КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

КАК ОБУЧАТЬ И КОНТРОЛИРОВАТЬ? СОВМЕСТИМО ЛИ ЭТО?

Алексей Леонов
ГК ЦФТ

#CODEIB

КАК ОБУЧАТЬ И КОНТРОЛИРОВАТЬ? СОВМЕСТИМО ЛИ ЭТО?

Алексей Леонов

ГК ЦФТ

о Компании ЦФТ

Позиция на рынке
ЦФТ входит в ТОР-5 крупнейших разработчиков ПО в России

Специализация
Разработка программного обеспечения
Процессинговые услуги
Аутсорсинг

Офисы
Новосибирск, Москва и в более 12 крупных городах России.
Зарубежные офисы: Алматы, Душанбе, Кишиневе.

Сотрудники
Более 3000 человек.

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Обучение сотрудников

С учетом специфики направлений, обучение также должно быть разнообразным

КУРСЫ ДЛЯ НОВИЧКОВ
При трудоустройстве всем сотрудникам назначается базовый курс обучения

КУРСЫ ПО СПЕЦИАЛИЗАЦИИ
У нас достаточно много специализаций, по наиболее критичным проводятся доп.обучения (администрирование, разработка Фронта и т.д.)

ПОВТОРЕНИЕ
По части направлений мы проводим повторение пройденного

Акценты в обучении

По версии Британских ученых для здорового и безопасного климата в Компании акцент в обучении сотрудников стоит сделать на

1

КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ
Виды КИ, Особенности обращения с КИ

2

ИНФОРМАЦИОННЫЕ РЕСУРСЫ
Виды ИР, особенности работы с информационными ресурсами, удаленный вариант работы

3

ПАРОЛЬНАЯ ПОЛИТИКА
Виды паролей, способы установки, что делать в различных случаях

4

ПРАВИЛА РАБОТЫ С ПОЧТОЙ
Наиболее важный пункт с точки зрения воздействия на человека в Компании

5

ВИРУСЫ И ПОСЛЕДСТВИЯ
К чему может привести, если «ты» поймал ВПО

6

КРИПТОГРАФИЯ
Правила работы и уместность

Мониторинг событий ИБ

Периодичность и важность мониторинга и контроля

МОНИТОРИНГ ФИШИНГА
Мониторинг фишинговой активности и направленность на наши сервисы

МОНИТОРИНГ СОБЫТИЙ ИБ
Мониторим инфраструктуру на появление аномалий со стороны пользовательских компьютеров

МОНИТОРИНГ ВИРУСНОЙ АКТИВНОСТИ
Мониторинг за состоянием компьютеров на предмет заражения ВПО

Статистика по событиям за 2018-2019

Угрозы	Частота/попадание
Внешний фишинг	3-5 %
Попытка скачивания ВПО	2-5 чел./мес.
Заражение на сайтах	Сошло в 0

Контроль за состоянием ИБ

Периодичность и важность мониторинга и контроля

ОРГАНИЗОВАННЫЙ ФИШИНГ
На постоянной основе организуем собственный фишинг

ПЕНТЕСТЫ
Проводим собственный пентест

ВНЕШНЯЯ RED TEAM
Заказываем внешний redteam с вкл.соц.инжинерией

Частота встречаемые события

Периоды	Частота «попадания» на рассылку		
	1 рассылка	2 рассылка	3 рассылка
2 полугодие 2017	4%	2,5%	2,5%
1 полугодие 2018	6,6%	6,2%	9,7%
2 полугодие 2018	16%		

ГЛАВНЫЙ ИСТОЧНИК УГРОЗ

— это ЧЕЛОВЕК.

#CODEIB

КАК ОБУЧАТЬ И КОНТРОЛИРОВАТЬ ОДНОВРЕМЕННО?

1

ОБУЧАЮЩИЕ КУРСЫ
Не все понимаю основы ИБ. В Организации должны быть разработаны основные правила обращения с критичной информацией и работа с СЗИ.

2

КУРСЫ ПО БЛОКАМ
Специализированные вещи должны быть доведены в виде отдельных курсов или блоков курса – модули.

3

ИНТЕРАКТИВНОСТЬ
В настоящее время запомимается все то, что необычно. Картинки, игры, интерактив.

4

ОН-ЛАЙН МОНИТОРИНГ. SOC ВАМ В ПОМОЧЬ
Сотрудники должны понимать, что безрассудство и беспечность будет обнаружена и это наказуемо

5

НЕПРЕРЫВНОЕ ТЕСТИРОВАНИЕ
Службой ИБ должно проводится непрерывное обучение сотрудников на предмет работы с почтой. Интернетом, флешками. Звучит банально, а спасает от множества проблем.

6

ВНЕШНЕЕ ТЕСТИРОВАНИЕ
При внешних аудитах стоит всегда заказывать тестирование методом соц.инженерии

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ

a.leonov@cft.ru
+7 913 487 20 62

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ