Глава 1

ВВЕДЕНИЕ В КОМПЬЮТЕРНУЮ БЕЗОПАСНОСТЬ

Обзор области компьютерной безопасности

Компьютерная безопасность, также известная как *кибербезопасность* или *информационная безопасность*, — это практика защиты компьютерных систем, сетей и конфиденциальной информации от несанкционированного доступа, использования, раскрытия, нарушения, модификации или уничтожения. Она представляет собой сочетание технических и организационных мер для обеспечения конфиденциальности, целостности и доступности информации и систем.

Компьютерная безопасность важна, поскольку она помогает защитить организации и отдельных людей от широкого спектра угроз, существующих в цифровом мире. Эти угрозы могут принимать различные формы, такие как вирусы и вредоносные программы, фишинговые аферы и попытки взлома. Без надлежащих мер компьютерной безопасности эти угрозы могут нанести значительный ущерб, включая финансовые потери, репутационный ущерб и потерю личной информации.

В организациях компьютерная безопасность имеет решающее значение для защиты конфиденциальной информации, такой как данные клиентов, финансовые документы и интеллектуальная собственность. Нарушение безопасности может привести к потере доходов, судебным искам и ущербу для репутации компании. Кроме того, организации несут юридическую и этическую ответственность за защиту личной информации своих клиентов и сотрудников.

Для частных лиц компьютерная безопасность также важна: им требуется защищать личную информацию, такую как номера кредитных карт, номера социального страхования и т. п. Нарушение безопасности может привести к краже личных данных, финансовым потерям и ущербу для репутации.

В современном цифровом мире компьютерная безопасность важна как никогда. С ростом использования технологий во всех сферах нашей жизни количество конфиденциальной информации, хранящейся в интернете и передаваемой через него, растет экспоненциально. Так что ставки в случае нарушения безопасности еще никогда не были столь высоки. Поэтому очень важно, чтобы организации и частные лица применяли проактивный подход к защите своих систем и данных путем внедрения средств контроля безопасности и передовой практики.

Обзор типов угроз

В цифровом мире существует множество типов угроз, которые могут принимать различные формы. Рассмотрим некоторые из наиболее распространенных.

- *Вирус* — это тип вредоносного ПО, предназначенного для самовоспроизведения и распространения на другие компьютеры. Заразив компьютер, вирус может вызвать широкий спектр проблем, таких как замедление его работы, удаление файлов и кража личной информации.
- *Вредоносное ПО* — это широкий термин, который охватывает любой тип вредоносных программ, включая вирусы, червей, троянских коней и программы-вымогатели. Вредоносное ПО может использоваться для кражи личной информации, удержания компьютерных систем в заложниках и распространения вредоносных программ на другие компьютеры.
- *Фишинг* — это тип атаки социальной инженерии, направленный на то, чтобы обманом заставить человека предоставить личную информацию, например учетные данные для входа в систему или номера кредитных карт. Фишинговые атаки часто осуществляются через электронную почту, текстовые сообщения или социальные сети, и они могут быть очень убедительными.
- *Хакерство* — это несанкционированный доступ к компьютерной системе или контроль над ней. Хакеры могут задействовать различные методы для получения доступа к компьютерной системе, такие как использование уязвимостей

в программном обеспечении, применение украденных учетных данных для входа в систему или тактика социальной инженерии.

- *Ransomware* — это тип вредоносного ПО, которое шифрует файлы жертвы и требует оплаты в обмен на ключ дешифровки. Оно может вызвать значительные сбои в работе организаций и частных лиц, делая их данные недоступными.
- *Целенаправленная постоянная угроза (Advanced Persistent Threat, APT)* — это тип кибератаки, осуществляемой сложным способом, злоумышленником, хорошо обеспеченным ресурсами. Цель APT — установление долгосрочного присутствия в сети объекта атаки и утечка данных в течение длительного времени.
- *Распределенный отказ в обслуживании (Distributed Denial of Service, DDoS)* — это тип кибератаки, цель которой — сделать веб-сайт или онлайн-сервис недоступным, перегрузив его трафиком из множества источников.

Это лишь несколько примеров типов угроз, существующих в цифровом мире. По мере развития технологий постоянно появляются новые угрозы, поэтому важно быть в курсе последних тенденций в области компьютерной безопасности, чтобы защитить себя и свою организацию.

Виды компьютерной безопасности

Компьютерную безопасность можно разделить на несколько типов, каждый из которых имеет свою уникальную направленность и цели. Рассмотрим некоторые из наиболее распространенных типов компьютерной безопасности.

- *Сетевая безопасность*. Этот тип безопасности направлен на защиту целостности и доступности сети и проходящих через нее данных. Меры сетевой безопасности включают брандмауэры, системы обнаружения вторжений и виртуальные частные сети (VPN).
- *Безопасность конечных точек*. Этот тип безопасности направлен на защиту отдельных устройств, подключаемых к сети, таких как компьютеры, смартфоны и планшеты. Меры безопасности конечных точек включают антивирусное программное обеспечение, системы предотвращения вторжений и решения по управлению мобильными устройствами (Mobile Device Management, MDM).
- *Безопасность приложений*. Этот тип безопасности направлен на защиту программных приложений, которые работают на компьютере или мобильном устройстве. Меры безопасности приложений включают подписание кода, «песочницу» и самозащиту приложений во время выполнения (Runtime Application Self-Protection, RASP).
- *Облачная безопасность*. Этот тип безопасности направлен на защиту данных и приложений, размещенных в облаке. Меры безопасности в облаке включают контроль доступа, шифрование и сегментацию сети.
- *Безопасность IoT*. Этот тип безопасности направлен на защиту устройств интернета вещей (Internet of Things, IoT) и сетей, к которым они подключены. Меры безопасности IoT включают защиту встроенного программного обеспечения устройства, протоколов связи и интерфейсов управления.
- *Оперативная безопасность*. Этот вид безопасности направлен на защиту физических активов и персонала, а также конфиденциальной информации и данных. Меры оперативной безопасности включают контроль доступа, проверку биографических данных и планы реагирования на инциденты.

Каждый из этих видов безопасности важен сам по себе и играет решающую роль в защите компьютерных систем, сетей и конфиденциальной информации от несанкционированного доступа и угроз. Для обеспечения полной защиты организациям необходимо реализовать комплексную стратегию безопасности, включающую все эти виды безопасности. Кроме того, важно отметить, что безопасность — это непрерывный процесс, поэтому регулярный мониторинг, тестирование и обновление средств контроля безопасности необходимы, для того чтобы они оставались эффективными при защите активов организации.

Важность управления рисками

Управление рисками — значимый аспект компьютерной безопасности. Оно включает в себя *выявление*, *оценку* и *определение приоритетов* потенциальных рисков безопасности для организации, а также *принятие мер* по их смягчению или устранению.

Одной из основных причин важности управления рисками является то, что оно позволяет организациям сосредоточить усилия по обеспечению безопасности в наиболее важных для них областях. Выявляя и оценивая потенциальные риски, организации могут определить, какие из них наиболее вероятны и какие будут иметь наибольшие последствия в случае возникновения. Это позволяет им определить приоритетность своих усилий по обеспечению безопасности и направить ресурсы в наиболее важные сферы.

Управление рисками также помогает организациям быть проактивными в своем подходе к безопасности. Организации, управляющие рисками, способны не только ждать, пока произойдет инцидент безопасности, а затем реагировать на него, но и предвидеть потенциальные проблемы безопасности и предпринимать шаги для их предотвращения.

Для оценки рисков и управления ими используются различные методы, такие как моделирование угроз и оценка уязвимостей. *Моделирование угроз* — это процесс, который помогает организациям определить и понять потенциальные угрозы для их систем, приложений и данных. Сначала устанавливают активы, которые необходимо защитить, затем выявляют то, что может им угрожать, и оценивают вероятность и влияние каждой угрозы.

Оценка уязвимостей — это процесс нахождения и оценки слабых мест в системах и сетях организации. Сюда входит выявление прорех в системе безопасности организации, таких как отсутствующие исправления или неправильно настроенные системы, и оценка их возможного влияния.

Организациям важно регулярно пересматривать свои стратегии и процессы в этой области, чтобы убедиться, что они позволяют эффективно управлять рисками для своих систем и данных.

Роль стандартов и лучших практик

Следование отраслевым стандартам и передовой практике в области компьютерной безопасности — важный аспект поддержания безопасной среды. Стандарты и передовая практика представляют собой основу деятельности организаций, гарантирующей, что в них внедрены необходимые средства контроля для защиты своих систем и данных.

Одним из основных преимуществ соблюдения стандартов и следования передовым практикам является то, что они обеспечивают общий язык и единое

понимание средств и методов контроля безопасности. Это позволяет организациям эффективно общаться друг с другом и со сторонними поставщиками о применяемых мерах безопасности.

Стандарты являются для организаций эталоном, по которому они могут оценивать собственные меры безопасности. Это позволяет им определить области, в которых необходимо совершенствоваться, и сравнить собственные меры безопасности с мерами других организаций.

К наиболее широко используемым стандартам безопасности относятся ISO 27001 — международный стандарт по управлению информационной безопасностью и NIST 800-53 — стандарт, опубликованный Национальным институтом стандартов и технологий (NIST) и содержащий рекомендации по обеспечению безопасности федеральных информационных систем.

Помимо стандартов существует также ряд лучших практик, которым организации могут следовать для повышения уровня безопасности. К ним относятся регулярные тренинги по безопасности для сотрудников, внедрение политики надежных паролей, регулярное исправление и обновление систем и программного обеспечения.

Организациям необходимо внедрять средства контроля безопасности, соответствующие отраслевым стандартам и передовой практике, чтобы защитить свои системы и данные от угроз. Кроме того, важно быть в курсе последних стандартов безопасности и передовой практики, поскольку ландшафт угроз постоянно меняется и для борьбы с новыми угрозами разрабатываются новые стандарты и практики.

Важность реагирования на инциденты

Реагирование на инциденты — важнейший аспект компьютерной безопасности. Под ним понимаются действия, которые предпринимает организация, когда подозревает или подтверждает, что произошел инцидент безопасности. Цель реагирования на инцидент — минимизировать нанесенный им ущерб, как можно быстрее восстановить нормальную работу и извлечь уроки из сложившейся ситуации, чтобы предотвратить подобное в будущем.

О важности реагирования на инциденты безопасности можно судить по тому, что даже самые эффективные превентивные меры не гарантируют, что проблемы не возникнут. Организации должны быть готовы своевременно и эффективно реагировать на инциденты, чтобы минимизировать нанесенный ими ущерб.

Эффективное реагирование на инциденты требует наличия четко разработанного *плана реагирования*, в котором указаны роли и обязанности лиц, занятых в устранении инцидентов, процедуры, которым необходимо следовать, и используемые при этом протоколы связи. План должен включать процедуры

обнаружения, локализации и ликвидации инцидента, а также восстановления после него.

Группы реагирования на инциденты должны быть обучены и оснащены для работы с широким спектром проблем, включая вспышки активности вредоносного ПО, несанкционированный доступ и стихийные бедствия. Они также должны иметь необходимые инструменты и оборудование для реагирования на инциденты, например инструменты для криминалистики и системы резервного копирования.

Еще одним важным аспектом реагирования на инциденты является способность извлекать из них уроки и вносить улучшения в систему безопасности организации. Сюда входят анализ инцидента для определения причины и масштабов ущерба, а также выявление областей, в которых можно усилить контроль безопасности организации.

Даже принятие самых эффективных превентивных мер не способно застраховать от возникновения инцидентов безопасности, поэтому организации должны быть готовы своевременно и результативно реагировать на них. Это позволяет минимизировать ущерб, нанесенный инцидентом, как можно быстрее восстановить нормальную работу и извлечь уроки, чтобы предотвратить подобное в будущем.

Роль сторонних поставщиков услуг безопасности

Многие организации полагаются на сторонних поставщиков услуг безопасности, которые помогают им защитить свои системы и данные от угроз. Эти поставщики предлагают широкий спектр услуг, включая консультирование по вопросам безопасности, анализ угроз, управление уязвимостями и реагирование на инциденты.

Одним из основных преимуществ обращения к сторонним поставщикам услуг безопасности является то, что они могут привнести в организацию такой уровень знаний и опыта, которого сложно достичь собственными силами. Например, консалтинговые фирмы по вопросам безопасности могут дать рекомендации по реализации комплексной программы безопасности, включая выявление потенциальных угроз, оценку уязвимостей и внедрение средств контроля для снижения рисков.

Поставщики данных об угрозах могут помочь организациям оставаться в курсе последних угроз, предоставляя в режиме реального времени информацию о новых уязвимостях и вредоносных программах. Это может помочь организациям быстро выявлять потенциальные угрозы и реагировать на них до того, как они смогут нанести значительный ущерб.

Поставщики услуг по управлению уязвимостями могут помочь организациям выявить и устранить уязвимости в их системах и сетях. Сюда могут входить

регулярное сканирование уязвимостей, тестирование на проникновение и оценка рисков.

Поставщики услуг по реагированию на инциденты могут помочь организациям в случае возникновения проблем с безопасностью, предоставив экспертные знания и ресурсы для локализации инцидента, восстановления после него и извлечения уроков из ситуации.

Еще один важный аспект привлечения сторонних поставщиков услуг безопасности заключается в том, что они могут помочь организациям соответствовать отраслевым нормам и стандартам. Многие организации обязаны соблюдать такие нормы, как HIPAA, PCI DSS и SOX, которые содержат особые требования к безопасности. Сторонние поставщики услуг безопасности могут помочь организациям в этом, оценивая безопасность, выполняя тестирование на проникновение и оказывая другие услуги. Однако организациям важно тщательно оценить и выбрать подходящего поставщика услуг безопасности, соответствующего конкретным потребностям и бюджету, а также иметь четкое представление об объеме и ограничениях предоставляемых им услуг.

Эволюция компьютерной безопасности

Первые дни компьютерной безопасности

Первые дни компьютерной безопасности можно отнести к 1950–1960-м годам, когда компьютеры впервые стали использоваться правительственными структурами и бизнесом. В то время основной задачей была защита конфиденциальных сведений, таких как секретные правительственные документы и служебная информация. Основное внимание уделялось физической безопасности, например защите компьютерной комнаты от несанкционированного доступа и ограничению числа людей, имеющих доступ к компьютеру.

Одно из первых задокументированных нарушений компьютерной безопасности произошло в 1963 году, когда компьютер в Массачусетском технологическом институте (MIT) был использован для совершения междугородных телефонных звонков без разрешения. Этот инцидент привел к разработке первой системы компьютерной безопасности, названной Compatible Time-Sharing System (CTSS), в которой были реализованы такие меры безопасности, как аутентификация пользователей и разрешения на применение файлов.

В 1970–1980-х годах, когда компьютеры стали использоваться более широко, акцент в компьютерной безопасности сместился на защиту компьютерных сетей. Развитие интернета в 1980-х годах создало новые возможности для хакеров получить несанкционированный доступ к компьютерным системам и привело к появлению новых угроз безопасности, таких как вирусы и черви. В это время за компьютерную безопасность отвечал в основном ИТ-отдел,

а особых специалистов по безопасности было немного. Область компьютерной безопасности все еще находилась в зачаточном состоянии, и существовало мало стандартов или лучших практик.

На заре компьютерной безопасности основной задачей была защита конфиденциальной информации, и основное внимание уделялось физической безопасности. Первые системы компьютерной безопасности были разработаны в 1960-х годах для защиты от несанкционированного доступа, но по мере роста использования компьютеров и сетей росла и потребность в более совершенных мерах безопасности для защиты от новых видов угроз.

Рост числа киберугроз

Увеличение количества киберугроз можно проследить с первых дней существования компьютерных сетей и интернета. По мере того как компьютеры становились все более тесно связанными между собой, у киберпреступников появлялись возможности для получения несанкционированного доступа к компьютерным системам.

Одной из первых широко распространенных киберугроз стал червь Морриса, который в 1988 году поразил тысячи компьютерных систем и продемонстрировал уязвимость компьютерных сетей для вредоносных программ. За этим последовало появление вирусов, которые могли быстро распространяться через электронную почту и другие формы электронной коммуникации.

По мере роста популярности интернета в 1990–2000-х годах киберугрозы продолжали развиваться и становились все более изощренными. Хакеры начали атаковать веб-сайты и веб-приложения, что привело к появлению новых типов угроз, таких как межсайтовый скриптинг (Cross-Site Scripting, XSS) и атаки с использованием SQL-инъекций.

С развитием социальных сетей киберпреступники начали применять тактику социальной инженерии, чтобы обманом заставить пользователей предоставить личную информацию или перейти по вредоносным ссылкам. Все более распространенными стали фишинговые атаки, когда хакеры рассылают электронные письма или сообщения, выдавая себя за надежный источник, чтобы украсть личную информацию или учетные данные для входа в систему. Кроме того, появление мобильных устройств и интернета вещей привело к росту количества новых типов угроз, таких как мобильные вредоносные программы и IoT-атаки.

Рост индустрии безопасности

Рост индустрии безопасности можно рассматривать как ответ на увеличение числа и изощренности киберугроз. По мере расширения использования компьютеров и сетей возникла необходимость в более совершенных мерах безопасности

для защиты от новых видов угроз. Это привело к появлению новой отрасли, ориентированной на обеспечение компьютерной безопасности.

Индустрия безопасности начала формироваться в 1990-х годах с появлением антивирусного программного обеспечения и брандмауэров, которые были предназначены для защиты компьютерных систем от вирусов и несанкционированного доступа. Индустрия безопасности реагировала на рост популярности интернета, разрабатывая новые продукты и услуги для защиты от веб-угроз, таких как межсайтовый скриптинг (XSS) и атаки SQL-инъекций.

В 2000-х годах индустрия безопасности продолжала развиваться, появлялись новые продукты и услуги, такие как системы обнаружения и предотвращения вторжений (intrusion detection and prevention systems, IDPS), системы управления информацией и событиями безопасности (security information and event management, SIEM) и платформы аналитики безопасности. Рост количества облачных вычислений и мобильных устройств привел к разработке новых продуктов и услуг безопасности, предназначенных именно для этих технологий.

Кроме того, индустрия безопасности разрастается и включает в себя широкий спектр услуг в области безопасности, таких как тестирование на проникновение, управление уязвимостями, реагирование на инциденты и консультирование по вопросам соответствия. Это позволяет организациям передавать обеспечение части или всех своих потребностей в области безопасности на откуп экспертам по безопасности. К тому же к индустрии безопасности теперь относится широкий спектр сертификатов безопасности и стандартов соответствия, таких как ISO 27001, SOC 2 и PCI DSS, которые помогают организациям обеспечить безопасность своих систем и данных.

Современное состояние компьютерной безопасности

Нынешнее состояние компьютерной безопасности непростое и постоянно меняющееся, поскольку продолжают появляться новые технологии и угрозы. Киберугрозы становятся все более сложными и разнообразными, и организации должны применять многосторонний подход к своей защите.

Один из основных аспектов современного состояния компьютерной безопасности — растущая угроза кибератак. Хакеры и киберпреступники используют различные тактики для получения несанкционированного доступа к компьютерным системам и кражи конфиденциальной информации. К ним относятся *фишинг*, *вредоносные программы*, *программы-вымогатели* и *современные постоянные угрозы (APT)*.

Еще одним важным аспектом является растущее использование облачных вычислений и мобильных устройств. По мере того как все больше организаций переносят свои данные и приложения в облако, а сотрудники применяют мобильные устройства для доступа к данным компании, поверхность атаки для

киберпреступников расширяется. Это привело к разработке новых продуктов и услуг безопасности, специально предназначенных для облачных и мобильных сред.

Кроме того, в современном состоянии компьютерной безопасности все большее внимание уделяется соблюдению нормативных требований. Организации должны соответствовать различным нормам, таким как GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act) и PCI DSS (Payment Card Industry Data Security Standard), которые содержат конкретные требования к защите конфиденциальных данных.

Современное состояние компьютерной безопасности включает в себя все более широкое использование искусственного интеллекта и машинного обучения (ИИ и МО) для повышения безопасности. ИИ и МО применяются для обнаружения киберугроз и реагирования на них в режиме реального времени, автоматизации задач безопасности и улучшения общего уровня безопасности.

Тенденции и будущие разработки в области компьютерной безопасности

Тенденции и будущие разработки в области компьютерной безопасности направлены на устранение все более сложных и разнообразных киберугроз, с которыми сталкиваются организации. Перечислим некоторые из этих тенденций.

- *Квантовые вычисления*. С их появлением традиционные методы шифрования станут неактуальными. Это связано с тем, что квантовые компьютеры могут легко взломать существующие методы шифрования. Поэтому разработка методов шифрования, устойчивых к квантовым вычислениям, — это приоритетная задача для будущего компьютерной безопасности.
- *Искусственный интеллект и машинное обучение*. По мере совершенствования технологии ИИ/МО будут использоваться для повышения уровня кибербезопасности за счет автоматизации задач безопасности, обнаружения угроз и реагирования на них в режиме реального времени, а также повышения общего уровня безопасности.
- *Безопасность интернета вещей*. По мере того как все больше устройств подключается к интернету, расширяется поверхность атаки для киберпреступников. Безопасность IoT — это новая область, которая направлена на защиту этих устройств от кибератак.
- *Технология блокчейна*. Все чаще используется для защиты данных и транзакций. Она обеспечивает неизменную и прозрачную запись всех транзакций, затрудняя злоумышленникам подделку данных или мошеннические действия.
- *Облачная безопасность*. По мере того как все больше организаций переносят свои данные и приложения в облако, потребность в решениях по обеспечению