КРИТЕРИИ КЛАССИФИКАЦИИ СОЦИОИНЖЕНЕРНЫХ АТАК

А.Г. Давыдовский

Цель исследования – анализ критериев классификации социоинженерных атак на информационные социотехнические системы (ИСТС) и их пользователей.

В 2011 г. K. Ivaturi и L. Janczewski впервые предложили классификацию различных социоинженерных атак (СИА). В 2013 г. Algarni A., Xu Y., Chan T., Tian Y.-C. предложили подразделять все социоинженерные атаки на одно- и многоступенчатые. Krombholz K., Hobel H., Huber M., Weippl E. (2013, 2015) предложили классификация СИА на основе трех критериев: канала, оператора и типа. Причем каналы могут быть как техническим, так и нетехническими (психофизиологическими), операторы представлены людьми или программным обеспечением, а типы зависят от физических, технических, социальных и социотехнических способов и средств атаки. При этом могут быть использованы такие методы социальной инженерии, как «погружение в мусорные контейнеры», «спасательные работы», фишинг (вишинг), договоренности quid pro quo, «дорожное яблоко», претекстинг, «слежка». В зависимости от эксплуатируемых эмоций жертв все СИА можно классифицировать на негативно ориентированные (используют вину, сочувствие, невежество, двусмысленность и аффилированность) и позитивно ориентированные (используют дружелюбие, олицетворение, соответствие, предлога, диффузии ответственности и приманки). Для классификации СИА необходимо учитывать модели поведения социальных инженеров и их жертв, включая человеческие ошибки, особенности восприятия информации онлайн, способы восприятия и оценки низко- или высококонтекстуальных медиасообщений [1].

Критерии классификации СИА могут быть основаны на использовании технологических платформ (аппаратное и программное обеспечение, сетевая инфраструктура), атаки на мобильные устройства и их приложения, атаки рабочих столов, атаки физических инфраструктур [2]. Широко распространены методы атак, использующие мобильные телефоны, IP-технологии голосового обмена сообщениями, методы фишинга (вишинга). Отдельно можно выделить видео-СИА, а также СИА на основе использования ботнетов, руткитов (Gregio A.R.A., et al., 2015).

Учитывая вышеизложенное, впервые разработана многокритериальная классификация СИА, характеризующая динамику атаки как вектор в N-мерном гиперпространстве критериев, включающем причины и мотивацию, модели поведения социальных инженеров и их жертв, посредников, технологические платформы, информационные, социотехнические среды реализации атаки, время эффекта (быстрый, с отсрочкой, поздний), тип эффекта и его последствий. Для классификации атакующих воздействий предложен ряд базовых моделей: «человек (сообщество)→человек (сообщество)» и опосредованные «человек (сообщество)→медиасреда→человек (сообщество)», «человек (сообщество)→ИСТС→человек (сообщество)», «человек (сообщество)→ИСТС→медиасреда→ИСТС →человек (сообщество)».

Литература

1. Internet-of-things security and vulnerabilities: taxonomy, challenges, and practice/ K. Chen, [et al.] // J. of Hardware and Systems Security. – 2018. – Vol. 2, № 2. – P. 97–110.

2. Aldawood H.A., Skinner G. Taxonomy for Social Engineering Attacks via Personal Devices // Intern. J. of Comp. Appl. – 2019. – Vol. 178, N50. – P. 19–26.