Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 81 (2003)

Heft: 10

Artikel: Content security management

Autor: [s. n.]

DOI: https://doi.org/10.5169/seals-876694

Content Security Management

Jedes Unternehmen, das die Potenziale des Internets für seine Geschäftsprozesse ausschöpfen will, sollte sich sämtlicher Risiken bewusst sein, die aus der Internet-Nutzung resultieren. Eine unkontrollierte Internet-Nutzung bringt nicht nur erhebliche Produktivitätseinbussen mit sich, sondern auch massive Sicherheitsrisiken.

Wenn es beim E-Business heute darum geht, Systeme und Prozesse solide abzusichern, gewinnt *Content Security Management* (CSM) an Bedeutung. An eine CSM-Lösung werden heute hohe Anforderungen gestellt. Immer mehr Kunden suchen nach einer integrierten Gesamtlösung, die unterschiedliche Einzellösungen ersetzt.

Content Security Management gewinnt zurzeit stark an Bedeutung, weil der Einsatz einzelner Sicherheitslösungen – Firewalls, Viren-Checker, E-Mail-Management – für Unternehmen längst nicht mehr ausreicht. Viele Gefahren aus dem Internet können mit einem klassischen Firewall-Konzept nicht mehr abgewehrt werden – denn Webinhalte drängen längst durch Firewalls hindurch. Gefragt sind daher umfassende, integrierte und intelligente Konzepte, die der zunehmenden Bedrohung durch Internet-Inhalte Rechnung tragen. CSM umfasst folgende Technologien bzw. Funktionen:

- Internet Access Management – unerwünschte Inhalte per URL-Blocking fernhalten
- Internet Content Filtering – Filterung unerwünschter und gefährlicher Inhalte aus Internet-Seiten
- E-Mail-Management – Regelung des Mail-Verkehrs durch Kontrolle der Inhalte, HTTP und SMTP
- Malicious Code- und Virenschutz für HTTP, SMTP und FTP
- Reporting – statistische Analysen des Internet- und Mail-Verkehrs (HTTP und SMTP)

Neben CSM-Lösungen spielen heute hauptsächlich folgende Themen eine Rolle, wenn es um Internet-Sicherheit geht:

- Hardware-basierte Security-Produkte – (Appliances) wie Firewalls und Internet-Caching-Server
- Verschlüsselung und Krypto-Software – VPI (Virtual Private Network), PKI (Public Key Infrastructure)
- Intrusion Detection (IDS)

Anforderungen an eine CSM-Lösung

Content Security Management ist ein relativ neuer und stark wachsender Markt, den IDC für das Jahr 2005 auf 4,2 Mia. US-$ schätzt und der den Bedarf von Unternehmen und Behörden nach umfassenden Lösungen in diesen Bereichen widerspiegelt. Dabei geht es um die Überprüfung sämtlicher Web- und E-Mail-Inhalte mit dem Ziel, Risiken und Produktivitätseinbussen zu vermeiden, die aus der unsachgemässen Internet-Nutzung resultieren. Ziel von CSM ist es also, den Informationsfluss in ein Unternehmen und aus einem Unternehmen heraus so zu gestalten, dass der gesamte Datenverkehr und damit alle Geschäftsprozesse geschützt und abgesichert werden. Die Anforderungen, die an eine brauchbare und praxisorientierte CSM-Lösung heute gestellt werden, lassen sich wie folgt veranschaulichen:

Vollständigkeit der Lösung und Integration der Komponenten

Kunden suchen eine Paket-Lösung, die alle CSM-Themen abdeckt und alle damit verbundenen Sicherheitsrisiken in den Griff bekommt. Niemand möchte ein Konglomerat unterschiedlicher Einzellösungen, die alle einzeln installiert, integriert und mit teilweise redundant gehaltenen Informationen verwaltet werden müssen. Überdies besitzen viele Insellösungen oft keine standardisierten

Schnittstellen. Das alles kostet nicht nur Zeit und Geld. Einzellösungen sind auch fehleranfällig und können selbst zu einem Sicherheitsproblem werden, wenn beispielsweise vergessen wird, den Remote-Access-Zugang eines ausgeschiedenen Mitarbeiters zu sperren.

Nutzerfreundlichkeit durch zentrale Administration

Zur Reduzierung des Verwaltungsaufwands ist ein einziger Administrationspunkt (Single Point of Administration) sinnvoll, von dem aus die unterschiedlichen CSM-Funktionen zentral verwaltet werden können – Filtereinstellungen, Benutzerverwaltung, Reporting und Logging.

Ein zentraler Administrationspunkt, der auch das zentrale Umsetzen der unternehmensinternen Sicherheitsrichtlinien (Policy) erheblich erleichtert, sollte zudem «remote» und per Web-Interface administrierbar sein – von überall im Unternehmensnetz oder sogar von ausserhalb.

Hohe Skalierbarkeit

Von professionellen Lösungen wird heute erwartet, dass sie auch in Netzen mit weit über 100 000 Nutzern – auch in Spitzenzeiten der Internet-Nutzung – nichts von ihrer Funktionalität einbüssen. So muss eine skalierbare Lösung auch in komplexen heterogenen Netzen unentwegt ihre Dienste verrichten – und zwar ohne Einbusse der Performance, wenn die Internet-Nutzung weit über das übliche Mass hinaus zunimmt. Auch mit dem schnellen Wachsen einer Unternehmens-Infrastruktur sollte eine CSM-Lösung Schritt halten können.

Kompatibilität zu vorhandenen Systemumgebungen

Brauchbare CSM-Lösungen sollten sich reibungslos in die unterschiedlichen IT-Umgebungen einfügen. Daher sollten CSM-Lösungen mit unterschiedlichen Server-Betriebssystemen genauso zurechtkommen wie mit Schnittstellen zu gängigen Firewalls oder Internet-Caching-Lösungen. Auch wollen Kunden gerne vorhandene Autorisierungs- und Authentifizierungs-Methoden nutzen und für CSM keine zusätzliche Datenbasis installieren und pflegen. Die Integrierbarkeit und Offenheit einer CSM-Lösung garantiert überdies, dass getätigte Investitionen nicht in Frage gestellt werden.

Qualität, Aktualität und Support

Die Zeitintervalle, mit denen neue Risiken aus dem Internet auftauchen, werden immer kürzer. In gleichem Masse steigen auch die Anforderungen an eine CSM-Lösung. Ständig neue Bedrohungen, neue Viren, neue unerwünschte URLs oder Media Types – eine leistungsstarke CSM-Lösung muss ständig auf dem Laufenden sein. Kunden erwarten kurze Update-Zyklen und schnelle Reaktionszeiten bei eventuell auftretenden Problemen. Ohne verlässlichen Service und Support können auch Sicherheitslösungen selbst zum Sicherheitsrisiko werden.

Protokollübergreifendes Konzept

Häufig werden unterschiedliche Tools für die Kontrolle von E-Mail- und Web-Verkehr eingesetzt. Die Risiken, die diese Protokolle mit sich bringen, werden aber immer ähnlicher. Ein eindrucksvolles Beispiel dafür war der Nimda-Virus. In erster Linie über E-Mail verteilt, konnte sich Nimda auch durch das Aufrufen einer infizierten Internet-Seite verbreiten. Der Anteil der Sicherheitsrisiken, die über HTTP ins Unternehmen gelangen, nimmt stetig zu, während der Anteil SMTP-bedingter Risiken im Verhältnis dazu – nicht absolut – abnimmt. Eine brauchbare CSM-Lösung sollte ihre Filter- und Sicherheitstechnologien protokollübergreifend zur Anwendung bringen.

Rechtssicherheit

Internet am Arbeitsplatz involviert auch juristische Risiken: strafrechtlich relevante Inhalte, Jugendschutzauflagen und Copyright-Verstösse. Eine CSM-Lösung sollte diese Risiken durch Filtern, Blocken und Sperren der relevanten Inhalte minimieren. Überdies sollte sie bei ihren Logging- und Reporting-Prozessen mit den geltenden Datenschutzrichtlinien und dem Betriebsverfassungsgesetz konform sein. In Unternehmen und Behörden, wo mitunter darauf geachtet wird, dass Mitarbeiter nicht in ihrem Surf-Verhalten ausspioniert werden können, müssen Log-Dateien verschlüsselt werden können (2-Schlüssel-Prinzip). Den einen Schlüssel bekommt dann die Betriebsleitung oder der Systemverwalter, den anderen der Datenschutzbeauftragte oder der Leiter des Personalwesens.

Geringe Gesamtkosten (TCO)

Für viele Unternehmen ist eine bestmögliche Sicherheit zu komplex, zu teuer, zu personal- und zu zeitaufwändig. Gerade hier muss eine CSM-Lösung die Kostenvorteile von Sicherheitsinvestitionen transparent machen. Oft wird nur einmalig in standardisierte Sicherheits-Software investiert, um Kosten zu sparen. Langfristig rächt sich diese Sorglosigkeit.

WebWasher®-Produkte erfüllen diese Anforderungen

Mit den Produkten der Webwasher AG stehen heute leistungsstarke Lösungen für unternehmensweites Content Security Management bereit. Die WebWasher® CSM Suite zum Beispiel ist die weltweit erste Sicherheitslösung auf dem Markt, die den gesamten Web-, E-Mail- und FTP-Datenstrom zentral am Internet-Gateway administriert und filtert. Mittels Internet Access Management, Web-Content-Filterung, Viren- und Malicious-Code-Schutz, E-Mail-Filterung und -Reporting werden alle Sicherheitsrisiken aus dem Internet eliminiert. Darüber hinaus werden sämtliche Inhalte ausgefiltert und geblockt, die für die Internet-Nutzung von Unternehmen und Behörden nicht relevant sind und die Mitarbeiter bei ihrer Arbeit behindern. WebWasher-Produkte kombinieren die Funktionen unterschiedlicher Filter-Technologien zu einem umfassenden und protokollübergreifenden CSM. Ausserdem bieten sie die erforderlichen Schnittstellen zu marktgängigen Firewalls und Cache-Servern und ermöglichen das reibungslose Aufsetzen auf die im Unternehmen vorhandenen Authentizierungsmethoden.

Absolute Sicherheit kann es nicht geben – da sollte sich niemand etwas vormachen. Aber man kann eine ganze Menge für die Sicherheit tun. Content-Security-Management-Lösungen sind ein wichtiger Baustein dazu. [4]

Webwasher AG
Vattmannstrasse 3
D-33100 Paderborn
Tel. + 49 (0)52 51 5 00 54 31
Fax: + 49 (0)52 51 5 00 54 11
E-Mail: berni.loerwald@webwasher.com
Homepage: www.webwasher.com