BitDefender Sicherheitsprogramm

Kaskadierte Sicherheit in Unternehmens-Netzwerken

bitdefender

Inhalt

Schützen Sie Ihr Unternehmen mit den Sicherheitstools von BitDefender

Die rasante Verbreitung von LANs und WANs innerhalb der letzten zwei Jahrzehnte hat den Umstieg von Einzelarbeitsplätzen hin zum vernetzten Arbeiten wesentlich erleichtert. Diese Entwicklung ermöglicht es heutzutage sowohl Privatanwendern als auch Unternehmen, ihr Tagesgeschäft schneller und effizienter als je zuvor zu erledigen. Darüber hinaus bietet die globale Vernetzung eine Vielfalt an neuen Möglichkeiten der Interaktion und Kollaboration.

So sind, beispielsweise durch die zunehmende Verbreitung von Hochgeschwindigkeits-Internetzugängen innerhalb der letzten zehn Jahre, zahlreiche neue Kommunikationsformen entstanden, die sich auch im Business-Bereich etabliert haben. Dazu gehören E-Mail, High-speed-Dateitransfer, Instant- und Mobile-Messaging und Online-Webkonferenzen etc.

Diese innovativen Technologien und ihre rasante Weiterentwicklung sind Wegbereiter für eine neue Form der Interaktion zwischen Individuen; insbesondere Unternehmen bieten sie neue Möglichkeiten in der Kundenansprache und -information.

Netzwerke, ob kabelgebunden oder wireless, schaffen aber nicht nur virtuelle Umgebungen, die Menschen mit gemeinsamen Interessen und Aktivitäten auf produktive Art und Weise verbinden – unabhängig davon, ob sie im selben Gebäude sitzen oder über mehrere Kontinente verteilt sind. Aufgrund ihrer Struktur und der Grundlagen, nach denen sie konzipiert wurden, drohen ihnen auch jede Menge Gefahren und Risiken.

Den Feind erkennen – das aktuelle Bedrohungs-Szenario

Cyberkriminelle lassen nichts unversucht, um Schwachstellen von Benutzern und Computersystemen auszunutzen. Zu diesem Zweck setzen sie die unterschiedlichsten verhaltens- und technologiebasierenden Taktiken und Strategien ein. Das gegenwärtige Bedrohungs-Szenario, welches sich aus den straff organisierten und rein profitgetriebenen Aktivitäten der Gauner zeichnen lässt, erschreckt:

- Gut ein Fünftel der Weltbevölkerung, die mit dem Internet verbunden ist, kämpft Tag für Tag gegen ca. 2.000 neue oder mutierte Viren.
- Jeder Einzelne ist Monat für Monat in Gefahr, das Opfer eines von mehr als 50.000 Phishing-Versuchen zu werden.
- Weit mehr als 1.000.000 gekaperte Computer, sogenannte Zombies, verbreiten das ganze Jahr hindurch Bots, Rootkits und andere Malware.

Diese sogenannten E-Threats sind maßgeblich verantwortlich für einen erheblichen Anstieg der:

- *Infrastrukturkosten* – Dazu gehört das Netzwerkmanagement von Internet Service-Providern und anderen Unternehmen sowie die Bereitstellung, Implementierung und Aktualisierung von Antimalware-Lösungen (für Desktop-, Server- und Internetlevel), der Technische Support usw.
- *Produktivitätseinbußen* – generiert durch lahmende Netzwerkverbindungen als Folge von nutzlosem Traffic; generiert durch digitale Schädlinge, eingeschränkte Verarbeitungsmöglichkeiten von E-Mails und schwindende Speicherkapazitäten; erhöhter Zeitaufwand für das Aussortieren und Löschen von unerwünschten Nachrichten, ressourcenvernichtende Kollateralschäden durch das zwingend notwendige Erkennen und Entfernen von Malware etc.

Allein im Jahr 2005 mussten Unternehmen weltweit aufgrund von Spam-E-Mails Mehrkosten in Höhe von 50 Milliarden US-Dollar kompensieren[1]. 2007 beliefen sich Schätzungen zufolge die Kosten für diese unerwünschten digitalen Postwurfsendungen auf mehr als rund 198 Milliarden US-Dollar[2].

Vor diesem Hintergrund muss die Netzwerksicherheit in Hinblick auf die folgenden Aspekte entscheidend priorisiert werden:

- Schutz von Vermögenswerten, geistigem Eigentum und sensiblen Daten
- Evaluierung und Verbesserung von Standards und Regularien sowie Risikomanagement und Einhaltung von relevanten EU-Richtlinien, Compliance, wie z. B. Sarbanes-Oxley, Basel II und andere[3]
- Absicherung von Investitionen und Optimierung der Gesamtbetriebskosten
- Reduzierung der TCO (Total Cost of Ownership) für eingesetzte Sicherheitslösungen
- Steigerung der Produktivität im Netzwerk und ein erhöhter ROI

Risiken und Gefahren entschärfen – mit der richtigen Abwehrtechnologie

BitDefender hat sich zum Ziel gesetzt, Unternehmen und Einrichtungen weltweit zu schützen. Zu diesem Zweck wurde eine ganze Reihe innovativer Sicherheitstechnologien entwickelt, die zudem ständig optimiert werden. Alle Sicherheitslösungen, die mittlerweile Millionen von unterschiedlichen Plattformen, Systemen, Daten und Anwendern auf der ganzen Welt sichern, sind anerkanntermaßen effizient und bieten zusätzlich einen echten Mehrwert in Form von:

- *Flexible Sicherheitslösungen* – einfache Integration und Kompatibilität zu den wichtigsten Softwareprodukten und Anwendungen eines Unternehmens
- *Zuverlässiger Schutz gegen Malware* – sichere Erkennung, genaue Identifikation und Desinfektion von Viren, Würmern, Trojanern, Adware, Spyware, Bots usw.
- *Effiziente Antispam-Technologie* – mehrere, aufeinander abgestimmte Tools für den E-Mail-Schutz – zusammengefasst in einem intelligenten und lernfähigen Modul
- *Dedizierte Lösungen* – Echtzeitschutz für Server, Desktops, Laptops und Mobile Computing
- *Schnelle Reaktion* auf neue digitale Bedrohungen – Updates und Virensignaturen innerhalb von zwei und vier Stunden
- *Proaktive Sicherheit* – zuverlässiger Schutz auch vor völlig neuen, unbekannten Angriffen

---

[1] David Ferris, Richi Jennings, Chris Williams, „The Global Economic Impact of Spam, 2005. Bericht Nr. 409. Ferris Analyzer Information Service“, veröffentlicht am 24. Februar 2005, auf Ferris Research, http://www.ferris.com/2005/02/24/the-global-economic-impact-of-spam-2005/.

[2] Laut Robert Jaques wird „Spam Unternehmen dieses Jahr Kosten in Höhe von 20,5 Milliarden US-Doller verursachen“, veröffentlicht am 10. Juni 2003 unter Incisive Media's www.vnunet.com, http://www.vnunet.com/vnunet/news/2122506/spam-cost-business-5bn.

[3] Der Aktionsplan für Finanzdienstleistungen der Europäischen Union (FSAP), die Jahresabschlussrichtlinie (Vierte gesellschaftliche Richtlinie; 78/660/EWG), die 7. Richtlinie über den konsolidierten Abschluss (83/349/EWG), die Prüferbefähigungsrichtlinie (Achte gesellschaftliche Richtlinie 1984 (84/253/EWG) und 2006 (2006/43/EC), die Richtlinie Consolidated Admissions and Reporting (CARD) (2001/34/EG), die Richtlinie zur Transparenz (2004/109/EG), die Richtlinie zur Koordinierung der Vorschriften betreffend Insider-Geschäfte (1989/592/EG) & die Richtlinie über Marktmissbrauch (2003/6/EG).

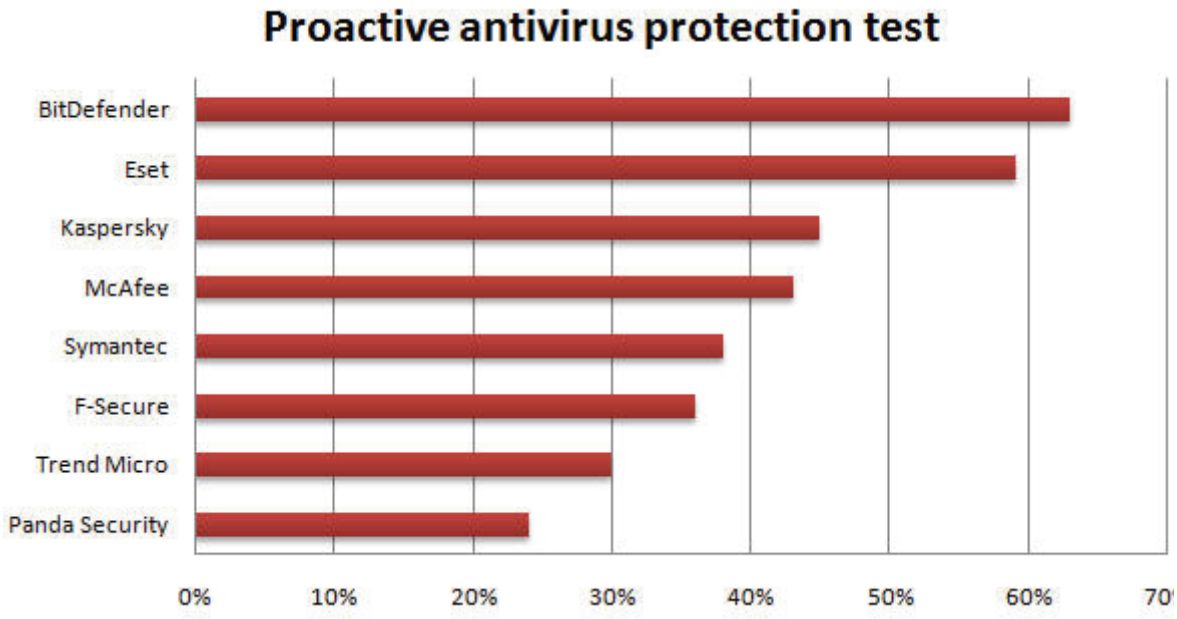
BitDefender erforscht, analysiert und verfolgt kontinuierlich die jeweils aktuellsten Methoden, nach denen E-Threats entwickelt werden. Auf dieser Basis entwickelt BitDefender ständig neue Filter, um potenzielle Angriffe abzublocken und den gestiegenen Sicherheitsbedürfnissen der Anwender gerecht zu werden.

Weitere Schlüsselelemente im Kampf gegen digitale Schädlinge ist die Weiterentwicklung der proaktiven und verhaltensbasierenden Erkennung und damit eine Verkürzung der Reaktionszeiten auf neue, bislang unbekannte Bedrohungen.

Die Anzahl der E-Threats ist in den letzten Jahren exponentiell angestiegen. Dieser Trend wird sich in Zukunft weiter verschärfen. Daher gehört zu den Hauptaufgaben der Virenjäger die Weiterentwicklung und Implementierung von automatischen E-Threat-Analyseprozessen. Beispielsweise hat BitDefender innovative Eigenentwicklungen wie B-HAVE, Active Virus Control (AVC) und NeuNet in seine Antimalware- und Antispam-Lösungen implementiert. Denn im Vergleich zu dem Desinfektionsaufwand eines bereits infizierten Systems oder Netzwerks ist die Prävention erheblich einfacher und spart so Zeit und Kosten.

B-HAVE und AVC sind dynamische, heuristische Scanner. Sie verbessern die aktuelle, signaturbasierende Sicherheitstechnologie und sorgen für einen proaktiven Schutz.

NeuNet ist ein intelligenter Spamfilter. Er verwendet ein neurales Netzwerk, das auf eine Vielzahl von digitalen Massenwurfsendungen (Spam-E-Mails) trainiert ist. Neue oder mutierte Arten von Malware können anhand ihrer Struktur oder ihres Verhaltensmusters aufgespürt und vernichtet werden. Eine Liste von bereits bekannten E-Threats ist dazu nicht erforderlich. Die Zeit, die zwischen dem Ausbruch eines neuen digitalen Schädlings und der Verteilung eines Updates aktueller Antimalware-Signaturen vergeht (auch „Gefährdungsfenster“ genannt), konnte dadurch erheblich verringert werden. Die im Januar 2008 von Anti-Malware Test Lab durchgeführten, unabhängigen Tests haben bestätigt, dass sich mit der heuristischen Erkennung von B-HAVE 63 Prozent aller E-Threats auch ohne hinterlegte Signaturen aufspüren lassen[4].



[4] Siehe „Testing of proactive antivirus protection: Key results from the proactive antivirus protection test“, veröffentlicht am 14. Januar 2008 in Anti-Malware Test Lab, http://www.anti-malwaretest.com/?q=node/39.

Active Virus Control (AVC), die neueste Entwicklung der BitDefender Labs, ist ein fortschrittlicher heuristischer Scanner. Er wurde speziell dafür entwickelt, die auf einem Computersystem ausgeführten Programme und Anwendungen in Echtzeit zu prüfen. Potenziell gefährliche Prozesse überwacht AVC ab dem Zeitpunkt seines Starts kontinuierlich; verdächtige Aktivitäten werden analysiert und mit bekannten Mustern verglichen. Sobald die Software einen bestimmten Gefahrenschwellenwert registriert, blockt sie die Anwendung und stuft sie als schädlich ein. Die Systemintegrität bleibt dabei gewahrt. In Kombination mit den signaturbasierenden und heuristischen Erkennungsverfahren wird so eine Erkennungsrate von bis zu 99,9 Prozent erreicht.

Spam erfordert aufgrund seiner vielfältigen Ausprägungen und der hohen Geschwindigkeit seines Auftretens besondere Aufmerksamkeit. Die Erkennungsmethoden für Spam müssen sich dabei permanent den veränderlichen Rahmenbedingungen anpassen. Komplexere Spam-Varianten erfordern außerdem intelligentere Scan-Engines. Um besser und schneller auf neue Spam-Wellen zu reagieren, hat BitDefender den leistungsstarken Antispam-Filter NeuNet[5] entwickelt (Abkürzung für „Neurales Netzwerk“). NeuNet wird durch das BitDefender Antispam Lab auf zahlreiche Spam-Mitteilungen vorgeschult. Neue Spamvarianten können so durch einen Vergleich mit bereits analysierten und somit bekannten Spam-Typen zuverlässig erkannt werden. Neu geschulte Versionen werden regelmäßig im Rahmen des regulären Update-Vorgangs der BitDefender-Sicherheitslösungen verteilt.

Strategische Ebenen für eine wirksame Abwehr

BitDefender Business Security kann für die unterschiedlichsten Anforderungsprofile und den optimierten Schutz in mittleren und großen Computernetzwerken maßgeschneidert werden. Zur Minimierung des Administrationsaufwandes sind zahlreiche Funktionen bereits nach der Installation automatisiert, die Verwaltung und Konfiguration erfolgt zentral von einem einzelnen Arbeitsplatzrechner aus. Netzwerkadministratoren können damit auf einfache Art und Weise Sicherheitsrichtlinien implementieren, Protokolle generieren und Benachrichtigungen über Updates und ausgeführte Scanvorgänge abrufen. So erkennt die Business Security Suite, wenn beispielsweise neue Arbeitsplatzrechner an das Netzwerk angeschlossen werden, und installiert die Sicherheitssoftware sofort vollautomatisch.

Um eine bestmögliche Sicherung der verschiedenen Netzwerkebenen zu ermöglichen, sind die einzelnen Komponenten der BitDefender Business Security Solutions exakt aufeinander abgestimmt:

Der Perimeter – der erste Wall

Der Perimeter ist die erste Abwehrlinie und damit gleichzeitig der erste und der letzte Kontaktpunkt für die Sicherheits-Tools, die das Unternehmensnetzwerk schützen bzw. den Übergangspunkt zwischen dem lokalen Netzwerk und dem Internet überwachen.

Der Netzwerkperimeter kann somit auch als Schnittstelle zur Außenwelt interpretiert werden. Ist sie gefährdet, besteht auch für die Unternehmung selbst Gefahr. Bestes Beispiel dafür sind Firmen, die ihre Geschäfte ausschließlich über das Internet abwickeln und ihren Umsatz durch Besucher generieren, die Online-Käufe oder -Transaktionen tätigen. Wird der Schutz des Perimeters durch externe Angriffe durchbrochen, sind auch die Server dahinter in Gefahr und damit schlimmstenfalls Bestellungen und Umsatz.

Die folgenden BitDefender-Lösungen schützen den Netzwerkperimeter:

- BitDefender Security for ISA Servers
- BitDefender Security for Mail Servers
- BitDefender Security Exchange Servers

[5] Eine ausführliche Beschreibung des NeuNet-Filters finden Sie im Whitepaper „BitDefender Antispam NeuNet“ unter BitDefender, http://www.bitdefender.com/files/Main/file/BitDefender_Antispam_NeuNet.pdf.

Das Netzwerk – Verteidigung von innen

Die Netzwerkebene repräsentiert das LAN und/oder WAN. In der Regel bestehen Netzwerke aus Clients und Servern, Desktopcomputern und Laptops sowie komplexen Remote-Verbindungen für Telecommuter, Teleworker und andere mobile Anwender.

Die Sicherheit auf Netzwerkebene ist von entscheidender Bedeutung – besonders im Hinblick auf mögliche Produktivitätseinbußen und die Kosten für die Infrastruktur. Ohne die richtige Abwehrstrategie ist das gesamte Netzwerk in Gefahr, sobald ein einzelner Rechner kompromittiert ist.

Die folgenden BitDefender-Lösungen sorgen für Sicherheit auf Netzwerkebene:

- BitDefender Management Server
- BitDefender Security for File Servers
- BitDefender Security for Samba Shares

Die Clients – Schutz der Endpoints

Im Gegensatz zu Servern, die im Hinblick auf Sicherheits- und Abwehrstrategien besonders im Fokus der Netzwerkadministratoren stehen, wird die Sicherheit der Clients oftmals vernachlässigt. Dabei ist die Anzahl der Clients in der Regel erheblich größer, was wiederum ihre Wartung um ein Vielfaches aufwendiger macht. Aufgrund ihrer Inhomogenität mutieren selbst Netzwerke kleinerer Unternehmen schnell zu einer sehr komplexen und damit schwer administrierbaren Infrastruktur.

Client-Computer bilden technisch gesehen das Einfallstor zu den unterschiedlichsten Arten von sensitiven Unternehmensinformationen und sensiblen Daten, die auf den Servern gehostet werden. Normalerweise können diese Inhalte nur über die angeschlossenen Arbeitsstationen abgerufen werden. Denn es ist fast unmöglich, dass ein Angreifer eine mobile Festplatte oder einen USB-Stick direkt an einen Server anschließt, um Daten zu stehlen. Viel wahrscheinlicher ist dagegen, dass ein Zugriff auf die Serverdaten über einen ungeschützten Client-Rechner erfolgt und die Daten auf ein anderes Trägermedium kopiert werden. Alle Sicherheitsbestimmungen und Schutzrichtlinien werden damit auf einen Schlag außer Kraft gesetzt.

Die folgenden BitDefender-Lösungen sorgen für die Sicherheit der Arbeitsplatzrechner:

- BitDefender Client Security
- BitDefender for Unices

Anwendungen und Daten – lückenlose Software

Unzureichend geschützte Anwendungen bergen ein hohes Gefahrenpotenzial, denn sie ermöglichen den einfachen Zugang zu vertraulichen Daten und Informationen. Ein weiteres Risiko stellen Anwendungen dar, die für einen einfachen externen Zugriff via Internet, z.B. durch Kunden oder Außendienstmitarbeiter, konfiguriert sind.

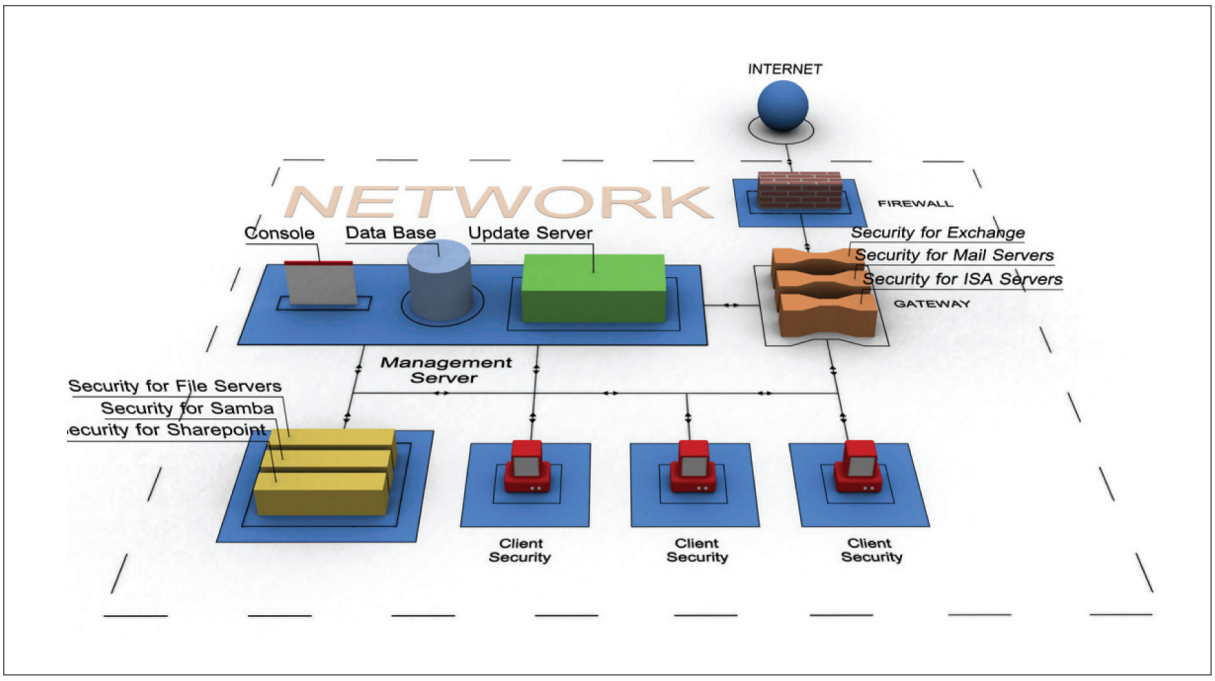
Vertrauliche Daten und sensitive Informationen wie Kundendaten, Konstruktions-, Marketing- und Finanzpläne müssen unbedingt vor unbefugtem Zugriff geschützt werden. Gelingt dies nicht, ist die gesamte Unternehmung in Gefahr. Daher müssen diese Daten in sämtlichen Sicherheitsstrategien entsprechend berücksichtigt werden. Fehlt beispielsweise ein restriktives Zugangsrichtlinien-Management, ist der Weg frei für Datendiebstahl und Industriespionage.

Die folgenden BitDefender-Lösungen sorgen für die Sicherheit von Anwendungen und Daten:

- BitDefender Security for File Servers

- BitDefender Security for Exchange Servers
- BitDefender Security for SharePoint Server
- BitDefender Security for Samba Shares

Die folgende Darstellung zeigt die verschiedenen Komponenten, die das Business Security-Paket umfassen kann:



Hauptkomponenten der BitDefender Business Security

Security for ISA Servers

BitDefender Security for ISA Servers bietet einen Antivirus- und Antispyware-Schutz für den Datenverkehr im Web, einschließlich eines Schutzes für eingehende Daten per E-Mail. BitDefender Security for ISA Servers arbeitet mit Microsoft ISA-Servern zusammen. Mithilfe zweier Anwendungsfilter (ISAPI) gewährleistet die Software so einen Antivirus- und Antispyware-Schutz für HTTP, FTP und FTP via HTTP-Datenverkehr.

BitDefender Security for ISA Servers schützt vor Malware aus dem Internet, indem sie den HTPP- und FTP-Datenverkehr, sofern er gefährliche aktive Codes enthält, filtert und blockiert. Außerdem schützt die Software Arrays, die mit der Microsoft ISA Server Enterprise Edition ausgeführt werden. Gefährliche oder eingeschränkte Dateien isoliert die Lösung zudem in einer Quarantänezone, solange bis entsprechende Maßnahmen durchgeführt werden.

BitDefender Security for ISA Servers verhindert das Risiko von Browser-Blockaden und Timeouts, die durch umfangreiche Datei-Downloads entstehen können. Die angeforderten Daten werden portionsweise während des Herunterladens gescannt und sukzessive an den Browser gesendet. Die Anwendung lässt sich außerdem in BitDefender Security for Mail Servers integrieren, um den SMTP-Datenverkehr vor Viren und Spam zu schützen.

Security for Mail Servers

BitDefender Security for Mail Servers für Unix- und Windows-basierende Plattformen kombiniert proaktive Antivirus-, Antispam- und Antiphishing-Technologien mit Inhalts- und Anhangfilterung, um einen sicheren E-Mail-Verkehr für Firmen und Service-Anbieter bereitzustellen. Das Produkt ist mit den meisten bestehenden E-Mail-Programmen kompatibel und bietet Unternehmensnetzwerken und Service-Providern einen sicheren Schutz gegen aktuelle Malware und Angriffe auf wichtige und vertrauliche Daten.

BitDefender Security for Mail Servers bietet einen Antiphishing-Schutz, indem gefälschte Nachrichten, die das Ziel verfolgen, an vertrauliche Daten des Empfängers zu gelangen, im Voraus entdeckt werden.

Die Lösung beinhaltet spezielle Agents für die automatische Integration mit vielen der bevorzugten E-Mail-Transfer-Agents, wie z.B. Sendmail (milter), Postfix, Courier, qmail und CommuniGate Pro. Ebenso ist der Einsatz als mehrschichtiger Mail Server Proxy möglich, um über Schnittstellen den Datenverkehr, der zu verschiedenen Mail-Servern geleitet wird, zu filtern.

Durch den optimierten Scanprozess wird die Geschwindigkeit des E-Mail-Verkehrs gesteigert und die Auslastung des Servers reduziert. Dadurch erhöht sich die Produktivität des Unternehmens, und dem Verlust von vertraulichen Informationen wird vorgebeugt.

BitDefender Security for Mail Servers bietet ein äußerst effizientes mehrschichtiges Antispam-Schutzsystem. Es sorgt dafür, dass der E-Mail-Datenverkehr durch die genaue Klassifizierung von Nachrichten als Spam, Phishing oder legitime E-Mails verringert wird.

Unerwünschte E-Mails blockiert die Lösung durch mehrere Verbindungsfilter wie IP-Liste und Sender Black List, einem lernfähigen Bayesschen-Filter sowie dem proaktiven NeuNet-Filter. Zusätzlich schützt der Directory-Harvesting-Filter vor Versuchen, gültige E-Mail-Adressen vom E-Mail-Server zu entwenden.

BitDefender Security for Mail Servers ermöglicht außerdem eine separate Behandlung von Riskware, also Anwendungen, die zwar eine potenzielle Bedrohung darstellen, jedoch von bestimmten Nutzergruppen benötigt werden.

Security for Exchange

BitDefender Security for Exchange beinhaltet Antivirus, Antispyware, Antispam, Antiphishing sowie eine Anhang- und Inhaltsfilterung und integriert sich nahtlos in den MS Exchange Server für eine virenfreie Messaging-Umgebung. Es schützt Exchange Server gegen die neueste und raffinierteste Malware und gegen Zugriffsversuche auf vertrauliche und wertvolle Daten.

Management Server

Neue Arbeitsplatzrechner werden automatisch erkannt, mit dem Business Client versehen und den Sicherheitsbestimmungen des Netzwerkes unter Verwendung von vorkonfigurierten Sicherheitsrichtlinien, die bis zur Gruppenebene konfiguriert werden können, angepasst.

Management Server aktiviert außerdem Windows Management Instrumentation(WMI)-Scripting auf Gruppen von Netzwerk-Arbeitsplatzrechnern. Zur Zentralisierung und Minimierung des Administrationsaufwands stehen umfangreiche Planungstools zur Verfügung, auf deren Basis IT-Administratoren sowohl das Netzwerk-Audit (Erfassen von Hard- und Systeminformationen von Arbeitsplatzrechnern) als auch administrative Tätigkeiten per Remote-Zugriff durchführen können.

Management Server sorgt mit Hilfe von zentralen Security Dashboards, ausführlichen Berichtsfunktionen und dem Netzwerk-Auditing für unternehmensweite Netzwerktransparenz. Das Dashboard überwacht den Netzwerkstatus und meldet wichtige Sicherheitsinformationen ebenso wie Schwachstellen. Es wird somit zum zentralen Informationspunkt, um tiefer in die Systemadministration und -konfiguration einzusteigen.

Mit dem erweiterten Berichtstool können Administratoren Statistiken zu Netzwerkproblemen, Updates, Installationen usw. generieren. Dafür stehen wahlweise fertige Vorlagen oder benutzerdefinierte Berichte auf der Basis von Crystal Reports zur Verfügung.

Die oben genannten erwähnten WMI-Administrationsskripts erfassen Hardwaredaten und Systeminformationen über Arbeitsplatzrechner, Hardware-Eigenschaften, Startup-Programme, installierte Software, Hot-Fixes sowie Service-Packs usw.

Security for File Servers

BitDefender Security for File Servers ist eine Lösung, die speziell auf Windows-basierende Server zugeschnitten ist. Sie ist einfach zu installieren und zu konfigurieren und schützt den Datenverkehr proaktiv gegen Viren, Spyware und Rootkits. Gleichzeitig wird der Verwaltungsaufwand für eine Server-Software-Lösung minimiert.

Security for File Servers trägt zur Produktivitätssteigerung bei, indem bei allen Sitzungen ein „Fingerabdruck“ von jeder geprüften, schreibgeschützten Datei gespeichert wird. Das Attribut „schreibgeschützt“ sorgt dafür, dass die Datei im Verlauf der jeweiligen Sitzung nicht modifiziert oder infiziert werden kann. So wird eine Datenbank mit den in der vergangenen Zeit geprüften Dateien erstellt, die für sicher befunden wurden. Nimmt der Nutzer eine Änderung vor, erfolgt eine erneute Prüfung.

Der Multithread Scan Modus ermöglicht eine parallele Programmausführung. Durch die Verwendung mehrerer Instanzen der BitDefender-Engine wird der Prüfungsvorgang verkürzt und ein schneller Dateizugriff gewährleistet.

Die On-Access-Prüfung bietet einen Echtzeit-Schutz für den File Server. Somit werden sowohl kopierte als auch verwendete Dateien vor dem Zugriff auf dem Server geprüft und gegebenenfalls bereinigt.

Der Multithread Scan Modus ermöglicht eine parallele Programmausführung. Durch die Verwendung mehrerer Instanzen der BitDefender-Engine wird der Prüfungsvorgang verkürzt und ein schneller Dateizugriff gewährleistet.

Administratoren haben die Möglichkeit, die On-Demand(nach Bedarf)-Virenprüfung und -Update-Funktion direkt von der Benutzeroberfläche aus durchzuführen. Ein Warn-Modul informiert sie darüber hinaus über bereits erfolgte Updates, On-Demand-Prüfungen oder aufgespürte Viren.

Security for Samba Shares

BitDefender Security for Samba bietet Antivirus- und Antispam-Schutz für Samba Network Shares. Alle Dateien, auf die ein Zugriff erfolgte, prüft die Lösung auf bekannte und unbekannte Viren. Der Netzwerkanwender ist somit auf der sicheren Seite und auch die Datenschutzrichtlinien im Unternehmen werden eingehalten. Das BitDefender „Open Source vfs-Modul“ ermöglicht die Kompatibilität zu allen Samba-Versionen. Damit ist BitDefender Security for Samba eine der flexibelsten und effektivsten Sicherheitslösungen für Unix-basierende Systeme.

Client Security

BitDefender Client Security ist eine robuste und leicht zu bedienende Sicherheitssoftware für Unternehmensnetzwerke. Sie bietet erstklassigen proaktiven Schutz vor Viren, Spyware, Rootkits, Spam, Phishing und anderer Malware.

BitDefender Client Security erhöht die Produktivität des Unternehmens und verringert die Management-Kosten durch den Einsatz einer zentralen Management-Administration. Diese erlaubt den netzwerkweiten Schutz und die Kontrolle individueller Arbeitsplatzrechner von einem einzigen Punkt aus.

BitDefender Client Security ist eine robuste und benutzerfreundliche Business-Security- und Management-Lösung, die auf zwei Hauptkomponenten basiert:

- Einmal installiert, bietet der Business Client bestmöglichen Schutz gegen Viren, Spyware, Rootkits, Spam, Phishing und andere Malware.
- BitDefender Management Server führt automatische Routineaktivitäten durch, um Netzwerksicherheit zu gewährleisten oder die Administration effizienter zu gestalten. Dabei wird die Einhaltung der Sicherheitsrichtlinien im gesamten Netzwerk gewährleistet. Ergänzend verwaltet und kontrolliert sie den BitDefender Business Client und andere BitDefender Server-Lösungen.

BitDefender for Unices

BitDefender Antivirus-Scanner für Unix ist eine vielseitige Lösung, die speziell für Linux und FreeBSD-Systeme entwickelt wurde. Sie beinhaltet Virus- und Spyware-Scan-Funktionen sowohl für Unix- als auch für Windows-basierende Partitionen.

Die Software zeichnet sich durch ihre Flexibilität aus, da sie die Möglichkeit einer Skript- oder Extension-basierenden Integration von verschiedenen Applikationen wie Dateimanagern oder Mail Clients wie beispielsweise Pine oder Evolution bietet.

Mit der Kompatibilität zu Terminplanern wie etwa Cron wird die Scan- und Update-Automation gesichert. Für Scans stehen eine klassische Kommandozeile oder ein grafisches User Interface (GUI) zu Gunsten einer besseren Integration in Desktop-Umgebungen zur Verfügung. Das GUI wird automatisch zum Systemmenü hinzugefügt. Des Weiteren stehen Open Source Plugins für die drei populären Dateimanager Konqueror (KDE), Nautilus (GNOME) und Thunar (Xfce) bereit. Das Aktionsschema richtet sich nach dem Typ der Scan-Ergebnisse.

Security for SharePoint Servers

BitDefender Security for SharePoint bietet Viren- und Spywareschutz für jeden Microsoft Sharepoint Server. Die Lösung prüft (mit ausgezeichneten Erkennungsraten) in Echtzeit eingehende und ausgehende Dateien in Dokumentenbibliotheken und Listen und verschiebt optional die infizierten Dateien in einen Quarantäneordner. Diese Lösung erlaubt eine sichere Teamzusammenarbeit in Unternehmensnetzwerken, indem infizierten Dateien der Zugriff auf vertrauliches Firmenmaterial verwehrt wird.

Dank seiner fortgeschrittenen und nahtlosen Integration mit der Microsoft-Virus-Scanning- Programmschnittstelle (API) wird eine sekundenschnelle und sichere Zusammenarbeit gewährleistet.

On-Demand-Scans und Updates können durch einen konfigurierbaren Zeitplaner festgelegt werden. Administratoren informiert das System außerdem mittels eines Benachrichtigungsmoduls über die Durchführung von Scan- und Updates.

Rechtlicher Hinweis