Когда связаны ОДНОЙ СЕТЬЮ

Как обеспечить информационную безопасность вашей компании

Организации все больше полагаются в своей деятельности на сетевую инфраструктуру. Ведь сетевая информация может содержать важные и конфиденциальные сведения: личные данные клиентов, финансовые отчеты, коммерческие и даже государственные тайны. Недостаточная их защита может привести к утечкам, мошенничеству и потере репутации. Нарушение работы сети в результате кибератаки может значительно повлиять на бизнес-процессы, стать причиной простоя и крупных финансовых потерь.

Во многих странах принимаются законы и стандарты, требующие от бизнеса адекватной защиты сетевой информации. При этом нарушение требований безопасности может привести к крупным штрафам и юридической ответственности. Поэтому владельцу бизнеса необходимо серьезно подойти к вопросу организации защиты информации в своей структуре, лично либо через своих менеджеров выстроить этот процесс.

ОТ ПРОСТОГО К СЛОЖНОМУ

Кажется очевидным, но персонал не всегда четко понимает, что надежные пароли – длинные, сложные, обновляемые. Если сотрудники не осознают серьезность последствий для компании и себя лично, они не станут усложнять свою работу и учитывать важные минимальные нормативы, поэтому их необходимо внедрять в работу, несмотря на кажущуюся очевидность.

Речь о таких вещах, как:

- рекомендуемая длина паролей (не менее 12 символов);
- использование комбинаций символов в паролях;
- отказ от использования предсказуемых сочетаний («password», «123456», «qwerty»);
- общеупотребимых словарных слов, которые подвержены атакам методом перебора словаря.

Как рядовой сотрудник, так и ТОП-менеджер должен понимать важность обеспечения уникальности пароля, недопу-

стимости использования личных данных, использования инструментов генерации и регулярного их обновления.

ПРАВИЛЬНАЯ ОРГАНИЗАЦИЯ РАБОТЫ С ДАННЫМИ

Владелец бизнеса должен организовать работу подразделений и, в частности, IT-отдела таким образом, чтобы работали следующие процессы:

1. Многофакторная аутентификация (МФА). Это метод защиты учетных записей и доступа к системам с использованием комбинации различных методов идентификации пользователя. В отличие от простой однофакторной аутентификации, которая основывается исключительно на имени пользователя и пароле, МФА подразумевает дополнительные уровни защиты, такие как одноразовый код или отпечаток пальца. Тем самым усложняется процесс аутентификации и повышается его надежность.

2. Обновление программного обеспечения.

3. Шифрование данных. Это особенно важно при работе с конфиденциальной информацией и передачей данных в открытых сетях.

4. Предотвращение вторжения.

5. Ограничение доступа. Является принципом информационной безопасности, заключающимся в предоставлении сотрудникам компании минимально необходимых прав доступа к ресурсам и конфиденциальной информации. Этот принцип основан на идее «привилегированного доступа», означающей, что пользователи могут получать доступ только к тому, что им действительно необходимо для выполнения своей работы.

ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОГРАНИЧЕНИЮ ДОСТУПА

1. Определение ролей пользователей. Устанавливайте различные уровни доступа в зависимости от ролей пользователей и функциональных обязанностей.

2. Контроль доступа. Обеспечивайте контроль доступа на уровне файлов, каталогов, баз данных и приложений. Сотрудники должны иметь доступ только к тому, что необходимо для выполнения рабочих обязанностей.

3. Введение привилегированных учетных записей. Привилегированные учетные записи предоставляются исключительно администраторам и техническому персоналу. Они используются только для выполнения основных задач в рамках повседневной работы.

4. Регулярный контроль доступа. Гарантирует, что назначенные права доступа соответствуют текущим потребностям.

ЧТО ДОЛЖЕН ЗНАТЬ, ПОНИМАТЬ И ДЕЛАТЬ ВАШ СОТРУДНИК

Обучение персонала должно начинаться с объяснения основных типов киберугроз и угроз безопасности. К таковым относятся фишинг, социальная инженерия, вредоносное ПО, DDoS-атаки и др. Сотрудники должны знать, что такие угрозы реальны и могут быть направлены как на организации, так и на отдельных лиц.

Именно фишинг и социальная инженерия являются распространенными методами атак, основанными на манипуляциях и обмане. Сотрудников следует обучить распознаванию подозрительных электронных писем, вредоносных ссылок, запросов паролей или других личных данных.

Персонал должен знать правила передачи конфиденциальной информации, особенно по электронной почте или другим электронным каналам.

Следует регулярно организовывать инструктажи о необходимости соблюдения осторожности при посещении ненадежных сайтов, загрузке файлов и открытии вложений электронной почты. Опасные сайты и вредоносные файлы могут стать источником заражения системы или кражи данных.

Обучение персонала должно включать инструкции о том, как реагировать на подозрительную деятельность или возможные инциденты безопасности. Пользователи должны знать, как сообщать о подозрительных событиях и куда обращаться за помощью в случае атаки.

Проверка осведомленности сотрудников поможет оценить уровень подготовки сотрудников и выявить области, требующие дополнительного обучения.

РЕЗЕРВНОЕ КОПИРОВАНИЕ ДАННЫХ

Резервное копирование данных представляет собой процесс создания копий важных данных с последующим хранением в безопасном и надежном месте. В случае чрезвычайной ситуации наличие резервных копий данных позволяет свести к минимуму время простоя и потери.

Резервное копирование обеспечивает защиту от потери данных в результате непредвиденных событий, таких как сбои оборудования, атаки вредоносных программ, стихийные бедствия, ошибки пользователей и др. Наличие резервной копии гарантирует возможность восстановления информации в случае возникновения таких ситуаций.

Резервные копии данных могут служить ключевым инструментом при восстановлении после кибератак, таких как шифрование данных (программы-вымогатели) или уничтожение данных злоумышленниками. Восстановление данных из резервных копий позволяет избежать уплаты выкупа или потери ценной информации.

Хранение резервных копий данных в облаке становится все более используемым вариантом. Облачное хранилище обеспечивает дополнительный уровень защиты, а также возможность доступа к данным из любой точки мира при наличии доступа в интернет.

Обеспечение регулярности резервного копирования данных имеет решающее значение для поддержания актуальности резервных копий. Автоматизация процедуры резервного копирования не только снижает риск ошибок, но также гарантирует бесперебойный и последовательный процесс.

Важное значение имеет периодическая проверка целостности данных в резервных копиях. Ведь поврежденные копии данных непригодны для восстановления.

Резервные копии данных должны храниться в безопасных местах, предотвращающих риск физических угроз безопасности, таких как кража или повреждение носителя.

Следует учитывать, что хранение резервных копий данных на том же устройстве, что и исходные данные, не обеспечивает полный уровень защиты. Лучше хранить резервные копии на отдельных носителях (внешние жесткие диски, облачное хранилище или сетевые сервера) и регулярно обновлять для поддержания в актуальном состоянии.

И НАПОСЛЕДОК – АУДИТ БЕЗОПАСНОСТИ

Это процесс систематического и всестороннего анализа всего механизма:

- сетевой инфраструктуры;
- программного обеспечения;
- политик и процедур безопасности с целью выявления уязвимостей и нарушений правил безопасности в вашей компании.

Лю Лимин (Liu Liming),
сотрудник Пекинского муниципального бюро общественной безопасности

Автор – гражданин КНР, специализируется в научных исследованиях по вопросам информационной и кибербезопасности, взаимодействует с местными партнерами и Китайско-Белорусским индустриальным парком «Великий камень».