

Leicht löslich, schwer verdaulich?!

Instant Messaging im Unternehmen: nützlich, vielfältig, sicher?

Kommunikation in Echtzeit ist in der modernen Geschäftswelt ein echter Wettbewerbsfaktor. Hier trumpfen Instant Messenger gegenüber E-Mails auf. Firmen fragen aber zu Recht: Ist das sicher? Genügen die Verfahren unternehmensinternen und behördlichen Richtlinien? Was ist noch tun, damit sie rundum sicher sind?

Von Michael Hartmann, München

Viele Unternehmen haben Instant Messaging (IM) bereits für ihre Geschäftskommunikation entdeckt. Schneller als E-Mail und unkompliziert wie ein Telefonanruf versprechen die praktischen Dienste das Beste zweier Welten. Nicht umsonst bescheinigt Nielsen NetRatings den führenden Anbietern Nutzerzahlen, die mit denen öffentlicher Web-E-Mail-Dienste vergleichbar sind; im März 2004 hielten die Marktforscher sogar eine weit höhere durchschnittliche Nutzungsdauer fest. Um Instant Messaging auch im Geschäftsalltag zur „Killerapplikation“ zu machen, gilt es jedoch einige (Sicherheits-)Fragen zu klären.

Instant-Messaging-Anwendungen ähneln in ihrer Funktion

Chat-Programmen: Aus einer Liste mit mehreren Gesprächspartnern, so genannten „Buddies“, wählt der Anwender den gewünschten. Beide tauschen dann über das Programm wechselseitig Textmitteilungen aus. Unterschied zur E-Mail und größter Vorteil: Die Kommunikation erfolgt unmittelbar in Echtzeit. Die virtuelle Präsenz des Gesprächspartners lässt sich dabei laufend erkennen: Ist das Gegenüber zum Beispiel nicht erreichbar, befindet er sich nicht an seinem Arbeitsplatz oder möchte nicht gestört werden, zeigt der Instant Messenger eine entsprechende Statusmeldung.

Diese Grundfunktionen sind bei den frei im Internet erhältlichen IM-Anwendungen praktisch gleich – zum Beispiel von AOL, Yahoo oder

MSN, den drei großen Namen des so genannten Public IM. Zusätzlich bieten diese Dienste vielfältige weitere Funktionen, denen sie ihre große Beliebtheit bei Heimanwendern verdanken: Dazu gehören unter anderem Dateiversand, SMS-Nachrichten oder Voice- und Video-Dienste. Auch Group-Chats, also Textkonferenzen mit mehreren Teilnehmern, Video-Konferenzen oder die Nutzung mit mobilen Endgeräten sind möglich.

Gerade diese Vielfalt macht die Dienste auch für den geschäftlichen Einsatz so interessant. Dies zeigen analog die Ergebnisse einer Umfrage, die Blue Coat in deutschen Unternehmen im ersten Quartal 2004 zum Thema Business-IM durchgeführt hat: Annähernd 60 % der Befragten bestätigen das Potenzial von Instant Messaging für die Geschäftskommunikation. Besonders im internationalen Austausch kann diese Technik ihre Vorteile ausspielen, sagt über die Hälfte der Teilnehmer.

Public vs. Private

Dabei ist die Unterscheidung zwischen den eben beschriebenen Public-IM-Diensten und den so genannten Private- oder Enterprise-Lösungen wichtig: Letztere sind dedizierte Lösungen auf Hard- oder Softwarebasis, die eine eigenständige IM-Kommunikation ausschließlich innerhalb des jeweiligen Unternehmens realisieren. Es gibt sie als IM-Appliances oder als Software für einen Kommunikationsserver. Bei solchen Lösungen, wie sie zum Beispiel IBM Lotus oder Reuters Messaging anbieten, wird die Datenübertragung verschlüsselt. Durch Nutzung eines Virtual Private Networks (VPN) als Übertragungskanal profitieren auch externe Partner von der Textkommunikation in Echtzeit.

Am zentralen Gateway können Sicherheitslösungen Internet-Datenströme besonders umfassend regulieren

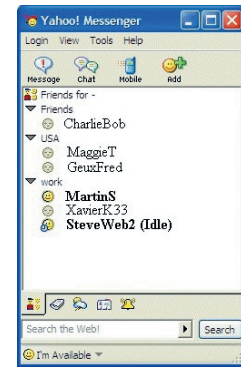


Die frei im Internet verfügbaren Public Instant Messenger hängen sind kleine Programme, die jeder Mitarbeiter selbst auf seinem PC installieren kann. Die Kommunikation läuft dann entweder direkt über den Server des IM-Anbieters (Server Proxy) oder wird zumindest von ihm vermittelt (Server Broker). Generell sucht der IM-Dienst beim Aufbau einer Web-Verbindung als Erstes zentral nach den Kontakten (Buddies) des jeweiligen Nutzers. Dazu stellt er eine Verbindung zum Server des jeweiligen Anbieters her. Dort erfährt das Programm, welche Kontakte eines Nutzers gerade online sind.

Bei der Server-Proxy-Kommunikation laufen die IM-Daten zwischen Client A und Client B immer über den Server-Proxy als Vermittler. Der Vorteil: Beide Clients versenden IM-Nachrichten, müssen aber keine eingehenden Nachrichten

von anderen Clients akzeptieren. Das ist wichtig, weil der dafür standardmäßig genutzte Port in der Regel aus Sicherheitsgründen per Firewall gesperrt ist. Davon abgesehen ist aber die Kommunikation über einen externen Server aus Sicherheits- und Performance-Gründen nicht die beste Wahl.

In einer Server-Broker-Architektur hingegen kommunizieren beide Clients direkt. Der Server initiiert diese Kommunikation lediglich: Wenn ein Client sich bereit erklärt, IM-Daten mit einem anderen auszutauschen, gibt der Server die notwendigen Daten wie IP-Adresse und Port-Nummer weiter. Beide Clients kommunizieren im Folgenden ohne Zwischenstation, was zwar sicherer ist, allerdings nur funktioniert, wenn der verwendete Port von der Firewall für eingehenden Verkehr freigegeben ist.



Rückzug installiert ermöglichen Instant Messenger den unmittelbaren Austausch mit Bekannten.

Für Server Proxy und Server Broker gilt gleichermaßen: Nutzen Anwender Public-IM, sind die übertragenen Daten meist unverschlüsselt. Funktionen wie Datenkodierung per SSL gibt es zwar zum Beispiel beim AOL Messenger. Damit steigt die Gefahr von geistigem Diebstahl aber deutlich, weil Firmen kaum kontrollieren können, welche Daten dann per IM das Unternehmensnetz

verlassen. Deshalb sind verschlüsselte IM-Verbindungen oft generell untersagt. Daher sind Public-IM-Daten meist unverschlüsselt und passieren einen „öffentlichen“ Server – zwei Tatsachen, die potenzielle Geschäftsanwender beachten sollten. Allerdings sind bislang keine Fälle bekannt geworden, in denen man IM-Kommunikation zwischen zwei Clients abgefangen hat. Diese Bedrohung ist, zumindest bisher, eher theoretischer Natur.

Anwendungsszenarien

Unternehmen sollten Instant Messaging als Ergänzung zu den etablierten Kommunikationsmitteln Telefon und E-Mail verstehen. Weil die Kommunikation in Echtzeit stattfindet und der Gesprächspartner – zumindest virtuell – ständig präsent ist, spielt IM seine Stärken auf ganz eigenen Gebieten aus. Die schwierige Kommunikation in internationalen Teams oder zwischen verschiedenen Standorten demonstriert dies sehr gut: Hier wird oft über verschiedene Zeitzonen hinweg kommuniziert. Im ungünstigsten Fall bedeutet dies, dass zum Beispiel E-Mails im Tagesrhythmus verzögert ankommen – eine morgens in den USA versandte Nachricht erreicht den Empfänger in Europa erst am Morgen des Folgetages.

Mit IM treten solche Verzögerungen nicht notwendigerweise auf: Der Nutzer sieht auf den ersten Blick, welcher seiner Ansprechpartner gerade erreichbar ist. Außerdem weiß er, welcher seiner verfügbaren Kontakte bei einem bestimmten Problem am schnellsten helfen kann. Spricht er nun genau diesen an, erhält er praktisch in Echtzeit die Antwort auf seine Frage. Deweiteren bleibt ihm trotzdem die Wahl, ein vertiefendes Telefongespräch zu führen; dazu kann er über IM erfragen, ob dieses Gespräch für sein Gegenüber nicht in einen unpassenden Zeitraum fällt. Will er hingegen mehrere Personen erreichen und zum Beispiel komplexe Sachverhalte erklären oder umfangreiche Dateien anfügen, wird er auf E-Mails zurückgreifen.

Instant Messaging ergänzt andere Kommunikationsmittel auch deshalb so gut, weil die Lernkurve sehr niedrig ist. Vom Download bis zur Inbetriebnahme benötigen Anwender kaum mehr als ein paar Mausklicks. Die grafischen Bedienoberflächen der Programme erklären sich praktisch von selbst. Auch Zusatzfunktionen wie Konferenzen oder das Übertragen von Botschaften per Webcam funktionieren sehr einfach. Dabei spielt es keine Rolle, wo genau sich der Gesprächspartner befindet. Die heute in Firmen verwendeten Breitband-Flatrates ermöglichen die Kommunikation per IM ohne Zusatzkosten – auch wenn Voice-over-IM-Dienste genutzt werden. IM ist also aufgrund der Kostenstruktur auch für kleinere Unternehmen interessant: Notwendige Bandbreite steht sowieso zur Verfügung, und für „Anschaffung“ und Betrieb eines Public Instant Messengers fallen keine Kosten

an. In der internationalen Kommunikation einen Telefonanruf durch eine kurze IM-Konversation zu ersetzen ist also nicht nur gut für die Produktivität, sondern spart sogar Geld.

Gefahr erkannt, Gefahr gebannt?

Das praktische Verfahren hat nicht zu Unrecht bereits viele Privat- und immer mehr Geschäftsanwender überzeugt. Der Prüfstein für die dauerhafte Etablierung im professionellen Bereich ist aber die Sicherheit. Nur wenn die IM-Nutzung keine schädlichen Auswirkungen auf das Unternehmensnetz und die Integrität der gespeicherten Daten hat, werden die Anwenderzahlen die IDC-Prognose von 300 Millionen bis 2005 tatsächlich erreichen. Dafür ist eine umfassende Absicherung notwendig: Unternehmen sollten einerseits die Nutzung von IM unter organisatorischen Aspekten der IT-Sicherheit kritisch begutachten. Andererseits gilt es, notwendige Sicherheitsmaßnahmen auch technisch umzusetzen.

Dass Mitarbeiter in vielen Unternehmen Instant Messaging bereits nutzen, ist ein offenes Geheimnis – unabhängig davon, ob dies pauschal erlaubt oder verboten oder feiner reglementiert ist. Weil die Programme beliebt und frei erhältlich sind, installieren Mitarbeiter sie oft ohne Wissen des Managements. So kann sich im Unternehmen jedoch kein Bewusstsein für Gefährdung oder Nutzen entwickeln. Häufige Folgen: Die Unternehmensführung evaluiert nicht die Vorteile, die eine firmenweite Nutzung von Instant Messaging böte. Außerdem bezieht die IT-Leitung die Dienste nicht in die unternehmensweite strategische Sicherheitsplanung mit ein.

Deshalb kann auch der Mitarbeiter nichts von IM-spezifischen Regelwerken erfahren – und übersieht leicht die potenziellen Gefahren dieser Technik: Ist ein Public Instant Messenger erst einmal auf dem Desktop installiert, bedeutet er im schlimmsten Fall eine ungesicherte Verbindung zum Internet. Denn IM-Daten laufen im Gegensatz zu E-Mails nicht über den abgesicherten Unternehmensserver, sie werden auch nicht auf Inhaltsebene überprüft. Weil Public IM außerdem Port-agil ist, also selbstständig offene Schnittstellen zur Kommunikation mit dem Internet sucht, kann Instant Messaging zu einem Einfallstor für Viren oder bösartigen Programmcode werden.

Ungesicherte Kommunikation findet aber auch in der Gegenrichtung statt: Sind keine zusätzlichen Sicherheitsmaßnahmen implementiert, so könnten Mitarbeiter jederzeit unbemerkt vertrauliche Firmendaten versenden. Auch deshalb gilt: Eine übliche IT-Sicherheitslösung genügt nicht, um IM sicher im Unternehmen zu betreiben.

Weiterhin ist nicht ausgeschlossen, dass Cyber-Kriminelle zukünftig verstärkt programmimmanente

Schwachstellen attackieren: Buffer-Overflow-Angriffe oder manipulierte Datenpakete können zum Beispiel ein Weg sein, illegal Zugriff auf einen Rechner mit installierter IM-Anwendung zu erhalten; ist diese erste Hürde genommen, vervielfacht sich das Bedrohungspotenzial enorm. Ähnliches gilt für Ad- oder Spyware: Klickt ein Anwender unbedarft auf eine unbekannt URL, kann er sich über einen „Malicious Link“ eventuell alle Arten von möglicherweise gefährlichen aktiven Inhalten einfangen.

Für Unternehmen ist außerdem wichtig, dass Nielsen NetRatings in ihrer Umfrage vom März 2004 für Public IM tägliche Spitzennutzungszeiten von bis zu drei Stunden ermittelt hat. Dementsprechend sollte man dem Thema Nutzungskontrolle erhöhte Aufmerksamkeit schenken. Vor allem nicht-arbeitsrelevantes Chatten sollte in der Firma auf ein Minimum beschränkt sein. Keine leichte Aufgabe, denn die private Nutzung von IM lässt sich auf die Schnelle nicht von normaler Bildschirmarbeit unterscheiden. Im Rahmen einer Umfrage von Blue Coat England im letzten Jahr gaben immerhin 65 % der Befragten zu, während der Arbeitszeit auch Privates per IM auszutauschen. Eine IM-Kontrolllösung sollte deshalb mehrere Möglichkeiten bieten: Einschränkung der IM-Kommunikation je nach Tageszeit oder Beschränkung der IM-Nutzung auf das eigene Netzwerk oder auch Verbot der Video- und Chatroom-Funktionen des Instant Messengers sowie ein Unterbinden des Datenversands per IM.

Sicherheit und Kontrolle

Das bei der geschäftlichen Nutzung von IM existierende Gefahrenpotenzial steht handfesten Vorteilen gegenüber: Im Finanzwesen, in internationalen oder großen Unternehmen und allen Branchen, die auf schnelle Reaktionen angewiesen sind, hat IM das Potenzial, langfristig ein alltägliches Kommunikationsmittel zu werden. Ein leichtfertiges Verbot dieser Art der Unternehmenskommunikation hindert Unternehmen daran, auch ihre Vorteile zu nutzen und sie als positiven Wettbewerbsfaktor zu erkennen. Außerdem ist es nicht einfach, die Funktion eines Instant Messenger in Netzwerken zu unterbinden. Zwar können Unternehmen die von IM-Diensten zur Kommunikation genutzten Ports per Firewall sperren. Wie bereits erwähnt suchen die Anwendungen aber standardmäßig freie Ports oder Proxies (vgl. S. 58) und stellen so dennoch eine Verbindung zum Internet her; und zumindest Port 80 bleibt letztlich fast immer offen, um Web-Zugriffe zu ermöglichen.

Eine Alternative ist die Nutzung von Private-IM-Angeboten. Softwarebasierte Lösungen wie Sametime von IBM Lotus sind über die bestehenden Netzwerksicherheitslösungen und integrierte Sicherheitsfunktionen wirkungsvoll zu schützen; ihre Kommunikation bleibt ohnehin auf das eigene Unternehmen beschränkt (evtl. ergänzt um

VPN-angebundene Partner) und läuft verschlüsselt ab. Allerdings gibt es keinen Austausch mit Public-IM-Anwendungen. Diese Vor- und Nachteile gelten auch für Private-IM-Lösungen auf Basis von Appliances.

Private-IM-Lösungen sichern zwar die „offizielle“ Kommunikation während der Arbeitszeit, können Mitarbeiter aber nicht von der Parallelnutzung Web-basierter Instant Messenger abhalten. Um auch Public IM zu kontrollieren, empfiehlt sich in jedem Fall eine ergänzende Lösung. Unternehmen sollten vor einer Entscheidung genau abwägen, ob sie auf eine spezifische IM-Komponente oder eine multifunktionale Security Appliance mit inte-

grierter IM-Kontrolle setzen. Solche Funktionen gibt es beispielsweise bei Proxy Appliances, die für den Unternehmenseinsatz optimiert sind und sämtliche Sicherheitsregelwerke zentral vorhalten. Derartige Geräte sind einerseits klassische Proxy-Server, die durch Caching die Bereitstellung von Web-Daten beschleunigen. Zusätzlich können sie aber auch unterschiedliche Sicherheitsregelwerke und so eine fast komplette Kontrolle des Internet-Datenverkehrs umsetzen: zum Beispiel Web-Daten auf Inhaltsebene filtern, Adware, Spyware und Pop-Ups kontrollieren und so weiter.

Diese Funktionen gelten analog für Public-IM: Mitarbeiter können – sofern erwünscht – beispielsweise nach der Arbeitszeit Web-basierte Instant Messenger für Privates nutzen, ohne dass eine Gefahr durch riskanten Programmcode droht. Die IM-Daten werden auf Inhaltsebene überprüft und im Zweifelsfall vom Sicherheitssystem gefiltert. Während des Arbeitstags lässt sich IM-Verkehr hingegen auf die firmeninterne Nutzung oder Kommunikation mit sicheren Kontakten beschränken. Die Nutzungsregeln – nicht nur für IM – lassen sich dabei nahezu beliebig fein justieren. Sofern die komplette Kontrolle zwischen Intranet und Internet an einem einzelnen Gateway stattfindet, profitiert die IT-Abteilung von einem hohen Maß an Transparenz des Datenverkehrs – Regelwerke können für alle Arten von Kommunikation, Dateitypen, Nutzungszeiten und -dauer, Nutzergruppen, verwendete Dienste und mehr definiert werden. Und für die Mitarbeiterinformation lassen sich idealerweise frei konfigurierbare Pop-ups oder „Splash-Pages“ definieren, die Web-Nutzer coachen und die Kommunikation der unternehmensweiten Sicherheitsstrategie erleichtern.

Fazit

Unternehmen können sicher sein: Auf manchen Clients in ihrem internen Netz sind bestimmt schon heute (Public) Instant Messenger installiert. Sie stehen deshalb vor zwei Herausforderungen: Einerseits müssen sie diese Technik für den Geschäftseinsatz fit machen, andererseits sollte sie in die Sicherheitsstrategie des Unternehmens eingebunden werden. Wie man diesen Herausforderungen letztendlich begegnet, hängt von den individuellen Bedürfnissen ab: Soll lediglich auf einigen Clients die Nutzung von Public IM unterbunden werden, so genügt vielfach eine einfache Software. Für höchste Sicherheit bei der Synchronkommunikation innerhalb einer begrenzten Nutzergruppe bieten sich Unternehmenslösungen für Private-IM an. Feingranulare Kontrolle von Public IM und größte Funktionsvielfalt bieten vor allem zentrale Sicherheitslösungen am Gateway. ■

Michael Hartmann ist Territory Sales Manager DACH & Eastern Europe bei Blue Coat Systems (www.bluecoat.de).

Verantwortungsvolles Instant Messaging im Geschäftsalltag

Unternehmen sollten folgende Punkte beachten, wenn sie mithilfe von Instant Messaging (IM) ihre Produktivität ohne Abstriche bei der Netzwerksicherheit steigern wollen:

_____ Risikoanalyse durchführen: Unternehmen sollten ermitteln, wie Instant Messaging bereits genutzt wird. Die Ergebnisse sind der Anhaltspunkt, um bestehende und neue Sicherheitsregelwerke zu beurteilen.

_____ Web-Nutzungsbedürfnisse bereits bei der Planung neuer Sicherheitsregelwerke beachten: Verschiedene Abteilungen stellen unterschiedliche Anforderungen an das Kommunikationsmittel Internet. Die IM-Lösung muss diese Anforderungen abbilden.

_____ IM-Nutzungsrichtlinien unternehmensweit und frühzeitig kommunizieren: Gute IM-Sicherheitslösungen bieten zum Beispiel die Möglichkeit, Mitarbeiter durch Hinweisseiten (Splash-Pages) über die IM-Nutzungsrichtlinien zu informieren.

_____ Schwachstellen in den IM-Regelwerken gezielt suchen und frühzeitig schließen: zum Beispiel feststellen, ob Mitarbeiter Zugang zu Rechnern mit unterschiedlichen Nutzungsbefugnissen haben oder Fernzugriff nutzen. In dieser Phase hilft ein Testbetrieb.

_____ Die eigene Rechtsabteilung informieren: zum Beispiel ist bei neuen Sicherheitsregelwerken eine Freigabe durch den Betriebsrat wichtig. Die Rechtsabteilung kennt sich auch mit Archivierungsvorgaben aus (z. B. im Rahmen der Richtlinien um Basel II).

_____ Die IM-Lösung auf die Bedürfnisse des eigenen Unternehmens abstimmen.