Десять элементов кибербезопасности: высокоуровневый обзор

Кибербезопасность направлена на защиту цифровых данных и технических средств их обработки – сетей, компьютеров, сетевых устройств – от несанкционированного цифрового доступа, атак или ущерба. Эффективный подход к обеспечению кибербезопасности начинается с первого и самого главного элемента – системы управления рисками кибербезопасности.

1. Система управления рисками

Формирование и внедрение надлежащей системы управления рисками является залогом успеха в обеспечении кибербезопасности любой организации. Такая система должна быть обеспечена необходимыми ресурсами для функционирования, а также поддерживаться советом директоров и руководством организации. Необходимо явно демонстрировать свой подход к управлению рисками при разработке соответствующих политик и правил. Они должны быть направлены на то, чтобы все сотрудники, клиенты и поставщики знали о подходе, способах принятия решений и любых применимых границах рисков.

2. Безопасная конфигурация

Наличие подхода для определения базовых технологий построения и процессов для обеспечения управления конфигурацией может значительно повысить безопасность систем. Следует разработать стратегию для удаления или отключения ненужных функций из систем и оперативного исправления известных уязвимостей. Несоблюдение этого требования, скорее всего, приведет к увеличению риска компрометации информационных систем и цифровой информации.

3. Сетевая безопасность

Подключение локальных сетей организации к информационно-телекоммуникационной сети «Интернет» и к другим сетям делает ИТ-инфраструктуру организации уязвимой для удаленных сетевых атак. Следуя базовым рекомендациям по сетевой безопасности, а также внедряя соответствующие архитектурные и технические решения, можно существенно уменьшить вероятность успешной реализации сетевых атак или снизить шансы на то, что попытка реализации атак сможет причинить побочный вред организации. Сети многих организаций часто являются территориально-распределенными со множеством точек подключения, а использование мобильных или удаленных рабочих мест и облачных сервисов затрудняет определение фиксированной границы сети. Вместо того, чтобы сосредоточиться исключительно на физической топологии сети организации, следует сфокусироваться на местах обработки цифровых данных и оценки их уязвимости перед атаками.

4. Управление привилегиями пользователей

Если пользователям предоставлены ненужные системные привилегии или права доступа к данным, последствия неправильного использования или компрометации таких учетных записей будут более серьезными, чем могли бы быть. Все пользователи должны обладать разумным (но как можно меньшим) уровнем системных привилегий и прав, необходимых для их роли. Предоставление расширенных системных привилегий должно тщательно контролироваться и управляться. Этот принцип иногда называют «принципом наименьших привилегий» (англ. Principle of least privilege).

5. Обучение и осведомленность пользователей

Пользователи играют решающую роль в обеспечении кибербезопасности организации, поэтому важно, чтобы правила безопасности и средства защиты информации позволяли пользователям выполнять свою работу, а также помогали обеспечивать кибербезопасность организации. Этому может способствовать систематическая реализация программ по повышению осведомленности и обучению, которые обеспечивают пользователей необходимыми экспертными знаниями и лучшими практиками в области безопасности, а также способствуют формированию культуры кибербезопасности.

6. Управление инцидентами

Все организации время от времени сталкиваются с инцидентами информационной безопасности. Инвестирование сил и средств в разработку эффективной политики и процессов управления инцидентами помогут повысить устойчивость, поддержать непрерывность бизнеса, повысить доверие клиентов и заинтересованных сторон, а также потенциально уменьшить любое

негативное влияние инцидентов. Следует уделять большое внимание поддержанию и развитию внутри организации экспертизы по управлению инцидентами путем выделения соответствующих специалистов.

7. Защита от вредоносных программ

Вредоносное программное обеспечение (в том числе, компьютерные вирусы) является общим термином для определения любого исполняемого кода или данных, которые могут оказать злонамеренное, нежелательное воздействие на информационные системы и цифровые данные. Любой обмен информацией сопряжен с определенным риском возможного обмена вредоносными программами, что может негативно повлиять на ИТ-инфраструктуру и операционную деятельность организации. Риск может быть уменьшен за счет разработки и внедрения соответствующих стратегий защиты от вредоносных программ в рамках общего подхода Defense-in-Depth, предполагающего создание эшелонированной и комплексной системы защиты организации от угроз в информационной сфере.

8. Мониторинг

Мониторинг показателей состояния и функционирования информационных систем обнаруживать фактические атаки или попытки атак на цифровые данные и ИТ-инфраструктуру организации. Хороший мониторинг необходим для эффективного реагирования на атаки. Кроме того, мониторинг позволяет обеспечить надлежащее использование систем в соответствии с их предназначением и внутренними требованиями организации. Мониторинг часто является жизненно необходимым для соблюдения правовых или нормативных требований.

9. Управление съемными носителями

Съемные (отчуждаемые) носители информации являются одним из наиболее популярных путей для распространения вредоносных программ и случайного или преднамеренного раскрытия конфиденциальных сведений. Необходимо четко определить и урегулировать ситуации, когда использование съемных носителей действительно является необходимым, а также применять соответствующие меры безопасности для их использования.

10. Удаленный доступ

Удаленный доступ к информационной системе дает большие преимущества, но также подвергает организацию новым рискам, которые необходимо контролировать. Следует установить политики и правила, основанные на оценке соответствующих рисков, которые буду регулировать предоставление удаленного доступа к системам. Действие таких политик и правил должно распространяться на всех пользователей, включая клиентов и поставщиков.

информационная безопасность, техническая защита информации