Гошев Павел Игоревич
доцент, канд. физ.-мат. наук
ФГБОУ ВО «Иркутский государственный университет»
г. Иркутск, Иркутская область
Корольков Юрий Дмитриевич
профессор, д-р физ.-мат. наук
ФГБОУ ВО «Байкальский государственный университет»,
ФГБОУ ВО «Иркутский государственный университет»
г. Иркутск, Иркутская область

ОРГАНИЗАЦИЯ АНТИВИРУСНОЙ ЗАЩИТЫ КАК ЭЛЕМЕНТ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Аннотация: *в работе предложена схема построения корпоративной сети, наиболее безопасная для атак извне вредоносным кодом. Рекомендованы основные мероприятия организации антивирусной защиты на предприятии, включая обучение персонала.*

Ключевые слова: *вредоносный код, корпоративная сеть, антивирусная защита, экономическая безопасность.*

Данное сообщение – перечень некоторых правил, выработанных в процессе решения задачи защиты от вредоносного кода в условиях конкретной корпоративной сети. Мы считаем организацию антивирусной защиты на предприятии элементом системы экономической безопасности, так как деструктивные функции вредоносного кода в основном предназначены для нанесения экономического ущерба, либо предполагают в итоге мошеннические схемы. Более подробно с тематикой можно ознакомиться в [1].

При налаженной работе корпоративной сети основные угрозы являются внешними в том смысле, что основным источником вредоносного кода являются съемные носители (или их эквиваленты) и сеть Интернет.

Защита от вредоносного кода должна быть эшелонированной – чем важнее информация, тем дальше от внешнего контура должны находиться компьютеры, ее обрабатывающие.

Разделение корпоративной сети

1. Отдельный сегмент сети постов антивирусной защиты для проверки всей информации, поступающей извне на внешних носителях

2. Отдельный интернет-сегмент сети для работы с Интернет.

3. Отдельный сегмент сети для внутрикорпоративной информации

4. Отдельный сегмент сети для обработки критически важной, конфиденциальной и т. п. информации.

5. Допускается ограниченное и регламентирование использование отдельными сотрудниками внешней (Интернет) почты через специальный шлюз, обеспеченный средствами защиты от вредоносного кода.

6. Антивирусный и интернет-сегменты являются периферийными и не должны быть напрямую связаны с критическим сегментом сети.

Передача информации между сегментами корпоративной сети

1. Рабочие места сотрудников не должны иметь доступа одновременно в два разных сегмента (например, в сегмент Интернет и во внутрикорпоративный сегмент).

2. Обмен информации между сегментами должен быть жестко ограничен и регламентирован. В идеале между сегментами должно быть только по одному каналу обмена информацией. Он может быть даже ручным.

Использование средств защиты

1. Для защиты от вредоносного кода должно использоваться одновременно несколько разных средств защиты (разных производителей).

2. Желательно, чтобы файловые сервера и рабочие станции обслуживались разными антивирусными средствами, чтобы обеспечить двойной контроль за обменом информации.

3. Централизованное управление антивирусными средствами и обеспечение контроля за их функционированием сразу нескольких сотрудников разных подразделений.

4. Регулярное обновление баз, регулярные проверки компьютеров.

Отслеживание состава программного обеспечения

1. Контроль за составом программного обеспечения путем фиксации его состояния на каждом компьютере и регулярных проверок.

2. Недопустимость самостоятельной установки программного обеспечения пользователями.

Обучение персонала

1. Для предотвращения попадания в корпоративную сеть вредоносного кода, в том числе еще не обнаруживаемого антивирусами, необходимо дополнительное обучение персонала, имеющего дело с внешней почтой, Интернет и информацией на внешних носителях из внешних источников.

2. Наличие специалистов для срочных консультаций в случае получения сомнительной почты, файлов и т. п.

3. «Презумпция виновности» для внешних данных – в случае сомнения данные как минимум блокируются или уничтожаются.

The research leading to these results has received funding from the People Programme (Marie Curie Actions) of the European Union's Seventh Framework Programme FP7/2007–2013/ under REA grant agreement number 609642.

Список литературы

1. Малюк А.А. Введение в информационную безопасность / А.А. Малюк, В.С. Горбатов, В.И. Королев, В.М. Фомичев, А.П. Дураковский, Т.А. Кондратьева. – М.: Горячая линия – Телеком, 2013. – 288 с.