Ксения Шудрова, shudrova.blogspot.ru

Поиски иголки в стоге сена

Поиск утечек информации является достаточно затратным по времени и ресурсам (сотрудники, специализированные программно-аппаратные средства) делом. Но мониторинг необходимо проводить постоянно, так как нарушение можно произойти в любой момент. В последнее время общение сотрудников, клиентов и поставщиков в основном происходит через электронную почту, а значит, e-mail является источником серьезной угрозы информационной безопасности.

Для того чтобы обнаружить утечки конфиденциальной информации через корпоративную почту, необходимо осуществлять мониторинг почтовых отправлений, но с юридической точки зрения все не так просто. Существует давний спор о том, возможно ли читать электронную почту сотрудников, так как согласно Конституции каждый имеет право на конфиденциальность своей переписки. С другой стороны, все, что создается на оборудовании предприятия в рабочее время, не является личной информацией, а принадлежит организации. Не будем останавливаться на тонкостях этих споров, на данную тему написано множество прекрасных статей и заметок в блогах, сразу же приступим к определению признаков писем, которые могут содержать конфиденциальную информацию. Такими признаками могут быть:

1. **Отсутствие темы.** Может показаться банальным, но многие сотрудники, осознавая, что совершают нарушение (пересылают важный документ на посторонний адрес), не могут подобрать этому сообщению тему.
2. **Тема сообщения не несет не никакой смысловой нагрузки**: «Привет», «***», «Re:», «Ответ», «1» и т.д.
3. **Размер вложения.** Большие файлы могут оказаться базой данных.
4. **Тип вложения** очень важен. Важные документы, это в первую очередь текст, таблицы. Особое внимание стоит уделить архивам с паролем.
5. Не только само письмо несет в себе признаки утечки информации, но и адреса, на которые оно пересылается. Если **адрес состоит из инициалов, цифр**, то, скорее всего, работник собрался поработать дома, для чего и отправляет себе документы. В этом случае необходимо смотреть, критичны ли эти документы для организации, либо стоит закрыть на это глаза и пойти навстречу сотруднику, который, чтобы сделать работу в срок, берет ее на дом. С другой стороны, когда такая пересылка документов входит в привычку, то сотрудники могут пересылать документы своим друзьям, знакомым и т. д.
6. Также стоит обратить внимание на **адреса, которые используются только одним сотрудником**. Если в организации обслуживают клиента, то ему могут отправлять информацию разные работники, часто даже сотрудники различных подразделений. Если на один адрес пишет только один сотрудник, то это либо постоянный клиент сотрудника, либо его домашняя почта, оформленная не так очевидно, как адреса, состоящие из инициалов и года рождения.
7. Также важно смотреть содержание писем. Если **письма всегда разные и их невозможно логически объединить, но они идут всегда на один и тот же адрес**, то стоит задуматься о том, что это за адрес. Вряд ли клиенту могут уходить договора по различным юридическим лицам.
8. Важно отметить, что письма, содержащие конфиденциальную информацию, часто **отправляются в нерабочее время**. Это легко объяснить – сотрудники остаются наедине со своим компьютером, никто им не мешает и никто не может посмотреть через плечо, чем

они заняты, соответственно возникает ощущение безнаказанности, вряд ли кто-то решится в разгар рабочего дня у всех на виду отправлять письмо на посторонний адрес.

Чтобы упростить задачу по поиску нежелательной почты можно принять следующие меры:

1. **Белый список адресов**: клиенты, поставщики – все, кому постоянно пишут сотрудники.
2. **Формат безопасных сообщений**. Также нужно определить сообщения, точно не несущие в себе коммерческую тайну, например, коммерческие предложения. Такие рекламные письма обычно обладают определенными признаками – это типовое сообщение. Стоит задать фильтр с текстом этого сообщения, чтобы значительно уменьшить объем просматриваемой корреспонденции.
3. **Единый формат сообщений** – классификатор тем, правила форматирования и т.д. Однако этот метод может затруднить мониторинг, так как письма, содержащие коммерческую тайну, будут надлежащим образом подписаны, и Вы уже не встретите непонятных заголовков, привлекающих внимание.
4. **Предупреждение.** Как было предложено одним иностранным журналом, можно выводить сообщения при каждой отправке письма на внешнюю почту – «Вы отправляете письмо за пределы организации и должны осознавать всю ответственность, которую на себя берете». В этом сообщении могут быть выдержки из законодательства, определяющие меру ответственности за разглашение коммерческой тайны. Если сотрудник нажимает кнопку «да», после того, как он прочитал сообщение, то можно сказать, что он был предупрежден и впоследствии нет оснований, чтобы воздержаться в отношении него крайних мер. Во многих случаях сотрудник будет напуган таким предупреждением и не станет отправлять нежелательное письмо.
5. **База ключевых слов**, куда войдут такие слова, как «отчет», «таблица», «план», «закупки», «реестр», «контракты», «контрагенты», «договора», «поставщики», «график», «ведомость», «отчет» и т.д. Чтобы составить этот список, необходимо проанализировать большое количество информации в различных структурных подразделениях, привлечь к этому анализу специалистов-экспертов для создания списка слов.
6. **Автоматизация.** Почта должна фильтроваться по содержанию, по адресам. Существуют программные решения с уже готовыми фильтрами для различных случаев: «резюме», «коммерческая тайна», «персональные данные».
7. **Настройка.** Стоит заметить, что в каждой организации существует различный порядок работы с ценной информацией и стоит разрабатывать такие фильтры самостоятельно. Даже в случае покупки готовой системы фильтрации, ее необходимо дорабатывать.
8. Неплохим средством анализа будет **сбор статистики**: количество писем в день, неделю, месяц для каждого сотрудника или отдела. Если работник отправляет в день 10-20 писем в среднем, а в один из дней пересылает сразу 100 сообщений, то это даже не признак утечки коммерческой тайны, а скорее всего результат вирусного заражения. Либо этот сотрудник чем-то недоволен и активно ищет работу и подработку на стороне.
9. **Отдельные категории лиц.** Особое внимание стоит уделить тем работникам, которые отправляют по корпоративной почте резюме, либо недовольны и собираются уволиться. Для таких сотрудников не существует правил организации, они не воспринимают себя частью компании и могут совершать нарушения, даже быть в этом заинтересованными. В случае обиды они тем более захотят компенсировать свой моральный (материальный) вред, украв какую-нибудь базу с целью продажи.