Безопасные средства обмена сообщениями online

Под аббревиатурой IM (instant messenger – «мгновенные сообщения», далее ИМ) подразумевается средство коммуникации, позволяющее создавать нечто вроде персональной чат комнаты совместно с другим человеком для общения в режиме онлайн по интернету по аналогу телефонных переговоров, с той разницей, что в качестве средства передачи данных используется текст, а не звук. Обычно, ИМ система сообщает о том, что кто-либо из вашего списка контактов находится в онлайне. Таким образом вы можете инициировать чат сессию с каким либо конкретным человеком.

В то время как ИМ становятся всё более распространёнными, ускоряют общение и предостовляют ещё один спрособ поделиться деловыми данными, ИТ менеджеры всё более обеспокаиваются, что они становятся ещё и новой уязвимостью к аттакам на корпоративные сети.

ИМ это наиболее «горячий» инструмент деловых офисов в наши дни. Возможность связываться с коллегами, задавать вопросы одногрупникам, и конечно общаться с друзьями, и всё это одновременно, привело к тому, что телефон и даже e-mail сильно сдали свои позиции как средства общения. Сегодня миллионы корпоративных пользователей имеют ИМ на своих рабочих машинах.

Первая проблема, связанная с этим, это то, что в большинстве случаев, пользователи устанавливают програмное обеспечение сами. ИТ отдел в большинстве случаев не имеет над ними ни контроля, ни наблюдения, ни каких либо стандартных процедур обеспечивающих безопасность.

Ещё одна проблема, в том, что «мгновенные сообщения» также могут означать и мгновенные проблемы.

Писатели Вирусов и спамеры не игнорируют дыры имеющиеся в ИМ. Аналитики безопасности и просто наблюдатели уже предсказывают что и те и другие уже нацелились на то, что кажется станет новым полем для развёртывания действий – ИМ.

«И хотя это небольшие риски сегодня, риск растёт» - говорит Ричард Стейнон, вице президент отдела исследований компании Гартнер Инк – «в то время, как использование и преобладание ИМ увеличивается, появление вирусов с большими деструктивными возможностями атакующих ИМ - это только вопрос времени»
Хотя по прежнему, основным источником заражения машин остаётся человеческий фактор – как например открытие почтовых вложений, от неизвестных вам людей, потенциально заражающих машину.

Вирусописатели уже обратили свой взор в сторону ИМ, добавляя своим «червям» и вирусам возможность пользоваться преимуществами ИМ. В большинстве случаев, это будет осуществляться через недостатки кода, примерно так, как сейчас это происходит с электронной почтой. Также возможно создание троянцев проникающих к ни о чём не подозревающему пользователю, и отдающих полные права на его машину вирусописателю.

И хотя до их пор было найденно относительно немного уязвимостей в безопасности основных ИМ продуктов, считается, что создатели вирусов и спаммеры просто только начинают прикладывать свои усилия к ИМ. При этом самой большой угрозой становятся сообщения уходящие за пределы корпоративной сети, которые вполне могут содержать критическую корпоративную информацию.

Хуже чем небезопасный

Беспокойство о безопасности нельзя назвать безосновательными. Для того, чтобы ИМ системы работали, рабочая станция пользователя должна оповещать окружающих, о том, что она в сети. После того, как две рабочих станции связываются с друг другом, через виртуальное соединение начинается диалог. Сегодня большинство ИМ систем не поддерживают такие основополагающие факты безопасности как аутентификация и шифрование. Это означает, что взломщики могут перехватывать любой обмен информацией. Неавторизированная личность может использовать ИМ соединение, чтоб получить доступ к корпоративным сетям, и, возможно, внедрить туда вирусы. Более того, в большинстве случаев обменн данными через ИМ не как не отражается в логах. Таким образом, корпоративному руководству не предоставляется возможным отслеживать и контролировать передачу данных.

При этом, несмотря на увеличивающееся число жалоб, популярность ИМ продолжает расти.

Примеры

Усложняет ситуацию то, что ИМ вирусы атакют используя множество различных механизмов.

MSN и ICQ два хороших примера протоколов, открыто публикующих свои API и пример червя который пользуется этими открытыми данными это W32.Choke.worm. Используя MSN Messenger, он просто посылает себя в качестве ответа на любое приходящее сообщение. Также, используя возможности Windows, вирус ‘Goner’ сканирует запущенные приложения, пытаясь захватить над ними контроль с целью своего распространения.

Вирус “Aplore”, например, распространяясь через AOL Instant Messenger посылает ссылку на червя расположенного на удалённом сервере. Нажимая на такую ссылку, пользователь становится жертвой «социальной инжинерии».

Факторы, обеспечивающие безопасность

Аутентификация

Первоначальная задача ИМ приложений, это, что вполне естественно, убедиться что пользователь, подключившийся к вашей корпоративной ИМ системе это тот, за кого он себя выдаёт. Возможны различные способы аутентификации пользователей, однако большинство корпоративных ИМ систем и порталов предпочитают использовать уже имеющиеся аутентификационные механизмы, такие, как например службы каталогов, вместо того, чтобы разрабатывать свои собственные.

Безопасность
Принимая во внимание тот факт, что ИМ становятся всё более популярным средством общения, разумно предположить, что переговоры проводимые чере ИМ в какой-то момент дойдут до того, что будут содержать конфиденциальную корпоративную информацию. Для этих целей необходима система предоставляющая некоторую безопасноть пересылаемых сообщений, даже если они будут происходить лишь в пределах локальной сети.

Анти-вирусы
Широко используемая возможность ИМ решений – это передача данных между пользователями. Точно так же, как это происходит сейчас с электронной почтой, необходимо убеждаться, что файлы которые вы получаете или отправляете не содержат вирусов.

Из-за дополнительных трудностей в плане разработки своих антивирусных систем, большинство корпроративных ИМ производителей предоставляют возможность установки плагинов от сторонних производителей.

Возможные решения проблем безопасности

Корпоративные (закрытые сети)

В настоящее время, наблюдается тенденция к тому, что всё больше и больше людей переходят на корпоративные версии ИМ. В этом случае, серверная часть находится внутри корпоративной сети, таким образом сообщения не выходят за её пределы. В этом случае, появляется возможность ввести учёт всей передачи данных и содержания. В случае когда сообщения уходят за пределы компании, есть возможность отправлять их через прокси, таким образом, опять же, вести учёт.

Установка firewall систем (либо интегрированных антивирс-файрвол систем) на все рабочие станции – одна из обязательных рекомендаций компаний занимающихся безопасностью. Такие системы позволяют блокировать использованние не одобренных ИМ приложений, и потенциально предотвратить отаки с этих и на эти рабочие станции.

Следующий список рекомендованный лидерами в области безопасности, призван уменьшить риски для корпоративных пользователей:

- Установка антивирусного програмного обеспечения и персональных файрвол систем на все рабочие станции
- Разработка и соблюдение корпоративной политики в плане использования ИМ – требование к пользователям не посылать конфиденциальную информацию через публичные ИМ системы
- Правильное конфигурирование корпоративных файрвол систем, для блокировки несанкционированного ИМ трафика извне
- По возможности, установка собственных корпоративных ИМ серверов, для изоляции корпоративных систем обмена сообщениями от остального мира
- Принудительная настройка клиентской ИМ части (например запрет на передачу файлов)
- Своевремнное установка обновлений ИМ приложений

К сожалению, в настоящий момент, лишь немногие компании применяют политику единого корпоративного ИМ приложения, оставляя возможность выбора за пользователями, и таким образом компромитируя безопасность в пределах огранизации. Большинство сегодняшних ИМ систем были разработаны больше для простого общения

потребителей, чем для безопасных корпоративных коммуникаций и как следствие, они содержат новые и часто неочевидные уязвимости для корпоративных клиентов.

Плагины и антивирусы

В настоящее время производители анти-вирусного ПО уже создали продукты, которые расширяют зону своего действия и на протоколы используемы ИМ, примерно так же как это реализуется в настоящее время для почтовых протоколов SMTP и POP3.

Большинство современных ИМ приложений, не шифруют передаваемые данные, таким образом, они могут быть легко перехваченны злоумышленниками. Для того чтобы разрешить эту проблему, на рынке уже появились специальные расширения-плагины для большинства наиболее популярных ИМ систем, шифрующие передаваемые данные.

Защита на физическом уровне

Одно из возможных решений для защиты ИМ систем – это защита на физическом уровне. Такое решение разрабатывается в настоящее время компаниями Validian и Sony Electroincs. То, что они создают представляет из себя флэш накопитель данных с USB интерфейсом, имеющем на себе развитые системы биометрической аутентификации (сканер отпечатков пальцев). ИМ приложение целиком размещается на таком носимом накопителе.

Устройство позволяет получать доступ к зашифрованным файлам только пользователям авторизированным по отпечаткам пальцев. К зашифрованным файлам и относится ИМ приложение, которое хранит на нём помимо испольнительных файлов ещё и записи разговоров.

В результате, корпоративные пользователи оснащённые этим «флэш комуникатором» могут получить доступ к ИМ практически с любого компьютера оснащённого USB портом – независимо от того будет ли это общая публичная точка доступа в интернет или домашний компьютер. При этом, пользователь практически не оставляет следа своих переговоров при отключении устройства. Устройсвто предполагается совместимым с большинством современных операционных систем и не требует установки специальных драйверов.

Разработанное решение занимается безопасностью и на физическом уровне, и на программном. Оно использует отпечатки пальцев и одновременно PKI (Public Key Infrastructure - Структура открытых ключей) функции. Распознаваемые образы отпечатков пальцев хранятся на самом устройстве, таким образом запрос об аутентификации не передаётся по сети, а производится в самом устройстве. Так исключается возможность их перехвата либо пропажа в результате взлома централизованной базы хранения.

Устройство основывается на RSA шифровании и поддерживает ключи длиной до 2048 бит, и совместимо с основными центрами сертификации.
Помимо того, что програмное обеспечение само по себе находится в защещённом состоянии, имеется возможность привязки конкретных приложений либо целой функциональности устройства к отпечаткам пальцев.

Заключение

Аналитики уверяют, что для того, чтобы избежать проблемы, наряду с ИМ вирусами и спамом, нужно просто запретить пользователям устанавливать ИМ приложения на свои машины. Ввести это как политику компании, и как ещё одно средство защиты – просто блокировать доступ к таким приложениям из корпоративной сети.

Но аналитики также признают, что это может быть слишком жёстким решением для многих компаний. Единственной альтернативой остаётся установка своих стандартов в области ИМ продуктов, разработанных для корпоративного использования – с такими функциями безопасности, как шифрование и локальные сервера, расположенные в пределах корпоративной сети. ИТ менеджерам необходимо относится к политике безопасности ИМ не менее серьёзно чем сейчас это происходит с электронными сообщениями.

Кажется, что большинству предприятих стоит задаться поиском решений уже сегодня. Рост продуктивности от использования ИМ приложений на лицо - сделав их безопасными, можно получить максимум преимуществ этого роста.

Источники

www.webopedia.com
www.instantmessagingplanet.com
www.serverwatch.com
www.secway.fr
www.opengroup.org/messaging/public/ oct-2003/im/saunders.pdf
www.symantec.com