

Анализ пробелов в организации

Перед началом анализа пробелов полезно иметь базовый уровень. Это дает вам над чем работать и представление о том, какими должны быть цели для вашей организации. Существует ряд различных исходных показателей на выбор, и некоторые из этих исходных показателей были специально созданы для определенных организаций.

Например, ваша организация может следовать набору базовых показателей Национального института стандартов и технологий. Они публикуют документ под названием "Специальная публикация 800-171, редакция 2". И название этого документа - "Защита контролируемой несекретной информации в нефедеральных системах и организациях".

Вы также можете использовать базовый уровень, созданный Международной организацией по стандартизации и Международной электротехнической комиссией. Это ISO/IEC 27001, или системы управления информационной безопасностью. И, конечно же, вы можете создавать свои собственные базовые показатели, исходя из ваших конкретных потребностей как организации.

Эти базовые показатели обычно включают анализ людей в вашей организации и процессов, которые вы используете для обеспечения безопасности. Оценивая людей, вы можете лучше понять их формальный опыт в области безопасности информационных технологий. Возможно, захочется понять, какую подготовку они прошли. И вы, возможно, захотите узнать, знают ли они о конкретных политиках и процедурах безопасности, которые вы можете использовать в своей организации.

Например, у нашей организации может быть семь разных локаций, и мы провели анализ пробелов по всем этим системным требованиям для всех семи из этих локаций. Места, которые относительно близки к базовому уровню, мы можем отметить зеленым цветом. Все, что может находиться в средней точке, мы можем отметить как желтое. А места, требующие большой работы, чтобы соответствовать нашим стандартизированным базовым показателям, мы будем отмечать красным.

Поэтому, если мы хотим оказать наибольшее влияние на улучшение нашей безопасности, мы можем начать с местоположений и требований безопасности, отмеченных красным, а затем перейти к тем, которые отмечены желтым цветом, а затем, наконец, зеленым. Отчет, очевидно, будет включать обширную информацию о том, почему использовались эти цвета, и краткое изложение того, как мы можем внедрить меры безопасности для лучшего достижения целей этих базовых показателей.