МЕТОДИ ЗАХИСТУ ВІД ФІШИНГОВИХ АТАК

Філатова А.С., Настенко А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Фішинг – це одна з найпопулярніших та найнебезпечніших атак з використанням методів соціальної інженерії, оскільки дозволяє отримати несанкціонований доступ до інформаційно-телекомунікаційних систем через фактор людської помилки користувачів, які можуть довіритись фішинговим email/sms повідомленням, що містять зловмисне програмне забезпечення та/або посилання на зловмисні ресурси.

Згідно з сучасними дослідженнями [1, 2] фінансові наслідки фішингових атак зросли, оскільки компанії переходять на віддалену та гібридну роботу. Такі атаки завдають великим компаніям збитків майже на 15 мільйонів доларів щорічно. Дослідження в Інституті Понемону [1] також продемонстрували, що добре навчений персонал здатен зменшити ефективність фішингових атак на 50%. Це означає, що окрім технічних методів протидії фішингу важливим чинником економічної та інформаційної безпеки компаній є обізнаність та навченість працівників щодо дій при отриманні фішингових повідомлень.

Метою доповіді є дослідження та моделювання сучасних методів захисту від фішингових атак для визначення та порівняння їхньої ефективності.

В доповіді наводяться результати моделювання наступних найпоширеніших методів фільтрації фішингових повідомлень [2]: автентифікація домену відправника; перевірка IP-адреси відправника та наявних у повідомленні URL-адрес за актуальними чорними списками; розпізнання фішингових повідомлень за їхнім вмістом та за структурою наявних у повідомленні URL-адрес методами машинного навчання.

Наведені дані показують, що найбільш високу ймовірність розрізнення фішингових повідомлень (для подальшого їх блокування) забезпечує комплексне застосування зазначених методів. Втім, завжди присутня в роботі таких методів ймовірність помилок першого та другого роду (що підтверджується іншими дослідженнями [2]) зумовлює те, що добре навчений персонал є важливою «останньою лінією захисту» від фішингових атак.

Список літератури

1. The Ponemon 2021 Cost of Phishing Study. URL: https://www.bankinfosecurity.com/whitepapers/-w-8959

2. Сєвєрінов О.В., Шевцов В.О., Сокол-Кутиловська А.С.. Аналіз сучасних методів атак на електронні ресурси органів управління // Системи озброєння і військова техніка 1. – 2017, С. 65-68.

3. Takashi Koide, Naoki Fukushi, Hiroki Nakano, Daiki Chiba. ChatSpamDetector: Leveraging Large Language Models for Effective Phishing Email Detection. DOI: https://doi.org/10.48550/arXiv.2402.18093