**Міністерство освіти та науки України**

**Державний торговельно-економічний університет**

***Кафедра інженерії програмного забезпечення та кібербезпеки***

**ЗВІТ**

***З ЛАБОРАТОРНОЇ РОБОТИ № 8***

*з дисципліни*

**«ОСНОВИ КІБЕРБЕЗПЕКИ»**

**НА ТЕМУ:**

ІНЦИДЕНТИ ПОРУШЕННЯ БЕЗПЕКИ

(назва теми)

**Виконала:** студентка факультету інформаційних технологій

Групи 4 курсу 3

Авєріна Наталія Ігорівна

**Викладач:** Ковальова Людмила Ігорівна

Київ 2024

**Лабораторна робота №8**

**Тема**: інциденти порушення безпеки

**Цілі та задачі**: Знайти інформацію та прочитати про деякі нещодавні порушення безпеки.

**Хід роботи:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Дата інциденту | Постраждала організація | Кількість постраждалих? Що було зроблено? | Які експлойти використовувалися? Яким чином налагоджено захист у Вас? | Джерело |
| Грудень 2013 | Neiman Marcus Group | Хакерам вдалося отримати доступ приблизно до 5200 облікових записів. Зловмисники використовували приблизно 70 зламаних облікових записів для здійснення несанкціонованих покупок на веб-сайтах Neiman Marcus | Інформація про експлойти обмежена. Після інциденту Neiman Marcus Group провела ретельний аналіз безпеки своїх мереж і систем, вдосконаливши заходи захисту, включаючи шифрування даних та покращення моніторингу мережі. | [Securityweek](https://www.securityweek.com/neiman-marcus-says-hackers-breached-customer-accounts) |
| 2016 | Centene | Зникли безвісти 6 жорстких дисків, на яких містяться дані про стан здоров’я приблизно 950 тисяч людей. | Можливо, що зловмисники скористалися фізичним доступом до систем або слабкими точками у безпеці, щоб отримати доступ до даних на дисках. | [managedhealthcareexecutive.com](https://www.managedhealthcareexecutive.com/view/centene-data-breach-underscores-escalating-problem) |
| 2017 | Equifax | Хакери використали вразливість в веб-додатку Equifax, щоб отримати доступ до особистої інформації близько 147 мільйонів осіб, включаючи інформацію про кредитні картки та соціальні страхові номери. | Хакери використали вразливість в Apache Struts. Після інциденту Equifax зробила значні інвестиції у покращення кібербезпеки, зміцнюючи мережу моніторингу та вдосконалюючи процедури виявлення і реагування на інциденти. | [Bloomberg](https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros) |
| 2018 | Marriott International | Було виявлено, що хакери отримали доступ до особистих даних понад 500 мільйонів клієнтів, включаючи імена, адреси електронної пошти, номери телефонів та інші дані. | Хакери використовували низку атак, включаючи атаку на систему бронювання готелів Marriott, щоб отримати доступ до бази даних клієнтів. Marriott зміцнила кібербезпеку, включаючи впровадження більш суворих процедур перевірки безпеки та покращення систем моніторингу даних. | [Reuters](https://www.reuters.com/article/idUSKCN1O02VG/#:~:text=(Reuters)%20%2D%20Marriott%20International%20said,at%20%24117%20in%20premarket%20trading.) |
| 2020 | SolarWinds | Зловмисники використали вразливість у програмному забезпеченні SolarWinds для внесення змін до оновлень програми, що призвело до компрометації десятків тисяч компаній та установ, включаючи урядові агентства США. | Хакери використовували вразливість у програмному забезпеченні SolarWinds Orion для внесення змін до оновлень програми та впровадження шкідливого коду. Після інциденту SolarWinds розробила нові процедури безпеки, включаючи більш строгий контроль коду та покращення систем виявлення загроз. | Звіт компанії SolarWinds, [businessinsider](https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12) |

**Висновок**: в ході виконання лабораторних робіт було знайдено та проаналізовано інформацію по порушення безпеки таких організацій, як Neiman Marcus Group, Centene, Equifax, Marriott International та SolarWinds. Запобігання подібним порушенням безпеки може включати ряд заходів для забезпечення безпеки особистої інформації та даних. Наприклад: використання сильних складних паролей, двоетапної автентифікації, вчасне оновлення ПЗ, обережність в мережі та обов’язкове резервне копіювання даних.