

Systematische Netzwerkabsicherung

Die Verwaltung von Desktops, Laptops und Servern an den Endpunkten von Unternehmensnetzwerken ist sehr komplex, zeitaufwändig und kostenintensiv. In diesem Beitrag werden verschiedene Aspekte der Netzwerkverwaltung untersucht, Hauptkriterien bei der Auswahl einer Lösung aufgeführt und Endpoint-Security-Lösungen vorgestellt, die den Verwaltungsaufwand verringern und die Kosten senken.

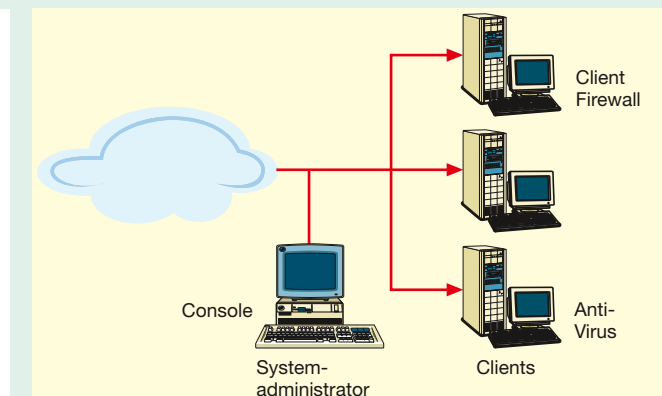
Aktuelle Bedrohungen

Der Schutz eines Unternehmensnetzwerks nimmt immer mehr Zeit und Ressourcen in Anspruch. Malware wird immer komplexer, da verschiedene Techniken für ihre schnellere Verteilung kombiniert werden und ihre Zielsetzung sich geändert hat. Die Angriffe richten sich nun gegen kleine Zielgruppen, um der Erkennung durch Schutz-Software zu entkommen. Zudem zielen Internetkriminelle darauf ab, unvorsichtigen Anwendern das Geld aus der Tasche zu ziehen. Die Anzahl der mit Viren infizierten E-Mails ist im vergangenen Jahr stark zurückgegangen, da Hacker jetzt zielgerichtete Angriffe mit Trojanern durchführen, die Spyware enthalten, anstatt wahllos Massenmails zu versenden. Im Mai 2005 war eine von 38 E-Mails infiziert. Diese Anzahl ist im Jahr 2006 auf nur eine von 141 E-Mails zurückgegangen, da Kriminelle nach neuen Wegen suchen, in Unternehmensnetzwerke einzudringen. Aufgrund des nicht abbreißenden Stroms neuer Bedrohungen, wie Spyware, Adware und Hacker, wird es für Unternehmen immer schwieriger, sich vor Übergriffen und Infektionen zu schützen. Gleichzeitig verändern sich IT-Anforderungen, da die Endbenutzer Internet und E-Mail auch außerhalb der kontrollierten Umgebung eines LAN (Local Area Network) nutzen möchten. Drahtlose Netzwerke, PDA, Laptops und USB-Speichergeräte ermöglichen Anwendern das Arbeiten außer Haus. Obwohl es für ein Unternehmen zahlreiche Gründe gibt, diese Entwicklung zu begrüßen, birgt sie doch auch Risiken. Mobile Computer, die nicht ausreichend geschützt sind, können das Unternehmensnetzwerk mit

unbekannten Bedrohungen infizieren und Geschäftsaktivitäten gefährden. Es ist daher äußerst wichtig, Bedrohungen bereits am E-Mail-Gateway zu stoppen, so dass sie erst gar nicht in das Unternehmensnetzwerk gelangen, doch die heutige Maxime „Jederzeit und überall verbunden sein“ führt dazu, dass der traditionelle Gateway-Schutz oft nicht ausreicht. Zahlreiche Bedrohungen werden erst auf den Endgeräten erkannt, d. h. auf Laptops, Desktops und Servern.

Herausforderungen für IT-Lösungen

Obwohl die Erstellung und Durchsetzung umfassender Sicherheits-Richtlinien höchste Priorität hat, können Einsatz und Steuerung verschiedener Sicherheitstechnologien zum Schutz jedes Netzwerk-Eintrittspunkts unnötig viel Zeit, Geld und Ressourcen in Anspruch nehmen. Die effektive Verwaltung des Schutzes aller Endpoints bringt Probleme mit sich, deren Behebung sich als komplex und kostenintensiv herausstellen kann. Es stellen sich die Fragen, woher man weiß, welche Computer betroffen sind, wie man sie sofort schützen kann und wie man die betroffenen Computer herausfiltern kann. Sicherheitsanbieter haben den neuen Trend von Bedrohungen erkannt und deshalb Software, Applikationen und Firewalls zum Schutz vor Malware auf den Markt gebracht, von denen sie sich Abhilfe dieses Problems versprechen. Ironischerweise sind es gerade die zur Abhilfe gedachten Funktionen dieser Produkte, die fehlschlagen. Diese Produkte sind oft so ausgefeilt und komplex, dass sie separat verwaltet



❶ Schematische Darstellung zur Netzwerkabsicherung mit dem vorgestellten System
Quelle: Sophos

werden müssen. Eine schnelle Reaktion auf sich rasch verändernde Bedrohungen wäre unerlässlich – ist aber oft nicht möglich. Es ist nicht wichtig, wie viele Funktionen ein Produkt bietet oder wie komplex sein Einsatz ist, sondern wie nützlich diese Funktionen wirklich sind, ob sie sich einfach integrieren lassen und benutzerfreundlich sind.

Endpoint-Security – Verringerte Kosten

Das Problem der Verwaltung von Sicherheitslösungen und Richtlinien in großen Netzwerken besteht in einzelnen Verwaltungsaufgaben, die bunt zusammengewürfelte Sicherheitslösungen kreieren. Solch eine Verwaltung ist sehr zeit- und kostenaufwändig. Um die Gesamtkosten, die so genannten Total Cost of Ownership (TCO), für die Verwaltung von Endpoint Security zu verringern, muss man eine Lösung finden, die eine leistungsstarke, skalierbare Verwaltung aller Endpoint-Computer bietet, aber trotzdem übersichtlich und bedienerfreundlich ist, so dass man die Sicherheits-Software für das gesamte Netzwerk von einem einzigen Punkt aus verwalten kann. Eine integrierte Lösung, wie z. B. Sophos Endpoint Security, spart sowohl Kosten als auch Zeit, so dass man sich auf wichtige Aufgaben konzentrieren kann.

Proaktiver Schutz vor allen Bedrohungen

Bei der Wahl einer Sicherheitslösung stehen Verlässlichkeit und Schutz vor bekannten und unbekannten Bedrohungen an erster Stelle. Die Lösung muss nicht nur

vor Viren und Würmern schützen, sondern auch vor Hackern, Spyware und potentiell unerwünschten Anwendungen, wie z. B. Adware. Experten des Herstellers, die im weltweiten Netzwerk aus Viren-, Spyware- und Spam-Analysecentern tätig sind, kombinieren Fachwissen, Technologien und Einsicht in gerade entstehende Bedrohungen zur Bereitstellung eines effizienten rund-um-die-Uhr-Schutzes mit kleinen automatischen Schutz-Updates. Die Anti-Virus-Applikation schützt dank der Überwachung des Verhaltens vor Spyware, Trojanern, Viren und Würmern. Hinzu kommen z. B. Port-Blocking-Funktionen durch die Client Firewall. Doch selbst diese preisgekrönten Lösungen reichen allein nicht aus. Schutz alleine, so umfassend er auch sein mag, rentiert sich nicht, wenn man viel Zeit damit verbringt, einzelne Computer aufzusuchen und zu warten oder wenn man die selben Richtlinien für Malware und Firewall wieder und wieder erstellen muss, um sie für verschiedene Computergruppen umzusetzen. Daher können Anti-Virus und die Client Firewall mit einer zentralen Management-Konsole verwaltet werden (Bild ❶). Nachfolgend werden weitere Kriterien aufgeführt, die neben dem Schutz für eine effiziente Verwaltungs-Lösung erforderlich sind.

Lösung ermöglicht zentrale Verwaltung und Steuerung

Das Erfordernis, zu vielen verschiedenen Computern zu gehen, um dort Software zu installieren, Richtlinien zu erstellen oder durchzusetzen oder durch Malware verursachte Schäden zu beheben, nimmt viel Zeit und auch IT-Ressourcen in Anspruch.

Zentrale Installation und Updates.

Die Enterprise Console – eine der Hauptkomponenten der Sophos Endpoint Security – ermöglicht Administratoren den Einsatz und das Update der dazu gehörigen Anti-Virus-Applikation und der Client Firewall im gesamten Netzwerk, einschließlich Remote-Computern – alles von einer einzigen Konsole aus. Dank der eingebauten Suchfunktion, über Microsoft Active Directory oder die Suche in IP-Subnetzbereichen können alle Computer des Netzwerks einfach gefunden werden.

Schnelle Erstellung und Durchsetzung von Richtlinien.

Dank Active Policies, einer der Hauptfunktionen der Konsole, lassen sich z. B. Sicherheits-Richtlinien schnell erstellen und auch aktualisieren. So kann eine einzige Richtlinie für mehrere Gruppen gleichzeitig umgesetzt werden und muss nicht für jede Gruppe, für die sie gelten soll, neu erstellt werden.

Zentrale Bereinigung. Die Bereinigung großer Netzwerke mithilfe einzelner Bereinigungswerkzeuge kann nach einem Malware-Angriff kosten- und zeitintensiv sein. Die Erkennung infizierter Computer und eine zielgerichtete Bereinigung von Viren, Spyware und Trojanern kann die Produktivität des Unternehmens enorm steigern und die Kosten solch eines Vorfalls erheblich senken.

Autorisieren ausgewählter PUA.

Potentiell unerwünschte Anwendungen (PUA), wie z. B. Adware, sind für eine Verwendung im Unternehmensnetzwerk normalerweise nicht angemessen, obwohl sie nicht schädlich sind. Aus diesem Grund werden PUA von der Anti-Virus-Anwendung standardmäßig blockiert. Weil manche Unternehmen jedoch einige dieser Anwendungen erlauben möchten, kann man diese von der Konsole aus problemlos auswählen und zentral erlauben. Ebenso lassen sich die Anwendungen auch zentral blockieren.

Steuerung des Netzwerkzugriffs.

Computer, die sich mit dem Netzwerk verbinden und nicht geschützt sind oder nicht mit den Richtlinien übereinstimmen, infizieren Netzwerke oftmals. Die Integration der Anti-Virus-Anwendung mit Cisco NAC (Network Admission Control) ermöglicht Administratoren die Steuerung

von Computern, die sich ab und an mit ihrem Netzwerk verbinden, so dass man sicherstellen kann, dass diese über einen aktuellen Schutz verfügen, bevor sie sich dann erneut mit dem Netzwerk verbinden.

Übersicht über das Netzwerk. Da sich die Bedrohungen immer schneller verbreiten, ist es unerlässlich, anfällige Bereiche des Netzwerks auf einen Blick zu erkennen. Smart Views, ein weiterer Bestandteil dieser Sicherheitslösung, zeigt alle anfälligen Computer an, die nicht mit den gewünschten Sicherheits-Richtlinien übereinstimmen, für die Updates erforderlich sind oder die bereinigt werden müssen.

Alarme in Echtzeit. Gelangt eine Bedrohung in das Netzwerk, muss man sofort darüber unterrichtet werden, um die Infizierung zu bereinigen und Schäden zu beheben. Bei erkannter Malware oder PUA wird ein Alarm auf dem Computer angezeigt und an den Administrator gesendet.

Steuerung der Bandbreitennutzung.

Wenn man nicht die Möglichkeit hat, die Durchführung von Updates des Malware-Schutzes oder der Firewall zu steuern, werden nicht nur das Netzwerk, sondern auch die IT-Ressourcen stark belastet. Das Sicherheitskonzept ermöglicht die Begrenzung von Bandbreite, so dass man den Zeitpunkt für Updates im gesamten Unternehmensnetzwerk festlegen kann.

Skalierbarkeit

Die Verwaltung und Steuerung des Einsatzes einer Sicherheits-Software ist in kleineren Netzwerken oft noch relativ einfach, doch bei größerer Anzahl an Computern und Computergruppen kann das erhebliche Probleme mit sich bringen.

Verwaltung großer Netzwerke.

Einige Lösungen sind theoretisch in der Lage, mehrere Tausend Computer zu verwalten, doch in der Praxis sieht das ganz anders aus: Da die Kommunikation zwischen Management-Servern und Clients stark verzögert wird, sind sie einfach ungeeignet. Die beschriebene Konsole verwendet dagegen intelligente Lösungen zum Vergleich und zur Priorisierung von Benachrichtigungen am

Glossar

Adware: Software die Werbefbanner u. Ä. enthält

Client: Anwendung, die Dienst eines Servers im Netzwerk in Anspruch nimmt; oft wird Rechner, auf dem Client-Anwendung läuft, als Client bezeichnet

Endpoint/Endpoint-Security: Endgerät/Endgeräte-Schutz

Firewall: System aus Soft- und Hardwarekomponenten, das den Zugriff zwischen verschiedenen Rechnernetzen beschränkt

Gateway: Gerät, das Verbindung und Kommunikation von Netzwerken ermöglicht, die auf verschiedenen Protokollen basieren

Hacker: Personen, die sich unbefugt Zutritt zu Rechnern/Netzwerken verschaffen

Malware: Programme, die unerwünschte, schädliche Funktionen getarnt im Hintergrund ausführen (z. B. ungewollte Datenlöschung u. Ä.)

Port-Blocking: Ports sind Anschlussbuchsen an Netzwerkkomponenten zum Verbinden untereinander oder zum Anschluss von Endgeräten; Port-Blocking bedeutet, dass an bestimmten Ports der Zugang zum Netzwerk blockiert wird

Remote Computer: Rechner, die sich von anderen Rechnern aus fernbedienen lassen

Relay: Weiterleitung von Daten

Server: Anwendung, die nach Anfrage Kontakt mit Client aufnimmt und mit ihm Daten austauscht oder ihm einen Dienst bereitstellt; oft wird Rechner, auf dem Serverprogramm läuft, auch als Server bezeichnet

Spyware: Software, die persönliche Daten eines PC-Benutzers ohne dessen Wissen oder Zustimmung an Dritte sendet

Trojaner: Programm, das als nützliche Anwendung getarnt ist, im Hintergrund aber ohne das Wissen des Anwenders eine andere meist schädliche Funktion erfüllt

Update: Aktualisierung einer Software, die Programmängel korrigiert oder Programmverbesserungen enthält

Client und verringert dadurch die Anzahl an Benachrichtigungen erheblich, die zwischen Client und Server versendet werden. Somit lassen sich Computer von einer einzigen Konsole aus verwalten. Message Relays, die dafür sorgen, dass Netzwerkcomputer als Relays zur Konsole agieren, entlasten den Server zusätzlich. So ist es möglich, mehrere Tausend Computer von einer einzigen Konsole aus zu verwalten.

Verwaltung gespeicherter Informationen. Das Sicherheitskonzept bietet verschiedene Datenbank-Lösungen, so dass große Unternehmen die Informationen effektiv verwalten können. Das System kann standardmäßig mit MSDE (Microsoft SQL Server Desktop Engine) integriert werden. Es lässt sich aber auch ein SQL-Server verwenden, um die erweiterten Funktionen und Skalierbarkeit für große Netzwerke zu nutzen.

Integrierter Bedrohungs-Report. Integrierte, netzwerkweite Reports bei Bedarf sind Voraussetzung zur Aufrechterhaltung des Netzwerkschutzes. Sie geben einen Überblick über Infektionen und den Schutzstatus des Netzwerks.

Die Konsole bietet kundenspezifische, integrierte Diagramme, Grafiken und Reports, die beispielsweise nach Bedrohung, Ort und Zeit aufgeschlüsselt sind.

Zusammenfassung

Die Verwaltung von Sicherheits-Software und die Durchsetzung von Richtlinien in großen und komplexen Netzwerken ist unerlässlich, doch sehr kostenspielig. Viele Produkte, die Lösungen für diese Probleme versprechen, steigern die Komplexität oft nur, da sich Administratoren mit einer Unmenge komplizierter Funktionen herumschlagen müssen, die sie größtenteils nie verwenden. Die hier vorgestellte Sicherheitslösung wurde speziell dazu entwickelt, die Komplexität der Verwaltung des Schutzes von Desktops, Laptops und Servern im Netzwerk zu verringern und bietet leistungsstarke, auf Richtlinien basierende Verwaltungsmöglichkeiten, so dass sich der Schutz des Netzwerks leicht überwachen und Zeitaufwand, Ressourcen sowie auch Kosten stark reduzieren lassen.

Neue Rauchwarnmelder

Die Aufklärungskampagne „Rauchmelder retten Leben!“ und die gesetzliche Rauchwarnmelderpflicht in derzeit sechs Bundesländern (Tafel 1) haben zahlreichen Endverbrauchern die tödliche Gefahr einer Rauchgasvergiftung bewusst gemacht. Und viele wissen auch, dass in diesem sicherheitsrelevanten Bereich No-Name-Produkte fehl am Platze sind. Sie setzen auf solide Markengeräte und die fachmännische Beratung durch das Elektrohandwerk.

Sortiment erweitert

Zahlreiche namhafte Hersteller der Branche haben sich auf den wachsenden Markt der Rauchwarnmelder eingestellt und ihr Produktsortiment ergänzt oder ausgebaut. So wurde beispielsweise erst kürzlich die Familie der Argus-Rauchmelder von Merten erweitert (Bild 1). Die fünf neuen VdS-erkannten Modelle erfüllen die Vorgaben der EN 14604 für die Installation nach DIN 14676 [1–3]. Bei allen Geräten erfolgt die Überwachung über das Streulichtprinzip, den so genannten Tyndall-Effekt. Beim Eintreten des Rauchs in die Messkammer erfolgt ein pulsierender Warnton mit ca. 85 db(A). Die korrekte Funktion des Gerätes lässt sich jederzeit durch einen Testknopf kontrollieren, darüber hinaus findet einmal pro Minute eine automatische Selbstkontrolle statt. Eine schwache Batterie zeigen die Melder etwa 30 Tage lang alle 45 Sekunden durch ein akustisches Signal und eine blinkende LED an.

Basismodell

Als Einsteigerversion in der Ausführung „polarweiß“ bietet sich das Modell „Basic“ an. Das Einzelgerät kann einfach an der Decke montiert werden. Es wird mit einer Lieferungsmenge enthaltenen 9-V-Blockbatterie betrieben, deren Lebensdauer rund drei Jahre beträgt. In der Variante „Basic Longlife“ liegt dem Gerät eine 9-V-Lithium-Batterie bei, die die Wartungsintervalle auf etwa zehn Jahre verlängert.

Vernetzte 230-V-Version

Der Rauchwarnmelder vom Typ 230 V in den Farben Polarweiß und Aluminium kann zusätzlich an eine 230-V-Versorgung angeschlossen werden. Er lässt sich über eine freie Ader der 230-V-Installation vernetzen. Damit melden alle Geräte einen Alarm, sobald ein einzelnes Rauch erkannt hat. Dies bietet sich vor allem in größeren Wohnungen an und bei der Absicherung von Flur-

Bundesweiter Rauchmeldertag

„Freitag der 13. wird Ihr Glückstag, wenn Sie heute Rauchmelder installieren.“ Das ist das Motto des diesjährigen Rauchmeldertages am Freitag, dem 13. Juli 2007. Initiator ist das Forum Brandrauchprävention in der Vereinigung zur Förderung des Deutschen Brandschutzes (vfdb).

Multiplikatoren sollen den Tag nutzen, um Verbraucher durch Aktionen oder Informationen an den lebensrettenden Nutzen von Rauchmeldern zu erinnern und zur Installation von Rauchmeldern zu motivieren. In Bundesländern mit einer Gesetzgebung zur Installation von Rauchmeldern in Privathaushalten (mit Nachrüstfristen für Bestandsbauten) sollen gezielt Vermieter und Wohnungsbesitzer aufgeklärt und angesprochen werden.

Das Forum Brandrauchprävention stellt zum diesjährigen „Freitag, dem 13.“ auf der Internetseite www.rri-insiders.de rechtzeitig Informationsmaterial zur Verfügung.

