В. О. САНЬКО
(г. Гомель, Гомельский государственный университет имени Ф. Скорины)
Науч. рук. **О. Е. Корнеенко**

СРЕДСТВА ОБЕСПЕЧЕНИЯ КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ БИЗНЕСА

Конфиденциальная информация в настоящее время имеется практически в каждой организации. Личные данные сотрудников, интеллектуальная собственность самой организации, торговые и технические секреты – всем этим данным может грозить опасность разглашения или утечки, и практически перед каждым субъектом хозяйствования стоит задача их защиты.

Для обеспечения всестороннего контроля над оборотом конфиденциальной информации в корпоративной сети используется два класса продуктов. Один позволяет управлять правами доступа к информации в масштабах организации (Enterprise Rights Management, ERM), а второй служит средством по выявлению и предотвращению утечек конфиденциальных данных (Information Leakage Detection and Prevention, ILD&P). Эти классы решений оба служат для обеспечения безопасности конфиденциальных данных, но продукты в сфере ERM защищают информацию от несанкционированного доступа, а ILD&P-продукты – от утечки, уничтожения и искажения при полностью санкционированном доступе к ней. Иначе говоря, это две разные категории продуктов, которые позволяют построить защиту от двух разных типов угроз IT-безопасности.

И, как показывает практика, основная угроза, подстерегающая пользователей корпоративных систем, заключается в отсутствии у большинства из них общей стратегии обеспечения информационной безопасности. А это влечет за собой непонимание рисков для бизнеса с точки зрения потери информации, отсутствие моделей угроз, отсутствие категорирования информации по важности и доступу, отсутствие регламентов реализации своей активности сотрудников и т.п. Отсутствие общей стратегии обеспечения IT-безопасности в первую очередь не позволяет пользователям корпоративных систем строить эффективную систему защиты своих интересов. Это негативно отражается на ведении бизнеса и возможностях получения высоких результатов.

Какие проблемы обеспечения корпоративной IT-безопасности представляются наиболее актуальными для руководителей субъектов хозяйствования в настоящее время и каких новых проблем им следует ожидать в ближайшем будущем.

Прежде всего стоит отметить, что руководители информационных служб не всегда несут ответственность за обеспечение IT-безопасности – зачастую это является обязанностью специальных структур, которые могут входить в общую службу безопасности.

Также одной из основных проблем является нехватка квалифицированных кадров, имеющих специальные компетенции. В стране есть специалисты, которые технически хорошо подготовлены для обеспечения IT-безопасности. Сложность заключается в поиске среди них тех, кто знает особенности построения и функционирования бизнеса, кто умеет формировать решения, основываясь на минимизации возможных рисков. Подобные задачи являются проблемами наивысшей сложности, а специалисты, способные их устранить, на вес золота. В настоящее время уже недостаточно знать, как выстроить решение. Необходимо уметь обосновать то, зачем данное решение следует строить и почему это следует делать именно так. При этом, на вопросы «зачем» и «почему» нужно отвечать только думая о бизнесе.

Самой распространенной ошибкой, которую совершают сисадмины и руководители информационных служб при организации защиты корпоративных информационных ресурсов от вредоносного программного обеспечения (ПО), прежде всего, является нерегулярное обновление основного ПО. Оно защищается антивирусными и другими программными средствами, и все привыкли к тому, что эти базы надо обновлять очень часто. Но обновление операционных систем, баз данных и приложений в нашей стране по-прежнему является необязательным. А ведь именно обновления основного ПО направлены на ликвидацию обнаруженных потенциальных уязвимостей, которыми пользуются злоумышленники. Сначала необходимо позаботиться об обновлении основного ПО, а уж потом заняться антивирусными или антишпионнскими инструментами.

Одним из антивирусных и антиспамовых продуктов, к слову, является Microsoft Antigen [1]. Основной его целевой аудиторией являются корпоративные пользователи, так как Antigen предназначен для серверов. Antigen имеет уникальную особенность проверять информацию в режиме реального времени. При этом он обрабатывает ее параллельно на 9 антивирусных ядрах разных независимых производителей (CA, Sophos, «Лаборатория Касперского», Microsoft и др.). Учитывая это, следует отметить, что данное решение ориентировано на разные по масштабу организации, включая как небольшие, так и крупные.

На наш взгляд руководителям следует также задуматься над тем, каких продуктов и решений не хватает для решения проблем безопасности и в чем заключается причина их отсутствия. Как правило, в современном бизнесе не хватает автоматизированных систем (например, роботов с искусственным интеллектом) для автоматического обеспечения задач IT-безопасности. А причина их отсутствия состоит в том, что человек является активно развивающимся созданием, и придуманные им проблемы пока еще может решать только он сам. И это хорошо. Значит, у нас, у людей, есть будущее.

Список использованной литературы

1 Ежемесячный компьютерный журна « КомпьютерПресс» [Электронный ресурс] / Официальный сайт. – 2021. – Режим доступа: https://compress.ru/. – Дата доступа: 16.01.2021.