Подготовка 1

Установить контакты, выработать процедуры, собрать информацию для оптимизации временных затрат во время инцидента.

Контакты

- Установить контакты с представителями департамента по связям с общественностью, отдела кадров и юристами.
- Вести централизованный журнал контактов
- Располагать единым процессом проверки и регулирования уровня доступа к внутренней информации. В рамках процесса, следить за удалением доступа для уволившихся сотрудников.
- Строго соблюдать процесс авторизацию при осуществлении доступа к критической информации и деталям производственных процессов предприятия.

Обнаружение 2

Зафиксировать инцидент, определить затрагиваемые интересы, привлечь компетентные контакты.
Факты инсайдерского злоупотребления тяжело поддаются раннему обнаружению; не существует способов, гарантирующих 100%-ый успех в данном деле.

Технические средства обнаружения

- **Оповещения системы управления информацией и событиями безопасности (SIEM) и средствами корреляции.**
Возможно обнаружение вредоносной деятельности посредством корреляции и анализа нескольких аномальных событий.
- **Оповещения IDS/IPS**
Системы обнаружения вторжений должны зафиксировать попытки взлома системного периметра со стороны инсайдера.

Средства человеческого обнаружения

- **Руководство**
Руководитель должен первым заметить подозрительную деятельность.
- **Отделы контроля и аудита, управления рисками, по контролю за соблюдением правовых норм**
Указанные команды имеют собственные системы оперативного обнаружения аномалий и должны предупредить причастные департаменты в случае выявления подозрительных фактов.
- **Сослуживцы**
Коллеги инсайдера являются одним из наиболее ценных каналов выявления и оповещения поскольку прекрасно осведомлены об особенностях рабочей деятельности данного лица.
- **Внешние источники**
Партнеры и внешние контакты также имеют возможности обнаружить вредоносную деятельность инсайдера и оповестить руководство предприятия об обнаруженных аномалиях.

Сдерживание 3

Минимизировать эффект от деятельности инсайдера
Не предпринимать никаких действий без письменного согласия руководства, CISO или ответственного лица. Лучше также заручиться письменным разрешением затронутых лиц. Обсудите все действия с юридическим отделом.

- **Привлечение компетентных лиц**
Необходимо уведомить и привлечь к управлению инцидентом различных лиц. Это могут быть представители отдела кадров, юристы, сотрудники отдела по связям с общественностью, руководство или сам подозреваемый.
- **Встреча с подозреваемым**
Представитель отдела кадров должен встретиться с подозреваемым в инсайдерской деятельности и объяснить ему, что было обнаружено, а также изложить последующие действия. На данном этапе может понадобиться поддержка со стороны юридического и технического отделов, а также со стороны руководства.
- **Понижение уровня доступа**
В случае если подозреваемый должен продолжать выполнение профессиональной деятельности в течение периода расследования, рекомендуется понизить его привилегии доступа.
- **Замораживание доступа**
Заморозить доступы подозреваемого лица: доступ к данным, системная учетная запись, ключи, бэджи, и т.д.
- **Удаленный доступ**
Приостановить возможности удаленного доступа: смартфоны, учетные записи VPN, токены.
- **Конфискация оборудования**
Конфисковать профессиональное оборудование доступа к системе информации: компьютер, планшет, телефон, и т.д.

Сдерживание 3

Вариант 1: Аномальная деятельность
Если вредоносная деятельность инсайдера не получила подтверждения на данный момент, необходимо инициировать две линии расследования:

- Компьютерная криминалистика оборудования подозреваемого;
- Анализ логов и иных компонентов информационной системы предприятия.

Вариант 2: Вредоносная деятельность
Если факт вредоносности деятельности инсайдера уже получила подтверждение, рассмотреть возможность подать жалобу на инсайдера.
Не предпринимать никаких дальнейших технических действий в данном случае. Предоставить все найденные доказательства вредоносной деятельности представителям юридического департамента или правоохранительным органам; быть готовым предоставить дополнительную поддержку в случае необходимости.
В случае если публичное обнародование деятельности инсайдера может нанести урон предприятию, обеспечить поддержку для сдерживания негативного эффекта до разглашения инцидента. В случае необходимости, проинформировать компетентные органы

Устранение 4

Принять меры для устранения угрозы и предотвращения будущих инцидентов.

Эффективность мер по устранению эффекта инцидента довольно ограничена в данном случае. Возможно принятие следующих мер:

- Дисциплинарные меры в отношении провинившегося / увольнение.
- Удаление вредоносных фиктивных операций, внесенных инсайдером.
- Анализ созданных инсайдером программ, скриптов и т.п.; их удаление или модификация.

Восстановление 5

Восстановить нормальное функционирование системы

Если инцидент не имел публичной огласки, уведомить всех заинтересованных лиц (клиенты, партнеры) и компетентные органы. Если речь идет о серьезном инциденте, уведомления должны быть озвучены непосредственно руководством.

Уведомить сотрудников повышения осведомленности по проблемам безопасности.

По нормализации ситуации можно снять официальное сообщение с сайта компании.

После инцидента 6

Задокументировать детали инцидента, обсудить извлеченные уроки, оптимизировать процессы защиты.

Отчет
Написать отчет об инциденте; сделать отчет доступным причастным лицам. Раскрыть следующие темы:

- Причины инфекции
- Действия и сроки
- Верные действия
- Неверные действия
- Стоимость инцидента

Капитализация опыта
Возможно внедрения следующих улучшений по предотвращению / раннему обнаружения инсайдерской деятельности:

- Улучшение процесса авторизации.
- Улучшение внутренних процессов контроля.
- Повышение уровня осведомленности о мошенничестве и вредоносной внутренней деятельности.

SOCIETE GENERALE | CERT | SOCIETE GENERALE

Incident Response Methodology

cert.sg@socgen.com / cert.societegenerale.com / @certsg

IRM #12

Инсайдерская деятельность

Реагирование на злоумышленные действия сотрудников

Автор IRM: CERT SG
Версия IRM: 1.1 (RU)

Об IRM

Данная методология по реагированию на инциденты ИБ является кратким руководством, предназначенным вниманию специалистов, работающих над проблемами безопасности:

- Системные администраторы
- Члены Security Operation Centers
- Начальники и представители отделов ИБ
- Представители CERT/CSIRT/IRT

Распространение IRM возможно в рамках SG Group.

В случае обнаружения признаков инцидента, следуйте рекомендациям IRM, делайте заметки, не поддавайтесь панике и немедленно оповестите свой CERT.

Фазы управления инцидентами ИБ

Шесть фаз управления инцидентами ИБ:

- **Подготовка**: подготовится к управлению инцидентом
- **Обнаружение**: идентифицировать проблему
- **Сдерживание**: ограничить негативный эффект
- **Устранение**: ликвидировать угрозу
- **Восстановление**: восстановить до нормального
- **После инцидента**: формализация и совершенствование процесса управления инцидентом

IRM предоставляет детальную информацию по каждой из фаз.