УДК 004

ОШИБОЧНЫЕ ИДЕИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Чашленкова А.А., студентка 3 курса экономического факультета
Научный руководитель - Голубев С.В., к.э.н. доцент
ФГБОУ ВО Ульяновский ГАУ

Ключевые слова: *Информационная безопасность, технология, система, безопасность, прогресс.*

В статье рассмотрены некоторые ошибочные идеи информационной безопасности. Данная статья рассматривает моменты, на которые необходимо обратить внимание, чтобы избежать промахов и лишней траты сил.

Информационная безопасность регулярно совершенствуется – мы наблюдаем неиссякаемый поток инноваций в данной сфере. Тема безопасности вызывает общественный интерес и беспокойство, ее активно обсуждают политики, идет процесс законотворчества в области защиты персональных данных, коммерческой и государственной тайны. С каждой новой идеей проблемы, казалось бы, должны решаться, а производительность и эффективность информационных систем возрастать.

Идея «разрешить по умолчанию». Ошибочность этой идеи кроется в различных формах. На первый взгляд принцип администрирования систем информационной безопасности, основанный на «разрешениях по умолчанию» прост и привлекателен [1].

Наиболее узнаваемые формы данной идеи проявляются в правилах брандмауэра. Еще при зарождении систем информационной безопасности было решено, что при подключении к Интернету сетевыми администраторами будет ограничен входящий Telnet, Rlogin и FTP трафик. Все остальное оставалось разрешено, отсюда и название «разрешение по умолчанию». Такой подход положил началу бесконечной гонки между специалистами по безопасности и хакерами. В основном новые уязвимости обнаруживаются в службах и приложениях, которые не были сразу заблокированы по причине смутной необходимости, либо надежд администратора, что их не обнаружат и не взломают. С появлением сетевых червей принцип «разрешено по умолчанию» должен был исчезнуть навсегда, но этого не произошло. Большинство современных

сетей по-прежнему построены на идее открытого ядра, отсутствии сегментации и запрета только определенных протоколов и служб.

Подобный принцип разрешения лежит и в отношении исполняемых файлов и приложений в системах. Как правило, по умолчанию к выполнению разрешено все, что запускает пользователь, если исполнению не препятствует что-то, вроде антивируса или блокировщика шпионских программ. Разрешив исполнение только определенных файлов, можно оградить систему от вредоносного, нежелательного или игрового программного обеспечения. К сожалению, операционные системы пока еще не обучены противостоять известным атакам, старому вирусу или части программ-шпионов, не запрашивая действий пользователя [2].

Определить, что используется подход «разрешено по умолчанию» просто – в этом случае потенциальные угрозы неизвестны, информационные риски не определены, а службы безопасности вовлечены в игру на опережение хакерских атак. Противоположный подход «запрещено по умолчанию» определяет только службы, процессы или приложения, разрешенные к выполнению, и повышает уровень безопасности организации.

Идея «подсчитать угрозы». На начальных этапах компьютерной безопасности существовало относительно небольшое число известных угроз, многие из которых были связаны с принципом «разрешено по умолчанию». Когда существуют только 15 всем известных способов взломать сеть, их можно хорошо изучить и определить способы нейтрализации. Так в области безопасности появилось понятие «число угроз» – список всех потенциальных опасностей, о которых что-либо известно.

Однако, с расширением организаций, росли и размеры корпоративных сетей, появлялись сети, которые насчитывали не одну тысячу компьютеров, функционирующих под управлением различных операционных систем. И с каждым днем появлялись десятки и сотни новых экземпляров вирусов, червей, троянов и другого вида вредоносного программного обеспечения. В какой-то момент времени количество угроз достигло такого значения, что считать их стало сложно и нецелесообразно. Сейчас на первое место выступают задачи по управлению разнообразными защитными механизмами и борьбе с угрозами за счет комплексного подхода к информационной безопасности.

Явным признаком того, что в информационной инфраструктуре присутствует принцип перечисления угроз, является то, что безопасность системы основана только на решениях, требующих обновления сигнатур на регулярной основе [3].

Идея «публикация уязвимостей». Управление уязвимостями, как и обеспечение информационной безопасности, является непрерывным процессом. Создание системы управления уязвимостями позволяет управлять информационными рисками и иметь информацию обо всех активах организации.

Одним из необходимых действий по управлению уязвимостями является применение критических обновлений для устранения «дыр» в программном обеспечении. Когда приложение становится доступным из-за пределов корпоративной сети, оно может подвергнуться хакерским атакам при отсутствии обновлений и наличии известных уязвимостей. В такое приложение внедряется вредоносный код, который затем распространяется по всей корпоративной сети [4].

Недостаток идеи подробной публикаций уязвимостей заключается в том, что хотя описание уязвимости становится известным и общедоступным, многие организации по различным причинам все равно откладывают внедрение системы управления обновлениями и оставляют свои приложения потенциальными целями для хакерских атак. В это время злоумышленники могут воспользоваться опубликованной информацией и, не прилагая особых усилий, нанести вред корпоративной сети.

Библиографический список

1. Будников, С.А. Информационная безопасность автоматизированных систем: учебное пособие / С.А. Будников, Н.В. Паршин.- 2-е изд., доп.- Воронеж: Изд-во им. Е.А. Болховитинова, 2011.
2. Кияев, В. Безопасность информационных систем / В. Кияев, О. Граничин. - Национальный Открытый Университет «ИНТУИТ», 2016. - 192с.
3. Куняев, Н.Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере / Н.Н. Куняев. – Логос, 2015. - 346с.
4. Мэйволд, Э. Безопасность сетей / Э. Мэйволд.- Национальный Открытый Университет «ИНТУИТ», 2016. - 572с.
5. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. - 416с.

THE ERRONEOUS IDEAS OF INFORMATION SECURITY

Chashlenkova A.A.

Key words: *Information security, technology, system, security, progress.*

The article considers some erroneous ideas of information security. This article describes the points to which you need to pay attention in order to avoid blunders and unnecessary expenditure of energy.