Системы контроля и кибербезопасность

Карл Вильямс

В статье рассматриваются пути решения проблем, связанных с угрозами безопасности и уязвимостью систем управления и контроля предприятия. Предлагаются подходы и принципы построения многоуровневой системы безопасности, обеспечивающей защищённую работу сетевых управляющих систем.

Осмысление задач: что является наиболее серьёзной угрозой

За последнее время системы управления и контроля претерпели значительное изменение: по сравнению с системами, применявшимися ранее и имевшими изолированную природу, в современных системах возросло значение подключений, а также использование открытых стандартов и протоколов. Применение готовых технологий, созданных с учетом потребностей в дополнительных приложениях, анализа операций и их прозрачности, подключение к коммерческим и другим сетям не только дают огромные преимущества, включая возможности взаимодействия и повышенную эффективность, но и создают постоянные угрозы безопасности.

Имеющиеся на сегодняшний день угрозы безопасности и уязвимости системы очень разнообразны, нередко сложны и не всегда вполне понятны, особенно с точки зрения того, могут ли они оказывать влияние на отдельную систему, часть системы или всё производство, и если да, то какое. Угрозы кроются во внутренних источниках, таких как съёмные носители, и во внешних источниках, таких как подключения к другим устройствам и сетям. Угрозы могут быстро изменяться по мере возникновения новых уязвимостей. Таким образом, системы управления и контроля могут поставить под удар свою нормальную работу лишь тем, что они совместно используют технологии или подключения (прямые и непрямые). Хотя это не обязательно окажет немедленное или непосредственное разрушительное воздействие на производство: может снизиться производительность, а это само по себе нежелательно, и если не будут приняты соответствующие меры, в конечном счете, это ослабит безопасность и приведёт к производственным потерям.

В настоящее время наибольшая угроза исходит от бездействия системы. Предпринимая шаги по оценке безопасности и средств её обеспечения, а затем – по пониманию и управлению безопасностью на основе эффективных решений, можно уменьшить риск и вместе с тем сохранить безопасность и надёжность работы предприятия на должном уровне.

Меры по решению проблем

Угроза и уязвимость

Поскольку используются разнообразные системы управления и контроля, начиная от самых современных и кончая установленными ранее, существует большая потребность в обеспечении их безопасности. Риски, с которыми сталкиваются эти новые и устаревшие системы, могут значительно отличаться друг от друга, но независимо от возраста необходимо уметь оценивать и предпринимать самые эффективные меры по укреплению их безопасности, при этом в случае необходимости нужно обеспечивать возможность выполнять критически важные функции.

Понимание наиболее вероятных угроз играет жизненно важную роль в разработке стратегии обеспечения необходимых уровней защиты. В последнее время ведётся много дискуссий на тему угроз и уязвимостей, основное внимание которых чаще всего сосредоточено на проблеме хакерства. Имеющаяся у нас информация не свидетельствует о том, что наибольшую угрозу представляют собой действия взломщиков, по крайней мере, на сегодняшний день. Намного больше вероятность того, что систему контроля может поразить вредоносный код, будь то вирус, «червь» или «троянский конь».

Безопасность следует расценивать как обязательный компонент, обеспечивающий работу предприятия путем принятия мер, которые поддерживают доступность системы, при этом эффективный процесс управления уязвимостями играет здесь важнейшую роль. Выявленные уязвимости необходимо оценить, а затем предпринимать действия в соответствии с величиной риска и степенью потенциального воздействия.

Решения по обеспечению безопасности

Сегодня первое место среди угроз занимает угроза, исходящая от вредоносных кодов. Чтобы уменьшить её воздействие, необходимо использовать хорошо зарекомендовавшую себя систему глубокой защиты, а также изолировать критически важные производственные активы. Кроме того, необходимо предпринимать внутренние меры безопасности, включая разработку политик и процедур, а также контроль их соблюдения, и, если случится самое

© СТА-ПРЕСС

худшее, уметь управлять инцидентом и осуществлять восстановление системы.

Можно предложить следующие основополагающие принципы для обеспечения безопасности.

- Безопасность должна оцениваться с точки зрения управления и технологических процессов.
- К обеспечению безопасности необходимо подходить как со стороны информационных технологий, так и со стороны систем управления и контроля.
- Необходимо спроектировать и разработать несколько уровней безопасности сети, системы и приложений.
- Необходимо обеспечить соблюдение отраслевых, правовых и международных стандартов.
- В производственных системах управления и контроля основную роль должны играть превентивные меры и средства своевременного обнаружения.

Многоуровневая система безопасности – глубокая защита

Говоря о разработке и реализации мер, направленных на уменьшение уязвимостей и угроз, рекомендуется использовать подход глубокой защиты. На приведённой схеме (рис. 1) изображена типичная архитектура, используемая для устранения различных угроз безопасности.

Для каждого уровня оценивается степень важности и сопряжённые риски, а также принимаются соответствующие меры по обеспечению безопасности. Чтобы пройти очередной уровень системы безопасности, угроза должна преодолеть соответствующий барьер, образованный управленческими (политики и процедуры) и техническими средствами. Такой подход создаёт наиболее устойчивую архитектуру.

Этот подход гарантирует, что самые важные активы будут защищены максимальным числом уровней безопасности. Таким образом, выявленная угроза вызовет своевременный запуск реакции на неё. При условии успешной реализации и правильного использования такая стратегия глубокой защиты сведёт до минимума вероятность успешных атак и позволит предотвратить несанкционированные вторжения в систему. Такой подход считается наиболее эффективным превентивным способом обеспечения безопасности.

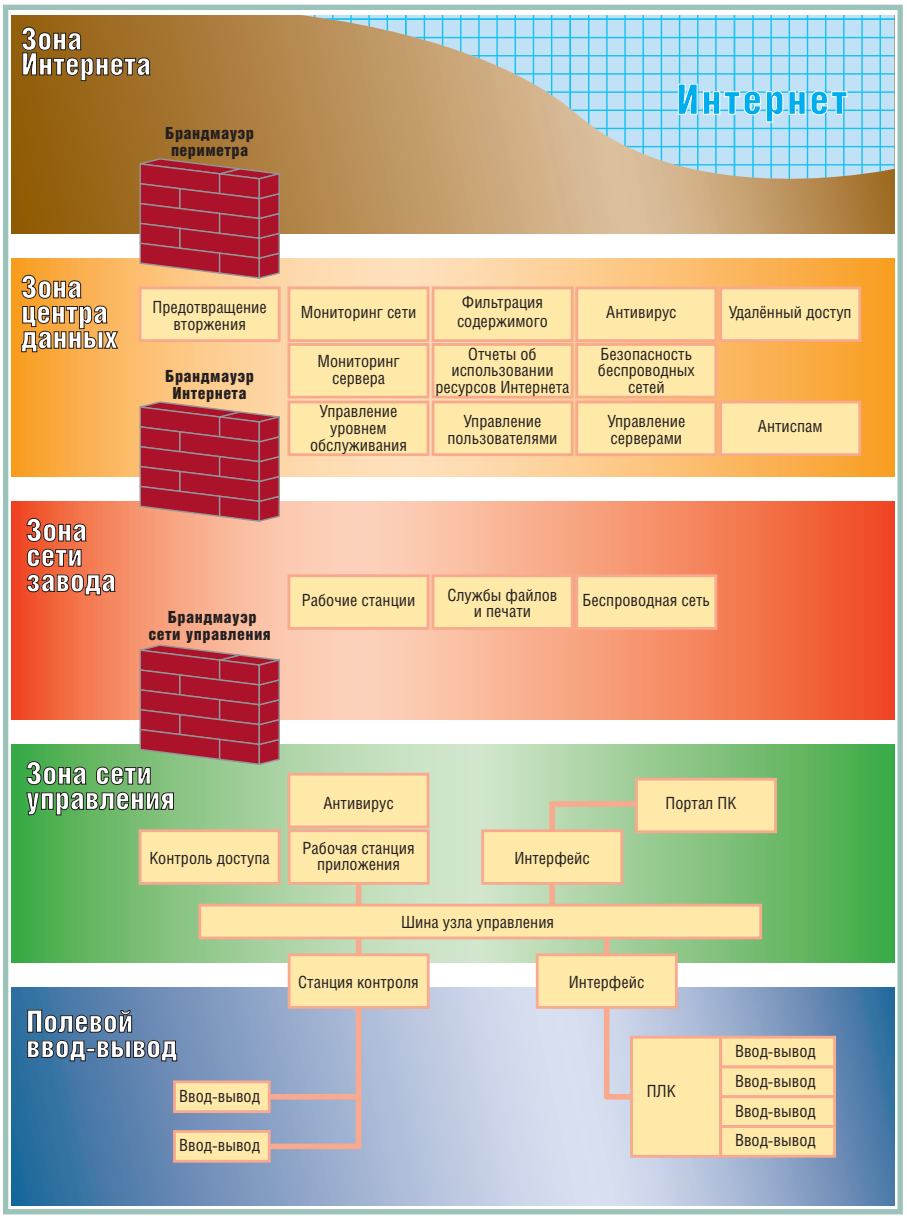


Рис. 1. Архитектура, используемая для устранения различных угроз безопасности

Кроме того, уменьшить угрозу можно с помощью дополнительных программных продуктов обеспечения безопасности, таких как брандмауэр узла, защита рабочих станций, антивирусные программы и приложения управления уязвимостями. Хотя реализация соответствующих мер по уменьшению рисков помогает укрепить безопасность, для поддержания эффективности системы безопасности необходимо осуществлять её постоянный контроль: систему нельзя просто «внедрить и забыть».

Программа безопасности должна соответствовать особым требованиям системы и среды внедрения, но необходимо также учитывать и общие положения, указанные далее:

- оценка безопасности;
- политики, процедуры и контроль обеспечения безопасности;
- защита с использованием соответствующей технологии;
- обучение принципам соблюдения безопасности при обмене данными;
- управление безопасностью.

Оценка безопасности

Оценка безопасности – один из первых шагов, который необходимо сделать в ходе анализа состояния безопасности. Оценивая текущее состояние, уязвимости и угрозы, можно получить представление о реальных рисках, на основе чего вырабатываются требования к программе обеспечения безопасности.

Политики, процедуры и контроль обеспечения безопасности

Эффективные политики, процедуры и контроль обеспечения безопасности (оценка, аудит и отслеживание) явля-

© СТА-ПРЕСС

PEPPERL+FUCHS
PROTECTING YOUR PROCESS

Созданы для безопасной работы
во взрывоопасных зонах

Взрывозащищённые средства операторского интерфейса

Взрывозащищённые персональные компьютеры и мониторы серии VisuNet, предназначенные для создания человеко-машинного интерфейса (ЧМИ) во взрывоопасных зонах с применением стандартной сетевой технологии Ethernet для передачи данных.
Установка во взрывоопасных зонах классов 1, 2 и 22

Взрывозащищённые диспетчерские блоки контроля и индикации серии TERMEX с монохромными графическими/текстовыми ЖК-дисплеями для подключения к ПЛК и системам с применением ПК.
Установка во взрывоопасных зонах классов 1, 2 и 22

Все оборудование сертифицировано и имеет Разрешение Ростехнадзора РФ

Официальный дистрибьютор продукции Pepperl+Fuchs в странах СНГ

ProSoft®

МОСКВА (495) 234-0636 • (495) 234-0640
info@prosoft.ru • www.prosoft.ru
С.-ПЕТЕРБУРГ (812) 448-0444 • (812) 448-0339
info@spb.prosoft.ru • www.prosoft.ru
ЕКАТЕРИНБУРГ (343) 376-2820 • (343) 376-2830
info@prosoftsystems.ru • www.prosoftsystems.ru
САМАРА (846) 277-9166 • (846) 277-9165
info@samara.prosoft.ru • www.prosoft.ru
НОВОСИБИРСК (383) 202-0960; 335-7001; 335-7002
info@nsk.prosoft.ru • www.prosoft.ru
КАЗАНЬ (843) 291-7555
info@kzn.prosoft.ru • www.prosoft.ru
УФА (347) 2925-216; 2925-217 • (347) 2925-218
info@ufa.prosoft.ru • www.prosoft.ru

Реклама

#123

ются необходимым условием безопасной и надёжной работы системы. Чтобы получить действенный и эффективный результат, необходимо вести разработку политик и вспомогательных процедур с учётом требований конечных пользователей и производственных подразделений, то есть в тесном сотрудничестве с заинтересованными лицами. Для достижения успеха в этой области необходима поддержка руководства на всех уровнях, вместе с тем необходимо учитывать все требования к соблюдению корпоративных и бизнес-политик и процедур.

Защита с использованием соответствующей технологии

Технология играет важную роль в реализации обеспечения безопасности в целом. Брандмауэр – лишь один пример технологии, являющейся частью схемы глубокой защиты; при успешном внедрении и правильном управлении он позволит уменьшить уязвимость и угрозу безопасности. Однако для обеспечения безопасности нужен не только брандмауэр.

Разработка и реализация архитектуры с помощью DMZ* делает доступ и контроль более безопасным. Кроме того, для укрепления защиты можно использовать дополнительные функции, такие как антивирус, глубокое сканирование пакетов с целью обнаружения и предупреждения вторжения. Необходимо тщательно продумать возможность постоянного управления брандмауэрами и другими техническими средствами.

Устаревший антивирус не защитит от новых вредоносных кодов. Необходимо предусмотреть механизм обновления систем с применением подключения к сети или без него. Это позволит защититься от вредоносных кодов, которые попадают в систему через сетевые подключения или со съёмных носителей, таких как USB-накопители или компакт-диски.

Обучение принципам соблюдения безопасности при обмене данными

Необходимо проводить периодический или разовый инструктаж по вопросам поддержания безопасности для пользователей, имеющих прямой или опосредованный доступ к системе управления и контроля, что позволит создать производственную среду с низким уровнем риска. Важно, чтобы сотрудники, взаимодействующие с критически важными системами, осознавали, какие последствия могут иметь их действия. Обучение также необходимо для того, чтобы пользователи систем управления имели ясное понимание политик, процедур, требований к соблюдению безопасности и получили более полное представление о них. Кроме того, может потребоваться провести инструктаж по техническим аспектам, таким как брандмауэры, ПО обнаружения и предотвращения вторжения, обновление антивирусов и т. д.

Управление безопасностью

Управление безопасностью включает в себя множество мероприятий, при этом важно учитывать все ресурсы, необходимые для их проведения. Такая работа требует изрядных усилий. В настоящее время существуют такие программы безопасности, в которых безопасность является «образом жизни»: уровень безопасности постоянно отслеживается, оценивается и анализируется. Этот подход также желательно применять к системам цифровой безопасности и средствам управления такими системами.

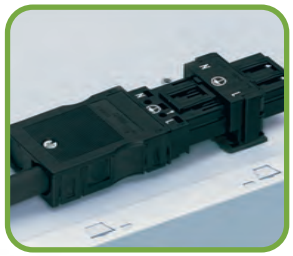
Некоторые элементы системы безопасности практически не требуют обновлений после внедрения (например, политика), другие же, напротив, нуждаются в частом или даже постоянном внимании (например, обновления антивируса, управление брандмауэром, управление доступом, управление уязвимостями, обеспечение соблюдения требований и т. д.). Оценку отдельных систем нужно проводить с учётом их потребностей и условий применения, однако использование модели непрерывного жизненного цикла «оценка – разработка – реализация – управление» с дополнительными элементами на каждой фазе позволит добиться гибкости, необходимой для создания среды с низким уровнем риска. ●

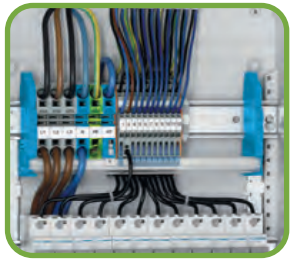
Автор – главный консультант по безопасности Invensys Process Systems

* DMZ (demilitarized zone, демилитаризованная зона) – часть компьютерной сети, находящаяся между локальной сетью и Интернетом. Обеспечивает выход в Интернет и внешнее присутствие в нём, скрывая при этом внутреннюю сеть организации и предотвращая прямое обращение к ней.

© СТА-ПРЕСС

ВСЁ ДЛЯ СТРОИТЕЛЬНОГО ЭЛЕКТРОМОНТАЖА

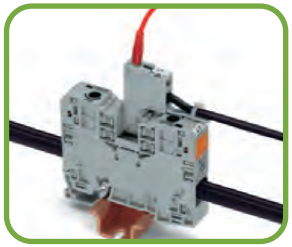


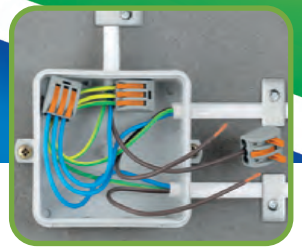


WAGO®

INNOVATIVE CONNECTIONS

ОТ КЛЕММ ДО ИНТЕЛЛЕКТУАЛЬНОГО ЗДАНИЯ





© СТА-ПРЕСС

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР WAGO В РОССИИ И СТРАНАХ СНГ

#403

Реклама

ProSoft®

МОСКВА	Тел.: (495) 234-0636 • Факс: (495) 234-0640 • E-mail: info@prosoft.ru • Web: www.prosoft.ru
С.-ПЕТЕРБУРГ	Тел.: (812) 448-0444 • Факс: (812) 448-0339 • E-mail: info@spb.prosoft.ru • Web: www.prosoft.ru
ЕКАТЕРИНБУРГ	Тел.: (343) 376-2820 • Факс: (343) 376-2830 • E-mail: info@prosoftsystems.ru • Web: www.prosoftsystems.ru
САМАРА	Тел.: (846) 277-9166 • Факс: (846) 277-9165 • E-mail: info@samara.prosoft.ru • Web: www.prosoft.ru
НОВОСИБИРСК	Тел.: (383) 202-0960; 335-7001/7002 • E-mail: info@nsk.prosoft.ru • Web: www.prosoft.ru
КИЕВ	Тел.: (+380-44) 206-2343/2478/2496 • Факс: (+380-44) 206-2343 • E-mail: info@prosoft-ua.com • Web: www.prosoft.ru
УФА	Тел.: (347) 2925-216; 2925-217 • Факс: (347) 2925-218 • E-mail: info@ufa.prosoft.ru • Web: www.prosoft.ru
КАЗАНЬ	Тел.: (843) 291-7555 • E-mail: kazan@prosoft.ru • Web: www.prosoft.ru
ОМСК	Тел.: (3812) 286-521 • E-mail: omsk@prosoft.ru • Web: www.prosoft.ru
ЧЕЛЯБИНСК	Тел.: (351) 239-9360 • E-mail: chelyabinsk@prosoft.ru • Web: www.prosoft.ru
КРАСНОДАР	Тел.: (861) 224-9513 • Факс: (861) 224-9513 • E-mail: krasnodar@prosoft.ru • Web: www.prosoft.ru