УДК 338.5:621.395.7

54. КИБЕРБЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ В ИНФОКОММУНИКАЦИОННОМ БИЗНЕСЕ

Дундер Н.А.[1], Гулевич Д.О.[1], студенты гр. 172301

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Ермакова Е. В. – канд. эконом. наук

Аннотация. В современном мире наблюдается стремительный рост числа киберугроз. Новостные ленты мировых СМИ ежедневно сообщают о новых инцидентах. Бизнес и госструктуры пытаются выстоять под шквалом атак, хакеры опустошают банковские счета простых граждан, и поэтому надежная защита от угроз цифрового мира становится базовой потребностью. В данной работе исследуются особенности кибербезопасности в инфокоммуникационном бизнесе.

Ключевые слова. Кибербезопасность, CISCO, HP, Security инфокоммуникационный бизнес.

При решении задач организации управления современной инфокоммуника-ционной сетью специального назначения необходимо учитывать требования по обеспечению безопасности, так как существует достаточно большая вероятность преднамеренного неправомерного вторжение в сеть из внешней среды, которое выполняется как с целью несанкционированного использования ресурсов (для хищения информации), так и с целью нарушения её работоспособности.[1]

Поэтому, без использования соответствующих средств защиты информации и реализации соответствующих механизмов защиты формируются «слепые зоны», а компании сталкиваются с необходимостью устранения большого количества потенциальных уязвимостей в различных платформах.

В основном предприниматели воспринимают ситуацию спокойно: 67% от всех предпринимателей — отметили, что не сталкивались с угрозами информационной безопасности за прошедшие 12 месяцев.[2] Однако это не означает, что компании действительно не сталкивались с такими угрозами: зачастую последствия взлома дают знать о себе далеко не сразу. В частности, трояны и бэкдоры могут годами работать незаметно, чтобы активизироваться в самый удобный для злоумышленника момент.[3]

Среди наиболее распространенных угроз, которые все же были зафиксированы, заражение рабочих компьютеров вирусами (16,1%), атаки на сайт (15,9%) и поломка оборудования с остановкой работы сайта (9,2%). Реже всего сталкивались с утечками корпоративных данных из-за ошибок сотрудников (2,7%), интернет-мошенничества (2,3%) и взлома хранилищ корпоративных данных (1,4%) [4].

К сожалению, на уровне малых и средних предприятий характерной является ситуация, когда между техническими и коммерческими руководителями организации-клиента существует коммуникационная пропасть. Компания Cisco разработала специальный набор решений для бизнеса коммуникаций и бизнес-план по их внедрению (Smart Business Roadmap), позволяющий предприятиям заполнить этот пробел. Решения компании Cisco для бизнес-коммуникаций предоставляют организациям «интеллектуальную» платформу; при этом интеллект закладывается на уровне элементов информационной системы. Такие решения обеспечивают безопасный, быстрый и гибкий доступ к данным компании — в любое время и из любой точки мира — что позволяет выстраивать более эффективные коммуникационные процессы как внутри компании, так и с поставщиками и заказчиками.

Архитектура решений компании Cisco для бизнес-коммуникаций (рисунок 1) задает направления развития информационных систем предприятия. [5] В этой архитектуре предусмотрены два уровня: уровень интегрированной защищенной сети (с внедренными сервисами интеллектуальных механизмов коммуникации) и уровень приложений, предусмотренный для ускорения внедрения и повышения производительности работы системы. Оба уровня поддерживаются специализированными партнерами Cisco в ходе разработки, внедрения или обслуживания информационных систем

Рисунок 1 - Архитектура решений компании Cisco для бизнес-коммуникаций

Бизнес-план Cisco Smart Business Roadmap (рисунок 2) позволяет достигать поставленных перед компанией целей путем правильного выбора стратегии технологического развития. Совместная работа с партнером Cisco приводит к подготовке согласованного плана, который ориентирован на решение текущих проблем и обеспечивает надежную работу систем в течение длительного времени. План предполагает поэтапное внедрение в удобном для организации темпе и помогает сформировать долговременные взаимоотношения с партнером Cisco.

Рисунок 2 – Бизнес-план Cisco Smart Business Roadmap

Используя бизнес-план, предложенный компанией Cisco, малые и средние предприятия смогут более системно и рационально управлять инвестициями в технологии, и получать высокую отдачу от капиталовложений.

Компании, которые находятся на этапе создания испытывают необходимость в построении более эффективных процессов коммуникации как внутри компании, так и с поставщиками и заказчиками. Возможно, они также рассматривают варианты предоставления более простого и полного доступа к информации для своих сотрудников и заказчиков используя web-технологии (размещая информацию на внешних и внутренних web-сайтах, интенсивно используя средства электронной почты и т.п.).[6] Таким образом, на этапе создания организации находятся в поиске технологического фундамента, который позволит им работать более эффективно, повысить качество предоставляемых клиентам услуг, и одновременно обеспечить сохранность важной информации.

Cisco Security Agent – программный продукт, обеспечивающий комплексную защиту серверов и персональных компьютеров, сочетает в себе. Программное обеспечение устанавливается на компьютер или сервер и обнаруживает, а также предотвращает действия злоумышленников еще до их осуществления. Это позволяет эффективно противостоять как известным, так и неизвестным атакам, угрожающим компьютерным сетям и приложениям.[7]

Еще одним решением по обеспечению безопасности является - HP Sure Click Pro — это адаптированная к потребностям малого и среднего бизнеса версия пакета HP Sure Click Enterprise, ориентированного на корпорации и государственные учреждения. Главное его предназначение — защита от фишинговых атак, которые производятся через браузеры, когда пользователя тем или иным способом заставляют открыть ведущую на вредоносный портал ссылку. HP Sure Click Pro реализует принципиально новый подход к обеспечению безопасного поиска в Интернете: не просто помечает потенциально угрожающие сайты как нежелательны, но препятствует заражению других вкладок и всей системы вредоносным ПО, программами-вымогателями и вирусами. Отдельный экземпляр HP Sure Click Pro запускается для каждой веб-ссылки, на которую переходит пользователь. Он защищает пользователей даже от заражённого вредоносного ПО, скрытого в документах Microsoft Office и PDF-файлах. Вирусный код в этом случае точно так же будет изолирован на аппаратно-программном уровне, что не позволит распространить заражение за пределы активного в данный момент контейнера.

После анализа двух решений для обеспечения безопасности в инфокоммуникационном бизнесе можно сказать что:

Cisco Security Agent (CSA) обеспечивает функции анализа и обнаружения в реальном времени, интегрируется с другими продуктами безопасности Cisco и предлагает комплексный подход к безопасности. Он может быть хорошим выбором для организаций, которые уже используют другие продукты Cisco и хотят обеспечить согласованность и совместимость в своей сетевой инфраструктуре.[8]

HP Pro Security Edition, с другой стороны, является пакетом безопасности, предназначенным для обеспечения безопасности серверов и рабочих станций. Он включает различные компоненты безопасности и может быть привлекательным выбором для организаций, которые предпочитают использовать продукты Hewlett Packard Enterprise и имеют специфические потребности в области безопасности рабочих станций и серверов.

В итоге, необходимо учесть требования вашей организации перед принятием окончательного решения о выборе между Cisco Security Agent и HP Pro Security Edition.

Список источников

1. Решения CISCO для бизнеса [Электронный ресурс] – Режим доступа https://www.cisco.com/c/dam/global/ru_ua/assets/downloads/cs4b.pdf – Дата доступа 25.02.2024.

2. Обзор "Средства защиты информации и бизнеса" [Электронный ресурс] – Режим доступа https://detsys.ru/article/sredstva_zashit_inform - Дата доступа 25.02.2024.

3. HP Inc.: кибербезопасность как приоритет — при работе из дома и не только [Электронный ресурс] – Режим доступа https://www.itweek.ru/security/article/detail.php?ID=212304 - Дата доступа 25.02.2024.

4. Пинчук, Т. Г. Исследование операций в экономике: учеб. -метод. пособие / Т. Г. Пинчук, С. А. Поттосина. – Минск: БГУИР, 2017. – 115 с.: ил.

5. Живицкая, Е. Н. Теория принятия решений в экономических исследованиях: учебное пособие / Е. Н. Живицкая. – Минск: БГУИР, 2017. – 294 с.

6. Беляцкая Т. Н. Формирование стратегических конкурентных преимуществ в электронной экономике // Конкурентные преимущества экономики Республики Беларусь в условиях модернизации: моногр. / А. А. Быков, Е. И. Велесько, Т. Н. Беляцкая [и др.]; под ред. А. А. Быкова и М. И. Ноздрин-Плотницкого. - Мисанта, 2014.

7. Орлова Е.И. К вопросу защиты чести, достоинства, деловой репутации физических и юридических лиц в сети Интернет. // Детерминанты развития малого и среднего предпринимательства в Республике Беларусь: сборник материалов XX Международной научно-практической конференции (Минск, 19 мая 2023)/ редкол.: В.Л.Цыбовский (гл.ред.) [и др.], - Минск: Ковчег, 2023.- 150 с. - С.37 - 41.

8. Насонова, И. В. Переход к цифровой экономике: перспективы и риски. /И.В. Насонова//Гермес -2022.- № 5 - С. 34-37