process one
INSTANT MESSAGES | CREATIVE BUSINESSES

GUIDE STRATÉGIQUE

Messagerie instantanée & Sécurité

1e édition

La majorité des entreprises admettent que la messagerie instantanée peut augmenter la productivité de leur personnel, mais bon nombre d'entre elles hésitent à encourager son utilisation compte-tenu des problématiques de sécurité qu'elle pose.

Ce Guide stratégique a pour vocation de présenter aux entreprises les risques réellement associés à la messagerie instantanée dans un environnement professionnel et de délivrer des solutions pour y faire face.

"Internet est le produit d'une combinaison unique de stratégie militaire, de coopération scientifique et d'innovation contestataire."
Manuel Castells, sociologue américain

Introduction

La messagerie instantanée n'est plus réservée aux *chats* entre amis sur des forums : elle est maintenant un mode précieux de communication dans l'environnement de travail, au même titre que le téléphone et l'e-mail. Elle permet d'obtenir une réponse instantanée aux questions, réunit des collaborateurs mobiles, et représente un point d'ancrage rapide et pratique pour échanger des idées et travailler sur un projet commun. Le cabinet d'analystes Gartner Group prévoit que **95 % des employés des 100 plus grandes compagnies mondiales vont choisir la messagerie instantanée comme « interface principale pour les discussions en temps réel sur ordinateur » d'ici 2013**.[1]

D'après une enquête menée par la société d'étude de marché indépendante Vanson Bourne[2], les entreprises sont tout à fait conscientes des avantages de la messagerie instantanée. Parmi les entreprises qui ont répondu à cette enquête, **74 % admettent que la messagerie instantanée améliore la collaboration des employés. Toutefois, 88 % des entreprises interrogées disent s'inquiéter des impacts de cette technologie sur leur politique de sécurité. 72 % d'entre elles ont même pris des mesures pour bloquer et interdire l'utilisation** de la messagerie instantanée dans leurs locaux par peur des menaces sur la sécurité.

74 % des entreprises admettent que l'IM renforce la collaboration entre leurs salariés, mais 72 % en interdisent son utilisation par crainte des failles de sécurité

Bien qu'elle soit compréhensible, cette réaction est, le plus souvent, abusive. Les risques liés à l'utilisation de la messagerie instantanée dans un environnement d'entreprise sont bien plus limités qu'on ne le pense. Parfois, il s'agit simplement d'une méconnaissance des nouvelles technologies de la part du personnel informatique, qui ne sait pas comment utiliser cette technique en toute sécurité dans l'entreprise.

Malgré tout, certaines inquiétudes sont tout à fait justifiées et les entreprises ont raison de procéder avec prudence.
De multiples questions, une réponse : avoir une approche réfléchie de la messagerie instantanée, afin de réduire proactivement les risques tout en permettant aux employés d'exploiter cette nouvelle technologie, en vue de renforcer leur collaboration avec leurs collègues et de travailler de façon plus productive.

---

[1] MarketScope for Enterprise Instant Messaging and Presence (Étude de marché de la messagerie instantanée et de son utilisation), The Gartner Group, 26 juin 2009

[2] Enquête menée auprès de 100 décisionnaires informatiques sénior dans des entreprises de 1 000 employés ou plus. Vanson Bourne, sponsorisé par ProcessOne, juillet 2008

La messagerie instantanée améliore la collaboration des salariés via :

- **L'accélération des communications**
  À la différence de l'e-mail, la messagerie instantanée permet aux employés de connaître les moments où leurs collègues sont disponibles pour recevoir des messages.

- **L'amélioration de la confidentialité pour les travailleurs mobiles**
  La messagerie instantanée combine l'instantanéité des appels téléphoniques et la confidentialité : les conversations ne peuvent pas être écoutées lorsque l'on travaille sur le site du client ou dans un lieu public.

- **La création d'équipes de travail**
  Plusieurs employés de l'entreprise, dans des pays et avec des fuseaux horaires différents, peuvent participer à des « discussions de groupe », presque instantanément, depuis leur ordinateur de bureau, leur PC personnel ou leur téléphone mobile.

- **La concentration sur les priorités**
  Les employés peuvent configurer leur messagerie instantanée afin de recevoir uniquement les messages de personnes spécifiques à des heures précises.

- **La création de rapports précis**
  Toutes les conversations peuvent être enregistrées : vous ne perdez aucune de vos idées et les actions réalisées ne sont ni perdues, ni oubliées.

Danger sous-jacent

Même si vous n'avez pas de plateforme de messagerie instantanée ou de stratégie à ce sujet, votre personnel utilise peut-être quand même cette technologie

L'augmentation soudaine de la popularité des messageries instantanées a pris un grand nombre de dirigeants par surprise. Tandis que les décideurs retardaient leur choix d'investissement dans des systèmes d'entreprise, la messagerie instantanée s'est introduite dans l'entreprise par la petite porte.

Renforcé par la multiplication des sites Web « d'échanges sociaux » et par le développement des messages texte, l'attrait de la messagerie instantanée a régulièrement augmenté ces deux dernières années. Dn fait, IDC identifie une nouvelle catégorie d'individus : les « hyperconnectés », c'est-à-dire les personnes passionnément convaincues de l'utilité des messageries texte et instantanées et plus gobalement des nouveaux modes de communication en temps réel. Le cabinet d'analystes calcule que 16 % des salariés informatiques du monde sont déjà « hyperconnectés »... et que 36 % de plus les rejoindront bientôt.[3].

Ces individus hyperconnectés/ Digital Natives tirent parti des services de messagerie instantanée publics, comme Googlemail et MSN, disponibles gratuitement en téléchargement et utilisation. C'est là qu'est le danger !

La plupart des gens téléchargent non seulement les logiciels de messagerie instantanée publics sur leur ordinateur personnel, mais les installent également sur leur ordinateur professionnel, à l'insu du service informatique. Bien qu'ils utilisent initialement ces services uniquement pour échanger des messages avec leurs amis et leurs proches, ils arrivent peu à peu à considérer la messagerie instantanée comme partie intégrante de leurs activités quotidiennes et se mettent à l'utiliser également pour leurs contacts professionnels. Ces personnes ne cherchent aucunement à nuire ; elles n'ont simplement pas conscience des dangers potentiels auxquels elles exposent leur entreprise.

Votre entreprise est-elle vraiment menacée ?
Dans le cadre d'une recherche menée auprès de 2 400 personnes travaillant dans 17 pays, IDC a constaté que deux tiers des personnes hyperconnectées utilisent la messagerie texte ou la messagerie instantanée à la fois pour leur travail et leur usage personnel. Plus d'un tiers utilisent également les sites Web de réseaux sociaux dans ces deux cas.

Les messageries instantanées grand public ne sont pas conçues pour une utilisation en entreprise et elles ne fournissent pas le niveau de sécurité indispensable à un environnement professionnel d'importance stratégique. Ces services permettent aux utilisateurs de joindre des fichiers à leurs communications et de les échanger avec un nombre illimité d'autres utilisateurs, dans n'importe quelle entreprise et n'importe quel pays. Il existe donc un risque fort de voir des données confidentielles sortir du cadre de la société ou à l'inverse de voir des documents infectés et corrompus entrer dans l'entreprise.

[3] The Hyperconnected: Here they come! (Voilà les hyperconnectés !) Rapport IDC, sponsorisé par Nortel, mai 2008

Quels sont les risques ?

Une utilisation non contrôlée de la messagerie instantanée expose l'entreprise à diverses menaces...

Attaques de vers, virus et chevaux de Troie

La plupart des menaces sur la sécurité concernent la propagation des virus, des vers et des chevaux de Troie. Pour les opérateurs des grands réseaux publics de messagerie instantanée, comme Yahoo, GoogleTalk et MSN, il s'agit d'une menace bien réelle. Les vers et virus sont souvent véhiculés par SPIM (Spam over Instant Messaging - Spam sur messagerie instantanée). Les utilisateurs reçoivent un e-mail non sollicité les invitant à cliquer sur un lien. Lorsqu'ils le font, ils lancent à leur insu une infection virale, ou un programme espion qui collecte les détails de leurs contacts et s'insinue dans leurs communications.

Selon une enquête de Cnet.com datant de juin 2008, seule la moitié des fournisseurs de messagerie instantanée grand public interrogés offrent un cryptage complet des flux de données...

Les utilisateurs du service de messagerie instantanée public ICQ sont particulièrement exposés au SPIM, car les ID d'utilisateurs n'étant que des numéros. Il est donc relativement facile pour des personnes mal intentionnées de générer des adresses aléatoires et de bombarder des milliers d'utilisateurs avec des communications infectées.

Perte de propriété intellectuelle

La perte d'informations confidentielles via una attaque externe est une menace réelle, que toutes les entreprises doivent prendre au sérieux. Les entreprises doivent en outre se prémunir contre les actions malfaisantes des anciens employés, qui peuvent, potentiellement, utiliser la messagerie instantanée pour transmettre des secrets aux médias ou à des concurrents. Attention également aux fraudes internes, qu'elles aient une raison lucratif ou psychologique, elles peuvent causer un tort considérable à l'entreprise.

Le risque de perte de propriété intellectuelle est d'autant plus grand que les systèmes de messagerie instantanée publics ne sont pas cryptés. Selon une enquête de Cnet.com datant de juin 2008[4], seule la moitié des fournisseurs de services publics de messagerie instantanée interrogés offrent un cryptage complet. Des services ultra-connus, comme Facebook Chat,

[4] http://news.cnet.com/8301-13578_3-9962106-38.html

Microsoft Windows Live Messenger et Yahoo Messenger n'offraient pas (à l'époque) la protection complète que tous les utilisateurs, particulièrement en entreprise, requièrent.

Vol de mots de passe et d'identités utilisateur

Les utilisateurs de comptes de messagerie instantanée publics courent également le risque de se faire dérober leurs mots de passe et leurs ID utilisateur. En février 2009, de nombreux utilisateurs de Gmail et de Yahoo ont été victimes d'importantes attaques par hameçonnage de leur compte de messagerie instantanée. Lorsque les utilisateurs cliquaient sur un lien dans le message factice, ils ouvraient la porte au vol d'identité. Les attaques par hameçonnage des messageries instantanées deviennent de plus en plus courantes. Le nombre des utilisateurs augmentant, il devient plus facile pour les pirates de découvrir une identité et ainsi l'usurper.

Les attaques par phishing des clients IM, notamment sur des messageries instantanée grand public utilisées en entreprise, deviennent de plus en plus courantes.

Le nombre des utilisateurs augmentant, il devient plus facile aux pirates informatique de deviner une identité et de l'usurper.

Bien sûr, la solution semble simple : s'assurer que les utilisateurs n'ouvrent pas les fichiers ou ne cliquent pas sur les liens venant de contacts qu'ils ne connaissent pas. Toutefois, dans un réseau de messagerie instantanée public, il peut être très difficile de vérifier l'expéditeur d'un message. Face à des noms d'utilisateur très vagues, comme Fred1234, il est facile de faire croire à l'utilisateur qu'il connaît l'expéditeur du message.

Manque de contrôle dans l'entreprise

Il est très difficile pour une direction informatique de surveiller efficacement l'utilisation des messageries instantanées grand public et d'en faire l'audit. Certains grands groupes peuvent ainsi être considérés comme étant en infraction, ne pouvant pas respecter les réglementations locales ou propres à l'entreprise qui exigent de conserver des traces auditables de toutes les transactions et communications de l'entreprise.

Par exemple, le Sarbanes Oxley Act de 2002 (également appelé Public Company Accounting Reform and Investor Protection Act, Acte sur la réforme de la comptabilité des entreprises publiques et sur la protection des investisseurs) exige que toutes les organisations américaines et leurs filiales à l'étranger soient à même de fournir un historique d'audit rigoureux de toutes leurs transactions.

De plus, le Health Insurance Portability and Accountability Act (HIPAA, Acte sur la portabilité et la responsabilité des assurances santé) qui régit les assurances santé aux USA,

ainsi que le Gramm-Leach-Bliley (GLB) Act qui régit les institutions financières américaines, exigent que l'entreprise conserve des enregistrements auditables de ses communications.

En Europe et dans d'autres régions du monde, il existe d'autres lois similaires qui affectent divers secteurs d'activités. Si les entreprises ne peuvent pas fournir d'historique d'audit, elles risquent d'être condamnées pour infraction et de faire face à des actions en justice très coûteuses. Elles risquent également une perte de revenus en raison des dommages que subit leur réputation en raison de cette infraction.

Comment répondre à ces défis ?

Prenez le contrôle

La principale mesure que doivent prendre les entreprises consiste à reprendre le contrôle de la messagerie instantanée, en déployant un système de messagerie instantanée d'entreprise dédié. Tous les messages instantanés envoyés et reçus par les employés doivent passer par un serveur central, être archivés pour référence future, être cryptés, et être intégrés aux processus et stratégies de sécurité de l'entreprise. Des programmes antivirus peuvent également être associés au serveur IM afin d'éviter la propagation involontaire de virus par des messages instantanés.

Via un client de messagerie instantanée de classe entreprise, les utilisateurs ont des noms explicites et identifiés (généralement identiques à leur adresse e-mail). Il est ainsi bien plus facile pour les employés de vérifier avec qui ils discutent et de s'assurer qu'ils ne sont pas victimes d'une attaque par hameçonnage. L'ajout d'un mécanisme de cryptage au système de messagerie instantanée d'entreprise renforce encore la confidentialité et la sécurité des échanges.

L'emploi d'une messagerie instantanée interne n'implique pas de couper les employés des réseaux de messagerie instantanée publics qui leur sont familiers. Il existe des solutions de passerelles vers des réseaux tels MSN ou GoogleTalk. Certains systèmes vont même plus loin et fournissent des ponts sécurisés avec des sites de réseaux sociaux comme Twitter. Cette souplesse et cette ouverture possible des messageries instantanées de classe entreprise ne sont pas contraires au principes de contrôle de l'utilisation du système par les directions informatiques. Les messages échangés peuvent être archivés, y compris ceux qui sont passés par des réseaux externes ou publics.

Réduisez les risques

Pour renforcer encore la sécurité de leur messagerie instantanée, les professionnels peuvent surveiller les domaines des utilisateurs qui contactent leurs salariés. À la différence de l'e-mail, la messagerie instantanée permet à l'administrateur système de préciser les domaines autorisés à envoyer ou à recevoir des messages, par le biais de certificats.

À la différence de l'e-mail, la messagerie instantanée permet à l'administrateur système de préciser les domaines autorisés à envoyer ou à recevoir des messages, par le biais de certificats.

Cette précaution rend les attaques par SPIM ou hameçonnage bien plus difficiles, car il est possible d'identifier de façon certaine l'expéditeur des messages. L'administrateur système peut donc bloquer la source des messages potentiellement dangereux.

Le but de la messagerie instantanée en entreprise est d'améliorer la collaboration entre les salariés et partenaires. L'objectif n'est pas de faciliter l'emploi de la messagerie instantanée pour les communications sociales et personnelles pendant les heures de travail.

De nombreuses entreprises décident donc d'autoriser uniquement les communications entre certains domaines et de bloquer les autres destinations via des certificats. Les administrateurs système les emploient pour limiter l'utilisation du système aux tiers de confiance.

La société interdisant (et empêchant) le transfert de fichiers aux organismes externes non spécifiées réduit immédiatement les risques liés à la perte d'informations confidentielles et aux infections virales.

Éduquez les utilisateurs

La mise en place d'une solution de messagerie instantanée d'entreprise doit obligatoirement être précédée d'une période de formation des utilisateurs.

Cette étape importante permet :

a) De **présenter la messagerie instantanée comme un outil de communication précieux**, au même titre que l'e-mail et le téléphone, et expliquer la façon dont elle peut être utilisée pour travailler plus efficacement.

b) De **fournir aux utilisateurs les connaissances nécessaires pour comprendre les menaces** de sécurité et mettre en place des comportements responsables.

Il est indispensable d'expliquer les risques de vol de propriété intellectuelle via l'usurpation d'identité. Les salariés peuvent alors valider l'identité d'un contact avant de lui envoyer des données sensibles. Une meilleure vigilance des employés réduit les risques sans faire obstacle aux gains de productivité potentiels.

Les clients de messagerie instantanée peuvent être extrêmement riches de fonctionnalités supplémentaires que les utilisateurs doivent apprendre à connaître : gestion de la présence, configuration du compte, de la réception des messages... Bien que ces fonctions en soi ne renforcent pas la sécurité, elles aident l'entreprise à garantir que son investissement dans un client de messagerie instantanée d'entreprise améliore réellement la productivité.

Conclusion

Les risques sont connus et peuvent être contrôlés.

Bien qu'il existe effectivement de nombreux risques de faillles de sécurité liées à l'utilisation de la messagerie instantanée en général, ces risques sont bien plus importants avec les services de messagerie instantanée grand public. Conçus pour des échanges sociaux et personnels, les réseaux publics sont souvent dépourvus de tout cryptage et n'offrent pas la protection indispensable aux environnements d'entreprise.

Si les utilisateurs utilisent leur compte de messagerie instantanée personnel sur leur ordinateur de bureau à la fois pour les communications personnelles et professionnelles, ils sont obligatoirement vulnérables et font courir des risques à leur organisation. Des centaines (ou même des milliers) d'échanges non sécurisés et sans audit peuvent en toute quiétude traverser le pare-feu de l'entreprise, et ce au quotidien.

Pour réduire les risques, la méthode la plus fiable consiste à déployer la messagerie instantanée en interne avec un serveur de messagerie instantanée centralisé. Ainsi, le service informatique peut prendre des mesures pour protéger les utilisateurs et la propriété intellectuelle de l'entreprise à l'aide du cryptage, de programmes antivirus, de stratégies d'entreprise et de certificats de domaine.

Dans ce cadre, les risques liés à la messagerie instantanée sont bien plus faibles. En effet, les messages sont généralement envoyés et reçus entre deux entreprises, et leur domaine d'action en est limité à l'entreprise et/ou à ses partenaires de confiance. Les organisations peuvent ainsi tirer parti de la messagerie instantanée pour améliorer la collaboration et la productivité de leur personnel, sans mettre leurs activités en danger.

Malgré tout, la sécurité reste un défi permanent dont les paramètres changent sans cesse et il faut en permanence la repenser. C'est pourquoi, lorsqu'une entreprise déploie son propre serveur de messagerie instantanée, elle peut choisir de prendre la précaution de souscrire un contrat de support auprès d'une société spécialisée dans ce domaine. Ainsi, lorsqu'une nouvelle menace apparaît, les services informatiques sont immédiatement avertis et peuvent rapidement accéder aux informations les plus récentes.
La meilleure défense : une vigilance constante soutenue par les conseils d'un spécialiste.

L'auteur : Mickaël Rémond, fondateur de ProcessOne

Juriste et gestionnaire de formation (Sciences Po - Eco. Fi 1996), Mickaël Rémond pratique l'informatique depuis le début des années 80. Il s'implique dès 1995 dans le milieu associatif autour des logiciels libres, au sein de l'association Apodeline, dont il devient ensuite Vice-Président. L'association participe à d'importantes manifestations de promotion des logiciels libres, tel que les « dimanches du libre » à la Cité des Sciences et de l'Industrie. Il est également contributeur du site Linux-France.org, site français de référence sur Linux et les logiciels libres.

Son parcours professionnel l'a conduit à travailler rapidement dans des grands comptes puis à se consacrer aux logiciels libres dans des sociétés de services (Idealx puis Capgemini), où il poursuit son travail de développement de solutions open source (Créateur et responsable de l'offre open source en France), tout en s'impliquant sur des projets pour des grands comptes. Il participe notamment à la rédaction du Guide de choix et d'usage des licences de logiciels pour les administrations (ex-ADAE). Il mène des missions de conseil sur les logiciels libres pour l'Institut Français du Pétrole, la Caisse d'Épargne, Orange (Mobile Internet for Business), CCI.fr (Chambres de Commerce et d'Industrie), Assistance Publique / Hopitaux de Paris, ACOSS, Ministère de la Culture, Direction Générale des Impôts, CNAM (Caisse Nationale d'Assurance Maladie).

Mickaël Rémond est spécialisé dans l'informatique distribuée et l'architecture des applications distribuées : applications tolérantes aux pannes, répartition de charge, haute-disponibilité. Il initie ou participe à plusieurs projets de développement de logiciels libres, en particulier autour du langage Erlang. Il est également l'auteur du livre "Erlang Programmation" (Eyrolles), et a été nommé "Utilisateur Erlang de l'année" en 2004.
Il est membre du comité de programme du salon "Solutions Linux". Il est le fondateur de ProcessOne un éditeur de logiciels, spécialisé en messagerie instantanée, s'appuyant largement sur le modèle Open Source.

Pour aller plus loin :

www.process-one.net
http://www.process-one.net/en/imtrends
http://www.process-one.net/fr/blogs/
http://twitter.com/mickael

À propos de ProcessOne

Créé en 1999, Process-one est un éditeur spécialisé dans les solutions de messagerie à haute performance. La société développe activement le serveur de messagerie instantanée ejabberd et propose un support commercial de haut niveau pour les installations d'ejabberd dans le monde entier. Process-one est ainsi un des principaux fournisseurs de solutions de messagerie et de services de communication en temps réel.

L'offre concerne les entreprises souhaitant déployer une messagerie interne avec ou sans inter connexion avec les réseaux existants (MSN, Yahoo!, AOL). Elle s'adresse aussi aux sociétés de l'Internet qui souhaitent enrichir les services offerts à leurs utilisateurs. Réputée pour sa très grande robustesse sous forte charge, la solution a été déployée chez d'importants clients dans le monde entier pour bâtir des services personnalisés (Meetic, Portugal Telecom, SIPPhone, Nero, ...), et est aujourd'hui utilisée par plus de 30 millions d'utilisateurs.