Шифровальщики атакуют

В настоящее время на территории Гомельской области участились случаи шифрования данных бухгалтерского сектора злоумышленниками, с целью последующего получения материальных выгод для расшифровки файлов.

Программы-шифровальщики относятся к классу троянцев-вымогателей – это вредоносное программное обеспечение, которое вносит несанкционированные изменения в пользовательские данные или блокирует нормальную работу компьютера. Для расшифровки данных и разблокировки компьютера злоумышленники обычно требуют денежного перевода (выкуп).

Принцип их действия заключается в поиске и шифровании найденных на компьютере файлов с определенными расширениями (для деловой сферы особенно опасны варианты вирусов, охотящиеся на файлы 1С). Затем пользователю предлагается заплатить злоумышленникам за ключ для расшифровки. Отметим, что некоторые версии вирусов могут быть реализованы таким образом, что возможность расшифровки данных не предусматривается вовсе и никак не зависит от получения выкупа. Восстановление же зараженных данных крайне сложно и не всегда возможно.

Вариантов заражения несколько:

Во-первых, прямое подключение злоумышленника к компьютеру-жертве, на котором не отключены средства удаленного управления Windows и используются легкие пароли для доступа к системе.

Во-вторых, внедрение в компьютер вируса под видом другой программы или прикрепленного к электронному письму файла. В этом случае расчет сделан на ошибку пользователя, который должен открыть или запустить такой файл. Как правило, злоумышленники маскируют адрес отправителя, в результате такое письмо может выглядеть как сообщение от известного пользователю контакта. В теме письма могут содержаться важные

сведения (например, о задолженности или возможной выгоде). К сожалению, такие вредоносные программы не всегда обнаруживаются антивирусами – значительно эффективнее меры профилактики.

Для профилактики такого вида преступлений необходимо пристальное внимание обратить на защиту деловой информации и использовать для этого резервные копии важных файлов, а также поддерживать их в актуальном состоянии. Помимо защиты от вирусов и троянских программ, данная мера позволит предотвратить потерю данных, например в случае физического повреждения исходного носителя. Резервные копии должны храниться на отдельном компьютере или внешнем носителе.

Компьютеры с критически важной информацией, в частности базами данных 1С, а также резервными копиями, не рекомендуется подключать к Интернету.

Обязательной должна стать антивирусная проверка файлов-вложений в электронных письмах. Подозрительные файлы, особенно архивы, нельзя открывать и запускать, даже если они пришли по почте от известного вам человека, поскольку адрес мог быть подменен. Совершенно недопустимо открывать подобные вложения, полученные от неизвестных отправителей.

Основываясь на вышеизложенной информации можно предложить следующие практические меры профилактического характера, рекомендуемые к исполнению на предприятиях и организациях:

1. Контроль за работой сотрудников в сети Интернет с мониторингом посещаемых ресурсов и установкой фильтров на ресурсы развлекательного характера, доступ к которым не предусмотрен служебной необходимостью (социальные сети, видео аудио хостинги, новостные ресурсы и т.п.). Избирательный подход к предоставлению доступа в сеть Интернет каждому конкретному сотруднику для выполнения своих служебных обязанностей. Обеспечение разграничения локальной сети предприятия и сети с доступом в Интернет.

2. Установка лицензионного антивирусного обеспечения на все персональные компьютеры(далее – компьютеры) работающие в сети Интернет и обеспечение своевременного обновления антивирусных баз.Установка на компьютеры, работающие в сети Интернет программное обеспечение позволяющее исключить подключение нежелательных съемных носителей.
3. Исключение использования сотрудниками личных почтовых ящиков в служебных целях. Всю служебную документацию отправлять и получать только через официальные ящики предприятия. Назначить лиц ответственных за получение/отправку электронной почты.
4. Инструктирование лиц ответственных за получение/отправку почты о необходимости проверки файлов-вложений в электронных письмах антивирусными программами до их запуска либо разархивации.
5. Архивация важных баз данных предприятия (в том числе 1С), с их записью на внешний носитель информации, должна производитсяответственным лицом, не реже одного раза в неделю.

ОРПСВТ КМ УВД Гомельского облисполкома