Improvinn
management consulting

Фирмена Киберсигурност

Изграждане на високо ниво на кибер-хигиена и защита на информационната сигурност

Внедряването включва няколко етапа:

1. Измерване на текущото ниво на киберсигурност.

а) Входящ тест по кибер-хигиена.

Целта е да се разбере до каква степен персонала е запознат с основните видове кибер атаки, дали може да ги разпознава и какви знания и умения има в създаването на правилни реакции.

Има въпроси относни фишинг атаки, работа с имейли, dns сървъри и др.

б) Тестове за онлайн проникване.

Целта е да се разбере колко е защитена информационната сигурност от хакерски атаки през Интернет. В зависимост от фирмата се проверяват имейл сървъри, файлови сървъри, активни директории и др.

в) Физическо проникване.

Проверките се извършват на място, като се проверява до какво ниво е контрола на достъп до компютри, мрежово осигуряване, рутери и др.

2. Доклад за текущото състояние.

На база на събраните данни се изготвя доклад, в който се включва описание на текущото състояние на киберсигурност и мерки за подобряване.

Докладът е разделен на четири част:

2.1 Резултати от тестовете.

2.2 Намерени пробиви при онлайн проверките за проникване.

2.3 Открити пробиви при физически проверки за проникване и достъп до информационната среда.

2.4 Мерки за подобряване по всички точки и теми за провеждане на обучения.

3. Обучения за повишаване нивото на киберсигурност.

а) Запознаване с основните видове атаки.

б) Примери за фишинг, социален инженеринг и др.

в) Как да се разпознават фалшиви имейли, sms-и, съобщения и обаждания.

г) Противодействия и реакции.

д) Защити - пароли, криптиране, софтуер за управление на пароли.

е) Видове заплахи.

ж) Социални мрежи.