Наращивание потенциала кибербезопасности Набор инструментов для финансовых организаций

Руководство по реагированию на инциденты

Подготовка

⇒ Совместно с высшим руководством вашей организации и другими соответствующими сотрудниками разработайте план реагирования на инциденты и план обеспечения непрерывности бизнеса, исходя из наиболее актуальных рисков, выявленных в ходе оценки киберрисков организации.

- Разработайте сценарии угроз для инцидентов, связанных с наиболее приоритетными киберрисками организации. Сосредоточьтесь на наращивании потенциала для реагирования на эти сценарии.
- Определите, составьте и представьте в вашей организации список контактных лиц для реагирования на инциденты.
- Найдите и запишите контактные данные соответствующих местных и федеральных правоохранительных органов и должностных лиц.
- Установите положения, определяющие, о каких типах инцидентов необходимо сообщать, когда и кому.
- Определите и представьте в письменном виде указания, определяющие, как быстро персонал должен реагировать на инциденты и какие действия должны быть выполнены на основе соответствующих факторов, таких как функциональное и информационное воздействие инцидента, а также вероятной возможности восстановления после него.
- Сообщите всем сотрудникам, чтобы в случае инцидента они связывались с вашей технической командой. Обычно это ИТ-персонал и/или директор по информационной безопасности / директор по ИТ / другой подобный менеджер.
- Выполните развертывание решений для мониторинга действий сотрудников и выявления угроз и инцидентов.
- Включите планы по обеспечению непрерывности бизнеса для координации работы организации с поставщиками и основными клиентами во время чрезвычайной ситуации, в том числе при необходимости осуществления руководства или проведения альтернативных бизнес-операций.
- Включите определенные в письменном виде процедуры отключения и перезапуска системы в чрезвычайной ситуации.
- Обеспечьте разработку и тестирование методов извлечения и восстановления резервных данных. Периодически проверяйте резервные данные на предмет их целостности.
- Заключите соглашения и процедуры ведения коммерческой деятельности в альтернативном учреждении/центре.
- Обеспечьте работу четкого канала распространения для всех клиентов.

Обучение

⇒ Организуйте небольшие теоретические занятия со всеми сотрудниками или представителями персонала всех уровней, в том числе с руководителями организации, специалистами по связям с общественностью, сотрудниками юридического отдела и отдела нормативно-правового соответствия.
⇒ Определите или лучше примите участие в отраслевых теоретических занятиях, связанных с деятельностью вашей организации.
⇒ Разработайте процедуру проверки того, что сделанные в ходе занятий выводы включены в стратегию обеспечения кибербезопасности компании.

Реагирование

⇒ Внедрите действия плана реагирования на инциденты, чтобы свести к минимуму последствия, в том числе в отношении подрыва репутации.
⇒ Определите поврежденные или находящиеся под угрозой системы и оцените повреждения.
⇒ Для уменьшения ущерба выполните удаление (отключение) поврежденных активов.
⇒ Начните запись всей информации сразу же после того, как команда выразит подозрения по поводу возможного инцидента. Попытайтесь сохранить доказательства инцидента при отключении/разделении поврежденного идентифицируемого актива, например, соберите данные о конфигурации системы, сети и журналов обнаружения вторжений из поврежденных активов.
⇒ Уведомите соответствующие внутренние стороны, сторонних поставщиков и органы власти и при необходимости запросите поддержку.
⇒ Инициируйте меры по уведомлению клиентов и оказанию помощи в соответствии с законами, нормативно-правовыми актами и межведомственным руководством.
⇒ Используйте такие платформы обмена угрозами, как FS-ISAC или MISP для уведомления об угрозах других организаций из вашей отрасли.
⇒ Задокументируйте все предпринятые во время инцидента шаги для последующего анализа.

Восстановление

⇒ По возможности восстановите активы с использованием периодических «точек восстановления» и используйте резервные данные для восстановления систем до последнего известного «исправного» состояния.
⇒ Обеспечьте создание обновленных «чистых» резервных копий из восстановленных активов и убедитесь, что все резервные копии критически важных активов хранятся в физически защищенном месте.
⇒ Выполните тестирование и убедитесь, что инфицированные системы полностью восстановлены. Убедитесь, что затронутые системы нормально функционируют.

Анализ

⇒ Обсудите «сделанные выводы» после инцидента. Организуйте встречу с руководящим составом, доверенными советниками и поставщиками услуг поддержки аппаратного обеспечения для проведения анализа возможных уязвимостей или выработки рекомендаций по внедрению новых мер.
⇒ По возможности определите уязвимости (будь то программное обеспечение, оборудование, бизнес-операции или поведение персонала), которые привели к инциденту и разработайте план по их устранению.
⇒ Разработайте план мониторинга для выявления аналогичных или потенциально возможных инцидентов, связанных с выявленными проблемами.
⇒ Поделитесь сделанными выводами и информацией об инциденте на платформах обмена угрозами, таких как FS-ISAC.
⇒ Включите сделанные выводы в протоколы реагирования на произошедшие в организации инциденты.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE · SWIFT INSTITUTE · FS-ISAC · Standard Chartered · CYBER READINESS INSTITUTE · GLOBAL CYBER ALLIANCE