УДК 004.056

СТАТИСТИКА КИБЕРАТАК И ИХ ВЛИЯНИЕ НА БИЗНЕС

Салова Т.Л.

кандидат технических наук, доцент,

кафедра Информационных технологий и математики,

Сочинский государственный университет,

Сочи, Россия

Ахметчин В.Р.

магистрант,

Сочинский государственный университет,

Сочи, Россия

Аннотация: В статье рассматриваются наиболее важные статистические данные: факты, цифры и тенденции в области кибербезопасности бизнеса. Перечисляются отрасли, наиболее уязвимые для кибератак, а также приводятся практические советы по усилению кибербезопасности бизнеса.

Ключевые слова: информационные технологии, статистика, кибератаки, кибербезопасность, киберпреступность, утечки информации.

CYBERATTACK STATISTICS AND THEIR IMPACT ON BUSINESS

Salova T.L.

Candidate of Technical Sciences, Associate Professor,

Department of Information Technologies and Mathematics,

Sochi State University,

Sochi, Russia

Akhmetchin V.R.

undergraduate,

Sochi State University,

Sochi, Russia

Abstract: The article discusses the most important statistical data facts, figures and trends in the field of business cybersecurity. The industries that are most vulnerable to cyberattacks are listed, as well as practical tips on strengthening business cybersecurity.
Keywords: information technology, statistics, cyberattacks, cybersecurity, cybercrime, information leaks.

Пандемия затронула все виды бизнеса - как крупные, так и малые. Она усилила киберпреступность из-за неопределенности в отношении удаленной работы и способов защиты бизнеса. В результате пандемии COVID-19 киберпреступность, которая включает в себя все - от кражи или хищения до уничтожения данных, выросла на 600%. Почти каждая отрасль вынуждена была внедрять новые решения, и это заставило компании быстро адаптироваться.

По прогнозам в 2025 году киберпреступность будет обходиться компаниям по всему миру в 10,5 триллионов долларов в год, по сравнению с 3 триллионами долларов в 2015 году [2]. По данным Cybersecurity Ventures [3], киберпреступность представляет собой крупнейшую в истории утечку экономического капитала, темпы роста которого составляют 15 процентов в год.

Кибератаки на все предприятия, но особенно на малый и средний бизнес, становятся все более частыми, целенаправленными и сложными. Согласно исследованию компании Accenture «Стоимость киберпреступлений» - 43% кибератак направлены на малые предприятия, но только 14% из них способны обеспечить свою защиту.

Кибератаки не только нарушают нормальную работу, но и могут нанести ущерб важным ИТ-активам и инфраструктуре, восстановить которые без достаточного бюджета или ресурсов будет невозможно. Из-за этого малые предприятия испытывают трудности с защитой. Отчет Ponemon Institute's State of Cybersecurity Report, описывает опыт малого и среднего бизнеса связанный с недавнем опытом кибератак:

– 45% утверждают, что их процессы неэффективны для смягчения последствий атак;

– 66% сталкивались с кибератаками за последние 12 месяцев;

– 69% утверждают, что кибер-атаки становятся все более целенаправленными.

Наиболее распространенные типы атак на малые предприятия включают:

– фишинг/социальная инженерия: 57%;

– скомпрометированные/ украденные устройства: 33%;

– кража учетных записей: 30%.

Долгосрочные издержки, связанные с утечкой данных, могут растянуться на месяцы и годы и включать значительные расходы, о которых компании не подозревают или не учитывают при планировании.

Эти затраты включают в себя потерю данных, перебои в работе бизнеса, потери доходов от простоя системы и даже ущерб репутации бренда.

Кибератаки могут повлиять на организацию различными способами - от незначительных сбоев в работе до крупных финансовых потерь. Независимо от типа кибератаки, каждое из последствий влечет за собой определенные затраты: денежные или иные.

Последствия инцидента, связанного с кибербезопасностью, могут сказаться на бизнесе спустя несколько недель, а то и месяцев. Ниже приведены пять областей, в которых может пострадать бизнес:

– финансовые потери;

– потеря производительности;

– ущерб репутации;

– юридическая ответственность;

– проблемы с бесперебойностью бизнеса.

Атаки с использованием Ransomware становятся все более распространенной проблемой. В конце 2016 года предприятие становилось

жертвой атаки Ransomware каждые 40 секунд. Согласно отчету компании Cybersecurity Ventures [3], к 2021 году этот показатель увеличится до 11 секунд. Ransomware – это вредоносное программное обеспечение, используемое для ограничения доступа к компьютерной системе или данным до тех пор, пока жертва не заплатит выкуп, требуемый преступником.

Некоторые отрасли более уязвимы для кибератак, чем другие, исключительно в силу характера их деятельности. Хотя утечка данных может произойти в любой отрасли, наибольшему риску подвержены предприятия, тесно связанные с повседневной жизнью людей.

Компании, хранящие конфиденциальные данные или личную информацию, являются распространенной мишенью для хакеров. К типам предприятий или организаций, наиболее уязвимых для кибератак, относятся:

– банки и финансовые учреждения: содержат информацию о банковских картах, счетах, личные данные клиентов;

– учреждения здравоохранения: хранят архивы медицинских записей, данные клинических исследований и данные о пациентах, такие как номера медицинского страхования;

– корпорации: имеет всесторонние данные, такие как концепции продуктов, интеллектуальная собственность, маркетинговые стратегии, базы данных клиентов и сотрудников, контрактные сделки, предложения клиентов и многое другое;

– вузы: хранят информацию о данных о зачислении, научных исследованиях, финансовых отчетах, а также личную информацию, идентифицирующую личность, такую как имена, адреса и информация о счетах;

Обнаружение утечки — это момент, когда компании или предприятию становится известно о том, что произошел инцидент. По данным IBM [1], компании требуется 197 дней для обнаружения бреши и до 69 дней для ее ликвидации.

Компании, которые устранили утечку информации менее чем за 30 дней, сэкономили более 1 млн. долл. по сравнению с теми, кому потребовалось более 30 дней. Медленное реагирование на утечку данных может привести к еще большим неприятностям для компании. Это может привести к потере доверия клиентов, снижению производительности или крупным штрафам.

План реагирования на утечку данных — это превентивный способ подготовиться на случай, если утечка все-таки произойдет. Наличие стратегии управления рисками для борьбы с такими инцидентами, как утечка данных, может минимизировать последствия для предприятия и его прибыли. План реагирования на происшествия, например, обеспечивает инструкции для команды на этапах обнаружения, локализации, расследования, устранения последствий и восстановления. Нельзя забывать и о персональной безопасности устройств каждого сотрудника, ведь несмотря на усиление мер защиты, количество атак на устройства личного пользования с каждым годом лишь увеличивается [5].

Согласно прогнозам, в течение пятилетнего периода с 2017 по 2021 год глобальные расходы на товары и услуги в области кибербезопасности в совокупности превысят 1 триллион долларов США. Это означает рост рынка кибербезопасности на 12-15% по сравнению с 2021 годом.

Учитывая растущие угрозы неправомерного использования данных хакерами, внедрение процессов для предотвращения нарушений безопасности данных является наиболее важным шагом после оформления надлежащего страхования от утечки данных.

Основными инструментами кибербезопасности являются:

1. Сокращение передачи данных.

Передача данных между рабочими и личными устройствами часто неизбежна в результате увеличения количества сотрудников, работающих удаленно. Хранение конфиденциальных данных на личных устройствах значительно повышает уязвимость к кибер-атакам.

2. Аккуратная загрузка.

Загрузка файлов из непроверенных источников может подвергнуть системы и устройства рискам безопасности. Важно загружать файлы только из источников и избегать ненужных загрузок, чтобы снизить восприимчивость устройства к вредоносным программам.

3. Повышение безопасности паролей.

Надежность пароля — это первая линия защиты от большинства атак. Использование строк символов, не имеющих смыслового значения, регулярная смена паролей, а также запрет записывать или передавать их - важнейший шаг к защите конфиденциальных данных.

4. Обновление программного обеспечения устройств.

Поставщики программного обеспечения прилагают все усилия для постоянного повышения безопасности своих программ, и регулярная установка последних обновлений сделает устройства менее уязвимыми для атак.

5. Мониторинг утечек данных.

Регулярный мониторинг данных и выявление существующих утечек поможет смягчить потенциальные последствия долгосрочной утечки данных [6]. Инструменты мониторинга утечек данных активно отслеживают и предупреждают о подозрительной активности [4].

6. Создание плана реагирования на утечку данных.

Утечки данных могут произойти даже с самыми осторожными и дисциплинированными компаниями. Создание официального плана по управлению потенциальными инцидентами, связанными с утечкой данных, основного плана реагирования на кибератаки и плана восстановления после кибератак поможет организациям любого размера реагировать на реальные атаки и сдерживать их потенциальный ущерб.

Очевидно, что предприятия находятся под постоянной угрозой киберпреступлений и должны принимать меры по защите своих данных. Как и

необходимость иметь адекватное страхование от риска кибер-атак, защита данных является важной частью защиты любого бизнеса.

Библиографический список

1. Cost of a data breach 2022 // IBM [Электронный ресурс]. — Режим доступа — URL: https://www.ibm.com/reports/data-breach (дата обращения: 24.04.2023).

2. Cybercrime To Cost The World $10.5 Trillion Annually By 2025 // GlobeNewswire [Электронный ресурс]. — Режим доступа — URL: https://www.globenewswire.com/news-release/2020/11/18/2129432/0/en/Cybercrime-To-Cost-The-World-10-5-Trillion-Annually-By-2025.html (дата обращения: 24.04.2023).

3. Global Ransomware Damage Costs Predicted To Exceed $5 Billion In 2017 // Cybercrime Magazine [Электронный ресурс]. — Режим доступа — URL: https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/ (дата обращения: 24.04.2023).

4. Аилимонов А.В., Осипов А.В., Плешакова Е.С, Гатауллин С.Т. Нейросетевые методы распознавания эмоций речи для противодействия мошенничеству в телекомукационных системах // Вопросы кибербезопасности. №6 (52). 2022. С. 83-92.

5. Безкоровайный М. М., Татузов А. Л. Кибербезопасность - подходы к определению понятия. // Вопросы кибербезопасности. №1. 2014. С. 22-27.

6. Найханова И.В. Основные этапы методики аудита системы менеджмента безопасности персональных данных. // Вопросы кибербезопасности. №4 (7). 2014. С. 55-59.

Оригинальность 86%