ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ЛОЖНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

PERSPECTIVE DIRECTIONS OF INFORMATION PROTECTION ON THE BASIS OF FALSE INFORMATION SYSTEMS

T. Dobrzhinskaja
O. Rogova
D. Yuriev

Summary. The article discusses the relevance of application about information systems (LIS) to ensure the protection of information. Classification LIS and options for building protection with the use of FOXES. The advantages and prospects of application of LIS for the protection of information and the shortcomings of the application of LIS.

Keywords: false information system, unauthorized access, protection effectiveness, system for preventing computer attacks; false information objects; fraud systems.

Добржинская Татьяна Юрьевна
Аспирант, Дальневосточный федеральный университет, г. Владивосток
Рогова Олеся Сергеевна
Аспирант, Дальневосточный федеральный университет, г. Владивосток
kozerog1991@gmail.com
Юрьев Дмитрий Русланович
Аспирант, Дальневосточный федеральный университет, г. Владивосток

Аннотация. В статье рассматриваются вопросы актуальности применения ложных информационных систем (ЛИС) для обеспечения защиты информации. Приведена классификация ЛИС и варианты построения защиты с применением ЛИС. Отмечены достоинства и перспективы применения ЛИС для защиты информации и рассмотрены недостатки применения ЛИС.

Ключевые слова: ложная информационная система, несанкционированный доступ, эффективность защиты, система предупреждения компьютерным атакам; ложные информационные объекты; обманные системы.

Введение

В современных системах защиты информации информационных систем основным методом защиты является «стратегия запрета». С помощью средств защиты информации (системы обнаружения вторжений, межсетевой экран, антивирусные программы т.д.) устраняются уязвимости, которые находятся в базе данных этих систем и делают невозможным не санкционированный доступ (НСД). Уязвимости самих информационных систем устраняются разработкой и выпуском обновлений программного обеспечения после обнаружения этих уязвимостей.

Однако, эта стратегия неэффективна против уязвимостей «нулевого дня» — времени между появлением информации об уязвимости и выпуском обновлений программного обеспечения, когда система уязвима для НСД.

При правильной настройке системы защиты информации все же остается вероятность не выявленных уязвимостей в информационных системах и в самих средствах защиты информации. При этом актуальной становится «стратегия обмана» и перенаправление злоумышленников на ложные информационные ресурсы [5].

Применение «стратегии обмана» используется совместно с традиционными средствами защиты информации и таким образом увеличивает общий уровень защищенности информационных систем (ИС). Это достигается путем сокрытия или имитации деятельности информационных систем (или других субъектов доступа) и создания неопределенности об информации атакуемой ИС.

Системы, реализующие «стратегию обмана» называют ложными информационными системами (ЛИС).

Для обеспечения функционирования ЛИС чаще реализуется через технологии виртуализации, которые обеспечивают намного меньше вычислительных ресурсов, чем остальные технологии. Для этих целей используют программы — VMware ESX/ESXi, Microsoft Hyper-V, Citrix Xen Server и др., которые могут создавать виртуальную инфраструктуру. [10]

Отвлекая злоумышленника на ложный ресурс, можно не только предотвратить НСД, но и найти ранее неизвестные уязвимости информационных ресурсов. Злоумышленник (или вредоносная программа) взаимодействуют с эмулируемыми машинами в составе компьютерной сети и НСД не достигает своей цели. [5]

Технология ЛИС позволяет на самых ранних стадиях обнаруживать подготовку к атаке ИС, изучить поведение злоумышленника при попытке проникновения в ИС, по-

лучить информацию о новых методах атак, обнаружить ранее неизвестные уязвимости в безопасности, дезинформировать нарушителя и принять меры для их устранения. ЛИС не используются легитимными пользователями системы и находятся под контролем специалистов информационной безопасности (ИБ). В целом сокращается количество ложных сообщений и объем обрабатываемых событий ИБ, так как в системе анализируются только реальные атаки или попытки сканирования. [7]

Классификация ложных информационных систем

Согласно [8] ЛИС подразделяются:

1. По способу реализации

1.1 реальные

1.2 виртуальные

2. По типу имитируемого объекта:

2.1 генерирующие сетевой трафик;

2.2 сетевые службы;

2.3 узлы;

2.4 вычислительные сети;

2.5 автоматизированные системы.

3. По типу структуры:

3.1 статические;

3.2 динамические;

3.3 самоорганизующиеся.

4. По уровню интеграции в ИС

4.1 отдельные с ИС;

4.2 параллельные с ИС;

4.3 в составе ИС.

5. По назначению:

5.1 производственные;

5.2 исследовательские;

5.3 смешанные.

6. По уровню корреляции состава и структуры:

6.1 идентичные целевой ИС;

6.2 частично совпадающие с ИС;

6.3 отличные от целевой ИС.

Дополнительно к выше перечисленной классификации в [10] ЛИС подразделяются:

1. По типу методов реагирования:

1.1 средства сдержания;

1.2 средства отклонения (системы приманки, системы молниеотводы, системы-карантины, системы-ловушки)

2. По типу механизма обмана:

2.1 сокрытие;

2.2 камуфляж;

2.3 дезинформация.

3. По типу моделируемого компонента автоматизированной системы:

3.1 средства моделирования главной вычислительной машины;

3.2 средства моделирования сети;

3.3 средства моделирования коммуникационного оборудования.

4. По способу моделирования:

4.1 средства имитации;

4.2 средства эмуляции.

5. По уровню модели сетевого взаимодействия:

5.1 физический;

5.2 канальный;

5.3 сетевой;

5.4 транспортный;

5.5 сеансовый;

5.6 представительский;

5.7 прикладной.

6. По способу встраивания в автоматизированные системы:

6.1 внутренние;

6.2 внешние.

7. По наличию обратной связи со средствами регистрации атак:

7.1 с обратной связью;

7.2 без обратной связи

8. По способу реализации ложного информационного объекта:

8.1 клон реального объекта;

8.2 имитация уязвимых мест;

8.3 имитация сервисов;

8.4 имитация трафика.

Несмотря на обилие возможных подходов к защите с помощью ЛИС в последнее время появляются новые, например, активная защита по теории игр. Также возможно комбинирование нескольких подходов, учитывая особенности защищаемых ИС и имеющегося оборудования и программного обеспечения.

Варианты построения ложных информационных систем

Рассмотрим некоторые возможные варианты построения защиты ИС.

Рассмотрим несколько возможных вариантов ЛИС:

1. Наиболее простым вариантом считается добавление в компьютерную сеть одной или нескольких объектов ЛИС для уменьшения вероятности атаки на ИС. Недостатком такого подхода является простота –для нарушителя лишь увеличивается время на анализ атакуемых сетей (объектов).

2. Статистические ЛИС с активной защитой. Для виртуализации ИС применяются виртуальные машины, параметры которых задаются вручную при создании и впоследствии не изменяются. Поступающие запросы обрабатываются МЭ и анализируются системой

обнаружения вторжений (СОВ). К недостаткам модели можно отнести то, что злоумышленник проанализировав поведение трафика, может установить ложность системы, система неэффективна для внутренних угроз и обеспечивает защиту только известных СОВ атак.

3. Динамические ЛИС с активной защитой. В эту систему входит средство управления виртуальной инфраструктурой (СУВИ). Логические объекты СУВИ (распределенные виртуальные коммутаторы) согласуют работу всех виртуальных коммутаторов серверов в составе ИС. Средство перемещения перемещает виртуальные машины между серверами не нарушая работы виртуальной машины. Средства настройки виртуальных машин периодически меняют сетевые и MAC-адреса настоящей и ложной ИС с целью усложнения анализа трафика злоумышленником. К недостаткам динамических ЛИС можно отнести — сведения о расположении компонентов ЛИС в СУВИ, увеличение вычислительной мощности для перемещения виртуальных машин, возможность демаскировки компонентов ЛИС путем анализа команд перемещения.

4. Активная защита по теории игр. В последнее время широкое применение для обеспечения ИБ находит математический аппарат теории игр. Теория игр является подходом, предназначенным для анализа взаимодействия нескольких участников игры (сторона нападения и сторона защиты).

Различают 2 игровые модели:

1. Моделирование взаимодействия сторон для конкретной атаки (нарушитель атакует цель нападения), что позволяет определить число ЛИС и их конфигурацию.

2. Моделирование взаимодействия сторон до проведения атаки, целью которой является обнаружение ЛИС в реальной сети[5].

Для реализации своих целей игроки могут применять различные стратегии игры [4].

Заключение.

В настоящей статье рассмотрены возможные методы защиты информации на основе ложных информационных систем. Исходя из разнообразия подходов ЛИС к ИБ можно заключить, что применяемые методы на практике постоянно совершенствуются, находятся новые решения, комбинируются уже известные способы защиты ИБ.

Мировой опыт в области ИБ показывает, что эффективной может быть только комплексная система защиты информации, а ЛИС может быть включена в систему ИБ только как часть инженерно-технических решений.

Перспективными направлениями защиты на основе ложных информационных сетей следует считать активную защиту на теории игр, так как способна взаимодействовать со злоумышленником и применяя различные стратегии для реализации защиты ИС.

Кроме того целесообразно совмещать несколько методов защиты исходя из технических возможностей и особенностей защищаемых систем.

Применение системы защиты на основе ложных информационных систем в целом увеличивает затраты злоумышленника на количество выполняемых действий, появляется возможность обнаружить нарушителя в более короткий промежуток времени и принять соответствующие меры, согласно правилам ИБ.

ЛИТЕРАТУРА

1. Данилюк С.Г., Маслов В. Г. Обоснование нечеткого ситуационного подхода к созданию модели системы Обоснование нечеткого ситуационного подхода к созданию модели системы защиты информации с использованием ложных информационных объектов. Известия ЮФУ. Технические науки. 2008. № 8 (85). С. 36–41.
2. Зорин Э.Ф., Поликарпов С. В. Способы защиты информации автоматизированных систем на основе ложных информационных объектов. Космонавтика и ракетостроение. 2011. № 3 (64). С. 107–112.
3. Калашников А.О., Савенков Г. А., Красноперов А. П. Вероятностный подход к выбору стратегии защиты в условиях реализации атаки на информационную систему с применением ложной информационной системы. Информация и безопасность. 2015. Т. 18. № 4. С. 532–535.
4. Калашников А.О., Савенков Г. А. Разработка чистых стратегий ложной информационной системы и злоумышленника в антагонистической игре в условиях реализации атаки на информационную систему. Информация и безопасность. 2016. Т. 19. № 2. С. 262–265.
5. Каракашев А. В. Методика оценки защищенности информационных систем при использовании ложных информационных систем. Научный альманах. 2016. № 9–1 (23). С. 409–413.
6. Поликарпов С. В. Роль и место ложных информационных объектов в системе защиты информации вычислительных сетей. Информационное противодействие угрозам терроризма. 2010. № 15. С. 74–81.
7. Шматова Е. С. Выбор стратегии ложной информационной системы на основе модели теории игр. Вопросы кибербезопасности. 2015. № 5 (13). С. 36–40.

8. Язов Ю.К., Сердечный А. Л., Бабурин А. В. К вопросу о классификации ложных информационных систем. Информация и безопасность. 2013. Т. 16. № 4. С. 522–525.
9. Язов Ю.К., Сердечный А. Л., Бабурин А. В. Способ контроля эффективности ложной информационной системы, основанный на анализе широковещательных сетевых пакетов. Информация и безопасность. 2013. Т. 16. № 4. С. 506–509.
10. Язов Ю.К., Сердечный А. Л., Шаров И. А. Методический подход к оцениванию эффективности ложных информационных систем. Вопросы кибербезопасности. 2014. № 1 (2). С. 55–60.

Дальневосточный федеральный университет, г. Владивосток