ПРОГРАММА ТРЕНИНГА

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЛЯ ВЫСШЕГО РУКОВОДСТВА ФИНАНСОВЫХ ОРГАНИЗАЦИЙ»

Дата: 13 октября 2017г.

Место: г.Бишкек, City Hotel

Время	Название	Спикер/тренер	Описание
09.00-10.00	Новости киберугроз. Центральная Азия 2016.	Евгений Питолин	Обзор киберугроз и киберинцидентов 2016 года в регионе
10.00-11.00	Методы современной социальной инженерии	Валерий Зубанов	Примеры основных методов и наиболее успешных практик
11.00-11.15	Кофе-брейк		
11.15-12.30	Курс Kaspersky Interactive Protection Simulation* Формирование понимания последствий киберинцидентов для бизнеса, возможных ошибок при построении системы защиты и готовности сотрудничать с коллегами для обеспечения непрерывности бизнес	Евгений Питолин, Валерий Зубанов	Деловая игра с элементами компьютерной симуляции
12.30-13.30	Обсуждение итогов деловой игры	Евгений Питолин, Валерий Зубанов	Обсуждение итогов, формирование выводов
13.30-14.30	Обед		
14.30-15.30	Типовые ошибки в построении системы информационной безопасности	Евгений Питолин	Обзор самых распространенных ошибок и их последствий
15.30-16.30	Лучшие практики в построении ИБ в организации. Системный подход к защите.	Валерий Зубанов	Обзор лучших примеров и описание первоочередных задач при построении системы ИБ
16.30-17.00	Завершение тренинга		

Kaspersky Interactive Protection Simulation*

Для повышения осведомленности в области информационной безопасности высшего руководства организаций «Лаборатория Касперского» проводит обучающий курс Kaspersky Interactive Protection Simulation для банков.

Цели обучения:

- тренинг показывает участникам, какое место информационная безопасность занимает в непрерывности и прибыльности бизнеса, какие новые вызовы и угрозы сейчас существуют;
- какие типичные ошибки совершают компании, строя свою политику ИБ,
- какое взаимодействие между департаментами и отделом информационной безопасности может обеспечить наиболее стабильную работу предприятия и устойчивость к киберугрозам.

Каждый из сценариев рассматривает соответствующий спектр угроз, позволяет проанализировать типовые ошибки в построении информационной безопасности и реагировании на инциденты в финансовом секторе.

Сценарий обучения:

Команды соревнуются в управлении условным банком с собственной сетью банкоматов, онлайн-банкингом. Политика информационной безопасности внедрена, соответствует стандартам и обеспечивает предсказуемый уровень мошенничества. Однако банк подвергся серии атак (Carbanak, Tyupkin, Cryptor, BlackEnergy), и их влияние на прибыль становится критическим, причем продолжает расти.
Командам нужно скорректировать свои финансовые, IT и ИБ стратегии и применить решения в области кибербезопасноститак, чтобы минимизировать влияние атак и сохранить доход.

В процессе игры участники сами приходят к важным и применимым в их каждодневной работе выводам:

- Кибербезопасность должна обеспечиваться не только специалистами по информационной безопасности, все остальные подразделения должны активно участвовать в ее поддержании
- Знание наиболее актуальных киберугроз критически важно для своевременного и успешного реагирования на атаки

Описание ключевых отрабатываемых ситуаций

№	Название модуля	Описание	Значение для обеспечения информационной безопасности
1.	Уязвимости в приложениях	Моделируется ситуация детектирования ранее неизвестной уязвимости в программном обеспечении, обслуживающем портал оказания финансовых услуг в режиме онлайн.	Данный модуль в обучающей форме дает понимание руководящим сотрудникам организации важность своевременного детектирования уязвимостей в приложениях и необходимость инвестирования ресурсов в закрытие уязвимостей. Раскрывается модель правильного поведение сотрудников службы

			информационной безопасности для быстрого принятия компенсирующих мер и планирования стратегии развития информационной безопасности для предотвращения подобных угроз в будущем.
2.	Атаки путем проведения SQL инъекции	Моделируется ситуация атаки на веб ресурсы организации путем проведения SQL инъекции	Данный модуль в обучающей форме объясняет, что такое атака на веб приложение (цель атаки - вывод из строя или внесения несанкционированных изменений в интернет ресурсы) и к каким последствиям может привести подобная атака. По результатам прохождения модуля руководство организации получает информацию о том, как правильно защищаться от веб атак и почему важно инвестировать ресурсы в защиту от них.
3.	Репутационные риски	Моделируется ситуация кражи персональных данных	Данный модуль в обучающей форме объясняет почему необходимо обеспечить всестороннюю защиту от кражи персональных данных, как правильно выстроить систему защиты персональных данных, какие компенсирующие меры необходимо принять при установлении факта утечки важной информации.
4.	Защита мобильного приложения	Моделируется ситуация использования мобильного приложения, разработанного для пользования в режиме онлайн	Данный модуль в обучающей форме объясняет почему необходимо обеспечить защиту мобильного приложения и мобильного доступа в рамках программы оказания финансовых услуг в режиме онлайн.
5.	Защита от таргетированных атак	Моделируется ситуация тарегитированной атаки на инфраструктуру банка	Данный модуль в обучающей форме объясняет почему традиционные решения по информационной безопасности недостаточны для отражения таргетированных атак.

Требования к участникам:

Понимание базовых элементов системы безопасности (например, что такое антивирус и сетевой экран). Не нужно быть экспертом по безопасности, но некоторое знание IT-систем требуется.