Что обозначает понятие «информационная безопасность»?

Информационная безопасность – это сохранение и защита информации, а также ее важнейших элементов, в том числе системы и оборудование, предназначенные для использования, сбережения и передачи этой информации. Другими словами, это набор технологий, стандартов и методов управления, которые необходимы для защиты информационной безопасности.

Цель обеспечения информационной безопасности – защитить информационные данные и поддерживающую инфраструктуру от случайного или преднамеренного вмешательства, что может стать причиной потери данных или их несанкционированного изменения. Информационная безопасность помогает обеспечить непрерывность бизнеса.

Для успешного внедрения систем информационной безопасности на предприятии необходимо придерживаться трех главных принципов:

Конфиденциальность. Это значит ввести в действие контроль, чтобы гарантировать достаточный уровень безопасности с данными предприятия, активами и информацией на разных этапах деловых операций для предотвращения нежелательного или несанкционированного раскрытия. Конфиденциальность должна поддерживаться при сохранении информации, а также при транзите через рядовые организации независимо от ее формата.

Целостность. Целостность имеет дело с элементами управления, которые связаны с обеспечением того, чтобы корпоративная информация была внутренне и внешне последовательной. Целостность также гарантирует предотвращение искажения информации.

Доступность. Доступность обеспечивает надежный и эффективный доступ к информации уполномоченных лиц. Сетевая среда должна вести себя предсказуемым образом с целью получить доступ к информации и данным, когда это необходимо. Восстановление системы по причине сбоя является важным фактором, когда речь идет о доступности информации, и такое восстановление также должно быть обеспечено таким образом, чтобы это не влияло на работу отрицательно.

Контроль информационной безопасности

Административный. Административный вид контроля состоит из утвержденных процедур, стандартов и принципов. Он формирует рамки для ведения бизнеса и управления людьми. Законы и нормативные акты, созданные государственными органами, также являются одним из видов административного контроля. Другие примеры административного контроля включают политику корпоративной безопасности, паролей, найма и дисциплинарные меры.

Логический. Логические средства управления (еще называемые техническими средствами контроля) базируются на защите доступа к информационным системам, программном обеспечении, паролях, брандмауэрах, информации для мониторинга и контроле доступа к системам информации.

Физический. Это контроль среды рабочего места и вычислительных средств (отопление и кондиционирование воздуха, дымовые и пожарные сигнализации, противопожарные системы, камеры, баррикады, ограждения, замки, двери и др.).

Виды средств защиты информации:

Антивирусные программы — программы, которые борятся с компьютерными вирусами и возобновляют зараженные файлы.

Облачный антивирус (CloudAV) – одно из облачных решений информационной безопасности, что применяет легкое программное обеспечение агента на защищенном компьютере, выгружая большую часть анализа информации в инфраструктуру провайдера. CloudAV – это также решение для эффективного сканирования вирусов на приспособлениях с невысокой вычислительной мощностью для выполнения самих сканирований. Некоторые образцы облачных антивирусных программ – это Panda Cloud Antivirus, Crowdstrike, Cb Defense и Immunet.

DLP (Data Leak Prevention) решения – это защита от утечки информации. Предотвращение утечки данных (DLP) представляет собой набор технологий, направленных на предотвращение потери конфиденциальной информации, которая происходит на предприятиях по всему миру. Успешная реализация этой технологии требует значительной подготовки и тщательного технического обслуживания. Предприятия, желающие интегрировать и внедрять DLP, должны быть готовы к значительным усилиям, которые, если они будут выполнены правильно, могут значительно снизить риск для организации.

Криптографические системы – преобразование информации таким образом, что ее расшифровка становится возможной только с помощью определенных кодов или шифров (DES – Data Encryption Standard, AES – Advanced Encryption Standard). Криптография обеспечивает защиту информации и другими полезными приложениями, включая улучшенные методы проверки подлинности, дайджесты сообщений, цифровые подписи и зашифрованные сетевые коммуникации. Старые, менее безопасные приложения, например Telnet и протокол передачи файлов (FTP), медленно заменяются более безопасными приложениями, такими как Secure Shell (SSH), которые используют зашифрованные сетевые коммуникации. Беспроводная связь может быть зашифрована с использованием таких протоколов, как WPA/WPA2 или более старый (и менее безопасный) WEP. Проводные коммуникации (такие как

ITU-T G.hn) защищены с использованием AES для шифрования и X.1035 для аутентификации и обмена ключами. Программные приложения, такие как GnuPG или PGP, могут применяться для шифрования информационных файлов и электронной почты.

Межсетевые экраны (брандмауэры или файрволы) – устройства контроля доступа в сеть, предназначенные для блокировки и фильтрации сетевого трафика. Брандмауэры обычно классифицируются как сетевые или хост-серверы. Сетевые брандмауэры на базе сети расположены на шлюзовых компьютерах LAN, WAN и интрасетях. Это либо программные устройства, работающие на аппаратных средствах общего назначения, либо аппаратные компьютерные устройства брандмауэра. Брандмауэры предлагают и другие функции для внутренней сети, которую они защищают, например, являются сервером DHCP или VPN для этой сети. Одним из лучших решений как для малых, так и для больших предприятий являются межсетевые экраны CheckPoint.

VPN (Virtual Private Network). Виртуальная частная сеть (VPN) дает возможность определить и использовать для передачи и получения информации частную сеть в рамках общедоступной сети. Таким образом, приложения, работающие по VPN, являются надежно защищенными. VPN дает возможность подключиться к внутренней сети на расстоянии. С помощью VPN можно создать общую сеть для территориально отдаленных друг от друга предприятий. Что касается отдельных пользователей сети – они также имеют свои преимущества использования VPN, так как могут защищать собственные действия с помощью VPN, а также избегать территориальные ограничения и использовать прокси-серверы, чтобы скрыть свое местоположение.

Proxy-server (Прокси-сервер) – это определенный компьютер или компьютерная программа, которая является связывающим звеном между двумя устройствам, например, такими как компьютер и другой сервер. Прокси-сервер можно установить на одном компьютере вместе с сервером брандмауэра, или же на другом сервере. Плюсы прокси-сервера в том, что его кэш может служить для всех пользователей. Интернет-сайты, которые являются наиболее часто запрашиваемыми, чаще всего находятся в кэше прокси, что несомненно удобно для пользователя. Фиксирование своих взаимодействий прокси-сервером служит полезной функцией для исправления неполадок.

Системы мониторинга и управления информационной безопасностью, SIEM. Чтобы выявлять и реагировать на возникающие угрозы информационной безопасности, используется решение SIEM, которое выполняет сбор и анализ событий из разных источников, таких как межсетевые экраны, антивирусы, IPS, оперативные системы и т.п. Благодаря системе SIEM у компаний появляется возможность централизованно хранить журналы

событий и коррелировать их, определяя отклонения, потенциальные угрозы, сбои в работе ИТ-инфраструктуры, кибератаки и т.д.

Основные меры обеспечения информационной безопасности

- **Криптографическая защита данных.** При реализации этой меры используются специальные механизмы защиты с помощью шифрования информации для обеспечения кибербезопасности организации. Криптографические защитные методы применяются в различных отраслях деятельности для хранения, обработки, передачи информации по сетям связи и на всевозможных носителях.

- **Обнаружение кибератак и защита от них**. В этом случае предполагается использование специализированных систем обнаружения вторжений (IDS), которые являются на сегодняшний день одними из наиболее важных элементов современных систем кибербезопасности внутренних сетей предприятий и организаций. Несмотря на то, что использование технологии IDS не гарантирует полную защиту данных, она всё равно играет значительную роль в этой сфере.

- **Разграничение доступа к информационным системам.** Разграничение доступа в современных организациях представлено в виде комплекса правил, определяющего для каждого субъекта, метода и объекта наличие или отсутствие прав доступа с помощью указанного метода. Наибольшее распространение сейчас имеют две модели разграничения доступа – дискреционная и полномочная.

- **Межсетевые экраны.** Представлены в виде программных или программно-аппаратных элементов компьютерных систем, основная задача которых заключается в контроле и фильтрации проходящего веб-трафика в соответствии с заданными правилами. Межсетевые экраны обеспечивают защиту сегментов сети или отдельных хостов от несанкционированного доступа с применением уязвимых мест в программном обеспечении или протоколах сетевой модели OSI.

- **Антивирусная защита.** Антивирусное программное обеспечение применяется для профилактики и диагностики вирусного заражения, а также для восстановления функционирования информационных систем, которые уже были поражены вредоносным ПО. Антивирусные программы представляют собой программное обеспечение, используемое для выявления, уничтожения вирусов, вредоносного ПО, программ-вымогателей, шпионского софта и т. д.

- **Резервное копирование данных (бэкап).** При резервном копировании создаются копии файлов на другом устройстве или в облачной инфраструктуре

на случай потери или повреждения основного устройства. Существует два основных способа резервного копирования: дифференциальное и полное. При полном выполняется копирование всех файлов, а при дифференциальном – в первый раз копируется всё, а в дальнейшем только те файлы, в которые были внесены изменения

- **Защита от утечек данных.** Защита такого типа представляет собой реализацию комплекса мер, которые направлены на то, чтобы обеспечить сохранность и целостность защищаемой информации компании для сведения к минимуму вероятности возникновения финансовых и репутационных потерь, если такая утечка всё же случится. Для защиты от утечек используются DLP-системы, обеспечивающие полноценный контроль информационных ресурсов предприятия, отслеживание содержимого сообщений и документооборота, предупреждение о нарушении политик безопасности, помощь при осуществлении расследований и предотвращении утечек данных.

- **Протоколирование и аудит.** Под протоколированием принято понимать процессы сбора и накопления информации о тех событиях, которые происходят в информационной системе. Аудит – анализ собранной информации, который осуществляется в режиме реального времени или с определенной периодичностью. Если аудит выполняется с автоматическим реагированием на обнаруженные нештатные ситуации, то его называют активным.

Что такое кибербезопасность

Кибербезопасность — это защита подключенных к интернету систем (оборудования, программного обеспечения и данных) от киберугроз.

Чем отличается кибербезопасность от информационной безопасности:

Понятия «кибербезопасность» и «информационная безопасность» довольно часто используются в качестве синонимов. Однако в действительности эти термины сильно различаются и не являются взаимозаменяемыми. Под кибербезопасностью понимают защиту от атак в киберпространстве, а под информационной безопасностью — защиту данных от любых форм угроз, независимо от того, являются ли они аналоговыми или цифровыми.

Что входит в сферу интересов кибербезопасности:

Практики кибербезопасности могут применяться в самых разных областях — от промышленных предприятий до мобильных устройств обычных пользователей:

Безопасность критической инфраструктуры — меры защиты компьютерных систем, сетей объектов критической информационной

инфраструктуры (КИИ). К объектам КИИ относятся электрические сети, транспортная сеть, автоматизированные системы управления и информационно-коммуникационные системы и многие другие системы, защита которых имеет жизненно важное значение для безопасности страны и благополучия граждан.

Сетевая безопасность — защита базовой сетевой инфраструктуры от несанкционированного доступа и неправильного использования, а также от кражи информации. Технология включает в себя создание безопасной инфраструктуры для устройств, приложений и пользователей.

Безопасность приложений — меры безопасности, применяемые на уровне приложений и направленные на предотвращение кражи, взлома данных или кода приложения. Методы охватывают вопросы безопасности, возникающие при разработке, проектировании, развертывании и эксплуатации приложений.

Облачная безопасность — взаимосвязанный набор политик, элементов управления и инструментов защиты систем облачных вычислений от киберугроз. Меры облачной безопасности направлены на обеспечение безопасности данных, онлайн-инфраструктуры, а также приложений и платформ. Облачная безопасность имеет ряд общих концепций с традиционной кибербезопасностью, но в этой области есть также собственные передовые методы и уникальные технологии.

Обучение пользователей. Программа повышения осведомленности в сфере информационной безопасности (security awareness) является важной мерой при построении надежной защиты компании. Соблюдение сотрудниками правил цифровой гигиены помогает усилить безопасность конечных точек. Так, пользователи, проинформированные об актуальных угрозах, не станут открывать вложения из подозрительных электронных писем, откажутся от использования ненадежных USB-устройств и перестанут прикреплять на монитор наклейки с логином и паролем.

Аварийное восстановление (планирование) непрерывности бизнеса — совокупность стратегий, политик и процедур, определяющих, каким образом организация должна реагировать на потенциальные угрозы или непредвиденные стихийные бедствия, чтобы должным образом адаптироваться к ним и минимизировать негативные последствия.

Операционная безопасность — процесс управления безопасностью и рисками, который предотвращает попадание конфиденциальной информации в чужие руки. Принципы операционной безопасности изначально использовали военные, чтобы не дать секретной информации попасть к противнику. В

настоящее время практики операционной безопасности широко используются для защиты бизнеса от потенциальных утечек данных.

Типы угроз кибербезопасности

Технологии и лучшие практики кибербезопасности защищают критически важные системы и конфиденциальную информацию от стремительно растущего объема изощренных кибератак. Ниже приведены основные типы угроз, с которыми борется современная кибербезопасность:

Вредоносное программное обеспечение (ВПО) Любая программа или файл, которые могут причинить ущерб компьютеру, сети или серверу. К вредоносным программам относятся компьютерные вирусы, черви, трояны, программы-вымогатели и программы-шпионы. Вредоносные программы крадут, шифруют и удаляют конфиденциальные данные, изменяют или захватывают основные вычислительные функции и отслеживают активность компьютеров или приложений.

Социальная инженерия Метод атак, основанный на человеческом взаимодействии. Злоумышленники втираются в доверие к пользователям и вынуждают их нарушить процедуры безопасности, выдать конфиденциальную информацию.

Фишинг Форма социальной инженерии. Мошенники рассылают пользователям электронные письма или текстовые сообщения, напоминающие сообщения из доверенных источников. При массовых фишинговых атаках злоумышленники выманивают у пользователей данные банковских карт или учетные данные.

Целевая атака Продолжительная и целенаправленная кибератака, при которой злоумышленник получает доступ к сети и остается незамеченным в течение длительного периода времени. Целевые атаки обычно направлены на кражу данных у крупных предприятий или правительственных организаций.

Внутренние угрозы Нарушения безопасности или потери, спровоцированные инсайдерами — сотрудниками, подрядчиками или клиентами — со злым умыслом или из-за небрежности.

DoS-атака, или атака типа «отказ в обслуживании» Атака, при которой злоумышленники пытаются сделать невозможным предоставление услуги. При DoS-атаке вредоносные запросы отправляет одна система; DDoS-атака исходит из нескольких систем. В результате атаки можно заблокировать доступ практически ко всему: серверам, устройствам, службам, сетям, приложениям и даже определенным транзакциям внутри приложений.

Сталкерское ПО Программное обеспечение, предназначенное для скрытой слежки за пользователями. Сталкерские приложения часто распространяются под видом легального ПО. Такие программы позволяют злоумышленникам просматривать фотографии и файлы на устройстве жертвы, подглядывать через камеру смартфона в режиме реального времени, узнавать информацию о местоположении, читать переписку в мессенджерах и записывать разговоры.

Криптоджекинг Относительно новый тип киберпреступлений, при которых вредоносное ПО скрывается в системе и похищает вычислительные ресурсы устройства, чтобы злоумышленники могли их использовать для добычи криптовалюты. Процесс криптоджекинга полностью скрыт от глаз пользователей. Большинство жертв начинают подозревать неладное, заметив увеличение счетов за электроэнергию.

Атаки на цепочку поставок Атаки на цепочку поставок эксплуатируют доверительные отношения между организацией и ее контрагентами. Хакеры компрометируют одну организацию, а затем продвигаются вверх по цепочке поставок, чтобы получить доступ к системам другой. Если у одной компании надежная система кибербезопасности, но есть ненадежный доверенный поставщик, то злоумышленники попытаются взломать этого поставщика, чтобы затем проникнуть в сеть целевой организации.

Атаки с использованием машинного обучения и искусственного интеллекта При таких атаках злоумышленник пытается обмануть машинный алгоритм, заставляя его выдавать неправильные ответы. Обычно киберпреступники используют метод «отравления данных», предлагая нейросети для обучения заведомо некорректную выборку.

Цели кибербезопасности

Основной целью кибербезопасности является предотвращение кражи или компрометации информации. Важную роль в достижении этой цели играет триада безопасной IT-инфраструктуры — конфиденциальность, целостность и доступность. Под конфиденциальностью в данном контексте подразумевается набор правил, ограничивающих доступ к информации. Целостность гарантирует, что информация является точной и достоверной. Доступность, в свою очередь, отвечает за надежность доступа к информации уполномоченных лиц. Совместное рассмотрение принципов триады помогает компаниям разрабатывать политики безопасности, обеспечивающие надежную защиту.

Классы продуктов в сфере кибербезопасности

Поставщики предлагают различные продукты и услуги для безопасности:

Средства защиты инфраструктуры (infrastructure security)

Средства управления событиями ИБ (security information and event management (SIEM))

Средства анализа киберугроз (threat Intelligence (TI))

Средства оркестровки (управления) систем безопасности (security orchestration, automation and response (SOAR))

Средства защиты промышленных систем управления (industrial control system (ICS) security)

Платформа реагирования на инциденты (incident response platform (IRP))

Платформа управления рисками (governance, risk and compliance (GRC))

Средства защиты сетей (network security)

Межсетевые экраны (firewall, next generation firewall (FW, NGFW))

Многофункциональные решения (unified threat management (UTM))

Системы обнаружения (предотвращения) вторжений (intrusion detection/prevention system (IDS/IPS))

Системы анализа трафика (network traffic analysis (NTA))

Средства контроля доступа к сети (network access control (NAC))

Средства защиты от сложных и неизвестных киберугроз (network detection and response (NDR))

Шлюзы информационной безопасности (secure web gateway, secure mail gateway (SWG, SMG))

Сетевые «песочницы» (network sandbox)

Виртуальные частные сети (virtual private network (VPN))

Средства защиты приложений (application security)

Средства контроля и оценки уязвимостей (vulnerability assessment (VA))

Средства управления уязвимостями (vulnerability management (VM))

Средства поиска уязвимостей в исходном коде ПО (application security testing (AST))

Межсетевой экран для веб-приложений (web application firewall (WAF))

Защита от DDoS-атак (DDoS protection)

Средства защиты данных (data security)

Средства защиты от несанкционированного доступа (unauthorized access protection (UAP))

Средства защиты от утечек информации (data loss prevention (DLP))

Средства шифрования (encryption)

Средства защиты пользователей (user security)

Средства управления идентификацией, аутентификацией и контролем доступа (identity and access management, identity governance and administration (IAM, IGA))

Средства контроля привилегированных пользователей (privileged access management (PAM))

Средства криптографической защиты информации пользователей (в т.ч. средства электронной подписи) (public key infrastructure (PKI))

Защита рабочих станций, конечных точек (endpoint security)

Антивирусная защита (antivirus protection (AVP))

Системы обнаружения и реагирования на угрозы на рабочих станциях пользователей (конечных точках) (endpoint detection and response (EDR))

Основными игроками на российском рынке кибербезопасности являются компании Positive Technologies, «Лаборатория Касперского», «ИнфоТеКС», «Код безопасности», «Фактор-ТС» и С-Terra.