УДК 678.55.157.

ИССЛЕДОВАНИЕ МЕТОДОВ ОБНАРУЖЕНИЯ УГРОЗ ОБЪЕКТУ В ИНФОКОММУНИКАЦИОННОЙ СРЕДЕ

Калчороева Айганыш Таалайбековна, *магистр БиПЗИм-1-17, Институт Электроники и Телекоммуникации при КГТУ имени И.Раззакова, Кыргызская Республика 720044, Бишкек, Проспект Ч.Айтматова 66, e-mail: ai.kalchoroeva@gmail.com*
Баракова Жанна Токтобековна, *к.т.н., доцент, Институт Электроники и Телекоммуникации при КГТУ имени И.Раззакова, Кыргызская Республика 720044, Бишкек, Проспект Ч.Айтматова 66, e-mail: janna05_05@mail.ru*

Аннотация. В данной статье были исследованы различные существующие методы обнаружения угроз объекту в инфокоммуникационной среде. На сегодняшний момент данный вопрос является одной из важнейших, так как современная техника достигла большого прогресса за довольно короткое время и большинство промышленных объектов переходят на автоматизированные системы управления. Все это заставляет защищать наши данные от угроз и атак, которые могут поступать от злоумышленников. В данной статье, в частности, были изучены возможные угрозы информационной безопасности в сфере энергетики и транспорта, в сфере банков, а также в социальных сетях.

Ключевые слова: информационная безопасность, автоматизированные системы управления (АСУ), киберугрозы, информационные технологии, источники угроз.

THE STUDY OF METHODS FOR DETECTING THREATS TO AN OBJECT IN AN INFOCOMMUNICATION ENVIRONMENT

Kalchoroeva Aiganysh Taalaybekovna, *Master Student of BiPZIm-1-17, Electronics Telecommunication Institute under the KSTU named after I.Razzakov; 66, Ch.Aitmatov Prospect, Bishkek, Kyrgyz Republic 720044, e-mail: ai.kalchoroeva@gmail.com*
Barakova Zhanna Toktobekovna, *Ph.D., Associate Professor, Electronics and Telecommunication Institute under the KSTU named after I.Razzakov; 66, Ch.Aitmatov Prospect, Bishkek, Kyrgyz Republic 720044; e-mail: janna05_05@mail.ru*

Abstract. This article explored various existing methods for detecting threats to objects in the info communication environment. This issue is one of the most important, since modern technology has made great progress in a relatively short time and most industrial facilities are switching to automated control systems now. All this forces us to protect our data from threats and attacks that may come from intruders. In this article, in particular, possible threats of information security in the sphere of energy and transport, in the sphere of banks, and in social networks were studied.

Key words: information security, automated control systems (ACS), cyber threats, information technologies, sources of threats.

Введение

В настоящее время безопасность и развитие любого предприятия зависит от способности обнаруживать возникающие угрозы в облачной, локальной и гибридной средах и быстро реагировать на них. Тем не менее, методы и стратегии атаки постоянно развиваются, что делает обнаружение угроз постоянно движущейся целью. Обнаружение сложных и развивающихся угроз требует передовых инструментов, знаний и обучения.

Вопрос информационной безопасности является особенно острой, так как в современном обществе автоматизированные системы управления используются практически во всех областях деятельности: в медицине, строительстве, машиностроении, образовании и т.д.

Любая атака на объект, может привести к потере персональных данных, к сбою работы всей системы, к утечке конфиденциальной информации, к материальному ущербу, к потере клиентов, а главное - к потере доверия. Перечислять ущерб, возникающий от атак на объект можно очень долго. Своевременное выявление угроз позволяет избежать всех этих проблем. И именно поэтому исследование и разработка новых методов обнаружения угроз и его уничтожения является на сегодняшний день очень актуальным не только в нашей республике, но и во всем мире.

На сегодняшний момент существуют множество разновидностей угроз защите данных. Для защиты от них необходимо проанализировать все возможные атаки угрозы, которые могут поступать как изнутри системы, так и снаружи. И основываясь на этих показателях можно грамотно составить весь комплекс мер для защиты от угроз [1].

Информационная безопасность

Информационная безопасность – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут привести к ущербу владельцам или пользователям информации и поддерживающей инфраструктуры. Информационная безопасность не сводится исключительно к защите информации. Субъект информационных отношений может пострадать (понести убытки) не только от несанкционированного доступа, но и от поломки системы, изменений и хищению данных вызвавшей перерыв в обслуживании клиентов. В связи с этим, в качестве цели защиты целесообразно сформулировать требования обеспечения конфиденциальности, целостности и доступности информационной среды [2].

Конфиденциальность - свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса.

Целостность - свойство сохранять правильность и полноту данных.

Доступность - свойство объекта находиться в состоянии готовности и возможности использования по запросу авторизованного индивидуума, логического объекта или процесса.

Под угрозой понимаются характеристики свойства системы и окружающей среды, которые в соответствующих условиях могут вызвать появление опасного события.

Угроза — это потенциальная возможность определённым образом нарушить информационную безопасность.

Попытка реализации угрозы называется **атакой**, а тот, кто предпринимает такую попытку — **злоумышленником**. Все злоумышленники являются источниками угроз.

Угрозы в отрасли банковских услуг

Сектор банковских и финансовых услуг играет жизненно важную роль в развитии экономики страны. Последние два десятилетия стали свидетелями драматического преобразования в ведении бизнеса. Все больше и больше различных технологических решений внедряются и используются в этих финансовых учреждениях. Внедрение технологических решений привело к удобству для клиентов и экономическая эффективность от банковского дела возросла. Таким образом, банки в значительной степени обязаны поддерживать целостность финансовых операций и защиту конфиденциальности клиентов. Тем не менее, принятие этих технологий принесли большое количество угроз информационной безопасности. Инциденты, связанные с нарушением информации могут привести к потере репутации банка и к значительному сокращению существующих клиентов. Следовательно, понимание угрозы информационной безопасности и предотвращения таких инцидентов требуется в профессиональной банковской среде.

Например, 2015 году банковская индустрия обнаружила поразительный новый тип угрозы: массивное киберпреступное кольцо предназначалось для банков, использующих вредоносное ПО Carbanak. Зараженные этим вредоносным ПО машины в течение двух лет находились под радаром, атаковав внутренние банковские службы обработки денег и банкоматы (банкоматы). К тому времени, когда они были обнаружены «Лабораторией Касперского», эти атаки уже проникли в более чем 100 банков в 30 странах, а ворам удалось выделить 1 миллиард долларов.

Разработка надежной стратегии безопасности предполагает оценку рисков и уязвимостей компании, связанных с текущим ландшафтом. Понимание этого может помочь реализовать правильные стратегии, которые будут защищать данные и сети с помощью технологий. Для того, чтобы построить правильную стратегию по обеспечению безопасности организации требуется:

1. **Анализ угроз.** Анализ угроз помогает определить уровень допустимого уровня риска, которую можно принять, избежать, перенести или предотвратить. Анализ рисков может помочь определить, как лучше составить бюджет и определить приоритеты инициатив в области безопасности.
2. **Классификация данных и активов.** Необходимо понимать данные и активы, которые поддерживает организация, и классифицировать их в зависимости от важности основных бизнес-задач. Это помогает устанавливать приоритеты для уровней безопасности и устанавливать разрешения для доступа к информации.
3. **Обучение безопасности пользователей.** Без сомнения, люди представляют наибольшую угрозу организации в результате случайного или злонамеренного неправильного использования или злоупотребления данными. Сотрудники должны быть должным образом обучены угрозам и тому, как правильно обращаться с данными. Осведомленность сотрудников о политике и процедурах компании, безусловно, может помочь предотвратить потерю данных.
4. **Безопасность приложений.** Безопасность приложения описывает тип безопасности, который включает аппаратное и программное обеспечение для защиты организаций от внешних угроз. По мере того, как мир финансовых услуг движется в сторону цифровых технологий, угрозы приложений становятся все более и более распространенными.

Для обеспечения надлежащей защиты приложений могут быть приняты различные меры. Для начала можно определить приоритеты различных угроз, обнаруживаемых в приложениях. Это может быть что угодно, от незапланированных событий до хакеров, или

неспособность хранить важную информацию. Во-вторых, можно применить ограничения доступа к операционной системе компьютера.

Процессы аутентификации

Аутентификация в основном работает для подтверждения того, что пользователи являются теми, кем они себя называют, и что их сообщение, файл или данные являются подлинными. Эта функция необходима в отрасли финансовых услуг из-за риска, с которым клиенты сталкиваются с мошенничеством с кредитными картами в связи с развитием онлайн-банкинга. Поскольку банки становятся мобильными как никогда, клиенты более уязвимы к этим угрозам. [5]

Чтобы банки могли справиться с этой задачей, методы аутентификации были интегрированы в мобильные инструменты, такие как аутентификация на основе имени пользователя и пароля. В последних разработках отпечаток пальца Touch ID оказал влияние на эти мобильные приложения, а также на распознавание лиц, таких как сканирование фотографий и возможности сопоставления лиц.

Процессы авторизации

Авторизация дает разрешение на выполнение каких-либо действий, таких как доступ к базам данных или системам, для выполнения задачи. Понятно, что это важно для обеспечения безопасности большинства задач в организации, особенно в финансовой индустрии. Авторизация просматривается при каждом использовании кредитной карты и получении квитанции. Он рассматривается как подпись клиента на обратной стороне кредитной или дебетовой карты, чтобы создать подлинное разрешение от пользователя. Наряду с этим, коды авторизации также можно найти на карточках. Это код, который отправляется банкирам напрямую для проверки платежей. Банки могут приостановить авторизацию, если подозревается мошенническое поведение. Чтобы клиент мог разблокировать это удержание, именно здесь играет роль аутентификация, такая как имя, секретные вопросы и другая личная информация.

Угрозы в отрасли энергетики

Роль, которую энергетический сектор играет в функционировании современной экономики, с ее возрастающей взаимосвязью и оцифровкой, с появлением интеллектуальных сетей и интеллектуальных устройств, делает энергетический сектор очень привлекательной целью для атак, направленных на срыв работы всей системы. В худшем случае эти атаки могут привести к остановке инфраструктуры, вызвать экономические и финансовые сбои или даже гибель людей и огромный ущерб окружающей среде. В новом докладе Мирового Энергетического Совета подчеркивается, что за прошедший год в энергетических компаниях наблюдалось значительное увеличение числа успешных атак.

Так, в 2015-году в Украине за день до Рождества три распределительные компании были взломаны одновременно, и хакерам удалось отключить электричество для четверти миллиона человек на несколько часов. В Интернете есть несколько видеоклипов, демонстрирующих, как системы управления в диспетчерских центрах компаний «принадлежали» хакерам. Курсор просто перемещался по экрану, пока персонал беспомощно наблюдал. Объяснение того, что это вообще возможно, можно найти в так называемых SCADA-системах. Системы SCADA (диспетчерский контроль и сбор данных) используются для управления энергетической сетью и извлечения данных из нее. Проблема с системами SCADA и другими промышленными системами управления заключается в том, что машины, которыми они управляют, просто не предназначены для кибербезопасности.

В сфере электроснабжения можно применять методы мониторинга ИТ: простой протокол сетевого управления (SNMP), который позволяет операторам управлять устройствами через IP, включая коммутаторы, маршрутизаторы, рабочие станции и принтеры

через систему управления сетью (NMS). В энергетическом секторе операторы могут использовать SNMP для мониторинга данных устройства на уровне NMS:

- **путем мониторинга состояния устройств;**
- **мониторинга производительности и связи устройств;**
- **обнаруживая вторжения;**
- **управляя конфигурацией.**

Чтобы избежать компьютерных ошибок, внедрение новых технологий и уровней безопасности недостаточно. Все заинтересованные стороны (команды на местах распространения, поставщики, специалисты по техническому обслуживанию и вводу в эксплуатацию) должны пройти обучение по технике безопасности [3]. Чтобы реализовать эти изменения и обеспечить безопасность ИТ, необходимо представить основные концепции безопасности, а именно:

Шаг 1. Определить политику безопасности,
Шаг 2: Определите процессы,
Шаг 3: Выберите технологию и внедрите ее.

Угрозы в сфере транспорта

Транспорт во всех видах является жизненно важной услугой во всех городах. По мере того, как города стали использовать все более взаимосвязанные и более сложные транспортные системы, вероятность нападения возросла, и появляются новые угрозы [4]. Поскольку все больше транспортной инфраструктуры города - таких как светофоры, дорожные датчики, железнодорожный или автобусный транспорт, порты и системы аэропортов - становятся подключенными к сети, злоумышленники все чаще могут атаковать не только информационные технологии, но и оперативные технологии, которые управляют городскими системами сигнализации и управления. Это означает, что преступники могут вызвать:

1. Серьёзные сбои в работе,
2. Остановку общественного транспорта,
3. Изменение сигналов светофора,
4. Удаленное управление транспортной инфраструктурой города.

Угрозы в социальных сетях

Социальные сети очень популярны в современном мире. Миллионы людей используют различные формы социальных сетей, так как они позволяют людям общаться с друзьями и семьей, а также делиться личной информацией. Однако могут возникнуть проблемы, связанные с поддержанием конфиденциальности и безопасности информации пользователя, особенно когда загружаемый пользователем контент является мультимедиа, таким как фотографии, видео и аудио. Загруженный мультимедийный контент несет информацию, которая может передаваться вирусно и почти мгновенно внутри сайта социальной сети и за ее пределами [5].

Социальные сети являются основными инструментами сбора частной информации, и при использовании злоумышленниками эта информация может и будет использоваться против людей. Это также место, где ребенок может вступать в контакт с очень неприятными или даже опасными людьми. Основная проблема заключается в том, что экстремисты, террористы и злоумышленники могут использовать социальные сети для вербовки новых членов в свою преступную группу.

Атака, исходящая из социальных сетей, часто на разных уровнях. Сначала хакеры пытаются получить доступ к учетной записи (через сайт или программу, которая захватывает пароли). Затем они используют взломанные аккаунты для своих собственных целей. Это может быть рассылка спама, кража банковских счетов или простой доступ к вашим личным

данным. Также опасно, что злоумышленники могут отправлять ссылки со вредоносных сайтов всем пользователям в списке друзей жертвы. Люди привыкли нажимать на ссылки, отправленные людьми, которым они доверяют, и вредоносная ссылка может установить вредоносное программное обеспечение

Угрозы, с которыми могут столкнуться клиенты, могут быть разделены на два класса:

1. **Угрозы, связанные с конфиденциальностью.** Вопросы конфиденциальности требуют, чтобы пользовательские профили никогда не распространять. Данные на отдельных личных страницах могут содержаться исключительно личную информацию, например, даты рождения, места жительства и индивидуальные номера и так далее. Эти данные могут быть использованы злоумышленниками для мошенничества, шантажа или использования имеющихся данных для других корыстных целей.
2. **Угрозы, связанные с безопасностью.** Злоумышленники создают ложные профили или копируют личность, для того, чтобы опорочить известного человека в социальной сети. Это может коснуться не только человека, но и мировые компании, которые используют платформу социальных сетей для рекламы и продвижения своей продукции.

С ростом популярности сайтов социальных сетей они стали основной целью различного рода угроз и атак. Киберпреступность становится широко распространенным и представляет серьезную угрозу для национальной и экономической безопасности. Как государственные, так и частные учреждения в секторе общественного здравоохранения, информации и телекоммуникаций, обороны, банковского дела и финансов находятся в опасности. Таким образом, организации должны принять надлежащие меры безопасности для защиты от киберпреступлений, и пользователи должны защищать свою личную информацию.

Типы угроз безопасности.

1. Фишинговые атаки

Масса электронных писем отправляется многим получателям, которые должны хранить конфиденциальную информацию (например, свой пароль, имя пользователя или банковские реквизиты). С помощью этой информации злоумышленник может выполнить взлом данных. Трудно обнаружить такое электронное письмо, потому что оно надежно скрывается, заставляя получателя посетить вредоносный веб-сайт. Фишинг - более целенаправленная форма атаки. Письмо предназначено для того, чтобы создать впечатление, что оно было отправлено кем-то, кого получатель знает или которому он доверяет. Руководители или владельцы привилегированных аккаунтов часто становятся жертвами фишинговых атак.

2. Внутренние угрозы

Это новый метод, обычно используемый во многих недавних взломах данных. Внутренние угрозы кибербезопасности организованы сотрудниками. Эти внутренние угрозы могут быть непреднамеренными (сотрудник является жертвой фишинг-атаки) или злонамеренными (недовольный сотрудник преднамеренно извлекает данные). В любом случае, внутреннее нарушение данных особенно трудно обнаружить.

3. Отказ в обслуживании (DoS)

Эти кибератаки происходят, когда хакер наводняет веб-сайт большим объемом трафика, чем он может обработать. В результате законные пользователи не могут получить доступ к сервисам. Это приводит к простоям сотрудников или дорогостоящих пользователей. При распределенных атаках типа «отказ в обслуживании» (DDoS) используется ботнет, представляющий собой группу скомпрометированных компьютеров или устройств IoT. Эти бот-сети генерируют то, что может быть законным трафиком, что делает различие между нормальным и вредоносным трафиком еще более трудным.

4. Вредоносные программы

Среди наиболее распространенных угроз кибербезопасности вредоносные программы - это несколько видов вредоносного программного обеспечения, которое запускается, когда

пользователь загружает их по ошибке. Некоторые из последних нарушений кибербезопасности связаны с такими вредоносными программами, как WannaCry и Petya / NotPetya. Традиционные вредоносные программы, такие как вирусы, трояны и бэкдоры, также все еще присутствуют.

5. Кража личных данных

Привилегированные учетные записи могут быть скомпрометированы, если учетные данные используются не по назначению или используются несколько раз. Злоумышленник может использовать то, что кажется законным веб-приложением, для получения учетных данных неискушенного сотрудника. Впоследствии, хакер может получить доступ к конфиденциальной информации и либо взломать или зашифровать (вымогателей) для достижения финансовой выгоды. Использование одного и того же пароля для всех систем особенно вредно, даже если этот объект заманчив для персонала. Повторное использование учетных данных в нескольких системах позволяет злоумышленнику более широко перемещаться по вашей инфраструктуре.

Методы обнаружения угроз

Методы обнаружения угроз и анализа несанкционированных воздействий на ресурс информационной системы можно разделить на:

− метод на основе анализа сигнатур

− метод обнаружения аномальных отклонений.

Метод обнаружения угроз на основе сигнатур - это процесс, в котором для конкретной угрозы устанавливается уникальный идентификатор, позволяющий идентифицировать угрозу в будущем. В случае антивирусного сканера это может быть уникальный шаблон кода, который присоединяется к файлу, или он может быть таким же простым, как хеш известного неверного файла. Если этот конкретный шаблон или подпись обнаружен снова, файл может быть помечен как зараженный.

По мере того как вредоносные программы становились все более изощренными, авторы вредоносных программ начали использовать новые методы, такие как полиморфизм , для изменения шаблона при каждом распространении объекта из одной системы в другую. Таким образом, простое сопоставление с образцом не будет полезным, если не считать небольшую кучку обнаруженных устройств.

Один из главных ограничивающих факторов, стоящих за сигнатурами, заключается в том, что они всегда носят реактивный характер: вам всегда нужно начинать с экземпляра вируса или понимания сетевой атаки, чтобы написать сигнатуру для их обнаружения. Это означает, что подписи не могут идентифицировать неизвестные и возникающие угрозы. Подписи только идентифицируют угрозы, которые уже известны.

Метод обнаружения аномальных отклонений. В отличие от обнаружения на основе сигнатур, метод обнаружения аномальных отклонений не ищет уникальные характеристики конкретной угрозы, а ищет результаты. С медицинской точки зрения, представьте, что подписи - это анализ крови, чтобы определить, заражены ли вы конкретной бактерией, а анализ поведения отслеживает ваши симптомы. Если у вас болит горло, насморк, лихорадка, застой в груди, вы, вероятно, больны.

Преимущество обнаружения аномальных отклонений заключается в том, что данный метод может обнаруживать неизвестные угрозы. Одним из побочных эффектов является то, что он склонен к ложным срабатываниям. В медицинской аналогии, вы можете быть горячим, потеть и иметь затрудненное дыхание из-за простуды ... или, возможно, вы только что занялись спортом. Дополнительный контекст помогает разобраться в этих результатах, но когда количество ложных срабатываний превышает количество подлинных обнаружений, решение может быть больше проблем, чем оно того стоит.

Кроме того, анализ поведения может быть гораздо более ресурсоемким, поэтому полагаться на него для выявления известных угроз может быть дорого и сопряжено с риском пропуска угрозы, которую можно легко идентифицировать с помощью подписи.

Сбалансированная и многослойная защита.

Оба метода обнаружения угроз полезны для сбалансированной и многоуровневой защиты от кибербезопасности. Можно использовать Принцип Парето (он же «правило 80/20»).

Восемьдесят процентов (или потенциально больше) инцидентов в вашей среде будут легко идентифицироваться с помощью обнаружения на основе сигнатур. На самом деле, подписи являются наиболее эффективным методом обнаружения известных угроз, что означает, что он остается принципиально важной методологией.

С другой стороны, двадцать процентов (или меньше) проблем не будут идентифицироваться подписями, но, скорее всего, вызовут восемьдесят процентов проблем. Если организация подвергается целенаправленной атаке, скорее всего, это не будет легко идентифицируемой или известной угрозой. Итак, метод обнаружения аномальных отклонений явно необходим [6]

Современная защита от кибербезопасности является сбалансированной и многоуровневой, что означает включение методов обнаружения как известных, так и неизвестных угроз. Эффективные организации могут легко идентифицировать, предотвращать и рассылать известные угрозы, используя решение на основе сигнатур, и дополнять этот метод решениями на основе метода обнаружения аномальных отклонений, чтобы обнаруживать неизвестные угрозы, которые может пропустить решение на основе сигнатур.

Список литературы:

1. Информационная безопасность. Учебное пособие под общей редакцией проф. Ясенева В.Н. http://www.unn.ru/books/met_files/infbezop.pdf (дата обращения 10.03.2019).
2. А.Н.Асаул. Организация предпринимательской деятельности. Учебник. СПб.: АНО ИПЭВ, 2009. 336с. http://www.aup.ru/books/m6/8_4.htm (дата обращения 09.03.2019).
3. Книга 5. Электроэнергетика и охрана окружающей среды. Функционирование энергетики в современном мире. http://energetika.in.ua/ru/books/book-5/part-4/section-1 (дата обращения 14.03.2019).
4. Угрозы транспортной безопасности Российской Федерации. Статьи по предмету Административное право. http://www.justicemaker.ru/view-article.php?id=25&art=1691 (дата обращения 14.03.2019).
5. Проблемы информационной безопасности в социальных сообществах в сети интернет. https://cyberleninka.ru/article/n/problemy-informatsionnoy-bezopasnosti-v-sotsialnyh-soobschestvah-v-seti-internet (дата обращения 11.03.2019).
6. Методы обнаружения вторжений: методы и лучшие практики https://www.alienvault.com/blogs/security-essentials/intrusion-detection-techniques-methods-best-practices(дата обращения 11.04.2019).
7. Источники угроз для банка. https://finlit.online/bankovskoe-delo-knigi/istochniki-ugroz-dlya-42527.html (дата обращения 11.03.2019).

References

1. Information security. The manual is edited by prof. Yaseneva V.N. http://www.unn.ru/books/met_files/infbezop.pdf (accessed 10/03/2019).
2. A.N. Asaul. Business organization. Textbook. SPb .: ANO IPEV, 2009. 336s. http://www.aup.ru/books/m6/8_4.htm (accessed 09/03/2019).

3. Book 5. Electricity and environmental protection. The functioning of energy in the modern world. http://energetika.in.ua/ru/books/book-5/part-4/section-1 (accessed 14/03/2019).

4. Threats to the transport security of the Russian Federation. Articles on the subject of administrative law. http://www.justicemaker.ru/view-article.php?id=25&art=1691 (accessed 03/14/2019).

5. Sources of threats to the bank. https://finlit.online/bankovskoe-delo-knigi/istochniki-ugroz-dlya-42527.html (accessed 11/03/2019).

6. Problems of information security in social communities on the Internet. https://cyberleninka.ru/article/n/problemy-informatsionnoy-bezopasnosti-v-sotsialnyh-soobschestvah-v-seti-internet (accessed 11/03/2019).

7. Intrusion Detection Techniques: Methods & Best Practices https://www.alienvault.com/blogs/security-essentials/intrusion-detection-techniques-methods-best-practices (accessed 11/03/2019).