Рекомендации beCloud по повышению кибербезопасности

1. Обеспечьте шифрование данных и SSL инспекцию

- Установите SSL-сертификаты для защиты передаваемых данных.
- Регулярно и вовремя передавайте SSL сертификаты провайдеру для последующей SSL инспекции и возможности на стороне провайдера выполнять ограничение к административным панелям сайта.

2. Используйте DNS хостинг-провайдера

- При размещении информационного ресурса используйте DNS-серверы, предоставленные хостинг-провайдером.

3. Усильте защиту учетных записей

- Используйте надежные пароли длиной от 12 символов с буквами, цифрами и специальными символами.
- Включите многофакторную аутентификацию (MFA) для всех критически важных систем и учетных записей.

4. Своевременно обновляйте программное обеспечение

- Регулярно устанавливайте обновления операционных систем, серверного программного обеспечения и бизнес-приложений, CMS и модулей.
- Используйте только проверенные источники обновлений, чтобы избежать внедрения вредоносного кода.

5. Внедрите надежное резервное копирование

- Автоматизируйте регулярное создание резервных копий данных.

6. Ограничьте доступ к административным панелям с вашей стороны

- Измените стандартные URL-адреса входа в административную панель сайта.
- Настройте доступ к важным системам или модулям сайта только с IP-адресов ответственных администраторов.

7. Обеспечьте дополнительную защиту информационных ресурсов

- WAF - это специальный инструмент, который обеспечивает безопасность вашего веб-приложения путем мониторинга и фильтрации входящего и исходящего трафика

8. Регулярно проверяйте безопасность информационных ресурсов

- Используйте сканеры уязвимостей для проверки веб-сайтов, серверов и сетей.

9. Применяйте принцип минимально необходимого доступа (Zerotrust)

- Ограничивайте права доступа сотрудников к данным и системам.
- Ведите журнал действий пользователей, чтобы отслеживать изменения и инциденты.
- Введите временной принцип доступа. Доступ только в рабочее время. При необходимости доступ разрешается при осуществлении определенной процедуры с последующим подтверждением ответственных руководителей

10. Обезопасьте базы данных

- Используйте сложные уникальные пароли и шифрование данных.
- Закройте внешние подключения и настройте защищенные соединения к базам данных.

11. Повышайте осведомленность сотрудников о кибербезопасности

- Организуйте обучение сотрудников по предотвращению фишинга и атак социальной инженерии.
- Разработайте и внедрите политику информационной безопасности в организации.
- Разделите рабочее и личное. Запретите использование рабочих устройств в личных целях.

12. Внедрите системы мониторинга угроз

- Используйте решения для обнаружения и анализа киберугроз в реальном времени.
- Настройте уведомления о подозрительной активности.
- Поставьте ваш ИР на мониторинг в центр кибербезопасности.

13. Используйте антивирусное ПО и фильтры безопасности

- Регулярно сканируйте корпоративные устройства на наличие вредоносных программ.
- Фильтруйте электронные письма и веб-контент для защиты от вирусов и атак.

14. Ограничьте попытки входа в систему

- Внедрите ограничения на количество неудачных попыток авторизации.
- Добавьте CAPTCHA на страницы входа и формы сбора данных.

15. Обеспечьте безопасность серверов и облачных ресурсов

- Используйте контейнеризацию (Docker, Kubernetes) для разделения сервисов.
- Следите за настройками CMS и конфигурациями безопасности серверов.

16. Защитите API и системы интеграции

- Применяйте аутентификацию и контроль доступа к API.
- Ограничьте число запросов, чтобы предотвратить атаки на системы.

17. Используйте VPN и безопасные соединения

- Не используйте открытые Wi-Fi-сети для работы с конфиденциальной информацией.

18. Удаляйте ненужные или устаревшие плагины и темы

- Удаляйте плагины и темы, которые не используются, так как они могут содержать уязвимости. Даже неактивные плагины могут быть уязвимыми для атак.

19. Логирование

- Включите логирование всех операций на сайте, включая попытки входа, изменения контента и установки новых плагинов.
- Регулярно анализируйте журналы для выявления аномальной активности.

20. Защита от SQL-инъекций

- Применяйте меры защиты от SQL-инъекций, например, через правильное использование подготовленных запросов и фильтрацию ввода.
- Обновляйте плагины и темы, которые могут быть уязвимы к таким атакам.

21. Используйте защиту от атак через XSS (межсайтовый скриптинг)

- Фильтруйте и экранируйте все пользовательские вводы, чтобы предотвратить внедрение вредоносного кода.
- Используйте защиту от XSS на всех формах на сайте.