УДК 004.056.53

В. Д. Бойко, к.т.н., доцент кафедри кібербезпеки, М. Д. Василенко, д.ф-м.н., д.ю.н., професор, в.о. завідувача кафедри кібербезпеки

СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕННЬ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ ЗВ'ЯЗАНИХ СПИСКІВ

Веб-сервера є основою ефективного функціонування світових інформаційно-комунікаційних мереж та інтернету речей і вважаються одним з найпоширеніших об'єктів атаки, несанкціонованого доступу і використання. Тому їх захист є **актуальним** та пріоритетним напрямком кібербезпеки.

Постановка задачі. Перш ніж факт зараження веб-серверу і вторгнення зловмисника виявляється і вживаються заходи щодо обмеження поширення шкідливого програмного забезпечення, часто проходить чимало часу[1],[2]. Намітився тренд, коли шкідливе програмне забезпечення редагує або видаляє журнали системних подій, щоб приховати факти вторгнення і здійснення шкідливих дій, що ускладнює і уповільнює час виявлення вторгнення[3]. За найгіршим сценарієм розвитку подій зловмисник отримує права адміністратора, що дає йому вільний доступ до системних журналів без ризику бути виявленим. Існуючі рішення вимагають додаткових ресурсів, вимагають високої кваліфікації обслуговуючого персоналу, при цьому вони не дають гарантії швидкого виявлення вторгнення, особливо за умови отримання зловмисником привілеїв адміністратора.

Для **розв'язання задачі** у роботі пропонується система, яка використовує технологію зв'язаних списків (блокчейн-технологія, *blockchain*) із зовнішнім ключем для верифікації логів і системного журналу з метою виявлення фактів можливого вторгнення і компрометації сервера[4].

Зв'язаний список будується з блоків інформації, які включаються до повідомлень у логах (або додаються до системи журналювання як повідомлення самостійного додатку) і представляють дані, які зв'язують записи журналу в безперервний та послідовний ланцюжок.

На початку роботи задається (або генерується) контрольний ключ у вигляді парольної фрази або окремого блоку даних. Далі створюється перший блок ланцюжку ("ключ") — блок даних, що включає в себе контрольну суму першої порції логів разом з контрольним ключем.

Після цього "ключ", що представляє собою початковий блок ("блок-0") ланцюжка зв'язаних списків, забирається із системи і зберігається поза нею, а отже і поза досяжністю зловмисника. Оскільки отримання зворотних значень хеш-функції пов'язано зі значними обчислювальними витратами, зловмисник, який не має доступу до "ключу", не може ані внести зміни в верифіковані зв'язковим списком записи, ані змінити хеш-суми, ані навіть видалити записи так, щоб це не було відмічено під час аудиту.

Висновки. Запропонована система дозволяє значно підвищити стійкість веб-серверу до атак ззовні шляхом контролю і аудиту записів в системних логах, завдяки якому виявляються факти приховування або видалення записів. При цьому система має наступні переваги:

- стійка до атак з боку зловмисника, який має привілеї адміністратора;
- невимоглива до обчислювальних ресурсів;
- використовує нативную систему зберігання логів;
- не потребує додаткової складної інфраструктури;
- не вимагає кваліфікованого персоналу для розгортання та експлуатації.

Література

1. Jason Andress. Foundations of Information Security: A Straightforward Introduction. – No Starch Press, 2019.
2. Michael Collins. Network Security Through Data Analysis: From Data to Action. – O'Reilly Media, 2 edition, 2017.
3. Управление логами - фундамент любой SIEM, в котором часто зияют прорехи ~ Бизнес без опасности [Електронний ресурс]. – Режим доступу : https://lukatsky.blogspot.com/2017/11/siem.html (дата звернення: 2020-06-19). – Назва з екрана.
4. Antonopoulos, A. M. Mastering Bitcoin: Programming the Open Blockchain. – O'Reilly Media, 2017