BITDEFENDER SECURITY FOR SHAREPOINT

GEMEINSAME BEARBEITUNG VON DOKUMENTEN WIRD POPULÄR

Die gemeinsame Bearbeitung von Dokumenten wird zunehmend zu einem Schlüsselelement für die Steigerung der Produktivität und Effizienz von Unternehmen. Dabei kommen webbasierte Kollaborationstechnologien wie Microsoft® SharePoint® zum Einsatz, die einzelnen Abteilungen die unbegrenzte Erstellung individueller SharePoint-Websites erlauben, um Projektdokumentationen einfach zu erstellen, verfügbar zu machen und zu verwalten. Jede Website ist per Standard-Browser aufrufbar, und SharePoint gestattet eine Versionsprüfung von Dokumenten als Standardprozedur bei der Ein- und Ausgabe.

Über einen Windows SharePoint-Portalserver können Unternehmen individuelle SharePoint-Websites ganz einfach unternehmensweit konsolidieren. Der Portalserver erweitert die Funktionen der Windows SharePoint-Dienste über Verwaltungstools für SharePoint-Websites, die verschiedene Abteilungen zur unternehmensweiten Informationsveröffentlichung befähigen.

SICHERE GEMEINSAME BEARBEITUNG VON DOKUMENTEN

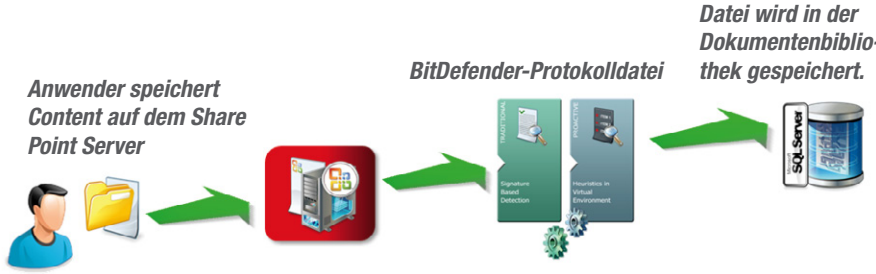
Kollaborationssysteme erlauben Mitarbeitern und Partnern deutliche Steigerungen der Produktivität, sind jedoch zugleich einfache Angriffspunkte für Schad-Software, die die Infrastruktur eines Unternehmens irreversibel schädigen und enorme Aufwendungen an Zeit und Geld zur Folge haben kann. Da Microsoft SharePoint von immer mehr Unternehmen als zentrales Repository verwendet wird, sollte der Schutz vor einem Befall durch Schad-Software aus SharePoint-Ressoucen weit oben auf den IT-Prioritätenlisten rangieren.

Leider sind zahlreiche Netzwerkadministratoren der irrigen Ansicht, ihre Desktop- und Datei-Server-Antivirenlösungen würden auch Viren und Schad-Software im SharePoint-Umfeld aufspüren. Unentdeckt haben Viren das Potenzial, in SQL-basierten Dokumentenbibliotheken über Monate, manchmal sogar Jahre gespeichert zu bleiben. Manche Kollaborationssysteme gestatten den Benutzern sogar, Dokumente abzurufen und zu ändern, ohne sie dabei auf ihrem lokalen System zu speichern. So umgehen die Dokumente die Desktop-Antivirenlösung. Wenn solche Dokumente infiziert sind, können sie Viren und Würmer im gesamten Unternehmensnetzwerk verbreiten.

Viren können über verschiedenste Wege ganz einfach in SharePoint-Sites eingeschleppt werden, beispielsweise wenn infizierte Dateien in der Dokumentenbibliothek oder HTML-Seiten mit schädlichen Makros, integrierten Viren oder Trojanern gespeichert werden, und nicht zuletzt über Infektionen zugeordneter Netzlaufwerke.

SHAREPOINT – SICHER MIT BITDEFENDER

Unternehmen können ihre SharePoint-Installationen vor Angriffen schützen, indem sie die Fähigkeit von BitDefender nutzen, Dokumente auf bestimmte Inhalte hin zu prüfen. So lässt sich die Einhaltung der Sicherheitsrichtlinien des Unternehmens gewährleisten, und sensible Daten sind vor einer Verbreitung außerhalb des Unternehmens sicher.



HAUPTMERKMALE UND -VORTEILE

- Preisgekrönte Virenerkennung, Bereinigung und Quarantäne
- Minimierte Ausfallzeiten des Netzwerks für mehr operative Effizienz
- Weniger Kosten und Aufwand für Ressourcen
- Prüft den Datenverkehr und bietet Echtzeitschutz zur Minimierung des Ausbreitungsrisikos von Malware im Netzwerk
- Prüft und kennzeichnet „Read-Only"-Dateien einmalig pro Sitzung und wiederholt die Prüfung erst bei einer neuen Sitzung, nach Updates oder bei Systeminfektionen
- Erlaubt flexible Planung von On-Demand- oder Immediate-Execution-Prüfungen zur Einschätzung möglicher Infektionen
- Infizierte und verdächtige Dateien werden zur Risikominimierung in Quarantäne verschoben
- Ermöglicht über eine Web-Konfigurationskonsole Remote-Konfigurationen von einem beliebigen Unternehmens-Computer aus
- Unterstützt E-Mail-Archive in den Dateiformaten Dbx, Mbx, Pst, Mime, Mbox, Hqx, Uudecode und Tnef

Bitdefender

ERWEITERTE FUNKTIONEN

- Integration mit dem BitDefender Management Server
- Zentrales Dashboard mit Bereitstellungsstatus und Alarmschwellen
- Angepasste Antivirus-Prüfprofile (hoch, mittel, niedrig, selbsterstellt) für mehr Flexibilität
- Sichere Unterbringung verdächtiger Dateien in Quarantäne mit optionaler Funktion für eine Wiederherstellung am Ursprungsort
- Integration mit der Virenscan-Schnittstelle API von Microsoft zur Optimierung und Beschleunigung des Prüfvorgangs

BITDEFENDER TECHNOLOGIEN

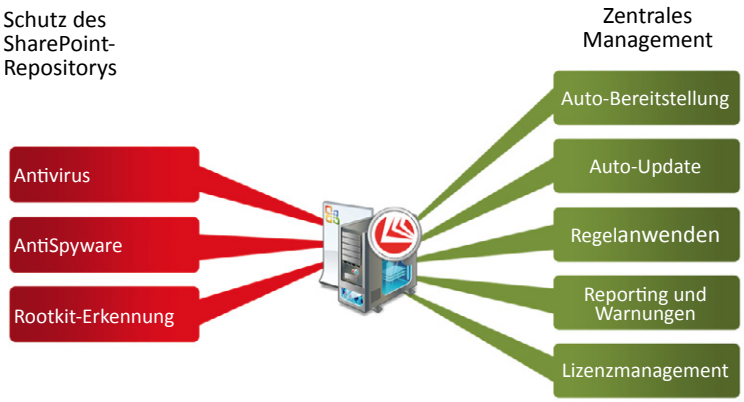
b-have Sämtliche Lösungen von BitDefender beinhalten B-HAVE, eine zum Patent angemeldete Technologie, die das Verhalten potenziell schädlicher Codes in einem virtuellen Computer analysiert, falsch positive Ergebnisse eliminiert und die Erkennungsraten neuer bzw. unbekannter Schad-Software signifikant erhöht.

UMFASSENDER SCHUTZ

BitDefender Security for SharePoint ist nur ein Element einer umfassenden Suite von Lösungen, die durchgängigen Netzwerkschutz vom Gateway bis zum Desktop bieten. Die proaktiven Multi-Plattform-Produkte erkennen und stoppen Viren, Spyware, Adware und Trojaner, die die Integrität Ihres Netzwerks bedrohen.

SYSTEMANFORDERUNGEN

- Windows Server 2003 mit SP1
- Windows Server 2008, Windows Server 2008 R2
- Microsoft SharePoint Portal Server 2003
- Microsoft Office SharePoint Server 2007
- Microsoft Windows SharePoint Services 2.0, 3.0
- Internet Explorer Version 6.0 oder höher



Die Funktionen von BitDefender zur Malware-Erkennung, für Management und Reporting gewährleisten Sicherheit bei der gemeinsamen Nutzung von Dokumenten im Unternehmen.

GRANULARE PRÜFUNGSKONFIGURATION UND -VERWALTUNG

BitDefender Security for SharePoint bietet Prüfmethodologien On-Access, On-Demand und nach Plan, um Schad-Software aufzuspüren und die Integrität des SharePoint-Repository durch Quarantänebereiche zu sichern. Dateien können gereinigt werden, zu Auswertungszwecken in Quarantäne verbleiben, nach erfolgreicher Validierung am Ursprungsort wiederhergestellt oder zur Einschätzung direkt ins BitDefender Antivirus Lab gesendet werden.

Antivirus –Zusätzlich zur signaturbasierten Erkennung bietet BitDefender auch heuristische Erkennungsmethoden, die einen virtuellen „Computer im Computer“ simulieren und hier alle Dateien und Software auf schädliches Verhalten hin überprüfen. Diese Technik liefert weniger falsch positive Ergebnisse und hat deutlich bessere Erkennungsraten bei Zero-Day- und unbekannten Bedrohungen.

Antispyware –BitDefender spürt bekannte Spy- und Adware über Dateiprüfmethoden auf, um Infektionen mit Spyware und damit verbundene Risiken von Datenlecks nach außen zu unterbinden.

Trojaner und Rootkits die dazu bestimmt sind, den Fernzugriff auf Computer-Systeme zu ermöglichen, können von der Prüf-Engine von BitDefender aufgespürt werden. Es kann ein aufwendiger Prozess sein, solche Bedrohungen manuell aufzuspüren und unschädlich zu machen. Oft ist eine komplette Neuinstallation des Systems erforderlich, wenn die Bedrohungen nicht vollständig entfernt wurden.

REPORTING- UND WARNMELDUNGSFUNKTIONEN

Das direkt mit der zentralen Verwaltungsoberfläche von SharePoint integrierte BitDefender Security for SharePoint bietet Reports über Infektionen, Dateien in Quarantäne, desinfizierte Dateien und den Update-Status. E-Mail-Benachrichtigungen können angepasst werden, um Administratoren zu informieren oder Helpdesk-Tickets zu erstellen.

INTEGRATION MIT DER CENTRAL MANAGEMENT-PLATTFORM VON BITDEFENDER

BitDefender Security for SharePoint ermöglicht die Integration mit den Sicherheits-Dashboards des Management Servers und schafft für Administratoren so eine unternehmensweite Transparenz der Netzwerkressourcen und der gesamten Sicherheitslage. Der BitDefender Management Server bietet einen zentralen Punkt für Remote-Installation, -Konfiguration und -Reporting sämtlicher BitDefender-Produkte auf den Clients, Servern und Gateways des Unternehmens. Administratoren werden mit Hilfe des umfassenden Warnmeldungsmoduls über Prüfleistung, Infektionen und Update-Aufgaben informiert.

vb 100 VIRUS virusbtn.com

Bitdefender