СТАТЬИ

Бизнес и безопасность: как защитить себя в digital-мире?

7 Ноября, 2018 12:59

По материалам Integrity Vision

Теги: безопасность, конференция, информационная безопасность, Integrity Vision, GDPR

В современном мире, всё уходит в digital и автоматизируется, потому *чтоб сохранить данные компании недостаточно поставить сигнализацию в офисе и усилить охрану.* Кибератаки на бизнес случаются всё чаще, уязвимости веб-сайтов и программ приводят к масштабным утечкам данных, а хакеры придумывают тысячи новых способов, как обойти защиту корпоративного периметра сети. Генеральный директор компании Integrity Vision Инна Соловьёва и руководитель направления информационной безопасности Олег Половинко рассказали о трендах 2019 года, проблемах бизнеса, связанных с ИТ-безопасностью и их решении в современном мире.

IT-БЕЗОПАСНОСТЬ В МИРЕ И УКРАИНЕ

Сталкивались ли вы лично с неэффективной защитой данных и систем?

Олег: Если оценивать по 10 бальной шкале среднюю температуру в Украине, то это будет 3. Но! Рывок от 1 до 3 мы осуществили за прошедший год. И я вижу положительную динамику. Ну а по сути, кейсов множество и мы их будем разбирать на UA.SC.

Какие громкие инциденты в ИТ-безопасности происходили?

Олег: На самом деле, я считаю, каждую неделю происходят инциденты мирового масштаба в ИТ-безопасности. Только за последний месяц с этим столкнулись такие компании-гиганты как Google и Facebook, плюс наша страна находится в состоянии кибервойны, где каждый день происходят события. Кроме того, сложно забыть о вирусе NonPetya и WannaCry - они имели мировой масштаб и нанесли сильный ущерб компаниям, которые с ними столкнулись.

Что будет трендом в ИТ-безопасности на 2019 год?

Олег: Первое - в Украине скоро выборы, кибератаки со стороны северного партнера будут нарастать. Печальный опыт Эстонии, Грузии и наш это доказывает. Вопрос как защитить критическую инфраструктуру, процесс выборов и что делать бизнесу во время массовых атак. Второе - активный мониторинг уязвимостей и угроз, особенно учитывая рост IoT устройств. Третье - облака, периметр расширился даже не на одно облако, а на 3-4, это новые вызовы для ИБ.

БИЗНЕС И IT-БЕЗОПАСНОСТЬ

Есть ли у бизнеса понимание, когда им необходимо обратиться за решением по ИТ-безопасности, или они обращаются только после инцидентов?

Олег: Информационная безопасность - история про риски. Кто-то учитывает эти риски, просчитывает, а кто-то постоянно надеется на лучшее. Вирус-шифровальщик

НОВЫЕ СТАТЬИ

Облачный сервис Zyxel для киберзащиты компаний
Владимир Смирнов Сегодня 09:03

VMware и HPE расширяют сотрудничество
Владимир Смирнов Вчера 08:36

LG Electronics и Siemens будут создавать "умные" заводы
Владимир Смирнов 2 Сентября 09:06

Рынок IoT для бизнеса уверенно растет
Владимир Смирнов 30 Августа 08:51

READERS' TOP

1 Intel пытается доказать, что ее процессоры все еще лучше, чем у AMD
2 Chrome и Firefox защитят от государственного spyware?
3 Ведущие мировые компании активно развивают проекты Интернета вещей
4 Huawei представила прогнозы по технологической отрасли
5 Amazon Web Services: Получи доступ к бесплатным видео-урокам

WEB NEWS & EDITORS' CHOICE

1 Кто есть кто на рынке гиперконвергенции
2 По схеме Ахметова. Аэро Телеком владеет очень дорогими частотами. При чем тут Порошенко?
3 Facebook, Amazon и Apple попались. Как и зачем они нас слушают на смартфонах
4 Дубилет: "Когда показываешь Privat24 или monobank европейцам, они плачут от умиления"
5 Android vs iOS. Кто проигрывает конкуренцию: инфографика

NonPetya это подтверждает, но это лишь прививка, эффект от которой до сих пор действует. Многие пережили этот момент и подумали: “класс, это пережили, переживём и остальное”, а кто-то задумался и изменил тактику. У каждого свой подход и все совершенно по-разному оценивают риски.

Плюс слабая позиция государства ведет к тому, что по большей мере угрозы каждый оценивает сам. GDPR драйвер решений в Европе, у нас же постановления больше декларативные. А если оценить ущерб который нанесен только NonPetya, только по скромным подсчетам это 0,5 ВВП.

Можно ли самостоятельно определить необходимость внедрить конкретное решение для защиты бизнеса?

Олег: Информационная безопасность - комплексные решения, и политика построения не может идти вразрез с работой бизнеса. В процессе определения, что внедрять - важно учитывать стратегические планы бизнеса на будущее, риски, которые перед ним стоять. Но это в классическом виде. На практике всё складывается иначе, от хаотичного тушения пожаров до покупок решений которые больше нравятся.

Важно еще помнить, что если хакеры еще ни разу не добрались до вас - не стоит об этом заявлять на весь мир, ведь для кого-то это может стать настоящим вызовом.

Существует ли показатель, после которого обязательно нужно улучшать ИТ-безопасность, звоночек, что всё под угрозой?

Олег: У владельцев украинского бизнеса этот звоночек звонит без остановки и громко. Украина - по сути, лаборатория для России по откатыванию кибератак, тестирования новых методов. Мы постоянно под прицелом и атакуют сейчас всех, и каждый может быть использован для таргетированной атаки в будущем.

Пора уже привыкнуть, что мы живём в эпоху digital, это подразумевает то, что ты можешь быть атакован. Когда мы говорим о людях, то нет ничего невозможного: взломать могут любого человека. Если тебя берут в разработку - никакая двухфакторная аутентификация или подтверждение через смс не спасут - всё перехватывается и ломается, цена вопроса совсем невелика. Ты просто должен быть готов к этому.

Что может сделать Integrity Vision для защиты ИТ-безопасности клиента?

Олег: Комплексная защита ИТ - это наша основная задача. Глобальный тренд на диджитализацию повышает требования к безопаности. Мы помогаем это сделать в соответствии со стандартами, такими как ISO2700(0-5), постановления НБУ #95 и требованиям GDPR.

Отдельно внимание мы уделяем работе с уязвимостями и предотвращением их эксплуатации. В нашем портфеле есть решения, которые постоянно сканируют инфраструктуру и помогают сотрудникам компании смотреть на компанию глазами злоумышленника, такой себе взгляд со стороны.

Следующий этап - предотвращение атак. Здесь мы имеем дело с аналитикой и выявлением угроз. Так же, по статистике 30% CISO считают источником угроз - собственных сотрудников и мы с этим согласны. Управление пользователями, мобильными устройствами сотрудников и особенно привилегированными пользователями эти решения сейчас особенно востребованы.

Отдельно отметим это внедрение SIEM систем, предназначенных для комплексного мониторинга и анализу событий и уязвимостей. Зонтик который собирает информацию со всех ИТ активов компании и анализирует данные на лету, согласно преднастроенных правил информационной безопасности. Решение без границ, мы можем видеть несанкционированную активность сотрудников или злоумышленников, контролировать работу критических сервисов или обнаруживать вектора потенциальных атак.

UA.SC - КОНФЕРЕНЦИЯ ПО IT-БЕЗОПАСНОСТИ

Почему вы создали конференцию по ИТ-безопасности?

Инна: Мы понимали, что на рынке дефицит таких платформ. Мы ежегодно делали конференции для заказчиков и говорили о тех решениях, которые считали актуальными и востребованными. Когда Integrity Vision запустили направление информационной безопасности, мы решили, что это простой способ собрать всех и обсудить насущные проблемы отрасли и тем самым принести пользу и заказчикам, и

партнерам.

Почему вы назвали конференцию UA.SC и охватили всеукраинский масштаб?

Инна: Integrity Vision - ведущий системный интегратор в Украине, потому логично было создать конференцию только всеукраинского масштаба. Мы позиционируем себя как платформа для корпоративного сегмента, где решаются вопросы построения комплексной защиты бизнеса: регуляторная политика, нормативная база и влияние мировых стандартов.

Чем отличается UA.SC от других конференций по ИТ-безопасности?

Олег: На протяжении года проходит много мероприятий связанных с ИБ, по большей части они для “хакеров” черных или белых, студентов, инженеров ИБ. Они разбирают уязвимости, анализируют атаки или участвуют в CTF (Capture the flag) соревнованиях.

Инна: UA.SC нацелена на людей, которые несут ответственность за построение системы ИБ, где важен взвешенный подход к выбору решений. За один день мы объединяем топ-вендоров, мировых экспертов и корпоративный сегмент, чтобы дать большой объём полезной информации, которую потом используют для выполнения ежедневных задач и для построения комплексной информационной защиты.

Конференция проходит третий год подряд: что изменилось, что будет нового?

Инна: Сегодня возросла востребованность в решениях информационной безопасности. Раньше по каждому направлению информационной безопасности на рынке были представлены решения только от 1-2 производителей (вендоров). Но, на данный момент, рынок стремительно развивается и растёт количество представителей решений для каждой конкретной задачи IT-безопасности. Поэтому с каждым годом на конференции мы объединяем все большее количество вендоров для покрытия растущих потребностей бизнеса. Будет интересно, приходите!

28 ноября 2018 года в Киеве состоится **третья всеукраинская конференция по IT-безопасности** UA.SC. Вы можете узнать больше, присоединиться к мероприятию на Facebook или купить билеты.

КОММЕНТАРИИ:

ВОЙДИТЕ ДЛЯ ТОГО, ЧТОБЫ ОСТАВИТЬ КОММЕНТАРИЙ