УДК 004.056

Самойлов Д. В.
аспирант
ГОУ ВО ЛНР «ДонГТИ», г. Алчевск, ЛНР

ПРОБЛЕМАТИКА ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

Любая современная организация в той или иной степени использует информационные технологии в своей работе, и с каждым годом их роль только возрастает. В цифровом виде хранят важную и ценную документацию, доступ на производственные объекты регулируют электронные системы контроля и управления доступом (СКУД), а электронная почта позволяет быстро обмениваться сообщениями между сотрудниками из разных подразделений. Как следствие, существует отдельная категория злоумышленников, специализирующихся на атаках цифровой корпоративной собственности.

Подобные атаки могут быть направлены на организацию извне, они еще называются внешними атаками, или изнутри, совершаемые сотрудниками с легальным доступом к этой информации (инсайдерами) [1].

Внешние атаки являются наиболее распространенным способом атак на информационную систему предприятия, но атаки инсайдерами сложнее предотвратить, так как им известна внутренняя структура информационной системы, а также проще получить доступ к закрытой информации [2].

Кибератаки — покушение на информационную безопасность компьютерной системы — на предприятия серьезно отличаются от распространенных в интернете атак на обычных пользователей. Эти два вида атак можно классифицировать как целевые и нецелевые атаки.

К нецелевым атакам можно отнести:

– массовое распространение вредоносного ПО;

– создание ботнетов — компьютерных сетей ботов;

– спам — массовая навязчивая рассылка сообщений, или рекламы.

Цели злоумышленников, занимающихся подобными атаками, редко заходят дальше простого вредительства. Основная причина в том, что массовые атаки на случайных людей не приносят никакой материальной выгоды, а массовость атаки делает её легко обнаружимой, и на подобные методы быстро находятся контрмеры.

Целевые атаки — атаки, направленные в отношении конкретных коммерческих организаций или государственных ведомств. Целями злоумышленников во время атаки могут быть:

– кража ценной информации;

– шпионаж или саботаж;

– выведение из строя компьютерной сети [3].

Большинство специалистов сходится во мнении относительно следующих особенностей целевых атак:

– это атаки, направленные в отношении конкретных коммерческих организаций, отраслей производства или государственных ведомств;

– объектами атаки являются весьма ограниченные какими-либо рамками или целями конкретные информационные системы;

– эти атаки не носят массовый характер и готовятся достаточно длительный период;

– вредоносное ПО, если оно используется при реализации атаки, специально разрабатывается для конкретной атаки, чтобы штатные средства защиты, достаточно хорошо изученные злоумышленниками, не смогли обнаружить ее реализацию;

– для реализации атаки могут использоваться уязвимости нулевого дня;

– как правило, целевые атаки используются для кражи информации, которую легко монетизировать, либо для нарушения доступности к критически важной информации;

– при осуществлении целевой атаки используются те же механизмы взлома, что и при массовых атаках. Отличие составляет подготовка атаки с целью предотвращения возможности ее обнаружения средствами защиты;

– после обнаружения и идентификации целевой атаки, уже по итогам ее осуществления, об угрозе этой атаки становится известно. После этого она переходит в категорию «массовых» — может массово использоваться злоумышленниками. При этом, как идентифицированная, угроза этой атаки уже может быть обнаружена средствами защиты, одной из задач которых является обеспечение минимальной продолжительности перехода угрозы атаки из категории целевых в массовые [4].

Целями же самой атаки являются:

– главный офис компании;

– научно-исследовательские и опытно-конструкторские работы (НИОКР);

– центры обработки данных;

– сеть поставщиков;

– облачные вычисления;

– производство, с системой компьютерного управления;

– базы данных;

– конечная продукция, активируемая с помощью информационной технологии;

– офисные сети;

– маркетинговые планы, информация о ценах и клиентах;

– мобильные устройства;

– интернет-магазин;

– телефонные звонки.

Следовательно, целевые атаки могут быть направлены практически против каждой области информационной системы предприятия, нарушая её работу, либо воруют конфиденциальную и ценную информацию.

Самым очевидным решением проблемы кибератак извне является изолирование системы от любых внешних сетей. Данная практика является довольно распространённой, однако имеет серьёзные недостатки.

Во-первых, отсутствие угрозы внешних атак не избавляет от угрозы инсайдеров.

Во-вторых, любое достаточно крупное предприятие располагает множеством подразделений как в пределах одного города, так и за его пределами, что уже само по себе создает огромную физическую сеть передачи данных. Даже если изолировать такую магистраль передачи данных от общественной, что само по себе огромный труд и трата финансов, всё ещё будет оставаться шанс на физический саботаж этих магистралей.

В-третьих, часто от предприятия может требоваться выводить какую-то часть данных системы для пользователей вне её. Например, почтовые службы (не информационные, а реальные) могут иметь сайт, для информирования клиентов и заказчиков о том, на каком отрезке маршрута находится их посылка, и как долго она ещё будет в пути. Такой сайт, для злоумышленников, становится ещё одной потенциальной точкой доступа к сети предприятия.

Таким образом, простая изоляция информационной системы предприятия становится простым, но очень неэффективным решением вопроса информационной безопасности. Требуется более совершенное решение защиты информации.

Ещё одним аспектом, усложняющим защиту информации, является её масштаб. Чем больше система, тем больше она имеет потенциальных уязвимых точек. И речь не только аппаратном и программном обеспечении, но и о человеческом факторе.

Последней проблемой, требующей рассмотрения, является постоянное совершенствование технологий. С развитием технологий растет и уровень пользователей данными технологиями, сложность методов и т. д. Обратной стороной монеты является то, что и уровень злоумышленников, и уровень киберугроз растет соответственно. Методы информационной защиты, считающиеся передовыми, могут устареть уже в течении пары лет, если не раньше.

Таким образом, требуется постоянно обновлять и сопровождать программу безопасности на предприятии [5].

Рассмотренные проблемы защиты информации на предприятии не являются исчерпывающими, однако хорошо демонстрируют уровень сложности поставленной задачи. Решение должно быть надежным, масштабируемым и адаптируемым к появляющимся со временем новым угрозам.

Повысить информационную безопасность (ИБ) на предприятии можно несколькими способами. Одним из самых распространенных решений является регулярное проведение инструктажа по ИБ среди сотрудников предприятия, контроль выполнения установленных требования и т. п. Что же касается решений, непосредственно связанных с информационными технологиями, то к ним можно отнести:

– аутентификацию;
– ограничение доступа к объектам;
– шифрующие файловые системы;
– цифровые подписи файлов;
– безопасные соединения в корпоративной сети;
– шифрование при подключении к глобальной сети;
– системы обнаружения вторжений.

Перечисленные решения лучше всего работают в совокупности друг с другом, и имеют множество возможных путей реализации. Одним из таких путей является использование адаптивного подхода. Например, система обнаружения вторжений способная адаптироваться будет способна обнаруживать больший диапазон угроз [6].

Список литературы

1. ГОСТ Р 56205–2014. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели (издание с поправкой). — Введ. 2016-01-01. — М. : Стандартинформ, 2020. — 117 с.

2. Мартянов, Е. А. Исследование и разработка методик оценки защищенности информационных объектов от потенциальных нарушителей : дис. ... канд. техн. наук : 05.13.19 / Мартянов Евгений Александрович ; Моск. гос. ун-т им. М. В. Ломоносова. — М., 2018. — 136 с.

3. ФСТЭК России. Банк данных угроз безопасности информации [Электронный ресурс]. — Режим доступа: https://bdu.fstec.ru/threat (дата обращения: 01.03.2021).

4. ООО «НПП «ИТБ» разработало и реализовало новую технологию защиты от целевых атак [Электронный ресурс]. — Режим доступа: https://club.cnews.ru/blogs/entry/ooo_npp_itb_razrabotalo_i_realizovalo_novuyu_tehnologiyu_zashchity_ot_tselevyh_atak (дата обращения: 01.03.2021).

5. Управление производством в условиях неопределенности на основе адаптивных цифровых моделей [Электронный ресурс]. — Режим доступа: https://oborona.ru/includes/periodics/priority/2020/1019/174630390/detail.shtml (дата обращения: 01.03.2021).

6. Дмитриенко, В. Д. Архитектуры и алгоритмы функционирования нейронных сетей Хемминга и Хебба, способных дообучаться и распознавать новую информацию / В. Д. Дмитриенко, А. Ю. Заковоротный // Радіоелектроніка, інформатика, управління. — 2014. — № 2. — С. 100–109.