Особенности интеграции Kaspersky Industrial CyberSecurity for Networks и СКДПУ НТ

АЙТИБАСТИОН kaspersky

БИЗНЕС-РИСКИ

АСУ ТП является наиболее уязвимыми и чувствительными объектами инфраструктуры и требует пристального внимания к обеспечению информационной безопасности: речь идет и соблюдении регламентов безопасности и о соответствии соблюдения требованиям законодательства как объектов КИИ. Разделение промышленной и корпоративной сетей и исключение доступа к интернету не гарантирует безопасность промышленному предприятию. Угрозой, способной нанести ущерб предприятию, могут являться не только злонамеренные действия внешних специалистов, но и ошибочные действия внутренних сотрудников.

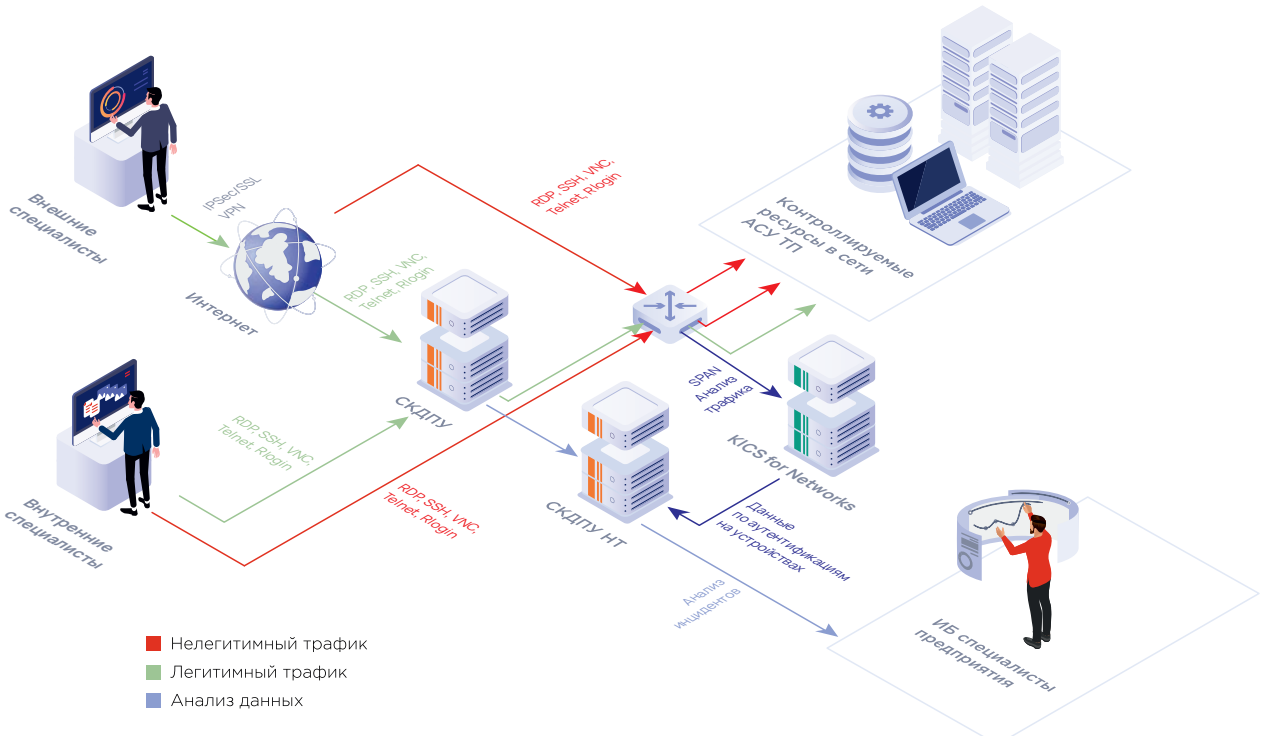
Отсутствие должного контроля за удалённым доступом в АСУ ТП может привести к серьёзным последствиям: от остановки технологического процесса до кражи коммерческой информации. Данные задачи решаются установкой шлюза доступа с возможностью контроля и мониторинга подключений. Но вместе с тем возникает вопрос – как офицер безопасности может быть уверен, что доступ к целевому устройству получен через шлюз, а не напрямую?

КАК СНИЗИТЬ РИСКИ?

Совместными усилиями компаний «АйТи БАСТИОН» и «Лаборатория Касперского» была разработана схема контроля удалённого доступа. Пользователями могут выступать любые специалисты (сотрудники ИБ, операторы и инженеры АСУ ТП и т.д.), удалённый доступ которых требуется контролировать для обеспечения функционирования АСУ ТП.

Удаленный доступ в сети разрешен только через СКДПУ НТ, обеспечивающий фиксацию и анализ событий пользовательских сессий. Kaspersky Industrial CyberSecurity for Networks определяет в общем траффике наличие сессий удаленного администрирования (ssh, RDP, telnet и т.д) и направляет данные о них в СКДПУ НТ для анализа.

СКДПУ НТ производит проверку, контролируется ли данное соединение шлюзом доступа. В случае, если соединение не входит в список разрешенных, оно считается несанкционированным и регистрируется системой как «инцидент», о котором оповещается оператор ИБ.



Преимущества интеграции СКДПУ НТ и Kaspersky Industrial CyberSecurity for Networks:

- Полностью контролируемый службой ИБ доступ к элементам критической инфраструктуры информационной системы;
- Блокирование доступа «в обход» со стороны привилегированных пользователей;
- Мгновенная реакция на несанкционированный доступ и занесение данной информации в базу инцидентов ИБ;
- База данных действий пользователей с ретроспективным поиском для расследования потенциальных инцидентов в рамках удаленного доступа внешних и внутренних специалистов;
- Формирование цифрового профиля каждого пользователя на основе его поведения, привычек, стандартного времени работы и др., в том числе попыток обхода системы удаленного доступа для доступа.

О продуктах:

СКДПУ НТ

СКДПУ НТ представляет собой решение по контролю действий привилегированных пользователей, которое включает в себя:

- центр управления системой контроля действий привилегированных пользователей;
- модуль поведенческого анализа и цифрового профиля пользователя;
- модуль отчетности;
- модуль отказоустойчивости и масштабирования;
- модуль контроля доступа привилегированных пользователей СКДПУ.

Kaspersky Industrial CyberSecurity for Networks

Решение для мониторинга и контроля сети в рамках промышленной сети, поставляемое в виде программного продукта или виртуального устройства, пассивно подключаемого к сети АСУ ТП.

Преимущества

- Инвентаризация активов;
- Контроль целостности сетей;
- Построение карты сетевых коммуникаций;
- Модуль системы обнаружения вторжений с набором сигнатур от Kaspersky ICS CERT;
- Контроль системных команд;
- Контроль уязвимостей прошивок ПЛК;
- Контроль параметров технического процесса;
- Интеграция с внешними системами через Rest API.

О компании:

«АйТи БАСТИОН» - российская компания, основанная в 2014 году. Производитель Системы контроля действий поставщиков ИТ-услуг. Продукты компании СКДПУ и СКДПУ НТ внесены в Реестр отечественного ПО. Заказчики «АйТи БАСТИОН» - более 100 российских компаний из разных отраслей, в том числе – нефтегазовой, энергетической, банковской, государственного сектора.

ООО «АйТи БАСТИОН»

119501, Россия, Москва,
ул. Староволынская, 15, к. 1.

E-mail: info@it-bastion.com
Тел.+7 (499) 322 36 67

Больше информации на сайте:
www.it-bastion.com