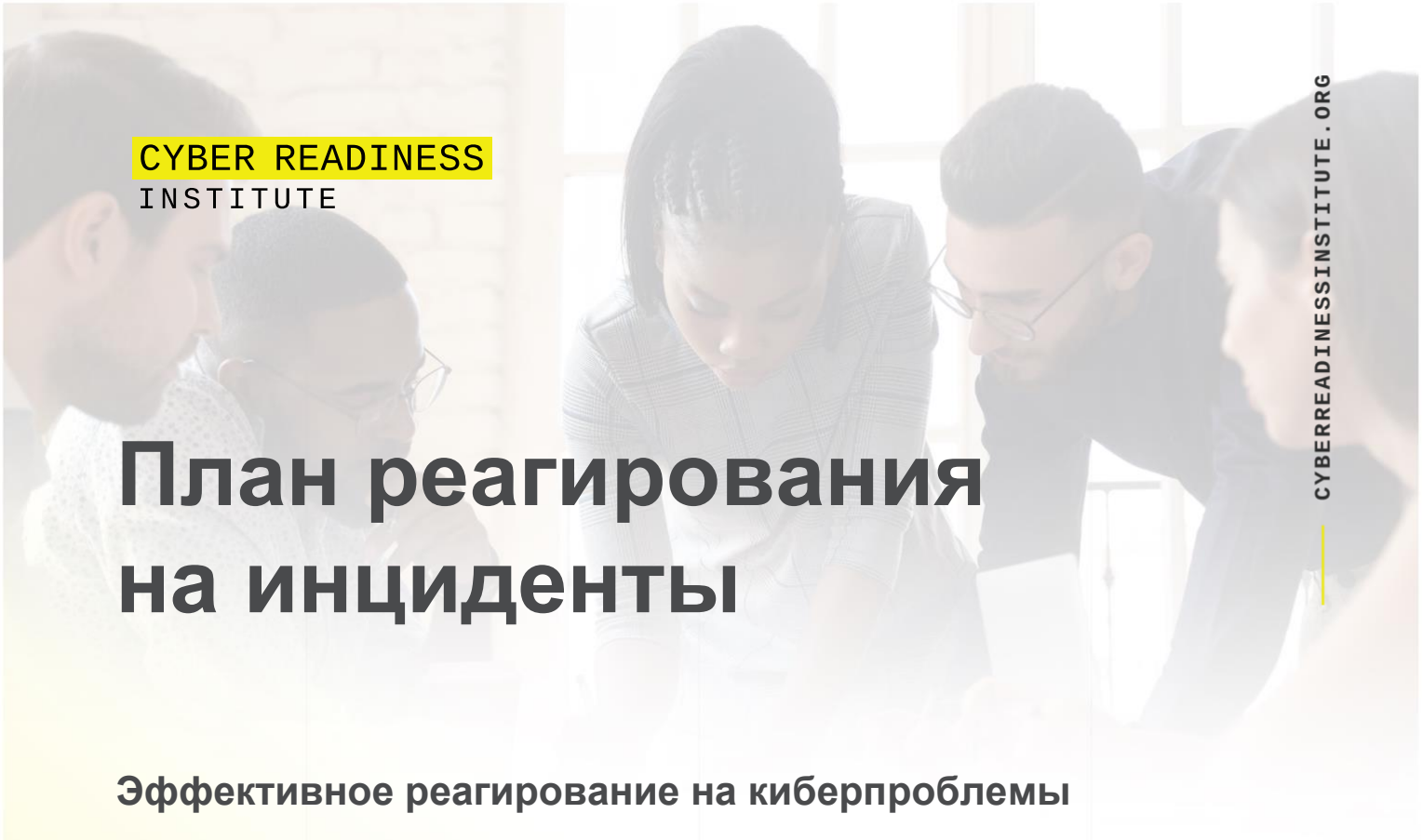

CYBER READINESS
INSTITUTE

CYBERREADINESSINSTITUTE.ORG

План реагирования на инциденты

Эффективное реагирование на киберпроблемы

Установление практики и политики киберготовности помогает снизить риск, но важно исходить из того, что нашей компании, вероятно, в какой-то момент придется столкнуться с инцидентом безопасности, который может повлиять на бизнес-операции. Пытаться определить, как реагировать во время инцидента, - не очень хорошая идея. Время реагирования имеет решающее значение для минимизации ущерба. Наличие четкого плана может предотвратить катастрофу в результате инцидента.

Обзор

Комплексный пошаговый план реагирования на инциденты позволяет нам быстро реагировать на инциденты, разрешать их и извлекать уроки из каждого инцидента. Этот план реагирования на инциденты служит дорожной картой того, что делать при реагировании на инцидент безопасности, и является гарантией того, что у нас имеется стратегический, а не реактивный ответ.

Реагирование на инциденты состоит из трех основных элементов:

1. **Подготовка** к возможному инциденту в будущем
2. **Реагирование** во время инцидента
3. **Восстановление** после инцидента

Как подготовиться

Организационные принципы:
Как и во многих других вещах, небольшая подготовка имеет большое значение. Есть несколько основных действий, которые необходимо выполнить как можно скорее, чтобы должным образом подготовиться к атаке и уменьшить ущерб от нее.

1. **Сделайте резервную копию данных и убедитесь, что вы можете восстановить данные из резервных копий.** Восстановление после атаки пройдет намного быстрее и повлияет на работу гораздо меньше, если у вас есть текущие резервные копии системного программного обеспечения, приложений и особенно важных данных. Вы также должны убедиться, что у каждого сотрудника в вашей организации есть резервные копии, если вы не делаете это централизованно. Необходимо регулярно тестировать резервные копии.
    - ✓ Дата копирования: [ДАТА]
2. **Убедитесь, что все знают, как сообщить о возможном инциденте.** Раннее выявление действительно важно. Каждый член команды должен знать то, как обнаружить подозрительную активность и к кому обратиться по этому поводу.
    - ✓ Назначенное контактное лицо компании: [КОНТАКТНЫЕ ДАННЫЕ]
    - ✓ Дата выполнения: [ДАТА]
3. **Найдите хорошую техническую внешнюю поддержку по реагированию на инциденты.** Знайте, к кому идти и как связаться со службой внешней поддержки в чрезвычайной ситуации. Пожар, который вы не в состоянии контролировать, требует вызова пожарных. Вам нужно знать, кому звонить, если вы не можете контролировать киберинцидент. Как минимум, это должен быть эксперт по ИТ-поддержке, которого вы знаете и которому доверяете. В зависимости от масштаба и характера вашего бизнеса целесообразно определить дополнительные средства связи и юридическую поддержку.
    - ✓ Назначенное контактное лицо службы внешней поддержки: [КОНТАКТНЫЕ ДАННЫЕ]
    - ✓ Дата выполнения: [ДАТА]

Как реагировать

На компьютере сотрудника происходит что-то безумное, и он не знает, что делать. Это то же самое, что почувствовать запах дыма или увидеть небольшое пламя в кофейне.

Вот что нужно сделать:

1. **Изолируйте проблему:** немедленно отключите устройство от сети
2. **Определите вид инцидента** и выполните следующие действия:

   - ✓ Вредоносное ПО – немедленно отключите устройство от сети
   - ✓ Кража учетных данных – заблокируйте, но не удаляйте аккаунт, сбросьте пароль
   - ✓ Утечка данных – позвоните в экстренный отдел ИТ
   - ✓ Программы-вымогатели – немедленно отключите устройство от сети
   - ✓ Отказ в обслуживании – свяжитесь с вашим менеджером/ИТ-специалистом/интернет-провайдером

3. **Определите масштаб** инцидента, задав эти вопросы:

   - ✓ Когда произошел инцидент?
   - ✓ Кто пострадал?
   - ✓ Какова техническая природа инцидента? Как это произошло?
   - ✓ Кто знает об инциденте?
   - ✓ Он все еще продолжается?

4. **Определите, можно ли должным образом контролировать его внутренними усилиями компании,** или нужно ли вам позвонить во внешнюю службу ИТ-поддержки чтобы убедиться, что вы справились со взломом надлежащим образом.
5. **Продолжайте проверять, не повторится ли проблема.** Если неясно, решена ли проблема, проявите осторожность и обратитесь к специалисту по поводу проблемы.

Как восстановить

Кризис миновал, пора возвращаться к нормальной жизни. Масштаб инцидента и серьезность воздействия будут определять то, сколько времени и усилий потребуется для восстановления. Тем не менее, основные шаги одинаковы.

Вот что вы должны сделать:

1. Уведомите все пострадавшие стороны
2. Смените идентификатор пользователя и пароль скомпрометированного устройства
3. Исправьте все устройства
4. При необходимости переустановите программное обеспечение и данные из резервных копий

Контрольный список реагирования на инциденты

Этот контрольный список должен помочь ИТ-менеджеру или киберкуратору

Подготовка

1. Резервное копирование ежедневно
   - ✓ **Настройка/подтверждение автоматического резервного копирования: [ДАТА]**
2. Тестовые резервные копии каждые три месяца
   - ✓ **Дата последнего копирования: [ДАТА]**
3. Обучение персонала протоколу регистрации личности (IRP)
   - ✓ **Дата последнего обучения: [ДАТА]**

Контактное лицо для экстренной связи по ИТ-поддержке: _____
Интернет-провайдер: _____
Контактное лицо для экстренной связи по юридическим вопросам: _____
Контактное лицо для экстренной связи: _____

Реагирование

1. Изолируйте проблему — отключите устройство от сети
2. Определите вид инцидента
   - ☐ Кража учетных данных
   - ☐ Программы-вымогатели
   - ☐ Вредоносное ПО
   - ☐ Отказ в обслуживании
   - ☐ Потеря конфиденциальных данных
3. Определите масштаб инцидента
   - ☐ Кто пострадал?
   - ☐ Когда это началось?
   - ☐ Это все еще продолжается?

Восстановление

1. Уведомите все стороны
2. Смените идентификатор пользователя и пароль скомпрометированного устройства
3. Установите исправности на всех устройства
4. При необходимости переустановите программное обеспечение и данные из резервных копий

Дополнительные рекомендации по реагированию на инциденты

Это руководство должно помочь ИТ-менеджеру или киберкуратор

Если вы хотите, чтобы в вашей организации был более надежный план реагирования на инциденты, ниже приведен четырехэтапный подход, основанный на рекомендациях Национального института стандартов и технологий США (NIST). Вероятно, вы не сможете следовать каждому шагу, но сделайте все возможное, чтобы действовать на каждом из четырех шагов таким образом, чтобы это имело смысл для вас и вашей организации.

1 Подготовка

Подготовка является ключом к быстрому реагированию. На этом этапе вы составляете список всех ваших активов — того, что позволяет вашей компании в сети свою деятельность. Этот список будет включать, помимо прочего, серверы, сети, приложения и критически важные конечные точки (например, ноутбуки). После того, как вы составили список активов, классифицируйте их по степени важности. Затем отследите их модели трафика, чтобы вы могли создать базовые показатели, которые будут использоваться для сравнения позже, или наймите поставщика услуг для мониторинга их моделей трафика, если вы можете выделить на это средства. Если вы не можете позволить себе поставщика услуг, на начальном этапе будет правильно составить список активов и уделить приоритетное внимание к вашим активам. Создайте план взаимодействия с рекомендациями о том, с кем связаться, как и когда для каждого вида инцидента. Не забудьте связаться со всеми из этого списка до того, как возникнет кризис. Обычный рефрен в антикризисном управлении: «Вы никогда не должны обмениваться визитными карточками во время кризиса». Убедитесь, что все в вашем списке знают, чего вы ожидаете от них во время инцидента.

Определите, какие события безопасности и при каких пороговых значениях будут запускать ваш план реагирования на инциденты. Чтобы помочь вам определить пороговые значения, подумайте о том, что может нарушить ваши бизнес-операции. После определения этих пороговых значений создайте план реагирования на инциденты для каждого вида инцидентов. Его можно улучшить с помощью промежуточных требований, во время которых вы будете выявлять пробелы в своих процессах, но его также можно улучшить после реальных событий (подробнее об этом позже). Суть в том, чтобы наладить процесс.

2 Обнаружение и анализ

На этом этапе процесса был выявлен инцидент безопасности. Здесь вы переходите в режим исследования. Соберите все, что сможете, об инциденте. Затем проанализируйте данные. Определите точку входа и ширину бреши. Этот процесс значительно упрощается и ускоряется, если все ваши инструменты безопасности фильтруются в одном месте. Возможно, вы наняли поставщика услуг, который может выполнять эти функции за вас.

3 Сдерживание, ликвидация, и восстановление

Сдерживание направлено на остановку «кровотечения». Здесь вы исправляете точку входа.

Ликвидация направлена на устранение угрозы. Если угроза проникла из одной системы и распространилась на другие, здесь у вас будет больше работы.

Восстановление направлено на приведение системы в рабочее состояние, если она вышла из строя, или просто вернуться к обычному режиму работы, если это не так.

4 Извлеченные уроки

Этот шаг дает возможность извлечь уроки из вашего опыта, чтобы вы могли лучше реагировать на будущие инциденты безопасности. Как бы ни было велико искушение пропустить этот шаг, особенно с вашим бесконечным списком дел, настоятельно рекомендуется выполнить его.

Взгляните на инцидент скромным, но критическим взглядом, чтобы определить области для улучшения. Затем добавьте эти улучшения в свою документацию.

Ни один процесс не идеален для всех возможных сценариев. Некоторые сценарии нельзя даже понять, пока они не произойдут. Ландшафт угроз также постоянно развивается, поэтому ваш процесс реагирования на инциденты, естественно, будет время от времени обновляться. Помните, завтра вы сами себе скажите спасибо. Как говорится: «Не упустите хороший кризис».