Снедков Александр Борисович
канд. техн. наук, доцент, доцент
Верясова Надежда Викторовна
студентка
Долина Екатерина Дмитриевна
студентка
ФГБОУ ВО «Московский технологический университет»
г. Москва

ПЕРСПЕКТИВЫ РАЗВИТИЯ СРЕДСТВ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ

Аннотация: *в работе рассматриваются принципы создания комплексных систем безопасности. Определены основные задачи и предложены пути их решения. Обсуждаются вопросы интеграции разноплановых инструментальных средств обеспечения безопасности в единую структуру. Обосновывается необходимость проведения внешнего мониторинга уязвимостей систем комплексной безопасности.*

Ключевые слова: *комплексная безопасность, инфраструктура систем безопасности, технологии систем безопасности.*

Последние десятилетия показали качественные изменения требований к системам безопасности предприятий и организаций. Люди, которые атакуют информационные структуры, технологические и производственные процессы предприятий уже далеко не любознательные студенты, а квалифицированные профессионалы, работающие в специально подобранных командах. Как результат, скорость поиска и создания уязвимостей в системах безопасности превосходит скорость, с которой производители программного обеспечения и технологических систем могут закрывать эти прорехи.

Из всего спектра используемых технологий IT-технологии являются самыми как быстро развивающимися, так и самыми полиморфными [1]. Соответ-

ственно, модель нарушения системы безопасности информационной сети предприятия можно спроецировать на любую другую инструментальную систему безопасности [2]. Основное различие – в скорости реакции системы безопасности – от секунд в информационной системе до минут и часов в инструментальной системе безопасности.

В результате эволюции систем комплексной безопасности предприятий в большинстве случаев имеется сложный набор разрозненных и устаревших инструментов безопасности, которые могут не соответствовать поставленной задаче. Для выхода из образовавшегося тупика необходимо решить, как минимум пять задач.

Интеграция инфраструктуры и системы управления безопасностью.

Как правило, система обеспечения безопасности состоит из десятков элементов разных производителей, произведенных в разное время и по различным требованиям. Разнообразие элементов системы дает большее ощущение защищенности, но и ведет к проблеме разрастания системы безопасности, в которой объединение всех элементов в целостную структуру уже не представляется возможным. Единственное решение заключается в модернизации и настройке программного обеспечения системы безопасности, позволяющих достаточно эффективно управлять собственной безопасностью за счет ограниченных ресурсов. Необходимо искать точки интеграции между различными средствами защиты, чтобы сделать их более эффективными и управляемыми.

Технологии защиты слишком статичны и отстают от технологий нападения.

На наших глазах происходит быстрая мутация атак и их методов. В результате многие традиционные «статические» защитные средства, такие как системы защиты от вирусов и предотвращения вторжений на основе сигнатур (IPS), оказываются не эффективными. Объем времени, необходимый для достаточного изучения новой атаки, а затем записи, тестирования и развертывания соответствующих средств оказывается недопустимо большим. Здесь необходимо разработка адаптивных технологий, которые быстро обновляются и способны остановить атаки, ранее не известные.

Наиболее перспективным представляется внедрение в системы анализа и идентификации угроз поведенческие технологий, прогнозирующих возможные изменения алгоритмов атак. Данный вид технологий поиска угроз должен постепенно замещать традиционные статические методы в областях предотвращения вторжений и защиты от вредоносных программ.

Не имеется однозначного способа измерения эффективности обеспечения безопасности.

За последние годы предприятия вложили колоссальные средства на усиление своей позиции в области безопасности. Насколько эффективны эти инструментальные и программные средства обеспечения безопасности? К сожалению, большинство аппаратных и программных средств, используемых в настоящее время, создают ложное ощущение безопасности. Отсутствие сигналов или информации от каждого конкретного элемента системы безопасности не означает, что Вы не подвергаетесь атаке. Данная проблема может иметь только комплексное решение в виде одновременного постоянного совершенствования внутренней системы безопасности и стороннего тестирования устойчивости систем защиты.

Объем поступающей информации от систем безопасности превышает скорость ее обработки

Объем данных, генерируемых совокупностью различных элементов и датчиков и программного обеспечения систем безопасности, растет опережающими темпами по сравнению со скоростью работы самой системы безопасности. Отчасти эта проблема связана с плохой интеграцией элементов системы, но в целом задача адекватной обработки и принятия своевременного решения относится уже к области задач «big data». Если не имеется возможности понять, какие сигналы передают инструменты безопасности или не хватает времени на сведение разрозненной информации в единую картину, необходимые решения не могут быть приняты. Решения, принимаемые человеком при недостатке, избытке или противоречивости входной информации называются интуитивными. Возмож-

ность «интуитивной» работы систем безопасности пока является делом отдаленного будущего. В настоящее время необходим способ иерархической интеграции данных систем безопасности в форму, позволяющую принимать то или иное решение. Здесь основное внимание уделяется созданию «приборной панели» более высокого уровня, которая может предоставить содержательную информацию.

В большинстве систем комплексной безопасности не разработаны алгоритмы работы в чрезвычайной ситуации

Работа любой системы безопасности может быть нарушена. Это ставит две взаимосвязанные задачи – обеспечение минимизации нанесенного ущерба и документирование происходящих процессов и действий противника. Следует подчеркнуть важность комплексного плана реагирования на чрезвычайные ситуации. В этом плане должны быть указаны шаги, которые будут предприняты в случае нарушения безопасности. В дополнение к этому, инструменты обеспечения безопасности должны обеспечить систему достаточным объемом актуальных данных для проведения анализа и дальнейшей экспертизы. В этом случае необходим подробный анализ того, что произошло, перечень данных, к которым был получен доступ извне, и были ли эти данные скромпроментированы.

Список литературы

1. Кашкин Е.В. Особенности обеспечения защиты данных в информационных системах [Текст] / Е.В. Кашкин, Е.В. Малахина, И.И. Антонова // Научные исследования: теория, методика и практика: Материалы Междунар. науч.-практ. конф. (г. Чебоксары, 21 мая 2017 г.). – Чебоксары: ЦНС «Интерактив плюс», 2017. – С. 301–302.

2. Мирсаитов С.Ф. Альтернативный подход в организации многоуровневой системы контроля доступа [Текст] / С.Ф. Мирсаитов, А.В. Коротких, О.А. Чернышова // Научные исследования: теория, методика и практика: Материалы Междунар. науч.-практ. конф. (г. Чебоксары, 21 мая 2017 г.). – Чебоксары: ЦНС «Интерактив плюс», 2017. – С. 308–310.