Добрый день!

Ленточкин Михаил.
Директор по информатизации ЗАО «Конфлекс СПб».

Мы – полиграфисты, занимаемся флексопечатью, выпускаем более 10 тысяч тонн продукции в год.

Опыт

В ИТ с начала 2000-ых годов (даже ранее.. любительский опыт начинался еще до массового внедрения windows 3.11)

Бекапы, реальность

Первопричина большинства проблем с бекапами: - многие люди уверены, что это очень простая тема, в ней все просто и понятно. Когда появляются трудности – это «простые» трудности, поэтому не будем на них фокусироваться - само рассосется.

В связи с этим, необходимо более «глубоко» изучать вопрос, проверять работу ответственных лиц и план работ.

Первый шаг – инвентаризация имеющихся бекапов
Нужно понимать, что у нас есть. Откуда оно берется, каким способом (скрипт, средства SQL сервера, архиватор, специальное ПО)

В случае скриптов, бывает еще нужно «вычислить» где же они лежат, «под кем» выполняются и как запускаются.

Маленький нюанс
Наличие бекапа не означает, что он свежий, делается достаточно часто, что задача по его созданию всегда отрабатывает штатно. Это все необходимо так же проверить.

Изучение активов

Мы должны определить, что именно нуждается в резервировании, какова «цена» потери, как долго мы можем себе позволить восстанавливать тот или иной ресурс.

Защита

Бекап, сам по себе является целью злоумышленников, они стараются так или иначе воздействовать на информацию, которую мы копируем или уже скопировали. В связи с этим, необходимы меры по защите бекапов, вплоть до хранения офлайн копий.

Так же, условно, к мерам по защите стоит отнести и файлы, которые должны находиться на соответствующих дисках, ведь дорогие пользователи так и норовят что-то положить «поближе к себе», а не в место хранения данных. Необходимо регулярно оповещать людей, что есть правила хранения данных, кто их соблюдает - защищен, кто не соблюдает – угроза для всех и нарушитель.

Защищаем от повреждения, уничтожения и похищения.

Планирование

Определяем цифровые активы:

- Образы дисков (серверных, АРМы и прочие)
- Виртуальные машины
- Прочее (конфиги сетевого оборудования например)
- Специальные данные (ПД, Тайны..)
- Базы данных
- Файлы рабочие, текущие
- Файлы архивные

Определяем:

- как часто необходимо создавать копии, как хранить, что нужно шифровать/паролить и т.д. (некоторые сетевые конфиги сами по себе представляют интерес для злодеев).
- Как часто удалять
- Как быстро растёт объем массива, сколько места необходимо на 5 лет

Составляем план, в котором должно быть так же еще и мероприятие по дополнению и актуализации самого плана.

Компетенции
Очень важно мотивировать коллег для расширения кругозора. Чтобы люди могли не просто «включить все нужные кнопочки» и ждать результат, а думали и повышали эффективность.
Теневые копии – многие специалисты просто в курсе что они существуют, но этого не достаточно.

Специальное ПО, экономика
Глядя на цены ПО, особенно отечественного, может возникнуть желание, понаделать скриптов, закинуть их в шедулера, базы бекапить средствами SQL, и много подобных идей по оптимизации затрат.

В реальности:
Написание и отладка скриптов, их добавление и изменение – долго, не всегда работает
Выявление ошибок – пока «все не поломается» их можно и не обнаружить
Управление копиями, доступами

Все это по отдельности не сложно, но вместе, «съедает» достаточно много времени, чтобы при определенном объеме задач все же купить специально придуманное для этого ПО. Просто купитв ПО мы инвестируем, вместо зарплаты – в то, что останется в компании и будет работать долгие годы.

Привычные недоработки, которые я видел часто:
Не удаленные бекапы, там, где их бы надо бы удалять (безопасность, дисковое пространство)
Самый старый бекап удаляется, хотя свежий сделан не был.
Игнорирование накопительных бекапов.
Не готовность к «разрыву» связи, отключению света, алерт должен был прилететь с сервера, который остался без связи из-за различных обстоятельств, в итоге нет бекапа и нет алерта,

Спасибо за внимание!!!