ІПЗ-33\1 Гоша Давід Олександрович

Лабораторна №8

Мета роботи: Знайти інформацію та прочитати про деякі нещодавні порушення безпеки.

Дослідження порушення безпеки. Що пропало? Що було зроблено?

Дата інциденту	Постраждала організація	Кількість постраждалих. Що пропало? Що було зроблено?	Які експлойти використовувалися? Яким чином захистити себе?	Посилання на джерело
18:12 / 10 листопад, 2022	Неназвана європейська дипломатична установа	APT29 побували в мережі жертви, виконавши в системі Active Directory безліч LDAP-запитів з нетиповими властивостями.	CVE-2022-30170. Mandiant заявила, що дослідження "дає уявлення про те, чому APT29 активно запитує відповідні атрибути LDAP в Active Directory", і закликала організації якнайшвидше застосувати вересневі виправлення.	https://www.securitylab.ru/news/534731.php
15:00 / 7 листопада, 2022	DSB – найбільша залізнична компанія Данії	Потяги по всій країні зупинилися вранці і знову почали ходити лише о першій годині дня, DSB очікує, що прикордонні поїзди та потяги далекого прямування завтра не ходитимуть за розкладом	Помилку у критично важливій для безпеки IT-системі під назвою "Den Digitale Rygsæk 2 Подробнее:	https://www.securitylab.ru/news/534679.php
09:19 / 11 жовтня,	Транспортні та	Програма Prestige шифрує дані жертви та	-	https://www.securitylab.ru/

2022	логістичні компанії Польщі та України Подробне: https://www.securitylab.ru/news/534391.php	залишає записку з вимогою викупу, в якій йдеться про те, що дані можна розблокувати лише при покупці спеціального інструменту для розшифровки.		news/534391.php
07:51 / 11 жовтня, 2022	Сайти аеропорті в США	Атаки порушили доступ до сайтів, які інформують про завантаженість та час очікування в аеропортах. Проте дії хакерів не торкнулися управління повітряним рухом, транспортної безпеки та лінії зв'язку з літаками.	За повідомленням CNN, у 14 аеропортах, що зазнали DDoS-атаки, не було зареєстровано ознак впливу на повітряні перевезення. Жодна з основних систем була зламана. Журналісти впевнені, що аеропорти були у списку цілей кіберголоворізів Killnet , яка оприлюднила список атакованих аеропортів.	https://www.securitylab.ru/news/534306.php?r=2
11:10 / 10 жовтня, 2022	Розумні системи освітлення від Ikea Подробне: https://www.securitylab.ru/news/534294.php	Дослідники із Synopsis продемонстрували , як зловмисник може отримати контроль над лампочками в розумній системі освітлення ТРОДФРІ від Ikea.	Для цього хакеру достатньо кілька разів відправити один і той же неправильно сформований кадр Zigbee (IEEE 802.15.4), а потім скористатися двома вразливістю (що відстежуються під ідентифікаторами CVE-2022-39064 та CVE-2022-39065)	https://www.securitylab.ru/news/534294.php

Висновки:

Проаналізувавши найпоширеніші форми кібератак, до яких вдаються хакери для викрадення персональних даних або коштів користувачів Інтернету, спеціалісти компанії Hacken склали список із 5 базових правил особистої безпеки в Інтернеті:

- Управління паролями: для кожного облікового запису користувачам слід використовувати різні надійні паролі та не повідомляти їх як стороннім особам, так і родичам чи колегам, і не зберігати їх у браузері. Окрім цього, навіть надійні паролі слід регулярно оновлювати. У випадку необхідності використовувати велику кількість паролів, користувачам слід встановити спеціалізовані програми для управління паролями;
- Використання двофакторної або багатофакторної автентифікації для входу в облікові записи, при чому для двофакторної автентифікації використання СМС-повідомлень не є надійним методом;
- Максимальне уникнення використання публічних мереж Wi-Fi. При необхідності піключення до публічних мереж Wi-Fi користувачам слід утриматись від проведення фінансових операцій чи здійснення входу в облікові записи, які містять великий масив персональних даних;
- Використання ліцензованих антивірусних програм для регулярної перевірки особистих пристроїв на наявність шкідливого програмного забезпечення. Для мінімізації ризиків користувачам слід уникати використання безкоштовних антивірусних програм, оскільки хакери часто саме під їх виглядом проникають у пристрої жертв;
- Контроль за інформацією, яку користувач надає у мережі Інтернет. Користувачу слід надавати свої персональні дані лише у випадку 100% впевненості у тому, що сторона, яка їх вимагає, є тим, за кого себе видає. Наприклад, при отриманні повідомлення із банку на електронну пошту з вимогою здійснити конкретні дії, у безпечності яких користувач не є певним, йому слід зателефонувати на гарячу лінію банку для перевірки інформації. У соціальних мережах користувачам не слід розголошувати інформацію про свій фінансовий стан, купівельні звички, уподобання в Інтернеті та інші факти, які можуть бути використані кіберзлочинцями.

Загалом, дотримання користувачами базових правил безпечної повідінки у мережі Інтернет зробить їх непростою мішенню для кіберзлочинців. Спеціалісти компанії Hacken відзначають наступну закономірність: кіберзлочинці намагаються уникати атак на користувачів, які мають хоча б базове розуміння принципів кібербезпеки. Фактично,

хакери діють за принципом найменшого супротиву, а тому дотримання користувачами правил безпечної поведінки в Інтернеті буде кроком на випередження у боротьбі з кіберзлочинцями за цифрову безпеку.

Тести

1. Б
2. А, Б
3. В
4. Б
5. В
6. А, Б, В
7. А, Б
8. В, Д
9. А
10. Б