

Es gibt Begriffe, die sind in aller Munde.
Doch oft gibt es unterschiedliche Definitionen.

IT-MITTELSTAND verschafft Klarheit:

Was ist eigentlich?...

... [Instant Messaging]

➔ Instant Messaging (IM) ist sowohl im Privatbereich als auch für die Geschäftskommunikation in internationalen Unternehmen eine gern genutzte Lösung. Wie viele neue Kommunikationsmittel verbreitete sich auch IM zuerst im englischsprachigen Raum. Im Gegensatz zu Europa wird dort die Technologie weit verbreitet im Geschäftsalltag genutzt. Die webbasierenden IM-Programme, sei es von AOL, Yahoo oder MS ähneln sich technisch und funktional: Wie bei einem Online-Chat können Nutzer das Web zur Echtzeitübertragung von Daten und Nachrichten nutzen. Dabei sehen sie jederzeit, welcher Gesprächspartner gerade erreichbar ist. In internationalen Projektteams erreichen Anfragen so gezielt die mit der Problematik vertrauten und am PC sitzenden Kollegen.

Diese Gründe qualifizieren IM als Ergänzung zu Telefon und E-Mail: Die IM-Dienste ermöglichen, bedingen aber nicht Kommunikation in Echtzeit. Besonders profitieren davon mittelständische Unternehmen, die mit räumlich verteilten Projektteams arbeiten. Auch gelten die Vorteile für Mittelständler mit verschiedenen Produktionsstandorten. Dabei ist der Einsatz auch ein Kostenfaktor, denn die Programme sind frei erhältlich und problemlos auf jedem Standard-PC installierbar.

Ist Instant Messaging sicher?

In der digitalen Datenübertragung gibt es keine hundertprozentige Sicherheit. Eine IT-Kommunikationslösung kann aber lückenhaft oder sehr gut abgesichert sein. Das gilt auch für IM: Denn per IM-Dienst übertragene Nachrichten und Dateien sind Netz-, also HTTP-Daten. Gängige Sicherheitslösungen wie Firewalls und Virens Scanner überprüfen diese nicht auf Inhaltsebene. Mit solchen Methoden ist es daher nicht möglich, bösartigem Programmcode oder Links zu Webseiten mit gefährlichen Applets, die sich in IM-Daten ver-

stecken können, Zugang zum Firmennetz zu verbieten. Ähnlich ist es im Umkehrschluss mit Daten, die das Firmennetz verlassen.

Mitarbeiter können beim vergleichsweise informellen Austausch per IM nur schwer sicher sein, wer sich genau am anderen Ende der „Leitung“ befindet. Es besteht das Risiko, dass sensible Firmendaten unbemerkt per IM das Unternehmen verlassen. Für die Betriebe umfasst diese Unsicherheit in gewissem Maße auch den eigenen Mitarbeiter: Einerseits integriert sich IM sehr gut in tägliche Geschäftsprozesse. Andererseits ist die private Nutzung während der Arbeitszeit möglich. Existieren hier keine Sicherheitsregelwerke, oder fehlen Mechanismen zur Umsetzung, kann solche Nutzung zum Produktivitätshemmnis werden. Um von IM-Diensten zu profitieren, sollten sie in eine umfassende IT-Sicherheitslösung eingebettet werden.

Welche Sicherheitsinfrastruktur?

Eine solche Sicherheitslösung heißt, dass globale und nutzerspezifische Sicherheitsregelwerke IM betreffend zentral und einfach umgesetzt werden können. Am Besten eignet sich eine Secure Proxy Appliance mit integrierter Instant-Messaging-Unterstützung. Sie gibt dem Management ein zentral steuerbares Werkzeug an die Hand, mit dem sich sämtliche Vorgänge der Mitarbeiter die Internet-Nutzung betreffend absichern und regulieren lassen. Entsprechende Geräte, die mit bestehenden Firewall- oder Antivirenlösungen zusammenarbeiten sind bereits auf dem Markt. D.h., dass für zusätzliche Sicherheit nicht kostspielig bestehende Lösungen ersetzt werden müssen. Vielmehr lässt sich Web-Sicherheit auf Inhaltsebene nahtlos in bestehende Strukturen integrieren. Mit solch einer kosteneffizienten Lösung gelingt dann auch der Spagat zwischen Produktivität und Netzwerksicherheit. ➔ *Michael Hartmann*



Der Autor **Michael Hartmann** ist Territory Sales Manager Deutschland, Österreich, Schweiz und Osteuropa bei Blue Coat Systems