

ФОРУМ CISO: все для информационной безопасности

В апреле 2014 года в конгресс-центре Swissotel "Красные Холмы" состоялся 7-й форум CISO, в котором приняли участие более 260 директоров по информационной безопасности из разных отраслей.

Открыл форум В.Минин (МОО АРСИБ). Он отметил, что в России активно ведется подготовка к формированию киберкомандования. Приведенные им цифры свидетельствовали о наличии серьезных угроз в сфере информационной безопасности (ИБ): совокупный убыток от киберпреступлений составил 25 млрд. долларов, это на 25% больше, количество компьютерных атак с целью кражи денег выросло на 27% по сравнению с предыдущим годом. Убыток от утечки информации в мире оценивается в 32 млн. долларов. Каждую секунду в России жертвами киберпреступлений становятся 12 человек.

Затем в дискуссионном клубе прозвучали мнения Д.Шевцова (ФСТЭК России), Ф.Цариковского, (ФАС России), С.Миროнова (Министерство финансов РФ), Д.Кострова (АРЕС Азиатско-Тихоокеанского экономического сотрудничества) и О.Зименкова (Департамент информационных технологий и связи Правительства РФ). Выступавшие коснулись вопросов совершенствования нормативно-правовой базы по технической информации, безопасности мобильных устройств и изменения в стандартах ISO27001 и ISO27002.

Первую сессию форума, посвященную архитектуре ИБ, открыл К.Коротнев ("Эльдорадо"), рассказав об опыте компании по стратегическому управлению ИБ. К.Эриксон (Philips) отнес к основным угрозам для ИБ государственный шпионаж, киберпреступления, инсайдеров, хакеров и конкурентов. А.Зеренков (Супаптес) остановился на практическом подходе к оценке рисков ИБ. Е.Тетенькин ("МФИ Софт") коснулся методов контроля увольняющихся сотрудников, которые представляют особый

риск для системы ИБ компании. Об опыте внедрения электронных подписей в своей компании рассказал А.Волков ("Северсталь"). Д.Ушаков (Stonesoft, а McAfee Group Company), в ходе своего выступления затронул вопрос о новой норме сетевой безопасности. А.Смирнов (НИИГлоБ) обозначил основные угрозы для системы ИБ и представил концепцию общественной безопасности РФ.

Следующая сессия была посвящена вопросам комплаенс – этот термин можно определить как способность действовать в соответствии с инструкциями, правилами и специальными требованиями. Комплаенс часто понимается как защита интересов фирмы путем контроля соблюдения сотрудниками положений действующего законодательства, требований надзорных органов, а также документов. П.Сотников (Qualys), рассказал о часто возникающих противоречиях между требованиями комплаенс и требованиями ИБ и о том, как можно как эти противоречия преодолеть. А.Дроздов (ISACA) отметил различия последних международных и российских стандартов управления ИБ.

В рамках лаборатории стратегии "Комплексный подход к управлению информационной безопасностью. Управление рисками" Д.Безкоровайный (Trend Micro) подчеркнул, что в последнее время число целевых атак значительно возросло. Е.Акимов (R-Style), отметил, что стоимость систем ИБ для небольших компаний в расчете на одного пользователя в несколько раз дороже, чем для крупных. А.Дашков (LETA) рассказал о решении AirMagnet Enterprise для превентивной безопасности Wi-Fi сети предприятий.

Первая сессия следующего дня была посвящена обсуждению мобильной безопасности и началась докладом В.Найма (PwC) об интеграции мобильных устройств в ИТ-структуру предприятия. А.Макар (Единая Европа-Холдинг) отметил, что кибератакам чаще всего подвергаются устройства на базе ОС Android. Е.Царев (Swivel Secure) рассказал, почему 80% компаний в течение трех лет меняют решения аутентификации. В качестве одной из причин он назвал интеграцию личных мобильных устройств в ИТ-структуру предприятия.

Одним из наиболее интересных событий форума стала лаборатория "Практика выявления мошенничества. Компьютерная криминалистика". В обсуждении этих вопросов приняли участие Е.Климов (RISSPA), Н.Липчанский (British Communications) и А.Зайцев (ЕС-лизинг). В докладах была обозначена роль компьютерной криминалистики в сфере ИБ и затронута проблема инсайдерства.

В фойе форума, образовав небольшую выставку, разместились стенды фирм – спонсоров форума. Журнал попросил рассказать представителей этих фирм о продуктах, которые они продвигают на российском рынке.



Григорий Белокобыльский,
специалист по развитию
бизнеса компании "ЗМ"

Дивизион "Оптические системы" компании "ЗМ Россия" представляет решение по защите визуальной информации. Это экран из полимерной пленки для установки на монитор, она ограничи-

вает угол обзора до 60°. Пленка немного ослабляет яркость изображения, но не искажает картинку, светопропускание пленки составляет порядка 95-97%. А при увеличении угла обзора более 60° она полностью затемняет изображение, сбоку виден просто черный экран. Посторонние люди, находящиеся сбоку от экрана, не видят информацию на вашем мониторе, она видна только пользователю, который располагается под прямым углом к экрану.

Экран устанавливается с помощью специальных креплений, он не наклеивается на монитор, и его можно при необходимости быстро снять, например, чтобы показать презентацию коллегам. Крепление представляет собой клеевые

полоски на рамку монитора, которые и удерживают экран. Пленка для планшетов наклеивается на стекло, при этом сенсорные дисплеи не теряют чувствительности к прикосновению. Существуют различные форматы экранов для мониторов, ноутбуков, планшетов, смартфонов и т.д. Более подробную информацию можно найти на нашем сайте 3mruussia.ru/screens.



Елена Белова,
старший специалист
направления защиты
от утечек информации
компании "МФИ Софт"

На форуме наши эксперты выступают с докладом о защите баз данных, покажут практические кейсы. На выставке компания демонстрирует свои направления по информационной безопасности, решения "Гарда" и "Периметр". "Гарда" – система класса DLP (Data Leak Prevention) для защиты от утечек информации и аудита безопасности баз данных. "Периметр" – система операторского класса для фильтрации трафика и защиты от DDoS-атак.

Мы ориентируем решения на крупный и средний бизнес. Нашими клиентами могут быть как единые предприятия, так и географически распределенные по филиалам. Традиционно решения "МФИ Софт" пользуются спросом у операторов связи, у нас широкие компетенции по работе с большими объемами данных. Среди наших клиентов есть почти все операторы связи а также крупные банки и промышленные предприятия, такие как "МТС-банк" и УАЗ.



Евгений Царев,
директор по развитию
бизнеса компании
Swivel

Мы представляем свое решение – платформу аутентификации Swivel. Это полноценная платформа, необходимая для организации двухфакторной и усиленной аутентификации в самых разных приложениях, будь то личный кабинет на сайте или защищенный доступ к почте. Все

привыкли к SMS с одноразовым кодом или использованию скрэтч-карт для доступа к системам интернет-банка, наша платформа аутентификации позволяет сделать аналогичный доступ практически к любой ИТ-системе компании.

Решение уникально тем, что нет профилирования ни по типу, ни по масштабу организации, оно одинаково эффективно работает везде. Крупные организации, используя одну платформу, одну систему, могут применять усиленную аутентификацию в любом количестве уже имеющихся приложений или в тех, что будут применяться в будущем. Для небольших организаций привлекательна цена, поскольку за небольшие деньги они могут обеспечить дополнительную безопасность для своего критически важного ресурса.

Компания существует более 10 лет, в Россию она пришла в конце 2012 года. Весь прошлый год шла активная работа по сертификации и продвижению, и в настоящий момент бренд является узнаваемым. Фактически рынок бес-токенной аутентификации сегодня полностью ассоциируется с компанией Swivel Secure.



Павел Сотников,
управляющий
директор компании
Qualys

Компания Qualys является пионером и ведущим поставщиком облачных решений в области безопасности и соответствия требованиям. Компания существует на рынке

уже более 15 лет и является мировым лидером в своем сегменте, что подтверждено рейтингами Gartner. У нас сейчас более 6700 клиентов по всему миру, включая большинство компаний из списков Forbes 50 и Forbes 100.

Ключевым отличием от аналогов является то, что мы предоставляем услугу из облака, расположенного в Швейцарии. Клиенту не нужно тратить деньги на покупку серверов, лицензий и т.д., он может купить наш сервис и сразу обеспечить безопасность своей инфраструктуры. Это что-то вроде подписки на журнал или премиум-доступ на сайт.

Система QualysGuard позволит корпоративному заказчику автоматизировать процесс управления уязвимостями и соответствия

политикам безопасности в рамках всей организации, обнаруживать сети и определять взаимосвязь между ними, определять приоритетность активов, оценивать масштаб угроз и следить за установкой исправлений в соответствии с рисками для бизнеса. Функции обеспечения соответствия требованиям позволят контролировать, обеспечивать и документировать соблюдение внутренних политик безопасности и правовых норм. Решения Qualys могут быть развернуты в течение нескольких часов в любой точке мира.

У нас есть решения как для огромных корпораций, так и для небольших фирм из трех-четырёх человек. Люди, желающие, например, открыть интернет-магазин, могут воспользоваться нашими услугами для обеспечения его безопасности, и при этом они сами могут иметь только базовые представления о том, что такое защита информации.

Разумеется, основные наши клиенты – это все-таки крупные компании. Если смотреть на карту мира, то наибольшее количество клиентов сейчас в США и Западной Европе, но в последние пять лет идет активное развитие нашего продукта в Восточной Европе, России, СНГ и странах Азии.



Михаил Кондрашин,
технический директор
Trend Micro, Россия

Компания Trend Micro разрабатывает широкий спектр средств информационной безопасности. Основными аспектами, представляемыми на форуме, являются средства защиты виртуальных и облачных систем, различные инновационные разработки в области защиты мобильных устройств и специализированные системы для защиты от нацеленных атак. Специально для форума мы подготовили демонстрационный стенд, позволяющий участникам убедиться, что для очень многих современных вызовов есть адекватные ответы для всех вышеперечисленных систем.

В первую очередь наши клиенты – фирмы крупного и среднего масштаба, но в нашем портфеле предложений, несомненно, есть очень интересные решения и для небольших компаний. Это комплексные, максимально

простые в установке и обслуживании решения. И конечно же, это продукты для домашних пользователей с широким спектром функций безопасности, которые нужны дома: сохранность файлов, родительский контроль, антивирусная безопасность.



Александр Белкин,
коммерческий
директор компании
LETA

Наша компания работает на рынке с 2003 года, и, по данным международного рейтингового агентства IDC, мы входим в пятерку крупнейших российских компаний

по информационной безопасности. На форуме мы представляем решение от Fluke Networks по защите беспроводных сетей. Оно позволяет контролировать подключение разрешенных и неразрешенных Wi-Fi-точек. Иногда возникают ситуации, когда пользователь самостоятельно создает Wi-Fi-доступ, просто используя свой мобильный телефон. Представленное нами решение позволяет выявить местоположение такой точки, отключить или, если это сделать не удастся, заблокировать ее с помощью белого шума. Это очень серьезное, интересное и перспективное решение, но достаточно дорогое, оно не для каждой компании. Недавно на его основе мы закончили проект по внедрению контроля беспроводных сетей у одного крупного оператора.

С экспонентами беседовал
А.Майстренко

НОВЫЕ КНИГИ ИЗДАТЕЛЬСТВА "ТЕХНОСФЕРА"



Р. Морелос-Сарагоса
ИСКУССТВО ПОМЕХОУСТОЙЧИВОГО
КОДИРОВАНИЯ.
МЕТОДЫ, АЛГОРИТМЫ, ПРИМЕНЕНИЕ

Рекомендовано ИГПИ РАН

МОСКВА: ТЕХНОСФЕРА,
2005. – 320 с.,
ISBN 5-94836-035-0

Цена: 225 руб.

Новейшее пособие по теории и практике цифровой связи, не имеющее аналогов в литературе на русском языке. Наиболее активно идеи помехоустойчивого кодирования внедряются в системах мобильной связи и в магистральных высокоскоростных линиях. Быстрое распространение Интернета и мультимедийных средств стимулирует применение кодов, исправляющих ошибки, для защиты банков данных огромной емкости от случайных или преднамеренных искажений. Помимо классических алгоритмов декодирования блоковых и сверточных кодов детально рассмотрены современные идеи декодирования с «мягким решением» и итеративного декодирования.

Идеальное учебное пособие для студентов, изучающих программирование и связь, инженеров-разработчиков и практиков.

КАК ЗАКАЗАТЬ НАШИ КНИГИ?

✉ 125319, Москва, а/я 91; ☎ (495) 956-3346, 234-0110; knigi@technosphaera.ru, sales@technosphaera.ru