ЭЛЕКТРОННОЕ ОБЛАКО
https://cloudserver.ru

ОТЧЕТ

12.04.2019 Офис: ул.Крылатская 25

Результаты проведенного тестирования

CHECK UP БЕЗОПАСНОСТИ

«Заказ N»

ЗАКЛЮЧЕНИЕ

Общий уровень безопасности в компании по результатам проведенного CheckUp оценивается в 43 бала по 100 бальной шкале, что означает значительный уровень рисков прерывания бизнес процессов.

43% 100%

Наиболее высокие риски связаны:

- Отсутствие в компании регламентов действий при ЧП.
- Отсутствие резервирования критических бизнес-процессов.
- Отсутствие внедренных регламентов безопасности.
- Отсутствие регулярного обучения персонала действиям при взаимодействии с правоохранителями.
- Отсутствие регламентов защиты коммуникаций и бесконтрольное использование незащищенными мессенджерами в корпоративных целях.

1. Осведомленность руководства и управление безопасностью

1.1	Сформированное понимание рисков	3	10
1.2	Система мониторинга рисков и управления рисками	2	10
1.3	Внедрение регламентов безопасности в компании	3	10
1.4	Наличие независимого контроля IT ресурсов	5	10
1.5	Общая осведомленность о практиках управления IT	3	10
1.6	Наличие результатов независимого аудита	1	10
1.7	Организация адвокатской службы	5	10
1.8	Наличие кризисного плана	1	10

2. Организационные меры безопасности

2.1	Входная группа и режим прохода в офис	3	10
2.2	Регламенты действий при ЧП у охраны и секретаря	4	10
2.3	Регламенты действий при ЧП в службе IT	4	10
2.4	Регламенты действий при ЧП у рядовых сотрудников	2	10
2.5	Обучение и проверка знаний персонала основам юридической грамотности	3	10
2.6	Обучение и проверка знаний персонала основам информационной безопасности	4	10
2.7	Режим хранения документов	5	10
2.8	Режим коммуникаций с контрагентами	3	10
2.9	Взаимодействие адвокатской службы и персонала	2	10

3. Технические меры безопасности

3.1	Системы автоматического оповещения при ЧП	3	10
3.2	Системы отключения IT систем при ЧП	5	10
3.3	Системы видеонаблюдения	6	10

4. Обеспечение непрерывности бизнес процессов на уровне IT

4.1	Использование облачной инфраструктуры	5	10
4.2	Резервирование ресурсов для критических бизнес процессов	5	10
4.3	Бекапы	6	10
4.4	Интернет	7	10
4.5	Защита платежных систем	3	10
4.6	Наличие плана на случай критических сбоев	1	10

5. Защита информации на уровне IT

5.1	Распределение прав доступа	6	10
5.2	Использование анивирусов	7	10
5.3	Использование рекомендованных настроек и обновлений	6	10
5.4	Защита от хранения информации на локальных устройствах пользователей	4	10
5.5	Политика паролей	6	10
5.6	Правила взаимодействия сотрудников IT с правоохранителями	2	10

6. Защита коммуникаций

6.1	Использование почты	3	10
6.2	Использование мессенджеров	2	10
6.3	Использование мобильной связи	3	10
6.4	IP телефония	5	10
6.5	Регламенты коммуникаций с контрагентами и внутри компании	2	10

ПЕРВООЧЕРЕДНЫЕ МЕРЫ

1. Внедрить в охрану и секретариат четкий регламент действий при полицейской проверке. Приоритет - оповещение адвокатов и руководства. Регламент может быть разработан и внедрен по запросу Заказчика.

2. Внедрить регламент действий при полицейской проверке среди рядовых сотрудников, назначить ответственных и оснастить их техническими средствами оповещения (тревожная кнопка). Регламент может быть разработан и внедрен по запросу Заказчика: технические решения Тревожная Кнопка предоставляются по запросу Заказчика.

3. Проводить раз в неделю тест средств оповещения.

4. Внедрить регламент действий при ЧП сотрудников IT. Регламент может быть разработан и внедрен по запросу Заказчика.

5. Внедрить системы автоматического отключения IT систем при ЧП, производить их тестирование раз в неделю. Технические решения Тревожная Кнопка с блокировкой серверов предоставляются по запросу Заказчика.

6. Внедрить регламент обмена информацией, Регламент может быть разработан и внедрен по запросу Заказчика.

7. Перейти на использование защищенных мессенджеров. Технические решения защищенный корпоративный мессенджер предоставляются по запросу Заказчика.

8. Отказаться от хранения документации в офисе, перенести правоустанавливающие документы в отдельное защищенное помещение.

9. Провести тренинг ключевых сотрудников по поведению при полицейских проверках, наладить онлайн обучение персонала общей безопасности бизнеса, провести тестирование знаний в начале и в конце курса обучения. Тренинг и онлайн платформа по обучению персонала предоставляется по запросу заказчика.

10. Утвердить план действий на случай критических сбоев.

ОБЩИЕ РЕКОМЕНДАЦИИ

1	Сформировать список первоочередных рисков и модель угроз. Оценить соответствие уровня защиты компании по отношению к этим рискам.
2	Сформировать регламенты и политики безопасности по всем ключевым бизнес-процессам.
3	Обеспечить документирование IT системы согласно ГОСТ и доступ руководства к актуальной версии документации.
4	Обеспечить доступ руководства к ключевым бекапам, актуальным кодам доступа и паролям.
5	Провести полный независимый аудит IT инфраструктуры.

Check Up провел

Дмитриев Александр
Клевогин Сергей