Кибербезопасность крупного бизнеса

KASPERSKY lab

Kaspersky Industrial Cybersecurity: обзор компонентов решения

ics.kaspersky.ru

Kaspersky Industrial Cybersecurity: обзор компонентов решения

Рост числа атак на промышленные системы

Число кибератак на промышленные системы растет. Если недавно эта проблема носила умозрительный характер, сейчас она приобрела реальные очертания[1].67% процентов офицеров безопасности определяют уровень угроз для АСУ ТП как критический или высокий — таким образом, по сравнению с предыдущим годом, этот показатель увеличился на 43%[2].

[1] PwC: Global State of Information Security («Глобальное состояние информационной безопасности»), 2015 г.

[2] SANS 2016 State of ICS Security Survey («Исследование о состоянии безопасности АСУ ТП»)

Операционные технологии и информационные технологии: в чем разница

Автоматизированные системы управления технологическими процессами (АСУ ТП) — собирательный термин, описывающий автоматизированные системы, которые контролируют производственный процесс. Термин АСУ ТП относится к широкому спектру компьютеров, специфических устройств управления и сетевых архитектур, используемых для контроля технологических процессов в самых разных отраслях промышленности.

АСУ ТП обычно включает в себя:

- SCADA (Supervisory Control And Data Acquisition — диспетчерское управление и сбор данных), РСУ (распределенные системы управления), УСО (устройство связи с объектом), ИЭУ (интеллектуальные электронные устройства), ПЛК (программируемые логические контроллеры) и системы диагностики.
- Связанные с этими технологиями автоматизации внутренние, человеческие, сетевые или машинные интерфейсы, которые используются для обеспечения контроля, безопасности и выполнения производственных процессов (непрерывных, серийных, дискретных и др.).

Многие стратегии обеспечения IT-безопасности прежде всего ориентированы на защиту данных и базируются на модели Конфиденциальность-Целостность-Доступность. В операционных технологиях самое важное — непрерывность, поэтому защищаются не данные, а сам процесс производства. Другими словами, в промышленных сетях порядок приоритетов безопасности обратный: Доступность-Целостность-Конфиденциальность. Это определяет специфические потребности в области кибербезопасности — высочайший уровень безопасности для промышленных предприятий бесполезен, если он подвергает риску непрерывность (или целостность) процессов.

В последние пять лет риск прерывания цепочек поставок и нарушения производства стал первостепенной проблемой для деловых кругов всего мира. Сегодня на передний план выходит риск кибератак[3]. Особенно велика их опасность для организаций, эксплуатирующих промышленные системы или объекты критически важной инфраструктуры.

Нарушение промышленной безопасности чревато последствиями, выходящими далеко за рамки финансового ущерба и потери деловой репутации. Во многих случаях защита промышленных систем от киберугроз имеет критическое значение с экологической, социальной и макроэкономической точки зрения.

Угрозы и риски

Несмотря на то, что угрозы для АСУ ТП стали широко известными, многие модели обеспечения кибербезопасности основаны на устаревших предположениях, что для защиты промышленного предприятия достаточно физической изоляции систем (через так называемые «воздушные зазоры») и концепции security by obscurity (безопасность через неясность). Это далеко не так — в эпоху четвертой промышленной революции большинство промышленных сетей так или иначе доступны через интернет[4].

Масштабное исследование «Лаборатории Касперского», которое опиралось на данные облачной сети Kaspersky Security Network, показало, что большинство промышленных рабочих станций подвержены тем же угрозам, что и бизнес-системы (IT), включая троянцы, компьютерные черви, потенциально нежелательные и опасные программы и эксплойты, которые используют уязвимости ОС Windows. Во второй половине 2016 года продукты «Лаборатории Касперского» заблокировали попытки атак на 39,2% защищаемых компьютеров, которые относятся к категории промышленной OT-инфраструктуры.

Червь Kido (известный также как Conficker), хотя и не предназначался специально для атак на промышленные сети, вызвал приостановку атомной электростанции в Германии в апреле 2016 года. Это произошло не в результате проникновения в АСУ ТП, а с помощью заражения смежной офисной сети.

Растет число угроз для АСУ ТП со стороны программ-вымогателей. За последние годы эта категория угроз стала гораздо масштабнее и разнообразнее. Особенно опасны программы-вымогатели для промышленных сред — заражение этих систем может иметь сильный эффект и вызвать широкомасштабный ущерб. Это делает АСУ ТП привлекательной мишенью для злоумышленников. При этом программы-вымогатели, атакующие АСУ ТП, имеют свою специфику: вредоносное ПО нацелено не на шифрование файлов, а на прерывание технологического процесса или блокирование доступа к важнейшим активам.

[3] Allianz Risk Barometer, 2017 г.

[4] ICS and their online availability (АСУ ТП и их доступность через интернет), «Лаборатория Касперского», 2016 г.

Помимо угроз общего характера, промышленный сектор сталкивается с целенаправленными атаками и специализированным вредоносным ПО. Stuxnet, Havex, BlackEnergy, PLC Blaster, Ladder Logic Bomb, Pin Control Attack — этот список постоянно пополняется. И, как показали атаки Stuxnet и Black Energy, одного зараженного USB-накопителя или фишингового письма достаточно, чтобы злоумышленники преодолели «воздушный зазор» и проникли в изолированную сеть.

Многие специализированные атаки разворачиваются и на уровне корпоративной сети, и на уровне АСУ ТП. Примером может служить атака BlackEnergy на украинские электростанции, которая в декабре 2015 году привела к многочасовому отключению электричества. Для реализации этой атаки злоумышленники использовали несколько векторов. Сначала они получили доступ к учетным данным системы SCADA с помощью таргетированной фишинговой рассылки. Обладая этими данными доступа, они начали выключать электрораспределительную сеть. После этого они внедрили вредоносный модуль KillDisk, который уничтожил или перезаписал важные системные файлы в промышленной сети. Параллельно с этим, колл-центр поставщика электричества подвергся DDoS-атаке, и это помешало потребителям электроэнергии вовремя сообщить об отключениях.

Помимо вредоносного ПО и целевых атак, промышленные организации сталкиваются с целым рядом угроз и рисков, направленных на людей, процессы и технологии. Как явствует из сказанного выше, недооценка этих опасностей может иметь серьезные последствия. «Лаборатория Касперского» разработала комплексный набор технологий, решений и сервисов, чтобы помочь своим клиентам предотвратить риски, включая следующие:

- ошибки операторов или подрядчиков (третьих сторон), работающих с системами SCADA;
- действия сотрудников (намеренные и случайные);
- несоблюдение требований регулирующих органов;
- неосведомленность о том, как расследовать инциденты и собирать о них достоверные данные.

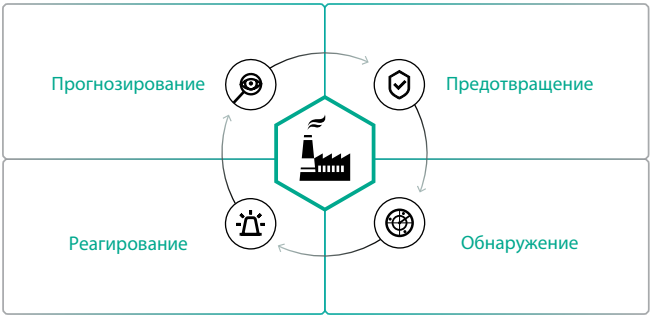
Только те поставщики защитных решений безопасности, которые понимают различия между промышленными системами и стандартными сетями коммерческих предприятий, могут предложить продукты, отвечающие уникальным потребностям систем ICS и операторов производственных инфраструктур. По мнению Forrester, промышленные предприятия, выбирающие поставщика решений безопасности, должны «ориентироваться на опыт специализированной работы в сфере промышленности»[5]. Аналитическая компания говорит о «Лаборатории Касперского» как об одном из немногих производителей, предлагающих специализированные решения в сфере промышленной безопасности, которые основаны на реальном опыте работы.

[5] «Профессионалы в области кибербезопасности больше не могут не замечать угрозы для критической инфраструктуры» (S&R Pros Can No Longer Ignore Threats to Critical Infrastructure), исследование Forrester, 2014

«Лаборатория Касперского» – надежный поставщик решений промышленной кибербезопасности

«Лаборатория Касперского» — признанный лидер в обеспечении кибербезопасности и защите промышленных систем[6]. Компания постоянно разрабатывает решения, которые успешно противостоят постоянно развивающимся угрозам для критически важных инфраструктур. Компания также помогает промышленных предприятиям, регулирующим органам и государственным учреждениям прогнозировать изменения в структуре угроз и противостоять атакам.

«Лаборатория Касперского» приобрела статус доверенного партнера и поставщика решений безопасности для ведущих промышленных предприятий, которые много лет пользуются ее защитой от вредоносного ПО. Кроме того, компания сотрудничает с признанными в мире организациями и производителями в сфере промышленной автоматизации (Emerson, SAP, Siemens, Schneider Electric, Industrial Internet Consortium и др.), чтобы обеспечить взаимную совместимость, а также создать специализированные процедуры и платформы сотрудничества, которые позволят защитить промышленные среды от существующих и возникающих киберугроз (в том числе комплексных целенаправленных атак).



Адаптивная стратегия обеспечения безопасности

[6] Справочное руководство по решениям в области безопасности операционных технологий, Gartner, 2017

«Лаборатория Касперского» развивает свой набор специализированных решений, удовлетворяющих специфические потребности промышленного сектора экономики. Эти решения обеспечивают защиту от киберугроз на всех уровнях промышленных систем (в том числе серверов SCADA, человеко-машинного интерфейса, рабочих станций, ПЛК и сетевых соединений), не влияя на непрерывность работы и стабильность технологического процесса.

Решение для защиты критической инфраструктуры Kaspersky Industrial CyberSecurity соответствует адаптивной стратегии обеспечения безопасности.

Kaspersky Industrial CyberSecurity: сервисы

Набор экспертных сервисов, предлагаемый «Лабораторией Касперского», составляет важную часть решения Kaspersky Industrial CyberSecurity. В него входят обучение сотрудников, анализ защищенности промышленных сетей, расследование инцидентов безопасности и другие сервисы.

Знания (обучение и аналитика)

- **Тренинги по кибербезопасности.** Курсы для специалистов по IT-безопасности, операторов и инженеров АСУ ТП. В процессе тренинга участники получают понимание актуальных угроз и эффективных методов защиты от них. Курсы также помогают повысить экспертизу специалистов по безопасности в таких областях, как тестирование на проникновение и цифровая криминалистика.

- **Аналитические отчеты.** Актуальные аналитические отчеты, подготовленные специально для вашей компании командой ICS CERT.

- **Повышение осведомленности.** Игровые тренинги, которые повышают осведомленность об угрозах, специфических для промышленных сред, и развивают навыки противодействия таким угрозам. В частности, игра Kaspersky Industrial Protection Simulation моделирует реальные атаки на автоматизированные промышленные системы и показывает, на что необходимо обратить особенное внимание при защите критической инфраструктуры.

Экспертные сервисы

- **Оценка защищенности от киберугроз.** Предварительная оценка защищенности инфраструктуры, которая проводится до установки решения и практически не влияет на производственные процессы. Это первый шаг к пониманию уровня защищенности от актуальных угроз и необходимых мер по защите инфраструктуры в контексте потребностей заказчика.

- **Интеграция решения.** Помощь экспертов «Лаборатории Касперского» в интеграции решения в архитектуру с уникальными или специализированными компонентами (аппаратными и программными), в том числе для специфических алгоритмов, протоколов, ПО и оборудования. Специалисты «Лаборатории Касперского» могут адаптировать средства защиты к работе с существующими системами.

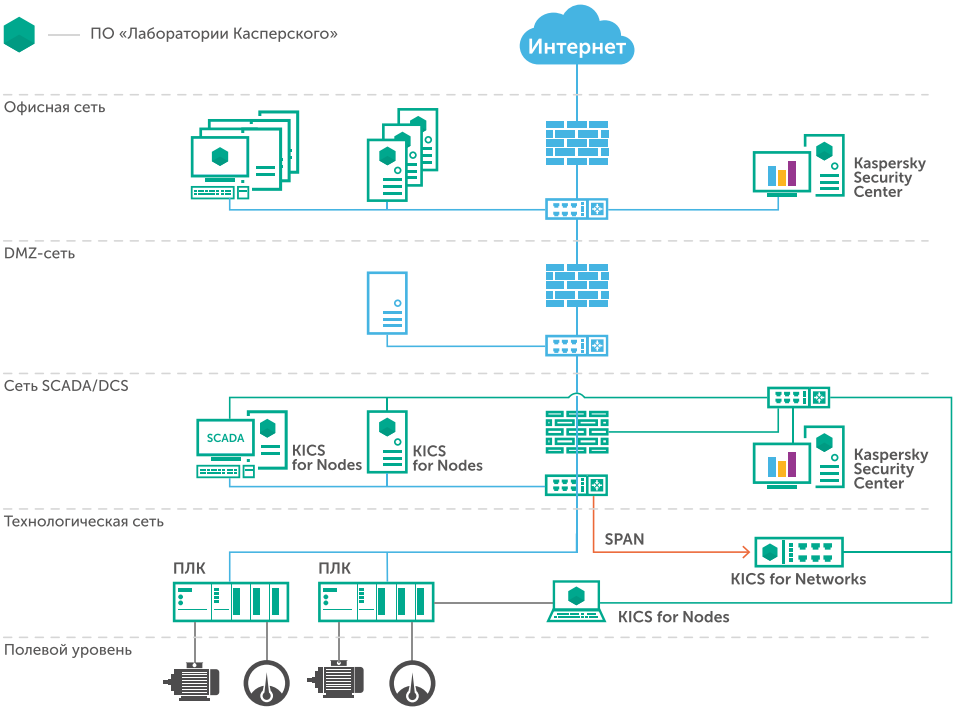
- **Расследование инцидентов.** Услуги по анализу вредоносного ПО и устранению последствий инцидентов. В случае возникновения инцидента в области кибербезопасности эксперты «Лаборатории Касперского» помогут собрать и проанализировать данные, реконструировать инцидент на временной шкале, определить источник и характер угроз и разработать план восстановления системы. Кроме того, «Лаборатория Касперского» предлагает сервис анализа вредоносного ПО — в соответствии с собственными методиками эксперты проанализируют образец вредоносного ПО, его функции и поведение, а также дадут пошаговые рекомендации по удалению его из системы и откату вредоносных действий.

Kaspersky Industrial CyberSecurity: централизованное управление

Kaspersky Security Center

Чтобы обеспечить высочайший уровень защиты производственной инфраструктуры от атак любой направленности, нужно обезопасить и узлы, и сеть. Управление решением Kaspersky Industrial CyberSecurity — как и всеми защитными продуктами «Лаборатории Касперского» — осуществляется из единой консоли Kaspersky Security Center. Это позволяет добиться оптимального контроля, простоты администрирования и прозрачности.

- Централизованное управление политиками безопасности — возможность установить разные защитные настройки для разных узлов и групп;
- Возможность тестирования обновлений перед распространением — позволяет сохранить целостность процессов.
- Доступ на основе ролей, связанный с политиками безопасности и срочными действиями.



Kaspersky Security Gateway

KICS может передавать данные о событиях в промышленной сети в другие системы, такие как SIEM, MES и системы бизнес-аналитики (BI). Все обнаруженные события и аномалии, отправляемые в сторонние системы – в том числе SIEM, почтовые системы, серверы syslog и системы управленью сетью, – передаются с помощью протоколов CEF 2.0, LEEF и Syslog. Это помогает обнаруживать и расследовать кибератаки и предоставляет расширенные возможности мониторинга для прогнозирования и предотвращения будущих атак.

Интеграция с человеко-машинными интерфейсами (HMI)

Решение может передавать уведомления о нарушениях безопасности напрямую в операторские панели – таким образом сотрудники промышленного уровня получают необходимую информацию для немедленного реагирования на инцидент или его эскалации.

Kaspersky Industrial CyberSecurity for Nodes

KICS for Nodes создано специально для защиты от угроз на уровне оператора в средах АСУ ТП. Оно обеспечивает безопасность на уровне сервера ICS/SCADA, человеко-машинного интерфейса и инженерных рабочих станций и отражает угрозы, которые могут быть вызваны человеческим фактором, вредоносным ПО, целевыми атаками и диверсиями. Решение совместимо с программными и аппаратными компонентами промышленных систем автоматизации, таких как SCADA, ПЛК и РСУ.

Риски и угрозы	Защитные технологии «Лаборатории Касперского»
Запуск нежелательного ПО	Белые списки; два режима – только обнаружение или обнаружение и блокирование
Вредоносное ПО	Передовые технологии сигнатурной защиты, облачные средства защиты с помощью репутационной базы Kaspersky Security Network или репутационной базы для изолированных сетей Kaspersky Private Security Network
Блокировщики и шифровальщики	Анти-Криптор
Сетевые атаки	Сетевой экран на уровне хоста
Подключение нежелательных устройств	Контроль устройств
Неавторизованные соединения с сетями Wi-FI	Контроль беспроводных сетей
Подмена программ ПЛК	Контроль целостности ПЛК
Особенности АСУ ТП - воздушные зазоры, ложные срабатывания и проч.	Доверенные обновления, которые тесируются с ПО ведущих производителей, сертификация продукта поставщиками решения для промышленной автоматизации

Контроль целостности аппаратного и программного обеспечения

Благодаря тому, что конфигурация конечных точек в ICS-системах относительно статична, меры контроля целостности в таких системах оказываются гораздо более эффективными, чем в динамических корпоративных сетях. KICS for Nodes содержит следующие технологии контроля целостности:

Контроль приложений

- Контроль установки и запуска приложений согласно белым и черным спискам.
- Контроль доступа приложений к ресурсам операционной системы: файлам, папкам, системному реестру и т. д.
- Контроль всех типов исполняемых файлов, используемые в среде Windows, включая файлы с расширением exe, dll, ocx, драйверы, элементы ActiveX, сценарии, интерпретаторы командных строк и драйверы режима ядра.
- Обновляющиеся данные о репутации приложений;
- Стандартные и заданные клиентом категории приложений для управления списками контролируемых приложений.
- Тонкая настройка контроля приложений для различных пользователей.
- Режимы предотвращения или только обнаружения: блокирование любых приложений, не включенных в белые списки, или (в режиме «наблюдения») разрешение запуска таких приложений, с обязательной регистрацией этой активности в Kaspersky Security Center, где может быть выполнена их оценка.

Контроль устройств

Управление доступом к съемным и периферийным устройствам и системным шинам на основе категорий и семейств устройств, а также идентификаторов конкретных устройств:

- поддержка политик белых и черных списков;
- точное назначение политик каждому отдельному пользователю или компьютеру либо группе пользователей или компьютеров;
- режим только предотвращения или только обнаружения.

Сетевой экран

Настройка и исполнение политики доступа к сети для защищенных узлов, в том числе серверов, диспетчерских пультов и рабочих станций. Компонент обладает следующими основными возможностями:

- контроль доступа к портам и сетям с ограничениями;
- обнаружение и блокирование сетевых атак, запускаемых из внутренних источников (таких как ноутбуки подрядчиков), которые могут распространять вредоносное ПО, находящее и заражающее хост при его подключении к промышленной сети.

Проверка целостности ПЛК

Возможность дополнительно контролировать конфигурацию ПЛК при помощи периодической сверки со специально выбранным сервером или рабочими станциями, защищенными «Лабораторией Касперского». Результирующие контрольные суммы сравниваются с сохраненными значениями (Etalon); формируется отчет об отклонениях.

Контроль беспроводных сетей

Эта возможность позволяет отслеживает любые попытки подключиться к неавторизованным сетям Wi-Fi. Контроль беспроводных сетей основан на технологии «Запрет по умолчанию», которая призвана автоматически блокировать соединения с любыми беспроводными сетям, помимо указанных как разрешенные.

Расширенная защита от вредоносного ПО

Надежные технологии «Лаборатории Касперского» для обнаружения вредоносного ПО и защиты от него, адаптированные и оптимизированные для использования в средах, где потребляется значительное количество ресурсов и важна постоянная доступность системы. Компонент рассчитан на статичные или редко обновляемые инфраструктуры.

Для защиты от вредоносного ПО «Лаборатория Касперского» использует полный спектр технологий:

- обнаружение вредоносного ПО при помощи сигнатур;
- обнаружение по запросу и во время обращения;
- обнаружение вредоносного кода в памяти (резидентного вредоносного ПО);

- обнаружение программ-шифровальщиков с помощью технологии Анти-Криптор;
- использование репутационных баз Kaspersky Security Network (KSN) и Kaspersky Private Security Network (KPSN) для повышения уровня защиты от новых угроз.

Доверенные обновления

Проверки совместимости, выполняемые до выпуска баз данных или компонентов и до обновления ПО или конфигурации систем управления производственными процессами, с целью предотвратить воздействие обновлений защиты от вредоносного ПО на доступность защищаемой системы.

Потенциальные проблемы чрезмерного потребления ресурсов решаются при помощи одной или нескольких из следующих мер:

- «Лаборатория Касперского» испытывает обновление базы данных на совместимость с ПО поставщика SCADA на собственном тестовом оборудовании;
- поставщик системы SCADA выполняет испытание на совместимость;
- «Лаборатория Касперского» проверяет обновления безопасности, интегрировав образы SCADA, рабочих станций,
  серверов и человеко-машинного интерфейса
  в собственное тестовое оборудование;
- обновления «Лаборатории Касперского» для защиты от вредоносного ПО испытываются на площадке клиента, и их развертывание автоматизируется при помощи Kaspersky Security Center.

Kaspersky Industrial CyberSecurity for Networks

KICS for Networks функционирует на уровне промышленных коммуникационных протоколов (Modbus, IEC stack, ISO, etc), анализируя трафик и выявляя аномалии с помощью передовой технологии DPI (Deep Packet inspection). Кроме того, предприятиям доступны широкие возможности контроля целостности сети и система обнаружения вторжений.

Риски и угрозы	Защитные технологии «Лаборатории Касперского»
Неавторизованные сетевые устройства в индустриальной сети	Контроль целостности сети обнаруживает новые и неизвестные устройства
Неавторизованные коммуникации в индустриальной сети	Контроль целостности сети отслеживает коммуникации между новыми/неизвестными устройствами
Вредоносные команды ПЛК, инициированные: • Оператором или сторонним специалистом (подрядчиком) • Инсайдером • Злоумышленником / вредоносным	Промышленный DPI анализирует коммуникации, происходящие на уровне промышленных протоколов, и детектирует появление аномалий в командах ПЛК и значениях параметров технологического процесса.
Сетевые атаки	Передовая система обнаружения вторжений (IDS) эффективна против всех известных шаблонов сетевых атак, в том числе против эксплуатации уязвимостей в индустриальном ПО и оборудовании.
Отсутствие данных для расследования и криминалистического анализа	Инструменты цифровой криминалистики: мониторинг и безопасная запись подозрительных событий в промышленной сети и данных об обнаруженных атаках

Неинтрузивное инспектирование трафика в производственной сети

Решение Kaspersky Industrial CyberSecurity for Networks выполняет пассивный анализ аномалий сетевого трафика, оставаясь невидимым для злоумышленников. Для установки достаточно активировать или настроить зеркальное отражение порта; интеграция в существующую производственную инфраструктуру очень проста и выполняется через SPAN-порт уже используемого коммутатора или ответвителя сетевого трафика.

Целостность сети и мониторинг сети

Решение Kaspersky Industrial CyberSecurity for Networks позволяет идентифицировать все активы, соединенные по Ethernet в общей сети — в том числе серверы SCADA, человеко-машинный интерфейс, ПЛК и RTU. Все новые и неизвестные устройства, а также все коммуникации между ними определяются автоматически. Это позволяет службам IT-безопасности развивать и поддерживать собственную надежную базу сетевых активов, что безопаснее, чем использование уязвимых инструментов управления, которые часто становятся мишенью атак.

Промышленный DPI для обнаружения аномалий

Решение «Лаборатории Касперского» предлагает надежную платформу для отслеживания передаваемых команд по управлению процессами, а также телеметрических данных. Среди прочего доступны следующие возможности:

- выявление любых команд, конфигурирующих ПЛК или изменяющих состояние ПЛК, включая команды остановки, паузы, изменения программы ПЛК, изменения прошивки ПЛК;
- контроль изменений параметров в технологичесих процессах;
- защита от внешних угроз, а также снижение риска вмешательства сотрудников, обладающих специальными знаниями, таких как инженеры, операторы SCADA и другие внутренние участники с прямым доступом к системам.

Машинное обучение

Промышленный DPI не только может быть настроен с помощью стандартного подхода на основе правил — он способен определять аномалии в технологическом процессе, благодаря передовой модели прогнозирования с использованием долгой краткосрочной памяти (LSTM). Возможности машинного обучения выводят уровень обнаружения угроз на новый уровень, позволяя обнаруживать угрозы в самых сложных и часто перенастраиваемых промышленных сетях.

Инструменты расследования инцидентов

Решение «Лаборатории Касперского» обеспечивает заказчиков системой безопасного ведения журналов, содержащей средства для анализа данных и расследования инцидентов. Дополнительное преимущество этой системы — способность предотвращать изменение логов АСУ ТП.

Контроль целостности сети для учета активов

KICS for Networks позволяет выявлять все активы, подключенные к сети Ethernet, в том числе серверы SCADA, HMI, инженерные рабочие станции, ПЛК и RTU.

Благодаря этому отделы IT-безопасности могут создавать собственные надежные и безопасные инвентарные перечни, не попадая в зависимость от потенциально уязвимых средств управления активами информационной и производственной систем, которые часто служат целью атак.

Дополнительные сервисы

Kaspersky Security Network (KSN)

Kaspersky Security Network — это облачная сеть со сложной распределенной структурой, выполняющая сбор и анализ данных об угрозах безопасности, поступающих с миллионов узлов по всему миру. KSN не только выявляет и блокирует новейшие угрозы и атаки «нулевого дня», но и помогает определять и заносить в черные списки источники интернет-атак, собирая данные о репутации веб-сайтов и приложений.

Подключать к сети KSN можно все корпоративные решения «Лаборатории Касперского», в том числе и промышленные. Основные возможности сети KSN:

- высокий уровень обнаружения;
- оперативное реагирование (традиционные решения на основе сигнатур реагируют на угрозы через несколько часов, с использованием KSN — через 40 секунд);
- более низкий уровень ложных срабатываний;
- сокращение потребления ресурсов решениями безопасности на локальном уровне.

Kaspersky Private Security Network (KPSN)

Для организаций с особыми требованиями к конфиденциальности данных «Лаборатория Касперского» создала сеть Kaspersky Private Security Network. Она обладает всеми преимуществами KSN, но без передачи информации за пределы корпоративной сети.

Сеть KPSN можно развернуть в собственном центре обработки данных любой организации, что позволяет внутренним IT-специалистам сохранять над ней полный контроль. Использование Kaspersky Private Security Network позволяет соблюдать требования, принятые в разных странах, и конкретные отраслевые нормативы.

Основные возможности сети KPSN

- Репутационный анализ файлов и URL-адресов: MD5-хэши файлов, регулярные выражения для проверки URL-адресов и модели поведения вредоносного ПО собираются в центральном хранилище, распределяются по категориям и оперативно передаются клиенту.
- Система управления записями (RMS): защитное ПО может ошибочно определять файлы и URL-адреса как доверенные или недоверенные. Система RMS помогает снизить количество ложных срабатываний, исправляя ошибки и выполняя постоянный анализ для повышения качества.
- Сбор и анализ данных при помощи облачных технологий.

Kaspersky® Industrial CyberSecurity

Kaspersky Industrial CyberSecurity — это набор технологий и сервисов, созданных для защиты различных уровней промышленной инфраструктуры и других элементов предприятия, в том числе серверов SCADA, операторских панелей, инженерных рабочих станций, ПЛК, сетевых соединений и даже самих инженеров. При этом решение не влияет на непрерывность технологических процессов. Узнайте больше на: www.kaspersky.ru/ics

www.kaspersky.ru

#ИстиннаяБезопасность