Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

СОЗДАНИЕ РАСПРЕДЕЛЕННОГО ОПЕРАЦИОННОГО ЦЕНТРА БЕЗОПАСНОСТИ

В.В. АНИЩЕНКО

Комитет по информационной безопасности Ассоциации «ИНФОПАРК»

Введение. Как показывают результаты наших исследований: в ряде крупных белорусских организаций и ведущих банков страны существует определённый набор услуг информационной безопасности, которые они готовы получить на условиях аутсорсинга. Это обусловлено очевидными экономическими причинами – возможностью сокращения бюджета при получении качественного сервиса. В докладе рассматриваются перспективы аутсорсинга услуг безопасности через призму нормативных требований белорусского регулятора.

Аутсорсинг сервисов информационной безопасности. Информационная безопасность как провайдерская услуга для массового пользователя развивается уже более 5 лет. Наиболее известны и распространены услуги информационной безопасности от оператора связи и Интернет-провайдеров. Данные услуги относятся к классу аутсорсинговых услуг Managed Security Services (MSS).

Характерная особенность модели MSS – постоянство. Это не разовые проекты по оказанию тех или иных услуг ИБ – напротив, клиент передает сторонней организации на обслуживание постоянные функции по обеспечению информационной безопасности для своей информационной инфраструктуры.

К классу MSS относят услуги:

анализа интернет-трафика и веб-фильтрации,

защиты от спама, антивирусной защиты, контентной фильтрации трафика,

услуги защиты от DDoS-атак, а также управления – межсетевыми экранами, системами обнаружения и предотвращения вторжений,

системами аутентификации и авторизации, криптографическими системами, включая построение VPN.

Традиционный подход построения систем информационной безопасности зиждется на принципе эшелонированности, включающем три уровня обороны и обеспечивающем стратегию полной защиты по худшему сценарию:

традиционные решения - межсетевые экраны, системы обнаружения сетевых вторжений (NIDS), управление сетевым доступом (NAC), защита от распределенных атак на отказ в обслуживании (DDoS), прокси-сервера, управление динамическими сетевыми протоколами хостов - DHCP / системой доменных адресов – DNS и IP адресацией (DDI), двухфакторная аутентификация (2FA);

выполнение аудита журналов протоколирования для обнаружения и отражения атак в реальном масштабе времени;

и наконец, наиболее продвинутый рубеж, заключающийся в интеграции внешней аналитической информации о возможностях злоумышленников в системы обнаружения атак в реальном масштабе времени, что имеет важное значение для повышения эффективности и улучшения безопасности.

Реализация эшелонированной обороны требует стратегических, а не одноразовых инвестиций в один бюджетный цикл – необходимы реальные инвестиции в людей, процессы и технологии.

Могут ли предприятия и организации сегодня в стране реально удержать высококвалифицированных специалистов по информационной безопасности для разработки и внедрения эшелонированной обороны?

В какой мере на белорусском рынке имеется экспертиза по успешному внедрению систем управления инцидентами и событиями безопасности? В состоянии ли даже крупнейшие из белорусских предприятий и банков создать и эксплуатировать операционный центр информационной безопасности. Для справки: за 3 месяца в начале 2016 года работы по разработке концепции создания оперативного центра информационной безопасности Сбербанк России заплатил IBM около миллиона долларов.

А каким образом в быстро меняющейся среде ИКТ привлечь к текущей работе ведущих разработчиков продуктов информационной безопасности для оперативного осмысливания актуальной информации о преобладающих угрозах?

Предложение по управляемым услугам безопасности. Что же сегодня предлагается для реализации управляемых услуг безопасности – MSS.

Для эшелонированной обороны:

выделенные команды консультантов профессиональных сервисов, имеющих навыки и опыт работы с развертыванием решений эшелонированной обороны;

проверенные методологии проектирования SIEM систем.

Для мониторинга в реальном масштабе времени:

круглосуточный (24/7) иерархический оперативный центр безопасности (SOC), в котором работают опытные аналитики в области безопасности;

SIEM платформа поставщика услуг;

безопасный портал для взаимодействия с клиентами.

Быстрое реагирование:

интегрированный доступ к службам реагирования на инциденты Оперативного центра кибероборонь.

Внешняя информация об угрозах:

и наконец, можно получить услугу комплексного интеллектуального анализа угроз от ведущих поставщиков (например, NCC Group (UK), Fox IT (the Netherlands), имеющих качестве партнёров в Беларуси компанию Софтклуб.

Стандартный набор услуг включает: мониторинг, оповещение, реагирование, управление, ответ на запросы клиентов, взаимодействие с техподдержкой.

Оперативный центр безопасности нашего партнёра имеет собственную интегрированную аналитическую технологию мониторинга и выявления сетевых угроз от злоумышленников.

Имеются специальные индикаторы, которые ранжируют риски от традиционных известных атак неквалифицированных злоумышленников до потенциальных атак, имеющих общенациональную угрозу по своим последствиям. Последние позволяют выявлять технологии обнаружения поведенческих аномалий.

Вопрос конфиденциальности данных. Источниками данных являются:

сеть – данные формируются посредством перехвата пакетов с помощью сенсоров в целевых сегментах;

конечный пункт (end-point) – данные поступают от отдельных устройств и серверов для обеспечения предупреждения о скрытых или зашифрованных угрозах;

инфраструктура – информацией берётся из журнала протоколирования высокого уровня, путём агрегирования и анализа для обеспечения обогащенной информацией для конкретных условий и деятельности;

ложная инфраструктура – используется для активов с высокой добавленной стоимостью для обнаружения вредоносной активности;

инциденты – определяются на основе методов, тактик и процедур анализа на базе опыта SOC по реагированию на киберинциденты;

другие наборы данных – это данные, полученные от сбора, аналитической обработки и научно-исследовательской деятельности.

Предлагаемое решение проблемы конфиденциальности данных, не покидающих границы страны:

развертывание оборудования на предприятии заказчика;

поддержка частично децентрализованных сервисов на ресурсах национального партнёра;

хранение данных журналов протоколирования и конфигурирования на устройствах в стране под контролем заказчика;

передача только мета-данных (подмножества полного журнала) в зарубежный SOC, чтобы позволить генерировать сигналы тревоги и вызывать принятие различных действий для реагирования.

ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ СТАНДАРТА CVSS 3.0

М.Н. БОБОВ, Д.Г. ГОРЯЧКО

ОАО «АГАТ-системы управления» – управляющая компания холдинга «Геоинформационные системы управления»

Оценка риска информационной безопасности в общем случае определяется как комбинация вероятности угрозы и ущерба от её реализации [1].

$$R_o = P * D,$$

где R_o – показатель риска,

P – оценка вероятности реализации угроз безопасности,

D – показатель ущерба.

Последовательность выполнения работ по оценке риска показана на рисунке 1.

Как видно из рисунка оценка вероятности реализации угроз безопасности P_{vi} определяется соотношением:

$$P_{vi} = F(f_{vi}, Vul), \quad (1)$$

где f_{vi} – оценка частоты воздействия источников угроз;

Vul – оценка уязвимостей (условий реализации угроз).

Оценка частоты воздействия источников угроз f_{vi} и оценка уязвимостей Vul в настоящее время осуществляется на основе использования экспертных методов. Существует ряд систем оценки уязвимостей, которые созданы коммерческими и некоммерческими организациями, в том числе CERT/CC, системы анализа уязвимостей SANS и Microsoft. Однако, на наш взгляд, наиболее подходящим средством оценки уязвимостей для определения риска информационной безопасности эксплуатируемых информационных автоматизированных систем является стандарт CVSS [2].