

Проект обследования уровня защищённости ИТ-инфраструктуры к киберугрозам

Киберпреступность переключилась с отдельных пользователей на организации, с причинения ущерба – на получение прибыли. Целью может стать бизнес любого размера.

Ущерб¹:

- Каждая 3-я компания в мире сталкивается с кибератакой, половина из них теряет важные данные
- 11 млн.руб. – расходы на устранение ущерба от кибератаки для крупной компании, 123 тыс.дол. – для малой
- 35% инцидентов простоя производства вызваны кибератаками, из них 18% простой более 24 часов
- 67% инцидентов связаны с человеческим фактором

Кроме прямого ущерба кибератаки сопровождаются утечкой информации, взломом сети, хищением средств.

Снижайте риски до 90% благодаря Cybersecurity:

Обеспечьте непрерывность процессов	Защитите критически важные сегменты инфраструктуры
Сократите неустойки за срывы сроков поставок	Обеспечьте целостность, доступность и конфиденциальность данных

Продолжительность проекта: 1-3 месяца

Этапы:



Результаты:

1. Оценка и рекомендации для повышения кибербезопасности по 20 направлениям на основе международного свода рекомендаций SANS 20 Critical Security Controls.
2. План ближайших шагов по устранению наиболее критичных уязвимостей, таких как: установка патчей и обновлений, настройка политик безопасности, активация средств антивирусной защиты, организация шифрования данных и резервного копирования.
3. Дорожная карта по внедрению передовых решений для построения гибкой ИТ инфраструктуры, быстро реагирующей на возникающие угрозы.

¹ Здесь и далее источник данных – «Лаборатория Касперского»

Типы угроз и инфраструктурные решения:

Угроза	Решение
Вирусы, черви, троянские программы, шифровальщики	Endpoint Detection and Response + Защитник Windows 10 + System Center Configuration Manager для обеспечения целостности и доступности информации Kaspersky Industrial CyberSecurity
Социальная инженерия	Enterprise Mobility + Security (EMS) — единственное комплексное облачное решение для обеспечения безопасности корпоративных данных в офисе и за его пределами Windows 10 для защиты корпоративных данных на личных устройствах сотрудников
Промышленный шпионаж и непреднамеренная утечка информации	Azure Rights Management Services (RMS) для исключения утечки данных авторизованными пользователями
DDoS и иные сетевые атаки	Azure для обеспечения надёжной защиты на уровне самой платформы; Windows Defender Advanced Threat Protection для обнаружения и быстрого реагирования
Атаки на конечные точки и электронную почту	Windows Security Center для мониторинга, отслеживания и принятия мер

Преимущества работы с нами:

- Реализуем комплексные проекты оптимизации ИТ-инфраструктуры: от аудита и постановки задачи до внедрения и обучения пользователей.
- Имеем собственную методологию проектов оптимизации инвестиций в ПО: обследования серверной инфраструктуры, готовности к переходу в облака, кибербезопасности.
- Разработчики ГОСТ Р ИСО/МЭК 19770-1-2014 (ISO/IEC 19770-1).

Наши награды:

- Финалист международного конкурса Microsoft Partner of the Year 2016.
- Победитель российского конкурса партнерских ИТ-решений Microsoft в номинации Software Asset Management 2016.
- Сертификат за лучшие Cloud-проекты.
- Сертификат за самые качественные рекомендации по модернизации ИТ-инфраструктуры.
- Сертификат за развитие Software Asset Management в SMB.

Свяжитесь с нами:

Антон Витвицкий

Руководитель Центра компетенций
vitvitskiy@iterbi.ru

Ольга Михайлова

Руководитель направления по консалтингу и обучению
mihaylova@iterbi.ru