Роджер Ченг

Инфраструктурная сетевая безопасность в эпоху IIoT

Для систем автоматизации, построенных в соответствии с концепцией Индустрии 4.0, крайне важна развитая инфраструктура передачи данных. Основной упор здесь делается на сети Ethernet, составляющие основу Интернета. Но чем теснее сплетается система промышленной автоматизации с глобальными сетями, тем важнее становится задача защиты её от киберугроз.

Люди постоянно стремятся оптимизировать производительность оборудования, создавая новые стандарты и компоненты автоматизации. В качестве основы для реализации концепции Индустрии 4.0 рассматривается в первую очередь промышленный Интернет вещей (IIoT – Industrial Internet of Things). В соответствии с этой концепцией благодаря связыванию через сеть Ethernet развёртываются и подключаются многочисленные датчики для сбора данных. Для последующего анализа и преобразования собранных данных в полезную информацию используется множество сетевых устройств и серверов, на которых основанные на человеческом опыте процессы анализа обеспечивают интеграцию и разделение собранных данных соответствующим конкретному применению образом.

Тем не менее дальнейшее наращивание возможностей подключения устройств к сети влечёт за собой повышенный риск: когда все устройства взаимосвязаны, они ещё более уязвимы для кибератак и несанкционированных вторжений. Таким образом, поскольку благодаря Ethernet инфраструктура IIoT становится всё более сетевой, безопасность Ethernet стала ключевой проблемой для современного мира. На рис. 1 показана рабочая сеть, связывающая вещи и людей как с информационными (ИТ), так и с операционными (ОТ) технологиями. Из каждого процесса стекаются необработанные данные, которые изучаются, анализируются на основе предыдущего опыта и, наконец, используются людьми. Ключевым выводом здесь является то, что для создания инфраструктуры IoT, которая сможет послужить платформой для передачи необработанных данных и полезной информации, ИТ необходимо интегрировать с ОТ. Это позволит пользователям сосредоточиться на разработках в их предметных областях и проведении ис-

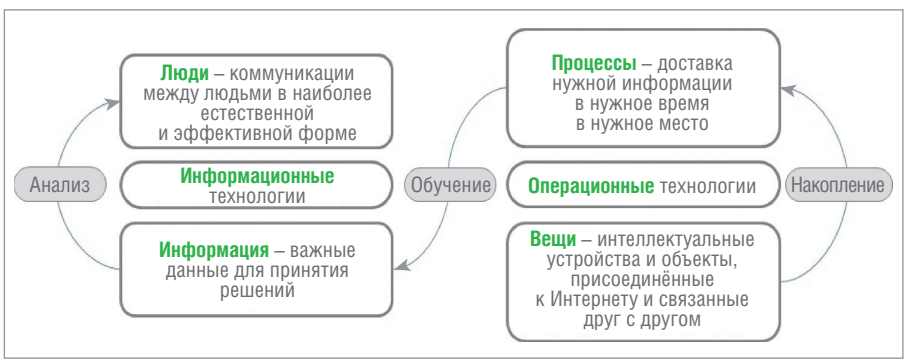


Рис. 1. Потоки данных IIoT

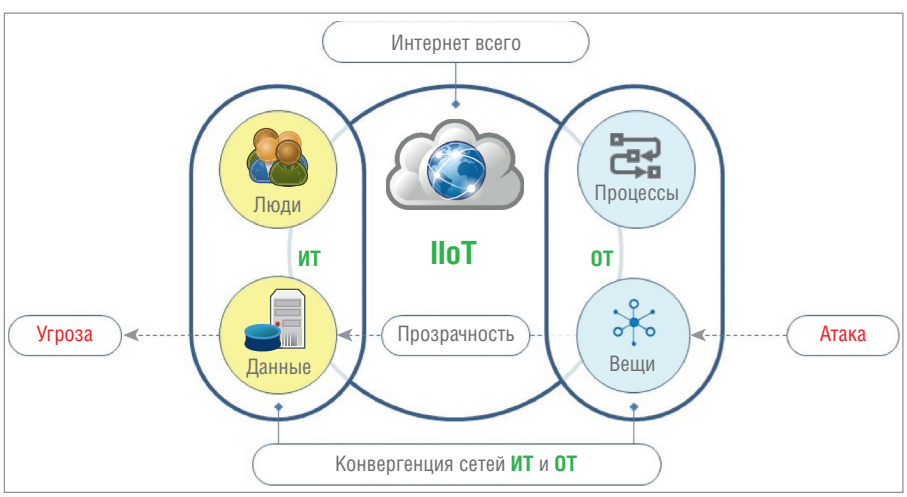


Рис. 2. Распространение угроз IIoT

следований. Однако если работа платформы нестабильна, поддержание высокого качества и точности данных станет затруднительным. По завершении стадии развёртывания сети переходят в стадию функционирования и обслуживания в процессе долгосрочной эксплуатации, когда стабильность во многом зависит от сетевых компонентов. В дополнение к аварийным отключениям оборудования серьёзную проблему на этом этапе представляет собой обеспечение кибербезопасности. Поскольку инфраструктуру IIoT стремятся создавать максимально прозрачной для всех приложений, кибератаки и несанкционированные вторжения стали серьёзными угрозами безопасности. В общем виде это представлено на рис. 2, из схемы можно сделать следующие выводы:

- IIoT основан на концепции Интернета всего (IoE – Internet of Everything) и реализуется благодаря конвергенции OT и IT;
- атаки и вторжения осуществляются с использованием инфраструктуры IIoT и становятся реальной угрозой для людей.

Интернет всего

В мире IoT число устройств, подключаемых к сетям, неуклонно растет. Это связано с тем, что на вертикальных рынках, таких как промышленная автоматизация, транспорт, нефтегазовая отрасль и энергетика, для обеспечения надлежащих рабочих процессов все операции, включая техническое обслуживание, требуют постоянного контроля. Возможность мониторинга и прогнозирования в режиме реального времени благодаря способности обнаружения аномальных событий формирует тенденции IoT во многих отраслях.

Технология Ethernet, основанная на стандартах IEEE 802.3, является наиболее массово внедряемой коммуникационной технологией, и вместе с различными устройствами ввода/вывода используется всё более широко и разнообразно. Полностью согласующийся с этой концепцией IIoT, использующий промышленный Ethernet и все разработанные на его основе зрелые компоненты и технологии, становится самой распространённой платформой для подключения устройств и создания конвергенции ИТ и ОТ. Однако при поиске возможностей соединения всего на свете необходим компромисс, и в этом случае он требуется между беспрепятственной связью и безопасностью.

Подключение позволяет пользователям легко получать доступ ко всем сетевым ресурсам, выполнять задачи мониторинга и устранять любые проблемы в сети, но оно также предоставляет недобросовестным злоумышленникам средства для кражи коммерческих секретов и незаконного обогащения. Такая открытость подключения означает, что даже локальные сети больше не являются безопасными, и по мере того как число людей, полагающихся на сеть для выполнения своих рабочих обязанностей, увеличивается, требуемый уровень безопасности удалённого доступа будет продолжать повышаться в полном соответствии с растущей зависимостью людей от облачных сервисов.

Отображаемая на мониторах и панелях в диспетчерских информация основана на данных, полученных от распределённых пограничных компонентов. Это даёт потенциальную возможность хакерам получить доступ к сети через пограничные компоненты или коммутаторы/маршрутизаторы, реализуя типичное вторжение снизу вверх, которое помимо потенциальной утечки коммерческой тайны может привести к ряду системных проблем, возникающих в результате зомби-атак – распределённых атак, вызывающих отказ в обслуживании (DDoS – Denial of Service) или подмену (Spoofing Attack – кибератака, в процессе которой человек или программа успешно маскируется под другую путём фальсификации данных). Вот почему в приложениях IIoT вопросы безопасности продолжают вызывать большую озабоченность. Следовательно, ключевым моментом кибербезопасности является определение средств для обнаружения, прогнозирования и предотвращения вторжений или атак.

Тенденция конвергенции ИТ/ОТ

Итак, конвергенция ИТ и ОТ обусловлена тенденциями развития IIoT. В общем случае сети ОТ представляют собой прозрачные соединения между машинами/приборами (локальный сайт) и средствами отображения информации (центр управления). Такие сети обмениваются трафиком и сигналами, контролирующими физическое состояние системы. Поскольку передаваемые данные могут иметь решающее значение для приложений мониторинга и управления (например, обнаружения дыма в туннеле и управления пожарной сигнализацией), качество мониторинга в режиме реального времени важно для обеспечения беспроблемной эксплуатации. Чтобы злоумышленники не могли парализовать сеть или перехватить конфиденциальную информацию во время её передачи, желательно обеспечить шифрование хотя бы наиболее важной части данных.

ИТ-сети работают с информацией, используя различные логические схемы и алгоритмы обработки данных. В основном после компиляции больших данных их полезная часть анализируется для выявления нормы и отклонений. Это обеспечивает искусственный интеллект (ИИ), который затем используется и для формирования правил в виде базы знаний, дающей основу для прогнозирования. Эта база знаний обычно функционирует на суперкомпьютере. Учитывая, что такой компьютер физически защищён шкафом и дверными замками (или даже биометрической аутентификацией в системах с высокой степенью безопасности), самым простым путём проникнуть в него остаётся лазейка через сеть. И поэтому самым актуальным вопросом с точки зрения безопасности

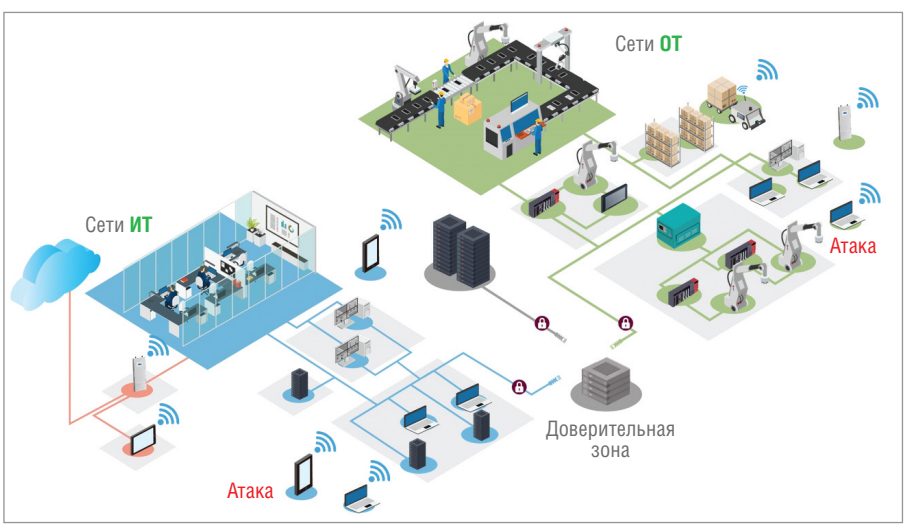


Рис. 3. Конвергенция ИТ/ОТ в реальном мире

системы является анализ наиболее уязвимых точек входа (рис. 3).

В сетях ОТ доступ контролировать сложно, потому что безопасность там менее строгая, чем в ИТ-сети. Фактически сеть ОТ является аналогом супермагистрали, которая предоставляет хакерам доступ к внутренней ИТ-сети, и именно поэтому конвергенция сетей ОТ/ИТ приводит к существенным проблемам безопасности.

Угрозы, с которыми мы сталкиваемся

Кибербезопасность – это обширная тема, которую можно рассматривать с разных точек зрения. Как правило, угрозы безопасности можно условно разделить на внешние или внутренние. Внешние угрозы требуют таких мер защиты для предотвращения атак, как брандмауэры, которые реализуются с использованием комбинации аппаратного и гибкого программного обеспечения.

Из-за больших масштабов сетевой инфраструктуры внутренние угрозы могут быть более сложными для прогнозирования и предотвращения. Поскольку всё взаимосвязано, существуют различные уязвимые места и средства для внутреннего проникновения в сеть. Таким образом, угроза может исходить от любого устройства или компьютера на границе сети. На рис. 4 показана разница между внутренними и внешними атаками. Будучи точкой доступа или первым мостом в широкополосной сети, коммутаторы уже давно стали основной целью кибератак и, таким образом, служат ключевой точкой безопасности системы. Когда возникает угроза, коммутатор обычно выступает в роли первой линии защиты. Поэтому необходимо, чтобы коммутаторы были оснащены различными механизмами аутентификации, авторизации и учёта для защиты сети и самих себя. Наиболее важной задачей кибербезопасности является предотвращение вторжений, и чтобы достичь этого, пограничные узлы сети должны обладать способностями прогнозирования и предотвращения угроз. Поскольку коммутаторы обычно используются в качестве основы сетевой инфраструктуры, они могут служить отличным многоуровневым механизмом безопасности.

Мотивы и типы угроз

Кража конфиденциальной информации

Конфиденциальность особенно важна как для оборонных и коммерческих сетей, так и для охраны личной жизни в целом. Утечки критических данных обычно происходят из-за незаконных сетевых подключений, захвата необработанных данных, их перенаправления и отслеживания.

Зомби-сеть

Хакеры могут нанести вред, заразив компьютеры вирусом или трояном с целью создания сети компьютеров-зомби. Вредоносные программы на компьютерах-зомби могут запускаться автоматически или контролироваться хакерами, создавая Botnet-шторм, приводящий к исчерпанию сетевых ресурсов.

Подмена данных

Злоумышленники могут, например, перехватывать данные полевой видеокамеры и затем передавать поддельные изображения в предполагаемую точку назначения исходного канала. В итоге те, кто отслеживает канал, не увидят на своих экранах ничего подозрительного.

Классификация атак по целям

Сеть состоит из нескольких узлов и связей между узлами. Сетевой узел играет важную роль в обмене трафиком и управлении маршрутизацией и может считаться лучшей целью для вторжения, потому что только узлы через проводное или беспроводное соединение обеспечивают физическую связь с сетью.

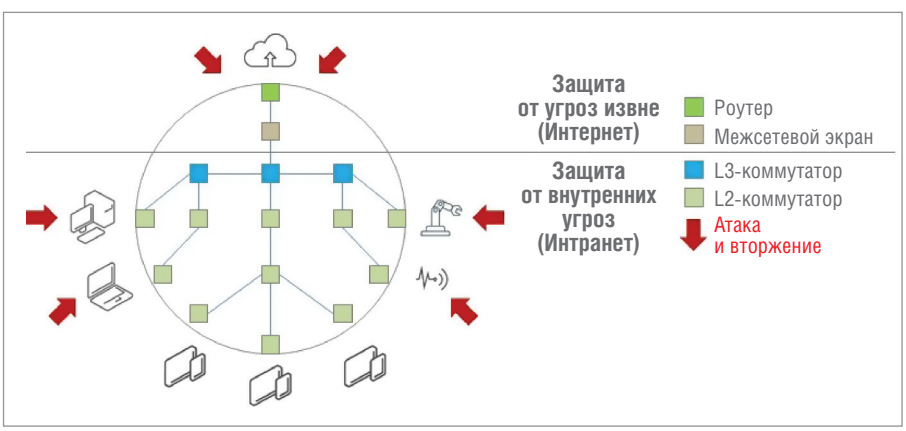


Рис. 4. Области безопасности в сетевой архитектуре

Сетевые узлы

Если при обслуживании сетевого узла игнорируются строгие меры безопасности (в частности, не производится аутентификация по имени пользователя и паролю), тогда становится легко войти в пользовательский интерфейс сетевого узла и изменить параметры его работы с целью повлиять на обмен трафиком и маршруты данных. После взлома коммутатора хакеры могут перенаправить трафик или даже закольцевать его, а затем, изменив параметры коммутатора, вызвать широковещательный шторм.

Терминальные устройства

Если нет механизма, позволяющего отличить неавторизованного пользователя от авторизованного, хакеры могут скомпрометировать как проводные, так и беспроводные соединения для доступа к сети. При отсутствии такого механизма невозможно предотвратить вторжения в оконечные устройства, такие как персональные компьютеры и серверы данных.

Классификация сетей по уровням

Сеть может быть разделена на разные сегменты в зависимости от направления трафика и иерархии данных и имеет пирамидальную иерархическую структуру. Нижний её слой содержит всё увеличивающееся количество конечных устройств или датчиков, которые собирают данные для передачи в централизованную диспетчерскую. Средний уровень отвечает за агрегацию данных и определение сетевых маршрутов. Именно здесь классифицируются различные типы трафика и выполняется маршрутизация данных. Верхний уровень обычно является базовой сетевой инфраструктурой. Помимо обмена трафиком с высокой пропускной способностью он отвечает за передачу больших объёмов данных в облако для анализа и работы конкретных приложений.

Уровень доступа к данным

Этот уровень объединяет конечные устройства или локальные сети меньшего размера. Поскольку такие сети относительно малы по масштабу, базовых

duagon

LEADING THE EMBEDDED FUTURE

Встраиваемые решения duagon

Защищённые компьютерные платы и системы для работы в жёстких условиях эксплуатации и для ответственных применений

Высокое качество продукции в соответствии с ISO 9001/14001, AN/AS 9100, IRIS

Высокая надёжность в соответствии с EN 50155, DO-254, E1

Обеспечение уровней безопасности до SIL 4, DAL-A

Компьютерные модули Rugged COM Express® (VITA 59) и ESMexpress®

Платы в форматах CompactPCI®/PlusIO/Serial и VME

Мезонинные модули PMC, XMC, M-Module™ I/O

Защищённые коммутаторы Ethernet

Встраиваемые и панельные компьютеры

функций безопасности уровня 2 для предотвращения незаконного доступа для них обычно бывает достаточно; такая безопасность достигается путём использования ограниченного числа хостов или выполнения процедур аутентификации. Уровень доступа представляет собой потенциальную точку входа, к которой хакеры могут легко подключиться с помощью ноутбука, поскольку этот сегмент сети развёрнут вблизи конечного пользователя. Вторжения могут быть осуществлены через проводные коммутаторы или беспроводные точки доступа. Если на указанных коммутаторах и точках доступа не предпринимаются никакие меры безопасности, это по сути похоже на оставление двери дома незапертой. Чтобы уменьшить риск, для ограничения доступа ненадёжных/неавторизованных хостов полезны такие процедуры проверки и идентификации, как проверка имени/пароля пользователя или MAC-адреса (Media Access Control – управление доступом к среде).

Уровень распределения

Для функционирования в качестве сборщика данных и обменного узла агрегированному уровню требуются качественно реализованные функции безопасности, такие как IP-аутентификация или фильтрация данных на уровне обслуживания. Для отправки трафика в восходящем направлении с целью ретрансляции или обмена данными уровень доступа связан с агрегированным уровнем распределения. Это означает, что даже если на данном уровне проверки безопасности не проводились, весь обмен трафиком в этом сегменте уже прошёл проверку на уровне доступа. Таким образом, уровень распределения становится второй линией защиты, на которой выполняются проверки всех кадров, что обычно означает проверку IP-адреса источника/приёмника и MAC-адреса источника/приёмника.

Уровень ядра сети

Угрозы коммутатору уровня ядра обычно являются внешними и могут отслеживаться и фильтроваться брандмауэром, что особенно важно для сетей WAN.

Этот уровень играет роль шлюза, подключаемого к глобальным сетям или известным облакам, и в качестве меры по защите внутреннего трафика запрещает доступ внешним потенциально опасным воздействиям. Область безопасности на этом уровне имеет отношение к кибербезопасности, но не к предотвращению вторжений снизу вверх.

Где же решение?

Пользовательские права доступа

Для управления сетевыми узлами разрешения для пользователей являются критически важной темой. Если неавторизованному пользователю разрешён доступ к узлам сети, то злоумышленник может легко выполнить перенаправление данных, отслеживание или даже организовать шторм Botnet. Как правило, сетевой узел хранит данные конфигурации, включая имена учётных записей и пароли, и если они не защищены, то легко могут быть скопированы. Шифрование пароля с использованием ключа безопасности, известного только сетевому узлу, предназначено для того, чтобы сделать такие данные нечитаемыми. Это предотвращает утечку паролей и обеспечивает строгий уровень безопасности управления. Чтобы обеспечить вторую линию защиты от неавторизованных пользователей, сетевой узел должен быть настроен на утверждение доступа к сети только для определённых IP-хостов и контролировать, какие протоколы (например, HTTP, TELNET или SNMP) разрешены.

При удалённом управлении на сетевых узлах не регистрируются операции и инструкции пользователей, имеющих авторизованную учётную запись и пароль. Для безопасности сетевой узел должен хранить полную историю пользовательских операций и инструкций и уметь генерировать журналы событий с синхронизированным временем. Это позволяет определить, кто изменил конфигурацию в случае проблемного переключения или поведения сети. Для этого должен быть доступен протокол синхронизации времени NTP/SNTP. Системный журнал (Syslog) и SMTP также являются важными элементами, которые позволяют публиковать текстовый журнал/сообщения электронной почты на удалённом сервере и записывать изменения в ситуации в течение определённого периода времени. Обычными средствами предотвращения незаконных действий при выполнении базового контроля пользователей являются реализация тайм-аута и определение максимального количества повторных попыток установления пользовательского сеанса (рис. 5).

Шифрование данных

Шифрование/дешифрование SSL (Secure Sockets Layer – уровень защищённых сокетов) может использоваться для обеспечения конфиденциальности во время обмена данными. Наиболее критичный контент зашифровывается на стадии выхода, а затем дешифруется на стадии входа, для чего используются криптографические алгоритмы, встраиваемые в приложения TCP/IP (например, HTTP, TELNET и SNMP). В соответствии с этими принципами работают HTTPS, SSH и SNMPv3, использующие для шифрования полезной информации кадра алгоритмы AES/DES/3DES, реализованные в библиотеке SSL. В случае если трафик перехватывается хакерами с целью кражи критической информации, шифрование/дешифрование между двумя сторонами доступа обеспечивает повышенный уровень безопасности. На стороне передачи пакеты данных зашифрованы, так что информация в них не может быть идентифицирована. На принимающей стороне зашифрованные пакеты дешифруются с помощью согласованного ключа безопасно-

Рис. 5. Контроль прав пользователей

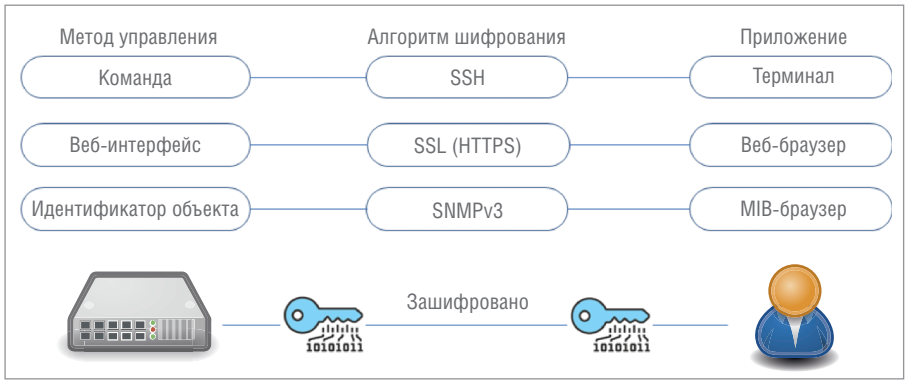


Рис. 6. Шифрование и дешифрование данных

сти, что делает контент идентифицируемым. Если пакеты всё же перехвачены, хакер может потратить практически бесконечное время, пытаясь взломать алгоритм шифрования, и оказаться неспособным сделать это (рис. 6).

Доступность сети

Реакция на события

Для обеспечения доступности сеть использует различные методы уведомления супервизоров о нерегулярном поведении сети. Самым простым из них является мигающий светодиод, указывающий на критическую ситуацию. Эта сигнализация может сопровождаться последующими процедурами, такими как сброс/перезагрузка системы. Например, если по неизвестным причинам создаётся сетевая петля, кроме генерации записи в журнале и мигания светодиода единственное последующее действие, выполняемое системой, – отключение порта, в котором была обнаружена петля, и изоляция её. Это, однако, всего лишь окольный путь, имеющий целью не допустить развития критической ситуации, – на самом деле изначальную проблему он не решает. Чтобы обеспечить соответствующий уровень реагирования, необходимо проводить постоянный мониторинг. Эта рутинная работа включает в себя опрос состояния узлов сети и выполнение выборки за определённый период. После сбора записей и выполнения обобщающих вычислений определяются нормальные границы функционирования. Впоследствии ненормальные условия оцениваются на основе выработанных пользовательских порогов. Предположим, что трафик в порту (загрузка порта) был, например, менее 10 МБ на протяжении последних двух недель, но затем в последней выборке внезапно увеличился до 100 МБ. Расчёт средней загрузки порта за последние 2 недели показал бы, что 10 МБ – это нормально; таким образом, пик трафика 100 МБ можно считать аномалией. В своей простейшей форме среднее значение каждого параметра выборки по времени вычисляется и сравнивается с текущим, чтобы определить, насколько новое значение выборки отличается от предыдущего среднего значения.

Сетевые ресурсы

Обеспечение пропускной способности является наиболее важной проблемой при рассмотрении сетевых ресурсов. Механизм ограниченной и гарантированной пропускной способности обеспечивает эффективную работу сети. Для обеспечения трафика без потерь гарантированная пропускная способность обеспечивает стабильность всех критически важных соединений, тогда как ограниченная пропускная способность отбрасывает недопустимые и опасные кадры в качестве превентивной меры против сетевых штормов. Для обеспечения доступности полосы пропускания компоненты сети оснащаются функциями контроля шторма и контроля скорости.

DDoS-атаки также представляют значительную угрозу доступности ресурсов, но такие атаки можно предотвратить, используя фильтр, выявляющий и отбрасывающий недопустимые кадры. Конечно, это не означает, что все DDoS-атаки можно распознать автоматически, поскольку некоторые кадры могут нести действительно ценный контент. Поэтому другим эффективным способом защиты от широковещательных, многоадресных или неизвестных одноадресных штормов является контроль штормов (рис. 7).

Блокировка вредоносного трафика

Отказ в доступе к порту

Самый простой способ предотвратить несанкционированный доступ через портовые соединения – отключить все необслуживаемые порты. Но хотя этот подход прост и эффективен, когда кому-то нужно использовать закрытый порт, он создаёт неудобства, поскольку системный администратор должен включить и настроить порт, прежде чем он станет доступным для использования. Для решения этой проблемы была разработана удалённая аутентификация 802.1X (стандарт EAP – Extensible Authentication Protocol – позволяет проверять подлинность при подключениях удалённого доступа). Этот процесс доверенной авторизации выполняет операции аутентификации с профессионального сервера безопасности RADIUS (Remote Authentication in Dial-In User Service – протокол для реализации аутентификации). Когда неавторизованный хост запускает процесс EAP для обмена информацией учётной записи с сетевыми компонентами, это, в свою очередь, запускает процесс RADIUS на сервере. По завершении аутентификации подключённый порт разблокируется для использования.

Отказ в доступе по MAC-адресу

Ещё один способ запретить доступ неавторизованным пользователям – добавить MAC-адреса доверенных пользователей в таблицу MAC-адресов коммута-

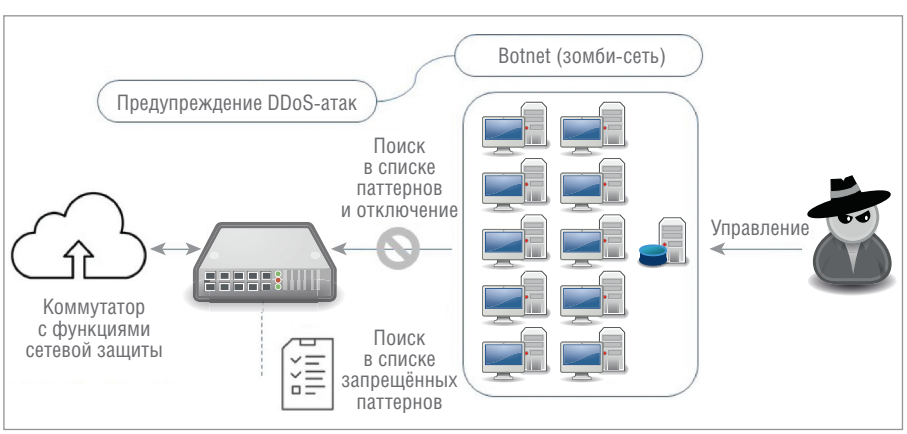


Рис. 7. Критерии определения доступности сети

тора и отключить механизм обучения подключённого порта. Эта таблица адресов доверенных пользователей называется белым списком MAC-адресов. Противоположностью белого списка является чёрный список MAC-адресов, куда записываются ненадёжные MAC-адреса. Если исходный MAC-адрес входящего кадра совпадает с адресом в чёрном списке, кадр немедленно отбрасывается. Другой, более продвинутой стратегией является ограничение максимального количества доверенных MAC-адресов для конкретного порта. Чтобы поддерживать соответствующий статус обучения, создаётся журнал нарушений, выявленных при анализе MAC-адресов, и системный администратор активно уведомляется об этих нарушениях.

Отказ в доступе по IP-адресу

Любой метод вторжения основан на одноранговом соединении через TCP/IP и маскируется в различных службах или приложениях (например, HTTP, TELNET и FTP). Хакеры могут подключаться к критически важным серверам данных, используя недопустимый IP-адрес. Эффективный способ защититься от этого и разрешить доступ к сети только доверенным IP-адресам заключается в создании белого списка IP-адресов. Чтобы гарантировать, что ненадёжным хостам не будет предоставлен доступ, белый список доверенных IP-адресов, также известный как список разрешённых IP-адресов, может быть настроен вручную, и только узлам с адресами из этого списка предоставляется доступ. В сети с доступным DHCP-сервером (DHCP – Dynamic Host Configuration Protocol – протокол динамической конфигурации узла) процедуры проверки безопасности обычно выполняются на нём (например, конкретным MAC-адресам разрешается назначать конкретные IP-адреса). Для обеспечения назначения только определённого диапазона IP-адресов можно использовать также опцию 82 DHCP (DHCP option 82 – опция протокола DHCP, использующаяся для того, чтобы проинформировать DHCP-сервер о том, от какого DHCP-ретранслятора и через какой его порт был получен запрос). Для обеспечения надёжности работы DHCP-сервера используется также механизм отслеживания законных назначений DHCP и автоматического добавления в белый список MAC-адреса, IP-адреса и подключённого порта доверенных хостов. Это предотвращает несанкционированный доступ со стороны настроенных IP-адресов. Попросту говоря, если сервером DHCP хосту не был назначен IP-адрес, это означает, что его не будет в белом списке. Таким образом, для этого хоста доступ к сети будет запрещён.

В соответствии с приведённым описанием, если ненадёжному хосту DHCP-сервером не может быть назначен IP-адрес, в качестве альтернативы не может использоваться фиксированный IP-адрес, поскольку он не будет находиться в белом списке, и, таким образом, ему всё равно не будет разрешён доступ к сети через данный коммутатор.

Отказ в доступе по содержимому кадра

Кадр является основной единицей сетевого трафика. Трафик в компьютерных сетях присутствует постоянно, и, за исключением специальной служебной информации, невозможно предугадать, когда появится новый трафик. Таким образом, гибкое определение значения каждого поля в кадре является сложной задачей, особенно потому, что создание белых и чёрных списков зависит от того, определены ли ненадёжные кадры. Создание белого списка приводит к удалению ненадёжных фреймов. Остаются лишь фреймы, считающиеся доверенными на основе совокупности фиксированных значений определённых полей. При создании чёрного списка кадры с фиксированными значениями для определённых полей в списке контроля доступа определяются как вредоносные, что приводит к отказу в доступе. Такие меры безопасности необходимы для защиты от вредоносных атак вирусов или попыток парализовать работу сети. Однако более гибким может быть подход с реализацией пользовательских фильтров содержимого или списков управления доступом для зонного шлюза. Такие фильтры разработаны в соответствии с архитектурой фрейма Ethernet и подразделяются на уровень 2 (уровень MAC), уровень 3 (уровень IP) и уровень 4 (уровень сервисов/приложений). Эта дифференциация предоставляет средства для организации различных действий, которые необходимо предпринять для предоставления или отклонения разрешения на передачу для трафика, ищущего доступ к сети (рис. 8).

Стратегии на будущее

Всё более изощрённые угрозы могут стать причиной серьёзных масштабных проблем, поэтому роль кибербезопасности неуклонно возрастает. Согласно отчёту Online Trust Alliance (OTA), дочерней компании организации Internet Society (Internet Society, ISOC, – международная профессиональная организация, занимающаяся развитием и обеспечением доступности сети Интернет), в 2017 году число кибератак в мире удвоилось. Пострадали организации всех размеров практически во всех отраслях. Статистика показывает, что чем крупнее бизнес, тем больше он подвержен атакам. И, конечно же, чем больше компания, тем выше стоимость простоя, вызванного атакой. Учитывая, что среднее время простоя на одну компанию в 2017 году составило 23 часа, финансовые затраты даже на одну кибератаку могут иметь катастрофические последствия для бизнеса.

Помимо денежных затрат кибератаки и потеря данных могут оказать существенное долговременное негативное влияние на репутацию бренда. Это особенно верно в чувствительных отраслях, где нарушения конфиденциальности могут разрушить доверие потребителей к компании или всему сегменту рынка. Вот почему так важна активная разработка надёжных методов кибербезопасности и безопасных систем управления паролями, а также не просто мероприятия по ликвидации последствий, но обучение сотрудников выявлению потен-

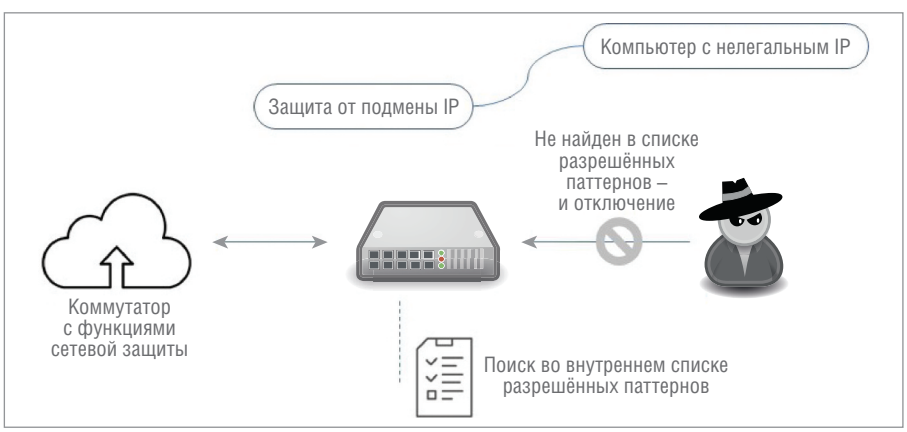


Рис. 8. Предотвращение злонамеренного доступа

циальных киберугроз. В современном онлайн-мире самые невинные, на первый взгляд, действия могут повлечь разрушительные последствия. Даже щелчок сотрудником по ссылке в электронном письме может фактически послужить стартом сложной фишинговой атаки или загрузки вируса. Но хорошая новость состоит в том, что, по оценкам экспертов, приблизительно 93% всех проблем такого рода можно избежать, если принять простые меры безопасности. По этой причине превентивные стратегии, нацеленные на защиту самых слабых точек сети, должны стать ключевой тенденцией для предотвращения катастрофических проблем в будущем.

Существует множество эффективных способов предотвращения кибератак, от регулярного обновления программного обеспечения и обучения сотрудников распознаванию фишинговых кампаний до внедрения двухфакторной аутентификации и проверки подлинности электронной почты. Но самое главное, что нужно усвоить для начала, – это тезис о том, что ни одна компания, ни большая, ни маленькая, не застрахована от киберугроз. ●

Статья подготовлена по материалам компании Advantech

Авторизованный перевод
Юрия Широкова
E-mail: textoed@gmail.com

НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ

ICONICS бесплатно предлагает ПО удалённого эксперта на время кризиса COVID-19

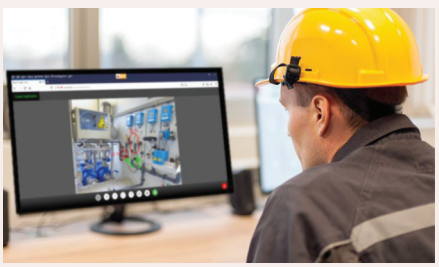
Компания **ICONICS** предлагает бесплатное использование своего программного обеспечения **CFSWorX™** в варианте «Удалённый эксперт» для специалистов, которые хотят решить проблемы с ограничениями по поездкам и с социальной изоляцией в период пандемии COVID-19.

ICONICS успешно работает на международном рынке промышленной автоматизации, диспетчеризации и умных зданий уже свыше 34 лет. Благодаря своему опыту с учётом современных тенденций ICONICS предлагает симбиоз программного обеспечения по организации выездного сервиса CFSWorX и технологии удалённого эксперта с MobileHMI, отвечающий всем современным стандартам по надёжности и уровню визуализации.

Даже после выхода из изоляционного периода Coronavirus/COVID-19 специалисты должны придерживаться мер по защите и безопасности ещё в течение долгого времени, чтобы избежать новых эпидемических вспышек. Перед руководителями предприятий в различных отраслях промышленности стоит задача, как обеспечить высокий уровень обслуживания с сохранением приоритета по безопасности работающих специалистов и ограничений по передвижению на удалённые объекты.

Решение для удалённого эксперта от ICONICS поможет руководителям организаций в различных отраслях промышленности найти выход, предоставив критическую дистанционную помощь там, где это необходимо. Операторы или специалисты заказчика на местах могут активировать режим удалённого эксперта ICONICS CFSWorX и MobileHMI на RealWear HMT-1 или любом другом поддерживаемом мобильном устройстве, чтобы мгновенно использовать знания интеграторов из диспетчерской или офиса. Можно запустить видеопоток с объекта в реальном времени и сделать отметки на изображениях, чтобы увеличить эффективность взаимодействия между объектом и офисом, действуя более быстро и продуктивно, без выезда группы специалистов на объект.

CFSWorX, в свою очередь, обеспечивает мониторинг подключённого оборудования в режиме реального времени, будь то локальное решение или работа через Интернет вещей. Когда подключённое оборудование сигнализирует о тревоге или неисправности, CFSWorX использует интеллектуальные алгоритмы и настраиваемую систему взвешенного анализа ситуации. На базе целого ряда настроек система самостоятельно определяет, какой специалист лучше всего подходит для выполнения конкретной заявки, возможно ли это починить удалённо. Диспетчеру в удалённом режиме через мобильное приложение предоставляются детальная информация о проблеме, а также полная история ремонта и рекомендации для быстрого устранения неисправности на объекте заказчика.



Предложение бесплатного использования программного обеспечения ICONICS CFSWorX™ в варианте «Удалённый эксперт» доступно сейчас только для новых проектов. Для подачи заявки на получение такого бесплатного программного пакета до конца 2020 года достаточно обратиться по электронному адресу marketing@iconics.com или оформить в свободной форме заявку на русском языке в компанию ПРОСОФТ по электронному адресу iconics@prosoft.ru.

Пакет предоставляет доступ к следующим функциям ПО:

- удалённая поддержка технических выездных специалистов и заказчиков для расширенного уровня взаимодействия и сотрудничества;
- потоковое видео и аудио для удалённых экспертов, чтобы улучшить качество решения проблем с расширенной базой знаний;
- поддержка удалённых пользователей на их существующих устройствах, а также носимых устройствах с помощью технологии дополненной реальности. ●

Basler занимает первое место среди производителей систем машинного зрения

Компания **Basler**, признанная лидером среди производителей промышленных систем машинного зрения, заняла первое место в сфере инноваций и подтвердила 7 из 8 критериев ранжирования, по данным исследовательской фирмы ABI Research, специализирующейся на глобальном рынке технологий. За Basler следуют Cognex и FLIR Systems, занявшие в общем зачёте второе и третье места соответственно. Все три вендора демонстрируют высокую узнаваемость брендов на рынке и имеют отличную репутацию, уделяют большое внимание простоте использования и развёртывания систем и являются инновационными и ориентированными на будущее компаниями по сравнению со своими конкурентами.

В процессе конкурсной оценки поставщиков промышленных камер машинного зрения проведены анализ и сравнение инновационной продукции двенадцати производителей промышленных датчиков машинного зрения и камер: Basler, Baumer, Cognex, FLIR Systems, FRAMOS, IDS Imaging, KEYENCE, Laon People, OMRON, SICK, Teledyne DALSA и TKH. Использовалась проверенная беспристрастная система критериев инноваций, внедрённая ABI Research. В ходе конкурентного исследования изучались технические возможности программного обеспечения вендора и оценивались реализации, ориентированные на коммерческую способность поставщика предоставлять свои решения по всему миру для применения на различных вертикальных рынках. ●