Интеллектуальная платформа приложений ИскраУралТЕЛ для энергетики (IAPE)

Кибербезопасность в платформе IAPE

Основные характеристики

- Защищенная разработка
- Строгая аутентификация
- Ролевое управление доступом
- Программное-конфигурируемый периметр

Почему именно ИскраУралТЕЛ?

- Собственные исследования и разработки и производство в ЕС
- Первая пилотная интеграция в ЕС на национальном уровне
- **70-летний** опыт ИскраУралТЕЛ

Платформа ИскраУралТЕЛ IAPE упрощает и оптимизирует интеграцию и конвергенцию ИТ и ОТ стандартным образом и, как таковая, является одной из основных систем энергетических компаний. Количество кибератак растет, поэтому это очень важный сегмент, который отлично покрывается данным решением.

РАЗАБОТКА БЕЗОПАСНОСТИ

Кибербезопасность является неотъемлемой частью IAPE. Она не рассматривается как дополнительная функция, добавляемая в конце поверх решения, а включена в жизненный цикл разработки системы, что обеспечивает безопасность всего решения на всех уровнях.

СТРОГАЯ АУТЕНТИФИКАЦИЯ

Для доступа к различным функциям IAPE вам необходимо пройти строгую аутентификацию. Это необходимо для пользователей, которые используют веб-приложения через API-интерфейсы, а также для компьютеров и пограничных устройств, подключающихся к платформе через Веб-сервисы или брокеры сообщений.

IAPE поддерживает общие типы аутентификации, а также их комбинацию, что формирует многофакторную аутентификацию:

- Имя пользователя / Пароль
- Сертификат клиента X.509
- Одноразовый пароль

IAPE может быть интегрирована с существующими решениями проверки подлинности клиента, такими как Kerberos и LDAP, которые часто встречаются в средах Windows и некоторых других, тем самым объединяя пользователей и, опционально, предоставляя единую точку входа.

Существующие решения поставщиков идентификации (IdP) также могут использоваться для аутентификации и авторизации, таким образом выступая в качестве брокера идентификации. Поддерживаемые и часто используемые корпоративные IdP включают:

- SAML v2.0
- OIDC v1.0

СТРОГАЯ АВТОРИЗАЦИЯ

Каждая функция имеет контролируемый доступ, реализованный через ролевое управление доступом, который является основным механизмом авторизации IAPE. Роли и привилегии могут отображаться в виде групп и синхронизироваться из таких сервисов каталогов клиента, как Microsoft AD или других сервисов LDAP. При отображении ролей с группами сервисов каталогов могут использоваться существующие группы, поэтому при настройке сервисов каталогов клиента изменения не потребуются.

ЗАЩИТА СЕРВИСОВ

Сервисы с публичным или широким доступом дополнительно защищены посредством Software Defined Perimeter (SDP), который эффективно минимизирует сетевые атаки и в первую очередь атаки DoS и DDoS.

Преимущества

- Комплексная **защита** встроена на **каждом уровне**
- Все сообщения **кодируются**
- **Безопасная интеграция** в среду клиента
- Соответствие отраслевым **стандартам**

ЗАЩИЩЕННОЕ ШИФРОВАНИЕ ДАННЫХ

Все сообщения между IAPE и внешними системами и клиентами кодируются с использованием протокола безопасности транспортного уровня (TLS) для предотвращения атак типа «незаконный посредник». TLS поддерживается автономной инфраструктурой открытых ключей (PKI) или может использоваться также PKI существующего клиента. Вместе с высокодоступной настройкой критически важных компонентов эти решения обеспечивают основные аспекты безопасности:

- Конфиденциальность
- Целостность
- Доступность

МОДЕЛИРОВАНИЕ УГРОЗ

Благодаря моделированию угроз и оценке угроз мы выявили критические угрозы для IAPE. Чтобы минимизировать или снизить риск уязвимости данных, были учтены самые важные из них:

- Защита аппаратного обеспечения, облачной платформы, операционных систем, серверов, платформ и каркасов приложений
- Безопасное кодирование
- Контроль безопасности

ПРОВЕРКА КИБЕРБЕЗОПАСНОСТИ

Регулярно выполняется проверка безопасности:

- Анализ системы безопасности
- Анализ кода
- Оценки уязвимости
- Тесты на проникновение (pentests)

ГЛУБОКАЯ ЗАЩИТА

Безопасность встроена во множество логических уровней решения. Каждый слой препятствует потенциальным атакам взломать платформу. Ключевыми слоями являются:

- Безопасность сети / связи
- Безопасность хоста / системы
- Безопасность приложений
- Безопасность данных

УПРАВЛЕНИЕ И СООТВЕТСТВИЕ СТАНДАРТАМ

Безопасность системы и программного обеспечения управляется и контролируется с помощью платформы "Software Assurance Maturity Model", которая определяет двенадцать методов защиты безопасности для разработки основных бизнес-функций программного обеспечения. Все принятые меры безопасности обеспечивают соответствие IAPE утвержденным отраслевым стандартам кибербезопасности.

БЕЗОПАСНАЯ ИНТЕГРАЦИЯ

Кибербезопасность конечного развертывания IAPE зависит от уровня интеграции в существующую среду клиента, а также от безопасности самой платформы. Наши сертифицированные специалисты предоставляют консалтинговые и интеграционные услуги, которые обеспечивают надлежащую и безопасную интеграцию в окружающую среду клиента.

ИскраУралТЕЛ

АО «ИскраУралТЕЛ»
620137, г. Екатеринбург
ул. Комвузовская, 9а
тел.: +7 343 210 69 51
факс: +7 343 341 52 40
iut@iskrauraltel.ru
www.iskrauraltel.ru

Московский филиал, 115114, г. Москва, ул. Дербеневская, д. 6, тел.: +7 (495) 727 08 10, факс: +7 (495) 727 08 78, эл. почта: contact@iskratel.ru
Санкт-Петербургский филиал, 190020, г. Санкт-Петербург, наб. Обводного канала, д. 138, корпус 101, БЦ «Треугольник», офис 119, тел.: +7 (812) 445 27 53, эл. почта: nekrasov@iskrauraltel.ru
Краснодарский филиал, 350015, г. Краснодар, ул. Красная/Северная, д. 160/354, офис 304, тел.: +7 (861) 212 58 66, факс: +7 (861) 212 58 77, эл. почта: tonkonog@iskrauraltel.ru
Представительство в Новосибирске, 630132, г. Новосибирск, ул. 1905 года, д. 21, корпус 2, тел.: +7 (383) 347 05 47, факс: +7 (383) 227 10 56, эл. почта: nsk@iskrauraltel.ru
ООО «ИСКРАУРАЛТЕЛ-СОФТ», 620137, г. Екатеринбург, ул. Комвузовская, 9-а, тел.: +7 (343) 210 69 71, факс: +7 (343) 341 52 40, эл. почта: soft-com@iskrauraltel.ru, сайт: iut-soft.ru