Что такое кибербезопасность?

Кибербезопасность - это практика защиты компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных от вредоносных атак. Она также известна как безопасность информационных технологий или безопасность электронной информации. Термин применяется в различных контекстах, от бизнеса до вычислений на мобильных устройствах, и может быть подразделен на несколько общих категорий.

- **Сетевая безопасность** - это практика защиты компьютерной сети от злоумышленников, будь то целенаправленные злоумышленники или ситуативно-обусловленные вредоносные программы.

- **Безопасность приложений** направлена на защиту программного обеспечения и устройств от угроз. Приложение, находящееся под угрозой, может предоставить доступ к данным, которые он долен защищать. Успешная безопасность начинается на этапе проектирования, задолго до использования программы или устройства.

- **Информационная безопасность** защищает целостность и конфиденциальность данных, как в хранилище, так и в пути.

- **Операционная безопасность** включает процессы и решения для обработки и защиты активов данных. Права доступа, которые пользователи получают при доступе к сети, и процедуры, которые определяют, как и где данные могут храниться или совместно использоваться, подпадают под это определение.

- **Аварийное восстановление и бесперебойная работа** определяют, как организация реагирует на инцидент кибербезопасности или любое другое событие, которое приводит к потере операций или данных. Стратегия аварийного восстановления определяет, как организация восстанавливает свои операции и информацию, чтобы вернуться к тем же эксплуатационным возможностям, что и до этого события. Бесперебойная работа - это план, к которому прибегает организация, пытаясь действовать без определенных ресурсов.

- **Обучение конечных пользователей** затрагивает самый непредсказуемый фактор кибербезопасности: людей. Любой человек может случайно внести вирус в безопасную систему, не соблюдая правила безопасности. Обучение пользователей удалять подозрительные вложения электронной почты, не подключать неопознанные USB-накопители и другие важные уроки имеют жизненно важное значение для безопасности любой организации.

Масштаб киберугрозы

Правительство США тратит 19 миллиардов долларов в год на кибербезопасность, но предупреждает, что кибератаки продолжают развиваться быстрыми темпами. Для борьбы с распространением вредоносного кода и помощи в раннем обнаружении Национальный институт стандартов и технологий (NIST) рекомендует осуществлять постоянный мониторинг всех электронных ресурсов в режиме реального времени.

Угрозы, которым противостоит кибербезопасность, имеют три аспекта:

1. Киберпреступность включает в себя отдельных субъектов или группы, нацеленные на системы для получения финансовой выгоды или нарушения работы.

2. Кибератака часто включает сбор политически мотивированной информации.

3. Кибертеррор предназначен для подрыва электронных систем, чтобы вызвать панику или страх.

Обычные методы, используемые злоумышленниками для управления компьютерами или сетями, включают вирусы, черви, шпионское ПО, трояны и вымогателей. Вирусы и черви могут самовоспроизводиться и повреждать файлы или системы, в то время как шпионские программы и трояны часто используются для скрытого сбора данных. Программы-вымогатели ожидает возможности зашифровать всю информацию о пользователе и требует оплаты, чтобы вернуть доступ пользователю. Вредоносный код часто распространяется через незапрошенное вложение электронной почты или через законно выглядящую загрузку, которая на самом деле несет данные вредоносного ПО.

Угрозы кибербезопасности затрагивают все отрасли, независимо от их объема. Отрасли, в которых было больше сообщений о кибератаках в последние годы, это здравоохранение, производство, финансы и правительство. Некоторые из этих секторов более привлекательны для киберпреступников, поскольку они собирают финансовые и медицинские данные, но все компании, использующие сети, могут быть нацелены на данные клиентов, корпоративный шпионаж или атаки клиентов.

Защита конечного пользователя

Итак, как меры кибербезопасности защищают пользователей и системы? Во-первых, кибербезопасность использует криптографические протоколы для шифрования электронной почты, файлов и других важных данных. Это не только защищает информацию в пути, но также защищает от потери или кражи. Кроме того, программное обеспечение безопасности конечного пользователя сканирует компьютеры на наличие фрагментов вредоносного кода, помещает его в карантин и затем удаляет с компьютера. ПО безопасности может даже обнаруживать и удалять вредоносный код, скрытый в основной загрузочной записи (MBR) и предназначенный для шифрования или удаления данных с жесткого диска компьютера.

Протоколы электронной безопасности также ориентированы на обнаружение вредоносных программ в режиме реального времени. Многие используют эвристический анализ и анализ поведения для мониторинга поведения программы и ее кода для защиты от вирусов или троянов, которые меняют свою форму при каждом выполнении (полиморфное и метаморфическое вредоносное ПО). Программы безопасности могут ограничивать потенциально вредоносные программы виртуальным пузырем, отдельным от сети пользователя, чтобы анализировать их поведение и узнавать, как лучше обнаруживать новые инфекции.

Программы безопасности продолжают развивать новые средства защиты, поскольку специалисты по кибербезопасности выявляют новые угрозы и новые способы борьбы с ними.

Определение кибербезопасности

Кибербезопасность, также называемая информационной безопасностью, относится к практике обеспечения целостности, конфиденциальности и доступности (ICA) информации. Кибербезопасность состоит из развивающегося набора инструментов, подходов к управлению рисками, технологий, обучения и передовых практик, предназначенных для защиты сетей, устройств, программ и данных от атак или несанкционированного доступа.

Почему кибербезопасность важна?

Сегодня мир доверяет технологиям больше, чем когда-либо прежде. В результате создание цифровых данных резко возросло. Сегодня предприятия и правительства хранят большую часть этих данных на компьютерах и передают их по сети на другие компьютеры. Устройства и их базовые системы имеют уязвимости, которые при эксплуатации подрывают здоровье и цели организации.

Утечка данных может иметь ряд разрушительных последствий для любого бизнеса. Это может разрушить репутацию компании через потерю доверия потребителей и партнеров. Потеря важных данных, таких как исходные файлы или интеллектуальная собственность, может стоить компании ее конкурентного преимущества. Более того, утечка данных может повлиять на корпоративные доходы из-за несоблюдения правил защиты данных. По

оценкам, в среднем утечка данных обходится пострадавшей организации в 3,6 миллиона долларов. С учетом утечек данных, наделавших много шума и вошедших в заголовки СМИ, важно, чтобы организации приняли и внедрили строгий подход к кибербезопасности.

Распространенные типы кибербезопасности

Сетевая безопасность защищает сетевой трафик, контролируя входящие и исходящие соединения, чтобы предотвратить проникновение или распространение угроз в сети.

Предотвращение потери данных (DLP) защищает данные, фокусируясь на расположении, классификации и мониторинге информации в состоянии покоя, при использовании и в движении.

Информационная облачная безопасность обеспечивает защиту данных, используемых в облачных сервисах и приложениях.

Системы обнаружения вторжений (IDS) или Системы предотвращения вторжений (IPS) работают для выявления потенциально враждебной кибер-активности.

Управление идентификацией и доступом (IAM) использует службы аутентификации для ограничения и отслеживания доступа сотрудников для защиты внутренних систем от вредоносных объектов.

Шифрование - это процесс кодирования данных, чтобы сделать их неразборчивыми, и часто используется во время передачи данных, чтобы предотвратить кражу при передаче.

Антивирусные / антивирусные решения сканируют компьютерные системы на наличие известных угроз. Современные решения даже способны обнаруживать неизвестные ранее угрозы на основе их поведения.