ЗАЩИТА ДАННЫХ

Стратегия и тактика защиты данных в современных условиях

Курило Андрей Петрович, ктн,
Советник по информационной безопасности ФБК CS,
Доцент кафедры КБ КВО РГУ им. Губкина

Стратегия без тактики – это самый медленный путь к победе.

Тактика без стратегии – это просто суета перед поражением

Сунь-Цзы

ЗАЩИТА ДАННЫХ

Главные цели действующей стратегии - защита жизненно важных личности путем повышения защищенности КИИ и обеспечения защиты информации ограниченного доступа /Доктрина ИБ/

Главный тактический приоритет - «ДЦК» - обеспечение доступности, целостности и конфиденциальности данных.

Главная реалия:

Абсолютная ИБ безопасность недостижима. Всегда остается риск удачной атаки.

ЗАЩИТА ДАННЫХ

- практически все ПД наших граждан уже стали достоянием злоумышленников
- с каждой новой утечкой, данные имеющиеся в распоряжении злоумышленников, только актуализируются и пополняются
- возникает ощущение, что на «той стороне» существует очень большая и подробная база данных о нас, содержащая ПД о нас и иные сведения. Эта база данных постоянно пополняется и обогащается новыми сведениями. Эта база пополняется не только за счет хищения ПД. Сейчас все большую роль играют системы типа OSINT
- на «той стороне» этой базой данных использует армия (до 50 -70 тыс. чел.) подготовленных людей для организации мошеннических атак на наших граждан, субъектов ПД
- практически все украденные данные весьма долго сохраняют свою актуальность и будут использованы. Для ПД человека это десятки лет, фактически время его жизни
- мошеннические действия с использованием украденных ПД будут только множиться и совершенствоваться в течение очень длительного времени

Таким образом, следует признать следующее:

- усилия, предпринимаемые для достижения стратегической цели – обеспечения приоритета «Д-Ц-К» как главного, не привели к желаемому результату в части сохранения конфиденциальности хранимых ПД.

-самыми востребованными для мошенников оказались общедоступные ПД: ФИО, телефон, эккаунты в социальных сетях, а также адрес, данные геолокации, сведения о движимом и недвижимом имуществе.

-специальные виды ПД мало кого интересуют.

Вместе с тем, тактика, направленная на обеспечение целостности и доступности, себя оправдывает.

Также оправдывает себя тактика принуждения операторов к выполнению требований по защите.

ЗАЩИТА ДАННЫХ

Рецептов нет. Есть мысли.

Необходимо признать, что злоумышленник имеет полный набор ПД и не только, о гражданах.
В основной массе «ворується уже своровванное»
Линия защиты должна проходить через каждую голову каждого гражданина страны.
Неоходимо переходить на главный тактический принцип защиты «Нулевое доверие».
Граждане должны иметь возможность удаления предоставленных данных,
Бесконечный сбор одних и тех же ПД с подписанием согласия на обработку ПД предствляет собой не эффективную процедуру с точки зрения защиты.
Объем собираемых данных должен быть максимально сокращен.
Необходимо контролировать **качество** реализации и выполнения установленных защитных мер.
Это возможно сделать только через **оценку зрелости соответствующих процессов**.
Изменение стратегических приоритетов – приоритет «ДЦК» должен быть модернизирован и разделен на отдельные цели.
Необходимо вводить временной критерий достижения цели защиты.
Основной источник утечки данных персонального характера – БД ПД. Необходимо усиливать их защиту, в том числе и на уголовно-правовом уровне, введя специальную норму в УК. Это один из ключей к решению проблемы.

ЗАЩИТА ДАННЫХ

Благодарю за внимание!