

PRESSEMELDUNG

ZUR SOFORTIGEN VERÖFFENTLICHUNG

Systems 2007: Neue Sicherheitsstrategie DLP (Data Loss Prevention)

Die sechs wichtigsten Regeln zum Schutz sensibler Daten

München, 18. Oktober 2007 – IronPort – Cisco-Geschäftseinheit und ein führender Anbieter von Anti-Spam-, Anti-Viren- und Anti-Spywarelösungen – stellt im Rahmen seiner neuen Data-Loss-Prevention-Studie sechs wichtige Regeln vor, um Informationslecks zu vermeiden, Compliance-Vorschriften durchzusetzen und so den Ruf und den Namen eines Unternehmens zu schützen (Data Loss Prevention, DLP). „Ob mit böswilliger Absicht oder durch einen unbeabsichtigten Fehler – sensible Daten, die in falsche Hände gelangen, können Unternehmen teuer zu stehen kommen. Schwerer Imageverlust, Aktienkurse, die in die Tiefe stürzen oder ein sinkender Markenwert sind nur ein paar Beispiele der möglichen Folgen für das Unternehmen“, weist Reiner Baumann, Regional Director Central and Eastern Europe, auf die Gefahren hin.

Die elektronische Kommunikation via E-Mail, Instant Messaging, Webmail oder Webformulare findet meist noch immer ohne wirkungsvolle Kontrolle statt. Die größte Gefahrenquelle ist dabei, dass vertrauliche Unternehmensinformationen an Unbefugte gelangen können. Marktübliche Firewalls und andere Lösungen für Netzwerksicherheit bieten keinen ausreichenden Schutz. Es fehlen wichtige Kontrollen wie das Scannen des Inhalts, das Blocken von Nachrichten mit vertraulichen Inhalten an unbefugte Empfänger sowie die automatische Verschlüsselung sensibler Daten.

Unternehmen, die eine Lösung für dieses Problem suchen, sollten die folgenden sechs wichtigen Regeln beachten:

Regel Nr. 1: Nehmen Sie sich die Zeit, ihre DLP-Anforderungen zu definieren

Der entscheidende erste Schritt ist die Bestandsaufnahme. Dies erfordert einen umfassenden Überblick über die im Unternehmen vorhandenen vertraulichen Daten und die notwendigen Richtlinien, um den Zugriff auf diese Daten zu kontrollieren und zu schützen. Dazu muss die Organisation genau die Verkettung ihrer Unternehmen und Agenturen, Compliance-Vorgaben, Urheberschutz und die angemessene Durchführung prüfen.

Regel Nr. 2: Priorisieren Sie unter den DLP-Bereichen

DLP ist ein komplexes Problem. Es erfordert die richtige Zusammenstellung an bewährten Lösungen, damit alle relevanten Aspekte für die jeweilige Organisation abgedeckt sind. Um Datenlecks möglichst schnell zu

schließen, sollten zuerst die wichtigsten DLP-Bereiche adressiert werden – nämlich diejenigen, die das größte Gefahrenpotenzial darstellen.

Regel Nr. 3: Stellen Sie eine effektive und umfassende Abdeckung sicher

Eine DLP-Lösung muss vor allem in der Lage sein, versuchte Verstöße gegen die Richtlinien effektiv und umfassend aufzudecken. Das erfordert folgende Funktionen:

- Multi-Protokoll-Monitoring und Prevention
- Inhaltsbasierte Analyse aller wichtigen Dokumenten- und Attachment-Typen
- Selektives Blocken und/oder Isolieren von Nachrichten
- Automatische Verschlüsselung analog der Unternehmensrichtlinien

Regel Nr. 4: Gestalten Sie die Lösung flexibel

Eine gute DLP-Lösung muss flexibel an die häufig wechselnden Anforderungen anpassbar sein. Um die Herausforderung einer effektiven Kommunikation mit gleichzeitiger Kontrolle vertraulicher Daten zu meistern, bedarf es durchdachter Richtlinien und Prozesse, um sämtliche Inhalte der Kommunikation zu überwachen. Organisationen sollten eine DLP-Lösung für E-Mail und Web auswählen, die das kontinuierlich ansteigende Nachrichtenvolumen und zukünftige Anforderungen an Bandbreiten managen kann. Diese Ziele sind heute umsetzbar, denn auf dem Markt gibt es bereits geeignete Lösungen mit hoher Skalierbarkeit und Leistung.

Regel Nr. 5: Achten Sie auf Workflow, Administration und Reporting

Eine DLP-Lösung ist nur dann effektiv, wenn sie detaillierte Berichte zu allen verdächtigen Vorkommnissen liefert. Administratoren und Compliance-Verantwortliche sollten in der Lage sein, ausführliche Reports über nachgewiesene Verstöße zu erhalten, die alle nötigen Informationen zum Handeln enthalten. Zu diesen Angaben zählt der Sender der Nachricht, Inhalte, Anhänge, beabsichtigte Empfänger und Informationen zur Art des Verstoßes.

Regel Nr. 6: Kombinieren Sie bewährte Lösungen

Ein Kennzeichen bewährter Lösungen ist die Möglichkeit, ihre Wirksamkeit durch die Integration anderer bewährter Tools zu erhöhen. Unternehmen sollten den Einsatz von DLP-Lösungen vermeiden, die zukünftige Integrationen ausschließen. Im Hinblick auf die industrielle Entwicklung wird in Zukunft die Flexibilität entscheidend sein, durch Konnektivität und Datenaustausch von den Lösungen anderer Anbieter zu profitieren.

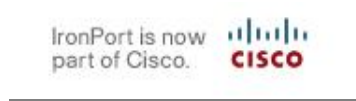
Reiner Baumann fasst zusammen: "Die neue Sicherheitsstrategie DLP richtet sich an alle Unternehmen und Behörden, die mit vertraulichen Daten umgehen. Als Ergänzung zum Schutz vor Spam, Viren und anderen Bedrohungen der E-Mail- und Web-Kommunikation bieten wir nun auch eine DLP-Lösung, die Organisationen die Benutzerfreundlichkeit, Flexibilität und Managementfunktionen bietet, die zur Sicherung ihrer sensiblen Unternehmensdaten erforderlich sind."

Der IronPort-Bericht "Data Loss Prevention - Best Practices" steht unter http://www.akima.de/transfer/Booklet_Data_Loss_Prevention.pdf kostenlos zum Download bereit.

Über IronPort Systems

IronPort Systems ist eine Geschäftseinheit von Cisco und ein führender Anbieter von Anti-Spam-, Anti-Viren- und Anti-Spywarelösungen. Die Appliances von IronPort wurden für kleine Firmen bis hin zu Global 2000 Unternehmen entwickelt und spielen in der Netzinfrastruktur eines Unternehmens eine geschäftsentscheidende Rolle. Die innovativen Systeme sind einfach zu bedienen und bieten höchste Leistungsfähigkeit. Sie verwenden SenderBase®, die weltweit größte Datenbank zur Beobachtung und Bewertung von E-Mail- und Web-Bedrohungen.

Mehr Informationen über Produkte, Lösungen und Services von IronPort finden Sie unter: www.ironport.com.



###

Ansprechpartner für die Presse:

Angelika Felsch
Marketing Manager
Central & Eastern Europe
IronPort Systems GmbH

Paul-Wassermann-Str. 3, 81829 München
Tel: +49 89 45 22 27-14
Fax: +49 89 45 22 27-10
E-Mail: afelsch@ironport.com