ÜBERBLICK

DIE CISCO SELF-DEFENDING NETWORK-STRATEGIE

SICHERHEIT ALS GESCHÄFTLICHER IMPERATIV

Die riesigen zusammengeschalteten Datennetze von heute sind unerlässlich für Unternehmen, die mit geschäftlichen Veränderungen Schritt halten müssen und wollen, denn sie stellen auch gleichzeitig eine Chance für die Unternehmen dar, ein höheres Leistungs- und Gewinnniveau zu erreichen. Allerdings wird es angesichts der Bedrohungen durch Informationsdiebstahl, Virusattacken und Missbrauch von Anwendungen auch immer kritischer für Unternehmen, das Unternehmensnetz und wertvolle Ressourcen zu schützen. Ganz gleich, ob es Mitarbeiter und andere Insider sind, die Informationen stehlen, oder Hacker, die versuchen, den nach außen gerichteten Schutz des Netzwerks zu durchbrechen – Unternehmen aller Größenordnungen müssen sich vor Informationsdiebstahl, Virusausbrüchen und Missbrauch von Anwendungen, sei es durch bekannte oder unbekannte Bedrohungen, interne oder externe Elemente, schützen. Es liegt klar auf der Hand, dass die Sicherheit des Netzwerks ein geschäftlicher Imperativ ist.

IMPLEMENTIERUNG VON SICHERHEITSMASSNAHMEN

Um Informationsdiebstahl zu verhindern bzw. seine Auswirkungen auf ein Minimum zu beschränken, müssen Unternehmen Sicherheitsmaßnahmen implementieren, so z.B. unternehmensweite Sicherheitsrichtlinien, Einschränkung der Zugriffsrechte auf authentisierte Nutzer und Schutz für die Daten- und Sprachübertragung. Technische Entscheidungsträger müssen sich mit einer Reihe von Problemen hinsichtlich der Netzwerksicherheit auseinandersetzen – ganz gleich, ob es ein Diebstahl vertraulicher Informationen oder ein Virusausbruch ist, der geschäftskritische Anwendungen zum Erliegen bringt und die PCs der Mitarbeiter lahmlegt, oder ein Missbrauch von Anwendungen, durch den wertvolle geschäftliche Ressourcen und Bandbreite „ausgehungert“ werden. Darüber hinaus müssen sie sich auch mit anderen Belangen auseinandersetzen, beispielsweise mit internen Zugriffskontrollen, Krisenplänen für den Angriffsfall sowie mit der Gesamtperformance des Netzwerks. Ein Sicherheitssystem muss vollständig in alle Aspekte des Netzwerks integriert sein, so dass potenziell schädliche Aktivitäten erkannt, Bedrohungen identifiziert und die Attacken durch entsprechende Anpassungsmaßnahmen koordiniert abgewehrt werden können.

DIE CISCO SELF-DEFENDING NETWORK-STRATEGIE

Das Cisco® Self-Defending Network schützt das Unternehmen vor internen und externen Bedrohungen, indem es sie identifiziert und Angriffe mithilfe von „Adaptive Security“-Lösungen verhindert. So geschützt kann die Organisation die Intelligenz ihrer Netzwerkressourcen besser ausnutzen, ihre geschäftlichen Prozesse verbessern und ihre Kosten senken. Diese Strategie des sich selbst verteidigenden Netzwerks ist auf Identifizierung und Verhinderung interner und externer Bedrohungen sowie eine der Bedrohung entsprechende Anpassung des Netzwerksbetriebs ausgelegt.

Die drei Standardmerkmale des Cisco Self-Defending Network

Integrationsstandard

Jedes Element im Netzwerk fungiert als Abwehrpunkt, und alle Elemente arbeiten im Verbund, um ein sicheres und adaptives System zu schaffen. Sicherheitsfunktionen, darunter Firewalls, Virtual Private Networking, Identitätsfunktionen und Intrusion Prevention Systems (IPS) sind in Router, Switches, Appliances und Endpunkte integriert. Darüber hinaus beinhaltet dieser Standard die im sicheren Betrieb von Netzwerkgeräten inhärenten Technologien wie Control Plane Policing und CPU/Memory Thresholding

Kollaborationsstandard

Verschiedene Netzwerkkomponenten arbeiten im Verbund, um neue Schutzmaßnahmen zu bilden, und Sicherheit wird zu einer das gesamte System umfassenden Kooperation von Endpunkten, Netzwerkelementen und Maßnahmen zur Durchsetzung der Sicherheitspolitik (Policy Enforcement). Das Network Admission Control-Programm (NAC) ist ein Beispiel dieses Prinzips, wobei Geräte, die den aktuellen Sicherheitsrichtlinien nicht entsprechen, gar nicht erst in das Netzwerk hineingelassen werden und Zugriffskontrollen von Netzwerkgeräten wie Routern und Switches durchgesetzt werden.

Anpassungsstandard

Das Adaptive Security-Konzept gestattet die automatische Verwendung innovativer Verhaltensweisen, um neue Bedrohungen bereits zu erkennen, wenn sie noch in der Entstehung begriffen sind. Zwischen den Sicherheitsdiensten und der Netzwerkintelligenz kann ein gemeinsames Bewusstsein geschaffen werden, durch das die Effektivität der Sicherheit erhöht und eine proaktivere Reaktion auf neue Bedrohungen möglich wird. Sicherheitsrisiken werden durch dieses gemeinsame Bewusstsein effektiv gemindert, da die Kapazitäten zur Erkennung und Abwehr von Bedrohungen auf mehreren Schichten des Netzwerks erweitert werden.

VORTEILE DER CISCO SELF-DEFENDING NETWORK-STRATEGIE

- Verbesserte Flexibilität und Einfachheit des Netzwerkschutzes
- Verbesserte IT-Verwaltung und Effizienz
- Koordinierte Erkennung verdächtiger Aktivitäten, Identifizierung von Bedrohungen und Abwehr von Attacken
- Schutz vor Nutzern mit unsicheren oder infizierten PCs
- Verbesserte Netzwerkbetriebszeiten durch Echtzeit-Reaktion auf bekannte und unbekannte Bedrohungen
- Schutz für die Vermögenswerte und den Ruf des Unternehmens
- Effektive unternehmensweite Durchsetzung der Sicherheitspolitik

Zur Cisco Self-Defending Network-Initiative gehörige Technologien und Produkte

- Day-Zero-Schutz mit dem Cisco Security Agent
- Zugriffskontrolle über NAC
- Sichere Konnektivität mit IPSec-VPN-Systemen (IP Security)
- Adaptive Security Appliance mit Stateful Firewall-Funktion, VPN, IPS und Antivirus
- CiscoWorks Managementlösung

CISCO IST DER BRANCHENFÜHRER FÜR NETWORKING- UND SICHERHEITSLÖSUNGEN

Cisco Systems® bietet das umfangreichste Angebot an integrierten Sicherheitslösungen, die Organisationen aller Größen vor Diebstahl schützen. Die Cisco Self-Defending Network-Lösung beruht auf einem systemweiten Sicherheitsansatz, der auf der Kollaboration von Networking- und Sicherheitstechnologien beruht und Sicherheitsintelligenz integriert, die Vermögenswerte des Unternehmens schützt und den Wert der vorhandenen Netzwerkinfrastruktur einer Organisation erhöht.

WEITERE INFORMATIONEN

Näheres zum Schutz Ihres Unternehmens vor Virusausbrüchen sowie weitere Einzelheiten zur Cisco Self-Defending Network-Strategie finden Sie unter: http://www.cisco.com/go/midsizedsecurity oder http://www.cisco.com/go/selfdefend

CISCO SYSTEMS GESCHÄFTSSTELLEN IN DEUTSCHLAND

Cisco Systems GmbH Kurfürstendamm 22 D–10719 Berlin www.cisco.de Tel: 00800-9999-0522	**Cisco Systems GmbH** Neuer Wall 77 D–20354 Hamburg www.cisco.de Tel: 00800-9999-0522	**Cisco Systems GmbH** Hansaallee 249 D–40549 Düsseldorf www.cisco.de Tel: 00800-9999-0522	**Cisco Systems GmbH** Ludwig-Erhard-Straße 3 D–65760 Eschborn www.cisco.de Tel: 00800-9999-0522	**Cisco Systems GmbH** Wilhelmsplatz 11 (Herold Center) D–70182 Stuttgart www.cisco.de Tel: 00800-9999-0522	**Cisco Systems GmbH** Am Söldnermoos 17 D–85399 Hallbergmoos www.cisco.de Tel: 00800-9999-0522

Cisco Systems ist mit mehr als 200 Niederlassungen in den folgenden Ländern vertreten. Adressen, Telefon- und Faxnummern finden Sie auf der Cisco Website unter **www.cisco.com/go/offices.**

Argentinien • Australien • Belgien • Brasilien • Bulgarien • Chile • Costa-Rica • Dänemark • Deutschland • Dubai, VAE • Finnland • Frankreich • Griechenland • Hongkong • Indien • Indonesien • Irland • Israel • Italien • Japan • Kanada • Kolumbien • Korea • Kroatien • Luxemburg • Malaysia • Mexiko • Neuseeland • Niederlande • Norwegen • Österreich • Peru • Philippinen • Polen • Portugal • Puerto-Rico • Rumänien • Russland • Saudi-Arabien • Schottland • Schweden • Schweiz • Simbabwe • Singapur • Slowakei • Slowenien • Spanien • Südafrika • Taiwan • Thailand • Tschechische Republik • Türkei • Ukraine • Ungarn • USA • Venezuela • Vereinigtes Königreich • VR China • Zypern

205353.M_ETMG_KL_8.05
Printed in the USA