People-Centric Security: Теперь все внимание на людей

Прозоров Андрей, CISM
Руководитель экспертного направления в Solar Security

Блог: 80na20.blogspot.com
Твиттер: twitter.com/3dwave
Группа в ВК: vk.com/isms8020

2018-04-05

Чей авторитет (влияние) выше?

CISO 1	CISO 2
Мы регулярно (несколько раз в год) собираем Комитет по ИБ	Комитет по ИБ? Все слишком заняты…
Я успешно обосновываю бюджеты по ИБ	Мне трудно согласовывать бюджет по ИБ, и его постоянно сокращают
Я регулярно посещаю продуктовые комитеты по ИТ	Иногда я даже не знаю, что внедрены новые ИТ
Все сотрудники понимают и соблюдают правила ИБ	Ну, вы же понимаете, что нам нельзя запрещать что-то ТОПам…
Политики и регламенты по ИБ у нас написаны кратко и понятным языком. Сотрудники знают, где их можно посмотреть и у кого уточнить	У нас обычный набор документов по ИБ, соответствует требованиям регуляторов
У нас есть Программа обучения и повышения осведомленности	Мы давно хотим начать обучать сотрудников, но как-то пока не до этого
У нас есть Политика по использованию BYOD	Мы не можем запретить и контролировать личные мобильные устройства
Сотрудники часто спрашивают совета по ИБ	Многие в компании даже не знают кто CISO

Мы выбираем…

Блокировать и запрещать нельзя использовать ИТ так, как нужно бизнесу!

*"Концепция People-Centric Security зародилась из-за того, что бизнес **запретил** безопасности **запрещать**".*

Антон Чувакин, Gartner

Запрещать и блокировать уже нельзя… А что делать?

Необходимо обучать пользователей работать «безопасно». Причем не просто обучать, а создавать культуру ИБ, поощряющую правильную (безопасную) работу с информацией, ИС и сервисами.

На этом и строится подход People-Centric Security…

Правило PCS №1

Бизнес первичен, а ИБ должна ему помогать.

ИБ – доверенный советник, который предлагает как лучше сделать.

Правило PCS №2

Руководство организации поддерживает и своим примером показывает необходимость и ценность ИБ, культура ИБ поощряется и поддерживается всеми сотрудниками.

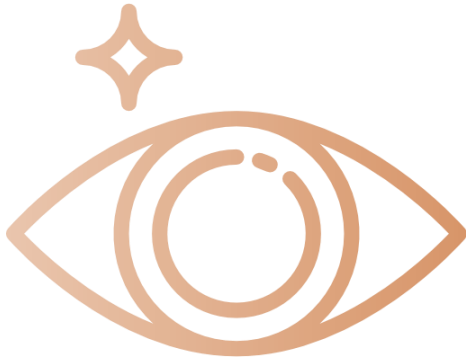
Правило PCS №3

Сотрудники лучше знают, что нужно бизнесу.

Но важно, чтобы они понимали и принимали на себя персональную ответственность за возможные последствия для бизнеса.

Правило PCS №4

Поведение сотрудников контролируется, все ошибки анализируются, и по ним дается обратная связь с целью их дальнейшего недопущения.



Правило PCS №5

Погрешности в работе персонала первоначально рассматриваются в качестве неумышленных ошибок, предполагающих объяснения и обучение. Но если потребуется наказание, то оно будет обоснованным и неминуемым.

	Data-Centric Security	People-Centric Security
Фокус внимания	Информация	Люди
Главная идея ИБ	Защита информации	Создание позитивной культуры ИБ
Разрешенное поведение	Запрещено все, что не разрешено	Разрешено все, но правильно (безопасно), вот так…
Кто прав?	ИБ лучше знает, как надо	Бизнес лучше знает, как надо
Принятие ответственности	Сотрудники должны...	Сотрудникам объясняют, но решение за ними
Документы	Требования и регламенты	Рекомендации, памятки, учебные материалы
Восприятие сотрудниками	ИБ — карающий контролер	ИБ — доверенный советник
Режим работы DLP	DLP в режиме блокировки	DLP в режиме мониторинга/отправка по требованию

Спасибо!

Прозоров Андрей, CISM
Руководитель экспертного направления в Solar Security

Блог: 80na20.blogspot.com
Твиттер: twitter.com/3dwave
Группа в ВК: vk.com/isms8020

2018-04-05