

УДК 338.48:519.86

Богуславська А.М.

канд. фіз.-мат. наук, доц. НУ «Запорізька політехніка»

КІБЕРБЕЗПЕКА У СФЕРІ ТУРИСТИЧНИХ ПОДОРОЖЕЙ

Цифрова трансформація у подорожах та туризмі, яка включає онлайн-транзакції, аналіз персональних даних клієнтів, хмарну інтеграцію, підключені пристрої та технологію цифрових платежів, призводить до усвідомлення того, що, збільшуючи свій цифровий слід, організації все частіше піддаються кіберзагрозам. Кібератаки можуть суттєво зашкодити довірі клієнтів та репутації торгової марки, а також часто мати серйозні фінансові, правові та регулятивні наслідки.

Збільшення кількості кібератак за останні роки в туристичній галузі, схоже, свідчить про зміну структури хакерів. Кіберзлочинці звернули свою увагу з роздрібної торгівлі на туристичний сектор. Туристичні компанії є привабливою мішенню для хакерів та кіберзлочинців, оскільки вони мають справу з великими та цінними обсягами персональних даних клієнтів.

При плануванні та здійсненні кібератак використовують широкий спектр методів та векторів атак, щоб обійти заходи з кібербезпеки, які організації застосовують для захисту своїх систем та даних. Атаки здебільшого залучають технічні навички високого рівня з програмування та

генерації коду, і переваги виявлених мережових та організаційних вразливостей безпеки.

Запобігання кіберзлочинам – це складне завдання і такої універсальної речі, як «срібна куля» немає. Однак компанії, уряди і міжнародні організації почали здійснювати скоординовані дії спрямовані на те, щоб обмежити або захиститись від кіберзлочинців. Скоординовані дії включають:

Створення комплексних баз даних відомих системних вразливостей і сигнатур атак (унікальна домовленість про зберігання інформації, що використовується для ідентифікації спроб зловмисників використовувати будь-яку відому вразливість). Організації по всьому світу діляться цими базами даних, щоб допомогти підготуватись та відбити велику кількість поширених атак.

Встановлення сенсорів раннього попередження та мереж оповіщення. Через високу вартість і неможливість моніторингу кожної мережі, організації контролюють важливі об'єкти або створюють пастки, які виглядають як важливі об'єкти. Оскільки на ці псевдоважливі цілі найчастіше здійснюються атаки, вони дозволяють попередити інших про потенційні напади.

Обмін інформацією в кібер-розвідці. На даний час бізнес, урядові організації і країни співпрацюють для обміну критичною інформацією про серйозні напади на найважливіші цілі, щоб запобігти подібним атакам в інших місцях. Багато країн створили агентства кібер-розвідки для міжнародної співпраці у боротьбі з великими кібератаками.

Створення стандартів керування інформаційною безпекою серед національних і міжнародних організацій. ISO 27000 є хорошим прикладом цих міжнародних зусиль.

Прийняття нових законів про запобігання кібератак і порушення безпеки даних. Ці закони передбачають суворі покарання для кіберзлочинців, спійманих за незаконними діями.

Існує багато важливих технічних сервісів, які необхідні для роботи мережі, а в кінцевому рахунку, Інтернету. Це такі служби, як маршрутизація, адресація, іменування доменів і керування базами даних. Вони є першочерговими цілями для кіберзлочинців.

Злочинці використовують інструменти перегляду пакетів (packet-sniffing) для захоплення потоків даних, що проходять через мережу. Це означає, що всі конфіденційні дані, такі як імена користувачів, паролі та номери кредитних карт, піддаються ризику. Інструменти перегляду пакетів моніторять і записують всю інформацію, що проходить через мережу. Злочинці можуть також використовувати підставні пристрої, такі як відкриті точки доступу Wi-Fi. Якщо злочинець встановлює їх близько до громадського місця, наприклад, кафе, туристи, нічого не підозрюючи,

можуть увійти в систему, а інструмент перегляду пакетів (сніфер пакетів) скопіює їх особисту інформацію.

Служба доменних імен (Domain Name Service, DNS) транлює доменне ім'я, в його числову IP-адресу. Якщо DNS-сервер не знає IP-адресу, він надішле запит на інший DNS-сервер. При підміні DNS (DNS spoofing), або це ще називають отруєнням DNS кешу (DNS cache poisoning), злочинець вводить недостовірні дані в кеш-пам'ять DNS-транслятора. Атаки отруєння кешу DNS використовують вразливість у програмному забезпеченні протоколу DNS, яка змушує DNS-сервери перенаправляти трафік для певного домену на комп'ютер злочинця, а не до законного власника цього домену.

Пакети переносять дані через мережу або Інтернет. Підробка пакетів (packet forgery) або як ще називають ін'єкція пакетів (packet injection), заважає встановленому мережному зв'язку, створюючи пакети таким чином, ніби вони є частиною цього сеансу зв'язку. Ця підробка дозволяє злочинцеві пошкодити або перехопити пакети. Цей процес дозволяє злочинцеві захопити авторизоване з'єднання або позбавити користувачів можливості використовувати певні мережні служби. Професіонали називають це атакою «людина по середині» (man-in-the-middle).