Облікова картка НДДКР

Державний обліковий номер: 0224U002354

Державний реєстраційний номер: 0123U100743

Відкрита

Дата реєстрації: 12-02-2024

1. Етапи виконання

Номер етапу: 1

Назва етапу: Дослідження сутності і методів соціальної інженерії, в тому числі в мережі Інтернет

Початок етапу: 01-2023

Закінчення етапу: 01-2024

Вид звітного документа: Проміжний звіт

2. Виконавець

Назва організації: Державний університет телекомунікацій

Код ЄДРПОУ/ІПН: 38855349

Підпорядкованість: Міністерство освіти і науки України

Адреса: вул. Солом'янська, буд. 7, м. Київ, 03680, Україна

Телефон: 380442488597

E-mail: dut.aspirantura@ukr.net

WWW: http://www.dut.edu.ua/ua/

3. Власник результатів НДДКР (продукції)

Назва організації: Державний університет інформаційно-комунікаційних технологій

Код ЄДРПОУ/ІПН: 38855349

Адреса: вул. Солом'янська, буд. 7, м. Київ, 03110, Україна

Підпорядкованість: Міністерство освіти і науки України

Телефон: 380442492555

E-mail: duikt.science@ukr.net

WWW: https://duikt.edu.ua

4. Джерела та напрями фінансування

Підстава для проведення робіт: 43 - власна ініціатива (якщо робота виконується з власної ініціативи за кошти виконавця НДР або безкоштовно)

КПКВК:

Напрям фінансування: 2.2 - прикладні дослідження і розробки

Джерела фінансування

Джерело фінансування: 7706 - безплатно (договір про науково-технічне співробітництво, тощо)

Фактичний обсяг фінансування за звітний етап: 0.000 тис. грн.

5. Науково-технічна робота

Назва роботи (укр)

Запобігання і протидія методам соціальної інженерії у забезпеченні інформаційної безпеки підприємства

Назва роботи (англ)

Prevention and countermeasures of social engineering methods in ensuring the information security of the enterprise

Реферат (укр)

Дані соціологічних досліджень у сфері кібербезпеки свідчать про величезні масштаби використання методів соціальної інженерії при здійсненні кібератак на підприємства і організації по всьому світу. Так, за останні три роки переважна кількість кібератак передбачали використання певного методу соцінженерії, із соціальною інженерією пов'язані майже 90% зловмисних витоків даних, а обсяги збитків внаслідок застосування соціоінженерних технологій сягають сотень мільйонів доларів на рік. З огляду на зазначене кожне сучасне підприємство має приділяти значну увагу запобіганню і протидії методам соціальної інженерії як важливої складової забезпечення корпоративної інформаційної безпеки. У першій частині роботи встановлено особливості соціальної інженерії у сфері інформаційної безпеки й виділено основні загрози соціальної інженерії для підприємства, серед яких фішинг, вішинг, смішинг, заманювання, залякування, претекстинг, «послуга за послугу», видавання себе за іншу особу, підглядання, збирання сміття тощо; проаналізовано типові загрози соціальної інженерії в мережі Інтернет та соціальних мережах, досліджено значення пентестингу як засобу виявлення вразливостей підприємства до соцінженерії. За результатами дослідження запропоновано практичні рекомендації щодо виявлення фішингових листів і діпфейк-технологій, запобігання соціоінженерним атакам в соціальних мережах, таким як захоплення і клонування акаунтів, збір інформації про персонал організації у соцмережах, виділено чинники ефективного пентестингу соціальної інженерії в організації, а також сформовано перелік методів і технік соціоінженерних атак, які доцільно використовувати в ході тестування на проникнення для виявлення вразливостей організації до соцінженерії.

Реферат (англ)

Data from sociological research in the field of cyber security testify to the huge scale of the use of social engineering methods in the implementation of cyber attacks on enterprises and organizations around the world. In particular, over the past three years, the majority of cyberattacks involved the use of a certain method of social engineering, almost 90% of malicious data leaks are associated with social engineering, and the amount of losses due to the use of social engineering technologies reaches hundreds of millions of dollars per year. In view of the above, every modern enterprise should pay considerable attention to the prevention and countermeasures of social engineering methods as an important component of ensuring the company's information security. The first part of the work establishes the features of social engineering in the field of information security and highlights the main threats of social engineering for the enterprise, including phishing, vishing, smishing, baiting, scareware, pretexting, Quid pro quo, impersonation, shoulder surfing, shoulder surfing, etc.; typical threats of social engineering on the Internet and social networks were analyzed, the value of pentesting as a means of detecting the company's vulnerabilities to social engineering was investigated. Based on the results of the research, practical recommendations are offered for detecting phishing emails and deepfake technologies, preventing social engineering attacks in social networks, such as account takeover and cloning, collecting information about the organization's personnel in social networks, identifying the factors of effective pentesting of social engineering in the organization, and also creating a list of methods and techniques of social engineering attacks, which should be used during penetration testing to identify the organization's vulnerabilities to social engineering.

Індекс УДК: , 004.056:316.776.23

Коди тематичних рубрик НТІ: 20.56.03

6. Науково-технічна продукція (НТП)

НТП 1

Назва продукції (укр): Практичні рекомендації щодо виявлення і запобігання атакам соціальної інженерії, підвищення ефективності тестування на проникнення для виявлення вразливостей підприємства до соціальної інженерії

Назва продукції (англ): Practical recommendations for detecting and preventing social engineering attacks, increasing the effectiveness of penetration testing to identify enterprise vulnerabilities to social engineering

Очікувані результати: Нормативні документи, Методичні документи, Аналітичні матеріали

Галузь застосування: забезпечення інформаційної безпеки підприємства

Опис продукції (укр): Практичні рекомендації щодо виявлення фішингових листів і діпфейк-технологій, запобігання соціоінженерним атакам в соціальних мережах, ефективного пентестингу соціальної інженерії в компанії, методів і технік соціоінженерних атак, які доцільно використовувати в ході тестування на проникнення для виявлення вразливостей підприємства до соцінженерії.

Соціально-економічна спрямованість НТП: підвищення результативності забезпечення інформаційної безпеки підприємства, сприяння його конкурентоспроможності

Стадія завершеності НТП: Звіт по НДДКР, Рекомендації щодо виявлення і запобігання атакам соціальної інженерії, підвищення ефективності тестування на проникнення для виявлення вразливостей підприємства до соціальної інженерії

Впровадження НТП: Не впроваджено

Строки впровадження: 01.202301.2024

Виробник продукції: ДУІКТ

Споживачі продукції:

Перспективні ринки:

Права інтелектуальної власності: В Україні

Форми та умови передачі продукції: Навчання персоналу, Інформування компаній-партнерів з можливістю подальшого застосування на практиці

7. Бібліографічний опис

8. Звітна документація

Кількість сторінок в звіті: 104

Мова звіту: Українська

Кількість файлів у звіті: 1

9. Заключні відомості

Перелік осіб-виконавців

Запорожченко Михайло Михайлович

Капелюшна Тетяна Вікторівна (к. е. н., доц.)

Мужанова Тетяна Михайлівна (к. держ.упр., доцент)

Рабчун Дмитро Ігорович (к. т. н.)

Тищенко Віталій Сергійович

Щавінський Юрій Віталійович (к. т. н.)

Якименко Юрій Михайлович (к. військ. н., доцент)

Керівник організації:

Толубко Володимир Борисович (д. т. н., професор)

Керівники роботи:

Легомінова Світлана Володимирівна (д. е. н., професор)

Керівник відділу реєстрації наукової діяльності УкрІНТЕІ

Юрченко Т.А.