***Сергали Аяулым***

*студент, Алматинский Технологический Университет*

***Букенова Индира Нурмуханбетовна***

*преподаватель, магистр технических наук, Алматинский Технологический Университет*

*Казахстан, г.Алматы*

***Төлеушова Айнур Төлендіқызы***

*Преподаватель,Алматинский Технологический Университет*

*Казахстан, г.Алматы*

**Кибербезопасность**

Аннотация: Статья направлен на изучение основ кибербезопасности, как раздела информационной безопасности, посвященного защите данных, представленных в цифровой форме.

Ключевые слова: Кибербезопасность, IT, киберпреступники, интернет, кибератака, програмное обеспечение, информационная безопасность.

Annotation: The article is aimed at studying the basics of cybersecurity, as a section of open security dedicated to the protection of data presented in digital forms, Information Security.

Key words: Cybersecurity, IT, cybercriminals, internet, cyberattack, software.

Введение: Кибербезопасность является наиболее важным вопросом, так как киберугрозы и атаки разрастаются. Злоумышленники теперь используют более сложные методы для нацеливания на системы. Люди, малый бизнес или крупная организация, подвергаются их воздействию. Таким образом, все эти фирмы, будь то ИТ или не ИТ-компании, осознали важность кибербезопасности и сосредоточились на принятии всех возможных мер для борьбы с киберугрозами.



**Что такое кибербезопасность?**

Кибербезопасность — это практика защиты критически важных систем и конфиденциальной информации от цифровых атак. Меры кибербезопасности, также известные как безопасность информационных технологий (ИТ), предназначены для борьбы с угрозами для сетевых систем и приложений, независимо от того, исходят ли эти угрозы изнутри или снаружи организации.

В 2020 году средняя стоимость утечки данных составила 3,86 млн долларов США во всем мире и 8,64 млн долларов США в США. Эти расходы включают расходы на обнаружение и реагирование на нарушение, стоимость простоя и упущенную выгоду, а также долгосрочный ущерб репутации бизнеса и его бренда. Киберпреступники нацеливаются на личную информацию клиентов — имена, адреса, национальные идентификационные номера (например, номер социального страхования в США, фискальные коды в Италии) и информацию о кредитной карте — и затем продают эти записи на подпольных цифровых рынках. Компрометация PII часто приводит к потере доверия клиентов, наложению штрафов со стороны регулирующих органов и даже к судебным искам. Сложность системы безопасности, созданная разрозненными технологиями и отсутствием собственного опыта, может увеличить эти затраты. Но организации с комплексной стратегией кибербезопасности, основанной на передовом опыте и автоматизированной с использованием передовой аналитики, искусственного интеллекта (ИИ) и машинного обучения, могут более эффективно бороться с киберугрозами и сокращать жизненный цикл и последствия взломов, когда они происходят.

**История кибербезопасности**

Кибербезопасность приобретает все большее значение из-за растущей зависимости от компьютерных систем, Интернета и стандартов беспроводной сети, таких как Bluetooth и Wi-Fi, а также из-за роста количества интеллектуальных устройств и различных устройств, составляющих «Интернет вещей».

Из-за своей сложности, как с точки зрения политики, так и технологий, кибербезопасность также является одной из основных проблем в современном мире. С чего все началось? Мы рассмотрим историю кибербезопасности от зарождения до наших дней.

1970-е: ARAPNET и Creeper

Кибербезопасность зародилась в 1970-х годах, когда исследователь Боб Томас создал компьютерную программу под названием Creeper, которая могла перемещаться по сети ARPANET, оставляя след, куда бы она ни пошла. Рэй Томлинсон, изобретатель электронной почты, написал программу Reaper, которая преследовала и удаляла Creeper. Reaper был самым первым образцом антивирусного программного обеспечения и первой самовоспроизводящейся программой, что сделало его первым компьютерным червем.

1980-е: рождение коммерческого антивируса

1987 год стал годом рождения коммерческого антивируса, хотя были и конкурирующие претензии на новатора первого антивирусного продукта. Андреас Люнинг и Кай Фигге выпустили свой первый антивирусный продукт для Atari ST, на котором также был выпущен Ultimate Virus Killer в 1987 году. Три чехословака создали первую версию антивируса NOD в том же году, а в США Джон Макафи основал McAfee. и выпустил VirusScan.

1990-е: мир переходит в онлайн

Когда Интернет стал общедоступным, все больше людей начали размещать свою личную информацию в Интернете. Организованная преступность увидела в этом потенциальный источник дохода и начала красть данные у людей и правительств через Интернет. К середине 1990-х угроз сетевой безопасности возросло в геометрической прогрессии, и для защиты населения пришлось массово выпускать брандмауэры и антивирусные программы.

2000-е: Угрозы диверсифицируются и множатся

В начале 2000-х годов преступные организации начали активно финансировать профессиональные кибератаки, а правительства начали пресекать преступность хакерских атак, вынося виновным гораздо более суровые приговоры. Информационная безопасность продолжала развиваться по мере роста Интернета, но, к сожалению, вирусы тоже.

2021: Следующее поколение

Индустрия кибербезопасности продолжает расти со скоростью света. По прогнозам Statista, к 2026 году объем мирового рынка кибербезопасности вырастет до 345,4 млрд долларов. Программа-вымогатель — одна из наиболее распространенных угроз безопасности данных любой организации, и, по прогнозам, ее число будет расти.

**Домены кибербезопасности**

Сильная стратегия кибербезопасности включает уровни защиты от киберпреступлений, включая кибератаки, которые пытаются получить доступ, изменить или уничтожить данные; вымогать деньги у пользователей или организации; или стремиться нарушить нормальную деловую деятельность. Контрмеры должны быть направлены на:

Безопасность критической инфраструктуры — методы защиты компьютерных систем, сетей и других активов, от которых зависит национальная безопасность, экономическое благополучие и/или общественная безопасность. Национальный институт стандартов и технологий (NIST) создал структуру кибербезопасности, чтобы помочь организациям в этой области, а Министерство внутренней безопасности США (DHS) предоставляет дополнительные рекомендации.

Сетевая безопасность — меры безопасности для защиты компьютерной сети от злоумышленников, включая как проводные, так и беспроводные (Wi-Fi) соединения.

Безопасность приложений — процессы, помогающие защитить приложения, работающие локально и в облаке. Безопасность должна быть встроена в приложения на этапе проектирования с учетом того, как обрабатываются данные, аутентификация пользователей и т. д.

Облачная безопасность — в частности, настоящие конфиденциальные вычисления, которые шифруют облачные данные в состоянии покоя (в хранилище), в движении (по мере их перемещения в облако, из него и внутри облака) и при использовании (во время обработки) для обеспечения конфиденциальности клиентов, бизнес-требований и соблюдения нормативных требований. стандарты.

Информационная безопасность. Меры по защите данных, такие как Общий регламент по защите данных или GDPR, которые защищают ваши самые конфиденциальные данные от несанкционированного доступа, раскрытия или кражи.

Обучение конечных пользователей. Повышение осведомленности о безопасности в организации для повышения безопасности конечных точек. Например, пользователей можно научить удалять подозрительные вложения электронной почты, избегать использования неизвестных USB-устройств и т. д.

Планирование аварийного восстановления/непрерывности бизнеса — инструменты и процедуры для реагирования на незапланированные события, такие как стихийные бедствия, перебои в подаче электроэнергии или инциденты кибербезопасности, с минимальным нарушением основных операций.

Безопасность хранения — IBM FlashSystem® обеспечивает надежную устойчивость данных с многочисленными мерами безопасности. Это включает в себя шифрование и неизменяемые и изолированные копии данных. Они остаются в одном пуле, поэтому их можно быстро восстановить для поддержки восстановления, сводя к минимуму воздействие кибератаки.

Мобильная безопасность — IBM Security MaaS360 с Watson позволяет управлять мобильными сотрудниками и обеспечивать их безопасность с помощью безопасности приложений, контейнерных приложений и защищенной мобильной почты.

**Опасные мифы о кибербезопасности**

Объем инцидентов кибербезопасности растет во всем мире, но неправильные представления продолжают сохраняться, в том числе представление о том, что:

Киберпреступники — аутсайдеры. На самом деле нарушения кибербезопасности часто являются результатом злонамеренных инсайдеров, работающих на себя или в сотрудничестве с внешними хакерами. Эти инсайдеры могут быть частью хорошо организованных групп, поддерживаемых национальными государствами.

Риски хорошо известны. На самом деле поверхность риска по-прежнему расширяется: сообщают о тысячах новых уязвимостей в старых и новых приложениях и устройствах. А возможности для человеческих ошибок — особенно со стороны небрежных сотрудников или подрядчиков, которые непреднамеренно вызывают утечку данных — продолжают расти.

Векторы атаки сдерживаются. Киберпреступники постоянно находят новые векторы атак, включая системы Linux, операционные технологии (OT), устройства Интернета вещей (IoT) и облачные среды.

Моя отрасль в безопасности. Каждая отрасль имеет свою долю рисков кибербезопасности, при этом киберпреступники используют потребности коммуникационных сетей почти в каждой государственной и частной организации. Например, атаки программ-вымогателей (см. ниже) нацелены на больше секторов, чем когда-либо, включая местные органы власти и некоммерческие организации, а также увеличились угрозы для цепочек поставок, веб-сайтов «.gov» и критической инфраструктуры.

Несмотря на то, что специалисты по кибербезопасности прилагают все усилия, чтобы устранить бреши в системе безопасности, злоумышленники всегда ищут новые способы избежать внимания ИТ-отдела, уклониться от мер защиты и использовать возникающие уязвимости. Последние угрозы кибербезопасности придают новый смысл «известным» угрозам, используя преимущества удаленной работы, инструменты удаленного доступа и новые облачные сервисы.



**Вредоносное ПО**

Термин «вредоносное ПО» относится к вариантам вредоносного программного обеспечения, таким как черви, вирусы, трояны и программы-шпионы, которые обеспечивают несанкционированный доступ или наносят ущерб компьютеру. Атаки вредоносного ПО становятся все более «безфайловыми» и предназначены для обхода привычных методов обнаружения, таких как антивирусные инструменты, которые сканируют вредоносные вложенные файлы.

**Программы-вымогатели**

Программа-вымогатель — это тип вредоносного ПО, которое блокирует файлы, данные или системы и угрожает стереть или уничтожить данные, либо сделать личные или конфиденциальные данные общедоступными, если киберпреступникам, запустившим атаку, не будет выплачен выкуп. Недавние атаки программ-вымогателей были нацелены на правительства штатов и местные органы власти, которые легче взломать, чем организации и вынуждены платить выкуп, чтобы восстановить приложения и веб-сайты, на которые полагаются граждане

**Фишинг/социальная инженерия**

Фишинг — это форма социальной инженерии, которая обманом заставляет пользователей предоставлять свои собственные персональные данные или конфиденциальную информацию. При фишинге электронные письма или текстовые сообщения кажутся отправленными законной компанией с просьбой предоставить конфиденциальную информацию, такую ​​как данные кредитной карты или данные для входа в систему. ФБР отметило всплеск фишинга, связанного с пандемией, связанный с ростом удаленной работы.



**Внутренние угрозы**

Нынешние или бывшие сотрудники, деловые партнеры, подрядчики или любой, кто имел доступ к системам или сетям в прошлом, может считаться внутренней угрозой, если они злоупотребляют своими разрешениями на доступ. Внутренние угрозы могут быть невидимы для традиционных решений безопасности, таких как брандмауэры и системы обнаружения вторжений, которые фокусируются на внешних угрозах.

**Распределенные атаки типа «отказ в обслуживании» (DDoS)**

DDoS-атака пытается вывести из строя сервер, веб-сайт или сеть, перегружая их трафиком, обычно из нескольких скоординированных систем. DDoS-атаки перегружают корпоративные сети через простой протокол управления сетью (SNMP), используемый для модемов, принтеров, коммутаторов, маршрутизаторов и серверов.

**Расширенные постоянные угрозы (APT)**

В APT злоумышленник или группа злоумышленников проникают в систему и остаются незамеченными в течение длительного периода времени. Злоумышленник оставляет сети и системы нетронутыми, чтобы злоумышленник мог следить за деловой активностью и похищать конфиденциальные данные, избегая при этом активации защитных мер противодействия. Примером APT является недавний взлом Solar Winds государственных систем США.

**Атаки «человек посередине»**

«Человек посередине» — это атака с прослушиванием, при которой киберпреступник перехватывает и передает сообщения между двумя сторонами с целью кражи данных. Например, в незащищенной сети Wi-Fi злоумышленник может перехватить данные, передаваемые между гостевым устройством и сетью.

**Ключевые технологии кибербезопасности и лучшие практики**

Следующие передовые методы и технологии могут помочь вашей организации внедрить надежную кибербезопасность, которая снизит вашу уязвимость к кибератакам и защитит ваши критически важные информационные системы, не влияя на работу пользователей или клиентов.



Управление идентификацией и доступом (IAM) определяет роли и привилегии доступа для каждого пользователя, а также условия, при которых им предоставляются или отменяются их привилегии. Методологии IAM включают единую регистрацию, которая позволяет пользователю войти в сеть один раз без повторного ввода учетных данных в течение одного и того же сеанса; многофакторная аутентификация, требующая двух или более учетных данных для доступа; учетные записи привилегированных пользователей, которые предоставляют административные привилегии только определенным пользователям; и управление жизненным циклом пользователя, которое управляет идентификацией каждого пользователя и привилегиями доступа от первоначальной регистрации до выхода на пенсию. Инструменты IAM также могут дать вашим специалистам по кибербезопасности более полное представление о подозрительной активности на устройствах конечных пользователей, включая конечные точки, к которым они не могут получить физический доступ. Это помогает ускорить расследование и время реагирования, чтобы изолировать и сдержать ущерб от нарушения.

Комплексная платформа безопасности данных защищает конфиденциальную информацию в нескольких средах, включая гибридные многооблачные среды. Лучшие платформы для обеспечения безопасности данных обеспечивают автоматизированный обзор уязвимостей данных в режиме реального времени, а также постоянный мониторинг, который предупреждает их об уязвимостях данных и рисках до того, как они станут утечкой данных; они также должны упростить соблюдение государственных и отраслевых правил конфиденциальности данных. Резервное копирование и шифрование также жизненно важны для обеспечения безопасности данных.

se

**ЗАКЛЮЧЕНИЕ**

Вместо того чтобы ждать атаки или нарушения, организации разрабатывают способы предотвращения угроз и устранения возможностей до того, как атаки могут произойти. Лучший способ защитить себя, поскольку технология продолжает развиваться быстрыми темпами, — это использовать антивирусное программное обеспечение с хорошим рейтингом. Внимательно следить за тем, где вы ею делитесь, и делайте разумный выбор в отношении ссылок, по которым вы щелкаете, и файлов, которые вы скачиваете с Интернета.

<https://4brain.ru/blog/kiberbezopasnost-chto-sdelat-chtoby-zashchitit-svoi-personalnye-dannye-ot-prestupnikov/>

<https://keypro2.ru/the-history-of-cyber-security/>

<https://itsecforu.ru/2019/02/26/введение-в-основы-кибербезопасности/>

<https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security>

<https://experience.dropbox.com/ru-ru/resources/cyber-security>