

CASE-2025-PRIJ-01

DIGITÁLNA FORENZNÁ ANALÝZA

Podozrenie z manipulácie databázy prijímacieho konania

ZÁVEREČNÁ FORENZNÁ SPRÁVA · 06. PREZENTAČNÁ FÁZA

VYPRACOVAL

Ľubomír Zubák

Univerzita sv. Cyrila a Metoda v Trnave · Fakulta prírodných vied

AKADEMICKÝ ROK

2025 / 2026

Semestrálna práca · DFA

Obsah prezentácie

01

Prípád a úlohy vyšetrovania

Kontext, zadanie a hypotézy

02

Zaistenie dôkazov a Chain of Custody

Zariadenia, integrita, reťazec zodpovednosti

03

Používané nástroje a metódy

FTK Imager, Autopsy, DB Browser, HxD

04

Nálezy a digitálne stopy

USB obraz, RAM, databázové logy, časová os

05

Vyhodnotenie hypotéz

Potvrdené / zamietnuté hypotézy

06

Záver a odporúčania

Identifikácia páchatela, opatrenia

Prípad: Manipulácia prijímacieho konania

ZHRNUTIE PRÍPADU

Na univerzite vzniklo podozrenie na manipuláciu výsledkov prijímacieho konania po sťažnosti uchádzača, ktorý si po teste odfotil svoje odpovede a po zverejnení výsledkov zistil nesúlad v bodovom hodnotení.

Interná kontrola preukázala, že databázový záznam bol upravený **tri dni pred zverejnením** výsledkov, a to z interného administrátorského účtu.

V kancelárii študijného oddelenia bol zaistený **pracovný notebook referenta** a **USB zariadenie**.

CIELE VYŠETROVANIA

- ▶ Identifikovať osobu zodpovednú za úpravu
- ▶ Rekonštruovať časovú os incidentu
- ▶ Overiť použitie externého USB nosiča
- ▶ Vypracovať forenznú správu pre disciplinárne konanie

WHO

Referent študijného oddelenia / IT admin / externý útočník

WHAT

Neoprávnená úprava databázy prijímacieho konania

WHEN

29. 8. 2025 • 3 dni pred zverejnením výsledkov

WHERE

Pracovná stanica referenta + interný DB server univerzity

WHY

Finančný prospech / kompromitácia účtu

HOW

Login + manuálna SQL úprava + USB ako pomocný nosič

Tri pracovné hypotézy

H1

**Úmyselná manipulácia
referentom**

Referent študijného oddelenia úmyselne upravil
výsledky výmenou za finančnú odmenu.

H2

**Kompromitácia účtu / externý
útočník**

Administrátorský účet bol kompromitovaný
škodlivým softvérom alebo neoprávneným
externým prístupom.

H3

USB ako pomocný nosič

USB zariadenie bolo použité ako pomocný nosič na
prenos SQL skriptu, exportu a iných súborov.

Zaistené zariadenia a integrita dôkazov

ZAISTENÉ ZARIADENIA

[01] Pracovný notebook referenta

Model: Lenovo ThinkPad E14 Gen 4
Operačný systém: Windows 10 Pro
Procesor: Intel Core i5-1235U
Operačná pamäť: 16 GB DDR4
Úložisko: 512 GB SSD NVMe
Rozhrania: USB 3.0, USB-C, HDMI, Ethernet
Rýchlosť čítania úložiska: približne 3000 MB/s
Rýchlosť zápisu úložiska: približne 1800 MB/s
Prístupová doba SSD: menej ako 0,1 ms



Pracovný notebook referenta študijného oddelenia predstavuje hlavné zariadenie, na ktorom mohlo dôjsť k otvoreniu databázy, úprave záznamov a vytvoreniu exportu výsledkov.

Číslo:	01	Typ súboru:	Disk Image	Obnovený súbor:	Nie	Veľkosť:	512GB
Popis prípadu:	Manipulácia výsledkov prijímacieho konania						
Názov súboru:	notebook_referent.E01						
Miesto získania digitálnej stopy:	Pracovný notebook referenta študijného oddelenia – kancelária študijného oddelenia univerzity						
Poznámky:	Diskový obraz zariadenia bol vytvorený pomocou nástroja FTK Imager. Pred vytvorením obrazu bol notebook odpojený od siete, aby sa zabránilo zmene dát. Originálne zariadenie bolo následne zabezpečené a uložené v zabezpečenom priestore pre digitálne dôkazy.						
Časové pečiatky							
Access:	03.09.2025 09:12:45	Modify:	03.09.2025 09:38:20		Change:	03.09.2025 09:44:11	
Digitálny odtlačok (heš)	MD5	d41d8cd98f00b204e9800998ecf8427e					
	SHA1	da39a3ee5e6b4b0d3255bfef95601890afd80709					
Časová pečiatka	Akcia vykonaná s digitálnou stopou						
03.09.2025 09:12	Zaistenie pracovného notebooku referenta študijného oddelenia						
03.09.2025 09:20	Dokumentovanie zariadenia a evidovanie dôkazu						
03.09.2025 09:30	Vytvorenie bitovej kópie disku pomocou FTK Imager						
03.09.2025 09:38	Dokončenie vytvárania diskového obrazu						
03.09.2025 09:44	Overenie hash hodnôt a uloženie dôkazu do zabezpečeného úložiska						

Zaistené zariadenia a integrita dôkazov

ZAISTENÉ ZARIADENIA

[02] USB flash disk

Typ zariadenia: USB flash disk
Model: Kingston DataTraveler 8GB
Kapacita: 8 GB
Rozhranie: USB 2.0 / USB 3.0
Súborový systém: FAT32
Rýchlosť čítania: približne 20–80 MB/s
Rýchlosť zápisu: približne 5–20 MB/s
Prístupová doba: menej ako 1 ms
Typ pamäte: NAND Flash
Hmotnosť: približne 10 g
Farba: čierna / čierno-biela
Sériové číslo: 0B8E6B0166E7



Pri vyšetrowaní bude skúmané, či sa na USB zariadení nachádzali súbory typu .sql, .csv, .txt alebo iné pomocné dáta, ktoré mohli byť použité pri manipulácii databázy. Dôležitá bude aj analýza časových pečiatok súborov, histórie pripojenia zariadenia a prípadnej súvislosti medzi použitím USB a úpravou databázového záznamu.

Číslo:	02	Typ súboru:	Disk Image (.E01)	Obnovený súbor:	Nie	Veľkosť:	8 GB
Popis prípadu:	Manipulácia výsledkov prijímacieho konania						
Názov súboru:	usb_device.E01						
Miesto získania digitálnej stopy:	USB kľúč nájdený v kancelárii študijného oddelenia na pracovisku referenta						
Poznámky:	USB zariadenie bolo zaistené na mieste pracoviska referenta študijného oddelenia. Pred analýzou bol vytvorený forenzný obraz zariadenia pomocou nástroja FTK Imager. Originálne zariadenie bolo následne zabezpečené a uložené v prostredí určenom na uchovávanie digitálnych dôkazov.						
Časové pečiatky							
Access:	03.09.2025 10:10:15		Modify:	03.09.2025 10:25:47		Change:	03.09.2025 10:30:12
Digitálny odtlačok (heš)	MD5	b2706fbc7c02170b62b098fc26f57be1					
	SHA1	7cc5624e53c370be2dc43e6144fc87442471a7a2					
Časová pečiatka							
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
03.09.2025 10:10		Zaistenie USB zariadenia v kancelárii študijného oddelenia					
03.09.2025 10:20		Dokumentovanie zariadenia (fotografia a označenie dôkazu)					
03.09.2025 10:25		Vytvorenie bitovej kópie USB zariadenia pomocou FTK Imager					
03.09.2025 10:35		Overenie hash hodnôt a uloženie dôkazu do zabezpečeného úložiska					

Použíte forenzné nástroje

FTK Imager

ZAISŤOVANIE

Imaging & integrita

Vytvorenie bitových kópií zariadení a obrazu RAM. Výpočet a overenie hash hodnôt (MD5/SHA-1).

Autopsy

ANALÝZA / EXTRAKCIA

Súborová analýza

Komplexná analýza obrazu USB. Prehľadávanie alokovaných aj dealokovaných súborov, obnova z unallocated space.

HxD

ANALÝZA

Hex / RAM analýza

Analýza RAM image, vyhľadávanie textových reťazcov (názvy súborov, SQL príkazov, webovej aktivity).

Nálezy a digitálne stopy

SÚBOROVÝ SYSTÉM USB OBRAZU

FAT32

Obraz: dfazubak.001 • Raw image (DD) • 15 974 400 sektorov × 512 B

ALOKOVANÉ (existujúce)

prijimacky_case_ascii.db

VEĽKOSŤ **12 288 B**

databáza prijímacieho konania

uchadzaci_export_ascii.csv

VEĽKOSŤ **881 B**

exportované výsledky

komunikacia.txt

VEĽKOSŤ **572 B**

lokálne uložený záznam komunikácie medzi dvoma osobami

DEALOKOVANÉ (obnovené z unallocated space)

modify_scores.sql.txt

VEĽKOSŤ **173 B**

SQL skript úpravy bodového hodnotenia

prijímačky.txt

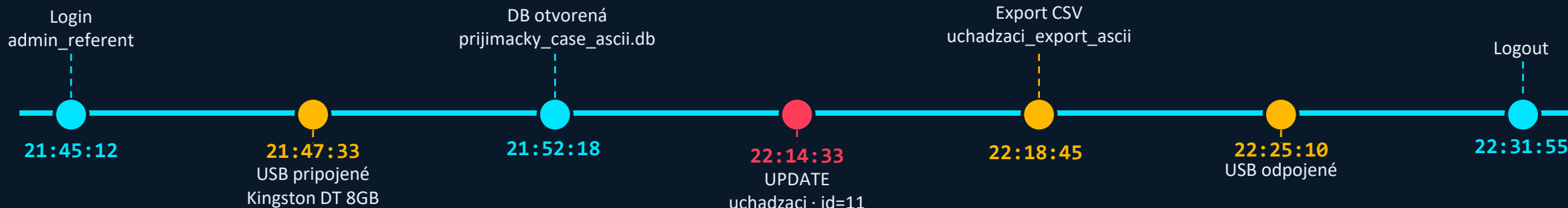
VEĽKOSŤ **326 B**

pomocné poznámky páchatel'a

⚠ *FAT32 nezapíše pri zmazaní fyzicky cez dáta — obsah súborov ostal čitateľný v unallocated space.*

Časová os incidentu • 29. 08. 2025

Data Content				
Hex	Text	Application	File Metadata	OS Account
Data Artifacts				
Analysis Results				
Context				
Annotations				
Other Occurrences				
Table: system_logy 7 entries Page 1 of 1 Export to CSV				
id	cas	udalost	pouzivatel	ip_adresa
1	2025-08-29 21:45:12	Login	admin_referent	192.168.1.45
2	2025-08-29 21:47:33	USB device connected: Kingston DataTraveler 8GB SN:0B8E6B0166E7	admin_referent	192.168.1.45
3	2025-08-29 21:52:18	Database file opened: prijimacky_case_ascii.db	admin_referent	192.168.1.45
4	2025-08-29 22:14:33	UPDATE query executed on table uchadzaci WHERE id=11	admin_referent	192.168.1.45
5	2025-08-29 22:18:45	Export to CSV: uchadzaci_export_ascii.csv	admin_referent	192.168.1.45
6	2025-08-29 22:25:10	USB device disconnected: Kingston DataTraveler 8GB	admin_referent	192.168.1.45
7	2025-08-29 22:31:55	Logout	admin_referent	192.168.1.45



KORELÁCIA Pripojenie USB → otvorenie DB → UPDATE → export → odpojenie USB tvorí súvislú postupnosť = 38 min 22 s

Úmyselná manipulácia referentom – POTVRDENÁ

■ POTVRDENÁ

DÔKAZ 01

Zmena záznamu v databáze
prijimacky_case_ascii.db

Data Content								
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences								
Table uchadzaci 15 entries Page 1 of 1 Export to CSV								
id	meno	priezvisko	rodne_cislo	email	body_po...	body_ak...	datum_zmeny	upravit
1	Jan	Novak	0301015432	novak@email.sk	78	78		
2	Maria	Kovacova	0455126789	kovacova@email.sk	65	65		
3	Peter	Horvath	0312087654	horvath@email.sk	82	82		
4	Lucia	Toth	0501234567	toth@email.sk	71	71		
5	Tomas	Balog	0289765432	balog@email.sk	88	88		
6	Eva	Szabo	0398765431	szabo@email.sk	59	59		
7	Martin	Varga	0276543210	varga@email.sk	92	92		
8	Zuzana	Molnar	0445567890	molnar@email.sk	67	67		
9	Adam	Kiss	0367890123	kiss@email.sk	74	74		
10	Petra	Nagy	0512345678	nagy@email.sk	81	81		
11	Daniel	Farkas	0234567891	farkas@email.sk	45	95	2025-08-29 22:14:33	admin_referent
12	Simona	Olah	0489012345	olah@email.sk	70	70		
13	Filip	Lakatos	0301234567	lakatos@email.sk	85	85		
14	Veronika	Toth	0467890123	veronika.toth@email.sk	63	63		
15	Michal	Bartos	0312345678	bartos@email.sk	77	77		

DÔKAZ 02

Vymazané poznámky páchatela
prijimacky.txt (obnovené)

Page: 1 of 1 Page Matches on page: - of

Poznámky k uprave vysledkov:

Farkas Daniel - id 11
povodne body: 45
nove body: 95
suma: 1500 EUR
splatnost: do tyzdna po zverejneni vysledkov

POZOR: pred zverejnenim vysledkov vymazat histori u

- vymazat .sql skript z USB
- vymazat history v prehliadaci
- vymazat recent files
- naformatovat USB ak by bol problem

-----METADATA-----

DÔKAZ 03

Komunikácia o úprave
komunikacia.txt

Data Content

Hex Text Application File Metadata OS Account Data Artifacts A

Strings Extracted Text Translation

Page: 1 of 1 Page Matches on page: - of - Match

[28.08.2025 14:23] - prijata sprava
"Dobry den, dohodli sme sa na 1500 EUR za upravu bodov pre Farkasa. Body potrebujeme minimalne 90, aby sa dostal. Kedy to bude hotove?"

[28.08.2025 14:45] - odosлана sprava
"Spravim to zajtra vecer ked budem v kancelarii sam. Body upravim na 95 aby to nebolo podozrive ze je to presne 90. Plat sa az po zverejneni oficialnych vysledkov."

[28.08.2025 14:47] - prijata sprava
"OK, dakujem. Suma bude pripravena v hotovosti."

[29.08.2025 22:35] - odosлана sprava
"Hotovo. Body upravene. Vysledky sa zverejnuju v piatok."

-----METADATA-----

ZÁVER H1 Kombinácia troch náleзов preukazuje úmysel, finančný motív aj konkrétny postup manipulácie.

Kompromitácia účtu – NEPOTVRDENÁ

✗ NEPOTVRDENÁ

POSTUP OVERENIA

- ▶ Hash Lookup obrazu (FTK Imager)
- ▶ Analýza systémových logov v DB
- ▶ Prehľadávanie obrazu USB v Autopsy
- ▶ Vyhľadávanie reťazcov v RAM (HxD)
- ▶ Kontrola IP a času prihlásení

ZISTENIA

- ▶ Žiadny škodlivý softvér v obraze
- ▶ Hash Lookup bez zhody so známymi hrozbami
- ▶ Žiadne neštandardné procesy v RAM
- ▶ Žiadna podozrivá sieťová aktivita

USB ako pomocný nosič – POTVRDENÁ

■ POTVRDENÁ

DÔKAZ 01

SQL skript v unallocated space

modify_scores.sql.txt – vymazaný a obnovený

```
Data Content
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results
Strings Extracted Text Translation
Page: 1 of 1 Page Matches on page: - of - Match 100%

-- Skript na upravu vysledkov prijimacieho konania
-- Datum: 29.08.2025
USE prijimacky_db;
-- Uprava bodoveho hodnotenia uchadzaca Daniel Farkas
UPDATE uchadzaci
SET body_aktualne = 95,
    datum_zmeny = '2025-08-29 22:14:33',
    upravil = 'admin_referent'
WHERE id = 11;
COMMIT;
-- Overenie zmeny
SELECT id, meno, priezvisko, body_povodne, body_aktualne
FROM uchadzaci
WHERE id = 11;
```

DÔKAZ 02

Exportovaný CSV súbor

uchadzaci_export_ascii.csv (881 B)

```
Page: 1 of 1 Page Matches on page: - of - Match 100%

id,meno,priezvisko,rodne_cislo,email,body_povodne,body_aktualne,datum_zmeny,upravil
1,Jan,Novak,0301015432,novak@email.sk,78,78,,
2,Maria,Kovacova,0455126789,kovacova@email.sk,65,65,,
3,Peter,Horvath,0312087654,horvath@email.sk,82,82,,
4,Lucia,Toth,0501234567,toth@email.sk,71,71,,
5,Tomas,Balog,0289765432,balog@email.sk,88,88,,
6,Eva,Szabo,0398765431,szabo@email.sk,59,59,,
7,Martin,Varga,0276543210,varga@email.sk,92,92,,
8,Zuzana,Molnar,0445567890,molnar@email.sk,67,67,,
9,Adam,Kiss,0367890123,kiss@email.sk,74,74,,
10,Petra,Nagy,0512345678,nagy@email.sk,81,81,,
11,Daniel,Farkas,0234567891,farkas@email.sk,45,95,2025-08-29 22:14:33,admin_referent
12,Simona,Olah,0489012345,olah@email.sk,70,70,,
13,Filip,Lakatos,0301234567,lakatos@email.sk,85,85,,
14,Veronika,Toth,0467890123,veronika.toth@email.sk,63,63,,
15,Michal,Bartos,0312345678,bartos@email.sk,77,77,,

-----METADATA-----
Content-Encoding: windows-1252
Content-Type: text/plain; charset=windows-1252
X-TIKA:Parsed-By: org.apache.tika.parser.DefaultParser
X-TIKA:Parsed-By-Full-Set: org.apache.tika.parser.DefaultParser
X-TIKA:detectedEncoding: windows-1252
X-TIKA:encodingDetector: UniversalEncodingDetector
```

DÔKAZ 03

Časová korelácia

USB DEVICE CONNECTED: 21:47:33 → USB
DEVICE DISCONNECTED : 22:25:10

2	2025-08-29 21:47:33	USB device connected: Kingston DataTraveler 8GB SN:0B8E6B0166E7
3	2025-08-29 21:52:18	Database file opened: prijimacky_case_ascii.db
4	2025-08-29 22:14:33	UPDATE query executed on table uchadzaci WHERE id=11
5	2025-08-29 22:18:45	Export to CSV: uchadzaci_export_ascii.csv
6	2025-08-29 22:25:10	USB device disconnected: Kingston DataTraveler 8GB

ZÁVER H3 USB bolo použité ako pracovný nosič počas celej operácie manipulácie databázy.

Doplnkové artefakty z RAM image

// HxD STRING SEARCH – RAM image

1.prijimacky_case_ascii.db

názov databázy v pamäti

```
6D1D59390 61 64 73 2F 70 72 69 6A 69 6D 61 63 6B 79 5F 63 ads/prijimacky c
6D1D593A0 61 73 65 5F 61 73 63 69 69 2E 64 62 04 03 00 06 ase_ascii.db....
```

2.uchadzaci_export_ascii.csv

názov exportovaného súboru

```
0014767B0 31 65 30 66 63 38 64 62 62 38 35 37 37 34 34 35 le0fc8dbb8577445
0014767C0 35 37 35 64 39 36 26 76 3D 30 75 63 68 61 64 7A 575d96&v=0uchadz
0014767D0 61 63 69 5F 65 78 70 6F 72 74 5F 61 73 63 69 69 aci_export_ascii
0014767E0 2E 63 73 76 6D 6F 63 2E 74 70 67 74 61 68 63 2E .csvmoc.tpgtahc.
```

3.uchadzaci_export_ascii.csv

názov exportovaného súboru

```
80BAC7D90 4A 11 00 36 15 01 23 02 43 15 01 37 02 02 00 00 0..6..#.C..7....
80BAC7DA0 1C 00 00 05 00 00 09 01 00 00 00 03 00 02 67 6D .....g
80BAC7DB0 6F 64 69 66 79 5F 73 63 6F 72 65 73 2E 73 71 6C odify scores.sql
80BAC7DC0 2E 74 78 74 1F F0 00 97 AA 9D AE 33 5C C0 DC 01 .txt.d.-st03/RÜ.
```

4.prijímačky.txt

otvorenie textového súboru

```
56DA12290 73 74 75 64 65 6E 74 5C 44 65 73 6B 74 6F 70 5C student\Desktop\
56DA122A0 70 72 69 6A ED 6D 61 E8 6B 79 2E 74 78 74 00 00 prijímačky.txt..
56DA122B0 25 00 2E 00 2E 00 5C 00 2E 00 2E 00 5C 00 2E 00 %.....\.....\...
```

WEBOVÁ AKTIVITA

- ▶ Vyhľadávania k zahadzovaniu stôp
- ▶ Hľadanie info o histórii USB v Win

```
001476C10 73 61 38 2E 63 6B 6B 6B 6B 6B 6B 6B 6B 6B 6B 6B y..f.....
001476C50 00 02 08 00 09 68 74 74 70 73 3A 2F 2F 73 75 70 ....https://sup
001476C60 65 72 75 73 65 72 2E 63 6F 6D 2F 71 75 65 73 74 eruser.com/quest
001476C70 69 6F 6E 73 2F 31 35 30 38 34 35 37 2F 77 68 65 ions/1508457/whe
001476C80 72 65 2D 64 6F 65 73 2D 77 69 6E 64 6F 77 73 2D re-does-windows-
001476C90 31 30 2D 73 74 6F 72 65 2D 74 68 65 2D 6C 61 73 l0-store-the-las
001476CA0 74 2D 76 69 73 69 74 65 64 2D 66 69 6C 65 73 2D t-visited-files-
001476CB0 72 65 63 65 6E 74 2D 66 6F 6C 64 65 72 73 2D 61 recent-folders-a
001476CC0 6E 64 2D 66 72 65 71 75 65 6E 74 57 68 65 72 65 ad-frequentWhere
001476CD0 20 64 6F 65 73 20 57 69 6F 6F 6F 77 73 20 31 30 does Windows 10
```

- ▶ Prihlásenie na Facebook krátko po incidente

```
85AF8EF00 30 31 2E 70 64 66 1B 04 02 02 33 1F A6 01 0C 66 01.pdf....3.!.
85AF8EF10 61 63 65 62 6F 6F 6B 20 6C 6F 67 69 6E 20 2E 70 acebook login .p
85AF8EF20 6F 67 12 04 02 02 31 1F A6 01 0C 64 73 69 76 65 ng...l...drive
```

INTERPRETÁCIA

Prítomnosť všetkých kľúčových reťazcov v RAM image potvrdzuje, že databáza, SQL skript aj export boli v čase incidentu na zariadení aktívne otvorené a spracovávané. Webová aktivita zároveň dokumentuje vedomé úsilie páchateľa zahľadiť stopy.

Tri pracovné hypotézy

H1

Úmyselná manipulácia referentom

Referent študijného oddelenia úmyselne upravil výsledky výmenou za finančnú odmenu.

■ POTVRDENÁ

H2

Kompromitácia účtu / externý útočník

Administrátorský účet bol kompromitovaný škodlivým softvérom alebo neoprávneným externým prístupom.

■ ZAMIETNUTÁ

H3

USB ako pomocný nosič

USB zariadenie bolo použité ako pomocný nosič na prenos SQL skriptu, exportu a iných súborov.

■ POTVRDENÁ

Z troch hypotéz boli dve potvrdené a jedna zamietnutá – manipulácia bola úmyselným interným konaním, nie externým útokom.

Záverečné zistenia a odporúčania

HLAVNÝ ZÁVER

Manipulácia databázy prijímacieho konania bola **úmyselné interné konanie** používateľa účtu **admin_referent**. Externý útok bol vyvrátený. USB slúžilo ako pomocný nosič SQL skriptu, exportu a poznámok.

2 / 3

Hypotézy potvrdené

38 min

Trvanie manipulácie

1500 €

Identifikovaná odmena

ODPORÚČANIA

01

Audit databázy a logov

Pravidelná kontrola UPDATE príkazov nad citlivými tabuľkami.

02

Dvojfaktorové overenie

MFA pre administrátorské účty informačného systému.

03

Zákaz USB na pracovných staniciach

Politika BIOS / endpoint protection na blokovanie médií.

04

Disciplinárne / trestné konanie

Postúpiť dôkazy zodpovedným orgánom UCM.

// END OF REPORT

ĎAKUJEM ZA POZORNOSŤ

Otázky a diskusia

Ľubomír Zubák

CASE - 2025 - PRIJ - 01

Univerzita sv. Cyrila a Metoda v Trnave · Fakulta prírodných vied · 2025/2026