



ТОП 10

РЕАЛЬНЫХ

УГРОЗ

ДЛЯ БИЗНЕСА

О КОТОРЫХ РУКОВОДИТЕЛИ
НЕ ЗАДУМЫВАЮТСЯ

ТОП-10 РЕАЛЬНЫХ УГРОЗ ДЛЯ БИЗНЕСА, о которых руководители не задумываются.

Современные IT-технологии требуют высококвалифицированный персонал и всесторонний подход для обеспечения безопасности компании. Руководители и/или собственники далеко не всегда обладают (да и не должны) необходимыми компетенциями. Поэтому предлагаем удостовериться, что Ваш IT-специалист сделал все возможное для защиты Вашего бизнеса от самых распространенных угроз. Выглядят они так:

УГРОЗА №1

Резервные копии по принципу «вроде есть»

Как показывает практика, информация может потеряться в самый неподходящий момент – вирусы-шифровальщики, саботаж, случайное удаление, выход из строя оборудования – поэтому резервных копий много не бывает. Но они должны быть не только в достаточном количестве, но и грамотно распределены и защищены. Ежедневные, еженедельные, ежемесячные и ежегодные копии на разных физических носителях – это аксиома. Но насколько они автоматизированы, настолько должны быть контролируемы.

Контрольные вопросы:

- Какая именно информация резервируется? По какому расписанию? В каком количестве?
- Где хранятся копии? Насколько эти носители надежны?
- Каким ПО делаются копии? Куда приходят отчеты об ошибках копирования? Кто их контролирует?

УГРОЗА №2

Взломанное сетевое оборудование.

На компьютерах стоит антивирусное ПО. Рядовые роутеры и шлюзы, через которые компании зачастую выходят в интернет, таковой защитой похвастаться не могут. В результате очень легко крадутся пароли к почте, соцсетям, онлайн-ресурсам, данные банковских карт и операций, реквизиты удаленного доступа, даже пересылаемые файлы. Поэтому контроль за сетевым оборудованием должен быть жесткий.

Контрольные вопросы:

- Как часто проверяется наш интернет-шлюз на безопасность?
- Насколько надежны методы контроля его безопасности?
- Какие средства мониторинга используются? Куда и как быстро приходят оповещения?

УГРОЗА №3

Огромные убытки от простоя оборудования, в том числе серверного .

Задумывались ли вы о том, что будет с компанией в случае выхода из строя, или кражи оборудования в офисе? Каковы будут убытки от потери информации и простоя бизнес-процессов? А ведь это вполне устранимо путем грамотного подбора резервных мощностей.

Контрольные вопросы:

- Насколько быстро будет восстановлена работа компании в случае выхода из строя самого важного оборудования?
- А если реально посмотреть на вещи?
- Какие компания понесет потери за это время?
- Что сделано для предотвращения и минимизации потерь? Что еще необходимо сделать?

УГРОЗА №4

Проверку компании на лицензионность ПО может инициировать любой обиженный сотрудник, или клиент.

Человеку достаточно просто анонимно написать заявление в соответствующие органы и проверка будет неизбежна. А это остановка бизнеса и изъятие техники на срок до 2х месяцев.

УГРОЗА №5

Огромная разница между стоимостью лицензионного ПО и выплат в случае проверок.

При проверках ущерб высчитывается по формуле:
Финансовая Ответственность = максимальная стоимость ПО (ущерб) +
ущерб * 2 (штраф).

Рассмотрим варианты затрат на примере установленной на одном компьютере одной копии Microsoft Office:

1. Прямые затраты при покупке лицензионной коробочной версии:
~14.000р

2. Прямые затраты в случае проведения проверки:

- Корпоративная лицензия без подписки для коммерческих организаций:
~35.000р

- Штраф за использование нелицензионного ПО: ~70.000р

Итого к оплате: ~105.000р.

Напомним, что ущерб по данному направлению свыше 100.000р считается тяжким преступлением, что влечет возбуждение уголовного дела. Со штрафов государство имеет большие выгоды, поэтому работа по выявлению нарушителей идет полным ходом. Очевидно, что приобрести лицензию куда выгоднее, чем оплачивать штрафы.

Но всегда есть еще один вариант:

3. Прямые затраты при установке бесплатного LibreOffice: 0р.

УГРОЗА №6

На компьютерах стоит большое количество ненужного дорогого ПО.

Очень часто встречаем в своей практике, что пользователи устанавливают на рабочем месте, например, мощный и дорогой Adobe Photoshop исключительно для просмотра и изменения размера картинок только потому, что так привыкли дома. Не смотря на наличие бесплатных аналогов и создание реальной угрозы для компании.

Контрольные вопросы:

- Есть ли список установленного на компьютерах ПО и его стоимости?
- Есть ли список разрешенного к установке ПО в компании?
- Что установлено лишнее, что можно заменить действительно бесплатными аналогами?
- Каковы варианты лицензирования остро необходимого ПО, сроки, стоимость?

УГРОЗА №7

Некомпетентность и безответственность системного администратора «по вызову» грозит серьезными потерями.

Насколько Вы доверяете и уверены в своем сисадмине? Руководитель никогда не скажет, что «да, у нас есть какая-то девочка-главбух. Что-то копошится в своих бумажках, чем занимается не понятно, но отчеты вроде сдаются, налоговая пока не беспокоит». Однако про того, кто может одним нажатием кнопки (в том числе непредумышленным) уничтожить всю компанию, подобные высказывания встречаются сплошь и рядом.

Контрольные вопросы:

- Насколько наш админ надежен как человек? Можно ли ему доверять самое главное – жизнеспособность бизнеса?
- Насколько он компетентен? Как быстро и легко выполняет свои обязанности?
- Остаются ли ключевые рычаги доступа и управления в руках руководителя/собственника, или все хранится только в голове админа? Как хранится ключевая информация и кто к ней имеет доступ?
- Что будет, если админ заболит, или уволится?

УГРОЗА №8

Отсутствие распределенного удаленного доступа, либо бесконтрольный доступ через пиратские и не безопасные сторонние сервисы.

TeamViewer – программа не только далеко не бесплатна, но еще и предназначена для экстренных ситуаций, а не регулярного использования в качестве повседневного удаленного доступа. Как результат – быстро растущая статистика взломов и краж средств с личных и корпоративных счетов и это очень серьезный вопрос.

Контрольные вопросы:

- Как организован удаленный доступ в сеть компании?
- Кто имеет этот доступ и к каким ресурсам/компьютерам?
- Используются ли для этого программы со сторонними серверными ресурсами, т.е. контролируемые третьей стороной?

УГРОЗА №9

Неограниченный доступ к данным по принципу «всем всё» ведет к снижению продуктивности работы и хаосу.

Сотрудники начинают терять данные, дублировать их, терять время на поиск информации среди общей «файловой свалки», а в качестве конфиденциальных мер начинают «прятать» файлы на своих компьютерах и, как следствие, терять их окончательно в случае выхода из строя носителей информации.

Контрольные вопросы:

- Как организован доступ к информации в компании?
- Какими документами регламентируется этот доступ?
- Где хранятся файлы и базы данных компании? Участвуют ли в хранении локальные компьютеры пользователей без регулярного резервного копирования?

УГРОЗА №10

Отсутствие разработанных и доведенных до сотрудников правил корпоративной безопасности резко повышает риск потери и утечки данных, в том числе персональных.

Очень часто сотрудники даже не осведомлены что в компании можно делать, а что нельзя, какова их ответственность за «слив данных» и вообще, что под этим подразумевает руководитель и говорит Закон РФ 152-ФЗ за соблюдением которого государство строго следит.

Контрольные вопросы:

- На основании каких документов и распоряжений происходит движение информации в компании?
- Разработаны ли Правила Корпоративной Безопасности?
- Доведена ли до сотрудников информация о работе с данными компании и об ответственности за их распространение, или уничтожение?
- Кто несет ответственность за контроль соблюдения требований компании?
- Что вообще в компании является ключевой информацией? Кто должен иметь к ней доступ, а от кого необходимо защитить?

Искренне благодарим за внимание к угрозам для бизнеса! Очень надеемся, что наш опыт поможет сделать Ваш бизнес еще более сильным, надежным и уверенно развивающимся! Если вдруг у Вас возникли вопросы, или на какие-то из перечисленных вопросов получили отрицательные ответы, - немедленно нам звоните, или пишите! Тянуть с вопросами безопасности нельзя, ибо беда может прийти неожиданно и в самое неподходящее время.

С уважением, команда профессионалов ООО «Профитек».

www.profi911.ru

info@profi911.ru

8(800) 350-42-03

8(351) 729-87-03



ООО «Профитек»



www.profi911.ru
info@profi911.ru
8(800) 350-42-03
8(351) 729-87-03