

Fast vollständiger Schutzschild für die Endgeräte

Mit dem Schutz der Server ist das Netzwerk nicht ausreichend gesichert. Oft sind die Endgeräte, allen voran Mobilcomputer, das eigentliche Einfallstor für Bedrohungen.

VON MARTIN KUPPINGER

Die Sicherheitsbedrohungen nehmen weiter zu. Längst wird das Feld nicht mehr von einzelnen Hackern, sondern von der organisierten Kriminalität dominiert. Und während man die Sicherheit der zentralen Server oft gut im Griff hat, stellen die Endgeräte oft ein erhebliches Sicherheitsrisiko dar. Das gilt sowohl für Angriffe, gerade bei mobilen Endgeräten wie Notebooks, die in unterschiedlichen Netzwerken betrieben werden, als auch für die Datenlecks. Und gerade dieses Thema, also der Verlust von sensiblen Informationen, hat deutlich an Gewicht gewonnen.

Zentrales Endgeräte-Management

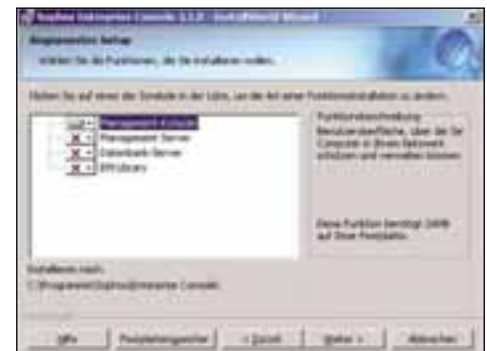
Lösungen für die Endpoint Security versprechen hier Abhilfe. Viele davon werden allerdings dem Anspruch nicht gerecht, weil sie wesentliche Anforderungen nicht erfüllen.

Rein zentrale Lösungen auf Appliance-Basis bieten eben nicht in allen Situationen Schutz für Endgeräte, weil sie nur innerhalb eines Netzwerks greifen können, aber beispielsweise nicht bei Notebooks, die mit einem externen W-Lan verbunden sind. Lösungen, die nur Teilfunktionen der Data Leakage Prevention (DLP) unterstützen oder sich nur auf die Grundfunktionen Virenschutz und lokale Firewall beschränken, reichen ebenfalls nicht aus, um eine umfassende Sicherheit von Endgeräten zu erreichen.

Endpoint Security ist auf die Anforderungen von Unternehmen ausgerichtet. Eine Kernfunktion ist die Fähigkeit zum zentralen Management der Clients über eine Konsole. Die Lösungen bestehen also aus Client- und Server-Komponenten. Die Client-Komponenten, oft als Agents bezeichnet, setzen die zentral konfigurierten Richtlinien um. Über zentrale

Konsolen können die Sicherheitseinstellungen definiert und der Gerätestatus kontrolliert werden.

Swiss IT Magazine vergleicht die Lösungen von McAfee (Total Protection for Endpoint), Novell (Zenworks Endpoint Security Management), Sophos (Endpoint Security and Data Protection) und Symantec (Endpoint Protection).



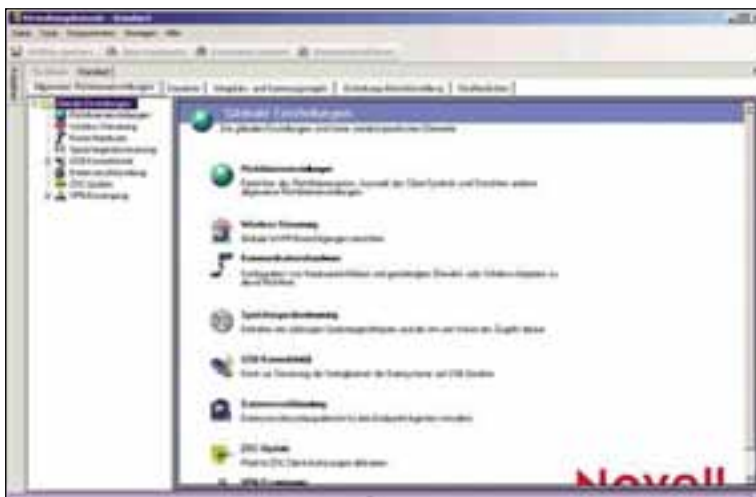
Auch bei Sophos lassen sich die zu installierenden Komponenten selektieren.

Es ist wenig überraschend, dass gerade die etablierten Anbieter von Virenschaltern auch in diesem Markt aktiv sind, aber auch Hersteller, die wie Novell eine Historie im Client-Management haben.

Ein breiter Satz an Funktionen

Endpoint-Security-Lösungen sollen sowohl Angriffe als auch den Verlust von Informationen verhindern, soweit davon die Endgeräte betroffen sind. Das erfordert eine Reihe unterschiedlicher Funktionen. Dazu gehören Anti-Virus- und Anti-Spyware-Filter und lokale Firewalls. Einige Anbieter nutzen dabei Anti-Virus-Lösungen von Drittherstellern. Die getestete Novell-Lösung zum Beispiel enthält zwar eine Personal Firewall, aber keine eigene Anti-Virus-Lösung. Soweit der Virenschutz sowohl in der Konfiguration als auch in der Überwachung eng eingebunden ist, ist dieser Ansatz durchaus valide. Allerdings zeigt sich bei Novell, dass die Integration im Vergleich mit den anderen Produkten nicht so eng ist.

Viele Anbieter führen die Intrusion Detection/Prevention als zusätzliche Funktionalität



Die Verwaltung der Richtlinien bei Novell ZESM erfolgt über eine einfach nutzbare Windows-Schnittstelle.



Symantec unterstützt über Assistenten auch die Einrichtung von Standorten und andere Konfigurationsschritte.

der lokalen Firewall sehen. Funktionen für die Kontrolle von Anwendungen, also beispielsweise der Zugriff auf spezielle DLLs und andere Module, werden aber von allen Herstellern angeboten.

Ein zweiter Funktionsblock von Endpoint-Security-Lösungen ist die W-Lan-Sicherheit. Nur Novell unterstützt bei ZESM explizit solche Richtlinien, wobei sich die Funktionen teilweise auch über die Firewall-Konfiguration und andere Bereiche umsetzen lassen.

Bei den Verschlüsselungsfunktionen bieten Sophos und Novell die umfassendste Unterstützung für vollständige Datenträger sowie einzelne Dateien und USB-Speichergeräte. Sowohl bei Symantec als auch bei McAfee müssen für die Verschlüsselung zusätzliche Produkte lizenziert werden.

Weitergehende Funktionen für die Data Leakage Prevention (DLP) wie die Kontrolle von USB-Speichergeräten und das Kopieren von Dateien werden ebenfalls von allen Herstellern in allerdings unterschiedlichem Umfang unterstützt. Auch hier sind bei McAfee und Symantec teilweise Zusatzprodukte erforderlich.

Am interessantesten ist aber der Bereich der Network Access Control (NAC), also der Überprüfung von Systemen vor dem Zugang zum Netzwerk. Dabei wird kontrolliert, ob die aktuellen Updates für das Betriebssystem und den Virensch scanner installiert sind und andere Anforderungen an den Systemstatus erfüllt sind. NAC ist eine Kernfunktion der Endpoint Security. Sophos und McAfee unterstützen diese Funktion standardmässig. Bei Symantec ist eine zusätzliche Lizenz erforderlich, bei Novell gibt es das Zusatzprodukt Zenworks Network Access Control.

Einige Anbieter offerieren in ihren Endpoint-

Security-Konzepten auch Komponenten für den Schutz von Servern an, darunter Virenschutz für Fileserver oder E-Mail-Server und Spam-Filter. Das sind nützliche Ergänzungen, aber keine zwingenden Komponenten von Endpoint-Security-Lösungen.

Schwächen bei heterogenen Infrastrukturen

Eine Schwachstelle stellt bei allen Herstellern die Unterstützung von heterogenen IT-Infrastrukturen dar. So unterstützen Sophos und Symantec zwar auch einzelne Nicht-Windows-Plattformen, aber nur mit Anti-Virus-Funktionen. Die restliche Funktionalität gibt es dagegen auch bei diesen Anbietern nur für Windows-Systeme. Wer nicht nur mit Windows arbeitet, hat mit den aktuellen Suites also noch ein Problem – umso mehr, als in letzter Zeit beispielsweise auch Mac OS X zu einem immer beliebteren Angriffsziel geworden ist.

Etwas besser sieht es bei mobilen Endgeräten aus, die zumindest teilweise von einigen der Anbieter unterstützt werden. Auch hier

TESTSIEGER: SOPHOS

Von den Produkten im Vergleich bietet Sophos Endpoint Security and Data Protection insgesamt den grössten Funktionsumfang – von den Anti-Virus-Funktionen bis hin zur Network Access Control. Das ist letztlich ausschlaggebend dafür, dass dieses Produkt im Vergleich Vorteile hat. Die Konsole und das Deployment sind gut nutzbar, die Integration mit dem Active Directory ist sinnvoll. Die anderen Anbieter, die näher betrachtet wurden, bieten aber auch leistungsfähige Lösungen – und haben zum überwiegenden Teil den Funktionsumfang in letzter Zeit deutlich ausgebaut. Bei Auswahlentscheidungen macht es durchaus Sinn, sich alle vier Anbieter näher anzuschauen, da der Markt von schneller Innovation geprägt ist.

Konzept, das zunächst definiert werden sollte, bevor man mit dem Rollout beginnt. Die Verteilung der Agents auf die Clients muss ebenfalls geplant werden und kann beispielsweise bei Symantec auch in enger Integration mit den Client-Lifecycle-Management-Lösungen von Altiris erfolgen.

Die meisten Lösungen setzen auch einen installierten Microsoft SQL Server und die Microsoft IIS voraus – das gilt beispielsweise für Novell, McAfee und Symantec, wobei man bei Symantec auch mit einer «Embedded Database» arbeiten kann, die mit dem Produkt geliefert wird und die für mittlere Netzwerke ausreichend ist.

Bedauerlicherweise gab es auch bei fast allen Produkten

einige kleinere Nickligkeiten bei der Konfiguration. Bei Sophos liess sich die Konsole zunächst nicht starten und bei McAfee gab es Schwierigkeiten in der Anbindung der Microsoft-SQL-Server-Datenbank. Gut gefiel bei der Installation vor allem Symantec mit einer Reihe von Assistenten, die den Installations- und Konfigurationsprozess unterstützen.

Die zentralen Konsolen sind dagegen alle ausgereift, wenn auch konzeptuell recht unterschiedlich. Alle Hersteller setzen auf die Definition von Richtlinien und bieten leistungsfähige Reporting-Funktionen an. Hier bleiben wenige Wünsche offen. Bis auf Novell gibt es bei allen Herstellern auch zusätzliche Online-Dienste oder Managed Services im Angebot.

Leider bietet keiner der Anbieter eine volle Integration mit den Windows-Gruppenrichtlinien, die ja wichtige Funktionen für die Endgerätesicherheit unterstützen. Immerhin finden

„Aspectra ist unsere Versicherung, was die Sicherheit unserer IT-Systeme betrifft.“

Philipp Meier, Director, Sales & Business Development
BST Banking Software Training AG

Hosting - Monitoring - Business Continuity www.aspectra.ch

gibt es aber doch erhebliche Einschränkungen sowohl bezüglich der unterstützten Geräte als auch der Funktionalität, so dass man in den meisten Fällen derzeit mit spezialisierten Lösungen für das Management von mobilen Endgeräten noch besser bedient ist.

Installation und Management

Alle betrachteten Lösungen arbeiten im Client/Server-Konzept, also mit einem zentralisierten Management und dezentralen Agents. Und alle sind auf mittlere und grössere Unternehmen ausgelegt, wie oft schon bei der Anforderung von Evaluationsversionen deutlich gemacht wird, wo mehrere Hersteller für Kleinunternehmen auf ihre Standardlösungen für Virenschutz und lokale Firewall verweisen.

Entsprechend setzen alle Produkte auch eine genaue Planung voraus. So gibt es beispielsweise bei Symantec ein spezielles Site-

sich bei einigen Anbietern wie Novell und Sophos Schnittstellen zum Active Directory. Die bessere Integration mit Windows-Standardfunktionen – auch die Network Access Control wäre hier zu nennen – ist aber sicherlich ein Bereich, in dem es für alle Anbieter noch einiges an Verbesserungspotenzial gibt.

Endpoint Security – ein Muss

Lösungen für Endpoint Security oder Endpoint Protection sind aufgrund der wachsenden Sicherheitsbedrohungen ein Muss. Zentrales Management ist zwingend – und genau das bieten die im Vergleich betrachteten Lösungen.


Allerdings kann man gerade im Windows-Umfeld einiges auch über die Standardlösungen von Microsoft erreichen – die Gruppenrichtlinien bieten hier schon einiges an Funktionalität und NAC-Funktionen werden auch standardmässig unterstützt. Der Funktionsumfang der betrachteten Lösungen ist allerdings einiges breiter.

Das gilt noch mehr mit Blick auf die Angebote für die Data Leakage Prevention, die sich heute im Markt finden. Im Vergleich mit diesen meist isolierten Lösungsansätzen bieten die integrierten Konzepte für die Endpoint Security deutlich mehr. Man sollte auf jeden Fall zuerst

vollständige Endpoint-Security-Lösungen betrachten und diese punktuell um spezielle DLP-Funktionen ergänzen, statt viel Geld in unvollständige DLP-Einzellösungen zu stecken.

Deutlich wird beim Vergleich aber auch, dass noch kein Hersteller eine vollständige Abdeckung bietet. Gerade bei der Integration mit Windows-Standardfunktionen und der Unterstützung heterogener Infrastrukturen gibt es doch noch erhebliche Schwächen. Dennoch bieten alle Lösungen das Potential, die Sicherheit in Netzwerken bei überschaubarem administrativem Aufwand signifikant zu erhöhen. ■

ENDPOINT-SECURITY-LÖSUNGEN				
ANBIETER	MCAFFEE	SOPHOS	SYMANTEC	NOVELL
Produkt	McAfee Total Protection for Endpoint	Sophos Endpoint Security and Data Protection 8.0	Symantec Endpoint Protection 11.0.4	ZENworks Endpoint Security Management
URL	www.mcafee.com/de/	www.sophos.de	www.symantec.com	www.novell.com
Features				
Lösungstyp	Client/Server	Client/Server, Standalone	Client/Server	Client/Server
Basis-Betriebssystem	1, 2, 3, 4	1, 2, 3, 4, 10, 11, 12	2, 3, 4	2, 3, 4
Personal Firewall/Anti-Virus	■	■	■	3rd Party
Wireless Security	□	■	■	■
Intrusion Detection/Prevention	■	■	■	■
File/Folder/Disk Encryption	optional via Total Protection for Data	1, 2, 3	optional via Symantec Endpoint Encryption, 3	1, 2, 3
Data Leakage Prevention	□	■	optional via Vontu Data Loss Prevention	■
Application Control/Whitelisting	■	■	■	■
Device Control/USB-Security	optional via Total Protection for Data	■	■	■
Network Access Control	■	■	optional	optional via ZENworks Network Access Control
Server				
Betriebssystem/Datenbank	5, 6, 7, 8, 9/-	6, 7, 8/1	7, 8/1, 3	6, 7/1
Clustering/Failover	OS-Cluster	DBMS-Cluster	■	OS-Cluster
Management				
Authentifizierung	lokal	Win/AD, LDAP	LDAP, RSA SecurID, lokal	LDAP, AD, eDirectory
Nutzt Win-Gruppenrichtlinien	□	□	□	□
Logging/Alarming				
Logging	zentral	dezentral, zentral	zentral, dezentral, Syslog	zentral
Alarming	1, 2	1, 2, 6	2, 7	1, 2, 8
Preis/Lizenzierung				
Preis pro User/Computer, Maintenance p.a.	116 €, 1 Jahr Gold Support inklusive	auf Anfrage	Ca. 44 €/Gerät bei 100 Lizenzen, ca. 31,50 € bei 1000 Lizenzen	80 € pro Benutzer, einschliesslich 1 Jahr Maintenance
Lizenzierung	pro Benutzer, ab 11 Benutzern	pro Gerät, ab 5 Geräten	pro Gerät, Staffelpreise	pro Benutzer, Staffelpreise
Wertung				
Funktionalität:	★★★★★	★★★★★	★★★★★	★★★★★
Bedienung:	★★★★★	★★★★★	★★★★★	★★★★★
Preis/Leistung:	★★★★★	★★★★★	★★★★★	★★★★★
Gesamt	★★★★★	★★★★★	★★★★★	★★★★★



■ = ja, □ = nein; k.A. = keine Angaben; Unterstützte Betriebssysteme: 1) Windows NT Workstation, 2) Windows 2000, 3) Windows XP, 4) Windows Vista, 5) Windows NT Server 6) Windows 2000 Server, 7) Windows Server 2003, 8) Windows Server 2007, 9) Netware, 10) Mac OS X, 11) Linux, 12) Windows 98, 13) eigenes OS; Unterstützte Datenbanken: 1) Microsoft SQL Server, 2) MySQL, 3) embedded; Alarming: 1) SNMP, 2) E-Mail, 3) Workflow, 4) API, 5) Ticketing, 6) Windows Eventlog, 7) ausführbare Datei/Scripts, 8) SMS; File/Folder/Disk Encryption: 1) File, 2) Folder, 3) Disk, 4) nur USB

Quelle: Swiss IT Magazine