

ГЛАВНЫЕ ОПАСНОСТИ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ ДЛЯ КОМПАНИЙ, РАБОТАЮЩИХ В СФЕРЕ СЕЛЬСКОГО ХОЗЯЙСТВА, И МЕТОДЫ ИХ НЕЙТРАЛИЗАЦИИ

С.В. Артёмова, Д.А. Потапова, П.И. Карасев, В.Е. Бушуев

ФГБОУ ВО «МИРЭА - Российский технологический университет»

Аннотация. В статье рассматриваются цели киберпреступников при атаках на чувствительные области агропромышленного комплекса. Приводятся примеры кибератак и их последствия. Даны рекомендации по снижению киберугроз.

Ключевые слова: кибератака, киберугроза, злоумышленник, получение финансовой выгоды, программа-шифровальщик, **кража**.

THE MAIN THREATS IN THE FIELD OF CYBERSECURITY FOR COMPANIES WORKING IN THE FIELD OF AGRICULTURE AND METHODS OF THEIR NEUTRALIZATION

S.V. Artemova, D.A. Potapova, P.I. Karasev, V.E. Bushuev

Moscow State Technical University of Radio Engineering, Electrical Engineering and Automation

Abstract. The article examines the goals of cybercriminals when attacking sensitive areas of the agro-industrial complex. Examples of cyber attacks and their consequences are given. Recommendations for reducing cyber threats are given.

Keywords: cyber attack, cyber threat, intruder, obtaining financial benefits, encryption program, theft.

Основные виды киберугроз:

- Вредоносное ПО: вирусы, черви, трояны, шпионские программы, вымогатели, которые наносят ущерб, уничтожают данные или предоставляют несанкционированный доступ.

- Фишинг: попытки мошенников получить конфиденциальную информацию, например, пароли, путем маскировки вредоносных файлов или ссылок.

- Атаки типа "отказ в обслуживании": перегружают системы, делая их недоступными для пользователей.

- Кража данных: несанкционированное копирование и использование конфиденциальных данных.

- Социальная инженерия: манипуляции, чтобы получить информацию путем обмана пользователей.

Для предприятий агропромышленного комплекса по статистике основными киберугрозами являются:

1. Программы-вымогатели: блокируют доступ к системе или данным, требуя выкуп для разблокировки.

2. Вредоносные почтовые рассылки: фишинговые письма, маскирующиеся под сообщения от популярных брендов или сервисов, ведущие на вредоносные сайты.

3. Атаки на корпоративные сети: несанкционированный доступ к конфиденциальной информации через социальную инженерию, вирусы или уязвимости в безопасности.

4. Утечки баз данных компаний: несанкционированная передача конфиденциальных данных из базы данных компании третьим лицам.

5. Атаки, связанные с взломом датчиков: нарушение работы датчиков, что может привести к сбоям в производственных процессах и финансовым потерям.

Основные цели злоумышленников при кибератаках на предприятия агропромышленного комплекса:

1) Промышленный шпионаж. Злоумышленники пытаются выяснить, что производят в компании, кому продают, в каком количестве, основные цепочки поставок и так далее, все это делается с целью передачи информации конкурентам.

2) Получение финансовой выгоды.

3) Нарушение работы предприятия. Злоумышленники оказывают воздействие на технологический процесс, с целью приостановки работы предприятия – например, останавливают станок, меняют температуру воздуха в холодильники или вызывают аварию при помощи перегрева оборудования.

Вот несколько примеров кибератак злоумышленников на предприятия агропромышленного комплекса РФ:

1) В марте 2022 года агрохолдинг «Мираторг» подвергся атаке шифровальщика BitLocker. В результате этой атаки были зашифрованы файлы, которые использовали 18 предприятий компании, и они долгое время не могли оформлять производственные и транспортные ветеринарные документы на продукцию.

2) Уже в марте 2023 в Ростовской области в результате атаки была временно остановлена работа завода «Тавр». Вредоносным программным обеспечением были атакованы серверы, рабочие станции, информационные системы предприятия.

3) В феврале 2023 злоумышленники попытались испортить 40 тонн продукции в агрохолдинге «Селятино»: получив несанкционированный доступ к ключевым системам, преступники изменили температуру хранения замороженной продукции на плюсовую.

4) В качестве примера атаки программы шифровальщика, показателен случай, который произошел на «Агрокомплексе им. Н. И. Ткачева». Инцидент привёл к краже и шифрованию данных на серверах организации. В результате сайт агрокомплекса не работал 8 и 9 апреля. По мнению экспертов, целью хакеров была не только остановка работы организации, но и выкуп за украденные данные. Запрос составил около 500 миллионов рублей. Доступ к данным агрокомплекса мог быть получен через фишинг, уязвимости в публичных приложениях или протокол удалённого рабочего стола.

Чтобы предотвратить кибератаки на агропромышленный комплекс, можно предпринять следующие меры:

1) Обучить сотрудников основам кибербезопасности. Также, регулярно проводить тренинги, чтобы привить сотрудникам полезные привычки: проверять ссылки.

2) Создать резервные копии данных. Это позволит, даже в случае нарушения информационной безопасности предприятия и потере или зашифровке чувствительных данных, выйти предприятию «сухим из воды».

3) Сегментировать сеть. Это позволит в гораздо быстрые сроки полностью вернуть сеть в работу.

4) Регулярно исправлять и обновлять программное обеспечение, такие как антивирусы и сетевые экраны. При выявлении уязвимостей в компьютерных системах и программном обеспечении вендоры регулярно дорабатывают их и обновляют системы для защиты своих клиентов.

5) Внедрить оптимальную политику паролей. Рекомендуется внедрить многофакторную аутентификацию для предотвращения несанкционированного доступа к устройствам и, по возможности, использовать биометрические системы контроля доступа.

Список литературы

1. Вострецова Е.В. Основы информационной безопасности: учебное пособие для студентов вузов. – Екатеринбург:Изд-во Урал,ун-та,2019. – С. 68-79.

2. F.A.C.S.T. защитит мясокомбинаты от кибератак // anti-malware.ru. – URL: https://www.anti-malware.ru/success_stories/2023-05-26/41262 (дата обращения: 07.09.2024).

3. Top Russian meat producer hit with Windows BitLocker encryption attack. – URL: <https://www.bleepingcomputer.com/news/security/top-russian-meat-producer-hit-with-windows-bitlocker-encryption-attack/> (дата обращения: 07.09.2024).

References

1. Vostretsova E.V. Fundamentals of information security: a tutorial for university students. - Ekaterinburg: Ural University Publishing House, 2019. - P. 68-79.

2. F.A.C.S.T. will protect meat processing plants from cyber attacks // anti-malware.ru. – URL: https://www.anti-malware.ru/success_stories/2023-05-26/41262 (accessed: 09/07/2024).

3. Top Russian meat producer hit with Windows BitLocker encryption attack. – URL: <https://www.bleepingcomputer.com/news/security/top-russian-meat-producer-hit-with-windows-bitlocker-encryption-attack/> (date of access: 09/07/2024). DOI: 10.58168/CISMP2024_21-28

УДК 004.9