kaspersky

Расследование киберинцидентов на промышленных предприятиях

Проблема

Кибератака на промышленное предприятие, результатом которой могут стать кража конфиденциальных данных, остановка производства и физический ущерб. Не всегда сразу ясны масштаб и первопричина атаки, цели и возможности злоумышленников. Необходимо в кратчайшие сроки принять эффективные меры для быстрой остановки атаки.

Решение

Координация действий по сбору артефактов, их оперативный анализ, подготовка стратегии защиты и активная помощь в ее реализации, быстрое определение последовательности шагов для противодействия атаке и минимизации ее последствий, поиск первопричин и формирование списка мер по предотвращению подобных инцидентов в будущем.

Для кого

Промышленные предприятия из любых отраслей.

Что мы предлагаем

Оперативная помощь в расследовании и ликвидации последствий киберинцидентов на промышленных предприятиях — при реализации следующих действий.

- Сбор информации как с ИТ- так и ОТ-систем. С учетом экспертных знаний о функционировании этих систем, их особенностях и важных ограничениях это можно сделать, минимизировав необходимость остановки технологического процесса и производственной деятельности.
- Обнаружение и исследование образцов нового, ранее неизученного вредоносного ПО, использованного в атаке, а также выявление и анализ информации о вредоносной инфраструктуре, использованной в атаке. Эти мероприятия помогают составить список индикаторов компрометации и найти затронутые атакой системы, сделать предположения о степени компрометации сети организации и получить дополнительные сведения для дальнейшего расследования.

- Поиск связи атаки с конкретными злоумышленниками. Это может помочь обнаружить дополнительный инструментарий, использованный в атаке, сделать предположение о тактике, целях и возможностях атакующих.
- Обнаружение и исследование деятельности злоумышленников в атаках на другие организации. Это может дать ценную информацию о потенциале, технических средствах и вероятных целях злоумышленников и при необходимости скорректировать процесс реагирования на инцидент и общий ход расследования.
- При необходимости оценка вероятности негативного влияния обнаруженного вредоносного инструментария на работу систем технологической сети и промышленного оборудования в случае сбоев.
- При необходимости разработка средств обнаружения инструментария злоумышленников и сбора информации для расследования, совместимых с работой ИТ- и ОТ-систем предприятия.
- Обнаружение и восстановление скрытых и затертых следов вредоносной активности злоумышленников в сети предприятия. Детальный анализ собранных данных и восстановление картины атаки, выявление первопричины и основных обстоятельств, повлиявших на ее развитие.
- Обнаружение и изучение проблем безопасности предприятия, использованных злоумышленниками в атаке, включая уязвимости в программно-аппаратных комплексах и ошибки их конфигурации, проблемы сетевой безопасности, некорректные настройки средств зашиты, недостатки практик и процедур обеспечения безопасности или пробелы в осведомленности сотрудников об угрозах и о правилах общей кибергигиены.
- Подготовка рекомендательного списка мер и средств обеспечения безопасности, адекватных угрозе, на основе информации, полученной в ходе расследования, знаний о тактиках, техниках и об арсенале злоумышленников, а также опыта организации защиты от подобных атак.
- Подготовка рекомендаций по исправлению прочих проблем информационной безопасности, обнаруженных в ходе расследования инцидента, включая такие, которые не имеют к исследованной атаке прямого отношения.

Помогаем найти ответы на вопросы

- Что произошло?
- Какие активы пострадали и какой ущерб им нанесен?

- Какие технические и организационные недостатки привели к инциденту? В частности, как злоумышленникам удалось проникнуть в инфраструктуру и распространиться по ней (какие инструменты и тактики они при этом использовали)?
- Как устранить последствия инцидента и минимизировать ущерб?
- Как предотвратить подобные инциденты в будущем?

Помогаем минимизировать ущерб от инцидента

- Прямые финансовые убытки
- Упущенная выгода
- Репутационные потери
- Порча сырья и продукта, повреждение оборудования и потеря доступа к критически важной информации
- Угроза жизни людей и ущерба окружающей среде
- Юридические риски и штрафные санкции со стороны регуляторов

Как мы работаем

Оперативно реагируем на запрос

Откликаемся на запрос, оставленный на нашем сайте или поступивший на почту ics-cert@kaspersky.com, чтобы дать знать: поддержка скоро будет.

Даем рекомендации по выявлению активов, затронутых инцидентом, и сдерживанию атаки

В течение 24 часов:

- уточняем детали, согласовываем методику работы и совместно обозначаем приоритетные задачи расследования (остановить атаку, определить/минимизировать ущерб, найти первопричину, восстановить картину инцидента, разработать рекомендации по предотвращению подобных инцидентов);
- даем, если это возможно, первоначальную оценку ситуации, включая оценку масштаба инцидента и возможного ущерба, прогноз вариантов развития атаки, рекомендации первоочередных мер и действий;
- договариваемся об объеме (координация, сбор и/или анализ улик) и формате (on-site или удаленно) работы экспертов Kaspersky ICS CERT.

Собираем цифровые улики

Выезжаем на место происшествия для сбора цифровых улик или консультируем, как сделать это самостоятельно.

Помогаем координировать действия по реагированию на инцидент

Как правило, в процессе реагирования на инцидент решаем следующие задачи:

- находим, изучаем и обезвреживаем весь использованный в атаке вредоносный арсенал. Часть его может не обнаруживаться в начале расследования, в таком случае требуется разработка обновлений средств защиты или специальных средств обнаружения;
- идентифицируем и исследуем скомпрометированные системы, чтобы гарантированно лишить злоумышленников точек присутствия в сети организации.
- обнаруживаем и анализируем все следы вредоносной активности, чтобы оценить масштаб ущерба;
- выясняем цели злоумышленников, чтобы спрогнозировать варианты дальнейшего развития ситуации и выбрать меры для предотвращения наиболее негативных сценариев;
- восстанавливаем картину происшествия и временной график развития атаки, чтобы выяснить, какими проблемами безопасности предприятия воспользовались злоумышленники, оперативно защитить предприятие от развития атаки и разработать перечень мер для предотвращения подобных ситуаций в будущем.

Помогаем минимизировать последствия инцидента

Предоставляем инструкции по возвращению систем предприятия к нормальной работе, при необходимости разрабатываем утилиты для поиска скомпрометированных систем и удаления вредоносного инструментария.

Готовим подробный отчет

Разъясняем результаты анализа собранных материалов и выявленных фактов.

> Обычно все работы в рамках этой услуги занимают от семи дней до месяца в зависимости от масштаба, технической сложности инцидента и степени готовности пострадавшей организации к совместным оперативным и слаженным действиям.

Что получает клиент

В процессе реагирования на инцидент

- Экспертная оценка ситуации
- Пошаговые рекомендации срочных мер и действий, необходимых для достижения целей расследования в соответствии с их приоритетами
- Техническая помощь и консультации или активная координация действий команды реагирования на инцидент

По результатам расследования

- Отчет, который содержит:
  - описание восстановленной картины инцидента: основных обнаруженных обстоятельств, временного графика развития, векторов, тактик и техник атаки, выявленной первопричины, эксплуатированных злоумышленниками проблем безопасности;
  - оценку последствий инцидента для информационных активов предприятия;
  - описание основных свойств и функциональных возможностей обнаруженного вредоносного ПО;
  - рекомендации по повышению уровня защищенности предприятия для недопущения подобных инцидентов в будущем, включая технические и организационные меры, мероприятия по повышению осведомленности персонала о практиках безопасной работы с информационными активами, курсы повышения квалификации для специалистов.

Мы гарантируем конфиденциальность данных, полученных в рамках расследования инцидента.

Запросить консультацию специалиста

Статьи по теме

- Атаки обновленного вредоносного ПО MATA на промышленные компании в Восточной Европе
- Техники, тактики и процедуры атак на промышленные компании. Импланты для удаленного доступа
- Техники, тактики и процедуры атак на промышленные компании. Импланты для сбора данных
- Техники, тактики и процедуры атак на промышленные компании. Импланты для выгрузки данных на сервер

- Таргетированная атака на промышленные предприятия и государственные учреждения

Рекомендуем дополнительно

- Разработка руководства и обучение реагированию на инциденты
- Расширенный тренинг «Цифровая криминалистика и расследование инцидентов в АСУ ТП»
- Поток данных об угрозах для систем промышленной автоматизации
- Поток машиночитаемых данных об уязвимостях АСУ ТП
- Информация об уязвимостях и угрозах для АСУ ТП

Запросить консультацию специалиста

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», направленный на координацию усилий производителей систем автоматизации, владельцев и операторов промышленных объектов, а также исследователей ИТ-безопасности для защиты промышленных предприятий от кибератак. Kaspersky ICS CERT направляет свои усилия в первую очередь на выявление потенциальных и существующих угроз, нацеленных на системы промышленной автоматизации и промышленный интернет вещей.

Kaspersky ICS CERT ics-cert@kaspersky.com