ОЦІНКА ВРАЗЛИВОСТІ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ ДЛЯ АТАК З ВИКОРИСТАННЯМ ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ

Снігуров А.В., Сацюк Д.В.

Кафедра «Інфокомунікаційної інженерії»
ім. В.В. Поповського», ХНУРЕ, Україна

E-mail: arkadii.snihurov@nure.ua
E-mail: denys.satsiuk@nure.ua

Abstract

The report analyzes the situation with information security of electronic document management systems, examples of large-scale attacks on electronic document management systems in Ukraine are given. The main objective of the report is analyzes the information attack on electronic document management systems using compromising emanations, presents the features of the implementation of this attack on electronic document management systems, assesses the level of vulnerabilities of these systems using the method of CVSSv3.1.

Сучасні системи електронного документообігу (СЕД) – це організаційно-технічні системи, що забезпечують процес створення, управління доступом і поширення електронних документів у комп'ютерних мережах, а також забезпечують контроль за потоками документів в організації [1]. На даний час існує ряд СЕД, до яких можна віднести такі як «FossDoc», «Док Проф», «МЕГАПОЛІС. Документообіг», «1С», «M.E.Doc», «АСКОД», El-Doc, 1С:Документообіг, "Діло" та інші. До основних переваг сучасних систем електронного документообігу належать скорочення часу доступу до інформації; скорочення дублювання документів та інформації; спрощення доступу до даних, автоматизація бізнес-процесів тощо.

Структура СЕД відрізняється у різних розробників таких систем, але є загальні елементи. До них відносяться сервер додатків, сервер баз даних, web-сервер, робочі місця адміністратора та користувачів СЕД. Дані елементи СЕД поєднані локальною інфокомунікаційною мережею компанії.

Дослідження питань побудови і функціонування сучасних СЕД неможливо без аналізу стану інформаційної безпеки даних систем. Проблеми інформаційної безпеки сучасних СЕД загострилася в останні роки після здійснення масштабних кібератак на ці системи [2,3]. Як приклад, можна навести атаку шифрувальника NotPetya на СЕД «M.E.Doc», яка відбулася 27 червня 2017 року, та атаку на СЕД «АСКОД», яка відбулася у лютому 2021 року. Щодо атаки шифрувальника NotPetya встановлено, що завантаження шифрувальника відбувалося під час оновлення програмного забезпечення «СЕД M.E.Doc». При цьому шифрувальник-вимагач не тільки шифрував інформацію, але і знищував MBR жорстких дисків та намагався розповсюджуватися в комп'ютерній мережі [4]. Щодо атаки на СЕД «АСКОД» зловмисники надсилали інфіковані документи до організацій, які використовували дану систему. Документи, які надсилались містили шкідливий код для експлуатації відомої вразливості «Microsoft Office» CVE-2017-0199, яка надає змогу зловмиснику виконати довільний код на пристрої користувача при відкритті інфікованого файлу [5].

Тому завдання розробки механізмів захисту сучасних СЕД є актуальним. При цьому необхідно зазначити, що СЕД – це організаційно-технічна система, в якій є як різні технічні елементи зі своїми вразливостями, так і персонал компаній, який експлуатує такі системи. Тому питання забезпечення інформаційної безпеки СЕД має вирішуватися комплексно з урахуванням

усіх потенційних загроз таким системам і потенційним вразливостям усіх їх елементів. В доповіді проведений аналіз такої загрози для СЕД, яка в класичній літературі з інформаційної безпеки називається як витік інформації через побічні електромагнітні випромінювання та наводки (ПЕМВН). В англомовній літературі фігурує термін «compromising emanations». Також використовується термін TEMPEST - Transient Electromagnetic Pulse Emanation Standard.

В 90-х роках 20–го сторіччя даний канал витоку інформації досліджувався багатьма дослідниками та структурами, були напрацьовані механізми захисту, такі як використання генераторів електромагнітних перешкод, екранування, заземлення елементів техніки та екранів та інші. На початку 21–го сторіччя у зв'язку з масованим поширенням кібератак через комп'ютерні мережі, розповсюдження шкідливих програм, розуміння небезпеки даного каналу витоку інформації почало відходити на другий план. Але на даний час даний канал витоку інформації почав вважатися як один з найнебезпечніших і при оцінці ризиків інформаційної безпеки та вибору комплексу захисту СЕД має бути врахованим.

Небезпека даного каналу витоку інформації для СЕД полягає в особливостях структури і порядку функціонування даних систем. Відомо, що інформативні побічні електромагнітні випромінювання виникають при введенні даних з клавіатури, виведення інформації на монітор, запису інформації на магнітні запам'ятовуючі пристрої, зчитування інформації з магнітних запам'ятовуючих пристроїв, передачі даних в каналах зв'язку, виведення даних на периферійні пристрої друку - принтери, плоттери; запис даних зі сканерів на магнітний носій та інше. Тобто даний канал витоку інформації виникає при управлінні системою електронного документообігу з робочого місця адміністратора, при функціонування робочих місць користувачів, при пересиланні електронних документів в системі. Наприклад, перехоплення зловмисником логіна та паролю адміністратора СЕД може призвести до взяття їм під контроль цієї системи, завантаження шкідливої програми в систему більш простим шляхом, ніж це відбулося під час атак на СЕД «M.E.Doc» та АСКОД, відключення системи антивірусного захисту. Існують дослідження щодо комбінації даного способу атаки та використання шкідливих програм (Маркус Г. Кун і Росс Дж. Андерсон - Markus G. Kuhn, Ross J. Anderson) – Soft Tempest. При цьому необхідно розуміти і складності для зловмисників такого способу атаки – необхідність мати складне обладнання та необхідну кваліфікацію, неможливість віддаленого доступу (зловмисник має проникнути в зону прийняття електромагнітного випромінювання, яка може бути невеликою і становити десятки метрів).

Проаналізуємо рівень вразливості СЕД для атаки через побічні електромагнітні випромінювання та наводки. Для оцінки вразливості будемо використовувати методику CVSSv3.1, яка є дуже популярною для оцінки вразливостей інформаційних систем [6].

В стандарті NIST CVSS v3.1 критичність вразливостей оцінюється на основі декількох глобальних груп метрик:

- базові метрики (вектор доступу - Attack Vector, складність атаки -Attack Complexity, обов'язкові привілеї - Privileges Required, взаємодія з користувачем - User Interaction, рівень збитків – конфіденційності, цілісності, доступності) – постійні та не змінюються з часом;
- часові метрики (зрілість Експлойт-коду - ExploitCodeMaturity, рівень відновлення - RemediationLevel, повідомлення про довіру - ReportConfidence) – не постійні та можуть змінюватися з часом;
- метрики навколишнього середовища (вимоги безпеки - Security Requirements) – дозволяють деталізувати базові та часові метрики та врахувати особливості середовища в якому знаходиться вразливість, що підлягає оцінці.

Проведемо аналіз вразливості СЕД від атаки ПЕМВН з використанням базових метрик. Результати оцінки приведені в таблиці 1.

Проведемо пояснення показників даної групи метрики.

Вектор доступу (Attack Vector).

Методика передбачає кілька потенційних варіантів дій зловмисника:

- потребується фізичний доступ - зловмисникові потрібен безпосередній фізичний доступ до об'єкта, на якому розташована вразливість (значення показника метрики - 0,2);
- потребується локальний доступ - зловмисник експлуатує вразливість за допомогою локального доступу, вразливий компонент не прив'язується до стеку мережі – (значення показника метрики - 0,55);

- можливий доступ із суміжної мережі - атака обмежена однією спільною фізичною (наприклад, Bluetooth, IEEE 802.11) або логічною (наприклад, локальною IP-підмережею) мережею, і не може бути виконана через границю шару OSI (наприклад, маршрутизатор) (значення показника метрики - 0,62),
- можливий доступ з будь-якої мережі - зловмисник може атакувати віддалено через OSI layer 3 (мережний рівень) (значення показника метрики - 0,85).

Тобто відповідно до даної методики дії зловмисника більш небезпечні, якщо він має можливість реалізації віддаленої атаки на систему. Для ситуації, що розглядається в доповіді зловмиснику потрібен локальний доступ.

Таблиця 1. Оцінка вразливості СЕД по базовим метрикам стандарту NIST CVSS v3.1

Значення	Опис	Числова характеристика параметра
Вектор доступу (Attack Vector)		
Потребується локальний доступ	Зловмисник має проникнути в зону R2 для атаки з використанням інформативних побічних електромагнітних випромінювань (ПЕМВ) або в зону розміщення систем електроживлення, заземлення, інших провідників, де рівень наводки ПЕМВ дозволяють здійснити перехоплення інформативного сигналу	0,55
Складність атаки (Attack Complexity)		
Висока	Успішність атаки вимагає від злочинця зрозуміти розміщення елементів СЕД, які можуть бути об'єктом атаки (наприклад розміщення робочого місця адміністратора СЕД)	0,44
Обов'язкові привілеї (Privileges Required)		
Висока	Враховуючи невеликий розмір зони, в якій зловмисник може перехопити електромагнітні або електричні сигнали з необхідними показниками якості, в значній кількості випадків зловмиснику необхідне проникнення в організацію, яка використовує СЕД	0,62
Взаємодія з користувачем (User Interaction)		
Немає	Вразливість системи може експлуатуватися зловмисником без необхідності дій будь-якого іншого (крім зловмисника) окремого користувача (або процесу, ініційованого користувачем)	0,85
Збиток конфіденційності (збиток цілісності та доступності відсутній)		
Високий	Існує можливість повного розкриття конфіденційної інформації	0,56

Складність атаки (Attack Complexity).

В метриці методики CVSS v3.1 існують наступні значення даного параметра:

- Низька - немає особливих умов для доступу зловмисником до вразливості (наприклад, коли система доступна багатьом користувачам одночасно або коли вразлива конфігурація працює на безлічі вузлів мережі) (значення показника метрики - 0,77);
- Висока - успішність атаки вимагає від злочинця здійснювати певні вимірювані зусилля для підготовки чи виконання атаки. Наприклад проведення розвідки системи захисту (значення показника метрики - 0,44).

Так як зловмисник має провести попередню розвідку для використання атаки через ПЕВМН, даний показник приймаємо рівним – Висока.

Обов'язкові привілеї (Privileges Required).

В метриці методики CVSS v3.1 існують наступні значення даного параметра:

- Немає - зловмиснику не потрібна авторизація перед атакою (значення показника метрики - 0,27);
- Висока - зловмиснику потрібні привілеї, які надають основні можливості користувача, (значення показника метрики - 0,62);
- Низька - зловмисник авторизований, тобто вимагає привілеїв, які забезпечують значний (наприклад, адміністративний) контроль, (значення показника метрики - 0,85).

Зловмисник має проникнути в зону, де він може перехопити сигнали елементів СЕД. У зв'язку з невеликим рівнем даних сигналів в значній кількості випадків проникнення має бути на територію організації, яка експлуатує СЕД (але в ряді випадків можливе перехоплення сигналів елементів СЕД за межами контрольованої зони). Відповідно до цього приймаємо значення даного показника – Висока.

Взаємодія з користувачем (User Interaction).

В метриці методики CVSS v3.1 існують наступні значення даного параметра:

- Потрібно - для успішної експлуатації уразливості зловмисником будь-якому іншому користувачеві (крім зловмисника) потрібно вжити певні дії, перш ніж вразливість може бути використана, (значення показника метрики - 0,62);
- Немає - вразливість системи може експлуатуватися зловмисником без необхідності дій будь-якого іншого (крім зловмисника) окремого користувача (або процесу, ініційованого користувачем), (значення показника метрики - 0,85).

Для експлуатації вразливості через атаку з використанням ПЕМВН будь-яка взаємодія з користувачем не потрібна, тому приймаємо значення даного показника – Немає.

Проведемо оцінку рівня вразливості СЕД для даної атаки з використанням онлайн калькулятора CVSS v3.1 [7]. Результати даної оцінки представлені на рис.1.

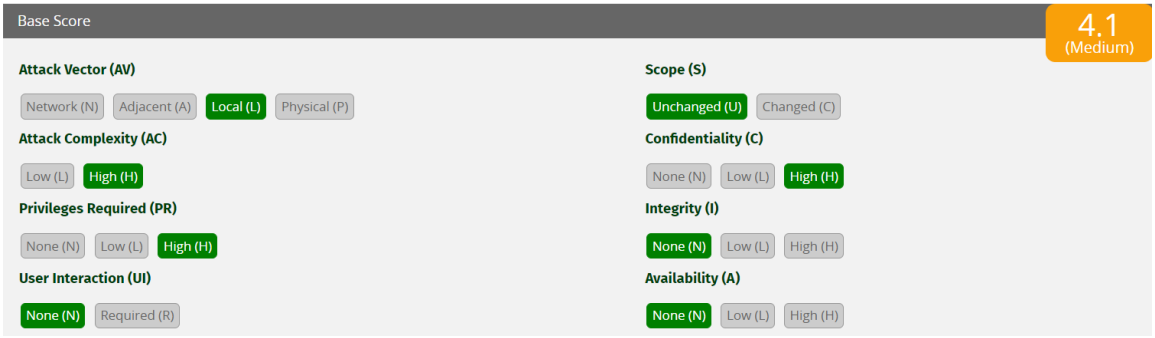

Рис. 1. Результати розрахунку рівня вразливості СЕД до атаки через використання побічних електромагнітних випромінювань та наводок

Можна побачити, що відповідно до підходу методики CVSS v3.1 рівень вразливості системи 4.1, тобто середній. Таким чином, використання методики CVSS v3.1 дозволяє оцінити рівні вразливостей СЕД для атак різного типу для подальшої оцінки ризиків інформаційної безпеки даних систем.

Література:

1. Радченко С.В. Особливості систем електронного документообігу в державних органах України [Електронний ресурс] / С.В.Радченко // Архіви України. – 2013. - №4. С. 39-53. – Режим доступу: http://nbuv.gov.ua/UJRN/ay_2013_4_3 .

2. НКЦК при РНБО України оновив інформацію щодо кібератаки на систему документообігу державних органів [Електронний ресурс]/ РНБО України // 24 лютого 2021 р. – Режим доступу: https://www.rnbo.gov.ua/ua/Diialnist/4824.html?PRINT.

3. Поновлення кібератак з використанням ШПЗ Pterodo хакерського угрупування Armageddon/Gamaredon \CERT-UA. [Електронний ресурс]. - 2021. - Режим доступу: https://cert.gov.ua/article/10702.

4. Snihurov A., Shulhin O., Balashov V. Experimental Studies of Ransomware for Developing Cybersecurity Measures // Proceedings of International Scientific-Practical Conference on Problems of Infocommunications Science and Technology. PIC S and T 2018, Kharkiv, 2018. P. 691-695.

5 National Vulnerability Database. [Електронний ресурс]. Режим доступу: https://nvd.nist.gov/.

6. Common Vulnerability Scoring System. [Електронний ресурс]. Режим доступу: https://www.first.org/cvss/.

7. Common Vulnerability Scoring System Version 3.1 Calculator. [Електронний ресурс]. Режим доступу: https://www.first.org/cvss/calculator/3.1.