КИБЕРБЕЗОПАСНОСТЬ

SAM CYBERSECURITY

ИССЛЕДОВАНИЕ УГРОЗ КИБЕРБЕЗОПАСНОСТИ

Выбрав исследование SAM Cybersecurity, вы получите полную оценку безопасности инфраструктуры, включающую анализ развёрнутого программного обеспечения и его использования. В дополнение вы сможете убедится, что используете необходимые процессы для минимизации цифрового риска, получите рекомендации на основе лучших мировых практик по кибербезопасности и сможете выбрать решения, соответствующие современным требованиям мобильности и защищенности.

Шаги проекта SAM Cybersecurity

ПЛАНИРОВАНИЕ

Определение потребностей и целей

Сбор информации о лицензировании, ИТ ландшафте и структуре бизнеса

Обсуждение проекта, согласование доступа и назначение ресурсов

СБОР ДАННЫХ

Инвентаризация аппаратного и программного обеспечения, имеющихся лицензий с применением программных инструментов

Опросы и интервью с участниками проекта

Сбор информации о процессах и процедурах

АНАЛИЗ ДАННЫХ

Обзор и проверка всех собранных данных

Оценка практик кибербезопасности SANS 20 и анализ рисков, связанных с развернутым ПО

Карта оптимизированного окружения, ориентированного на задачи стратегии по безопасности

РЕЗУЛЬТАТЫ И РЕКОМЕНДАЦИИ

Обсуждение финальных рекомендаций и участие в дискуссиях о полученных результатах для гарантированного достижения целей проекта

Предложение дальнейших шагов по внедрению решений, направленных на защиту от актуальных угроз

Результаты исследования SAM Cybersecurity

- Оценка безопасности программных активов и предоставление практических рекомендаций для повышения защищенности
- Минимизация рисков потери данных, увеличения простоя сотрудников, мошеннических действий
- Экономия средств на борьбу с кибератаками и увеличение эффективности
- Выбор передовых решений для построения гибкой ИТ инфраструктуры, быстро реагирующей на возникающие угрозы

Оценка и улучшение кибербезопасности

Методология SAM Cybersecurity компании ITERBI включает исследование действующих в вашей компании практик по защите от кибер-угроз, основанное на международном своде рекомендаций SANS 20.

SANS 20 Critical Security Controls – рекомендации, опубликованные Центром стратегических и международных исследований (CSIS) для усовершенствования кибербезопасности. Надежная автоматизация важнейших средств обеспечения безопасности позволяет уменьшить число «измеряемых» рисков более чем на 90%.

Исследование сфокусировано на двух группах пользователей: специалисты ИБ и бизнес пользователи. Это упрощает подход к оценке информационной безопасности компании и дает наиболее достоверную оценку реальной ситуации. По итогам оценки вы получите адресные рекомендации по улучшению аспектов безопасности в 20 различных областях.

Сценарии Cybersecurity – проблемы и решения

Выявить угрозы, исходящие от устаревшего и необновляемого ПО – это лишь одна из возможностей. Для противостояния новым вызовам мы рекомендуем использовать передовые технологии Microsoft при построении и развитии ИТ инфраструктуры. Вопросы качественного и многоуровневого улучшения защиты – одна из составляющих планирования перехода к гибридной и облачной инфраструктуре. Облачные сервисы Microsoft имеют более 40 сертификатов и аттестатов по безопасности – больше чем у остальных поставщиков облачных служб.

Вирусы (трояны, шифровальщики)

Совместное использование Endpoint Protection и Configuration Manager обеспечивает надежную защиту от данного вида угроз в корпоративной среде:

- Настройка политик защиты от вредоносных программ, параметров брандмауэра Windows и управление Advanced Threat Protection в Защитнике Windows для выбранных групп компьютеров
- Использование обновлений Configuration Manager для загрузки актуальных файлов определений вредоносных программ на клиентские ПК
- Отправка уведомлений по электронной почте, использование средств мониторинга в консоли и просмотр отчетов, чтобы информировать пользователей с правами администратора об обнаружении вредоносных программ на клиентских компьютерах

Социальная инженерия

Enterprise Mobility + Security (EMS) — это единственное комплексное облачное решение, которое обеспечивает безопасность корпоративных данных на самом устройстве и за его пределами благодаря четырем уровням защиты, охватывающим удостоверения, устройства, приложения и данные.

EMS помогает решить одну из ключевых проблем в ориентированной на мобильные и облачные технологии среде — как безопасно предоставлять данные сотрудникам вне офиса.

EMS позволяет ИТ-администраторам использовать службу Azure Information Protection для защиты корпоративных данных на уровне файлов. Благодаря этой возможности данные во время хранения и передачи защищены всегда, где бы они ни хранились и кому бы ни предоставлялись.

Хищение информации

Azure RMS (Azure Rights Management Services) позволяет настроить шифрование на уровне файлов и данных для исключения непреднамеренной или преднамеренной утечки данных авторизованными пользователями.

DDoS атаки и аналогичные

Данный вид атак снижает надежность сетевых ресурсов, которые являются основным драйвером продаж клиента. Azure на уровне самой платформы надежно защитит от атак DDoS на всех интерфейсах, принимающих входящий, исходящий и межрегиональный трафик.

Подтверждение соответствия решений требованиям законодательства

Предоставление данных по соответствию решений по безопасности Microsoft Федеральным законам:

- 149-ФЗ от 27.07.2016 «Об информации, информационных технологиях и защите информации»
- 152-ФЗ от 27.02.2006 «О персональных данных»
- 294-ФЗ от 26.12.2008 «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»
- 242-ФЗ от 21.07.2014 Статья 2 «О территориальности баз данных россиян»

Преимущества работы с ITERBI

Компания ITERBI более 7 лет активно участвует в разработке методик и проведении SAM проектов. За это время мы реализовали более 180 проектов и стали командой, признанной на российском и международном уровне. Опыт предыдущих исследований научил нас оптимизировать трудозатраты клиента и верно расставлять акценты при ведении консалтинговых проектов.

Основное внимание нашей команды обращено на:

- индивидуальный подход и адресные рекомендации для решения задач заказчика
- предоставление полной информации о существующих возможностях для достижения наиболее эффективной работы ИТ инфраструктуры и оптимизации расходов
- точность в расчетах и оценках при ведении проектов вне зависимости от размеров компании и сложности её организации
- формирование наглядных и удобных в использовании результатов исследования
- соответствие применяемых методологий современным тенденциям, в том числе связанным с цифровой трансформацией

Благодаря усилиям наших экспертов появились ГОСТ Р ИСО/МЭК 19770-1-2014 – российский аналог международного стандарта ISO/IEC 19770-1, методологии проведения проектов SAM SQL Workloads, SAM SPLA и SAM Cloud, дополнения к методологии SAM Cybersecurity в части оценки SANS 20.

Результаты работы компании ITERBI были отмечены наградами:

- Победитель российского конкурса партнерских ИТ-решений Microsoft в номинации SAM 2016
- Финалист международного конкурса Microsoft Partner of the Year 2016

Контакты

Свяжитесь с нами для консультации и обсуждения проекта

Андрей Щуренков
Руководитель ИТ консалтинга
shchurenkov@iterbi.ru

АО «АЙТЕРБИ»
Телефон: +7 (495) 272-4359
http://www.iterbi.ru
sam@iterbi.ru

Антон Витвицкий
Руководитель направления SAM
vitvitskiy@iterbi.ru