ИНТЕГРИРОВАННОЕ РЕШЕНИЕ:
PT ISIM и СКДПУ НТ

БИЗНЕС-РИСКИ

Удаленный доступ к технологическим сетям для мониторинга, управления, диагностики и наладки уже давно стал стандартом де-факто. Это удобно и позволяет быстро решить необходимые задачи, экономя затраты на логистику. Сегодня в условиях глобальной пандемии удаленный доступ стал еще более востребованным инструментом для специалистов.

Вместе с тем удаленный доступ порождает и серьезные риски безопасности предприятия: учетные данные для доступа в сеть АСУ ТП могут быть переданы третьим лицам или украдены; личные компьютеры пользователей, с которых производится удаленный доступ, могут быть заражены вредоносным ПО. Кроме того, удаленный доступ к технологической сети может быть организован (умышленно или случайно) в обход реализованной системы безопасности.

Отсутствие должного контроля за удаленным доступом в АСУ ТП может привести к серьезным последствиям. Это может быть полная остановка технологического процесса из-за распространения вирусов-шифровальщиков или целенаправленного саботажа, или кража коммерческих секретов компании и злонамеренные манипуляции параметрами тех. процесса в целях кражи доли сырья или выхода продукции.

КАК СНИЗИТЬ РИСКИ?

В условиях, когда невозможно контролировать непосредственно компьютеры удаленных пользователей, на помощь приходят средства инструментального мониторинга точек входа и действий пользователей, подключенных к сети АСУ ТП.

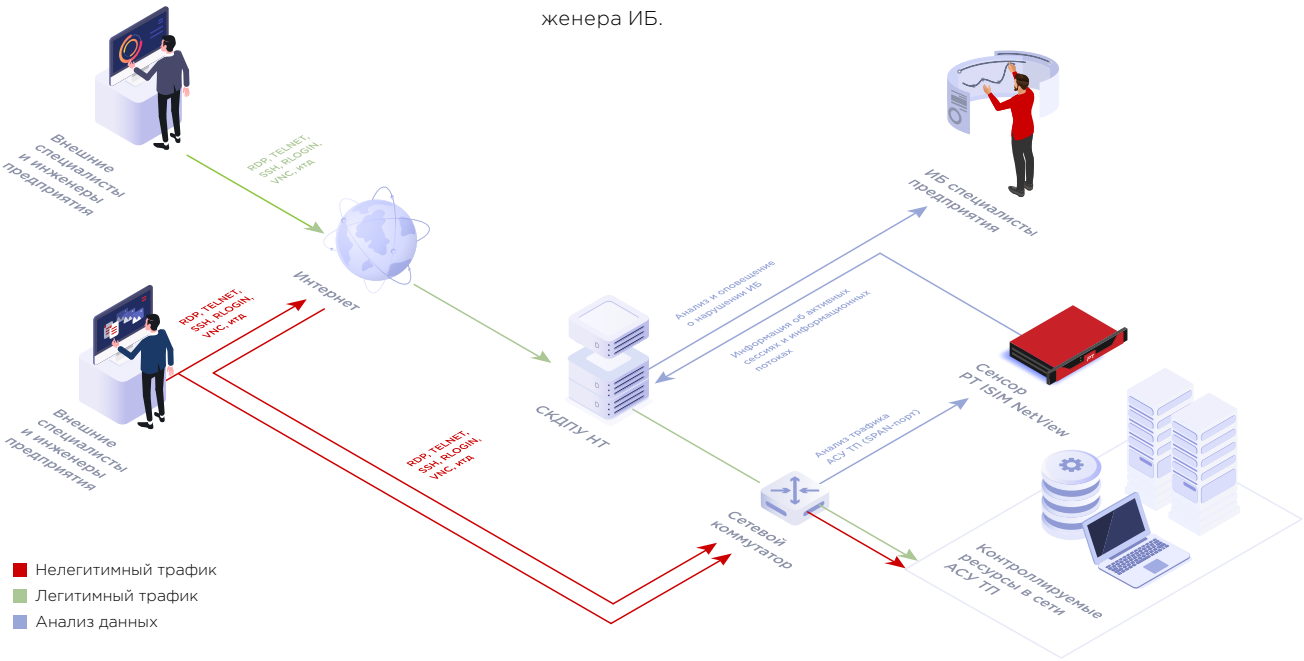
Совместное решение для контроля удаленного доступа в АСУ ТП от Positive Technologies и «АйТи БАСТИОН»[1] позволяет:

- Организовать единую точку входа для удаленных пользователей в сеть АСУ ТП — шлюз СКДПУ НТ;
- Выявлять нелегитимные подключения, минующие шлюз СКДПУ НТ, и вовремя оповещать специалиста по информационной безопасности об этом;
- Журналировать взаимодействие удаленных пользователей с оборудованием АСУ ТП (изменение проектов и конфигураций ПЛК, изменение режимов работы ПЛК и так далее);
- Выявлять следы проникновения вредоносного ПО в сеть АСУ ТП через удаленные соединения;
- Выявлять следы компрометации сети АСУ ТП через удаленные соединения;
- Оценивать активность подключенных пользователей, обнаруживать аномалии в их действиях и сигнализировать о нарушениях политик безопасности;
- Хранить полную копию трафика пользовательских сессий для аудита и расследования.

1 «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 российский компаний из разных отраслей, в том числе нефтегазовой, энергетической, банковской, государственного сектора. it-bastion.com, facebook.com/itbastion

Сценарий работы совместного решения Positive Technologies и «АйТи БАСТИОН» на базе PT ISIM и СКДПУ НТ.

Удаленный доступ к сети АСУ ТП пользователи получают только через центральный шлюз СКДПУ НТ. В свою очередь PT ISIM предоставляет шлюзу СКДПУ НТ данные обо всех зарегистрированных соединениях внутри сети. Это позволяет на уровне шлюза СКДПУ НТ выявить те соединения, что не контролируются шлюзом, и оповестить о них инженера ИБ.



СКДПУ НТ

СКДП 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.

Пользователями могут выступать любые специалисты (сотрудники ИБ, операторы и инженеры АСУ ТП и т.д.), удаленный доступ которых требуется контролировать.

PT ISIM

PT ISIM — программно-аппаратный комплекс глубокого анализа технологического трафика. Обеспечивает поиск следов нарушений информационной безопасности в сетях АСУ ТП, помогает на ранней стадии выявлять кибератаки, активность вредоносного ПО, неавторизованные действия персонала (в том числе злоумышленные) и обеспечивает соответствие требованиям законодательства (187-ФЗ, приказы ФСТЭК № 31, 239, ГосСОПКА).

В сценарии совместного решения задача PT ISIM — выявлять в АСУ ТП все сессии удаленного управления ресурсами технологической сети (например, RDP, TELNET, SSH, RLOGIN, VNC, итд.) и непрерывно предоставлять эту информацию шлюзу СКДПУ НТ для дальнейшего анализа.

Сенсор PT ISIM netView Sensor работает с копией трафика технологической сети и не оказывает влияния на функционирование АУС ТП.

PT ISIM является профессиональным продуктом класса NTA/NDR (Network Traffic Analysis / Network Detection & Response) для промышленных центров реагирования на инциденты информационной безопасности (SOC).

О компании

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

Positive Technologies уже 18 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга «Эксперт-400».

Следите за нами в соцсетях (Facebook, ВКонтакте, Twitter), а также в разделе «Новости» на сайте ptsecurity.com.