dell SonicWALL E10800 von NSS Labs die Bewertung "Recommended" (Empfohlen) erhalten hat.

an jedem Punkt an den Außengrenzen des Sicherheitsbereichs.

- Bereichsgrenzen ohne Firewalls sind schlecht, Bereichsgrenzen mit einem Sammelsurium von miteinander inkompatiblen Firewalls sind jedoch nicht viel besser. Alle TZ Firewalls bieten dasselbe effektive Sicherheitsniveau wie SonicWALL Enterprise-Produkte, damit Richtlinien, Signaturen und Updates unternehmensweit synchron bleiben.
- Ein integrierter Wireless-Controller liefert Firewall-Sicherheit für Wireless-Konnektivität und ermöglicht die Erstellung und Verwaltung von separaten Richtliniensätzen für Mitarbeiter mit umfassenden Zugriffsrechten und Besucher mit Gastzugriff. Sicheres High-Speed-Wireless gemäß 802.11ac ist in der Firewall integriert oder über Dell SonicPoint Wireless-Zugriffspunkte verfügbar.[4]

Die TZ Series wurde für zentrale Verwaltung und sichere Wireless-Konnektivität in geografisch verteilten Unternehmen entwickelt und koordiniert die Netzwerksicherheitsmaßnahmen an den Bereichsgrenzen mit denen der Unternehmens-Firewall. Allen IT-Administratoren im Unternehmen steht eine konsistente Benutzeroberfläche zur Verfügung, die die Remote-Standortverwaltung vereinfacht. Alle SonicWALL Firewalls basieren auf demselben Code und der Sicherheits-Engine SonicOS, für die die Dell SonicWALL E10800 von NSS Labs die Bewertung "Recommended" (Empfohlen) erhalten hat.

Das SonicWALL Global Management System (GMS) ermöglicht die zentralisierte Konfiguration und Überwachung aller SonicWALL Firewalls in Unternehmen mit geografisch verteilter Infrastruktur. Vom Hauptsitz aus können IT-Administratoren auf allen TZ Firewalls an jedem Standort weltweit Aktivitäten beobachten, Richtlinien und Updates implementieren und die Bedrohungserkennung prüfen (siehe Abbildung 1). Für neue Punkte an den Bereichsgrenzen können sie mit GMS Images auf neue TZ Firewalls aufspielen und so sicherstellen, dass sie alle dieselben Richtlinien und Regeln verwenden. Auch wenn die Bedrohungen sich weiterentwickeln und sich die Sicherheitsanforderungen ändern, können Organisationen mithilfe von GMS die Verwaltung am Hauptstandort zentralisieren, alle Remote-Standorte mit der Haupt-Firewall synchronisieren und an jedem Punkt an den Bereichsgrenzen dasselbe Sicherheitsniveau erzwingen.

SonicWALL TZ unterstützt das hierarchische Sicherheitskonzept, indem Inhalts-/URL-Filterung, Angriffsvermeidung, Malwareschutz sowie Anwendungserkennung und -kontrolle stufenweise angewendet werden, um Angriffe abzuwehren.

Abbildung 1: SonicWALL TZ und der koordinierte Sicherheitsbereich für geografisch verteilte Unternehmen

[4]802.11ac wird auf den Modellen TZ300, TZ400, TZ500 und TZ600 unterstützt.

Vorteile für das gesamte geografisch verteilte Unternehmen

Zentrale Verwaltung und sichere Wireless-Konnektivität bringen dem gesamten Unternehmen Vorteile.

- Die IT-Abteilung hat mehr Kontrolle. Die konsistente Benutzeroberfläche und der konsistente Betriebsmodus von SonicWALL bedeuten, dass die IT-Abteilung nicht eine Vielzahl von Appliances remote verwalten oder unterschiedliche Anweisungen für unterschiedliche Produkte ausgeben muss. Sie kann alle ein- und ausgehenden Daten im Netzwerk einheitlich prüfen und sich so jederzeit vergewissern, dass die Bereichsgrenzen sicher sind.
- Das Unternehmen kann mit den Forderungen nach höherem Datendurchsatz Schritt halten. SonicWALL TZ unterstützt eine stufenweise Erhöhung der Netzwerkgeschwindigkeit und blockiert gleichzeitig die stetig steigende Anzahl an Angriffen.
- Zweigstellen und Remote-Standorte sprechen endlich "dieselbe Sprache" wie der Hauptsitz. Wenn lokale Administratoren mit derselben TZ Benutzeroberfläche und Sicherheits-Engine arbeiten wie die IT-Abteilung am Hauptsitz, verringern sich an den Bereichsgrenzen die Risiken durch Kommunikationsfehler. Mitarbeiter an anderen Standorten, die eine TZ Firewall installieren, auf die das Image bereits am Hauptsitz aufgespielt wurde, können sicher sein, dass ihre Firewall dieselben Sicherheitseinstellungen nutzt wie die zentrale Firewall.
- Remote-Mitarbeiter werden Teil des Sicherheitsbereichs. Die Wahrscheinlichkeit, dass ein Remote- oder Telearbeiter hinter einer TZ Firewall das Unternehmen mit Malware infiziert, ist wesentlich geringer, vor allem, wenn die Firewall zentral konfiguriert und kontrolliert wird.
- Mobile Mitarbeiter bleiben sicher, wenn sie zwischen Zugriffspunkten wechseln. Das SonicWALL VPN basiert auf einer proprietären App, die Sicherheitsupdates schnell bereitstellt. Die Variabilität allgemeiner VPN-Clients ist kein Thema mehr.
- Kunden, Besuchern und Gästen steht ein vom Unternehmen bereitgestelltes sicheres WLAN zur Verfügung. Wenn Einzelhandelsunternehmen oder Betriebe im Gastgewerbe TZ Firewalls bereitstellen, um ihren Kunden High-Speed-WLAN zu bieten, können sie die Markentreue fördern, ohne Sicherheitsrisiken an den Bereichsgrenzen in Kauf nehmen zu müssen.

Fazit

Für geografisch verteilte Unternehmen wie Einzelhandelsketten, Banken und Gesundheitsdienstleister sind Cyberangriffe an den Bereichsgrenzen heute zu einer besorgniserregenden Gefahr für den Hauptsitz geworden. Da sie jedoch immer mehr Zweigstellen, Remote-Standorte und kleine Büros einrichten oder auf Heimarbeit setzen, dehnen Kunden, Zulieferer und Mitarbeiter ihren Bereich immer weiter aus. Obgleich Netzwerksicherheit aufgrund von Inkonsistenzen zwischen den im Unternehmen bereitgestellten Firewalls schwer zu erreichen ist, ist der koordinierte Sicherheitsbereich ein leistungsfähiges Modell, um Angriffe abzuwehren – überall.

SonicWALL TZ Firewalls mit einer Verbindung zur SonicWALL Firewall am Hauptstandort bieten die zentrale Verwaltung und sichere Wireless-Konnektivität, die für den Aufbau eines koordinierten Sicherheitsbereichs in Unternehmen mit geografisch verteilter Infrastruktur notwendig sind. Dank eines konsistenten Richtliniensatzes, konsistentem Malwareschutz und einer konsistenten Benutzeroberfläche in der gesamten Organisation hemmen die Sicherheitsmaßnahmen das Unternehmen nicht mehr, sondern werden zum Erfolgsfaktor.

Mitarbeiter an anderen Standorten, die eine TZ Firewall installieren, auf die das Image bereits am Hauptsitz aufgespielt wurde, können sicher sein, dass ihre Firewall dieselben Sicherheitseinstel-lungen nutzt wie die zentrale Firewall.

Weitere Informationen

Die Informationen in diesem Dokument beziehen sich auf Dell Produkte. Dieses Dokument sowie der Verkauf von Dell Produkten gewähren weder durch Rechtsverwirkung noch auf andere Weise ausdrückliche oder implizite Lizenzen auf geistige Eigentumsrechte. Es gelten ausschließlich die in der Lizenzvereinbarung von Dell für dieses Produkt festgelegten Geschäftsbedingungen. Dell übernimmt keinerlei Haftung und lehnt jegliche ausdrückliche oder implizierte oder gesetzliche Gewährleistung in Bezug auf die Produkte von Dell ab, einschließlich, jedoch nicht beschränkt auf, stillschweigende Gewährleistung der handelsüblichen Qualität, Eignung für einen bestimmten Zweck und Nichtverletzung der Rechte Dritter. In keinem Fall haftet Dell für direkte oder indirekte Schäden, Folgeschäden, beiläufig entstandene, besondere oder sonstige Schäden oder Schadensersatzansprüche, die durch die Nutzung oder die Unfähigkeit zur Nutzung dieses Dokuments entstehen können (einschließlich, jedoch nicht beschränkt auf, entgangene Gewinne, Geschäftsunterbrechungen oder Datenverlust), selbst wenn Dell auf die Möglichkeit derartiger Schäden hingewiesen wurde. Dell gibt keinerlei Zusicherungen oder Gewährleistungen hinsichtlich der Richtigkeit oder Vollständigkeit der Informationen in diesem Dokument und behält sich das Recht vor, die Spezifikationen und Produktbeschreibungen jederzeit ohne Benachrichtigung zu ändern. Dell verpflichtet sich nicht dazu, die Informationen in diesem Dokument zu aktualisieren.

Über Dell Software

Dell Software unterstützt Kunden dabei, ihr Potenzial durch den Einsatz von Technologie voll auszuschöpfen – mit skalierbaren, erschwinglichen und benutzerfreundlichen Lösungen, die die IT vereinfachen und Risiken minimieren. Das Portfolio von Dell Software deckt Kundenanforderungen in fünf Schlüsselbereichen ab: Rechenzentrums- und Cloud-Verwaltung, Informationsverwaltung, Verwaltung mobiler Mitarbeiter sowie Sicherheit und Datensicherung. In Kombination mit Hardware und Services von Dell versetzen unsere Softwareprodukte Kunden in die Lage, effizienter und produktiver zu arbeiten und schnellere Geschäftsergebnisse zu erzielen. dellsoftware.de.

Bei Fragen zur möglichen Nutzung dieses Dokuments wenden Sie sich bitte an:

Dell Software

dellsoftware.de
Informationen zu unseren regionalen und internationalen Büros finden Sie auf unserer Webseite.