ДОСТАТОЧНО ЛИ ЗАЩИЩЕН ВАШ КОРПОРАТИВНЫЙ ПОРТАЛ?

Согласно исследованию Group-IB 84% респондентов полностью или частично перешли на работу из дома в связи с объявленной пандемией. При этом, 71% опрошенных предоставил доступ сотрудникам к внутренним корпоративным системам и порталам, которые опубликованы в интернете. При несоблюдении должных правил информационной безопасности это может привести к проникновению злоумышленников в локальную сеть организации.

	Проверьте, насколько защищен ваш корпоративный портал	**Да**
1.	Используется защита от ботов — reCAPTCHA v3 (если корпоративный портал доступен в сети Интернет).	☐
2.	Используется межсетевой экран для защиты веб-приложений (WAF).	☐
3.	Используется решение для защиты от DDoS-атак (если корпоративный портал доступен в сети Интернет).	☐
4.	Применяются раздельные серверы для различных ролей - Front-End и Back-end или приложений.	☐
5.	Проведены внешний аудит или пентест в течение последних 6 месяцев.	☐
6.	Используется двухфакторная аутентификация (2FA) для доступа в личный кабинет.	☐
7.	Базы данных хранятся в зашифрованном виде, даже в состоянии покоя (Encryption at Rest).	☐
8.	Для доступа к порталу используется HTTPS SSL/TLS версии 1.3.	☐
9.	Используется система анализа поведенческого профиля (при авторизации учитывается индивидуальный профиль пользователя, единый для всех каналов взаимодействия с онлайн-ресурсом, и если профиль отличается, то система требует доп. подтверждение доступа).	☐
10.	Осуществляется мониторинг работоспособности оборудования и сервисов, отвечающих за работу портала с использованием автоматизированных сервисов (например Zabbix) с отслеживанием таких показателей как: диск, память, процессор, работоспособность служб веб-сервера.	☐

	Проверьте, насколько защищен ваш корпоративный портал	**Да**
11.	Логи доступа (access-logs) к порталу, также как системные логи и логи приложений веб-сервера, хранятся длительное время (например, 1 месяц) на отдельных носителях, и проводится их анализ в автоматическом режиме.	☐
12.	Веб-сервер запускается под отдельной учетной записью с ограниченными правами доступа (для предотвращения развития атаки в случае компрометации сервера).	☐
13.	Веб-сервер находится в отдельном сегменте сети (DMZ), не связанном с корпоративной сетевой инфраструктурой и корпоративными сервисами.	☐
14.	Для взаимодействия с БД используются хранимые процедуры, без прямых SQL-запросов.	☐
15.	Применяются сессионные и другие токены для защиты от replay и других видов атак (например, CSRF-токены).	☐
16.	Реализована политика резервного копирования баз данных и самого сайта: полный бэкап (например, еженедельно) и инкрементный бэкап (например, ежедневно).	☐
17.	Резервное копирование осуществляется по правилу 3-2-1 (3 резервные копии, на 2 разных носителях, при этом 1 из них отчуждаемый).	☐
18.	Существуют резервный сайт и план аварийного восстановления (Disaster Recovery Plan), который приводится в действие в случае недоступности основной площадки. План проверяется на регулярной основе (например, ежемесячно).	☐
	Посчитайте количество ответов «да»	____

Ваш результат

0-12 Корпоративный портал не защищен!

Упс, кажется вам нужно срочно пересмотреть политику и процедуры обеспечения безопасности. Рекомендуем обратиться к специалистам по информационной безопасности. Дополнительную информацию о том, как защитить ваш онлайн-ресурс можно получить на странице:

www.group-ib.ru/secure-portal.html

13-16 Корпоративный портал недостаточно защищен.

Но вы на правильном пути. Вы сделали уже много полезного, так держать! И всё же есть, что улучшить в вашей политике безопасности. Мы рекомендуем регулярно обмениваться опытом с коллегами из вашей индустрии. При необходимости свяжитесь с нами, и мы подскажем, к кому обратиться за дополнительной консультацией:

sp@group-ib.com

17-18 Корпоративный портал защищен.

Вы молодец! Вы хорошо разбираетесь в трендах современных угроз и понимаете процесс обеспечения информационной безопасности. Но не стоит расслабляться, злоумышленники постоянно находят новые способы проникновения в инфраструктуру. Следите за актуальной информацией на сайте Group-IB и на портале StayCyberSafe.