План непрерывности бизнеса

Как показывает опыт, во многих организациях сегодня отсутствует план непрерывности бизнеса, либо в нем не учтены многие из вопросов, которые сегодня все чаще поднимает жизнь. Многие со мной не согласятся, но это факт!

Что такое план непрерывности бизнеса?

План непрерывности бизнеса (Business Continuity Plan - BCP) – набор документов, позволяющих выстроить планирование непрерывности бизнеса вашей компании при возникновении различных происшествий и инцидентов. Результат – восстановление работоспособности информационных систем или их компонент в конечные временные рамки.

Выделяют три основных составляющих данного процесса:

1. **Управление инцидентами (Incident Management)**. Это оперативный уровень. На данном уровне рассматривается комплекс внутренних и внешних происшествий высокой и средней вероятности возникновения, например, мошенничество, человеческий фактор, сбой в работе оборудования. Задачи и цели: сохранность, доступность, целостность, аутентичность информации, отказоустойчивость.
2. **Управление непрерывностью бизнеса и аварийным восстановлением (Business continuity & disaster recovery management).** Это тактический уровень. Фактически на данном уровне мы рассматриваем инциденты, которые способны привести к остановке производства или основных бизнес-процессов. Несмотря на небольшую вероятность, ущерб может оказаться значительным, вплоть до банкротства.
3. Управление чрезвычайными (кризисными) ситуациями (Crisis & emergency management) - является стратегическим уровнем обеспечения бесперебойности бизнес-процессов.

Вместе с тем я ни разу не видел включение в такие планы таких событий как массовые беспорядки, эпидемии с возможностью заключения в карантин целых городов, а, возможно, и областей.

Если еще 10 лет назад такие события считались маловероятными, то сегодня нет. Стоит вспомнить события 2014 года в Донбассе или эпидемия 2019-2020 года, начавшаяся в Китае и распространившаяся по всему миру.

Короновирус и ИБ.

Угрозы включают два класса:

1. влияние на доступность ресурса "ЧЕЛОВЕК"
2. деградация(вплоть до краха) инфраструктуры и СЗИ в связи с попытками их трансформации для удаленного доступа и других фишек в режиме паники.

Основным решением в данном случае является трансформация для удаленного доступа и здесь возникает сразу несколько вопросов:

1. Знаете ли вы, есть ли компьютерное оборудование у ваших сотрудников дома?
2. Какое это оборудование?
3. Разрешат ли ваши сотрудники установку дополнительного программного обеспечения для работы из дома?

4. Удовлетворяют ли их компьютеры требованиям информационной безопасности и лицензионной чистоты?
5. Как быть с тем, что на персональном компьютере сотрудника есть и его домашняя информация и корпоративная? Как отследить утечки?

Как видите, вопросов масса. Но подготовиться заранее вы просто обязаны. Что посоветовать?

1. Заранее провести опрос и определить готовность сотрудников к работе из дома.
2. Определить готовность аппаратных средств к работе.
3. Там, где компьютеры поддерживают Windows 10, заранее подготовить флешки (внешние SSD) с Windows To Go и возможностью подключения по USB 3.0. Подробнее этот процесс описан в журнале CIS (Выпуск #4 (10) 2019) https://cismag.ru/. Статья «Работаем из дома?».
4. Для других ОС решение будет, безусловно, иным. Основная задача, подготовить ОС на сменном носителе таким образом, чтобы фактически домашний компьютер не имел доступа к своему жесткому диску, а работал как удаленный терминал.

Правда стоит отметить, что сделать это нужно заранее, тем более что введение карантина может быть внезапным.

Безусловно, это не единственный вопрос. Но начинать с чего-то надо!