Разработка руководства и обучение реагированию на инциденты

Проблема

Отсутствие в организации заранее подготовленных процедур и плана действий, а также схем коммуникаций и алгоритмов принятия решений в нештатной ситуации, помогающих быстро и эффективно реагировать на инциденты. Отсутствие у сотрудников необходимых навыков.

Решение

Подготовка руководства по реагированию на инциденты, в котором подробно описываются меры и действия в критической ситуации, в том числе по сдерживанию, оценке и минимизации последствий инцидента, с учетом особенностей инфраструктуры и бизнес-процессов организации.

Для кого

Организации любых отраслей промышленности, предприятия энергетики, коммунальных услуг, транспорта и логистики, включая организации с географически распределенной структурой.

Проблематика

Чтобы быстро и с минимальными потерями справиться с инцидентом, нужно быть к нему готовым. Надо заранее разработать план действий на случай возникновения нештатной ситуации и обучить персонал. Если требуется привлекать подрядчиков, то заблаговременно обеспечить их необходимыми полномочиями, согласовать способы связи и планы взаимодействия.

Многие промышленные предприятия имеют территориально распределенную структуру. Наличие удаленных площадок предъявляет особые требования к координации действий сотрудников, использованию методов централизованного сбора улик, разработке планов сдерживания инцидентов различных типов.

Первоочередные задачи предприятия, столкнувшегося с инцидентом безопасности

- Своевременно выявить инцидент: запоздалое обнаружение инцидента может привести к краже конфиденциальных данных,

остановке технологического процесса, задержкам поставок готовой продукции, угрозам функциональной безопасности и т. д.

- Быстро и правильно остановить развитие инцидента: выбор неверной стратегии реагирования может привести к большому убытку — иногда неправильные действия пострадавшей стороны наносят больший урон предприятию, чем действия злоумышленников.
- Собрать и проанализировать артефакты: незнание методов и отсутствие эффективных инструментов для сбора и анализа улик осложняет выявление причин инцидента, определение ущерба и поиск безопасного способа вернуть системы к нормальной работе.
- Провести работу над ошибками: без всестороннего анализа результатов расследования сложно определить, какие технические и организационные меры потребуются, чтобы минимизировать риск повторения подобных инцидентов в будущем.

Что необходимо для эффективного реагирования на инцидент

- Подготовленная команда специалистов, способных своевременно выявлять инциденты с использованием технических средств предприятия, точно классифицировать их и выбирать оптимальную стратегию реагирования.
- Подробный план реагирования на инциденты различных типов для всех критически важных объектов ИТ- и ОТ-инфраструктуры организации.
- Материально-техническая база с необходимым оборудованием и программным обеспечением для быстрого и успешного реагирования на инцидент.
- Внутренние нормативные акты, позволяющие специалистам своевременно получать необходимые доступы, в том числе в случае привлечения сторонних экспертов.
- Знание особенностей структуры предприятия, понимание распределения ролей и обязанностей всеми участниками расследования, включая представителей внешних организаций.
- Общее представление о технологическом процессе, знание основных технических деталей ключевых и типовых ИТ- и ОТ-систем всеми участниками расследования для реализации предусмотренных сценариев реагирования.
- Отработанные навыки выполнения базовых задач реагирования, таких как сбор цифровых доказательств для дальнейшего экспертного анализа и изоляция систем для сдерживания инцидента.

Что мы предлагаем

В ходе создания руководства по реагированию на инциденты в OT-инфраструктуре предприятия мы анализируем особенности бизнес- и технологического процессов, изучаем OT-системы. Это позволяет предложить эффективные методы обнаружения и реагирования на инциденты и подготовить инструкции по их применению, специфичные для каждой конкретной организации. Руководство содержит пошаговые инструкции по работе с утилитами для сбора и анализа информации, необходимой для расследования инцидента, а также рекомендации по сдерживанию инцидентов различных типов, позволяющие минимизировать ущерб.

При составлении инструкций мы опираемся на свой опыт в обнаружении, предотвращении и расследовании компьютерных атак по всему миру и обязательно учитываем защитные решения, которые уже используются на предприятии клиента.

Подготовив руководство, мы проводим тренинги специалистов организации, чтобы теоретические знания трансформировалась в реальные навыки. На тренингах мы используем специальные стенды, созданные с использованием элементов типовых промышленных систем автоматизации и позволяющие имитировать последствия различных атак на инфраструктуру клиента. Упражнения, которые мы даем на тренингах, основаны на реальных расследованиях, проведенных командой Kaspersky ICS CERT.

Как мы работаем

Определяем объем работ

Проводим семинар, на котором рассказываем об основных этапах реагирования на инциденты, задачах, которые чаще всего приходится решать, типичных ошибках и лучших практиках. Клиент решает, на какие объекты и системы ИТ- и OT-инфраструктуры будет распространено руководство, представители каких подразделений будут вовлечены в процессы реагирования на инциденты.

На этом этапе нам требуются:

- описание технического устройства и функций защищаемых систем;
- описание имеющихся средств ИБ;
- интервью со специалистами, вовлекаемыми в реагирование на инциденты.

Анализируем инфраструктуру, процессы, практики и доступные технические средства

Изучаем предоставленные нам материалы и результаты интервью с сотрудниками. Устанавливаем, какое компьютеризированное оборудование, какие компоненты систем, службы и приложения наиболее критичны для работы технологического и бизнес-процессов организации. Определяем, как эффективнее всего выстроить процесс реагирования на инциденты, исходя из особенностей защищаемого объекта, компетенции сотрудников предприятия, имеющихся у него технических средств и объективных ограничений. По согласованию с клиентом выезжаем на объект.

Создаем руководство по реагированию на инциденты

Руководство описывает процедуры реализации всех шести этапов реагирования на инциденты: подготовка (preparation), обнаружение (identification), сдерживание (containment), устранение (eradication), восстановление (recovery), выводы и работа над ошибками (lessons learned).

Все инструкции готовятся с учетом особенностей инфраструктуры предприятия. Например, инструкции по выявлению инцидента учитывают именно ту SIEM-систему, которая используется на конкретном предприятии, и те источники событий, которые к ней подключены, а инструкции для сдерживания инцидента учитывают имеющиеся на предприятии резервные устройства и каналы связи, топологию сети и т. д.

> Мы создаем практическое руководство, которым можно пользоваться сразу, без каких-либо доработок.

Также при создании руководства мы описываем наиболее вероятные, по нашим оценкам, сценарии атак с учетом особенностей инфраструктуры предприятия. По результатам анализа информации о выявленных недостатках безопасности мы предлагаем меры по усовершенствованию имеющихся внутренней нормативной и технической баз в области ИБ, которые позволят снизить риски возникновения инцидентов и серьезность их последствий.

Обучаем персонал и внедряем знания

Каждый специалист команды реагирования на инцидент должен понимать свою роль в этом процессе. Обучение поможет применить полученные знания на практике, опробовать свои силы и отладить рабочие процессы в реалистичных сценариях, построенных на основе реальных инцидентов из нашей и мировой практики. Этот этап имеет решающее значение для успеха всего проекта.

Что получает клиент

- Практическое руководство по реагированию на инциденты, учитывающее все существенные особенности организации.
- Обученный персонал, готовый самостоятельно реагировать на киберинциденты.

Бонус: 40 часов сервиса «Лаборатории Касперского» по реагированию на инциденты.

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

- Расследование киберинцидентов на промышленных предприятиях
- Расширенный тренинг «Цифровая криминалистика и расследование инцидентов в АСУ ТП»
- Информация об уязвимостях и угрозах для АСУ ТП
- Аналитика известных уязвимостей АСУ для принятия критически важных решений в части информационной безопасности
- Спроси эксперта

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