ПУТЕВОДИТЕЛЬ ПО ПРОДУКТУ

Средства защиты промышленных систем управления от компании Fortinet

Комплексная система обеспечения безопасности, соответствующая стандарту IEC-62443

Аннотация

В последнее время промышленные системы управления (ICS), играющие важную роль в корпоративных инфраструктурах и обрабатывающей промышленности, стали чаще подвергаться изощренным кибератакам.

Отчасти это последствие закономерного сближения эксплуатационных (OT) и информационных технологий (IT). Во всех вычислительных сферах происходит расширение сетевых подключений с помощью открытых стандартов, например Ethernet и TCP/IP, и сокращение затрат за счет замены специализированного оборудования серийным аппаратным и программным обеспечением. Эти тенденции не лишены преимуществ, однако приводят к росту количества уязвимостей.

В то время как отрицательные последствия нарушений безопасности для большинства ИТ-систем сводятся к материальным потерям, атаки на системы ICS также чреваты уничтожением оборудования и представляют собой угрозу для национальной безопасности и человеческих жизней.

Это играет принципиальную роль в том, как и почему действуют потенциальные злоумашленники. Львиную долю современных киберпреступлений составляют корыстные преступления, однако системы ICS в последнее время чаще становятся целями террористов и лиц, поддерживающих кибервойны. В силу этого злоумышленники располагают более значительными финансовыми и человеческими ресурсами, чем киберпреступники, действующие из корыстных побуждений. В особенности это относится к целевым атакам, спонсируемым государствами. Наиболее показательным примером является червь STUXNET, впервые обнаруженный в 2010 году.

Цель настоящего путеводителя — дать представление о том, каким образом решения Fortinet с помощью соответствующих стандартам многоуровневых средств защиты сетей способствуют устранению вышеперечисленных проблем и обеспечивают безопасность и надежность систем ICS, в частности тех, в которых задействована система диспетчерского управления и сбора данных (SCADA).

Потенциальные уязвимости

Разработка систем управления производственными процессами (ICS) исторически шла своим путем, независимым от развития ИТ-технологий, поэтому таким системам свойственны особые проблемы.

- Отсутствие средств обеспечения безопасности: большинство технологий, лежащих в основе систем ICS, отличаются повышенной надежностью, однако их разработчики не предусмотрели возможность доступа к ним из удаленных сетей, поэтому защитные меры сводились к ограничению физического доступа. Свою роль сыграла также относительно низкая распространенность компонентов систем (удаленные терминалы, программируемые логические контроллеры и т. д.) и в основном последовательных протоколов связи (Modbus, RP-570, Profibus, Conitel и т. д.).

- Ошибочная концепция «воздушной прослойки»: на первый взгляд привлекательная идея создания «воздушной прослойки» между системой ICS и остальными сетями продемонстрировала свою несостоятельность на практике. В настоящее время растет количество компонентов систем ICS, поддержание работоспособности которых требует обновления программного обеспечения и периодического внесения исправлений. В силу этого обстоятельства полностью избежать попадания в систему ICS данных извне практически невозможно. Даже при отсутствии постоянных сетевых подключений (или использовании только подключений, задействующих однонаправленные устройства, например диоды оптических данных) сети с «воздушными прослойками» остаются уязвимыми для проникновения вредоносных элементов с зараженных компьютеров и запоминающих устройств, таких как USB-накопители. Именно таким образом происходило распространение червя STUXNET.

- Появление новых направлений атак: по мере замены специализированного оборудования серийным аппаратным и программным обеспечением применение открытых стандартов, например Ethernet, TCP/IP и Wi-Fi, приводит к стремительному росту числа потенциальных уязвимостей. Распространение мобильных устройств и внедрение политики BYOD лишь усугубляют проблему.

- Использование устаревшего аппаратного и программного обеспечения, в том числе операционных систем (часто появившихся еще до возникновения понятия информационной безопасности), которые могут быть несовместимы со стандартными современными средствами защиты, например антивирусами.

- Нерегулярность обновлений и исправлений, связанная со сложностью процесса, высокой стоимостью и возможным прерыванием работы. Например, не всегда целесообразно прерывать работу предприятия для внесения исправлений в структуру одного из операционных серверов.

- Большое количество простых незащищенных телеметрических устройств, например датчиков и измерителей давления, манипуляции с данными которых могут негативно отразиться на безопасности и надежности системы в целом.

- Использование внедренного программного обеспечения, разработчики которого не уделили достаточного внимания техникам защиты и общепринятым стандартам кодирования.

- Недостаточно эффективное регулирование производства компонентов и системы поставок. Этот фактор чреват нарушением безопасности оборудования еще до его установки.

- Ограниченные возможности управления доступом/разрешениями: при связывании ранее изолированных или закрытых систем меры управления доступом конкретных лиц к определенным расположениям не всегда соответствуют стандартам безопасности в ИТ-сфере.

- Неудовлетворительно реализованная сегментация сети: в сетях ICS достаточно редко применяется стандартная мера обеспечения безопасности, заключающаяся в разделении сетей на функциональные сегменты. Эта мера ограничивает степень перекрытия данных и приложений между связанными сегментами.

- Недостаточная квалификация инженеров, занимающихся разработкой и обслуживанием систем, в сфере обеспечения безопасности.

Решение проблемы

Хорошая новость: в последнее время стали чаще проводиться исследования присущих системам ICS недостатков и уязвимостей и были предприняты первые шаги по их устранению.

Этому процессу могут способствовать правительственные органы, например, в США это Команда экстренного реагирования на кибератаки промышленных систем управления (Industrial Control Systems Cyber Emergency Response Team, ICS-CERT), в Великобритании — Центр защиты национальной инфраструктуры (Centre for Protection of National Infrastructure, CPNI). Обе эти организации публикуют указания и рекомендации по безопасности систем ICS.

Второй способ решения проблемы — установка единых стандартов по образцу ISA/IEC-62443 (ранее ISA-99). Стандарт ISA-99 был разработан Международной ассоциацией автоматизации (International Society for Automation, ISA), и впоследствии в целях обеспечения соответствия стандартам Международной электротехнической комиссии (International Electro-Technical Commission, IEC) ему был присвоен номер 62443. Эти документы дают представление о комплексной инфраструктуре разработки, планирования, интеграции и управления защищенными системами ICS.

В настоящее время стандарт находится в разработке и регулирует не все вопросы, связанные с основными уязвимостями систем, однако он содержит практические указания, например модель «зон, проводников, границ и уровней безопасности», направленную на устранение наиболее актуальных проблем сетевой безопасности систем ICS.

Организации ICS-CERT и CPNI рекомендуют предпринять меры по внедрению модели зон и проводников, которая значительно снижает риск вторжения и минимизирует негативные последствия нарушений.

Описанная в стандарте основная стратегия предусматривает разделение сети на функциональные «зоны» (которые в свою очередь могут делиться на подзоны) и определение «проводников», под которыми понимаются важные данные и приложения, перемещающиеся из одной зоны в другую. Затем каждой зоне присваивается уровень безопасности от 0 до 5, где 0 соответствует самому высокому уровню безопасности, а 5 — самому низкому. Для ограничения доступа к каждой зоне и проводнику применяются жесткие меры управления доступом, основанные на проверке подлинности пользователей и устройств.

Эта стратегия прекрасно сочетается с функциональностью корпоративных решений Fortinet, в частности брандмауэра Internal Segmentation Firewall (ISFW).

Защита сред ISC/SCADA с помощью средств Fortinet

Процесс развертывания эффективной системы обеспечения безопасности начинается с тщательной оценки деловых и операционных рисков и определения подходящей стратегии снижения этих рисков. На этом этапе согласно предписаниям стандарта IEC-62443 определяются зоны, проводники, границы и уровни безопасности.

В результате сеть приобретает вид, схожий с показанным на рисунке 1.

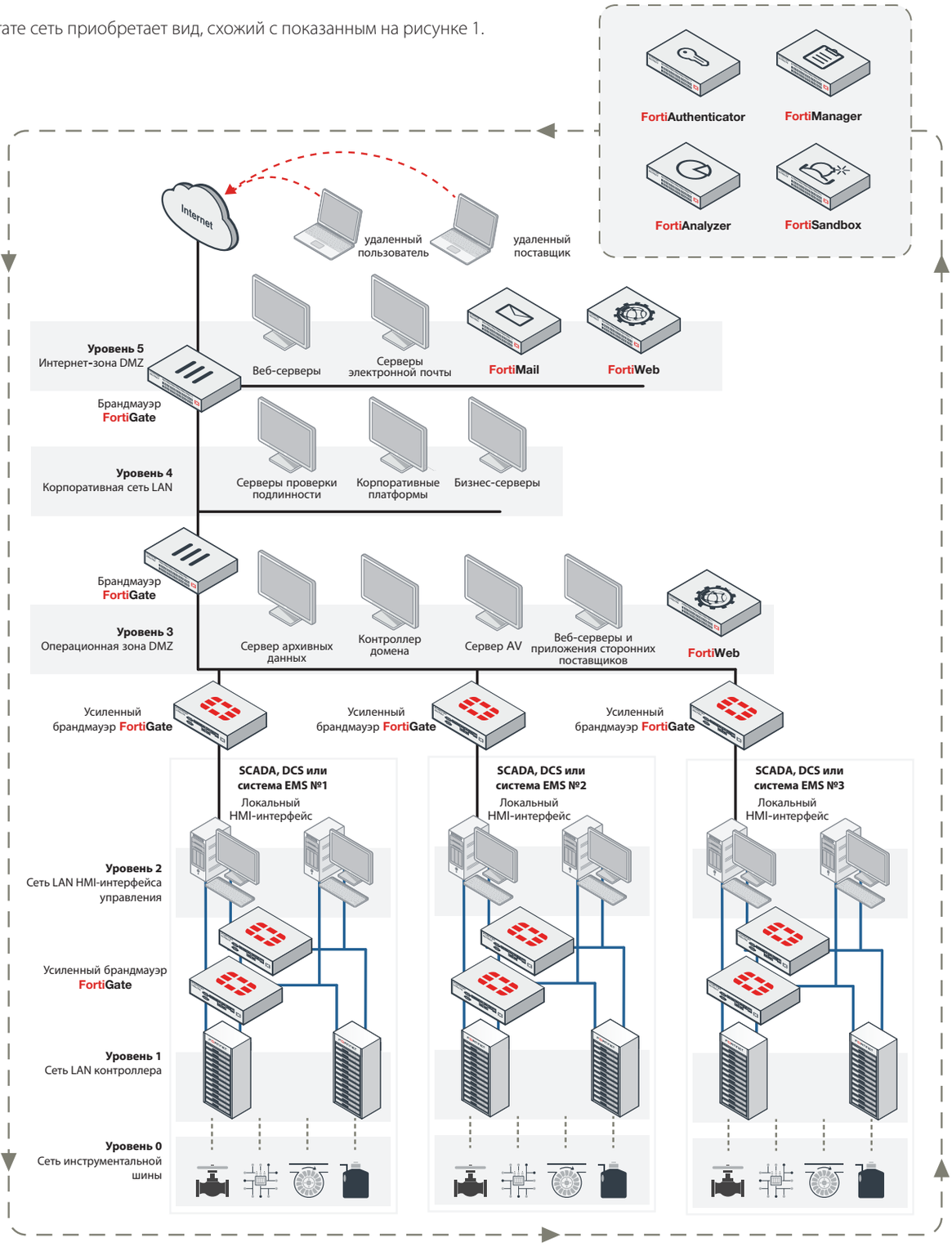


Рис. 1: уровни безопасности согласно стандарту ISA S99

Комплексная многоуровневая система безопасности

Многоуровневые средства обеспечения безопасности, входящие в линейку FortiGate, отличаются высокой доступностью и при необходимости поставляются в усиленном форм-факторе. Благодаря этому они идеально подходят для реализации модели зон и проводников независимо от важности инфраструктуры системы ICS и агрессивности среды.

Решение FortiGate использует режим развертывания брандмауэра «**Internal Segmentation Firewall**» (ISFW), поддерживающий функциональную и физическую сегментацию. В этом режиме функции высокопроизводительного брандмауэра сочетаются с антивирусом, средствами надежной двухфакторной проверки подлинности, предотвращения вторжений, фильтрации URL-адресов и Application Control. Решение FortiGate, оснащенное большим количеством высокоскоростных интерфейсов LAN и функцией аппаратного ускорения на основе особой технологии ASIC, поддерживает передачу данных между зонами на скорости более 100 Гбит/с.

В ходе реализации детализированных политик безопасности, доступных в режиме развертывания брандмауэров FortiGate ISFW, система ICS делится на зоны и проводники на основе таких факторов, как удостоверения пользователей, приложения, расположения и типы устройств. Таким образом, решение FortiGate™ может легко заблокировать любую зону и обеспечить прохождение между зонами только разрешенного и одобренного трафика, поступающего из авторизованных конечных точек.

Средства FortiGate и FortiSwitch™ также поддерживают альтернативный вариант развертывания подзон с маркировкой трафика VLAN 802.1Q. Однако в сетях VLAN рекомендуется использовать режим ISFW, так как он обеспечивает более эффективную изоляцию и сдерживание угроз, что актуально для критически важных систем.

Обеспечивающие безопасность продукты отличаются высокой гибкостью и масштабируемостью за счет комплексной работы операционной системы FortiOS™, решений для проверки подлинности FortiAuthenticator™ и FortiToken™, а также самообучающейся системы автоматического круглосуточного реагирования на угрозы FortiGuard™.

Централизованное управление, регистрация и составление отчетов

Решение FortiGate объединяет инфраструктуру в единую систему, управление которой осуществляется с помощью средств FortiManager™ и FortiAnalyzer™, которые сочетают централизованную настройку с регистрацией событий, их анализом и составлением отчетов, обеспечивая бесперебойную работу центра мониторинга и управления сетями.

Специальные функции с поддержкой систем ICS/SCADA

Средство FortiGate, использующее предопределенные и постоянно обновляющиеся сигнатуры, поддерживает идентификацию и реализацию политик для большинства популярных протоколов ICS/SCADA (см. список ниже) в целях определения проводников.

- Bacnet
- DLMS/COSEM
- DNP3
- EtherCAT
- ICCP
- IEC-60870.5.104
- Modbus/TCP
- OPC
- Profinet

Для этого применяется конфигурация политик безопасности, в которой каждому протоколу сопоставляются такие сервисы, как IPS, AV и Application Control.

Одновременно с поддержкой протоколов при помощи дополнительного набора сигнатур обеспечивается защита наиболее уязвимых точек приложений и устройств, произведенных основными поставщиками систем ICS (см. список ниже).

- ABB
- Advantech
- Elcom
- GE
- Rockwell
- Schneider Electric
- Siemens
- Vedeer Root
- Yokogawa

Эти меры способствуют реализации более детализированного управления трафиком между зонами на уровне приложений и обеспечивают обнаружение решением FortiGate попыток использования известных уязвимостей оборудования перечисленных поставщиков.

Управление доступом к зонам с помощью FortiAuthenticator и FortiToken

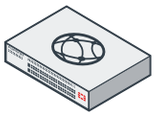
За счет интеграции с FortiGate и службами каталогов решение FortiAuthenticator обеспечивает реализацию детализированного управления доступом пользователей и устройств к каждой зоне и проводнику.

Средства управления проверкой подлинности пользователей FortiAuthenticator поддерживают двухфакторную проверку подлинности, проверку подлинности с помощью протоколов RADIUS и LDAP, проверку подлинности в беспроводной сети 802.1X, управление сертификатами и функцию единого входа Fortinet. Решение FortiAuthenticator совместимо с линейкой маркеров двухфакторной проверки подлинности FortiToken для безопасного удаленного доступа и дополняет ее, за счет чего становится возможной проверка подлинности различных средств обеспечения сетевой безопасности FortiGate и устройств сторонних производителей. Совместно работающие решения FortiAuthenticator и FortiToken поддерживают масштабируемую, экономичную и надежную проверку подлинности в пределах сетевой инфраструктуры.

Защита сервера архивных данных с помощью FortiDB

Потенциальными целями кибератак являются все центральные базы данных, однако наиболее уязвимы те из них, которые лежат в основе систем ICS. Это обусловлено тем, что исторически при создании и развертывании таких баз данных обеспечение их безопасности не входило в приоритеты разработчиков.

Решение FortiDB можно использовать для оценки текущего уровня безопасности, устранения уязвимостей и отслеживания доступа в целях обнаружения подозрительной активности. Гибкая инфраструктура политик обеспечивает эффективную защиту важных ресурсов.



Защита веб-интерфейса HMI с помощью FortiWeb

Несмотря на бесспорные преимущества управления производственными процессами с помощью удобных и экономичных веб-консолей, негативные последствия вторжения для серверной части в этой среде значительно выше, чем для большинства других веб-серверов.

Решение FortiWeb создает дополнительный уровень защиты систем ICS благодаря современным технологиям обеспечения двунаправленной защиты от поступления данных из сомнительных источников, DoS-атак на уровне приложений и изощренных угроз, например внедрения кода SQL и межсайтовых сценариев.

Обеспечение безопасности на основном направлении атак с помощью FortiMail

Незащищенные взаимодействия по электронной почте остаются основной уязвимостью, на которую нацелено большинство известных угроз. Этой уязвимостью пользуются не только авторы атак на системы ICS и их компоненты, и при разработке атак нередко применяются техники социальной инженерии.

Решение FortiMail™ обеспечивает защиту от атак снаружи, в том числе с применением современных вредоносных программ, а также от исходящих угроз и утечек данных. Это единственное решение, сочетающее функции защиты от нежелательной почты, фишинга и вредоносных программ, «песочницы», предотвращения утечки данных (DLP), шифрования на основе удостоверения (IBE) и архивации сообщений.

Реагирование на продвинутые постоянные угрозы

До недавнего времени приоритетными направлениями исследований являлись обнаружение и блокировка атак с помощью сигнатур. Слабое место этого подхода заключается в том, что он основан на применении данных о ранее обнаруженных угрозах. В ходе постоянного отслеживания тысяч активных клиентских сетей по всему миру в базе данных решения FortiGuard накоплен огромный массив сведений о существующих угрозах, однако для систем ICS негативные последствия вторжения слишком велики, поэтому важно обеспечить защиту от новых угроз.

В этом случае ключевыми факторами становятся быстрое обнаружение угрозы, предотвращение ее распространения и минимизация отрицательных последствий. Эти задачи выполняет средство FortiSandbox™ — важный компонент инфраструктуры защиты от продвинутых постоянных угроз Fortinet, разработанный специально для обнаружения и анализа современных атак, которые могут обойти более традиционные средства защиты на базе сигнатур.

Государственная сертификация и гарантии

Надежные и доказавшие свою эффективность решения Fortinet соответствуют стандарту правительства США FIPS 140-2 уровня 2 для модулей шифрования и международному стандарту сертификации Common Criteria EAL 4+. Проведенные независимыми организациями испытания продемонстрировали высочайший уровень эффективности наших многоуровневых средств обеспечения безопасности.

Сводная информация

Задача обеспечения безопасности систем ICS достаточно сложна, и не все ее аспекты освещены в настоящем путеводителе. Однако следование требованиям стандартов безопасности ICS-CERT/CPNI и применение прошедших государственную сертификацию средств (например, описанных выше решений, входящих в портфель Fortinet) значительно снижают вероятность успешных кибератак и их отрицательные последствия для систем ICS.

Поддержка сред ICS/SCADA является одним из основных направлений деятельности компании Fortinet, лидирующей на рынке многоуровневых средств обеспечения безопасности корпоративных сетей. Компания Fortinet обладает уникальными возможностями для решения задач безопасности, стоящих перед ее клиентами в сфере промышленного производства, и обеспечения надежной защиты наиболее важных инфраструктур и сервисов.

ГЛАВНЫЙ ОФИС
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
США
Телефон: +1.408.235.7700
www.fortinet.com/sales

ОТДЕЛ ПРОДАЖ В ЕБВА
120 rue Albert Caquot
06560, Sophia Antipolis,
Франция
Телефон: +33.4.8987.0510

ОТДЕЛ ПРОДАЖ В АТР
300 Beach Road 20-01
The Concourse
Сингапур 199555
Телефон: +65.6513.3730

ОТДЕЛ ПРОДАЖ В ЛАТИНСКОЙ АМЕРИКЕ
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
Ф.О. Мехико
Телефон: 011-52-(55) 5524-8480