УДК 004. 056

МОНИТОРИНГ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ НА МАЛОМ ПРЕДПРИЯТИИ

А.Н. ПРУЗАН, В.Л. НИКОЛАЕНКО, Г.В. СЕЧКО

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 29 октября 2015

Приведены результаты анализа данных мониторинга с помощью продукта SkyHigh инцидентов информационной безопасности в модели облачных вычислений SaaS на одном из малых предприятий. Анализ показал экономичность применения облачных вычислений для данного предприятия при одновременном обеспечении требуемого уровня защиты информации в облаках.

Ключевые слова: информационная безопасность, мониторинг, инцидент, облачные вычисления.

Введение

Облачные вычисления – это новая информационно-технологическая концепция, подразумевающая обеспечение повсеместного и удобного сетевого доступа по требованию заказчика к общему объектному пулу (англ. object pool – порождающий шаблон проектирования, набор инициализированных и готовых к использованию объектов) конфигурируемых вычислительных ресурсов (например, сетям передачи данных, серверам, устройствам хранения данных, приложениям и сервисам. Концепция позволяет заказчику заменить собственные вычислительные ресурсы потребляемыми из облака. Главным преимуществом данной концепции является отсутствие у заказчика затрат на установку и поддержку собственных вычислительных ресурсов. Архитектура облачных вычислений основана на web-технологиях, поэтому для нее актуальны угрозы, связанные с уязвимостями сетевых протоколов, серверов приложений и операционных систем (ОС). В облачных вычислениях мониторинг небезопасных событий, происходящих внутри системы, обеспечивающей работу облака, практически всегда автоматизируется. Инциденты фиксируются на уровне приложений или аппаратуры, и их обнаружение и внесение в единый реестр инцидентов информационной безопасности (ИБ) является чисто технической процедурой [1].

Методика эксперимента

На предприятии ООО «Стримцентр», где практически все программные приложения перенесены в облака, в зависимости от необходимости используются все три основных облачных варианта (три модели) применения информационных технологий (ИТ) в облаках – IaaS (инфраструктура как сервис), PaaS (платформа как сервис) и SaaS (софт как сервис). Модель SaaS (Software as a Service) используется чаще других. Мониторинг инцидентов ИБ в модели SaaS проводится с помощью программного продукта SkyHigh компании Salesforce.com. На рис. 1 показано окно продукта SkyHigh, позволяющее инженеру техподдержки оперативно подучать сведения об инцидентах ИБ.

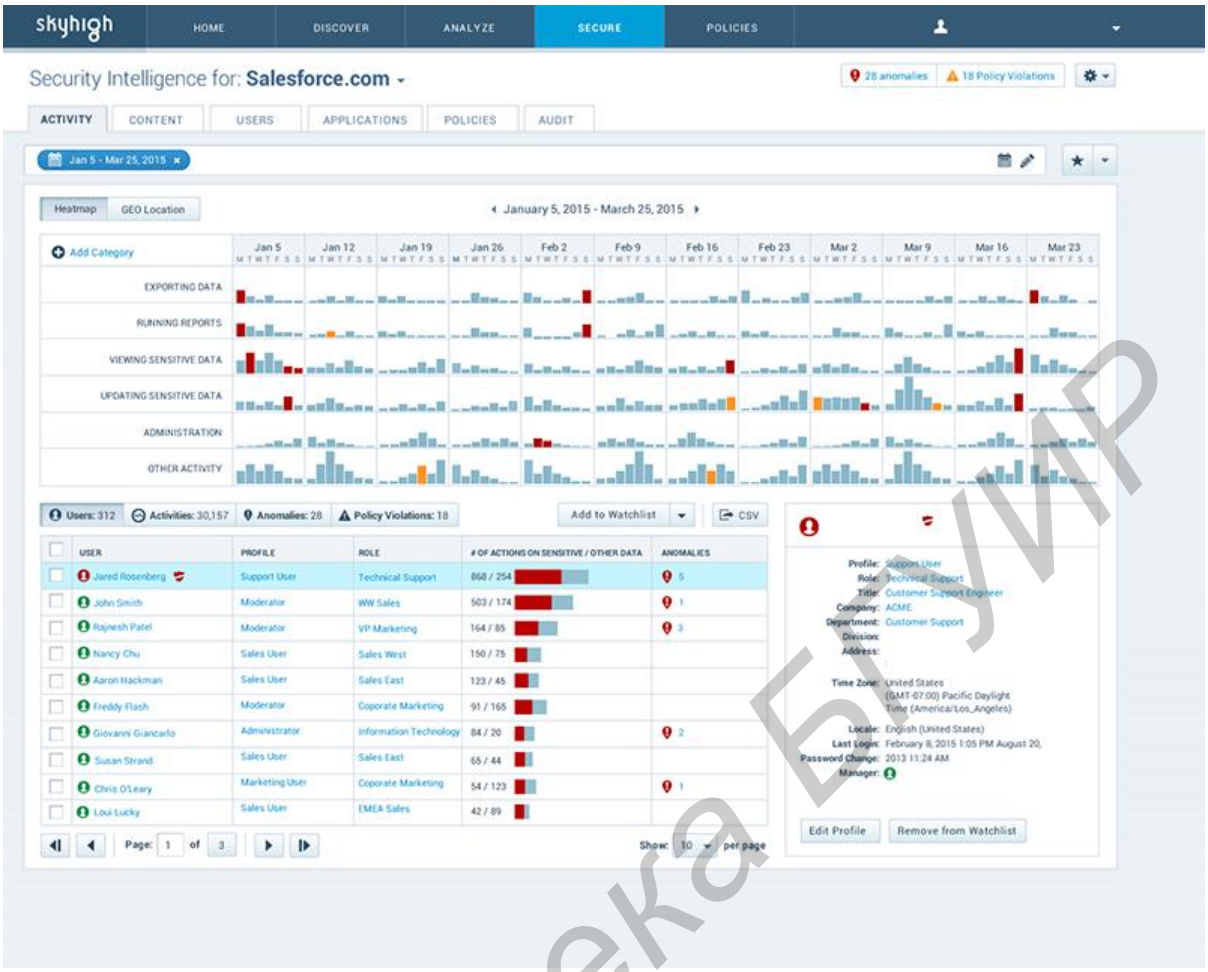

Рис. 1. Окно программного продукта SkyHigh

Продукт SkyHigh дает возможность вести мониторинг инцидентов ИБ в модели SaaS, возникающих от воздействия пяти основных видов угроз:

– угрозы от несанкционированных сторонних приложений; мониторинг приложений кроме блокирования запуска запрещённых для конкретного пользователя программ выполняет контроль целостности программ, которые разрешено запускать на данном компьютере, что полностью блокирует распространения любого злонамеренного ПО, выполняющего модификацию исполняемых файлов;

– угрозы от привилегированных пользователей; собственные привилегированные пользователи (например, администраторы и др.) могут допустить неквалифицированные либо злонамеренные действия в части защищенности информации и поддерживающей инфраструктуры при работе в облаках;

– угрозы, связанные с изменением архитектуры;

– угрозы из взломанных аккаунтов; здесь имеется в виду взлом учетных записей к облачным сервисам;

– угрозы от уволившихся сотрудников: часть сотрудников, покинувших или потерявших свои рабочие места, долго могут держать у себя конфиденциальные корпоративные данные и использовать их на своих новых рабочих местах.

Результаты и их обсуждение

Результаты проведенного на предприятии ООО «Стримцентр» мониторинга с помощью продукта SkyHigh инцидентов ИБ в модели SaaS показали, что наиболее значимой причиной возникновения инцидентов в течение 2014 г. стала угроза информационной безопасности от уволившихся сотрудников. Для парирования этой угрозы в политику безопасности предприятия ООО «Стримцентр» в 2015 г. внесены изменения, которые позволили

предприятию сократить на 44 % число инцидентов ИБ, вызванных вышеуказанной угрозой. Работа по совершенствованию политики безопасности предприятия ООО «Стримцентр» продолжается. Парирование других угроз ИБ ведется способами, изложенными в [2, 3].

Заключение

Годичный опыт использования на предприятии ООО «Стримцентр» мониторинга с помощью продукта SkyHigh инцидентов ИБ в модели SaaS показал экономичность применения облачных вычислений для данного малого предприятия при одновременном обеспечении требуемого для ООО «Стримцентр» уровня защиты информации в облаках.

MONITORING OF INFORMATION SECURITY INCIDENTS IN THE CLOUD COMPUTING AT SMALL BUSINESS

A.N. PRUZAN, V.L. NIKOLAENKO, G.V. SECHKO

Abstract

Monitoring results of SkyHigh product are presented. This product has been used to analyse the incidents of information security in SaaS cloud computing model in one of the companies. Analysis showed economical use of cloud computing for the given company while also ensuring the needed level of data security in the cloud.

Список литературы

1. *Николаенко В.Л., Прузан А.Н., Сечко Г.В. и др.* // Сб. статей III Междунар. заоч. НПК «Информационные системы и технологии: управление и безопасность». Тольятти, декабрь, 2014. С. 209–215.
2. *Прузан А.Н., Николаенко В.В.* // Матер. XVIII Междунар. науч.-техн. конф. «Современные средства связи». Минск, 15–16 октября 2013 г. С. 176–177.
3. *Прузан А.Н., Николаенко Е.В., Таболич Т.Г.* // Матер. XX МНТК «Информационные системы и технологии» (ИСТ–2014). Нижний Новгород, 18 апреля 2014 г. С. 268.