УДК 004.056.5
В. Бурса; І. Мудрик, доктор філософії
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ПЕРСПЕКТИВИ АВТОМАТИЗОВАНОГО ОПОВІЩЕННЯ ПРО ВРАЗЛИВОСТІ ПРОГРАМНИХ ПРОДУКТІВ НА ОСНОВІ ДАНИХ NVD ТА ІДЕНТИФІКАТОРІВ CPE

UDC 004.056.5
V. Bursa; I. Mudryk, PhD.

PROSPECTS OF AUTOMATED VULNERABILITY ALERTING FOR SOFTWARE PRODUCTS BASED ON NVD DATA AND CPE IDENTIFIERS

Зважаючи на стрімке зростання кількості відомих вразливостей та постійне оновлення бази National Vulnerability Database, ручний моніторинг безпекових повідомлень стає малоефективним і створює ризик пропуску критичних загроз для програмних продуктів [1]. Навіть за наявності фільтрів у NVD спеціалісти змушені витрачати значний час на відбір релевантних записів.

Виникає питання: чи можна створити веб-сервіс, який автоматично відбиратиме потрібні записи з NVD на основі формального опису продуктів за допомогою Common Platform Enumeration та повідомлятиме фахівців про важливі вразливості електронною поштою [2]?

Метою роботи є проєктування веборієнтованої системи моніторингу, що періодично звертається до NVD, фільтрує вразливості за CPE-ідентифікаторами і ключовими словами та формує автоматичні e-mail-сповіщення для визначених отримувачів. Основна ідея полягає у налаштуванні користувачем «моніторингів», кожен з яких задає цільові продукти, ключові слова та пороговий рівень критичності; система регулярно виконує перевірку і надсилає стислий звіт із переліком актуальних CVE.

Подальший розвиток передбачає підключення додаткових джерел (вендорські бюлетені, списки активно експлуатованих вразливостей), розширення каналів сповіщення (месенджери, інтеграція з SIEM) та додавання аналітичних засобів для оцінки динаміки ризиків [3]. Це дозволить перетворити систему на гнучкий компонент комплексного процесу управління інформаційною безпекою.

Література

1. National Vulnerability Database (NVD). National Institute of Standards and Technology [Електронний ресурс]. – Режим доступу: https://nvd.nist.gov.
2. Cheikes B. A., Waltermire D., Scarfone K. Common Platform Enumeration: Naming Specification. Version 2.3 : NIST Interagency Report 7695 [Електронний ресурс]. – Gaithersburg, MD : NIST, 2011. – Режим доступу: https://csrc.nist.gov/pubs/ir/7695/final.
3. Кавун С. В., Носов В. В., Манжай О. В. Інформаційна безпека : навч. посіб. – Харків : Вид-во ХНЕУ, 2008. – 352 с.