«Безопасность должна не только выполнять функции страховой компании, но и помогать бизнесу развиваться», - в Москве завершился Код ИБ ПРОФИ.

Послушать практикующих экспертов по кибербезопасности приехали ИБ и ИТ-руководители из разных городов России, Казахстана и Латвии. На вводной секции, предваряющей программу из 17 эксклюзивных мастер-классов, куратор конференции Алексей Лукацкий поинтересовался у участников мероприятия, какие темы их волнуют больше всего.

Самым насущным оказался вопрос взаимодействия бизнеса и безопасности. По мнению многих ИБ-руководителей, зачастую собственники бизнеса так далеки от безопасников, как и безопасники далеки от бизнеса. Ставшую уже сакраментальной тему выделения бюджета на ИБ **Рустем Хайретдинов** (к слову, сам являющийся собственником бизнеса) прокомментировал так: *«Руководство относится к выделяемому бюджету на кибербезопасность, как на налогам, то есть старается минимизировать. Безопасники же любят преувеличить возможные риски, и руководство, поняв, что ничего плохого не случилось, начинает скептически относиться к бюджетам на ИБ».* По словам **Рустема Хайретдинова** (Атак Киллер, г. Москва), любая не стопроцентная вероятность реализации риска воспринимается бизнесом, как пятидесятипроцентная, а затем и как нулевая. А значит, и траты на безопасность признаются избыточными, в отличие от инвестиций в рост бизнеса.

Илья Борисов (ThyssenKrupp, г. Нижний Новгород) справедливо отметил, что финансы на приобретение ИБ решений тратить нужно с умом, переходя от покупки этих продуктов к тактике и стратегии управления ИБ, чтобы добиться максимальной интеграции безопасности в бизнес-процессы компании. В этом **Илье Борисову** видится будущее ИБ.

Развивая тему бюджетирования ИБ, **Рустем Хайретдинов** подчеркнул, что крупный бизнес менее защищен от рисков, чем средний в силу наличия большого объема хранящейся информации, которую можно зашифровать или получить к ней доступ. По этой причине крупный бизнес вынужден тратить значительные суммы не только на Compliance, но и на реальную защиту своих активов.

Еще одним вопросом, поднятым на пленарной дискуссии, стало вовлечение собственников и руководителей бизнеса в процессы ИБ. По словам **Владимира Щурова** (Мортранс, г. Петропавловск-Камчатский), безопасники у руководства ассоциируются с плохими новостями, и когда дело доходит до разбора последствий инцидента, руководители «впадают в ступор» и никак не стремятся включаться процесс. Рустем Хайретдинов так прокомментировал эту ситуацию: *«Серьезные инциденты с ИБ требуют внимания руководства. На случай крупного инцидента должны быть разработаны инструкции и сценарии со сменой ролей: в критической ситуации, связанной, как с пожарной, так и с информационной безопасностью, сотрудники компании должны четко понимать, кто за что отвечает, у каждого должна быть своя роль сценарии выхода из инцидента. В процесс разработки таких сценариев руководство вовлекается намного проще».*

Программа конференции содержала также длительные мастер-классы от **Алексея Лукацкого** (CISCO), **Дмитрия Мананникова, Льва Палея** (СО ЕЭС), **Моны Архиповой** (МИРЦ), **Алексея Плешкова** (Газпромбанк), **Дениса Горчакова** (Ростелеком), **Александра Леонова** (Тинькофф Банк) и других ведущих экспертов кибербезопансости. Разнообразить деловую части мероприятия помогли киберучения, которые провели **Илья Борисов** и **Алексей Лукацкий.** Темой интерактива Ильи Борисова стала командная работа в ИБ. Участники в течение двух часов решали 9 вполне реальных кейсов: защита облаков, мобильных устройств, Windows, импортозамещение. Учения

Алексея Лукацкого были целиком посвящены борьбе с фишингом. Безопасники разрабатывали антифишинговую стратегию, включающую в себя не только выбор технических и организационных мер, но и разработку playbook для SOCa или группы реагирования на инциденты. Подводя итог киберучений, куратор конференции отметил: *«Участники отлично знают различные методы обнаружения, предотвращения и нейтрализации фишинга, но ни разу не упомянули про реагирование на него. Такое впечатление, что все верят в 100%-ю защиту».*

Приятным дополнением к насыщенной деловой программе стали 2 дня приключений, способствовавших новым знакомствам и тесному общению участников.

Это не последняя конференция Код ИБ ПРОФИ, проводимая в формате 2 дня учебы + 2 дня приключений. Следующее подобное мероприятие пройдет с 25 по 28 июля в г. Сочи. Предварительная продажа билетов на него уже открыта и доступна по ссылке: https://sochi.codeib.ru

Впечатления участников

Очень рад быть здесь, видеть новых людей, подчеркнуть для себя много качественной информации, Морской стандарт- бункер, Шуров Владимир

Все супер! Идей и работы - на целый год, до следующей конференции в Москве!
Инвестмент Партнерс, Смирнов Илья

Как всегда - на высоте! Спикеры - профессионалы, готовые делиться накопленным опытом. Код ИБ Профи стал одним из лучших и знаковых мероприятий! Так держать!
НИПИ НГ ПЕТОН, Аксютин Юрий

Наши благодарности

Партнерам мероприятия:

Доктор Веб, Netwrix, SearchInform, Атом Безопасность,

Медиа-партнерам:
Anti-Malware.ru (Стратегический медиа-партнер), порталу ISO27000.ru, порталу GlobalCIO, Information Security, Единому порталу электронной подписи, Dom.ru Бизнес, порталу Xakep, Бизнес порталу Security Lab, Ассоциации руководителей служб информационной безопасности, журналам “Системный администратор”, BIS Journal, IT-EVENTS, Журналу CIS, Интернет-агентству IT Delta, ИТ Порталу JetInfo, Нижегородскому Клубу ИТ-директоров, Клубу ИТ-директоров ЦФО «я-ИТ-ы» , Клубу ИТ-директоров Одессы и Санкт-Петербургскому клубу ИТ-директоров.