Только что

Как туриндустрия может противостоять киберугрозам

Туристический и гостиничный бизнес в последние годы стал прибыльной мишенью для киберпреступников, которые воруют у предприятий в ходе атак, на выявление которых часто уходит более полугода.

Согласно исследованию IntSights , только за последние три года гостиничная индустрия столкнулась с 13 серьезными атаками . Согласно исследованию TransUnion, во втором квартале во всем мире в секторах путешествий и досуга число предполагаемых попыток онлайн-мошенничества увеличилось на 155,9% по сравнению с аналогичным периодом прошлого года , по сравнению с увеличением общего количества предполагаемых вторжений на 16,5%. А преступники не сдавались во время пандемии, поэтому авиакомпаниям пришлось продолжать борьбу с мошенничеством и киберпреступностью.

Гостиничная индустрия привлекает киберпреступников, потому что она обрабатывает огромное количество финансовых транзакций во многих странах. Каких типов атак следует опасаться ИТ-персоналу и подрядчикам отелей?

Главная кибер-проблема отелей

Главной угрозой для отелей является фишинг , мошенничество, при котором гости отеля могут получать поддельные телефонные звонки от лица стойки регистрации. Звонящий может заявить, что возникла проблема с кредитной картой в файле и что ему необходимо повторно подтвердить способ оплаты.

Взломы DarkHotel — еще одна серьезная угроза. Они нацелены на путешественников через Wi-Fi в отеле. Цифровые сертификаты отправляются гостям, как знакомое обновление Adobe, которое извлекает конфиденциальную информацию. Сети отелей борются с этими взломами, предлагая гостям использовать виртуальную частную сеть.

Вредоносное ПО (вредоносное программное обеспечение) — это то, что преступники рассылают по электронной почте сотрудникам под видом вложения или ссылки, которые выглядят невинными или законными. Но когда пользователь открывает файл или нажимает на ссылку, его система (и не только) может быть взломана преступником. Отели борются с вредоносными программами, устанавливая и регулярно обновляя антивирусное программное обеспечение и блокировщики рекламы, а также обучая сотрудников тому, когда нужно обращаться к ссылкам или файлам.

Другие гарантии

Существуют различные методы , которые могут помочь уменьшить вероятность кибервзлома. Например, ИТ-отдел должен регулярно обновлять операционные системы и создавать резервные копии данных и файлов, а каждый сотрудник должен дважды проверять источники

при запросе разрешений администратора программного обеспечения. Кроме того, надежные брандмауэры могут ограничивать плохой трафик и обеспечивать безопасность.

Программное и аппаратное обеспечение может помочь предотвратить взлом, но обучение сотрудников также является важной частью кибербезопасности любого отеля. Президент Sabre Hospitality Клинтон Андерсон отмечает, что представители отрасли были бы шокированы « количеством злонамеренных, злонамеренных действий, происходящих в крупных компаниях, особенно в сфере гостеприимства, где у вас много текучки на стойке регистрации».

Что происходит, когда вас взломали?

В 2018 году была взломана система бронирования Marriott . Было украдено более 500 миллионов записей о клиентах , включая данные кредитных карт и номера паспортов. Компания заявила, что взлом произошел за четыре года до открытия, и когда его заметили, компания начала использовать программное обеспечение для мониторинга компьютеров и мобильных устройств.

«Гости могут зарегистрироваться в службе под названием WebWatcher, которая отслеживает сайты, на которых может быть передана личная информация, и предупреждает гостей, если обнаруживаются доказательства их личных данных», — сказал президент и генеральный директор Marriott International Арне Соренсон. «В Соединенных Штатах регистрация в WebWatcher дает два дополнительных преимущества: покрытие возмещения убытков от мошенничества и неограниченные консультационные услуги по мошенничеству».

Авиакомпании тоже взламывают

Не только отели становятся мишенью киберпреступников: авиационная отрасль также столкнулась с серьезными кибератаками, и многие авиакомпании до сих пор не в состоянии справиться с ними. В этом году система обслуживания пассажиров SITA сообщила, что только около 35% авиакомпаний и 30% аэропортов готовы к кибератакам . Поставщик средств связи и информационных технологий, который обслуживает 90% мировых авиакомпаний, однажды был взломан. Это была «сложная атака», в ходе которой были украдены данные о пассажирах с серверов компании в США. Пострадали более 580 000 клиентов Singapore Airlines , а New Zealand Air и Japan Airlines были двумя из многих авиакомпаний , подвергшихся взлому.

Взлом SITA стал тревожным звонком для многих. Он выявил масштабы опасностей, с которыми сталкивается авиационная отрасль в результате кибератак.

«Распространяющийся эффект атаки на SITA — еще один пример того, насколько уязвимыми могут быть организации исключительно из-за их связей со сторонними поставщиками», — сказал Ран Нахмиас, соучредитель Cyberpion . «Если такие, казалось бы, законные соединения не будут должным образом контролироваться и защищаться, они могут привести к разрушительным нарушениям, которые высвободят высококонфиденциальные данные, как показано в этой ситуации».

Авиационная отрасль сталкивается с такими опасностями, как программы-вымогатели и распределенные атаки типа «отказ в обслуживании». После атаки SITA архитектор решений HackerOne Шломи Либероу подчеркнул, что авиакомпаниям необходимо готовиться к худшему.

«Мы видели, что авиационная отрасль особенно сильно пострадала за последний год, возможно, потому, что преступники знают, что они будут уязвимы, и их внимание и приоритеты направлены на то, чтобы оставаться в бизнесе», — сказал Либероу . «Однако

традиционные предприятия, такие как авиакомпании, всегда были привлекательной мишенью, поскольку немногие из них ориентированы на цифровые технологии и поэтому полагались на устаревшее программное обеспечение, которое, скорее всего, устарело или имеет существующие уязвимости, которые можно использовать».

Продавцы представляют угрозу безопасности

Авиакомпании должны контролировать сторонних поставщиков, когда речь идет о защите информации. Учитывая высокие ставки, эксперты предполагают, что слепое доверие — не вариант.

« Вы просто не можете знать, соответствуют ли ваши третьи стороны мерам безопасности вашей компании и склонности к риску, пока вы не завершите полную оценку безопасности их поставщиков», — сказал главный технический директор Panorays Деми Бен-Ари. «Но с помощью автоматических анкет, внешних оценок воздействия и учета влияния отношений на бизнес вы можете получить четкую и актуальную картину рисков безопасности поставщика. Важно отметить, что наилучшей практикой является не разовое действие, а непрерывный мониторинг в режиме реального времени».

Кибератаки приводят к серьезным последствиям, в том числе к остановке полетов. В 2015 году хакеры атаковали систему наземных операций польской авиакомпании LOT , затронув 1400 пассажиров. Хакеры сделали невозможным создание планов полетов и полетов. Это была первая в своем роде атака, и она вызвала опасения, что в один прекрасный день кибератаки могут дистанционно взять под контроль самолеты.

Лучшие практики безопасности

Хакеры — разрушительная сила в туристической индустрии. Эти преступники наносят расчетливые удары, чтобы заработать деньги и вызвать хаос. Стандартным советом для устранения угрозы является резервное копирование и хранение данных в нескольких местах, в том числе за пределами вашего физического помещения, и наличие одной копии в автономном режиме. Для взлома многофакторной аутентификации и длинных и сложных паролей потребуется больше времени. Регулярное обновление и исправление систем помогает компаниям не стать жертвами при обнаружении нового эксплойта. Сокращение или устранение теневых технологий помогает компаниям избежать небольшой дыры в своей броне, которую они не знали, что нужно залатать. Отношение к кибербезопасности как к проблеме всей компании, не связанной с ИТ, поощряет каждого сотрудника брать на себя ответственность за свои действия и знания и активно обращаться за помощью вместо того, чтобы совершать «невинные» ошибки, которые обходятся компании в миллионы долларов. Игровое обучение и микрообучение могут увеличить запоминание учебных уроков, снижая риск успешной атаки. Нулевое доверие , несмотря на то, что его сложно реализовать, также может резко сократить количество нарушений. Наконец, компаниям не следует просто бросать деньги на проблему : не все решения в области кибербезопасности работают вместе, что приводит к пустой трате денег и увеличивает риск взлома.

Ссылка на статью: Как туриндустрия может противостоять киберугрозам