УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В ТУРИСТИЧНІЙ ГАЛУЗІ

Богдан Мізюк[1], Орест Полотай[2]

1. Львівський торговельно-економічний університет, м. Львів, Україна
2. Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

The basic methods of information security threats that accompany the activities of tourist companies.

Keywords: Information security, security of personal data, travel company

Сучасний розвиток світової економіки характеризується все більшою залежністю ринку від значного обсягу інформаційних потоків. Незважаючи на дедалі більші зусилля по створенню технології захисту даних, їх вразливість не тільки не зменшується, а й постійно зростає. Тому актуальність проблем, пов'язаних із захистом потоків даних і забезпеченням інформаційної безпеки їх обробки і передачі, все більш посилюється. Проблема забезпечення внутрішньої інформаційної безпеки стає все більш актуальною для компаній туристичної галузі. Це пов'язано і з загостренням конкурентної боротьби на внутрішніх ринках, і з виходом компаній на міжнародний рівень. Багато з них вже не можуть забезпечити захист комерційної інформації власними силами і змушені користуватися послугами професіоналів.

Варто зазначити, що інформаційна безпека в туристичній галузі виступає одним з восьми складових безпеки туризму, під якою розуміють «особисту безпеку туристів, збереження їх майна та ненанесення шкоди навколишньому природному середовищу при здійсненні подорожей» [2].

Інформаційна безпека туристичної фірми, як правило, забезпечується тими ж процедурами і засобами, що і будь-якого іншого комерційного підприємства, але з урахуванням підвищеної кількості чутливих даних і транзакцій.

Інформаційну безпеку в туристичній галузі умовно можна поділити на два підвиди: безпека персональних даних та безпека інформаційного середовища [1].

Туристична галузь - одна з найбільш чутливих до загроз інформаційної безпеки. Це й не дивно - адже туристичні компанії обробляють різну конфіденційну інформацію про своїх клієнтів, а навіть звичайні відомості про туриста можуть сказати дуже багато про його смаки, звички, уподобання і стан здоров'я. Інформаційна безпека туристичної фірми може бути забезпечена тільки за умови суворого дотримання норм у сфері захисту персональних даних.

Крім цього, туризм - одна з галузей, у якій найбільш часто використовують платежі через мережу Інтернет. Бронювання номерів в готелях, резервування авіаквитків і іншої інфраструктури з оплатою через Всесвітню мережу - звичайнісіньке явище в сфері подорожей і туризму. Це все збільшує ризик втрати інформації про стан банківських рахунку, номери банківських карток та ін.. Тому однією з найважливіших завдань туристичних компаній є безпечна обробка банківських даних і реалізація всіх вимог PCI DSS (стандарту захисту даних в індустрії платіжних карт).

Для того, щоб захистити себе від витоку конфіденційної інформації, компанія, що працює в туристичній галузі, змушена запровадити внутрішню політику інформаційної безпеки, яка повинна забезпечувати дотримання певних вимог, серед яких основними є такі:

1) установка на всіх комп'ютерах антивірусного програмного забезпечення і регулярне його оновлення;

2) використання брандмауера - програмного або апаратного маршрутизатора, поєднаного з firewall (особливою системою, що здійснює фільтрацію пакетів даних), він не пропускає назовні внутрішні пакети локальної мережі підприємства і блокує доступ до неї чужих комп'ютерів ;.

3) захист електронної пошти (поставлений антивірус на корпоративний сервер електронної пошти);

4) використання Proxy-сервера. По-перше, це дозволить трохи скоротити інтернет-трафік. По-друге, це дозволить приховати від сторонніх очей внутрішні імена і адреси комп'ютерів. І, по-третє, це дозволить виявляти порушників, які підключилися до мережі підприємства з метою отримання доступу в Інтернет. [9]

5) постійний моніторинг стану комп'ютерів користувачів і локальної мережі;

6) документообіг підприємства в більшому ступені ведеться в електронному вигляді;

7) запроваджувати у функціонал компанії потужні технічні засоби захисту інформації, які повинні бути об'єднані в комплекс. Тільки одночасна злагоджена робота програмних і апаратних складових такого комплексу дає змогу оптимізувати службу інформаційної безпеки в повній мірі.

8) завдяки контролю над співробітниками туристичних агентств і моніторингу комп'ютерів в локальній мережі можна проводити ретельний аналіз усіх пересувань інформаційного потоку.

Наведені способи забезпечення інформаційної безпеки у компанії туристичної галузі є мало затратними і досить ефективними, з точки зору забезпечення безпеки компанії від безлічі загроз як зовнішніх, так і внутрішніх.

Варто відзначити й інший спосіб, такий як тотальне стеження за співробітниками, хоча відноситься цей спосіб до категорії складних і не потрапляє під категорію простих засобів. Крім того, не варто забувати, що забезпечення інформаційної безпеки не повинно завдавати шкоди діяльності компанії або створювати перешкоди для роботи співробітників, оскільки цей процес повинен доповнювати основну діяльність компанії.

Література

1. Голод А.П. Безпека туризму як об’єкт регіональних економічних досліджень // А.П. Голод // Інноваційна економіка. – 2014. – № 4 (53). – С. 190-194
2. Маркіна І.А. Управління безпекою туристичного бізнесу / І.А. Маркіна // Экономика Крыма. – 2012. – № 1 (38). – С. 174-176.