КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.26.704
УДК 004.77 (045)

Вавіленкова Анастасія Ігорівна
д.т.н., професор, завідувач кафедри кібербезпеки
Національна академія Служби безпеки України, Київ, Україна
ORCID ID: 0000-0002-9630-4951
vavilenkovaa@gmail.com

ЗАГРОЗИ ВІД ВИКОРИСТАННЯ CLOUD-СЕРВІСІВ У СФЕРІ КІБЕРБЕЗПЕКИ

Анотація. У матеріалах статті описуються переваги та недоліки використання cloud-сервісів, можливість застосування як слабких, так і сильних сторін хмарних середовищ кіберзловмисниками з метою отримання доступу до конфіденційної інформації, що зберігається у хмарі. Cloud-сервіси є інструментами, які дають змогу організувати віддалену роботу та залежно від потреб використовувати як інфраструктуру, платформу або програмне забезпечення. Незважаючи на заходи, що вживаються хмарними провайдерами для забезпечення безпеки та надійності сервісів, які вони пропонують, сфера використання cloud-сервісів є одним із потенційних слабких місць у організації кібербезпеки підприємств. Однією із тенденцій розвитку cloud-сервісів є широке використання штучного інтелекту для створення інтуїтивно зрозумілих та автоматизованих рішень, що додає у свою чергу ризиків у сфері кібербезпеки. Тому використання cloud-сервісів вимагає ретельного дослідження технологій і стратегій здійснення захисту, а також пошуку уразливостей конкретних хмарних провайдерів, на що і спрямовані матеріали даної статті. Автором описане дослідження щодо використання cloud-сервісу хмарного середовища Google Cloud з метою здійснення спроби DDoS-атаки на цілі за визначеним списком з використанням експлойту MHDDOS_PROXY. Для реалізації подібного виду атаки з метою порушення доступності атакованих ресурсів кіберзловмисники аналогічним чином можуть використати будь-який cloud-сервіс, при цьому алгоритм, на відміну від наведених вище кроків тестування, буде відрізнятися лише налаштуваннями. Експлойти, які можна знайти в мережі Інтернет, використання інфраструктури cloud-сервісів та завчасно підготовлені списки адрес можуть служити механізмом здійснення кібератак. Превентивними заходами щодо організації кібербезпеки на підприємствах та при роботі з cloud-сервісами є тонке налаштування фаєрвола, фільтрація трафіку програмними і апаратними засобами, міграція в хмару, розподіл навантаження між ресурсами та використання сканерів вразливостей.

Ключові слова: кіберзахист; cloud-сервіси; cloud-технології; хмарні обчислення; кібербезпека; VPN; інфраструктура.

ВСТУП

Хмарні технології є потужним засобом для роботи з ресурсами через мережу Інтернет, що дозволяє зберігати конфіденційну інформацію, аналізувати великі дані, розгортати віртуальні робочі столи, одночасно працювати над одним проєктомдекільком командам та, власне, здійснювати хмарні обчислення [1]. Фактично, cloud-сервіси — це онлайн-програми та інструменти, які дають змогу організувати віддалену роботу та які залежно від потреб можна використовувати як інфраструктуру, платформу або програмне забезпечення, а також пропонуються сервіси резервного копіювання та відновлення після катастроф [2].

Використання cloud-сервісів надає ряд очевидних переваг для користувачів:

– безпека даних — забезпечення надійного зберігання та обробки даних, які є однією з основних цілей кіберзловмисників;

- зниження витрат — відсутність необхідності у придбанні та обслуговуванні власного дорогого обладнання, оскільки його надає провайдер;
- додаткові функції та засоби захисту інформації — використання систем моніторингу та аналітики для виявлення внутрішніх та зовнішніх загроз;
- масштабування — можливість застосовувати стільки IT-ресурсів, скільки це потрібно конкретній компанії та відповідно знижувати або збільшувати їх масштаби залежно від потреб;
- мобільний доступ — дозволяє використовувати корпоративні дані у будь-який момент, приєднуючись з кінцевих мобільних точок чи інших пристроїв та знаходячись далеко від підприємства;
- ступінь контролю — надання доступу до конфіденційних даних, що зберігаються у хмарі, лише певним співробітникам та максимальний контроль над цим;
- можливість аварійного відновлення — cloud-сервіси дають змогу відновити роботу після відключення електроенергії чи інших непередбачуваних обставин та не втратити дані;
- технічна підтримка від провайдера — адмініструванням хмарних сервісів займається постачальник послуг.

Проте під час організації та використання засобів кіберзахисту потрібно звертати увагу на те, що кіберзловмисники можуть так само користуватися всіма перевагами cloud-сервісів у злочинних цілях, а також використовувати недоліки хмарних рішень. Наприклад, безпека даних клієнта знаходиться під загрозою, якщо хмарний провайдер розгортає хмари клієнтів на базі сумнівних дата-центрів, які не проходили сертифікацію та не використовують додаткові засоби захисту інформації. Також стабільна робота cloud-сервісів залежить від хмарного провайдера та від стабільного та швидкого Інтернет-з'єднання. Тому можна спостерігати паузи в роботі, які можуть використовувати у своїх цілях кіберзловмисники. Ще одним недоліком використання cloud-сервісів є те, що клієнт не може адмініструвати, оновлювати вбудовані програми та керувати ними.

Постановка проблеми. Незважаючи на заходи, що вживаються хмарними провайдерами для забезпечення безпеки та надійності сервісів, які вони пропонують, сфера використання cloud-сервісів є одним із потенційних слабких місць у організації кібербезпеки підприємств. Так, наприклад, власники cloud-сервісів часто розміщують декілька клієнтських інфраструктур на одному сервері, і злам однієї з них може торкнутися витоку даних з інших. Провайдери не надають клієнтам повної інформації про структуру свого хмарного середовища, а тому важко відстежити, хто має доступ до даних, та виявити слабкі місця в безпеці. Не застраховані також провайдери і від помилок персоналу та недотримання ним правил кібергігієни, зокрема, не дотримання політик безпеки, використання несанкціонованих точок доступу, володіння надмірними правами, через що хмарні сервіси можуть ставати вразливими до кібератак.

Однією із тенденцій розвитку cloud-сервісів є широке використання штучного інтелекту для створення інтуїтивно зрозумілих та автоматизованих рішень, що додає у свою чергу ризиків у сфері кібербезпеки. Тому використання cloud-сервісів вимагає ретельного дослідження технологій і стратегій здійснення захисту, а також пошуку уразливостей конкретних хмарних провайдерів, на що і спрямовані матеріали даної статті.

Аналіз останніх досліджень і публікацій. Сьогодні на ринку хмарних технологій багато провайдерів, серед яких найпопулярнішими у світі за статистикою 2023 року є Amazon Web Service (34%) [3], Microsoft Azure (21%) [4], Google Cloud (11%) [5], Alibaba Cloud (5%) [6] та IBM Cloud (3%) [7], пропонують свої послуги для користування cloud-

сервісами. Кожен з провайдерів надає хмарне сховище даних, програмні продукти для здійснення хмарних обчислень та роботи з базами даних, сервіси для роботи з великими даними, машинне навчання та ін.

Крім світових лідерів на ринку програмних послуг України є вітчизняні провайдери cloud-сервісів, такі як De Novo [8] та Giga Cloud [9], що дають змогу здійснювати міграцію великого обсягу даних, керувати хмарною інфраструктурою, проводити моніторинг, резервне копіювання даних, будувати гібридні інфраструктури.

Крім статистики популярності використання того чи іншого провайдера, на вибір хмарного середовища впливає фактор безпеки, зокрема, те, як для cloud-сервісів налаштована політика використання надійних паролів, застосування багатофакторної автентифікації, програмного забезпечення для шифрування файлів, VPN-сервісів та ін.

В основному літературні джерела, що висвітлюють тематику віртуалізації та хмарних технологій [10] – [12], містять відомості щодо видів хмарних послуг, різновидів хмарних обчислень та інструкцій з використання конкретних програних продуктів. Проте проблема дослідження cloud-сервісів на вразливості залишається актуальною та потребує ретельного аналізу.

Метою статті є висвітлення основних загроз у сфері кібербезпеки від використання cloud-сервісів та опис алгоритму пошуку уразливостей за допомогою використання хмарного середовища Google Cloud.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Як видно із попереднього аналізу, використання cloud-сервісів як надає переваги, так і має недоліки від використання у сфері кібербезпеки. Зокрема, було проведено дослідження для демонстрації потенційного здійснення атаки на систему за допомогою використання cloud-сервісів з віддалених машин (AWS, Google Cloud, Azure, Digital Ocean та ін.), з яких можна атакувати, не завантажуючи при цьому канали та обладнання кіберзловмисників. При цьому робота машин (інстансів) триває 24/7. Проте cloud-сервіси можуть заблокувати через підозру у неправомірній діяльності, але в більшості випадків блокують тільки один інстанс, а інші — ні. Саме тому даний експеримент демонструє небезпечність застосування cloud-сервісів в рамках організації заходів з кібербезпеки.

Для початку роботи кіберзловмисникам достатньо розпочати свою роботу зі створення віртуальної машини, наприклад, на хмарі від Google, зайшовши за посиланням https://cloud.google.com/ (рис. 1).

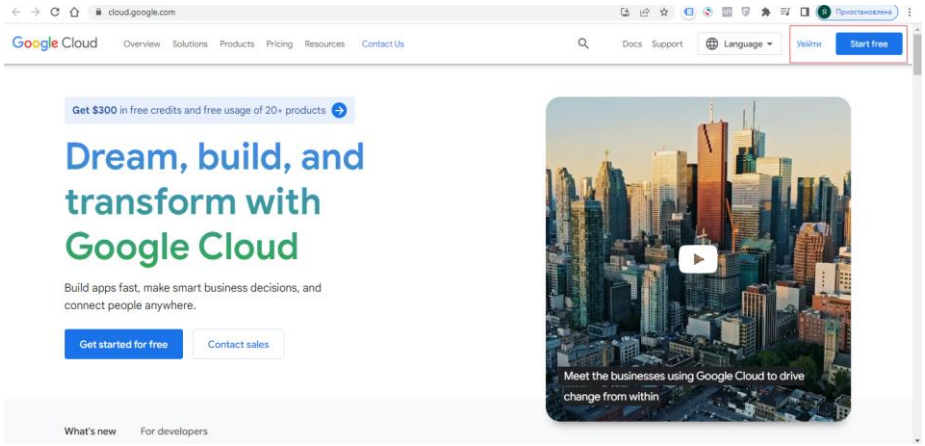

Рис. 1. Інтерфейс створення віртуальної машини на хмарі від Google

ISSN 2663 - 4023

Процес створення віртуальної машини, яку можна буде використати для здійснення атак, вимагає заповнення сторінки з особистими даними або авторизації за допомогою акаунта в Google, а також введення даних реальної розрахункової картки, після чого можна створювати інстанс.

Шляхом заповнення форми (рис. 2) створюється виділений сервер, у якому кіберзловмисник може обрати будь-який регіон, щоб не висвітлювати свою реальну країну перебування.

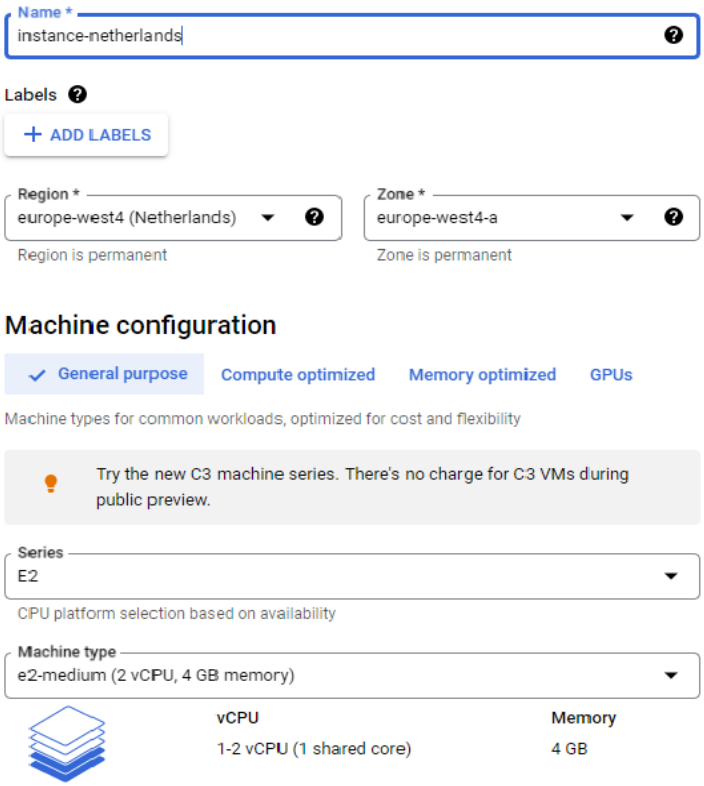

Рис. 2. Форма для створення виділеного сервісу на хмарі від Google

Після створення сервера можна розпочинати процес тестування, обираючи з'єднання через протокол SSH (рис.3), який для аутентифікації віддалених систем та забезпечення шифрування даних в рамках віддаленого доступу використовує клієнт-серверну модель [13].

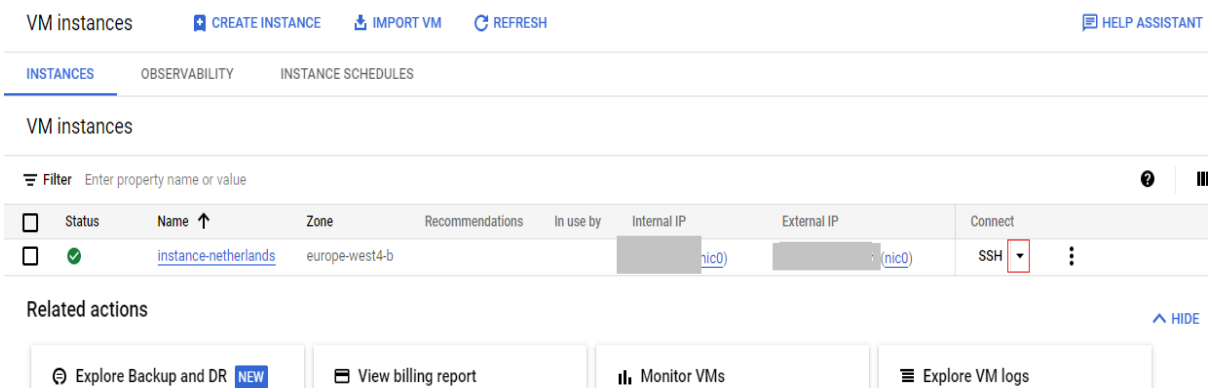

Рис. 3. Тестування через протокол SSH

ISSN 2663 - 4023

Для подальшого тестування на проникнення переходимо в командний рядок та тестуємо експлойт MHDDOS_PROXY — це надбудова над методом атаки MHDDOS [14]. Дана програма володіє більш ніж 50 способами атак, вона працює через проксі, список яких постійно оновлюється. Тепер у термінал почергово вводяться рядки коду:

```
sudo apt update -y && sudo apt install --upgrade wget screen -y
cd ~ && wget https://github.com/porthole-ascend-
cinnamon/mhddos_proxy_releases/releases/latest/download/mhddos_proxy_linu
x && chmod +x mhddos_proxy_linux
```

Небезпечними моментами у використання mhddos_proxy є:

– здійснення атаки декількох цілей з автоматичним балансуванням навантаження;
– використання різних методів для атаки та зміна їх в процесі роботи;
– відсутність необхідності використання VPN, оскільки відбувається автоматичне скачування та підбір робочих проксі для заданих цілей;
– простий та зрозумілий інтерфейс.

Після запуску команди *screen -S "mhddos_proxy" ./mhddos_proxy_linux* бачимо цілі, що атакуються, атаковані порти та методи, які використовуються (рис. 4).

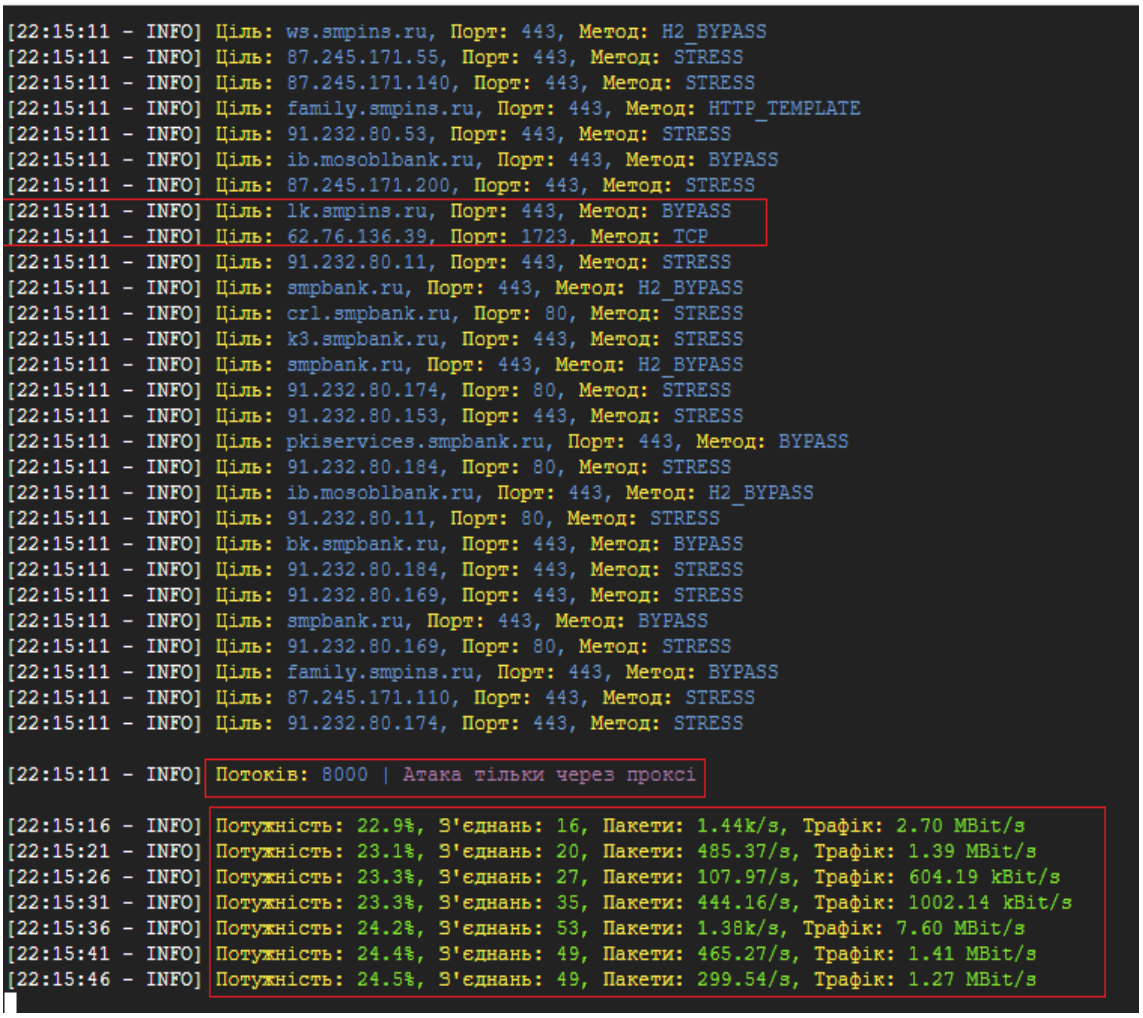

Рис. 4. Результат виконання команди screen -S "mhddos_proxy" ./mhddos_proxy_linux

Крім того, видно статистику атак. Атака розвивається з часом. На рис. 5 можна побачити, що відбувається через декілька хвилин після початку атаки.

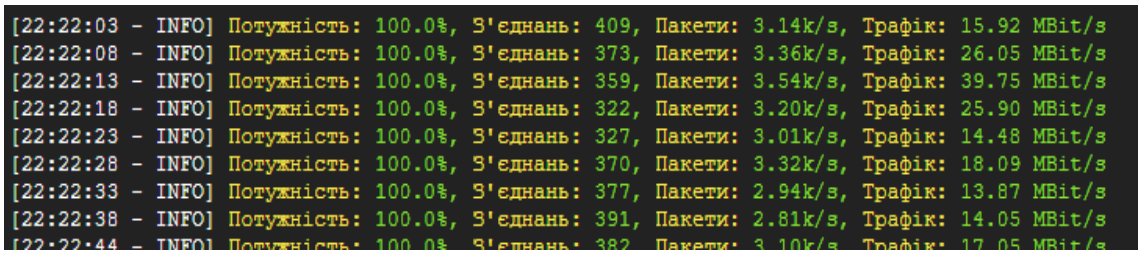

Рис. 5. Приклад розвитку атаки з часом

Отже, бачимо яскравий приклад використання cloud-сервісу хмарного середовища Google Cloud з метою здійснення спроби DDoS-атаки на цілі за визначеним списком з використанням експлойту MHDDOS_PROXY.

Для реалізації подібного виду атаки з метою порушення доступності атакованих ресурсів кіберзловмисники аналогічним чином можуть використати будь-який cloud-сервіс, при цьому алгоритм, на відміну від наведених вище кроків тестування, буде відрізнятися лише налаштуваннями.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Cloud-сервіси по великому рахунку — це окрема індустрія, яка буде продовжувати розвиватися у майбутньому, оскільки велика кількість організацій переходить на хмарні сервіси з метою пошуку більш гнучкої, ефективної та безпечної інфраструктури. Створюючи аккаунт на одній з платформ хмарних провайдерів користувач може отримувати доступ до власної інформації з будь-якої точки. Розвиток cloud-сервіси неодмінно передбачає залучення до технологій хмарних обчислень генеративних моделей штучного інтелекту, машинного навчання, інтернету речей та розумних пристроїв, що дозволить опрацьовувати та аналізувати дані швидше, а також приймати рішення на основі даних, отриманих з багатьох джерел.

За залученням до роботи cloud-сервісів нових методів роботи стоїть величезна робота з тестування на вразливості для того, щоб зробити їх більш безпечними та надійними для використання, зберігання та обробки конфіденційних даних.

Дослідження, описане в матеріалах статті показує, що cloud-сервіси можуть використовуватися як з метою організації захисту у сфері кіберпростору, так і з метою надійного приховування даних кіберзловмисників.

Експлойти, які можна знайти в мережі Інтернет, використання інфраструктури cloud-сервісів та завчасно підготовлені списки адрес можуть служити механізмом здійснення кібератак. Саме тому важливо вживати превентивних заходів щодо організації кібербезпеки на підприємствах та при роботі з cloud-сервісами, зокрема, здійснювати [14]:

- тонке налаштування фаєрвола;
- фільтрацію трафіку програмними, наприклад, Cloudflare і апаратними засобами;
- міграцію в хмару;

- створення каналу/апаратного забезпечення з надлишковою пропускною здатністю для можливості оперативно масштабувати обчислювальну здатність чи пропускну спроможність інфраструктури;
- розподіл навантаження між ресурсами;
- використання сканерів вразливостей та систем виявлення вторгнень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ilkevich, N. C. (2021). *Cloud Technologies in education. Educational and Methodological Guide for Students of the Faculty of Physics and Mathematics.*
2. Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology: NIST Special Publication.*
3. *Cloud Computing Services - Amazon Web Service (AWS).* (n. d.). https://aws.amazon.com/
4. *Perform the build in the cloud using the account Azure.* (n. d.). https://azure.microsoft.com/
5. *The new way to cloud starts here.* (n. d.). https://cloud.google.com/
6. *Alibaba Cloud Security Acceleration.* (n. d.). https://www.alibabacloud.com/en?_p_lc=7
7. *IBM Cloud: AI-ready, secure and hybrid by design.* (n. d.). https://www.ibm.com/cloud
8. *De Novo is a reference provider of VMWare cloud infrastructure.* (n. d.). https://denovo.ua/
9. *Cloud infrastructure for any tasks.* (n. d.). https://gigacloud.ua/
10. Radenković, B., & Kočović, P. (2015). From Mainframe to Cloud. *Cloud Technology.* 116–145. https://doi.org/10.4018/978-1-4666-6539-2.ch006
11. Lee, G. (2010). *Cloud Computing: Principles, Systems and Applications*. Springer.
12. Dotson, C. (2019). *Practical Cloud Security: A Guide for Secure Design and Deployment*. O'REILLY.
13. Tanenbaum, A., Wetherall, D. (2021). *Computer Networks. Global Edition*. Pearson.
14. Vavilenkova, A. (2023). *Methods and Models for Countering Cyberattacks*. Kyiv: NA SSU.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023

Anastasiia Vavilenkova
Doctor of Technical Sciences, Professor, Head of the Department of Cyber Security
National Academy of the Security Service of Ukraine, Kyiv, Ukraine
ORCID ID: 0000-0002-9630-4951
vavilenkovaa@gmail.com

THE THREATS FROM USING CLOUD SERVICES IN THE FIELD OF CYBER SECURITY

Abstract. The article discusses the advantages and disadvantages of using cloud services, as well as the potential for cybercriminals to exploit both the weaknesses and strengths of cloud environments to gain access to confidential information stored in the cloud. Cloud services are tools that enable remote work and, depending on the needs, can be utilized as infrastructure, platforms, or software. Despite the measures taken by cloud providers to ensure the security and reliability of the services they offer, the use of cloud services remains one of the potential weak points in the organization of corporate cybersecurity. One of the trends in the development of cloud services is the widespread use of artificial intelligence to create intuitive and automated solutions, which, in turn, introduces additional cybersecurity risks. Therefore, the use of cloud services requires thorough research of technologies and defense strategies, as well as the identification of vulnerabilities specific to certain cloud providers, which is the focus of this article. The author describes a study involving the use of the Google Cloud service to attempt a DDoS attack on targets from a predefined list, using the MHDDOS_PROXY exploit. To carry out such an attack, aiming to disrupt the availability of targeted resources, cybercriminals can similarly use any cloud service. However, the attack algorithm will only differ in its configuration settings compared to the steps outlined in the testing process. Exploits, available on the internet, the use of cloud service infrastructure, and precompiled lists of addresses can serve as mechanisms for executing cyberattacks. Preventive measures for organizing cybersecurity in enterprises and when working with cloud services include fine-tuning firewalls, filtering traffic with software and hardware tools, cloud migration, load balancing between resources, and the use of vulnerability scanners.

Keywords: Cyber Protection; Cloud Services; Cloud Technologies; Cloud Computing; Cyber Security; VPN; Infrastructure.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Ilkevich, N. C. (2021). *Cloud Technologies in education. Educational and Methodological Guide for Students of the Faculty of Physics and Mathematics.*
2. Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology: NIST Special Publication.*
3. *Cloud Computing Services - Amazon Web Service (AWS).* (n. d.). https://aws.amazon.com/
4. *Perform the build in the cloud using the account Azure.* (n. d.). https://azure.microsoft.com/
5. *The new way to cloud starts here.* (n. d.). https://cloud.google.com/
6. *Alibaba Cloud Security Acceleration.* (n. d.). https://www.alibabacloud.com/en?_p_lc=7
7. *IBM Cloud: AI-ready, secure and hybrid by design.* (n. d.). https://www.ibm.com/cloud
8. *De Novo is a reference provider of VMWare cloud infrastructure*. (n. d.). https://denovo.ua/
9. *Cloud infrastructure for any tasks.* (n. d.). https://gigacloud.ua/
10. Radenković, B., & Kočović, P. (2015). From Mainframe to Cloud. *Cloud Technology.* 116–145. https://doi.org/10.4018/978-1-4666-6539-2.ch006
11. Lee, G. (2010). *Cloud Computing: Principles, Systems and Applications*. Springer.
12. Dotson, C. (2019). *Practical Cloud Security: A Guide for Secure Design and Deployment*. O'REILLY.
13. Tanenbaum, A., Wetherall, D. (2021). *Computer Networks. Global Edition*. Pearson.
14. Vavilenkova, A. (2023). *Methods and Models for Countering Cyberattacks*. Kyiv: NA SSU.