УДК 004.4
DOI: 10.18101/978-5-9793-1397-9-75-81

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. РЕШЕНИЯ НА ПРИМЕРЕ ПРОДУКТОВ ПАО «РОСТЕЛЕКОМ»

© **Макшанова Лариса Михайловна**
кандидат технических наук, доцент,
Бурятский государственный университет имени Доржи Банзарова
Россия, 670000, г. Улан-Удэ, ул. Смолина, 24а
E-mail: lorimak@list.ru

© **Мангадаева Юлия Степановна**
бакалавр,
Бурятский государственный университет имени Доржи Банзарова
Россия, 670000, г. Улан-Удэ, ул. Смолина, 24а
E-mail: mangadaeva@mail.ru

В статье рассматривается проблема киберпреступности и средства информационной безопасности как пути ее решения. Приводятся типы кибератак на предприятия и государственные структуры. Описаны средства информационной безопасности на примере продуктов ПАО «Ростелеком», их возможности и результаты применения.

Ключевые слова: информационная безопасность; проблема киберпреступности; ПАО «Ростелеком»; хакерские атаки; защита информации; хакерство; фишинг; DDos-атаки.

Введение

В эпоху телекоммуникационных технологий и тотальной цифровизации информации во всех сферах жизни — образовании, бизнесе, властных структурах, развлечениях и так далее — появилась такая проблема, как киберпреступность. Чем сложнее сфера, тем более изощренно действуют преступники. С возрастающей цифровизацией всех областей жизни растут возможности и масштабы киберпреступлений. Сейчас преступники не ограничиваются простыми манипуляциями в сети вроде взлома страниц. Хакерам высокого уровня не составляет труда нанести урон крупным компаниям и шантажировать их, взламывать правительственные базы, обнародовать компрометирующую информацию, не говоря уже о воровстве денег со счетов (фишинге) и прочих преступлениях (рис. 1) [1].

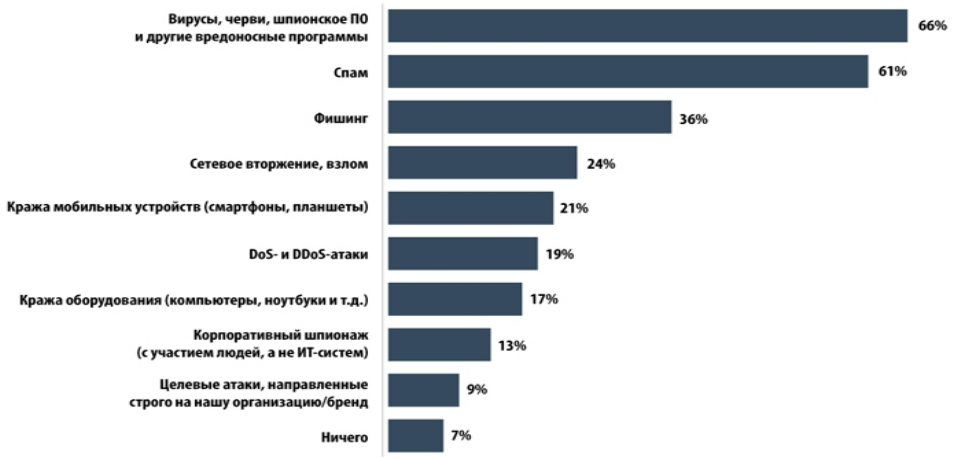

Рис. 1. Типы кибератак в корпоративном секторе

Поскольку сегодня данная проблема стоит остро, появилось такое направление деятельности, как информационная безопасность. Это целый спектр средств защиты от хакерских атак, а также непрерывная работа специалистов, которые адаптируют защиту для отражения и предупреждения возможности взломов, повреждений и краж информации, установки вредоносного программного обеспечения, промышленного шпионажа и прочих противоправных действий [2].

В России действует федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 9 августа 2006 г. В нем описаны основные понятия и определения в области информационных технологий, принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации, а также регулирования отношений при осуществлении права на поиск, получение, передачу, производство и распространение информации с помощью информационных технологий. Существуют и национальные стандарты в области информационной безопасности — это Перечень государственных стандартов Российской Федерации в области защиты конфиденциальной информации и персональных данных. Этот документ регламентирует, например, работу с информацией о получении гражданами каких-либо государственных услуг либо медицинской помощи. Все мы заполняли соглашение на обработку персональных данных в поликлинике или другом учреждении/компании [3]. Безусловно, есть еще ряд других документов, которым подчиняется вся структура информационной безопасности в России. В данной статье рассмотрим средства информационной безопасности на примере продуктов компании «Ростелеком». У этой телекоммуникационной компании существует целое направление по осуществлению информационной безопасности, и она является национальным провайдером сервисов и технологий кибербезопасности в России.

В основе технологий компании лежит понимание, что настоящая информационная безопасность возможна только через непрерывный мониторинг и удобное управление системами информационной безопасности. Этот принцип реализован в продуктах и сервисах «Ростелекома». Среди клиентов организации есть как государственные учреждения, так и бизнес-гиганты российского рынка — надежная защита в киберпространстве, безусловно, нужна всем.

Рассмотрим подробно и максимально доступно решения, которые разработала данная компания.

Безопасность из облака (ЕПСК) — это набор сервисов по информационной безопасности, предназначенных для защиты информационной инфраструктуры и приложений заказчиков от различных сетевых угроз и вредоносного ПО. ЕПСК применяется для защиты периметра информационных систем и приложений, расположенных на площадках заказчика либо размещенных в облаке: межсетевое экранирование, обнаружение и предотвращение вторжений, мониторинг и реагирование на инциденты нарушения ИБ (информационной безопасности), защита от атак на веб-приложения, фишинговых атак, защита электронной почты, контроль приложений, антивирусная защита, защита от DDoS атак [4].

Универсальный шлюз безопасности (UTM) — услуга предназначена для снижения вероятности реализации актуальных для клиента сетевых угроз и предполагает наличие опций:

- межсетевое экранирование на уровне сети (FW);
- межсетевое экранирование на уровне сети и обнаружение/предотвращение вторжений (FW + IPS);
- комплексное решение (UTM), включающее в себя межсетевое экранирование на уровне сети, обнаружение/предотвращение вторжений, фильтрацию трафика веб-приложений, контроль использования приложений, а также защиту от вредоносного ПО [4].

Мониторинг и реагирование на инциденты нарушения ИБ — услуга предназначена для выявления нарушения информационной безопасности в инфраструктуре заказчика и последующего реагирования на них с целью нейтрализации ущерба. В рамках сервиса SOC обеспечивается принятие проактивных мер, направленных на предотвращение нарушения ИБ, обнаружение актуальных угроз и атак, реагирование на них раньше, чем будет оказано влияние на работоспособность и деятельность информационных систем заказчика.

Возможности данного решения:

- выявление и реагирование на случаи нарушения ИБ в режиме 24x7 с целью обеспечения защищенности конфиденциальной информации и сети заказчика;
- повышение устойчивости к киберугрозам за счет применения проактивных мер обеспечения ИБ по мере выявления новых атак или уязвимостей;
- выявление и нейтрализация непреднамеренной нежелательной активности или действий, носящих криминальных характер;

- получение бизнес-аналитики поведения пользователей в сети заказчика с целью формирования и определения приоритетов в стратегии развития ИТ-систем заказчика.

Защита от DDoS — анализ интернет-трафика в адрес клиента и защита ресурсов от DoS- и DDoS-атак посредством фильтрации этого трафика. В результате происходит снижение риска как косвенных репутационных потерь, так и прямых финансовых потерь (в связи с невозможностью осуществления прямой деятельности) в случае недоступности или ограниченной функциональности интернет-ресурсов[1].

Security Awareness — это облачный сервис по оценке и формированию устойчивых навыков ИБ у сотрудников. Заказчику предоставляется доступ к личному кабинету платформы для самостоятельной работы либо разовая услуга по оценке персонала.

Такой сервис необходим прежде всего для сотрудников, ведущих активную переписку с внешними контрагентами, а также для всех остальных сотрудников с доступом к важной информации. Результатом его использования является снижение риска финансовых потерь из-за ошибок персонала в распознавании атак злоумышленников через фишинговые письма и сайта[2].

Аттестация информационных систем — это мероприятия по оценке соответствия информационных систем требованиям законодательства по защите информации. Итогом оказания услуги является аттестат соответствия. Услуга необходима для информационных систем, расположенных на площадках заказчика или размещаемых в облаке, в случаях, если:

- в системе обрабатываются персональные данные;
- информационная система имеет статус государственной или муниципальной;
- в системе обрабатывается информация, содержащая служебную тайну.

Услуга позволяет заказчикам подтвердить выполнение требований законодательства по защите информации[3].

Тестирование на проникновение (pentest) — консалтинговая услуга для оценки уровня защищенности инфраструктуры и приложений организации. По результатам выполнения оценки предоставляются отчет об обнаруженных уязвимостях и рекомендации по их устранению.

Результаты оказания услуги позволяют как оценить эффективность уже выполненных инвестиций в ИБ, так и выбрать приоритетные направления для новых инвестиций[4].

Защита веб-приложений (WAF)

Web Application Firewall (WAF) — межсетевой экран уровня приложений, позволяющий детектировать и блокировать атаки, направленные на веб-приложения.

---

[1] Описания продуктов ИБ ПАО «Ростелеком» : пособие для сотрудников. М., 2018. 6 с.
[2] Там же.
[3] Там же.
[4] Там же.

WAF позволяет создавать правила, которые способствуют защите от таких распространенных сетевых угроз, как внедрение SQL-кода или межсайтовый скриптинг. Услуга используется для защиты веб-приложений, расположенных на площадках заказчика или размещенных в облаке.

Услуга обеспечивает следующий функционал: фильтрацию сетевого трафика веб-приложений клиента на стороне оператора с целью его анализа на прикладном уровне; создание индивидуального профиля защиты для каждого веб-приложения клиента; обучение и настройку WAF для обеспечения корректной фильтрации трафика; корректировку индивидуальных профилей защиты в случае выявления некорректных срабатываний; изменения состава веб-приложений, в том числе по запросу клиента (рис. 2).

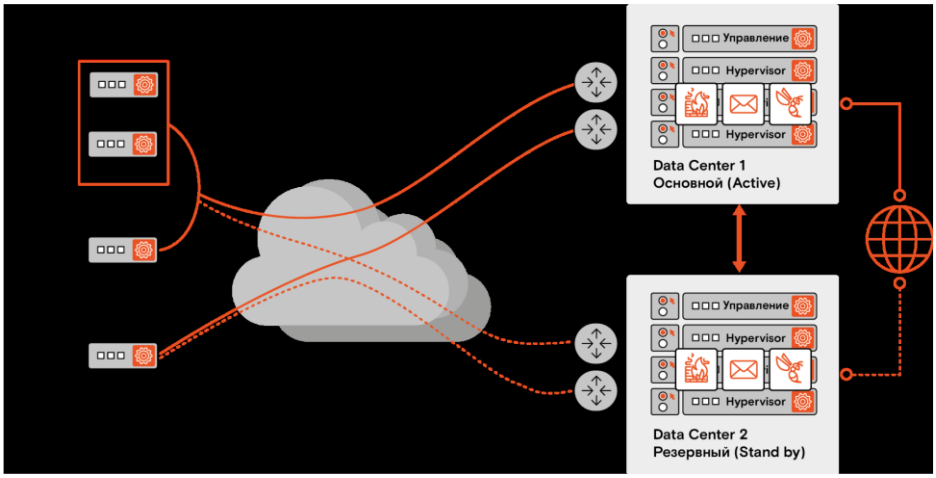

Рис. 2. Схема функционирования услуг по информационной безопасности

Анализ защищенности — облачный сервис по инструментальной оценке защищенности IT-активов предприятия. Заказчик может выбрать либо готовый отчет по сканированию требуемых узлов, либо доступ к личному кабинету платформы для самостоятельного сканирования узлов. Регулярное получение отчета по защищенности нужного количества узлов с определенной периодичностью для своевременного устранения критических уязвимостей является экономически эффективным процессом (рис. 3)[1].

[1] Описания продуктов ИБ ПАО «Ростелеком» : пособие для сотрудников. М., 2018. 6 с.

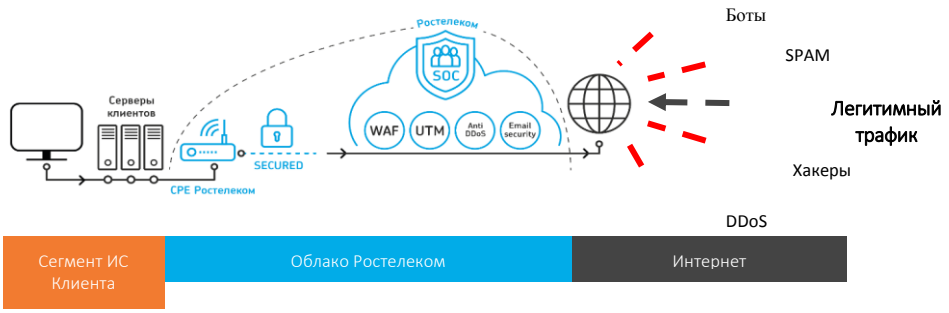

Рис. 3. Схема подключения услуг по информационной безопасности.

Заключение

Таким образом, понятно, что основной целью всех мероприятий и сервисов информационной безопасности является недопущение утечки, повреждения, раскрытия или неправомерного использования конфиденциальной информации, а также защита от проникновения злоумышленников в охраняемую информационную систему.

С ростом киберпреступности развиваются направления информационной безопасности, причем не просто пропорционально, а с опережением, предупреждая возможность совершения такого рода преступлений, целью которых зачастую являются шантаж, обогащение, получение контроля над деятельностью, нанесение урона репутации атакуемых организаций либо людей.

Литература

1. Запечинков С. В. Информационная безопасность открытых систем : в 2 т. М. : Изд-во ГЛТ, 2006. Т. 1. 536 с.

2. Гришина Н. В. Информационная безопасность предприятия : учеб. пособие. М. : Форум, 2017. 159 с.

3. Шаньгин В. Ф. Информационная безопасность и защита информации. М. : ДМК, 2014. 702 с.

4. Ярочкин В. И. Информационная безопасность : учебник для вузов. М. : Академический проспект, 2008. 544 с.

INFORMATION SECURITY. SOLUTIONS ON THE EXAMPLE OF ROSTELECOM PRODUCTS

Larisa M. Makshanova
Cand. Sci. (Engineering), Senior Lecturer,
Dorzhi Banzarov Buryat State University
24a Smolina St., Ulan-Ude 670000, Russia
E-mail: lorimak@list.ru

Yuliya S. Mangadaeva
Bachelor,
Dorzhi Banzarov Buryat State University
24a Smolina St., Ulan-Ude 670000, Russia
E-mail: mangadaeva@mail.ru

The article deals with the problem of cybercrime and means of information security as a way to solve it. Types of cyber attacks on enterprises and government structures are given. Information security tools are described on the example of PJSC Rostelecom products, their capabilities and the results of their work.

Keywords: information security; the problem of cybercrime; Rostelecom Solar; hacker attacks; information protection; hacking; phishing; DDos attacks.