

Redaktionskontakt:

essential media GmbH
Rainer Bock
+49-89-747262-44
rainer.bock@essentialmedia.de

essential media GmbH
Isabella Fröhlich
+49-89-747262-41
isabella.froehlich@essentialmedia.de

InfoWatch präsentiert Studie zu Sicherheitsrisiken durch Instant Messenger

Moskau/Ingolstadt, 27. August 2007 – Die Nutzung von Instant Messengern (IM) im Unternehmensnetzwerk wird immer beliebter – doch sie ist nicht ungefährlich. Das Hauptrisiko, mit dem die Unternehmen konfrontiert werden, besteht im Abfluss vertraulicher Daten. Zu diesem Schluss kommt das Sicherheitsunternehmen InfoWatch in seiner neuen Studie „IM – Instant Messenger oder Informations-Missbrauch?“.

Wichtigstes Ziel der Studie war die Definition der Risiken durch die Verwendung von IM in Unternehmen und die Erarbeitung effektiver Schutzmethoden. Am Projekt nahmen über 1200 Nutzer des Portals SecurityLab.ru teil.

Den Umfrageergebnissen zufolge verwendet die überwiegende Mehrheit der Befragten – nämlich 87,2 Prozent – Instant Messenger, wobei ICQ die größte Popularität erreicht. 74,3 Prozent der IM-Nutzer setzen ICQ ein. Mehr als die Hälfte der Befragten nutzen daneben allerdings auch andere IM-Programme, was die Wahrscheinlichkeit möglicher Risiken zusätzlich erhöht. Nur etwas über die Hälfte (51,4 Prozent) der Befragten schützt sich vor den möglichen Gefahren.

Die Ergebnisse der Studie zeigen, dass das mit Abstand am häufigsten genannte Risiko im Abfließen vertraulicher Informationen (42,3 Prozent) besteht. Dieser Abfluss passiert durch Fahrlässigkeit der Mitarbeiter oder als Ergebnis geplanter Insider-Aktionen. Nur 60,3 Prozent der Befragten sind sich sicher, dass sie nie vertrauliche Informationen über IM verschicken.

Um sich vor dieser Gefahr zu schützen, nutzen die Unternehmen vorwiegend Maßnahmen in Form einer Blockierung des Traffics. Rein kontrollierende Maßnahmen (Monitoring) sind bisher nicht weit verbreitet, ihre Einführung ist offensichtlich mit technischen Problemen und dem Widerstand der Mitarbeiter verbunden. Nach Ansicht der Experten von InfoWatch wird sich diese Situation jedoch mittelfristig ändern.

Die steigende Bedeutung von Instant Messengern als Kommunikationsinstrument im Geschäftsumfeld ist nicht von der Hand zu weisen. Die Anzahl von Schutzprogrammen wird ebenso beständig zunehmen wie die Nachfrage nach derartigen Lösungen seitens der Kunden. Der Anteil jener Unternehmen, die den Schutz von IM-Kanälen ignorieren, wird dementsprechend sinken. Sowohl die Hersteller von Sicherheitslösungen als auch die



Kunden werden sich in dem Maße um einen immer besseren Schutz bemühen, in dem die Bedrohungen zunehmen – sowohl von außen als auch - und insbesondere - durch Insider.

Über Infowatch:

InfoWatch bietet mehrstufige Lösungen zur Einhaltung von gesetzlich vorgeschriebenen Sicherheitsrichtlinien und zum Schutz vor Datenlecks. Die InfoWatch-Monitore sichern sensible Daten, indem sie die unautorisierte Manipulation oder Weitergabe kritischer Informationen unterbinden. Neben dem Schutz unternehmensinterner Assets vor Missbrauch und fahrlässigem Umgang sichern die InfoWatch-Lösungen so persönliche Daten von Kunden und Mitarbeitern (zum Beispiel Kreditkarten- oder Patientendaten sowie Personalien).

Die auf linguistischen Analysemethoden aufbauenden InfoWatch-Monitore überprüfen den Datenfluss an verschiedenen Knoten des Unternehmensnetzwerks, wie beispielsweise E-Mail-Server, Internet-Gateway, Ports (Laufwerke, Drucker- und USB-Schnittstellen) sowie am Arbeitsplatzrechner. Das mehrstufige Konzept umfasst eine umfangreiche und maßgeschneiderte Beratung und Anpassung der Lösungen an die Sicherheitsrichtlinien und Anforderungen des Unternehmens.

InfoWatch wurde 2003 gegründet und ist eine hundertprozentige Tochterfirma von Kaspersky Lab, einem führenden Unternehmen im Bereich Viren-, Spam- und Hacker-Schutz.