PENETRAČNÉ TESTOVANIE

Správa pre *vedenie.*

DontBeHacked s. r. o. — účtovný a mzdový systém. Testovacie obdobie 1. – 7. apríl 2026.

KLIENT	OBDOBIE	TESTER	DÁTUM SPRÁVY
DontBeHacked s. r. o.	1. – 7. 4. 2026	Nabu technologies	8. apríl 2026

Identifikované *kritické ohrozenie.*

KRITICKÁ ZÁVAŽNOSŤ

Počas testovania sme identifikovali zraniteľnosť, ktorá útočníkovi z internetu umožňuje získať prístup k **mzdovým a osobným údajom všetkých zákazníkov systému DontBeHacked** — vrátane rodných čísel, výplatných pások a bankových účtov. Na zneužitie postačí bežný trial účet a voľne dostupné nástroje.

Celkovo sme identifikovali **7 bezpečnostných nálezov** — jeden kritickej, dva vysokej, dva strednej a dva informatívnej závažnosti.

1	2	2	2
KRITICKÝ	**VYSOKÉ**	**STREDNÉ**	**INFORMATÍVNE**
Existenčné ohrozenie	Vážna, zotaviteľná škoda	Významná expozícia	Hygienické pozorovania

02 • BIZNIS DOPAD

Čo to znamená pre *vašu firmu.*

Najzávažnejší nález sa týka spôsobu, akým systém DontBeHacked overuje prístup k programovému rozhraniu. Útočník dokáže bez prihlasovacích údajov čítať dáta všetkých zákazníkov.

Únik osobných údajov

Prístup k menám, rodným číslam, adresám a bankovým účtom. Rozsah: **~ 85 000 zamestnancov** naprieč všetkými zákazníkmi.

Únik mzdových údajov

Kompletné výplatné pásky, mzdové zložky, odvody a daňové podklady. GDPR čl. 9, zákon č. 18/2018 Z. z.

Regulačné dôsledky

Sankcia ÚOOÚ až **4 % ročného obratu** podľa GDPR čl. 83. Povinné oznamovanie dotknutým osobám.

Reputačné riziko

Zákazníci DontBeHacked zverujú systému najcitlivejšie údaje svojich zamestnancov. Verejný únik sa rovná strate dôvery a odchodu klientov.

Zoznam identifikovaných *problémov.*

Sedem potvrdených nálezov zoradených podľa závažnosti. Technické detaily, reprodukčné kroky a odporúčania na opravu sú v samostatnom **technickom reporte** určenom pre vývojový tím.

F-01	KRITICKÝ	Neoprávnený prístup k mzdovým údajom všetkých zákazníkov cez API bez autorizácie	POTVRDENÝ
F-02	VYSOKÝ	Zraniteľná knižnica umožňujúca vzdialené spustenie kódu na aplikačnom serveri	POTVRDENÝ
F-03	VYSOKÝ	Prístupové kľúče k cloudovému úložisku vložené priamo do mobilnej aplikácie	POTVRDENÝ
F-04	STREDNÝ	Administrátorské rozhranie prístupné z ľubovoľnej IP bez sieťového obmedzenia	POTVRDENÝ
F-05	STREDNÝ	Chýbajúce obmedzenie počtu pokusov o prihlásenie (rate limiting)	POTVRDENÝ
F-06	INFO	Zastarané verzie pomocných knižníc s publikovanými opravami, bez známeho zneužitia v kontexte aplikácie	POZOROVANIE
F-07	INFO	Chýbajúce bezpečnostné HTTP hlavičky na webovom portáli	POZOROVANIE

Fakturovateľné sú nálezy kritickej, vysokej a strednej závažnosti; informatívne pozorovania sú súčasťou správy bez poplatku. V zmysle zmluvy sa fakturuje **výlučne za najzávažnejší nález** — F-01.

Odporúčané *priority.*

01

F-01 — Neoprávnený prístup k API

Nasadiť autorizačnú kontrolu na payroll endpointoch. Odhad prácnosti: 1 – 2 pracovné dni.

DO 48 HODÍN

02

F-03 — Prístupové kľúče v mobilnej aplikácii

Rotovať kľúče, nahradiť za server-generované SAS tokeny s obmedzenou platnosťou. Skontrolovať log prístupov za posledných 90 dní.

DO 7 DNÍ

03

F-02 — Zraniteľná deserializácia

Zmeniť konfiguráciu JSON knižnice, prípadne migrovať na bezpečnú alternatívu. Regresné testovanie API.

NAJBLIŽŠÍ RELEASE

04

F-04 a F-05 — Admin panel, rate limiting

Obmedziť admin portál na firemný VPN alebo IP whitelist. Nasadiť rate limiting na prihlasovací endpoint (max 5 pokusov / 15 min).

NAJBLIŽŠÍ RELEASE

Čo bolo *testované.*

PARAMETER	HODNOTA
Aktíva	Webový portál (**app.dontbehacked.sk**), REST API (**api.dontbehacked.sk**), mobilná aplikácia Android (v 4.2.1), administrátorský portál (**admin.dontbehacked.sk**), 38 identifikovaných subdomén.
Metodológia	OWASP Testing Guide v4.2, PTES a NIST SP 800-115. Tri fázy: automatizované skenovanie, statická analýza a manuálne testovanie. Nálezy boli validované expertnou kontrolou pred zápisom do správy.
Obmedzenia	Nepokrýva internú sieť, fyzickú bezpečnosť, sociálne inžinierstvo ani systémy tretích strán. Bez deštruktívneho testovania — dôkazy boli zbierané cez nedeštruktívne reprodukčné cesty.

06 • ĎALŠIE KROKY

Odporúčaný *harmonogram.*

#	KROK	TERMÍN
1	Záverečná konzultácia s technickým tímom a vedením (1 hodina, vzdialene)	Do 5 pracovných dní
2	Oprava kritického nálezu F-01	Do 48 hodín
3	Lehota na prípadné námietky voči závažnosti nálezov	14 kalendárnych dní
4	Bezplatné opakované overenie opráv (max. 3× na nález)	Do 60 dní

Obmedzenie rozsahu a platnosti. Táto správa opisuje nálezy identifikované počas penetračného testovania v období 1. – 7. apríla 2026 na aktívach definovaných v sekcii 05. Testovanie je bodové overenie — odzrkadľuje stav systémov v čase vykonania; neskoršie zmeny môžu priniesť nové zraniteľnosti. Metodológia pokrýva najčastejšie triedy zraniteľností, ale nie je vyčerpávajúca; absencia nálezu neznamená absenciu zraniteľnosti. Správa nepredstavuje certifikáciu zhody s bezpečnostnými normami. Odporúčame pravidelné opakovanie testovania minimálne každých 6 mesiacov alebo po významných zmenách systému.