Что такое критическая инфраструктура

Критическая инфраструктура (КИ) — это системы управления технологическими процессами в отраслях, имеющих стратегическую важность для экономики, государственных институтов и общества.

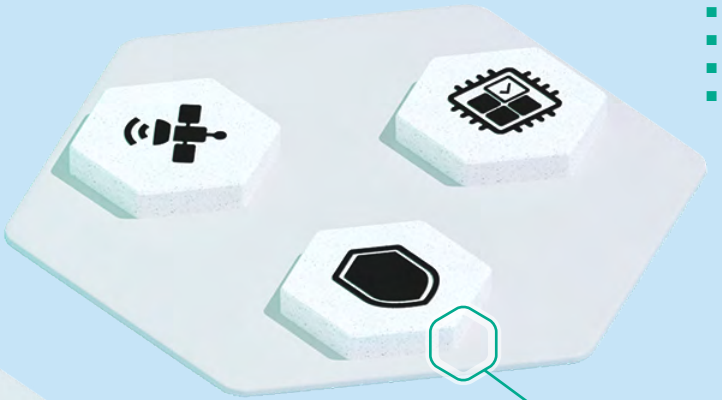
Критическая инфраструктура в промышленности

Тяжелая промышленность

- Добыча топлива
- Производство и поставка электроэнергии
- Горнорудная промышленность
- Металлургия
- Химическая промышленность
- Автомобильное производство
- Машиностроение
- Производство стройматериалов
- Целлюлозно-бумажная отрасль

Легкая промышленность и социальная инфраструктура

- Логистика и транспорт
- Пищевая промышленность
- Фармацевтика
- Объекты ЖКХ



Критически важное производство

- Оборонная промышленность
- Ракетно-космическая отрасль
- Производство микрочипов и электроники

Как мы защищаем критическую инфраструктуру и промышленные предприятия

Обеспечиваем промышленную кибербезопасность

Задача

Исключение киберинцидентов на промышленных объектах наших клиентов

На сегодняшний день промышленная кибербезопасность — это активирующая технология для устойчивого развития предприятий. Наши решения могут использоваться для защиты предприятий из любой отрасли с любым уровнем цифровизации — с классическим или новейшим парком компьютерного оборудования.

Согласно нашему краткому обзору основных инцидентов промышленной кибербезопасности за второе полугодие 2023 года, подавляющее большинство атакованных организаций относятся к производственному сектору.

Взломы критической инфраструктуры в 2022–2023 годах

- Остановлено производство автомобильных запчастей компании ThyssenKrupp из-за кибератаки.
- Производитель элементов питания Varta приостановил производство на всех предприятиях компании из-за взлома IT-систем.
- Хакеры взяли под контроль IT-систему, связанную с одной из насосных станций компании Municipal Water Authority of Aliquippa, которая предоставляет услуги водоснабжения в американском штате Пенсильвания.
- Кибератака на международного оператора контейнерных терминалов DP World привела к серьезным сбоям в работе международных портов Австралии.
- Почти 2 млн жителей Техаса столкнулись с перебоями в подаче воды в результате кибератаки на их водопроводную компанию NTMWD.
- Группа хактивистов SiegedSec взломала Национальную ядерную лабораторию Айдахо, которая является центром ядерных исследований Министерства энергетики США, и похитила конфиденциальные данные.

Отрасли, наиболее подверженные кибератакам во втором полугодии 2023 года

По данным Kaspersky ICS CERT[1], в 2023 году вредоносные объекты[2] были заблокированы на 38,5% компьютеров автоматизированных систем управления (АСУ).

Наш вклад в минимизацию рисков и сокращение ущерба от кибератак на производственные предприятия

Помогаем клиентам экономить деньги с помощью наших решений

Кибератаки могут привести к перебоям в работе или полной остановке процессов и услуг, что может повлечь снижение экономических показателей. Внедрение наших продуктов для защиты критической инфраструктуры и промышленных предприятий позволяет избежать этого. В апреле 2021 года компания Forrester провела исследование того, как наше решение для промышленной безопасности KICS for Networks повлияло на экономические показатели крупного поставщика электроэнергии, сравнив сумму возможных убытков нашего клиента со стоимостью лицензии KICS.

Что в результате?

$2,5 млн
сокращение риска нарушений безопасности

$338 тысяч
сокращение возможного ущерба для оборудования

$1,6 млн NPV[3]

135% ROI

Исследователи пришли к выводу, что решение окупилось всего за восемь месяцев, а показатель ROI составил 135% за три года. Кроме того, внедрение KICS помогло предприятию соотнести реальную и задокументированную сеть и внесло прозрачность в отношении сетевых активов и точек доступа.

1 Industrial Control Systems Cyber Emergency Response Team — группа реагирования на киберугрозы в промышленных системах управления.
2 Все виды угроз.
3 Чистая приведенная стоимость (Net Present Value) — финансовый показатель величины денежных средств, которые инвестор ожидает получить от проекта, после того как денежные притоки окупят его первоначальные инвестиционные затраты и периодические денежные оттоки, связанные с осуществлением проекта.

Решения

Защищаем все уровни систем и сетей промышленного предприятия

KOTCS

Мы стремимся предоставить каждому заказчику, независимо от его отрасли, уровня зрелости и сложности запроса, актуальную для него ценность от внедрения систем кибербезопасности.

Наша экосистема киберфизической безопасности промышленных предприятий Kaspersky OT CyberSecurity (KOTCS) снижает угрозы кибератак и исключает возможность возникновения недопустимых событий. Она содержит:

- **технологии**: полный спектр защитных решений, протестированных вендорами АСУ ТП;
- **знания**: достоверная аналитика угроз в АСУ ТП и специальные тренинги;
- **экспертизу**: набор экспертных сервисов для комплексной промышленной безопасности.

Экосистема KOTCS состоит из 18 продуктов и сервисов для промышленных предприятий, разработанных специалистами «Лаборатории Касперского» с высочайшим уровнем экспертизы — 15 лет опыта в защите промышленных объектов и 10 лет развития направления KICS. Это самая зрелая экосистема на рынке кибербезопасности, которая обеспечивает защиту всех уровней промышленного предприятия с управлением из единого центра. Она имеет расширенный функционал защиты от всех киберфизических угроз (например, собственную уникальную систему Antidrone) и способна обеспечить безопасность промышленных объектов, включая атомные электростанции, к надежности которых предъявляются самые строгие требования регулирующих органов.

KOTCS — защита на каждом уровне

Уровень 3. Корпоративные системы

- Конвергенция IT и OT, корреляция данных из всех доступных источников.
- Унифицированные процессы и подходы к обеспечению безопасности с помощью технологии расширенного обнаружения и реагирования на угрозы гибридного типа (Hybrid XDR).
- Программы обучения, консалтинг, расширенная аналитика угроз.

Уровень 2. Мониторинг и управление

- IIoT[1], возможности подключения, охрана периметра и защита систем автоматизации верхнего уровня (SCADA).
- Контроль доступа и использования, аудит и видимость OT-систем.
- Экспертная поддержка на месте.

Уровень 1. Контроллеры и защита

- Обнаружение вторжений, попыток взлома и компрометации, а также уязвимостей микропроцессорного технологического оборудования нижнего уровня автоматизации: контроллеров, терминалов защиты, измерительных центров.
- Глубокая инспекция протоколов (DPI); защита встроенных операционных систем в промышленном оборудовании от сетевых угроз и попыток вредоносного воздействия на уставки (параметры) технологического процесса.
- Обнаружение аномалий в технологическом процессе с помощью машинного обучения по выборке из баз данных или получаемых в реальном времени.

Уровень 0. Технологический процесс

Мониторинг воздушного пространства для защиты основного оборудования от киберфизических угроз и обеспечения безопасности подключенных транспортных средств.

[1] Industrial Internet of Things, или промышленный интернет вещей, — многоуровневая система, включающая в себя датчики и контроллеры, установленные на узлах и агрегатах промышленного объекта, средства передачи собираемых данных и их визуализации, мощные аналитические инструменты интерпретации получаемой информации и многие другие компоненты.