УТВЕРЖДАЮ
Начальник отдела
информационной безопасности
Костенко Е. В.

СОГЛАСОВАНО
председатель правления
ООО «АВС»
Иванов А. Г.
«09» 11/ 2023 г.

Группа реагирования на инцидент состоит из работников отдела ИБ и администрирующего IT инфраструктуру персонала.

Общие меры реагирования на инцидент:

1. Определение типа атаки или иного происшествия которое может повлечь нарушение целостности/доступности/конфиденциальности информации на основе данных SIEM или иных данных из которых следует что инцидент произошел или происходит в данный момент.

2. Сдерживание. На этом этапе нужно иметь приблизительное понимание какому типу атаки мы подвергаемся, на основании этого принимаем меры направленные на недопущение распространения/развития. Лучшим способом изоляции является помещение узлов в отдельный изолированный сегмент или VLAN

3. Сохранение следов атаки или другого вредоносного воздействия для дальнейшего расследования - это могут быть фрагменты кода вредоноса, дампы памяти, IP адреса атакующие ресурс при DDOS

4. Ликвидация последствий инцидента ИБ.

5. Восстановление штатной работы систем подверженных атаке или другому негативному влиянию - это может быть физическое повреждение сервера например в результате затопления или пожара.

6. Обновление политики реагирования на инциденты ИБ с учетом новых угроз выявленных в результате расследования.

Некоторые частные меры реагирования на определенные типы инцидентов:

Утечка персональных данных:
Уведомление в установленные сроки - в течение 1 суток об инциденте связанном с персональными данными.
В соответствии с законодательством и отраслевыми стандартами финансовых организаций, нужно уведомить Роскомнадзор и Банк России.

Вредоносное ПО:
Поместить узлы в отдельный изолированный сегмент или VLAN.
Сохранение и анализ дампа памяти машин с вредоносным ПО.
Восстановление из бекапа или переустановка ОС и смена всех логин/паролей.

DDOS:
Логирование атаки - сбор IP адресов, занесение в черные списки firewall, перераспределение сетевой нагрузки при необходимости. Выявление цели и источника атаки.

Аномальная активность административных аккаунтов:
Сохранение и анализ логов, определение времени начала аномалии, выявление возможных инсайдерских атак, смена паролей всех аккаунтов в том числе не административных, проверка на наличие повышенных привилегий у простых пользовательских аккаунтов.